Tohoku Math. J.
60 (2008), 183–218

TWISTED KUMMER AND KUMMER-ARTIN-SCHREIER THEORIES

NORIYUKI SUWA

(Received July 27, 2006, revised August 21, 2007)

Abstract. We discuss an analogue of the Kummer and Kummer-Artin-Schreier theories, twisting by a quadratic extension. 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 common to deduce the Kummer theory from an exact sequence of algebraic groups over a field K:

$$0 \longrightarrow \boldsymbol{\mu}_{n,K} \longrightarrow \boldsymbol{G}_{m,K} \xrightarrow{n} \boldsymbol{G}_{m,K} \longrightarrow 0 . \tag{1}$$

If n is invertible in K and all the n-th roots of unity are contained in K, the group scheme $\boldsymbol{\mu}_{n,K}$ is isomorphic to the constant group scheme $\boldsymbol{Z}/n\boldsymbol{Z}$. Hence it follows from the Hilbert 90 that the exact sequence (1) yields an isomorphism

$$K^{\times}/n \xrightarrow{\sim} H^1(K, \boldsymbol{Z}/n\boldsymbol{Z}) = \mathrm{Hom}_{\mathrm{cont}}(\varPi_K, \boldsymbol{Z}/n\boldsymbol{Z}) ,$$

where $\varPi_K$ denotes the absolute Galois group of K.

However, if the field K does not contain all the n-th roots of unity, the Kummer theory does not work any longer, which requires us to modify the theory. Recently Komatsu [6] formulated a descent Kummer theory, twisting the Kummer theory by a quadratic extension. In this article, we give a formulation and a generalization of the descent Kummer theory developed in [6] in the framework of group schemes.

Now we explain the contents of the article. In Section 1, we recall the Kummer, Artin-Schreier and Kummer-Artin-Schreier theories in the framework of group schemes. This shows us a way to develop twisted Kummer and Kummer-Artin-Schreier theories. In Section 2, we define group schemes $U_{B/A}$ and $G_{B/A}$, which are needed to describe the twisted Kummer and twisted Kummer-Artin-Schreier theories. The first half of the section is devoted to statements on elementary facts concerning the group schemes $U_{B/A}$ and $G_{B/A}$. In particular, we have two exact sequences of group schemes

$$0 \longrightarrow U_{B/A} \longrightarrow \prod_{B/A} \boldsymbol{G}_{m,B} \xrightarrow{\mathrm{Nr}} \boldsymbol{G}_{m,A} \longrightarrow 0 \tag{2}$$

2000 *Mathematics Subject Classification.* Primary 13B05; Secondary 14L15, 12G05.
Partially supported by Grant-in-Aid for Scientific Research No.16540040.

and

$$0 \longrightarrow \boldsymbol{G}_{m,A} \xrightarrow{i} \prod_{B/A} \boldsymbol{G}_{m,B} \longrightarrow G_{B/A} \longrightarrow 0\,, \tag{3}$$

where A is a ring, B is a quadratic extension of A and $\prod_{B/A}$ denotes the Weil restriction functor with respect to the extension B/A (cf. 2.1). The sequence (2) plays an important role in the twisted Kummer theory, and the sequence (3) in the twisted Kummer-Artin-Schreier theory. These two exact sequences enable us to calculate the cohomology groups with coefficients in $U_{B/A}$ and $G_{B/A}$, notably to establish the Hilbert 90 for $U_{B/A}$ and $G_{B/A}$ (Proposition 2.6). We owe the description of the group scheme $G_{B/A}$ to Waterhouse-Weisfeiler [15].

In the latter half of Section 2, we construct equivariant compactifications $\iota : G_{B/A} \to \boldsymbol{P}^1_A$ and $\iota : U_{B/A} \to \boldsymbol{P}^1_A$. Our starting point is a commutative diagram with exact rows of group schemes

$$\begin{array}{ccccccccc}
0 & \longrightarrow & \boldsymbol{G}_{m,A} & \longrightarrow & \prod_{B/A} \boldsymbol{G}_{m,B} & \longrightarrow & G_{B/A} & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow{\scriptstyle \rho} & & \downarrow{\scriptstyle \tilde{\rho}} & & \\
1 & \longrightarrow & \boldsymbol{G}_{m,A} & \longrightarrow & GL(2) & \longrightarrow & PGL(2) & \longrightarrow & 1\,,
\end{array}$$

where $\rho : \prod_{B/A} \boldsymbol{G}_{m,B} \to GL(2, A)$ is a regular representaion.

Section 3 is devoted to a description of an exact sequence of group schemes over $\boldsymbol{Z}[\omega, 1/n]$

$$0 \longrightarrow \boldsymbol{Z}/n\boldsymbol{Z} \longrightarrow U_{B/A} \xrightarrow{n} U_{B/A} \longrightarrow 0\,, \tag{4}$$

where n is a positive integer ≥ 3 and $\omega = e^{2\pi i/n} + e^{-2\pi i/n}$ (Theorem 3.2). Calculating cohomology groups of the sequence (4) together with the Hilbert 90 for $U_{B/A}$, we obtain the following

COROLLARY 3.3. *Let R be a local $\mathbf{Z}[\omega, 1/n]$-algebra. If n is odd, $H^1(R, \mathbf{Z}/n\mathbf{Z})$ is isomorphic to $U_{B/A}(R)/n$.*

This was established by Komatsu [6] in a different manner when R is a field. Moreover, using an equivariant compactification $\iota : U_{B/A} \to \boldsymbol{P}^1_A$, we arrive at the following assertion.

COROLLARY 3.12. *Let R be a local $\mathbf{Z}[\omega, 1/n]$-algebra and S an unramified cyclic extension of degree n. If n is odd, there exists a morphism* Spec $R \to \boldsymbol{P}^1_A$ *such that the square of rational maps*

$$\begin{array}{ccc}
\operatorname{Spec} S & \longrightarrow & \boldsymbol{P}^1_A \\
\downarrow & & \downarrow{\scriptstyle \nu} \\
\operatorname{Spec} R & \longrightarrow & \boldsymbol{P}^1_A
\end{array}$$

is cartesian.

The cyclic covering $\nu : \boldsymbol{P}^1_A \to \boldsymbol{P}^1_A$ is defined in Lemma 3.11. In a certain sence the rational map ν is a geometric expression of the generic polynomial for cyclic extensions of degree n, discovered by Rikuna [7].

Section 4 is devoted to a description of an exact sequence of group schemes over $\boldsymbol{Z}[\omega]$

$$0 \longrightarrow \boldsymbol{Z}/p\boldsymbol{Z} \longrightarrow G_{B/A} \xrightarrow{\Psi} G_{\tilde{B}/A} \longrightarrow 0\,, \tag{5}$$

where p is an odd prime and $\omega = e^{2\pi i/p} + e^{-2\pi i/p}$ (Theorem 4.2). Calculating cohomology groups of the sequence (5) together with the Hilbert 90 for $G_{B/A}$, we obtain the following

COROLLARY 4.3. *Let R be a local $\mathbf{Z}[\omega]$-algebra. Then $H^1(R, \boldsymbol{Z}/p\boldsymbol{Z})$ is isomorphic to* $\mathrm{Coker}[\Psi : G_{B/A}(R) \to G_{\tilde{B}/A}(R)]$.

Furthermore, using an equivariant compactification $\iota : G_{B/A} \to \boldsymbol{P}^1_A$, we also arrive at the following assertion.

COROLLARY 4.7. *Let R be a local $\boldsymbol{Z}[\omega]$-algebra and S an unramified cyclic extension of degree p. Then there exists a morphism* $\mathrm{Spec}\, R \to \boldsymbol{P}^1_A$ *such that the square*

$$\begin{array}{ccc} \mathrm{Spec}\, S & \longrightarrow & \boldsymbol{P}^1_A \\ \big\downarrow & & \big\downarrow \Psi \\ \mathrm{Spec}\, R & \longrightarrow & \boldsymbol{P}^1_A \end{array}$$

is cartesian.

The cyclic covering $\Psi : \boldsymbol{P}^1_A \to \boldsymbol{P}^1_A$ is defined in Lemma 4.6. In a sence the morphism Ψ is a geometric expression of the everywhere generic polynomial for cyclic extensions of degree p, discovered by Komatsu [6].

The author expresses his gratitude to Boris Kunyavski for valuable discussions at Stellenbosch under the Southern Cross. The author thanks also the referee for his careful reading of the munuscript.

NOTATION. For a commutative ring R, the multiplicative group $\boldsymbol{G}_m(R)$ is denoted by $R^\times$.

For a commutative group M and an endomorphim φ of M, ${}_\varphi M$ and M/φ stand for $\mathrm{Ker}[\varphi : M \to M]$ and $\mathrm{Coker}[\varphi : M \to M]$, respectively.

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.

- $\boldsymbol{G}_{a,A}$: the additive group scheme over A
- $\boldsymbol{G}_{m,A}$: the multiplicative group scheme over A
- $\boldsymbol{\mu}_{n,A}$: $\mathrm{Ker}[n : \boldsymbol{G}_{m,A} \to \boldsymbol{G}_{m,A}]$
- $GL(2)$: the general linear group scheme over A

$PGL(2)$: the projective linear group scheme over A
$\mathcal{G}^{(\lambda)}$: recalled in 1.3
$U_{B/A}, G_{B/A}$: defined in 2.2 and in 2.3, respectively

LIST OF MORPHISMS AND RATIONAL MAPS.
$\alpha^{(\lambda)} : \mathcal{G}^{(\lambda)} \to \boldsymbol{G}_{m,A}$: recalled in 1.3
$s : U_{B/A} \otimes_A B \to \boldsymbol{G}_{m,B}, \sigma : G_{B/A} \otimes_A B \to \mathcal{G}^{(\lambda)}$: defined in 2.2
$\alpha : G_{B/A} \to U_{B/A}, \beta : U_{B/A} \to G_{B/A}$: defined in 2.3
$\iota : G_{B/A} \to \boldsymbol{P}^1_A$: the open immersion defined in 2.9
$\iota : U_{B/A} \to \boldsymbol{P}^1_A$: defined in 2.11
$\sigma : \boldsymbol{P}^1_B \to \boldsymbol{P}^1_B, s : \boldsymbol{P}^1_B \to \boldsymbol{P}^1_B$: defined in 2.12

1. Recall: Kummer and Kummer-Artin-Schreier theories. In this section, we recall the Kummer, Artin-Schreier and Kummer-Artin-Schreier theories. We refer to [1] or [13] on formalisms of affine group schemes, Hopf algebras and the cohomology with coefficients in group schemes.

1.1. (Kummer theory). Let $\boldsymbol{G}_m = \operatorname{Spec} \boldsymbol{Z}[U, 1/U]$ denote the multiplicative group scheme. The multiplication is given by $U \mapsto U \otimes U$.

Let n be an integer ≥ 2 and ζ a primitive n-th root of unity. Then $\boldsymbol{\mu}_n = \operatorname{Ker}[n : \boldsymbol{G}_m \to \boldsymbol{G}_m]$ is isomorphic to the constant group scheme $\boldsymbol{Z}/n\boldsymbol{Z}$ over $\boldsymbol{Z}[\zeta, 1/n]$. Hence, if X is a $\boldsymbol{Z}[\zeta, 1/n]$-scheme, the exact sequence of group schemes (called Kummer sequence)

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

induces a long exact sequence

$$\begin{aligned} 0 \longrightarrow H^0(X, \boldsymbol{Z}/n\boldsymbol{Z}) \longrightarrow H^0(X, \boldsymbol{G}_m) \xrightarrow{n} H^0(X, \boldsymbol{G}_m) \\ \longrightarrow H^1(X, \boldsymbol{Z}/n\boldsymbol{Z}) \longrightarrow H^1(X, \boldsymbol{G}_m) \xrightarrow{n} H^1(X, \boldsymbol{G}_m) \longrightarrow \cdots . \end{aligned}$$

Furthermore, we obtain an exact sequence

$$0 \to \Gamma(X, \mathcal{O})^\times/n \to H^1(X, \boldsymbol{Z}/n\boldsymbol{Z}) \to {}_n\operatorname{Pic}(X) \to 0 ,$$

noting $H^1(X, \boldsymbol{G}_m) = \operatorname{Pic}(X)$ (Hilbert 90).

In particular, if $X = \operatorname{Spec} K$ (K is a field), we have an isomorphism

$$K^\times/n \xrightarrow{\sim} H^1(K, \boldsymbol{Z}/n\boldsymbol{Z}) ,$$

which implies that $t^n - u \in K(u)[t]$ is a generic polynomial for $\boldsymbol{Z}/n\boldsymbol{Z}$-extensions of K.

1.2. (Artin-Schreier theory). Let $\boldsymbol{G}_a = \operatorname{Spec} \boldsymbol{Z}[T]$ denote the additive group scheme. The addition is defined by $T \mapsto T \otimes 1 + 1 \otimes T$.

Let p be a prime number. Then $\operatorname{Ker}[F - 1 : \boldsymbol{G}_{a,\boldsymbol{F}_p} \to \boldsymbol{G}_{a,\boldsymbol{F}_p}]$ is isomorphic to the constant group scheme $\boldsymbol{Z}/p\boldsymbol{Z}$, where F denotes the Frobenius endomorphism. Hence, if X is an $\boldsymbol{F}_p$-scheme, the exact sequence of group schemes (called Artin-Schreier sequence)

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

induces a long exact sequence

$$\begin{aligned}0 \longrightarrow H^0(X, \boldsymbol{Z}/p\boldsymbol{Z}) \longrightarrow H^0(X, \boldsymbol{G}_{a,\boldsymbol{F}_p}) \xrightarrow{F-1} H^0(X, \boldsymbol{G}_{a,\boldsymbol{F}_p}) \\ \longrightarrow H^1(X, \boldsymbol{Z}/p\boldsymbol{Z}) \longrightarrow H^1(X, \boldsymbol{G}_{a,\boldsymbol{F}_p}) \xrightarrow{F-1} H^1(X, \boldsymbol{G}_{a,\boldsymbol{F}_p}) \longrightarrow \cdots .\end{aligned}$$

Furthermore, we obtain an exact sequence

$$0 \to \Gamma(X, \mathcal{O})/(F-1) \to H^1(X, \boldsymbol{Z}/p\boldsymbol{Z}) \to {}_{F-1}H^1(X, \mathcal{O}) \to 0,$$

noting $H^1(X, \boldsymbol{G}_a) = H^1(X, \mathcal{O})$.

