International Journal of Pure and Applied Mathematics
Volume 96 No. 4 2014, 407-425
ISSN: 1311-8080 (printed version); ISSN: 1314-3395 (on-line version)
url: http://www.ijpam.eu
doi: http://dx.doi.org/10.12732/ijpam.v96i4.1

ijpam.eu

ON THE TORSOS FOR SOME GROUP SCHEMES OF PRIME-POWER ORDER

Yohei Toda
Department of Mathematics
Faculty of Science and Engineering
Chuo University
1-13-27, Kasuga, Bunkyo-ku, Tokyo 112-8551, JAPAN

Abstract: By the classification theorem by F. Oort and J. Tate [6], any group scheme of prime order is isomorphic to a group scheme $G_{a,b}$ under the suitable choice of a and b. We computed the torsors for some kinds of group schemes $G_{a,b}$ in [8], which is a joint work with T. Sekiguchi, as in the following way: denote by p a prime number and by $m = \phi(p-1)$ the value of the Euler function ϕ. Suppose $\mathfrak{p}$ is a prime ideal lying over p (which splits completely in $\mathbb{Z}[\zeta]$), where ζ is a primitive $(p-1)$-st root of the unity. In case $\mathfrak{p}$ is principal, the sequence

$$0 \to \mu_{p,B} \to \mathbb{G}_{m,B}^m \xrightarrow{\mathfrak{p}} \mathbb{G}_{m,B}^m \to 0$$

is exact, and the Galois descent of $\mu_{p,B}$ is isomorphic to $G_{a,b}$ under the suitable choice of a and b, thus one can compute the torsors for this kinds of group schemes. The non-principal case is solved by Y. Koide [3] by using our method. The aim of this paper is to study some group schemes of order a power of a prime number. In section from 1 to 3, we would like to review the main result of the papers [6] by F. Oort and J. Tate, [4] by Y. Koide and T. Sekiguchi, and [8] by T. Sekiguchi and Y. Toda. In section 4, we give our main result, namely, the torsor for the Galois descent of $\mu_{p^n,B}$.

Received: October 10, 2013

1. The Classification Theorem by F. Oort and J. Tate

We denote by p a prime number, by ζ a primitive $(p-1)$-st root of the unity, and by A a Λ_p-algebra, where

$$\Lambda_p = \mathbb{Z}\left[\zeta, \frac{1}{p(p-1)}\right] \cap \mathbb{Z}_p,$$

and $\mathbb{Z}_p$ being the ring of p-adic integers.

Theorem 1.1 (F. Oort and J. Tate [6]). *Any finite group A-scheme of order p is isomorphic to the group scheme*

$$G_{a,b} = \operatorname{Spec}\left(A[x]/(x^p - ax)\right)$$

with the group scheme structure

$$m^*(x) = x \otimes 1 + 1 \otimes x - \frac{b}{p-1}\sum_{i=1}^{p-1} \frac{x^i}{\omega_i} \otimes \frac{x^{p-i}}{\omega_{p-i}},$$

where $a, b, \omega_i \in A$ with $ab = \omega_p = p\omega_{p-1}$ and $\omega_i \equiv i! \pmod{p}$.

If A is a local ring, then $G_{a,b} \cong G_{a',b'}$ if and only if there exists $u \in A^\times$ such that $a' = u^{p-1}a$ and $b' = u^{1-p}b$, where $A^\times$ is a multiplicative group of the invertible elements of A. If A has characteristic p, then

$$G_{0,0} = \boldsymbol{\alpha}_p, \quad G_{1,0} = \mathbb{Z}/p\mathbb{Z}, \quad G_{0,1} = \boldsymbol{\mu}_p.$$

2. The Cyclotomic Twisted Torus by Y. Koide and T. Sekiguchi

We denote by n an integer with $n \geq 2$, by $m = \phi(n)$ the value of the Euler function ϕ, by ζ a primitive n-th root of the unity, by G a cyclic group of order n with a generator σ_0, and by $\operatorname{Spec} B/\operatorname{Spec} A$ a G-torsor. Let

$$\Phi_n(x) = \prod_{k \in (\mathbb{Z}/n\mathbb{Z})^\times} (x - \zeta^k) = x^m + a_1 x^{m-1} + \cdots + a_m$$

be the cyclotomic polynomial, and I be the representing matrix of the action of ζ on $\mathbb{Z}[\zeta]$ by the multiplication;

$$I = \begin{pmatrix} 0 & 0 & \cdots & 0 & -a_m \\ 1 & 0 & \cdots & 0 & -a_{m-1} \\ 0 & 1 & \cdots & 0 & -a_{m-2} \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & -a_1 \end{pmatrix}.$$

For a vector $\boldsymbol{x} = (x_1, x_2, \ldots, x_m)$ and a matrix $M = (m_{ij}) \in \mathrm{M}_{m\times l}(\mathbb{Z})$, we define the matrix power $\boldsymbol{x}^M$ by

$$\boldsymbol{x}^M = \left(\prod_{j=1}^{m} x_j^{m_{j1}}, \prod_{j=1}^{m} x_j^{m_{j2}}, \ldots, \prod_{j=1}^{m} x_j^{m_{jl}} \right).$$

G acts on the algebraic torus

$$\mathbb{G}_{m,B}^m = \operatorname{Spec} B \left[x_1, x_2, \ldots, x_m, 1/\prod_{i=1}^{m} x_i \right]$$

by

$$\boldsymbol{x}^{\sigma_0} = (x_1^{\sigma_0}, x_2^{\sigma_0}, \ldots, x_m^{\sigma_0}) = \boldsymbol{x}^I.$$

By this G-action, we obtain the Galois descent of $\mathbb{G}_{m,B}^m$, which we call *a cyclotomic twisted torus of degree* n, and denote it by $\mathbb{G}(n)_A$.

Theorem 2.1 (Y. Koide and T. Sekiguchi [4]). *The cyclotomic twisted torus can be written as*

$$\mathbb{G}(n)_A = \operatorname{Spec} A[\xi_1, \xi_2, \ldots, \xi_n]/\mathsf{A},$$

where $\xi_1, \xi_2, \ldots, \xi_n$ are G-invariant, and the ideal A is given explicitly. Furthermore, the cyclotomic twisted torus is canonically isomorphic to the group scheme

$$\bigcap_{l|n} \operatorname{Ker} \left(\mathrm{Nm}_l : \mathrm{Res}_{B/A} \mathbb{G}_{m,B} \to \mathrm{Res}_{B_l/A} \mathbb{G}_{m,B_l} \right),$$

where Nm_l is the norm map from B to $B_\ell = B^{\left\langle \sigma_0^{n/\ell} \right\rangle}$, and $\mathrm{Res}_{B/A}$ is the Weil restriction from B to A.