In particular, if $X = \operatorname{Spec} K$ (K is a field), we have an isomorphism

$$K/(F-1) \xrightarrow{\sim} H^1(K, \boldsymbol{Z}/p\boldsymbol{Z}),$$

which implies that $t^p - t - u \in K(u)[t]$ is a generic polynomial for $\boldsymbol{Z}/p\boldsymbol{Z}$-extensions of K.

DEFINITION 1.3. Let A be a ring and $\lambda \in A$. We define a group A-scheme $\mathcal{G}^{(\lambda)}$ by

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

with

(1) the multiplication: $T \mapsto T \otimes 1 + 1 \otimes T + \lambda T \otimes T$;
(2) the unit: $T \mapsto 0$;
(3) the inverse: $T \mapsto -\dfrac{T}{1+\lambda T}$.

Moreover, we define a homomorphism of group A-schemes

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

by

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

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

Let B be an A-algebra. It is known that $H^1(B, \mathcal{G}^{(\lambda)}) = 0$ if B is a local ring or if λ is nilpotent in B ([10], 1.3 and 1.4).

1.4. (Kummer-Artin-Schreier theory). Let p be a prime number and ζ a primitive p-th root of unity. Put $A = \boldsymbol{Z}[\zeta]$, $K = \boldsymbol{Q}(\zeta)$ and $\lambda = \zeta - 1$. Then we have

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

and

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

A homomorphism of group A-schemes

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

is defined by

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

Then it is verified that $\mathrm{Ker}[\Psi : \mathcal{G}^{(\lambda)} \to \mathcal{G}^{(\lambda^p)}]$ is isomorphic to the constant group scheme $\boldsymbol{Z}/p\boldsymbol{Z}$. We obtain an exact sequence of group schemes

$$(\#) \qquad 0 \longrightarrow \boldsymbol{Z}/p\boldsymbol{Z} \longrightarrow \mathcal{G}^{(\lambda)} \xrightarrow{\Psi} \mathcal{G}^{(\lambda^p)} \longrightarrow 0\,.$$

Furthermore, the sequence $(\#) \otimes_A K$ is isomorphic to the Kummer sequence

$$0 \longrightarrow \boldsymbol{\mu}_{p,K} \longrightarrow \boldsymbol{G}_{m,K} \xrightarrow{p} \boldsymbol{G}_{m,K} \longrightarrow 0\,.$$

On the other hand, the residue ring $A/(\lambda)$ is isomorphic to the finite field $\boldsymbol{F}_p$, and the sequence $(\#) \otimes_A \boldsymbol{F}_p$ is isomorphic to the Artin-Schreier sequence

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

Let X be an A-scheme. Then the exact sequence of group schemes (#) induces a long exact sequence

$$\begin{aligned} 0 &\longrightarrow H^0(X, \boldsymbol{Z}/p\boldsymbol{Z}) \longrightarrow H^0(X, \mathcal{G}^{(\lambda)}) \xrightarrow{\Psi} H^0(X, \mathcal{G}^{(\lambda^p)}) \\ &\longrightarrow H^1(X, \boldsymbol{Z}/p\boldsymbol{Z}) \longrightarrow H^1(X, \mathcal{G}^{(\lambda)}) \xrightarrow{\Psi} H^1(X, \mathcal{G}^{(\lambda^p)}) \longrightarrow \cdots\,. \end{aligned}$$

In particular, if $X = \mathrm{Spec}\, B$ (B is a local A-algebra), we have an isomorphism

$$\mathrm{Coker}[\Psi : \mathcal{G}^{(\lambda)}(B) \longrightarrow \mathcal{G}^{(\lambda^p)}(B)] \xrightarrow{\sim} H^1(B, \boldsymbol{Z}/p\boldsymbol{Z})\,.$$

One may say that $\{(\lambda t+1)^p - 1\}/\lambda^p - u \in A[u][t]$ is a *generic* polynomial for $\boldsymbol{Z}/p\boldsymbol{Z}$-extensions of A.

REMARK 1.5. The exact sequence (#) was discovered independently by Waterhouse [14] and [11]. The equation

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

ascends to the work of Furtwängler [2, 3].

2. Group schemes. In this section, we fix a ring A, $r, s \in A$ and $B = A[t]/(t^2 - rt + s)$.

2.1. Let A be a ring and $r,\ s \in A$. Put $D = r^2 - 4s$ and $B = A[t]/(t^2 - rt + s)$. Let ε denote the image of t in B. Then $B = A[\varepsilon]$ and $\varepsilon^2 - r\varepsilon + s = 0$. The functor $R \mapsto (R \otimes_A B)^\times$ is represented by the group scheme (the Weil restriction of $\boldsymbol{G}_{m,B}$ to B/A)

$$\prod_{B/A} \boldsymbol{G}_{m,B} = \mathrm{Spec}\, A\left[U, V, \frac{1}{U^2 + rUV + sV^2}\right]$$

with

(a) the multiplication

$$U \mapsto U \otimes U - sV \otimes V\,, \quad V \mapsto U \otimes V + V \otimes U + rV \otimes V\,;$$

(b) the unit

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

(c) the inverse

$$U \mapsto \frac{U + rV}{U^2 + rUV + sV^2}\,, \quad V \mapsto \frac{-V}{U^2 + rUV + sV^2}\,.$$

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

$$i : \boldsymbol{G}_{m,A} = \operatorname{Spec} A\left[T, \frac{1}{T}\right] \to \prod_{B/A} \boldsymbol{G}_{m,B} = \operatorname{Spec} A\left[U, V, \frac{1}{U^2 + rUV + sV^2}\right],$$

defined by

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

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

$$\mathrm{Nr} : \prod_{B/A} \boldsymbol{G}_{m,B} = \operatorname{Spec} A\left[U, V, \frac{1}{U^2 + rUV + sV^2}\right] \to \boldsymbol{G}_{m,A} = \operatorname{Spec} A\left[T, \frac{1}{T}\right],$$

defined by

$$T \mapsto U^2 + rUV + sV^2\,.$$

It is readily seen that

(1) $i : \boldsymbol{G}_{m,A} \to \prod_{B/A} \boldsymbol{G}_{m,B}$ is a closed immersion;

(2) $\mathrm{Nr} : \prod_{B/A} \boldsymbol{G}_{m,B} \to \boldsymbol{G}_{m,A}$ is faithfully flat;

(3) $\mathrm{Nr} \circ i : \boldsymbol{G}_{m,A} \to \boldsymbol{G}_{m,A}$ is the square map.

DEFINITION 2.2. Put

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

Then

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

with

(a) the multiplication

$$U \mapsto U \otimes U - sV \otimes V\,, \quad V \mapsto U \otimes V + V \otimes U + rV \otimes V\,;$$

(b) the unit

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

(c) the inverse

$$U \mapsto U + rV\,, \quad V \mapsto -V\,.$$

If D is invertible in A, $U_{B/A}$ is a torus over A. More generally, if D is not nilpotent in A, $U_{B/A} \otimes_A A[1/D]$ is a torus over $A[1/D]$, splitting over $B[1/D]$. In fact, $T \mapsto U + \varepsilon V$ defines a homomorphism

$$\sigma : U_{B/A} \otimes_A B = \operatorname{Spec} B[U, V]/(U^2 + rUV + sV^2 - 1) \to \boldsymbol{G}_{m,B} = \operatorname{Spec} B\left[T, \frac{1}{T}\right],$$

inducing an isomorphism over $B[1/D]$. The inverse of $\sigma \otimes_A B[1/D]$ is given by

$$U \mapsto \frac{1}{2\varepsilon - r}\left\{(\varepsilon - r)T + \frac{\varepsilon}{T}\right\}, \quad V \mapsto \frac{1}{2\varepsilon - r}\left(T - \frac{1}{T}\right).$$

DEFINITION 2.3 (Waterhouse-Weisfeiler [15]). We define a group scheme $G_{B/A}$ over A by

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

with

(a) the multiplication

$$X \mapsto X \otimes 1 + 1 \otimes X - rX \otimes X - 2sX \otimes Y - 2sY \otimes X - rsY \otimes Y\,,$$
$$Y \mapsto Y \otimes 1 + 1 \otimes Y + (r^2 - 2s)Y \otimes Y + rX \otimes Y + rY \otimes X + 2X \otimes X\,;$$

(b) the unit

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

(c) the inverse

$$X \mapsto -X - rY\,, \quad Y \mapsto Y\,.$$

Then $G_{B/A}$ is smooth over A.

Furthermore, a homomorphism of group schemes

$$\gamma : \prod_{B/A} \boldsymbol{G}_{m,B} = \operatorname{Spec} A\left[U, V, \frac{1}{U^2 + rUV + sV^2}\right]$$
$$\to G_{B/A} = \operatorname{Spec} A[X, Y]/(X^2 + rXY + sY^2 - Y)$$

is defined by

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

It is readily seen that the sequence

$$0 \longrightarrow \boldsymbol{G}_{m,A} \xrightarrow{i} \prod_{B/A} \boldsymbol{G}_{m,B} \xrightarrow{\gamma} G_{B/A} \longrightarrow 0$$

is exact.

The two group schemes $U_{B/A}$ and $G_{B/A}$ are related by a homomorphism

$$\begin{aligned}\alpha : G_{B/A} &= \operatorname{Spec} A[X, Y]/(X^2 + rXY + sY^2 - Y) \\ \to U_{B/A} &= \operatorname{Spec} A[U, V]/(U^2 + rUV + sV^2 - 1)\end{aligned}$$

defined by

$$U \mapsto 1 - rX - 2sY\,, \quad V \mapsto 2X + rY\,.$$

If D is invertible in A, α is an isomorphism. More generally, if D is not nilpotent in A, α is isomorphic over $A[1/D]$. Indeed, the inverse of $\alpha \otimes_A A[1/D]$ is given by

$$X \mapsto \frac{r - rU - 2sV}{D}\,, \quad Y \mapsto \frac{-2 + 2U + rV}{D}\,.$$

We define also a homomorphism

$$\begin{aligned}\beta : U_{B/A} &= \operatorname{Spec} A[U, V]/(U^2 + rUV + sV^2 - 1) \\ \to G_{B/A} &= \operatorname{Spec} A[X, Y]/(X^2 + rXY + sY^2 - Y)\end{aligned}$$

as the composite

$$U_{B/A} \longrightarrow \prod_{B/A} \boldsymbol{G}_{m,B} \xrightarrow{\gamma} G_{B/A}.$$

Then β is given by

$$X \mapsto UV\,, \quad Y \mapsto V^2\,,$$

and therefore,

$$\begin{aligned}\alpha \circ \beta : U_{B/A} &= \operatorname{Spec} A[U, V]/(U^2 + rUV + sV^2 - 1) \\ \to U_{B/A} &= \operatorname{Spec} A[U, V]/(U^2 + rUV + sV^2 - 1)\end{aligned}$$

is given by

$$U \mapsto 1 - rUV - 2sV^2 = U^2 - sV^2\,, \quad V \mapsto 2UV + rV^2\,,$$

that is, $\alpha \circ \beta$ is the square map.

Put $\lambda = 2\varepsilon - r \in B$. Then

$$T \mapsto X + \varepsilon Y\,, \quad \frac{1}{1 + \lambda T} \mapsto 1 - \lambda\{X + (r - \varepsilon)Y\}$$

defines an isomorphism over B

$$\begin{aligned}\sigma : G_{B/A} \otimes_A B &= \operatorname{Spec} B[X, Y]/(X^2 + rXY + sY^2 - Y) \\ \xrightarrow{\sim} \mathcal{G}^{(\lambda)} &= \operatorname{Spec} B\left[T, \frac{1}{1 + \lambda T}\right].\end{aligned}$$

The inverse of σ is given by

$$X \mapsto \frac{T - (r - \varepsilon)T^2}{1 + \lambda T}\,, \quad Y \mapsto \frac{T^2}{1 + \lambda T}\,.$$

Furthermore the diagram of group B-schemes

$$\begin{array}{ccc} G_{B/A}\otimes_A B & \xrightarrow[\sigma]{\sim} & \mathcal{G}^{(\lambda)} \\ {\scriptstyle \alpha\otimes I_B}\downarrow & & \downarrow{\scriptstyle \alpha^{(\lambda)}} \\ U_{B/A}\otimes_A B & \xrightarrow[\sigma]{} & \boldsymbol{G}_{m,B} \end{array}$$

is commutative.

REMARK 2.4.1. It is verified without difficulty that the composite $\beta\circ\alpha : G_{B/A}\to G_{B/A}$ is the square map.

REMARK 2.4.2. Assume that D is not invertible in A, and put $A_0 = A/(D)$. If 2 is invertible in A_0, the group scheme $G_{B/A}\otimes_A A_0$ is isomorphic to the additive group scheme $\boldsymbol{G}_{a,A_0}$. Indeed,

$$\begin{aligned} G_{B/A}\otimes_A A_0 &= \operatorname{Spec} A_0[X,Y]/(X^2+rXY+sY^2-Y) \\ &= \operatorname{Spec} A_0[X,Y]/\Big(\Big(X+\frac{r}{2}Y\Big)^2 - Y\Big), \end{aligned}$$

and $X\mapsto S-(r/2)S^2$, $Y\mapsto S^2$ defines a isomorphism

$$\boldsymbol{G}_{a,A_0} = \operatorname{Spec} A_0[S] \xrightarrow{\sim} G_{B/A}\otimes_A A_0 = \operatorname{Spec} A_0[X,Y]/\Big(\Big(X+\frac{r}{2}Y\Big)^2 - Y\Big).$$

Furthermore, if D is a non zero divisor in A, we have an exact sequence

$$0\longrightarrow G_{B/A}(A) \xrightarrow{\alpha} U_{B/A}(A) \longrightarrow U_{B/A}(A_0)\,.$$

Indeed, let $u, v\in A$ with $u^2+ruv+sv^2=1$, and assume that $u\equiv 1 \mod D$, $v\equiv 0 \mod D$. Putting $u = 1+D\alpha$, $v = D\beta$ ($\alpha,\beta\in A$), we obtain

$$(2\alpha+r\beta)+D(\alpha^2+r\alpha\beta+s\beta^2)=0\,.$$

Put now $x=-r\alpha-2s\beta$, $y=2\alpha+r\beta$. Then we see that

$$(x^2+rxy+sy^2)-y = -D(\alpha^2+r\alpha\beta+s\beta^2)-(2\alpha+r\beta)=0$$

and

$$\alpha(x,y) = (1+D\alpha, D\beta)\,.$$

2.5. Let X be an A-scheme. Then the exact sequence of group schemes

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

induces a long exact sequence

$$\begin{aligned}
0 &\longrightarrow \Gamma(X, U_{B/A}) \longrightarrow \Gamma(X \otimes_A B, \boldsymbol{G}_m) \xrightarrow{\text{Nr}} \Gamma(X, \boldsymbol{G}_m) \\
&\longrightarrow H^1(X, U_{B/A}) \longrightarrow \operatorname{Pic}(X \otimes_A B) \xrightarrow{\text{Nr}} \operatorname{Pic}(X) \\
&\longrightarrow H^2(X, U_{B/A}) \longrightarrow H^2(X \otimes_A B, \boldsymbol{G}_m) \xrightarrow{\text{Nr}} H^2(X, \boldsymbol{G}_m) \longrightarrow \cdots .
\end{aligned}$$

On the other hand, the exact sequence of group schemes

$$0 \longrightarrow \boldsymbol{G}_{m,A} \xrightarrow{i} \prod_{B/A} \boldsymbol{G}_{m,B} \longrightarrow G_{B/A} \longrightarrow 0$$

induces a long exact sequence

$$\begin{aligned}
0 &\longrightarrow \Gamma(X, \boldsymbol{G}_m) \xrightarrow{i} \Gamma(X \otimes_A B, \boldsymbol{G}_m) \longrightarrow \Gamma(X, G_{B/A}) \\
&\longrightarrow \operatorname{Pic}(X) \xrightarrow{i} \operatorname{Pic}(X \otimes_A B) \longrightarrow H^1(X, G_{B/A}) \\
&\longrightarrow H^2(X, \boldsymbol{G}_m) \xrightarrow{i} H^2(X \otimes_A B, \boldsymbol{G}_m) \longrightarrow H^2(X, G_{B/A}) \longrightarrow \cdots .
\end{aligned}$$

If $X = \operatorname{Spec} R$, we obtain exact sequences

$$\begin{aligned}
0 &\longrightarrow U_{B/A}(R) \longrightarrow (R \otimes_A B)^\times \xrightarrow{\text{Nr}} R^\times \\
&\longrightarrow H^1(R, U_{B/A}) \longrightarrow \operatorname{Pic}(R \otimes_A B) \xrightarrow{\text{Nr}} \operatorname{Pic}(R) \\
&\longrightarrow H^2(R, U_{B/A}) \longrightarrow H^2(R \otimes_A B, \boldsymbol{G}_m) \xrightarrow{\text{Nr}} H^2(R, \boldsymbol{G}_m) \longrightarrow \cdots
\end{aligned}$$

and

$$\begin{aligned}
0 &\longrightarrow R^\times \xrightarrow{i} (R \otimes_A B)^\times \longrightarrow G_{B/A}(R) \\
&\longrightarrow \operatorname{Pic}(R) \xrightarrow{i} \operatorname{Pic}(R \otimes_A B) \longrightarrow H^1(R, G_{B/A}) \\
&\longrightarrow H^2(R, \boldsymbol{G}_m) \xrightarrow{i} H^2(R \otimes_A B, \boldsymbol{G}_m) \longrightarrow H^2(R, G_{B/A}) \longrightarrow \cdots .
\end{aligned}$$

In particular, we have

PROPOSITION 2.6 (Hilbert 90). *Let R be a local A-algebra. Then we have exact sequences*

$$(R \otimes_A B)^\times \xrightarrow{\text{Nr}} R^\times \longrightarrow H^1(R, U_{B/A}) \longrightarrow 0$$

and

$$0 \longrightarrow H^1(R, G_{B/A}) \longrightarrow H^2(R, \boldsymbol{G}_m) \xrightarrow{i} H^2(R \otimes_A B, \boldsymbol{G}_m) .$$

Furthermore, $H^1(R, U_{B/A})$ and $H^1(R, G_{B/A})$ are annihilated by 2.

PROOF. Since $R \otimes_A B$ is a semi-local ring, we obtain the first asserion, noting that $\operatorname{Pic}(R \otimes_A B) = 0$. The second assetion follows from the fact that the composite $\text{Nr} \circ i$ is the square map.

Hereafter we devote ourselves to constructing equivariant compactifications $\iota : G_{B/A} \to \boldsymbol{P}^1_A$ and $\iota : U_{B/A} \to \boldsymbol{P}^1_A$.

2.7. Let $GL(2)$ denote the general linear group scheme of degree 2. Then

$$GL(2) = \operatorname{Spec} \boldsymbol{Z}\left[T_{11}, T_{12}, T_{21}, T_{22}, \frac{1}{T_{11}T_{22} - T_{12}T_{21}}\right]$$

with the multiplication

$$\begin{pmatrix} T_{11} & T_{12} \\ T_{21} & T_{22} \end{pmatrix} \mapsto \begin{pmatrix} T_{11} \otimes T_{11} + T_{12} \otimes T_{21} & T_{11} \otimes T_{12} + T_{12} \otimes T_{22} \\ T_{21} \otimes T_{11} + T_{22} \otimes T_{21} & T_{21} \otimes T_{12} + T_{22} \otimes T_{22} \end{pmatrix}.$$

The regular representation

$$\Big(\prod_{B/A} \boldsymbol{G}_{m,B}\Big)(R) = (R \otimes_A B)^\times \to GL(2, R) : u + \varepsilon v \mapsto \begin{pmatrix} u & -sv \\ v & u + rv \end{pmatrix}$$

is represented by a homomorphism of group A-schemes

$$\rho : U_{B/A} = \operatorname{Spec} A[U, V]/(U^2 + rUV + sV^2 - 1) \to GL(2)_A$$

defined by

$$\begin{pmatrix} T_{11} & T_{12} \\ T_{21} & T_{22} \end{pmatrix} \mapsto \begin{pmatrix} U & -sV \\ V & U + rV \end{pmatrix}.$$

It is readily seen that ρ is a closed immersion. Moreover, we have a cartesian square

$$\begin{array}{ccc} U_{B/A} & \xrightarrow{\rho} & SL(2)_A \\ \big\downarrow & & \big\downarrow \\ \prod_{B/A} \boldsymbol{G}_{m,B} & \xrightarrow[\rho]{} & GL(2)_A\,, \end{array}$$

where the right vertical arrow is the canonical closed immersion.

Now put $\varDelta = T_{11}T_{22} - T_{12}T_{21}$, and let $\boldsymbol{Z}[T_{11}/\varDelta, T_{12}/\varDelta, T_{21}/\varDelta, T_{22}/\varDelta]^{(2)}$ denote the subring of $\boldsymbol{Z}[T_{11}, T_{12}, T_{21}, T_{22}, 1/\varDelta]$ generated by the fractions $T_{ij}T_{kl}/\varDelta$, $1 \le i, j, k, l \le 2$. Then $\boldsymbol{Z}[T_{11}/\varDelta, T_{12}/\varDelta, T_{21}/\varDelta, T_{22}/\varDelta]^{(2)}$ is a Hopf subalgebra of $\boldsymbol{Z}[T_{11}, T_{12}, T_{21}, T_{22}, 1/\varDelta]$, and

$$PGL(2) = \operatorname{Spec} \boldsymbol{Z}\left[\frac{T_{11}}{\varDelta}, \frac{T_{12}}{\varDelta}, \frac{T_{21}}{\varDelta}, \frac{T_{22}}{\varDelta}\right]^{(2)}.$$

The kernel of the canonical surjection $GL(2) \to PGL(2)$ is isomorphic to the multiplicative group $\boldsymbol{G}_m$, and the canonical injection

$$\boldsymbol{G}_m = \operatorname{Spec} \boldsymbol{Z}\left[T, \frac{1}{T}\right] \to GL(2) = \operatorname{Spec} \boldsymbol{Z}\left[T_{11}, T_{12}, T_{21}, T_{22}, \frac{1}{\varDelta}\right]$$

is given by

$$\begin{pmatrix} T_{11} & T_{12} \\ T_{21} & T_{22} \end{pmatrix} \mapsto \begin{pmatrix} T & 0 \\ 0 & T \end{pmatrix}.$$

The commutative diagram

$$\begin{array}{ccc} \boldsymbol{G}_{m,A} & \xrightarrow{i} & \prod_{B/A} \boldsymbol{G}_{m,B} \\ \| & & \downarrow \rho \\ \boldsymbol{G}_{m,A} & \longrightarrow & GL(2)_A \end{array}$$

is extended to a commutaive diagram with exact rows of group A-schemes

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \boldsymbol{G}_{m,A} & \xrightarrow{i} & \prod_{B/A} \boldsymbol{G}_{m,B} & \xrightarrow{\gamma} & G_{B/A} & \longrightarrow & 0 \\ & & \| & & \downarrow \rho & & \downarrow \tilde{\rho} & & \\ 1 & \longrightarrow & \boldsymbol{G}_{m,A} & \longrightarrow & GL(2)_A & \longrightarrow & PGL(2)_A & \longrightarrow & 1\,. \end{array}$$

Furthermore, the homogeneous space of $PGL(2)_A$ by the upper triangular subgroup is identified to the projective line $\boldsymbol{P}^1_A$. The multiplication on $PGL(2)$ induces an action by $PGL(2)$ on $\boldsymbol{P}^1$, that is to say, we have a commutatice diagram

$$\begin{array}{ccc} PGL(2) \times PGL(2) & \xrightarrow{\text{multiplication}} & PGL(2) \\ \downarrow & & \downarrow \\ PGL(2) \times \boldsymbol{P}^1 & \xrightarrow[\text{action}]{} & \boldsymbol{P}^1\,. \end{array}$$

We denote by ι the composite $G_{B/A} \xrightarrow{\tilde{\rho}} PGL(2)_A \to \boldsymbol{P}^1_A$. Then we have gotten a commutative diagram

$$\begin{array}{ccc} G_{B/A} \times_A G_{B/A} & \xrightarrow{\text{multiplication}} & G_{B/A} \\ {\scriptstyle \tilde{\rho}\times\iota}\downarrow & & \downarrow \iota \\ PGL(2)_A \times_A \boldsymbol{P}^1_A & \xrightarrow[\text{action}]{} & \boldsymbol{P}^1_A\,. \end{array}$$

REMARK 2.7.1. The surjective morphism $PGL(2) \to \boldsymbol{P}^1$ mentioned above is described explicitly as follows.

Let $\boldsymbol{P}^1 = \operatorname{Proj} \boldsymbol{Z}[T_1, T_2]$, and put $T = T_1/T_2$. Then the projective line $\boldsymbol{P}^1$ is covered by affine open subsets $\operatorname{Spec} \boldsymbol{Z}[T]$ and $\operatorname{Spec} \boldsymbol{Z}[1/T]$. Define now morphisms

$$\operatorname{Spec} \boldsymbol{Z}\left[T_{11}, T_{12}, T_{21}, T_{22}, \frac{1}{\Delta}\right]\left[\frac{1}{T_{21}}\right] \to \operatorname{Spec} \boldsymbol{Z}[T]$$

and

$$\operatorname{Spec} \boldsymbol{Z}\left[T_{11}, T_{12}, T_{21}, T_{22}, \frac{1}{\Delta}\right]\left[\frac{1}{T_{11}}\right] \to \operatorname{Spec} \boldsymbol{Z}\left[\frac{1}{T}\right]$$

by $T \mapsto T_{11}/T_{21}$ and $1/T \mapsto T_{21}/T_{11}$, respectively. Gluing the two morphisms, we obtain a morphism

$$GL(2) = \operatorname{Spec} \boldsymbol{Z}\left[T_{11}, T_{12}, T_{21}, T_{22}, \frac{1}{\Delta}\right] \to \boldsymbol{P}^1,$$

since we have $(T_{11}, T_{21}) = \boldsymbol{Z}[T_{11}, T_{12}, T_{21}, T_{22}, 1/\Delta]$. It is readily seen that $GL(2) \to \boldsymbol{P}^1$ is factorized as $GL(2) \to PGL(2) \to \boldsymbol{P}^1$.

Let R be a local ring. Then the map $PGL(2, R) \to \boldsymbol{P}^1(R)$ is given by

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \mapsto (a : c),$$

and the action of $PGL(2, R)$ on $\boldsymbol{P}^1(R)$ is given by

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} (\alpha : \beta) = (a\alpha + b\beta : c\alpha + d\beta),$$

as is well-known.