3. The Torsor for $G_{a,b}$ by T. Sekiguchi and Y. Toda

Let $n = p_1^{f_1} p_2^{n_2} \cdots p_r^{f_r}$ be the prime decomposition of a positive integer n. For integers $1 \le i_0 < i_1 < \cdots < i_s \le r$, we set $n_{i_0 i_1 \cdots i_s} = n/p_{i_0} p_{i_1} \cdots p_{i_s}$ and $K_{i_0 i_1 \cdots i_s} = \mathbb{F}_{q^{n_{i_0 i_1 \cdots i_s}}}$.

Theorem 3.1 (T. Sekiguchi and Y. Toda [8]). *There exists a following exact sequence which we call a cyclotomic resolution:*

$$0 \to \mathbb{G}(n)_k(k) \xrightarrow{\varepsilon} K^\times \xrightarrow{\partial^0} \prod_{i=1}^{r} K_i^\times \xrightarrow{\partial^1} \prod_{1\le i<j\le r} K_{ij}^\times \xrightarrow{\partial^2} \cdots \xrightarrow{\partial^{r-1}} K_{12\cdots r}^\times \to 0,$$

where the morphisms (∂^i)'s are defined by

$$\partial^0 x = \left(\mathrm{Nm}_{K^\times/K_1^\times} x, \mathrm{Nm}_{K^\times/K_2^\times} x, \ldots, \mathrm{Nm}_{K^\times/K_r^\times} x\right)$$

and

$$(\partial^s \boldsymbol{x})_{i_0 i_1 \cdots i_s} = \prod_{j=0}^{s} \left(\mathrm{Nm}_{K^\times_{i_0 i_1 \cdots \hat{i_j} \cdots i_s}/K^\times_{i_0 i_1 \cdots i_s}} x_{i_0 i_1 \cdots \hat{i_j} \cdots i_s}\right)^{(-1)^j}.$$

Furthermore, one can deduce the following exact sequence of sheaves of groups on $(\mathrm{Spec}\, A)_{\mathrm{flat}}$*:*

$$\begin{aligned} 0 \to \mathbb{G}(n)_A \xrightarrow{\varepsilon} \mathrm{Res}_{B/A}\mathbb{G}_{m,B} &\xrightarrow{\partial^0} \prod_{i=1}^{r} \left(\mathrm{Res}_{B_i/A}\mathbb{G}_{m,B_i}\right) \\ &\xrightarrow{\partial^1} \prod_{1\le i<j\le r} \left(\mathrm{Res}_{B_{ij}/A}\mathbb{G}_{m,B_{ij}}\right) \xrightarrow{\partial^2} \cdots \xrightarrow{\partial^{r-1}} \mathrm{Res}_{B_{12\cdots r}/A}\mathbb{G}_{m,B_{12\cdots r}} \to 0, \end{aligned}$$

where $B_{i_0 i_1 \cdots i_s} = B^{\left\langle \sigma_0^{n_{i_0 i_1 \cdots i_s}} \right\rangle}$.

The next theorem is also essential to compute torsors.

Theorem 3.2 (T. Sekiguchi and Y. Toda [8]). *There exists the canonical isomorphism*

$$\mathrm{End}\,(\mathbb{G}(n)_A) \cong \mathbb{Z}[\zeta],$$

where ζ is a primitive n-th root of the unity. For $\varphi \in \mathrm{End}(\mathbb{G}(n)_A)$, we have that

$$\det\varphi = \mathrm{Nm}\,\varphi = \mathrm{ord}\,(\mathrm{Ker}\,\varphi)\,,$$

where $\det\varphi = \det M$ for the representing matrix M, and $\mathrm{Nm}\,\varphi$ is the norm as an element of $\mathbb{Z}[\zeta]$.

Combining these results, one can compute the torsors for some kinds of group schemes $G_{a,b}$ in the following way: from the exact sequence

$$0 \to \mathbb{G}(n)_A \xrightarrow{\varepsilon} \mathrm{Res}_{B/A}\mathbb{G}_{m,B} \xrightarrow{\partial^0} \mathrm{Ker}\,\partial^1 \to 0,$$

which is obtained by the cyclotomic resolution in Theorem 3.1, we have a long exact sequence

$$\begin{aligned}0 \to H^0(X, \mathbb{G}(n)_A) &\xrightarrow{H^0(X,\varepsilon)} H^0\left(X, \mathrm{Res}_{B/A}\mathbb{G}_{m,B}\right) \xrightarrow{H^0(X,\partial^0)} H^0(X, \mathrm{Ker}\,\partial^1)\\ \xrightarrow{\partial} H^1(X, \mathbb{G}(n)_A) &\xrightarrow{H^1(X,\varepsilon)} H^1\left(X, \mathrm{Res}_{B/A}\mathbb{G}_{m,B}\right) = 0,\end{aligned}$$

where $X = \mathrm{Spec}\, A$. Hence the correspondence $\overline{f} \mapsto \partial f$ gives the isomorphism

$$\mathrm{Coker}\, H^0(X, \partial^0) \xrightarrow{\sim} H^1(X, \mathbb{G}(n)_A),$$

where ∂f is given by the diagram

$$\begin{tikzcd} & & \partial f = f^*\left(\mathrm{Res}_{B/A}\mathbb{G}_{m,B}\right) \arrow[r] \arrow[d] \arrow[dr, phantom, "\square"] & X \arrow[d, "f"] & \\ 0 \arrow[r] & \mathbb{G}(n)_A \arrow[r, "\varepsilon"] & \mathrm{Res}_{B/A}\mathbb{G}_{m,B} \arrow[r, "\partial^0"] & \mathrm{Ker}\,\partial^1 \arrow[r] & 0. \end{tikzcd}$$