PROPOSITION 2.8. *The homomorphism of group A-schemes*

$$\begin{aligned} \tilde{\rho} : G_{B/A} &= \operatorname{Spec} A[X, Y]/(X^2 + rXY + sY^2 - Y) \\ &\to PGL(2)_A = \operatorname{Spec} A\left[\frac{T_{11}}{\Delta}, \frac{T_{12}}{\Delta}, \frac{T_{21}}{\Delta}, \frac{T_{22}}{\Delta}\right]^{(2)} \end{aligned}$$

is given by

$$\begin{pmatrix} T_{11} & T_{12} \\ T_{21} & T_{22} \end{pmatrix} \mapsto \begin{pmatrix} \dfrac{2 - rX - 2sY}{\sqrt{4 + DY}} & -\dfrac{2sX + rsY}{\sqrt{4 + DY}} \\ \dfrac{2X + rY}{\sqrt{4 + DY}} & \dfrac{2 + rX + (r^2 - 2s)Y}{\sqrt{4 + DY}} \end{pmatrix}.$$

PROOF. The homomorphism of Hopf A-algebras

$$A[X, Y]/(X^2 + rXY + sY^2 - Y) \to A\left[U, V, \frac{1}{U^2 + rUV + sV^2}\right] :$$
$$X \mapsto \frac{UV}{U^2 + rUV + sV^2}, \quad Y \mapsto \frac{V^2}{U^2 + rUV + sV^2}$$

gives correspondences

$$2 - rX - 2sY \mapsto \frac{U(2U + rV)}{U^2 + rUV + sV^2}, \quad 2X + rY \mapsto \frac{V(2U + rV)}{U^2 + rUV + sV^2},$$
$$4 + DY \mapsto \frac{(2U + rV)^2}{U^2 + rUV + rV^2},$$

and therefore

$$\begin{pmatrix} \dfrac{2-rX-2sY}{\sqrt{4+DY}} & -\dfrac{2sX+rsY}{\sqrt{4+DY}} \\ \dfrac{2X+rY}{\sqrt{4+DY}} & \dfrac{2+rX+(r^2-2s)Y}{\sqrt{4+DY}} \end{pmatrix} \mapsto \begin{pmatrix} \dfrac{U}{\sqrt{U^2+rUV+sV^2}} & -\dfrac{sV}{\sqrt{U^2+rUV+sV^2}} \\ \dfrac{V}{\sqrt{U^2+rUV+sV^2}} & \dfrac{U+rV}{\sqrt{U^2+rUV+sV^2}} \end{pmatrix}.$$

This implies the commutativity of the diagram

$$\begin{array}{ccc} A\left[\dfrac{T_{11}}{\Delta}, \dfrac{T_{12}}{\Delta}, \dfrac{T_{21}}{\Delta}, \dfrac{T_{22}}{\Delta}\right]^{(2)} & \xrightarrow{\text{inclusion}} & A\left[T_{11}, T_{12}, T_{21}, T_{22}, \dfrac{1}{\Delta}\right] \\ \downarrow & & \downarrow \rho \\ A[X, Y]/(X^2+rXY+sY^2-Y) & \longrightarrow & A\left[U, V, \dfrac{1}{U^2+rUV+sV^2}\right], \end{array}$$

since

$$\begin{vmatrix} \dfrac{2-rX-2sY}{\sqrt{4+DY}} & -\dfrac{2sX+rsY}{\sqrt{4+DY}} \\ \dfrac{2X+rY}{\sqrt{4+DY}} & \dfrac{2+rX+(r^2-s)Y}{\sqrt{4+DY}} \end{vmatrix} = 1$$

in $A[X, Y]/(X^2+rXY+sY^2-Y)$. Here the left vertical arrow is defined by

$$\begin{pmatrix} T_{11} & T_{12} \\ T_{21} & T_{22} \end{pmatrix} \mapsto \begin{pmatrix} \dfrac{2-rX-2sY}{\sqrt{4+DY}} & -\dfrac{2sX+rsY}{\sqrt{4+DY}} \\ \dfrac{2X+rY}{\sqrt{4+DY}} & \dfrac{2+rX+(r^2-2s)Y}{\sqrt{4+DY}} \end{pmatrix}.$$

We obtain the conclusion, noting that the homomorphism $\gamma : \prod_{B/A} \boldsymbol{G}_{m,B} \to G_{B/A}$ is faithfully flat.

REMARK 2.8.1. It appears that the matrix

$$\begin{pmatrix} \dfrac{2-rX-2sY}{\sqrt{4+DY}} & -\dfrac{2sX+rsY}{\sqrt{4+DY}} \\ \dfrac{2X+rY}{\sqrt{4+DY}} & \dfrac{2+rX+(r^2-2s)Y}{\sqrt{4+DY}} \end{pmatrix}$$

does not have the entries in the affine ring $A[X, Y]/(X^2+rXY+sY^2-Y)$. However, we can verify that the image of the Hopf algebra $A[T_{11}/\Delta, T_{12}/\Delta, T_{21}/\Delta, T_{22}/\Delta]^{(2)}$ by $\tilde{\rho}$ is contained in $A[X,Y]/(X^2+rXY+sY^2-Y)$, noting that

$$(2-rX-2sY)^2 = (1-rX-sY)(4+DY)+r^2(X^2+rXY+sY^2-Y)\,,$$
$$(2-rX-2sY)(2X+rY) = X(4+DY)-2r(X^2+rXY+sY^2-Y)\,,$$
$$(2X+rY)^2 = Y(4+DY)+4(X^2+rXY+sY^2-Y)\,.$$

COROLLARY 2.9. *The morphism*

$$\iota : G_{B/A} = \mathrm{Spec}\, A[X,Y]/(X^2+rXY+sY^2-Y) \to \boldsymbol{P}^1_A = \mathrm{Proj}\, A[T_1,T_2]$$

is given by

$$T = \frac{T_1}{T_2} \mapsto \frac{2-rX-2sY}{2X+rY}\,.$$

Moreover, $\iota : G_{B/A} \to \boldsymbol{P}^1_A$ *is an open immersion with image* $\boldsymbol{P}^1_A - V(T_1^2+rT_1T_2+sT_2^2)$, *and the inverse of the birational map* ι *is given by*

$$X \mapsto \frac{T}{T^2+rT+s}\,, \quad Y \mapsto \frac{1}{T^2+rT+s}\,.$$

PROOF. Combining Proposition 2.8 and Remark 2.7.1, we obtain the first assertion.

Put now $\tilde{\Delta} = T_1^2+rT_1T_2+sT_2^2$, and let $A[T_1/\tilde{\Delta}, T_2/\tilde{\Delta}]^{(2)}$ denote the subring of $A[T_1/\tilde{\Delta}, T_2/\tilde{\Delta}]$ generated by the fractions $T_iT_j/\tilde{\Delta}$. Then $\mathrm{Spec}\, A[T_1/\tilde{\Delta}, T_2/\tilde{\Delta}]^{(2)}$ is isomorphic to the open subscheme $\boldsymbol{P}^1_A - V(T_1^2+rT_1T_2+sT_2^2)$. Moreover, it is verified without difficulty that

$$A\left[\frac{T_1}{T_1^2+rT_1T_2+sT_2^2}, \frac{T_2}{T_1^2+rT_1T_2+sT_2^2}\right]^{(2)} = A\left[\frac{T_1T_2}{T_1^2+rT_1T_2+sT_2^2}, \frac{T_2^2}{T_1^2+rT_1T_2+sT_2^2}\right].$$

and that

$$X \mapsto \frac{T_1T_2}{T_1^2+rT_1T_2+sT_2^2}\,, \quad Y \mapsto \frac{T_2^2}{T_1^2+rT_1T_2+sT_2^2}$$

induces an isomorphism of rings

$$A[X,Y]/(X^2+rXY+sY^2-Y) \xrightarrow{\sim} A\left[\frac{T_1T_2}{T_1^2+rT_1T_2+sT_2^2}, \frac{T_2^2}{T_1^2+rT_1T_2+sT_2^2}\right].$$

This implies the second assertion. □

REMARK 2.9.1. Let R be a local A-algebra. Then the map $\tilde{\rho} : G_{B/A}(R) \to PGL(2,A)$ is given by

$$(a,b) \mapsto \begin{pmatrix} 2-ra-2sb & -2sa-rsb \\ 2a+rb & 2+ra+(r^2-2s)b \end{pmatrix},$$

and the map $\iota : G_{B/A}(R) \to \boldsymbol{P}^1(R)$ by

$$(a,b) \mapsto (2-ra-2sb : 2a+rb)\,.$$

2.10. The homomorphism of group A-schemes.

$$\begin{aligned}\alpha : G_{B/A} &= \operatorname{Spec} A[X,Y]/(X^2+rXY+rY^2-Y)\\ \to U_{B/A} &= \operatorname{Spec} A[U,V]/(U^2+rUV+sV^2-1)\end{aligned}$$

defined by

$$U \mapsto 1-rX-2sY\,, \quad V \mapsto 2X+rY$$

is birational, since α induces an isomorphism over $A[1/D]$, as remarked in 2.3. Then we obtain rational maps

$$U_{B/A} \xrightarrow{\alpha^{-1}} G_{B/A} \xrightarrow{\tilde{\rho}} PGL(2)_A$$

and

$$U_{B/A} \xrightarrow{\alpha^{-1}} G_{B/A} \xrightarrow{\iota} \boldsymbol{P}^1_A\,,$$

which we also denote by $\tilde{\rho}$ and ι, respectively.

PROPOSITION 2.11. *The rational maps*

$$\begin{aligned}\tilde{\rho} : U_{B/A} &= \operatorname{Spec} A[U,V]/(U^2+rUV+sV^2-1)\\ \to PGL(2)_A &= \operatorname{Spec} A\left[\frac{T_{11}}{\Delta}, \frac{T_{12}}{\Delta}, \frac{T_{21}}{\Delta}, \frac{T_{22}}{\Delta}\right]^{(2)}\end{aligned}$$

and

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

are given by

$$\begin{pmatrix} T_{11} & T_{12} \\ T_{21} & T_{22}\end{pmatrix} \mapsto \begin{pmatrix} \dfrac{1+U}{\sqrt{2+2U+rV}} & -\dfrac{sV}{\sqrt{2+2U+rV}} \\ \dfrac{V}{\sqrt{2+2U+rV}} & \dfrac{1+U+rV}{\sqrt{2+2U+rV}}\end{pmatrix},$$

and

$$T = \frac{T_1}{T_2} \mapsto \frac{1+U}{V} = \frac{rU+sV}{1-U}\,,$$

respectively. Moreover, $\iota : U_{B/A} \to \boldsymbol{P}^1_A$ *induces an open immersion over* $A[1/D]$, *and the inverse of the birational map* ι *is given by*

$$U \mapsto \frac{T^2-s}{T^2+rT+s}\,, \quad V \mapsto \frac{2T+r}{T^2+rT+s}\,.$$

PROOF. We can conclude the assertion immediately from the definition of $\tilde{\rho} : U_{B/A} \to PGL(2)_A$ and $\iota : U_{B/A} \to \boldsymbol{P}^1_A$, referring to Proposition 2.8 and Corollary 2.9, and noting that the birational maps $\alpha^{-1} : U_{B/A} \to G_{B/A}$ and $\alpha : G_{B/A} \to U_{B/A}$ are given by

$$X \mapsto \frac{r-rU-2sV}{D}\,, \quad Y \mapsto \frac{-2+2U+rV}{D}$$

and

$$U \mapsto 1 - rX - 2sY\,, \quad V \mapsto 2X + rY\,,$$

respectively.

REMARK 2.11.1. Let R be a local A-algebra. Then the map $\tilde{\rho} : U_{B/A}(R) \to PGL(2, A)$ is given by

$$(a, b) \mapsto \begin{pmatrix} 1+u & -2sv \\ v & 1+u+rv \end{pmatrix}\,,$$

and the map $\iota : G_{B/A}(R) \to \boldsymbol{P}^1(R)$ by

$$(u, v) \mapsto (1+u : v) = (ru + sv : 1 - u)\,,$$

if defined.

REMARK 2.12.1. We have a commutative diagram with exact rows of group schemes over $A[1/D]$

$$\begin{array}{ccccccccc} 1 & \longrightarrow & \boldsymbol{\mu}_{2,A} & \longrightarrow & U_{B/A} & \xrightarrow{\text{square}} & U_{B/A} & \longrightarrow & 1 \\ & & \| & & \downarrow{\scriptstyle\rho} & & \downarrow{\scriptstyle\tilde{\rho}} & & \\ 1 & \longrightarrow & \boldsymbol{\mu}_{2,A} & \longrightarrow & SL(2)_A & \longrightarrow & PGL(2)_A & \longrightarrow & 1\,. \end{array}$$

REMARK 2.12.2. Define an automorphism

$$\sigma : \boldsymbol{P}^1_B = \operatorname{Proj} B[T_1, T_2] \to \boldsymbol{P}^1_B = \operatorname{Proj} B[T_1, T_2]$$

by

$$(T_1, T_2) \mapsto (T_2, T_1 + (r - \varepsilon)T_2)\,.$$

Then we have a cartesian square of B-schemes

$$\begin{array}{ccc} G_{B/A} \otimes_A B & \xrightarrow{\iota} & \boldsymbol{P}^1_B \\ {\scriptstyle\sigma}\downarrow{\scriptstyle\wr} & & \downarrow{\scriptstyle\wr\,\sigma} \\ \mathcal{G}^{(\lambda)} & \xrightarrow[\iota]{} & \boldsymbol{P}^1_B\,, \end{array}$$

where the horizontal arrow below is defined by the inclusions

$$\mathcal{G}^{(\lambda)} = \operatorname{Spec} B\left[T, \frac{1}{\lambda T + 1}\right] \subset \operatorname{Spec} B[T] \subset \boldsymbol{P}^1_B = \operatorname{Proj} B[T_1, T_2]\,, \quad T = T_1/T_2\,.$$

REMARK 2.12.3. Define a rational map

$$s : \boldsymbol{P}^1_B = \operatorname{Proj} B[T_1, T_2] \to \boldsymbol{P}^1_B = \operatorname{Proj} B[T_1, T_2]$$

by

$$(T_1, T_2) \mapsto (T_1 + \varepsilon T_2, T_1 + (r - \varepsilon)T_2)\,.$$

Then we have a commutative diagram of birational maps

$$\begin{array}{ccc} U_{B/A} \otimes_A B & \xrightarrow{\iota} & \boldsymbol{P}^1_B \\ {\scriptstyle s}\downarrow & & \downarrow{\scriptstyle s} \\ \boldsymbol{G}_{m,B} & \xrightarrow[\iota]{} & \boldsymbol{P}^1_B\,, \end{array}$$

where the horizontal arrow below is defined by the inclusions

$$\boldsymbol{G}_{m,B} = \mathrm{Spec}\left[T, \frac{1}{T}\right] \subset \mathrm{Spec}\, B[T] \subset \boldsymbol{P}^1_B = \mathrm{Proj}\, B[T_1, T_2]\,, \quad T = T_1/T_2\,.$$

3. Twisted Kummer theory. In this section, we fix an integer $n \geq 3$ and a primitive n-th root of unity ζ.

3.1. Let n be an integer ≥ 3 and ζ a primitive n-th root of unity. Put $\omega = \zeta + \zeta^{-1}$ and $D = (\zeta - \zeta^{-1})^2$. Let $A = \boldsymbol{Z}[\omega]$ and $B = \boldsymbol{Z}[\zeta]$. Then B is isomorphic to $A[t]/(t^2 - \omega t + 1)$, and therefore, we have a commutaive group scheme over A

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

with the multiplication

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

The group scheme $U_{B/A} \otimes_A A[1/D]$ is a torus of dimension 1 over $A[1/D]$ as remarked in 2.2.

REMARK 3.1.1. Assume that n is odd. Then $-\zeta$ is a primitive $2n$-th root of unity. Moreover, $U \mapsto U,\ V \mapsto -V$ gives rise to an isomorphism

$$\mathrm{Spec}\, A[U, V]/(U^2 + \omega UV + V^2 - 1) \xrightarrow{\sim} \mathrm{Spec}\, A[U, V]/(U^2 - \omega UV + V^2 - 1)\,.$$

REMARK 3.1.2. It is well-known that

(1) if $n = 2^r$, $(D)^{2^{r-2}} = (4)$ in A;

(2) if $n = p^r$ or $n = 2p^r$ (p is an odd prime), $(D)^{(p-1)p^{r-1}/2} = (p)$ in A, that is, (D) is a prime ideal of A, totally ramified over p;

(3) otherwise, D is invertible in A.

On the other hand, it holds that

(1) if $n = 4$, $\omega = 0$;

(2) if $n = 2^r$ ($r \geq 3$), $(\omega)^{2^{r-2}} = (2)$ in A, that is, (ω) is a prime ideal of A, totally ramified over 2;

(3) otherwise, ω is invertible in A.

The assertions follow from the following well-known formulae on the cyclotomic polynomial $\Phi_n(t)$:

$$\Phi_n(1) = \begin{cases} p & n = p^r, \text{ where } p \text{ is a prime and } r \geq 1\,, \\ 1 & n \text{ is not a prime power}\,, \end{cases}$$

and

$$\Phi_n(-1) = \begin{cases} p & n = 2p^r, \text{ where } p \text{ is a prime and } r \geq 1\,, \\ 1 & n \text{ is not twice a prime power}\,. \end{cases}$$

In particular, it follows that, *if n is not a prime power nor twice a prime, $U_{B/A}$ is a torus over A.*

REMARK 3.1.3. If $n = p^r$, p being an odd prime, $U_{B/A}$ is smooth over A. More precisely, $U_{B/A} \otimes A[1/p]$ is a torus over $A[1/p]$. Put now $A_0 = A/(D)$. Then $U_{B/A} \otimes_A A_0$ is isomorphic to $\boldsymbol{G}_a \times \boldsymbol{\mu}_2$. Indeed,

$$\begin{aligned} U_{B/A} \otimes_A A_0 &= \operatorname{Spec} A_0[U, V]/(U^2 + \omega UV + V^2 - 1) \\ &= \operatorname{Spec} A_0[U, V]/\big((U + (\omega/2)V)^2 - 1\big)\,, \end{aligned}$$

and $U + (\omega/2)V$ is a group-like element of $A_0[U, V]/\big((U + (\omega/2)V)^2 - 1\big)$, and therefore $T \mapsto U + (\omega/2)V$ defines a homomorphism

$$\begin{aligned} \pi : U_{B/A} \otimes_A A_0 &= \operatorname{Spec} A_0[U, V]/\big((U + (\omega/2)V)^2 - 1\big) \\ &\to \boldsymbol{\mu}_{2,A_0} = \operatorname{Spec} A_0[T]/(T^2 - 1)\,. \end{aligned}$$

Moreover, $U \mapsto 1 - (\omega/2)S,\ V \mapsto S$ defines a homomorphism

$$\boldsymbol{G}_{a,A_0} = \operatorname{Spec} A_0[S] \to U_{B/A} \otimes_A A_0 = \operatorname{Spec} A_0[U, V]/\big(U + (\omega/2)V)^2 - 1\big)\,,$$

and we have obtain an exact sequence of group schemes

$$0 \longrightarrow \boldsymbol{G}_{a,A_0} \longrightarrow U_{B/A} \otimes_A A_0 \xrightarrow{\ \pi\ } \boldsymbol{\mu}_{2,A_0} \longrightarrow 0\,.$$

Moreover, $U \mapsto T,\ V \mapsto 0$ defines a homomorphism

$$\begin{aligned} s : \mu_{2,A_0} &= \operatorname{Spec} A_0[T]/(T^2 - 1) \\ &\to U_{B/A} \otimes_A A_0 = \operatorname{Spec} A_0[U, V]/\big((U + (\omega/2)V)^2 - 1\big)\,. \end{aligned}$$

It is easily verified that $s : \boldsymbol{\mu}_{2,A_0} \to U_{B/A} \otimes_A A_0$ is a section of $\pi : U_{B/A} \otimes_A A_0 \to \boldsymbol{\mu}_{2,A_0}$.

THEOREM 3.2 (twisted Kummer theory). *The homothety by n on $U_{B/A} \otimes A[1/n]$ is finite and étale with the kernel isomorphic to the constant group scheme $\mathbf{Z}/n\mathbf{Z}$.*

PROOF. The homothety by n on $U_{B/A} \otimes_A A[1/D]$ is finite and flat with the kernel locally isomorphic to the group scheme $\boldsymbol{\mu}_n$, since the group scheme $U_{B/A} \otimes_A A[1/D]$ is a torus of dimension 1 over $A[1/D]$. It follows that the homothety by n on $U_{B/A} \otimes_A A[1/n]$ is finite and étale. Furthermore, $\operatorname{Ker}[n : U_{B/A} \to U_{B/A}] \otimes_A A[1/n]$ is isomorphic to the constant group scheme $\mathbf{Z}/n\mathbf{Z}$, since the A-valued point of $U_{B/A}$ defined by $(U, V) \mapsto (0, 1)$ is of order n.

REMARK 3.2.1. The theorem can be restated as follows. The isogeny of commutative group schemes $n : U_{B/A} \otimes_A A[1/n] \to U_{B/A} \otimes_A A[1/n]$ is an étale covering with Galois group $\mathbf{Z}/n\mathbf{Z}$, whose generator is given by $U \mapsto -V$, $V \mapsto U + \omega V$.

We shall call the exact sequence of group schemes over $\mathbf{Z}[\omega, 1/n]$

$$0 \longrightarrow \mathbf{Z}/n\mathbf{Z} \longrightarrow U_{B/A} \xrightarrow{n} U_{B/A} \longrightarrow 0$$

the twisted Kummer sequence.

COROLLARY 3.3. *Let R be a local $\mathbf{Z}[\omega, 1/n]$-algebra. If n is odd, $H^1(R, \mathbf{Z}/n\mathbf{Z})$ is isomorphic to $U_{B/A}(R)/n$.*

PROOF. From the twisted Kummer sequence over $\mathbf{Z}[\omega, 1/n]$

$$0 \longrightarrow \mathbf{Z}/n\mathbf{Z} \longrightarrow U_{B/A} \xrightarrow{n} U_{B/A} \longrightarrow 0\,,$$

we obtain a long exact sequence

$$U_{B/A}(R) \xrightarrow{n} U_{B/A}(R) \longrightarrow H^1(R, \mathbf{Z}/n\mathbf{Z}) \longrightarrow H^1(R, U_{B/A}) \xrightarrow{n} H^1(R, U_{B/A})\,.$$

By Proposition 2.6, $H^1(R, U_{B/A})$ is annihilated by 2. Then the homothety by n on $H^1(R, U_{B/A})$ is bijective, since n is odd.

COROLLARY 3.4. *Let R be a local $\mathbf{Z}[\omega, 1/n]$-algebra and S an unramified cyclic extension of R of degree n. If n is odd, there exists a morphism* Spec $R \to U_{B/A}$ *such that the square*

$$\begin{array}{ccc} \operatorname{Spec} S & \longrightarrow & U_{B/A} \\ \big\downarrow & & \big\downarrow{\scriptstyle n} \\ \operatorname{Spec} R & \longrightarrow & U_{B/A} \end{array}$$

is cartesian.

We can give a more concrete description of the statement mentioned above.

LEMMA 3.5. *Let l be an integer ≥ 2. The homothety by l on the commutative group scheme $U_{B/A} =$ Spec $A[U, V]/(U^2 + \omega UV + V^2 - 1)$ is given by*

$$U \mapsto \frac{\zeta^{-1}(U + \zeta V)^l - \zeta(U + \zeta^{-1}V)^l}{\zeta^{-1} - \zeta}\,, \qquad V \mapsto \frac{(U + \zeta V)^l - (U + \zeta^{-1}V)^l}{\zeta - \zeta^{-1}}\,.$$

PROOF. Let $\tilde{l}$ denote the ring endomorphism of $A[U, V]/(U^2+\omega UV+V^2-1)$ which defines the homothety by l on $U_{B/A}$. As remarked in 2.2,

$$T \mapsto U + \zeta V\,, \quad \frac{1}{T} \mapsto U + \zeta^{-1}V$$

defines an isomorphism of group schemes over $B[1/n]$

$$\begin{aligned} s : U_{B/A} \otimes_A B\left[\frac{1}{n}\right] &= \operatorname{Spec} B\left[\frac{1}{n}\right][U, V]/(U^2 + \omega UV + V^2 - 1) \\ &\xrightarrow{\sim} \mathbf{G}_{m, B[1/n]} = \operatorname{Spec} B\left[\frac{1}{n}\right]\left[T, \frac{1}{T}\right]. \end{aligned}$$

Then we obtain

$$\tilde{l}(U+\zeta V)=(U+\zeta V)^l\,,\quad \tilde{l}(U+\zeta^{-1}V)=(U+\zeta^{-1}V)^l\,,$$

which implies the assertion.

Combining Corollay 3.4 with Lemma 3.5, we obtain:

COROLLARY 3.6. *Let R be a local $\boldsymbol{Z}[\omega,1/n]$-algebra and S an unramified cyclic extension of R of degree n. If n is odd, there exist $u, v\in R$ such that $u^2+\omega uv+v^2=1$ and that S is isomorphic to*

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

Moreover, the map

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

yields a generator of $\mathrm{Gal}(S/R)$.

Hereafter we establish a one-parameter version of Corollaries 3.4 and 3.6, using the equivariant compactification $\iota: U_{B/A}\to \boldsymbol{P}^1_A$.

3.7. As is shown in Proposition 2.8 and Corollary 2.9, the rational maps

$$\begin{aligned}\tilde{\rho}: U_{B/A}&=\mathrm{Spec}\,A[U,V]/(U^2+\omega UV+V^2-1)\\ &\to PGL(2)_A=\mathrm{Spec}\,A\left[\frac{T_{11}}{\Delta},\frac{T_{12}}{\Delta},\frac{T_{21}}{\Delta},\frac{T_{22}}{\Delta}\right]^{(2)}\end{aligned}$$

and

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

are defined by

$$\begin{pmatrix}T_{11}&T_{12}\\T_{21}&T_{22}\end{pmatrix}\mapsto\begin{pmatrix}\dfrac{1+U}{\sqrt{2+2U+\omega V}}&-\dfrac{V}{\sqrt{2+2U+\omega V}}\\[2ex]\dfrac{V}{\sqrt{2+2U+\omega V}}&\dfrac{1+U+\omega V}{\sqrt{2+2U+\omega V}}\end{pmatrix}$$

and

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

respectively. The inverse of the birational map $\iota: U_{B/A}\to\boldsymbol{P}^1_A$ is given by

$$U\mapsto\frac{T^2-1}{T^2+\omega T+1}\,,\quad V\mapsto\frac{2T+\omega}{T^2+\omega T+1}\,.$$

Let R be a local A-algebra. Then the map $\tilde{\rho}: U_{B/A}(R)\to PGL(2,R)$ is given by

$$(u,v)\mapsto\begin{pmatrix}1+u&-v\\v&1+u+\omega v\end{pmatrix},$$

and $\iota : U_{B/A}(R) \to \boldsymbol{P}^1(R)$ by

$$(u, v) \mapsto (1 + u : v) = (\omega u + v : 1 - u)\,,$$

if defined.

PROPOSITION 3.8. *The rational map* $\tilde{\rho} : U_{B/A} \to PGL(2)_A$ *is defined*

(1) *everywhere if* n *is not a prime power nor twice a prime power*;

(2) *outside the locus defined by the ideal* $(2 + 2U + \omega V, p)$ *if* $n = p^r$ *or* $2p^r$, *where* p *is an odd prime*;

(3) *outside the locus defined by the ideal* (2) *if* $n = 2^r$.

PROOF. By the definition, the rational map $\tilde{\rho} : U_{B/A} \to PGL(2)_A$ is defined outside the locus defined by the ideal (D). If n is not a power of a prime nor twice a power of a prime, D is invertible, which implies the assertion (1). In the cases (2) and (3), the rational map $\tilde{\rho} : U_{B/A} \to PGL(2)_A$ is defined outside the locus defined by the ideal (p) by Remark 3.1.2. Moreover, the rational map $\tilde{\rho}$ is defined outside the locus defined by the ideal $(2+2U+\omega V)$, which follows from the description of $\tilde{\rho}$ mentioned in 3.7.