Let $\mathfrak{p}$ be a principal prime ideal lying over an odd prime p which splits completely over $\mathbb{Q}(\zeta)$. In fact, p splits completely if and only if $p \equiv 1 \pmod n$ (cf. [10, Prop. 2.14.]). We assume that $n = p - 1$. Let $\theta \in \mathbb{Z}[\zeta]$ be a generator of $\mathfrak{p}$. Then we have an exact sequence

$$0 \to \mu\!\!\mu_{p,B} \xrightarrow{\iota} \mathbb{G}^m_{m,B} \xrightarrow{\theta} \mathbb{G}^m_{m,B} \to 0,$$

where we recognize $\theta \in \mathrm{End}(\mathbb{G}(n)_A)$. The Galois descent theory gives an exact sequence

$$0 \to (\mu\!\!\mu_{p,B})^G \xrightarrow{\iota} \mathbb{G}(n)_A \xrightarrow{\theta} \mathbb{G}(n)_A \to 0.$$

By Theorem 1.1, we have that

$$\mu\!\!\mu_{p,B} \cong \mathrm{Spec}\, B[y]/(y^p - \omega_p y)$$

with the group scheme structure

$$m^*(y) = y \otimes 1 + 1 \otimes y - \frac{1}{p-1}\sum_{i=1}^{p-1} \frac{y^i}{\omega_i} \otimes \frac{y^{p-i}}{\omega_{p-i}},$$

where $\omega_i \in A$ with $\omega_p = p\omega_{p-1}$ and $\omega_i \equiv i! \pmod p$. The Galois group G acts on $\mathrm{Spec}\, B[y]/(y^p - \omega_p y)$ by $y^{\sigma_0} = \zeta^l y$ for some integer $l \in \mathbb{Z}$. Now we assume that there exists $u \in B$ a n-th root of $b \in A^\times$ with $a = b^{-1}\omega_p \in A$, and

$B = A[u]$. We may assume without loss of generality that $u^{\sigma_0} = \zeta^\ell u$, thus $u^{-1}y$ is G-invariant. Therefore by the following equalities

$$y^p - \omega_p y = u^p\left(\left(\frac{y}{u}\right)^p - a\left(\frac{y}{u}\right)\right)$$

and

$$m^*\left(\frac{y}{u}\right) = \left(\frac{y}{u}\right)\otimes 1 + 1\otimes\left(\frac{y}{u}\right) - \frac{b}{p-1}\sum_{i=1}^{p-1} U(i)\left(\frac{y}{u}\right)^i \otimes \left(\frac{y}{u}\right)^{p-i},$$

we have that the Galois descent of $\mu\!\!\mu_{p,B}$ is given by $G_{a,b}$, that is to say, we obtain an exact sequence

$$0 \to G_{a,b} \xrightarrow{\iota} \mathbb{G}(n)_A \xrightarrow{\theta} \mathbb{G}(n)_A \to 0.$$

From this sequence, we obtain a long exact sequence

$$\begin{aligned} 0 \to H^0(X, G_{a,b}) &\xrightarrow{H^0(X,\iota)} H^0(X, \mathbb{G}(n)_A) \xrightarrow{H^0(X,\theta)} H^0(X, \mathbb{G}(n)_A) \\ \xrightarrow{\partial} H^1(X, G_{a,b}) &\xrightarrow{H^1(X,\iota)} H^1(X, \mathbb{G}(n)_A) \xrightarrow{H^1(X,\theta)} H^1(X, \mathbb{G}(n)_A) \\ \xrightarrow{\partial} \cdots, \end{aligned}$$

thus the correspondence

$$\left(\overline{g}, f^*\left(\mathrm{Res}_{B/A}\mathbb{G}_{m,B}\right)\right) \mapsto \partial\, g + \varphi^{-1}\left(\{0\}\times X\right)$$

gives the non-canonical isomorphism

$$\mathrm{Coker}\, H^0(X,\theta) \times \mathrm{Ker}\, H^1(X,\theta) \cong H^1(X, G_{a,b}),$$

where $\varphi^{-1}\left(\{0\}\times X\right)$ is given by the diagram

$$\begin{tikzcd}
G_{a,b} \arrow[d, "\iota"] & \curvearrowright & \varphi^{-1}(\{0\}\times X) \arrow[r] \arrow[d] & X \arrow[d, equal] \\
\mathbb{G}(n)_A \arrow[d, "\theta"] & \curvearrowright & f^*\left(\mathrm{Res}_{B/A}\mathbb{G}_{m,B}\right) \arrow[r] \arrow[d, "\varphi"] & X \arrow[d, equal] \\
\mathbb{G}(n)_A & \curvearrowright & \theta_* f^*\left(\mathrm{Res}_{B/A}\mathbb{G}_{m,B}\right) \arrow[r] & X.
\end{tikzcd}$$

Note that $\theta_* f^*\left(\mathrm{Res}_{B/A}\mathbb{G}_{m,B}\right) \cong \mathbb{G}(n)_A \times X$.

4. The Torsor for the Galois Descent of $\boldsymbol{\mu}_{p^n,B}$

As in the previous section, we denote by p an odd prime number, by $m = \phi(p-1)$ the value of the Euler function ϕ, by ζ a primitive $(p-1)$-st root of the unity, by G a cyclic group of order $p-1$ generated by σ_0, and by $\operatorname{Spec} B/\operatorname{Spec} A$ a G-torsor. We assume that the base scheme lies over $\operatorname{Spec} \Lambda_p$, where

$$\Lambda_p = \mathbb{Z}\left[\zeta, \frac{1}{p(p-1)}\right] \cap \mathbb{Z}_p,$$

and $\mathbb{Z}_p$ being the ring of p-adic integers. We suppose that $\mathsf{p} \subset \mathbb{Z}[\zeta]$ is a principal prime ideal lying over p. Note that p splits completely in $\mathbb{Z}[\zeta]$. Then we obtain the exact sequence

$$0 \to \boldsymbol{\mu}_{p^n,B} \to \mathbb{G}_{m,B}^m \xrightarrow{\mathsf{p}^n} \mathbb{G}_{m,B}^m \to 0,$$

for $n \in \mathbb{Z}$. We now study the group scheme

$$\boldsymbol{\mu}_{p^n,B} = \operatorname{Spec} B[z]/(z^{p^n} - 1).$$

Note that this argument can be generalized to the non-principal case by using the concept of the homomorphisms defined by ideals, which is introduced by Y. Koide [3].

Lemma 4.1. *The group $(\mathbb{Z}/p^n\mathbb{Z})^\times$ is cyclic and*

$$(\mathbb{Z}/p^n\mathbb{Z})^\times \cong \mathbb{Z}/p^{n-1}\mathbb{Z} \times \mathbb{Z}/(p-1)\mathbb{Z}.$$

Proof. We define the subgroups $H_{p^{n-1}}$ and H_{p-1} of $(\mathbb{Z}/p^n\mathbb{Z})^\times$ by

$$H_{p^{n-1}} = \{\, x \in (\mathbb{Z}/p^n\mathbb{Z})^\times \mid x^{p^{n-1}} = 1 \,\}$$

and

$$H_{p-1} = \{\, x \in (\mathbb{Z}/p^n\mathbb{Z})^\times \mid x^{p-1} = 1 \,\}.$$

Since $(\mathbb{Z}/p^n\mathbb{Z})^\times \cong H_{p^{n-1}} \times H_{p-1}$, it suffices to show that $H_{p^{n-1}}$ and H_{p-1} are cyclic. By Lemma 4.2, we have that $1+p$ is a generator of $H_{p^{n-1}}$, thus $H_{p^{n-1}}$ is cyclic. Next we consider the exact sequence

$$1 \to 1 + p\,(\mathbb{Z}/p^n\mathbb{Z}) \to (\mathbb{Z}/p^n\mathbb{Z})^\times \to (\mathbb{Z}/p\mathbb{Z})^\times \to 1.$$

Since $1 + p\,(\mathbb{Z}/p^n\mathbb{Z}) \cong H_{p^{n-1}}$, we have that

$$H_{p-1} \cong (\mathbb{Z}/p^n\mathbb{Z})^\times / (1 + p\,(\mathbb{Z}/p^n\mathbb{Z})) \cong (\mathbb{Z}/p\mathbb{Z})^\times,$$

thus H_{p-1} is cyclic. $\square$

Lemma 4.2. *$1+p$ is of order p^{n-1} in $(\mathbb{Z}/p^n\mathbb{Z})^\times$.*

Proof. In fact, we see that

$$(1+p)^{p^l} = 1 + \binom{p^l}{1}p + \binom{p^l}{2}p^2 + \cdots + \binom{p^l}{k}p^k + \cdots + p^{p^l}.$$

Since

$$\begin{aligned}
\operatorname{ord}_p \binom{p^l}{k} &= \operatorname{ord}_p \left(p^l \cdot \frac{p^l - 1}{1} \cdot \frac{p^l - 2}{2} \cdots \frac{p^l - (k-1)}{k-1} \cdot \frac{1}{k} \right) \\
&= \operatorname{ord}_p \left(p^l\right) + \operatorname{ord}_p \left(\frac{1}{k}\right) \\
&= l - \operatorname{ord}_p k,
\end{aligned}$$

we have that

$$\operatorname{ord}_p \left(\binom{p^l}{k} p^k \right) = l + k - \operatorname{ord}_p k \geq l + k - \log_p k = l + k - \frac{\log k}{\log p}.$$

By setting

$$f(x) = x - \frac{\log x}{\log p},$$

we have

$$f'(x) = 1 - \frac{1}{x \log p},$$

thus $f(x)$ is monotonic increase for $x \geq (\log p)^{-1}$. Since $f(3) \geq 2$ and $p \neq 2$, we have that $k - \operatorname{ord}_p k \geq 2$ for $k \geq 2$, and

$$\operatorname{ord}_p \left(\binom{p^l}{k} p^k \right) \geq l + 2 \quad \text{for} \quad k \geq 2.$$

Hence

$$(1+p)^{p^l} = 1 + p^{l+1} \left(1 + (\text{multiple by } p)\right),$$

and we obtain that

$$(1+p)^{p^l} \begin{cases} \not\equiv 1 \pmod{p^n} & \text{if } l < f - 1, \\ \equiv 1 \pmod{p^n} & \text{if } l = f - 1. \end{cases}$$

□

Remark. In case $p = 2$, we have the isomorphisms

$$(\mathbb{Z}/4\mathbb{Z})^\times \cong \mathbb{Z}/2\mathbb{Z}, \quad \text{and} \quad (\mathbb{Z}/2^n\mathbb{Z})^\times \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2^{n-2}\mathbb{Z} \quad \text{for } n \geq 3,$$

thus $(\mathbb{Z}/2^n\mathbb{Z})^\times$ is not cyclic for $n \geq 3$. In fact, we can define group homomorphism

$$\varphi : \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2^{n-2}\mathbb{Z} \to (\mathbb{Z}/2^n\mathbb{Z})^\times$$

by $\varphi(a, b) = (-1)^a 3^b$. We show that 3 is or order 2^{n-2} in $(\mathbb{Z}/2^n\mathbb{Z})^\times$. It is clear that 3 is of order 2 in $(\mathbb{Z}/8\mathbb{Z})^\times$. Suppose $n \geq 4$. By the same argument in Lemma 4.2, we have that

$$\operatorname{ord}_2\left(\binom{2^l}{k}2^k\right) = l + k - \operatorname{ord}_2(k) \begin{cases} = l+1 & \text{for } k = 1, 2, \\ = l+2 & \text{for } k = 4, \\ \geq l+3 & \text{for } k = 3 \text{ or } k \geq 5, \end{cases}$$

where $l \geq 2$. Hence

$$\begin{aligned} (1+2)^{2^l} &= 1 + \binom{2^l}{1}2 + \binom{2^l}{2}2^2 + \cdots + \binom{2^l}{k}2^k + \cdots + 2^{2^l} \\ &= 1 + 2^{l+1}\left(1 + (2^l - 1) + 2s + 2^2 t\right) \\ &= 1 + 2^{l+1}\left(2^l + 2s + 2^2 t\right) \\ &= 1 + 2^{l+2}\left(s + 2^{l-1} + 2t\right), \end{aligned}$$

where $s, t \in \mathbb{Z}$ with $(s, 2) = 1$. Therefore we have that

$$3^{p^l} \begin{cases} \not\equiv 1 \pmod{2^n} & \text{if } l < n-2, \\ \equiv 1 \pmod{2^n} & \text{if } l = n-2. \end{cases}$$

Suppose $\varphi(a, b) = 1$, then $3^b \equiv 1$ or $-1 \pmod{2^n}$. If $3^b \equiv 1$, then it contradicts that 3 is of order 2^{n-2} in $(\mathbb{Z}/2^n\mathbb{Z})^\times$. If $3^b \equiv -1$, then it contradicts that $3^l \not\equiv -1 \pmod 8$ for $l \in \mathbb{Z}$. Hence φ is injective. By comparing the orders of the groups, we see that φ is isomorphism. $\square$