REMARK 3.8.1. Let $n = p^r$ or $2p^r$, where p is an odd prime, and put $A_0 = A/(D)$. Then $U_{B/A} \otimes_A A_0$ is a disjoint union of Spec $A_0[U, V]/(2+2U+\omega V)$ and Spec $A_0[U, V]/(2 - 2U - \omega V)$. Also Spec $A_0[U, V]/(2 - 2U - \omega V)$ is isomorphic to the additive group scheme $\boldsymbol{G}_{a,A_0}$, as remarked in 3.1.3. The restriction of $\tilde{\rho} : U_{B/A} \to PGL(2)_A$ to Spec $A_0[U, V]/(2 - 2U - \omega V) \subset U_{B/A} \otimes_A A_0$ is given by

$$\begin{pmatrix} T_{11} & T_{12} \\ T_{21} & T_{22} \end{pmatrix} \mapsto \begin{pmatrix} \dfrac{1+U}{2} & -\dfrac{V}{2} \\ \dfrac{V}{2} & \dfrac{1+U+\omega V}{2} \end{pmatrix}.$$

PROPOSITION 3.9. *The birational map* $\iota : U_{B/A} \to \boldsymbol{P}^1_A$ *is defined*

(1) *outside the locus defined by the ideal* $(U - 1, V, 2)$ *if* n *is a power of* 2;

(2) *everywhere otherwise.*

PROOF. By the definition, the rational map $\iota : U_{B/A} \to \boldsymbol{P}^1_A$ is defined outside the locus defined by D. If n is not a power of a prime nor twice a power of a prime, D is invertible. Hence ι is defined everywhere.

By the assertion in 3.7, we can conclude that the rational map $\iota : U_{B/A} \to \boldsymbol{P}^1_A$ is defined outside the locus $(1-U, V)$. The locus $(1-U, V)$ is nothing but the unit section of the group A-scheme $U_{B/A}$. It follows from Proposition 3.8 that, if $n = p^r$ or $2p^r$ (p is an odd prime), the rational map $\iota : U_{B/A} \to \boldsymbol{P}^1_A$ is defined outside the locus $(2 + 2U + \omega V, p)$. Hence it is sufficient to note that $(2 + 2U + \omega V, p)$ is disjoint with the unit section of $U_{B/A}$ over A.

If $n = 2^r$, the rational map $\iota : U_{B/A} \to \boldsymbol{P}^1_A$ is defined outside the locus (2), which implies the first assertion.

REMARK 3.10. Let K be a field. Assume that $1/n \in K$ and $\omega \in K$. Komatsu [6] established the twisted Kummer theory, introducing a commutative group $T_K = \boldsymbol{P}^1(K) -$

$\{\zeta, \zeta^{-1}\}$ with the multiplication

$$(t, t') \mapsto \frac{tt' - 1}{t + t' - \omega}\,.$$

It is easily verified that $(u, v) \mapsto -(1 + u)/v$ gives rise to an isomorphism $U_{B/A}(K) \xrightarrow{\sim} T_K$.

On the other hand, the rational map $\iota : U_{B/A} \to \boldsymbol{P}^1_A$ defines a map $U_{B/A}(K) \to \boldsymbol{P}^1(K)$ by $(u, v) \mapsto (1 + u)/v$, and $\iota(K) = \boldsymbol{P}^1(K) - \{-\zeta, -\zeta^{-1}\}$. Under this identification, the multiplication of $\boldsymbol{P}^1(K) - \{-\zeta, -\zeta^{-1}\}$ is given by

$$(t, t') \mapsto \frac{tt' - 1}{t + t' + \omega}\,.$$

LEMMA 3.11. *Define a rational map* $\nu : \operatorname{Proj} A[T_1, T_2] \to \operatorname{Proj} A[T_1, T_2]$ *by*

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

Then the diagram of rational maps

$$\begin{array}{ccc} U_{B/A} & \xrightarrow{\iota} & \boldsymbol{P}^1_A \\ {\scriptstyle n}\downarrow & & \downarrow{\scriptstyle \nu} \\ U_{B/A} & \xrightarrow[\iota]{} & \boldsymbol{P}^1_A \end{array}$$

is commutative.

PROOF. We have a commutative diagram of birational maps

$$\begin{array}{ccc} U_{B/A} \otimes_A B & \xrightarrow{\iota \otimes I_B} & \boldsymbol{P}^1_B \\ {\scriptstyle s}\downarrow{\scriptstyle \wr} & & \downarrow{\scriptstyle \wr\, s} \\ \boldsymbol{G}_{m,B} & \xrightarrow[\iota]{} & \boldsymbol{P}^1_B\,, \end{array}$$

as remarked in 2.12.3. Here the birational map $s : \boldsymbol{P}^1_B \to \boldsymbol{P}^1_B$ is defined by

$$(T_1, T_2) \mapsto (T_1 + \zeta T_2, T_1 + \zeta^{-1} T_2) : B[T_1, T_2] \to B[T_1, T_2]\,.$$

Then the birational map $s^{-1} : \boldsymbol{P}^1_B \to \boldsymbol{P}^1_B$ is given by

$$(T_1, T_2) \mapsto \left(\frac{\zeta^{-1} T_1 - \zeta T_2}{\zeta^{-1} - \zeta}, -\frac{T_1 - T_2}{\zeta^{-1} - \zeta}\right).$$

Defining the morphism $n : \boldsymbol{P}^1_B \to \boldsymbol{P}^1_B$ by

$$(T_1, T_2) \mapsto (T_1^n, T_2^n) : B[T_1, T_2] \to B[T_1, T_2]\,,$$

we can verify that the composite of rational maps $\boldsymbol{P}^1_B \xrightarrow{s} \boldsymbol{P}^1_B \xrightarrow{n} \boldsymbol{P}^1_B \xrightarrow{s^{-1}} \boldsymbol{P}^1_B$ is given by

$$(T_0, T_1) \mapsto \left(\frac{\zeta^{-1}(T_0 + \zeta T_1)^n - \zeta(T_0 + \zeta^{-1} T_1)^n}{\zeta^{-1} - \zeta}, -\frac{(T_0 + \zeta T_1)^n - (T_0 + \zeta^{-1} T_1)^n}{\zeta^{-1} - \zeta}\right).$$

Hence we have gotten a commutative diagram of rational maps

$$\begin{array}{ccccccc} U_{B/A} \otimes_A B & \xrightarrow{s} & \boldsymbol{G}_{m,B} & \xrightarrow{\iota} & \boldsymbol{P}^1_B & \xrightarrow{s^{-1}} & \boldsymbol{P}^1_B \\ \big\downarrow n & & \big\downarrow n & & \big\downarrow n & & \big\downarrow \nu\otimes I_B \\ U_{B/A} \otimes_A B & \xrightarrow[s]{} & \boldsymbol{G}_{m,B} & \xrightarrow[\iota]{} & \boldsymbol{P}^1_B & \xrightarrow[s^{-1}]{} & \boldsymbol{P}^1_B \end{array} .$$

This implies the commutativity of the diagram

$$\begin{array}{ccc} U_{B/A} & \xrightarrow{\iota} & \boldsymbol{P}^1_A \\ n\big\downarrow & & \big\downarrow \nu \\ U_{B/A} & \xrightarrow[\iota]{} & \boldsymbol{P}^1_A \end{array} ,$$

since B is faithfully flat over A.

COROLLARY 3.11.1. *The rational map* $\nu : \boldsymbol{P}^1_A \to \boldsymbol{P}^1_A$ *is defined*

(a) *everywhere if* n *is not a prime power nor twice a prime power*;

(b) *outside the locus defined by the ideal* $(T_1 + T_2, p)$ *if* $n = p^r$, *where* p *is a prime*;

(c) *outside the locus defined by the ideal* $(T_1 - T_2, p)$ *if* $n = 2p^r$, *where* p *is a prime.*

PROOF. By the definition, the rational map $s^{-1} : \boldsymbol{P}^1_B \to \boldsymbol{P}^1_B$ is defined outside the locus defined by the ideal (D). Hence the rational map $\nu : \boldsymbol{P}^1_A \to \boldsymbol{P}^1_A$ is defined outside the locus defined by the ideal (D). If n is not a prime power nor twice a prime power, D is invertible in A. Hence the rational map $\nu : \boldsymbol{P}^1_A \to \boldsymbol{P}^1_A$ is defined everywhere. If $n = p^r$ or $n = 2p^r$ (p is a prime), $\nu : \boldsymbol{P}^1_A \to \boldsymbol{P}^1_A$ is defined outside the locus defined by the ideal (p). We obtain the second and third assertions from the following congruence relations:

$$\begin{aligned} &\frac{\zeta^{-1}(T_1 + \zeta T_2)^{p^r} - \zeta(T_1 + \zeta^{-1} T_2)^{p^r}}{\zeta^{-1} - \zeta} \\ &\qquad = \sum_{j=0}^{p^r} \frac{\zeta^{j-1} - \zeta^{-j+1}}{\zeta^{-1} - \zeta} \binom{p^r}{j} T_1^{n-j} T_2^j \equiv (T_1 + T_2)^{p^r} \mod p , \end{aligned}$$

$$\frac{(T_1 + \zeta T_2)^{p^r} - (T_1 + \zeta^{-1} T_2)^{p^r}}{\zeta^{-1} - \zeta} = \sum_{j=1}^{p^r - 1} \frac{\zeta^{j} - \zeta^{-j}}{\zeta^{-1} - \zeta} \binom{p^r}{j} T_1^{n-j} T_2^j \equiv 0 \mod p$$

and

$$\begin{aligned} &\frac{\zeta^{-1}(T_1 + \zeta T_2)^{2p^r} - \zeta(T_1 + \zeta^{-1} T_2)^{2p^r}}{\zeta^{-1} - \zeta} \\ &\qquad = \sum_{j=0}^{2p^r} \frac{\zeta^{j-1} - \zeta^{-j+1}}{\zeta^{-1} - \zeta} \binom{2p^r}{j} T_1^{n-j} T_2^j \equiv (T_1 - T_2)^{2p^r} \mod p , \end{aligned}$$

$$\frac{(T_1+\zeta T_2)^{2p^r}-(T_1+\zeta^{-1}T_2)^{2p^r}}{\zeta^{-1}-\zeta} = \sum_{j=1}^{2p^r-1} \frac{\zeta^j-\zeta^{-j}}{\zeta^{-1}-\zeta}\binom{2p^r}{j} T_1^{n-j}T_2^j \equiv 0 \mod p\,.$$

COROLLARY 3.11.2. *The morphism* $\nu : \boldsymbol{P}^1_{A[1/D]} \to \boldsymbol{P}^1_{A[1/D]}$ *is finite flat, and unramified outside the locus defined by* $(T_1^2+\omega T_1T_2+T_2^2)$. *Moreover, the finite covering* $\nu : \boldsymbol{P}^1_{A[1/D]} \to \boldsymbol{P}^1_{A[1/D]}$ *is cyclic of degree n, and the Galois group of* ν *is generated by*

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

PROOF. The morphism $n : \boldsymbol{P}^1_{A[1/D]} \to \boldsymbol{P}^1_{A[1/D]}$ is finite flat and unramified outside the locus defined by (T_1T_2). Hence the morphism $\nu = s^{-1}\circ n \circ s : \boldsymbol{P}^1_{B[1/D]} \to \boldsymbol{P}^1_{B[1/D]}$ is finite flat, and unramified outside the locus defined by $(T_1+\zeta T_2)(T_1+\zeta^{-1}T_2) = (T_1^2+\omega T_1T_2+T_2^2)$. We obtain the first assertion, since B is faithfully flat over A.

Furthermore, under the identification $\mathrm{Ker}[n : U_{B/A} \to U_{B/A}] \otimes_A A[1/D] = \boldsymbol{Z}/n\boldsymbol{Z}$, the commutative diagram

$$\begin{array}{ccc} U_{B/A} \times_A U_{B/A} & \xrightarrow{\text{multiplication}} & U_{B/A} \\ {\scriptstyle \tilde\rho\times\iota}\downarrow & & \downarrow{\scriptstyle \iota} \\ PGL(2)_A \times_A \boldsymbol{P}^1_A & \xrightarrow[\text{action}]{} & \boldsymbol{P}^1_A \end{array}$$

yields over $A[1/D]$ a commutative diagram

$$\begin{array}{ccc} \boldsymbol{Z}/n\boldsymbol{Z} \times_A U_{B/A} & \xrightarrow{\text{multiplication}} & U_{B/A} \\ {\scriptstyle \tilde\rho\times\iota}\downarrow & & \downarrow{\scriptstyle \iota} \\ \boldsymbol{Z}/n\boldsymbol{Z} \times_A \boldsymbol{P}^1_A & \xrightarrow[\text{action}]{} & \boldsymbol{P}^1_A\,. \end{array}$$

It follows that the rational map $\nu : \boldsymbol{P}^1_A \to \boldsymbol{P}^1_A$ is isomorphic to the canonical surjection $\boldsymbol{P}^1_A \to \boldsymbol{P}^1_A/(\boldsymbol{Z}/n\boldsymbol{Z})$ over $A[1/D]$.

Now, let ξ denote the A-valued point of $U_{B/A}$ defined by $(U, V) \mapsto (0, 1)$. Then ξ is of order n, and we have

$$\tilde\rho(\xi) = \begin{pmatrix} 1 & -1 \\ 1 & 1+\omega \end{pmatrix}.$$

It follows that the Galois group of ν is generated by $(T_1, T_2) \mapsto (T_1 - T_2, T_1 + (1+\omega)T_2)$.