We now continue our discussion in case $p \neq 2$. We fix elements $\alpha, \beta \in (\mathbb{Z}/p^n\mathbb{Z})^\times$ with $\beta \equiv \zeta \pmod p$, whose orders are p^{n-1} and $p - 1$ respectively. Using α and β, we define the actions of $\langle 1\rangle \in \mathbb{Z}/p^{n-1}\mathbb{Z}$ and $[1] \in \mathbb{Z}/(p-1)\mathbb{Z}$ on $\boldsymbol{\mu}_{p^n,B}$ by

$$\langle 1\rangle z = z^\alpha \quad \text{and} \quad [1]z = z^\beta.$$

The augmentation ideal J of $B[z]/(z^{p^n}-1)$ is given by

$$J=(z-1)B[z]/(z^{p^n}-1),$$

and has a B-basis $\{\,1-z^k \mid 1\le k\le p^n-1\,\}$. For $j\in\mathbb{Z}$, we set

$$e_j=\frac{1}{p-1}\sum_{k=1}^{p-1}\zeta^{-(k-1)j}[k-1]\in B\big[\mathbb{Z}/(p-1)\mathbb{Z}\big]$$

and $J_j=e_jJ$. Clealy e_j, hence also J_j, depends only on $j \pmod{p-1}$.

Lemma 4.3. *J is the direct sum of J_j for $1\le j\le p-1$. Furthermore, we have that*

$$J_j=\Big\{\, f\in B[z]/(z^{p^n}-1)\mid [k]f=\zeta^{kj}f\,\Big\},$$

and $J_iJ_j\subset J_{i+j}$ for $i,j\in\mathbb{Z}$.

Proof. The elements $e_1,e_2,\dots,e_{p-1}$ are orthogonal idempotents in the group ring $B\big[\mathbb{Z}/(p-1)\mathbb{Z}\big]$, whose sum is 1, since

$$\begin{aligned} e_ie_j &= \left(\frac{1}{p-1}\right)^2\sum_{1\le s,t\le p-1}\zeta^{-(s-1)i-(t-1)j}[(s+t-1)-1]\\ &= \left(\frac{1}{p-1}\right)^2\sum_{1\le s,k\le p-1}\zeta^{-(s-1)i-(k-l)j}[k-1]\\ &= \left(\frac{1}{p-1}\right)^2\sum_{k=1}^{p-1}\zeta^{-kj+i}\left(\sum_{s=1}^{p-1}\zeta^{-(i-j)s}\right)[k-1]\\ &= \begin{cases} \dfrac{1}{p-1}\displaystyle\sum_{k=1}^{p-1}\zeta^{-(k-1)j}[k-1] & \text{if } i=j,\\ 0 & \text{if } i\ne j, \end{cases} \end{aligned}$$

and

$$\sum_{j=1}^{p-1}e_j=\frac{1}{p-1}\sum_{k=1}^{p-1}\left(\sum_{j=1}^{p-1}\zeta^{-(k-1)j}\right)[k-1]=1.$$

Furthermore, we see that

$$[k]e_j=\frac{1}{p-1}\sum_{s=1}^{p-1}\zeta^{-(s-1)j}[k+s-1]=\zeta^{kj}e_j.$$

Hence J is the direct sum of J_j for $1 \le j \le p-1$, and J_j consists of $f \in J$ such that $[k]f = \zeta^{kj} f$ for $k \in \mathbb{Z}/(p-1)\mathbb{Z}$. Then we see that $J_i J_j \subset J_{i+j}$ for $f \in J_i$ and $g \in J_j$, since

$$[k](fg) = ([k]f)([k]g) = \zeta^{ki} f \zeta^{kj} g = \zeta^{k(i+j)}(fg).$$

□

We set

$$q = (p^n - 1)/(p-1) = \sum_{k=1}^{n} p^{n-k},$$

$$p_i = \begin{cases} 1 & \text{if } 1 \le \bar{i} \le p^{n-1}, \\ p^j & \text{if } \displaystyle\sum_{k=1}^{j} p^{n-k} + 1 \le \bar{i} \le \sum_{k=1}^{j+1} p^{n-k}, \end{cases}$$

and

$$y_{i,j} = (p-1)\, e_j \,(1 - \langle i-1 \rangle z^{p_i})$$

for $i, j \in \mathbb{Z}$, where $\bar{i} = i \pmod q$. Note that $y_{i,j}$ depends only on $i \pmod q$ and $j \pmod{p-1}$. By the definition of $y_{i,j}$, we have the equality

$$\begin{aligned} y_{i,j} &= \sum_{k=1}^{p-1} \zeta^{-(k-1)j} \,(1 - [k-1]\langle i-1 \rangle z^{p_i}) \\ &= \begin{cases} (p-1) - \displaystyle\sum_{k=1}^{p-1} z^{a_{i,k}} & \text{if } j \equiv 0 \pmod{p-1}, \\ -\displaystyle\sum_{k=1}^{p-1} \zeta^{-(k-1)j} z^{a_{i,k}} & \text{otherwise,} \end{cases} \end{aligned}$$

where $a_{i,k} = p_i \alpha^{i-1} \beta^{k-1}$. Therefore we have that

$$1 - z^{a_{i,k}} = \frac{1}{p-1} \sum_{j=1}^{p-1} \zeta^{(k-1)j}\, y_{i,j}, \tag{1}$$

for $k \in \mathbb{Z}$, and

$$\begin{aligned} &m^*(y_{i,j}) - y_{i,j} \otimes 1 - 1 \otimes y_{i,j} \\ &\qquad = -\sum_{k=1}^{p-1} \zeta^{-(k-1)j} \big((1 - z^{a_{i,k}}) \otimes (1 - z^{a_{i,k}})\big) \end{aligned}$$

$$
\begin{aligned}
&= -\frac{1}{(p-1)^2}\sum_{k=1}^{p-1}\zeta^{-(k-1)j}\sum_{s=1}^{p-1}\sum_{t=1}^{p-1}\zeta^{(k-1)s}\zeta^{(k-1)t}y_{i,s}\otimes y_{i,t} \\
&= -\frac{1}{p-1}\sum_{\substack{s+t\equiv j \\ (\mathrm{mod}\ p-1)}} y_{i,s}\otimes y_{i,t}.
\end{aligned}
$$

Hence

$$m^*(y_{i,j}) = y_{i,j}\otimes 1 + 1\otimes y_{i,j} - \frac{1}{p-1}\sum_{k=1}^{p-1} y_{i,k}\otimes y_{i,j-k}.$$

Formula (1) shows that

$$J = \sum_{i=1}^{q}\sum_{j=1}^{p-1} By_{i,j},$$

hence

$$J_j = \sum_{i=1}^{q} By_{i,j}$$

for $j \in \mathbb{Z}$. Setting $y_i = y_{i,1}$, we can therefore define elements $b_{i,j,k} \in B$ by

$$y_i^k = \sum_{j=1}^{q} b_{i,j,k}y_{j,k},$$

that is to say, we have the equality

$$\begin{pmatrix} y_1^k \\ y_2^k \\ \vdots \\ y_q^k \end{pmatrix} = \begin{pmatrix} b_{1,1,k} & b_{1,2,k} & \cdots & b_{1,q,k} \\ b_{2,1,k} & b_{2,2,k} & \cdots & b_{2,q,k} \\ \vdots & \vdots & \ddots & \vdots \\ b_{q,1,k} & b_{q,2,k} & \cdots & b_{q,q,k} \end{pmatrix} \begin{pmatrix} y_{1,k} \\ y_{2,k} \\ \vdots \\ y_{q,k} \end{pmatrix}.$$

Setting $M_{p^n,k} := (b_{i,j,k})_{1\le i,j\le q}$, we have the following.

Lemma 4.4. *The matrix $M_{p^n,k}$ is formed of*

$$M_{p^n,k} = \begin{pmatrix} M_{p^n,k,1} & & & * \\ & M_{p^n,k,2} & & \\ & & \ddots & \\ O & & & M_{p^n,k,n} \end{pmatrix},$$

where $M_{p^n,k,j}$ is a matrix of size p^{n-j}, satisfies $M_{p^n,k,j} = M_{p^{n-1},k,j-1}$ for $2 \leq j \leq n$, and each matrix $M_{p^n,k,j}$ is formed of

$$M_{p^n,k,j} = \begin{pmatrix} m_1 & m_2 & m_3 & \cdots & m_{p^{n-j}} \\ m_{p^{n-j}} & m_1 & m_2 & \cdots & m_{p^{n-j}-1} \\ m_{p^{n-j}-1} & m_{p^{n-j}} & m_1 & \cdots & m_{p^{n-j}-2} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ m_2 & m_3 & m_4 & \cdots & m_1 \end{pmatrix}.$$

Proof. Set

$$M_{p^n,k,j} = (b_{r+i,r+j,k})_{1\leq i,j\leq p^{n-j}} \quad \text{and} \quad M_{p^{n-1},k,j-1} = (b'_{r'+i,r'+j,k})_{1\leq i,j\leq p^{n-j}},$$

where

$$r = \sum_{k=1}^{j-1} p^{n-k} \quad \text{and} \quad r' = \begin{cases} 0 & \text{if } j = 2, \\ \displaystyle\sum_{k=2}^{j-1} p^{n-k} & \text{otherwise.} \end{cases}$$

Let z', e'_j and y'_i be the analogous for $\mu\!\!\mu_{p^{n-1},B}$ of z, e_j and y_i for $\mu\!\!\mu_{p^n,B}$. For $1 \leq i \leq p^{n-j}$, we have the equalities

$$\begin{aligned} y^k_{r+i} &= \sum_{s=1}^{q} b_{r+i,s,k} y_{s,k} \\ &= \sum_{s=1}^{p^{n-j}} b_{r+i,r+s,k} y_{r+s,k} + \left(\text{terms of } z^{p^j}, z^{2p^j}, \ldots\right) \end{aligned} \tag{2}$$

and

$$\begin{aligned} (y'_{r'+i})^k &= \sum_{s=1}^{q} b'_{r'+i,s,k} y'_{s,k} \\ &= \sum_{s=1}^{p^{s-j}} b'_{r'+i,r'+s,k} y'_{r'+s,k} + \left(\text{terms of } (z')^{p^{j-1}}, (z')^{2p^{j-1}}, \ldots\right), \end{aligned}$$

where $z^{p^n} = 1$, $(z')^{p^{n-1}} = 1$,

$$y_{r+i,k} = (p-1)e_j \left(1 - \langle i-1\rangle z^{p^{j-1}}\right)$$

and

$$y'_{r'+i,k} = (p-1)e_j \left(1 - \langle i-1\rangle (z')^{p^{j-2}}\right).$$

Setting $Z = z^p$, we have $Z^{p^{n-1}} = 1$, and therefore we can identify

$$y_{r+i,k} = (p-1)e_j \left(1 - \langle i-1 \rangle Z^{p^{j-2}}\right)$$

as $y'_{r'+i,j}$, thus $b_{r+i,r+j,k} = b'_{r'+i,r'+j,k}$ for $1 \le i, j \le p^{n-j}$. Furthermore, by the relation (2), we have that

$$\begin{aligned}
b_{r+i,r+j,k} &= -\left(\text{the coefficient of } z^{\alpha^{r+j-1}} \text{ of } y^k_{r+i}\right) \\
&= - \sum_{\substack{0 \le e_1, e_2, \ldots, e_k \le p-2 \\ \alpha^{r+j-1} \equiv \alpha^{r+i-1}(\beta^{e_1} + \beta^{e_2} + \cdots + \beta^{e_k}) \\ (\mathrm{mod}\ p^n)}} \zeta^{-(e_1 + \cdots + e_k)} \\
&= - \sum_{\substack{0 \le e_1, e_2, \ldots, e_k \le p-2 \\ \alpha^{r+j} \equiv \alpha^{r+i}(\beta^{e_1} + \beta^{e_2} + \cdots + \beta^{e_k}) \\ (\mathrm{mod}\ p^n)}} \zeta^{-(e_1 + \cdots + e_k)} \\
&= -\left(\text{the coefficient of } z^{\alpha^{r+j}} \text{ of } y^k_{r+i+1}\right) \\
&= b_{r+\bar{i}+1, r+\bar{j}+1, k}.
\end{aligned}$$

□

Lemma 4.5. *For a prime number p and a positive integer l, the determinant of the matrix*

$$M = \begin{pmatrix} m_1 & m_2 & m_3 & \cdots & m_{p^l} \\ m_{p^l} & m_1 & m_2 & \cdots & m_{p^l-1} \\ m_{p^l-1} & m_{p^l} & m_1 & \cdots & m_{p^l-2} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ m_2 & m_3 & m_4 & \cdots & m_1 \end{pmatrix}$$

is given by

$$\det M \equiv \sum_{i=1}^{p^l} m_i \pmod{p}.$$

Proof. Let ω be a primitive p^l-th root of the unity. Setting

$$\Omega = \left(\omega^{(i-1)(j-1)}\right)_{1 \le i,j \le p^l},$$

we see that

$$M\Omega = \Omega \begin{pmatrix} \sum_{i=1}^{p^l} m_i & & & \\ & \sum_{i=1}^{p^l} \omega^{i-1} m_i & & \\ & & \ddots & \\ & & & \sum_{i=1}^{p^l} \omega^{(p^l-1)(i-1)} m_i \end{pmatrix}.$$