COROLLARY 3.12. *Let R be a local* $\boldsymbol{Z}[\omega, 1/n]$*-algebra and S an unramified cyclic extension of degree n. If n is odd, there exists a morphism* Spec $R \to \boldsymbol{P}^1_A$ *such that the square of rational maps*

$$\begin{array}{ccc} \mathrm{Spec}\, S & \longrightarrow & \boldsymbol{P}^1_A \\ \downarrow & & \downarrow{\scriptstyle \nu} \\ \mathrm{Spec}\, R & \longrightarrow & \boldsymbol{P}^1_A \end{array}$$

is cartesian. More precisely, there exists $c \in R$ such that S is isomorphic to

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

Moreover,

$$T \mapsto \frac{T-1}{T+(1+\omega)}$$

defines a generator of $\mathrm{Gal}(S/R)$.

PROOF. Combining Corollary 3.4 with Lemma 3.11, we obtain the first assertion. Now, take an R-valued point $(u, v) \in U_{B/A}(R)$ such that the square

$$\begin{array}{ccc} \operatorname{Spec} S & \longrightarrow & U_{B/A} \\ \downarrow & & \downarrow n \\ \operatorname{Spec} R & \longrightarrow & U_{B/A} \end{array}$$

is cartesian. Let $\mathfrak{m}$ denote the maximal ideal of R. If $v \in R - \mathfrak{m}$, we can take $c = (1+u)/v$. Assume now that $1 + u \in A - \mathfrak{m}$ and $v \in \mathfrak{m}$. We have $(-1, 0) = (0, -1)^n$ in $U_{B/A}(R)$, since n is odd. Hence, replacing (u, v) by $(-u, -v)$, we can take $c = (-\omega u - v)/(1+u)$. The last assertion follows from Corollary 3.11.2.

REMARK 3.13. Replacing T by $-T$, we obatian the generic polynomial for cyclic extensions of degree n

$$\frac{\{\zeta^{-1}(T-\zeta)^n - \zeta(T-\zeta^{-1})^n\} - Y\{(T-\zeta)^n - (T-\zeta^{-1})^n\}}{\zeta^{-1}-\zeta},$$

discovered by Rikuna [7].

REMARK 3.14. Kida [5] established Kummer theories for norm tori over a field. It is not so difficult to generalize the arranged arguments in [5] as is done here.

4. Twisted Kummer-Artin-Schreier theory. In this section, we fix an odd prime p and a primitive p-th root of unity ζ.

4.1. Let p be a prime number > 2 and ζ a primitive p-th root of unity. Put $\omega = \zeta + \zeta^{-1}$. Let $A = \mathbf{Z}[\omega]$ and $B = \mathbf{Z}[\zeta]$. Then we have a commutative group scheme

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

with the multiplication

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

Put now

$$\lambda = \zeta - \zeta^{-1}$$

and

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

Then we have

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

Furthermore, put

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

and

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

Then $\tilde{B} = A[\theta]$ is a quadratic extension of A defined by $\theta^2 - \tilde{\omega}\theta + \tilde{\eta} = 0$. Then we have a commutative group scheme

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

with

(a) the multiplication

$$\Delta : \begin{cases} X \mapsto X \otimes 1 + 1 \otimes X - \tilde{\omega}X \otimes X - 2\tilde{\eta}X \otimes Y - 2\tilde{\eta}Y \otimes X - \tilde{\omega}\tilde{\eta}Y \otimes Y , \\ Y \mapsto Y \otimes 1 + 1 \otimes Y + (\tilde{\omega}^2 - 2\tilde{\eta})Y \otimes Y + \tilde{\omega}X \otimes Y + \tilde{\omega}Y \otimes X + 2X \otimes X , \end{cases}$$

(b) the unit

$$\varepsilon : \begin{cases} X \mapsto 0 , \\ Y \mapsto 0 , \end{cases}$$

(c) the inverse

$$S : \begin{cases} X \mapsto -X - \tilde{\omega}Y , \\ Y \mapsto Y . \end{cases}$$

THEOREM 4.2 (twisted Kummer-Artin-Schreier theory). *A homomorphism of group A-schemes*

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

is defined by

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

Moreover, Ψ *is finite and étale*, *and* $\mathrm{Ker}\, \Psi$ *is isomorphic to the constant group scheme* $\mathbf{Z}/p\mathbf{Z}$.

PROOF. Define homomorphisms of group schemes

$$\sigma : G_{B/A} \otimes_A B = \operatorname{Spec} B[X, Y]/(X^2 + \omega XY + Y^2 - Y) \\ \to \mathcal{G}^{(\lambda)} = \operatorname{Spec} B\left[T, \frac{1}{1+\lambda T}\right]$$

and

$$\tilde{\sigma} : G_{\tilde{B}/A} \otimes_A B = \operatorname{Spec} B[X, Y]/(X^2 + \tilde{\omega} XY + \tilde{\eta} Y^2 - Y) \\ \to \mathcal{G}^{(\lambda^p)} = \operatorname{Spec} B\left[T, \frac{1}{1+\lambda^p T}\right]$$

by

$$T \mapsto X + \zeta Y, \quad \frac{1}{1+\lambda T} \mapsto 1 - \lambda(X + \zeta^{-1} Y)$$

and

$$T \mapsto X + \Theta(\zeta) Y, \quad \frac{1}{1+\lambda^p T} \mapsto 1 - \lambda^p \{X + \Theta(\zeta^{-1}) Y\},$$

respectively. Then σ and $\tilde{\sigma}$ are isomorphisms, as remarked in 2.4. Moreover we have gotten a commutative diagram of group schemes over B

$$\begin{array}{ccc} G_{B/A} \otimes_A B & \xrightarrow{\Psi \otimes B} & G_{\tilde{B}/A} \otimes_A B \\ \sigma \downarrow \wr & & \downarrow \wr\, \tilde{\sigma} \\ \mathcal{G}^{(\lambda)} & \xrightarrow[\Psi_B]{} & \mathcal{G}^{(\lambda^p)} . \end{array}$$

Here the homomorphism

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

is defined by

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

The homomorphism $\Psi_B : \mathcal{G}^{(\lambda)} \to \mathcal{G}^{(\lambda^p)}$ is surjective and $\operatorname{Ker}[\Psi_B : \mathcal{G}^{(\lambda)} \to \mathcal{G}^{(\lambda^p)}]$ is isomorphic to the constant group scheme $\boldsymbol{Z}/p\boldsymbol{Z}$, as recalled in 1.4. Hence $\Psi : G_{B/A} \to G_{\tilde{B}/A}$ is finite and étale, since B is faithfully flat over A. Moreover, the map $(X, Y) \mapsto (0, 1)$ defines an A-valued point of $\operatorname{Ker}[\Psi : G_{B/A} \to G_{\tilde{B}/A}]$, which is of order p. It follows that $\operatorname{Ker}[\Psi : G_{B/A} \to G_{\tilde{B}/A}]$ is isomorphic to $\boldsymbol{Z}/p\boldsymbol{Z}$.

REMARK 4.2.1. The theorem can be restated as follows. The isogeny $\Psi : G_{B/A} \to G_{\tilde{B}/A}$ is an étale covering with Galois group $\boldsymbol{Z}/p\boldsymbol{Z}$, whose generator is given by

$$X \mapsto -X - \omega Y, \quad Y \mapsto 1 + \omega X + (\omega^2 - 1) Y .$$

We shall call the exact sequence of group schemes over $\boldsymbol{Z}[\omega]$

$$0 \longrightarrow \boldsymbol{Z}/p\boldsymbol{Z} \longrightarrow G_{B/A} \xrightarrow{\Psi} G_{\tilde{B}/A} \longrightarrow 0$$

the twisted Kummer-Artin-Schreier sequence.

REMARK 4.2.2. Define homomorphisms of group schemes over A

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

and

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

by

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

and

$$U \mapsto 1 - D^{(p-1)/2} \omega X - D^{(p-1)/2}\{\zeta^{-1}\Theta(\zeta) + \zeta\Theta(\zeta^{-1})\}Y ,$$
$$V \mapsto 2D^{(p-1)/2} X + D^{(p-1)/2} \tilde{\omega} Y ,$$

respectively. Then we have a commutative diagram with exact rows of group schemes over A

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \boldsymbol{Z}/p\boldsymbol{Z} & \longrightarrow & G_{B/A} & \xrightarrow{\Psi} & G_{\tilde{B}/A} & \longrightarrow & 0 \\ & & \downarrow & & \downarrow{\scriptstyle \alpha} & & \downarrow{\scriptstyle \tilde{\alpha}} & & \\ 0 & \longrightarrow & \boldsymbol{\mu}_{p,A} & \longrightarrow & U_{B/A} & \xrightarrow[p]{} & U_{B/A} & \longrightarrow & 0 . \end{array}$$

Hence

$$(0 \longrightarrow \boldsymbol{Z}/p\boldsymbol{Z} \longrightarrow G_{B/A} \xrightarrow{\Psi} G_{\tilde{B}/A} \longrightarrow 0) \otimes_A A[1/D]$$

is isomorphic to the twisted Kummer sequence

$$(0 \longrightarrow \boldsymbol{Z}/p\boldsymbol{Z} \longrightarrow U_{B/A} \xrightarrow{p} U_{B/A} \longrightarrow 0) \otimes_A A[1/D] .$$

On the other hand,

$$(0 \longrightarrow \boldsymbol{Z}/p\boldsymbol{Z} \longrightarrow G_{B/A} \xrightarrow{\Psi} G_{\tilde{B}/A} \longrightarrow 0) \otimes_A A/(D)$$

is isomorphic to the Artin-Schreier sequence

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

PROPOSITION 4.3. *Let R be a local $\boldsymbol{Z}[\omega]$-algebra. Then $H^1(R, \boldsymbol{Z}/p\boldsymbol{Z})$ is isomorphic to* $\operatorname{Coker}[\Psi : G_{B/A}(R) \to G_{\tilde{B}/A}(R)]$.

PROOF. We obtain the assertion from the exact sequence

$$G_{B/A}(R) \xrightarrow{\Psi} G_{\tilde{B}/A}(R) \longrightarrow H^1(R, \boldsymbol{Z}/p\boldsymbol{Z}) \longrightarrow H^1(R, G_{B/A}) \xrightarrow{\Psi} H^1(R, G_{\tilde{B}/A}) ,$$

noting that $H^1(R, G_{B/A})$ is annihilated by 2.

COROLLARY 4.4. *Let R be a local $\mathbf{Z}[\omega]$-algebra and S an unramified cyclic extension of degree p. Then there exists a morphism* $\operatorname{Spec} R \to G_{\tilde{B}/A}$ *such that the square*

$$\begin{array}{ccc} \operatorname{Spec} S & \longrightarrow & G_{B/A} \\ \big\downarrow & & \big\downarrow \Psi \\ \operatorname{Spec} R & \longrightarrow & G_{\tilde{B}/A} \end{array}$$

is cartesian. More precisely, there exist $a, b \in R$ such that $a^2 + \omega ab + b^2 = b$ and that S is isomorphic to

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

Moreover, the map

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

yields a generator of $\operatorname{Gal}(S/R)$.

EXAMPLE 4.5. Let $p = 3$. Then we have

$$\zeta = \frac{-1 + \sqrt{-3}}{2}\,, \quad \omega = -1\,,$$

and therefore

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

with multiplication

$$\begin{aligned} X &\mapsto X \otimes 1 + 1 \otimes X + X \otimes X - 2X \otimes Y - 2Y \otimes X + Y \otimes Y\,, \\ Y &\mapsto Y \otimes 1 + 1 \otimes Y - Y \otimes Y - X \otimes Y - Y \otimes X + 2X \otimes X\,. \end{aligned}$$

On the other hand, we have

$$\theta = \Theta(\zeta) = \frac{5 - 3\sqrt{-3}}{2}\,, \quad \tilde{\omega} = 5\,, \quad \tilde{\eta} = 13\,,$$

and therefore

$$G_{\tilde{B}/A} = \operatorname{Spec} A[X, Y]/(X^2 + 5XY + 13Y^2 - Y)$$

with multiplication

$$\begin{aligned} X &\mapsto X \otimes 1 + 1 \otimes X - 5X \otimes X - 26X \otimes Y - 26Y \otimes X - 65Y \otimes Y\,, \\ Y &\mapsto Y \otimes 1 + 1 \otimes Y - Y \otimes Y + 5X \otimes Y + 5Y \otimes X + 2X \otimes X\,. \end{aligned}$$

Moreover, the homomorphism

$$\begin{aligned} \Psi : G_{B/A} &= \operatorname{Spec} A[X, Y]/(X^2 - XY + Y^2 - Y) \\ \to G_{\tilde{B}/A} &= \operatorname{Spec} A[X, Y]/(X^2 + 5XY + 13Y^2 - Y) \end{aligned}$$

is defined by

$$X \mapsto -X - 2Y + 4XY + 3Y^2 - 3XY^2 - Y^3\,, \quad Y \mapsto Y - 2Y^2 + Y^3\,.$$

A generator of the Galois group of the étale covering $\Psi : G_{B/A} \to G_{\tilde{B}/A}$ is given by

$$X \mapsto -X + Y\,, \quad Y \mapsto 1 - X\,.$$

Hereafter we establish a one-parameter version of Corollary 4.4, using the equivariant compactification $\iota : G_{B/A} \to \boldsymbol{P}^1_A$.

LEMMA 4.6. *Define a morphism* Ψ : Proj $A[T_0, T_1] \to$ Proj $A[T_0, T_1]$ *by*

$$(T_0, T_1) \mapsto \left(\frac{\Theta(\zeta^{-1})(T_0+\zeta T_1)^p - \Theta(\zeta)(T_0+\zeta^{-1}T_1)^p}{p(\zeta - \zeta^{-1})}, -\frac{(T_0+\zeta T_1)^p - (T_0 + \zeta^{-1}T_1)^p}{p(\zeta - \zeta^{-1})}\right).$$

Then the diagram of A-schemes

$$\begin{array}{ccc} G_{B/A} & \xrightarrow{\iota} & \boldsymbol{P}^1_A \\ {\scriptstyle\Psi}\downarrow & & \downarrow{\scriptstyle\Psi} \\ G_{\tilde{B}/A} & \xrightarrow[\iota]{} & \boldsymbol{P}^1_A \end{array}$$

is cartesian.