Since

$$\det \Omega = \sum_{1 \le i < j \le p^l} \left(\omega^i - \omega^j \right) \neq 0,$$

we obtain

$$\det M = \sum_{j=1}^{p^l} \sum_{i=1}^{p^l} \omega^{(i-1)(j-1)} m_i \equiv \sum_{i=1}^{p^l} m_i \pmod{p}.$$

□

Lemma 4.6. *We have* $\det M_{p^n,k,j} \equiv k! \pmod{p}$, *thus* $\det M_{p^n,k} \equiv (k!)^n \pmod{p}$ *and* $M_{p^n,k}$ *is invertible for* $1 \le k \le p-1$.

Proof. By Lemma 4.4, it suffices to show that $M_{p^n,k,1} \equiv k! \pmod{p}$. By setting $Z = z^{p^{n-1}}$, we have

$$y_q = \sum_{k=1}^{p-1} \zeta^{-(k-1)} \left(1 - Z^{\beta^{k-1}} \right)$$

with $Z^p = 1$. Hence we can reduct it the case of Oort-Tate's one, thus $b_{q,q,k} \equiv k! \pmod{p}$. On the other hand,

$$\begin{aligned} b_{q,q,k} &= -\left(\text{the coefficient of } Z \text{ of } y_q^k \right) \\ &= - \sum_{\substack{0 \le n_1, n_2, \ldots, n_k \le p-2 \\ 1 \equiv \beta^{n_1} + \beta^{n_2} + \cdots + \beta^{n_k} \pmod{p}}} \zeta^{-(n_1+n_2+\cdots+n_k)} \end{aligned}$$

$$
\begin{aligned}
&= -\sum_{j=1}^{p^{n-1}} \sum_{\substack{0\le n_1,n_2,\dots,n_k\le p-2\\ \alpha^{j-1}\equiv \beta^{n_1}+\beta^{n_2}+\cdots+\beta^{n_k} \pmod{p^n}}} \zeta^{-(n_1+n_2+\cdots+n_k)}\\
&= -\sum_{j=1}^{p^{n-1}} \left(\text{the coefficient of } z^{\alpha^{j-1}} \text{ of } y_q^k\right)\\
&= \sum_{j=1}^{p^{n-1}} b_{1,j,k}.
\end{aligned}
$$

Therefore we have that

$$
\det M_{p^n,k,j} \equiv \sum_{j=1}^{p^{n-1}} b_{1,j,k} \equiv k! \pmod{p}.
$$

□

For $i, j \in \mathbb{Z}$, we define elements $c_{i,j,k} \in B$ by

$$
y_i y_j = \sum_{k=1}^{q} c_{i,j,k} y_k^2.
$$

Setting

$$
F_{ij} = y_i y_j - \sum_{k=1}^{q} c_{i,j,k} y_k^2, \quad F_i = y_i^p - \sum_{j=1}^{q} b_{i,j,p} y_j
$$

and $M_k^{-1} = (d_{i,j,k})_{1\le i,j\le q}$, we have that

$$
B[z]/(z^{p^n}-1) = B[y_1, y_2, \dots, y_q]/\mathsf{A}
$$

with the co-multiplication

$$
m^*(y_i) = y_i \otimes 1 + 1 \otimes y_i - \frac{1}{p-1}\sum_{k=1}^{p-1}\left(\sum_{s=1}^{q} d_{i,s,k} y_s^k \otimes \sum_{t=1}^{q} d_{i,t,p-k} y_t^{p-k}\right),
$$

where the ideal A is given by

$$
\mathsf{A} = \big(\{\, F_{ij} \mid 1 \le i < j \le q \,\}, \{\, F_i \mid 1 \le i \le q \,\}\big).
$$

The Galois group G acts on $\operatorname{Spec} B[y_1, y_2, \dots, y_q]/\mathsf{A}$ by $y_i^{\sigma_0} = \zeta y_i$ under the suitable choice of β. Now we assume that there exists $u \in B$ a $(p-1)$-st root of $b \in A^\times$ with $B = A[u]$. We may assume without loss of generality that $u^{\sigma_0} = \zeta u$. Hence $u^{-1}y_i$ is G-invariant. By the equalities

$$\frac{F_{ij}}{u^2} = \left(\frac{y_i}{u}\right)\left(\frac{y_j}{u}\right) - \sum_{k=1}^{q} c_{i,j,k}\left(\frac{y_k}{u}\right)^2, \quad \frac{F_i}{u^p} = \left(\frac{y_i}{u}\right)^p - \frac{1}{b}\sum_{j=1}^{q} b_{i,j,p}\left(\frac{y_j}{u}\right),$$

and

$$\begin{aligned} m^*\left(\left(\frac{y_i}{u}\right)\right) &= \left(\frac{y_i}{u}\right)\otimes 1 + 1 \otimes \left(\frac{y_i}{u}\right) \\ &\quad - \frac{b}{p-1}\sum_{k=1}^{p-1}\left(\sum_{s=1}^{q} d_{i,s,k}\left(\frac{y_s}{u}\right)^k \otimes \sum_{t=1}^{q} d_{i,t,p-k}\left(\frac{y_t}{u}\right)^{p-k}\right), \end{aligned}$$

we obtain the Galois descent $(\mu_{p^n,B})^G$ and the exact sequence

$$0 \to (\mu_{p^n,B})^G \to \mathbb{G}(p-1)_A \xrightarrow{\mathsf{p}^n} \mathbb{G}(p-1)_A \to 0,$$

where p is a prime ideal of $\mathbb{Z}[\zeta]$ lying over p. Therefore in the same argument in the previous section, one can compute the torsors for $(\mu_{p^n,B})^G$.