PROOF. We have a commutative diagram

$$\begin{array}{ccc} G_{B/A} \otimes_A B & \xrightarrow{\iota \otimes I_B} & \boldsymbol{P}^1_B \\ {\scriptstyle\sigma}\downarrow\wr & & \wr\downarrow{\scriptstyle\sigma} \\ \mathcal{G}^{(\lambda)} & \xrightarrow[\iota]{} & \boldsymbol{P}^1_B\,, \end{array}$$

as remarked in 2.12.2. Here the open immersion

$$\iota : G_{B/A} = \text{Spec}\, A[X, Y]/(X^2 + \omega XY + Y^2 - Y) \to \boldsymbol{P}^1_A = \text{Proj}\, A[T_1, T_2]$$

is defined by

$$T = \frac{T_1}{T_2} \mapsto \frac{2 - \omega X - 2Y}{2X + \omega Y}\,,$$

and the automorphism $\sigma : \boldsymbol{P}^1_B \to \boldsymbol{P}^1_B$ is given by

$$(T_1, T_2) \mapsto (T_2, T_1 + \zeta^{-1}T_2) : B[T_1, T_2] \to B[T_1, T_2]\,.$$

Moreover, we have a commutative diagram

$$\begin{array}{ccc} G_{\tilde{B}/A} \otimes_A B & \xrightarrow{\iota \otimes I_B} & \boldsymbol{P}^1_B \\ {\scriptstyle\tilde{\sigma}}\downarrow\wr & & \wr\downarrow{\scriptstyle\tilde{\sigma}} \\ \mathcal{G}^{(\lambda^p)} & \xrightarrow[\iota]{} & \boldsymbol{P}^1_B\,. \end{array}$$

Here the open immersion

$$\iota : G_{\tilde{B}/A} = \text{Spec}\, A[X, Y]/(X^2 + \tilde{\omega} XY + \tilde{\eta} Y^2 - Y) \to \boldsymbol{P}^1_A = \text{Proj}\, A[T_1, T_2]$$

is defined by

$$T = \frac{T_1}{T_2} \mapsto \frac{2 - \tilde{\omega}X - 2\tilde{\eta}Y}{2X + \tilde{\omega}Y},$$

and the automorphism $\tilde{\sigma} : \boldsymbol{P}^1_B \to \boldsymbol{P}^1_B$ is given by

$$(T_1, T_2) \mapsto (T_2, T_1 + \Theta(\zeta^{-1})T_2) : B[T_1, T_2] \to B[T_1, T_2].$$

Then the automorphism $\tilde{\sigma}^{-1} : \boldsymbol{P}^1_B \to \boldsymbol{P}^1_B$ is defined by

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

Define now a morphism $\Psi_B : \boldsymbol{P}^1_B \to \boldsymbol{P}^1_B$ by

$$(T_1, T_2) \mapsto \left(\frac{(\lambda T_1 + T_2)^p - T_2^p}{\lambda^p}, T_2^p\right) : B[T_1, T_2] \to B[T_1, T_2].$$

Then it is verified that the composite of morphisms $\boldsymbol{P}^1_B \stackrel{\sigma}{\to} \boldsymbol{P}^1_B \stackrel{\Psi_B}{\to} \boldsymbol{P}^1_B \stackrel{\tilde{\sigma}^{-1}}{\to} \boldsymbol{P}^1_B$ is given by

$$(T_0, T_1) \mapsto \left(\frac{\Theta(\zeta^{-1})(T_0 + \zeta T_1)^p - \Theta(\zeta)(T_0 + \zeta^{-1}T_1)^p}{p(\zeta - \zeta^{-1})}, -\frac{(T_0 + \zeta T_1)^p - (T_0 + \zeta^{-1}T_1)^p}{p(\zeta - \zeta^{-1})}\right).$$

Hence we obtain a commutative diagram

$$\begin{array}{ccccccc} G_{B/A} \otimes_A B & \xrightarrow{\sigma} & \mathcal{G}^{(\lambda)} & \xrightarrow{\iota} & \boldsymbol{P}^1_B & \xrightarrow{\sigma^{-1}} & \boldsymbol{P}^1_B \\ \downarrow{\scriptstyle \Psi \otimes I_B} & & \downarrow{\scriptstyle \Psi_B} & & \downarrow{\scriptstyle \Psi_B} & & \downarrow{\scriptstyle \Psi \otimes I_B} \\ G_{\tilde{B}/A} \otimes_A B & \xrightarrow[\tilde{\sigma}]{} & \mathcal{G}^{(\lambda^p)} & \xrightarrow[\tilde{\iota}]{} & \boldsymbol{P}^1_B & \xrightarrow[\tilde{\sigma}^{-1}]{} & \boldsymbol{P}^1_B, \end{array}$$

which implies the commutativity of the diagram

$$\begin{array}{ccc} G_{B/A} & \xrightarrow{\iota} & \boldsymbol{P}^1_A \\ {\scriptstyle \Psi}\downarrow & & \downarrow{\scriptstyle \Psi} \\ G_{\tilde{B}/A} & \xrightarrow[\tilde{\iota}]{} & \boldsymbol{P}^1_A, \end{array}$$

since B is faithfully flat over A.

COROLLARY 4.6.1. *The morphism $\Psi : \boldsymbol{P}^1_A \to \boldsymbol{P}^1_A$ is finite flat, and unramified outside the locus defined by $(T_1^2 + \tilde{\omega}T_1T_2 + \tilde{\eta}T_2^2)$. Moreover, the finite covering $\Psi : \boldsymbol{P}^1_A \to \boldsymbol{P}^1_A$ is cyclic of degree p, and the Galois group of Ψ is generated by*

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

PROOF. The morphism $\Psi : \boldsymbol{P}^1_A \to \boldsymbol{P}^1_A$ is finite flat, and unramified outside the locus defined by (T_1T_2). Hence the morphism $\Psi \otimes I_B = \sigma^{-1} \circ \Psi_B \circ \sigma : \boldsymbol{P}^1_B \to \boldsymbol{P}^1_B$ is finite flat, and unramified outside the locus defined by $(T_1 + \Theta(\zeta)T_2)(T_1 + \Theta(\zeta^{-1})T_2) = (T_1^2 + \tilde{\omega}T_1T_2 + \tilde{\eta}T_2^2)$. We obtain the first assertion since B is faithfully flat over A.

Furthermore, under the identification $\mathrm{Ker}[\Psi : G_{B/A} \to G_{\tilde{B}/A}] = \boldsymbol{Z}/p\boldsymbol{Z}$, the commutative diagram presented in 2.7

$$\begin{array}{ccc} G_{B/A} \times_A G_{B/A} & \xrightarrow{\text{multiplication}} & G_{B/A} \\ {\scriptstyle \tilde{\rho}\times\iota}\downarrow & & \downarrow{\scriptstyle \iota} \\ PGL(2)_A \times_A \boldsymbol{P}^1_A & \xrightarrow[\text{action}]{} & \boldsymbol{P}^1_A \end{array}$$

yields a commutative diagram

$$\begin{array}{ccc} \boldsymbol{Z}/p\boldsymbol{Z} \times_A G_{B/A} & \xrightarrow{\text{multiplication}} & G_{B/A} \\ {\scriptstyle \tilde{\rho}\times\iota}\downarrow & & \downarrow{\scriptstyle \iota} \\ \boldsymbol{Z}/p\boldsymbol{Z} \times_A \boldsymbol{P}^1_A & \xrightarrow[\text{action}]{} & \boldsymbol{P}^1_A . \end{array}$$

It follows that the morphism $\Psi : \boldsymbol{P}^1_A \to \boldsymbol{P}^1_A$ is isomorphic to the canonical surjection $\boldsymbol{P}^1_A \to \boldsymbol{P}^1_A/(\boldsymbol{Z}/p\boldsymbol{Z})$.

Now, let ξ denote the A-valued point of $G_{B/A}$ defined by $(X, Y) \mapsto (0, 1)$. Then ξ is of order p, and we have

$$\tilde{\rho}(\xi) = \begin{pmatrix} 1 & -1 \\ 1 & 1+\omega \end{pmatrix} .$$

It follows that the Galois group of Ψ is generated by $(T_1, T_2) \mapsto (T_1 - T_2, T_1 + (1+\omega)T_2)$.

COROLLARY 4.7. *Let R be a local $\boldsymbol{Z}[\omega]$-algebra and S an unramified cyclic extension of degree p. Then there exists a morphism* $\mathrm{Spec}\, R \to \boldsymbol{P}^1_A$ *such that the square*

$$\begin{array}{ccc} \mathrm{Spec}\, S & \longrightarrow & \boldsymbol{P}^1_A \\ \downarrow & & \downarrow{\scriptstyle \Psi} \\ \mathrm{Spec}\, R & \longrightarrow & \boldsymbol{P}^1_A \end{array}$$

is cartesian. In particular, if the extension S/R does not split completely at the maximal ideal of R, there exists $c \in R$ such that S is isomorphic to

$$R[T]/\left(\frac{\Theta(\zeta^{-1})(T+\zeta)^p - \Theta(\zeta)(T+\zeta^{-1})^p}{p(\zeta-\zeta^{-1})} - c\frac{(T+\zeta)^p - (T+\zeta^{-1})^p}{p(\zeta-\zeta^{-1})}\right).$$

Moreover,

$$T \mapsto \frac{T-1}{T+(1+\omega)}$$

defines a generator of $\mathrm{Gal}(S/R)$.

PROOF. Combining Corollary 4.4 with Lemma 4.6, we obtain the first assertion. Now, take an R-valued point $(a, b) \in G_{\tilde{B}/A}(R)$ such that the square

$$\begin{array}{ccc} \operatorname{Spec} S & \longrightarrow & G_{B/A} \\ \downarrow & & \downarrow n \\ \operatorname{Spec} R & \longrightarrow & G_{\tilde{B}/A} \end{array}$$

is cartesian. Let $\mathfrak{m}$ denote the maximal ideal of R. If the extension S/R does not split completely at $\mathfrak{m}$, we have $2a + \tilde{\omega} b \in A - \mathfrak{m}$. Hence we can take $c = (2 - \tilde{\omega} a - 2\tilde{\eta} b)/(2a + \tilde{\omega})$. The last assertion follows from Corollary 4.6.1.

REMARK 4.8. By a slight modification, we obtain again the everywhere generic polynomial for cyclic extensions of degree p

$$\frac{\{\zeta^{-1}(T-\zeta)^p - \zeta(T-\zeta^{-1})^p\} - Y\{(T-\zeta)^p - (T-\zeta^{-1})^p\}}{p(\zeta^{-1}-\zeta)},$$

discovered by Komatsu [6].

EXAMPLE 4.9. Let $p = 3$. Then the morphism $\Psi : \boldsymbol{P}^1_A \to \boldsymbol{P}^1_A$ is defined by

$$(T_0, T_1) \mapsto (T_0^3 + T_0^2 T_1 - 4T_0 T_1^2 + T_1^3, T_0^2 T_1 - T_0 T_1^2).$$

Moreover, a generator of the Galois group of finite covering $\Psi : \boldsymbol{P}^1_A \to \boldsymbol{P}^1_A$ is given by

$$(T_0, T_1) \mapsto (T_0 - T_1, T_0).$$

REMARK 4.10. In [12, Ch. VI], Serre formulated the existence of a normal basis in a Galois extension of a field in the framework of algebraic groups, deducing the Kummer theory and Artin-Schreier-Witt theory. At the end of Section 9, he remarked:

Lorsqu'on ne suppose plus que k contienne ε, la théorie de Kummer ne s'applique plus. Toutefois, on peut encore, dans certains cas, réduire la dimension de $G(N)$. Lorsque $n = 3$ par exemple, on peut prendre pour quotient de $G(N)$ le groupe orthogonal G pour la forme quadratique $x^2 - xy + y^2$; on voit facilement que ce groupe contient un sous-groupe N cyclique d'ordre 3 formé de points rationnels sur le corps premier, et que l'isogénie $G \to G/N$ vérifie la propriété universelle de la prop. 7.

It is possible also to formulate the twisted Kummer and twisted Kummer-Artin-Schreier theory in the manner of [12], as done for the Kummer-Artin-Schreier-Witt theories of degree p and p^2 in [9] and [10].

REFERENCES

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

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

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

[4] A. GROTHENDIECK, Le groupe de Brauer, Dix exposés sur la cohomologie des schémas, North-Holland (1968), 46–188.
[5] M. KIDA, Kummer theory for norm algebraic tori, J. Algebra 293 (2005), 427–447.
[6] T. KOMATSU, Arithmetic of Rikuna's generic cyclic polynomial and generalization of Kummer theory, Manuscripta Math. 114 (2004), 265–279.
[7] Y. RIKUNA, On simple families of cyclic polynomials, Proc. Amer. Math. Soc. 130 (2002), 33–35.
[8] T. SEKIGUCHI AND N. SUWA, Théories de Kummer-Artin-Schreier, C. R. Acad. Sci. Paris Sér. I Math. 312 (1991), 417–420.
[9] T. SEKIGUCHI AND N. SUWA, On the structure of the group scheme $\mathbf{Z}[\mathbf{Z}/p^n]^\times$, Compos. Math. 97 (1995), 253–271.
[10] T. SEKIGUCHI AND N. SUWA, Théorie de Kummer-Artin-Schreier et applications, J. Théor. Nombres Bordeaux 7 (1995), 177–189.
[11] 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.
[12] J. P. SERRE, Groupes algébriques et corps de classes, Hermann, Paris, 1959.
[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.
[15] W. C. WATERHOUSE AND B. WEISFEILER, One-dimensional affine group schemes, J. Algebra 66 (1980), 550–568.

DEPARTMENT OF MATHEMATICS
CHUO UNIVERSITY
1–13–27 KASUGA, BUNKYO-KU
TOKYO 112–8551
JAPAN

E-mail address: suwa@math.chuo-u.ac.jp