Example 4.7. If $p = 5$, then $\mathsf{p} = (2+\zeta) \subset \mathbb{Z}[\zeta]$ is one of the prime ideals lying over 5, where ζ is a primitive 4th root of the unity. Set

$$\theta = (2+\zeta)^2 = 3 + 4\zeta \in \mathbb{Z}[\zeta].$$

The endomorphism corresponding θ is given by

$$\Theta = \begin{pmatrix} 3 & -4 \\ 4 & 3 \end{pmatrix}.$$

Since

$$\begin{pmatrix} 1 & 0 \\ 7 & 1 \end{pmatrix}\begin{pmatrix} 3 & -4 \\ 4 & 3 \end{pmatrix}\begin{pmatrix} -1 & 4 \\ -1 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 5^2 \end{pmatrix},$$

we have that

$$\begin{aligned} \operatorname{Ker}\Theta &\cong \operatorname{Spec} B[x, y, 1/xy]/(x - y^7, y^{5^2} - 1) \\ &\cong \operatorname{Spec} B[z]/(z^{5^2} - 1) \\ &\cong \mu_{5^2,B} \end{aligned}$$

with the G-action $z^{\sigma_0} = z^{18}$. We can define actions of $\langle 1 \rangle \in \mathbb{Z}/5\mathbb{Z}$ and $[1] \in \mathbb{Z}/4\mathbb{Z}$ on $\mu_{5^2,B}$ by $\langle 1 \rangle z = z^6$ and $[1]z = z^{18}$. The group scheme $\mu_{5^2,B}$ is isomorphic to $\operatorname{Spec} B[y_1, y_2, y_3, y_4, y_5, y_6]/\mathsf{A}$ with co-multiplication

$$m^*(y_i) = y_i \otimes 1 + 1 \otimes y_i - \frac{1}{4}\sum_{k=1}^{4}\left(\sum_{s=1}^{6} d_{i,s,k} y_s^k \otimes \sum_{t=1}^{6} d_{i,t,5-k} y_t^{5-k}\right).$$

G acts on $\operatorname{Spec} B[y_1, y_2, y_3, y_4, y_5, y_6]/\mathsf{A}$ by

$$\begin{aligned} y_i^{\sigma_0} &= -\sum_{l=1}^{4} \zeta^{-(l-1)} (z^{\sigma_0})^{a_{i,l}} \\ &= -\sum_{l=1}^{4} \zeta^{-(l-1)} z^{a_{i,l+1}} \\ &= -\zeta \sum_{l=1}^{4} \zeta^{-l} z^{a_{i,l+1}} \\ &= \zeta y_i. \end{aligned}$$

Now we assume that there exists $u \in B$ a 4th root of $b \in A^\times$ and $B = A[u]$. We may assume without loss of generality that $u^{\sigma_0} = \zeta u$. Then $u^{-1} y_i$ is G-invariant.

Example 4.8. If $p = 7$, then $\mathsf{p} = (2+\zeta) \subset \mathbb{Z}[\zeta]$ is one of the prime ideals lying over 7, where ζ is a primitive 6th root of the unity. Set

$$\theta = (2+\zeta)^3 = 1 + 18\zeta \in \mathbb{Z}[\zeta].$$

The endomorphism corresponding θ is given by

$$\Theta = \begin{pmatrix} 1 & -18 \\ 18 & 19 \end{pmatrix}.$$

Since

$$\begin{pmatrix} 1 & 0 \\ -18 & 1 \end{pmatrix} \begin{pmatrix} 1 & -18 \\ 18 & 19 \end{pmatrix} \begin{pmatrix} 1 & 18 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 7^3 \end{pmatrix},$$

we have that

$$\begin{aligned} \operatorname{Ker} \Theta &\cong \operatorname{Spec} B[x, y, 1/xy]/(x - y^{-18}, y^{7^3} - 1) \\ &\cong \operatorname{Spec} B[z]/(z^{7^3} - 1) \\ &\cong \mu_{7^3, B} \end{aligned}$$

with the G-action $z^{\sigma_0} = z^{19}$. We can define actions of $\langle 1 \rangle \in \mathbb{Z}/5\mathbb{Z}$ and $[1] \in \mathbb{Z}/4\mathbb{Z}$ on $\mu_{7^3,B}$ by $\langle 1 \rangle z = z^8$ and $[1] z = z^{19}$. The group scheme $\mu_{7^3,B}$ is isomorphic to $\operatorname{Spec} B[y_1, y_2, \ldots, y_{57}]/\mathsf{A}$ with co-multiplication

$$m^*(y_i) = y_i \otimes 1 + 1 \otimes y_i - \frac{1}{6} \sum_{k=1}^{6} \left(\sum_{s=1}^{57} d_{i,s,k} y_s^k \otimes \sum_{t=1}^{57} d_{i,t,7-k} y_t^{7-k} \right).$$

G acts on $\operatorname{Spec} B[y_1, y_2, \ldots, y_{57}]/\mathsf{A}$ by $y_i^{\sigma_0} = \zeta y_i$. Now we assume that there exists $u \in B$ a 6th root of $b \in A^\times$ and $B = A[u]$. We may assume without loss of generality that $u^{\sigma_0} = \zeta u$. Then $u^{-1} y_i$ is G-invariant.

References

[1] N. Bourbaki, *Algèbre Commutative, Éléments de Mathématique*, Springer-Verlag Berlin Heidelberg 2006, Chap. I, II.

[2] A. Grothendieck, M. Artin and J. L. Verdier, *Théorie des topos et cohomologie étale des schémas* (1963–64), Lecture Notes in Math. 269, 270, 305, Springer, Heidelberg, 1972–73.

[3] Y. Koide, *On the Torsors for General Twisted Finite Group Schemes of Prime Order*, Preprint, 2012.

[4] Y. Koide and T. Sekiguchi, *On the Cyclotomic Twisted Torus*, Preprint, 2011.

[5] J. S. Milne, *Étale Cohomology*, Princeton University Press, 1980.

[6] F. Oort and J. Tate, *Group Schemes of Prime Order*, Annales Scientifiques de l'É.N.S., 4^{e} série, tome 3, 1970, p.1–21.

[7] L. G. Roberts, *The Flat Cohomology of Group Schemes of Rank p*, American Journal of Mathematics, The Johns Hopkins University Press, Vol.95, No.3, (Autumn, 1973), p.688–702, DOI: 10.2307/2373735.

[8] T. Sekiguchi and Y. Toda, *On the cyclotomic twisted torus and some torsors*, Preprint, 2013.

[9] J.-P. Serre, *Groupes Algébriques et Corps de Classes*, Hermann, Parris (1959).

[10] L. C. Washington, *Introduction to Cyclotomic Fields*, Graduate Texts in Mathematics 83, Springer-Verlag, New York Heidelberg Berlin, 1982.