ON THE TORSORS 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 $\phi$. Suppose $\mathfrak{p}$ is a prime ideal lying over $p$ (which splits completely in $\mathbb{Z}[\zeta]$), where $\zeta$ is a primitive $(p-1)$-st root of the unity. In case $\mathfrak{p}$ is principal, the sequence

$$0 \to \mu^m_{p,B} \to \mathbb{G}_m^{m,B} \xrightarrow{\mathfrak{p}} \mathbb{G}_m^{m,B} \to 0$$

is exact, and the Galois descent of $\mu^m_{p,B}$ 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 $\mu^m_{p^n,B}$. 

Received: October 10, 2013
1. The Classification Theorem by F. Oort and J. Tate

We denote by \( p \) a prime number, by \( \zeta \) a primitive \((p - 1)\)-st root of the unity, and by \( A \) a \( \Lambda_p \)-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

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

with the group scheme structure

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

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

\[
G_{0,0} = \mathbb{G}_m, \quad G_{1,0} = \mathbb{Z}/p\mathbb{Z}, \quad G_{0,1} = \#_p.
\]

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 \( \phi \), by \( \zeta \) a primitive \( n \)-th root of the unity, by \( G \) a cyclic group of order \( n \) with a generator \( \sigma_0 \), and by \( \text{Spec} \mathcal{B}/\text{Spec} \mathcal{A} \) a \( G \)-torsor. Let

\[
\Phi_n(x) = \prod_{k \in (\mathbb{Z}/n\mathbb{Z})^\times} (x - \zeta^k) = x^m + a_1x^{m-1} + \cdots + a_m
\]

be the cyclotomic polynomial, and \( I \) be the representing matrix of the action of \( \zeta \) 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 \( \mathbf{x} = (x_1, x_2, \ldots, x_m) \) and a matrix \( M = (m_{ij}) \in M_{m \times l}(\mathbb{Z}) \), we define the matrix power \( \mathbf{x}^M \) by

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

\( G \) acts on the algebraic torus

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

by

\[
\mathbf{x}^{\sigma_0} = (x_1^{\sigma_0}, x_2^{\sigma_0}, \ldots, x_n^{\sigma_0}) = \mathbf{x}^I.
\]

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

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

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

\[
\bigcap_{l|n} \text{Ker } (\text{Nm}_l : \text{Res}_{B/A}\mathbb{G}_{m,B} \to \text{Res}_{B_\ell/A}\mathbb{G}_{m,B_\ell}),
\]

where \( \text{Nm}_l \) is the norm map from \( B \) to \( B_\ell = B^{(n/\ell)} \), and \( \text{Res}_{B/A} \) is the Weil restriction from \( B \) to \( A \).

**3. The Torsor for** \( G_{a,b} \) **by T. Sekiguchi and Y. Toda**

Let \( n = p_1^{i_1}p_2^{i_2} \cdots p_r^{i_r} \) be the prime decomposition of a positive integer \( n \). For integers \( 1 \leq i_0 < i_1 < \cdots < i_s \leq r \), we set \( n_{i_0i_1 \cdots i_s} = n/p_{i_0}p_{i_1} \cdots p_{i_s} \) and \( K_{i_0i_1 \cdots i_s} = \mathbb{F}_q^{n_{i_0i_1 \cdots i_s}} \).
Theorem 3.1 (T. Sekiguchi and Y. Toda [8]). There exists a following exact sequence which we call a cyclotomic resolution:

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

where the morphisms $(\partial^i)$'s are defined by

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

and

$$(\partial^s x)_{i_0i_1\ldots i_s} = \prod_{j=0}^s \left( \text{Nm}_{K_{i_0i_1\ldots i_j/K_{i_0i_1\ldots i_s}}} x_{i_0i_1\ldots i_j} \right) (-1)^j.$$

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

$$0 \rightarrow \mathbb{G}(n)_A \xrightarrow{\varepsilon} \text{Res}_{B/A} \mathbb{G}_{m,B} \xrightarrow{\partial^0} \prod_{i=1}^r \left( \text{Res}_{B_i/A} \mathbb{G}_{m,B_i} \right)$$

$$\xrightarrow{\partial^1} \prod_{1 \leq i < j \leq r} \left( \text{Res}_{B_{ij}/A} \mathbb{G}_{m,B_{ij}} \right) \xrightarrow{\partial^2} \cdots \xrightarrow{\partial^{r-1}} \text{Res}_{B_{12\ldots r}/A} \mathbb{G}_{m,B_{12\ldots r}} \rightarrow 0,$$

where $B_{i_0i_1\ldots i_s} = B \langle \sigma_0^{n_{i_0i_1\ldots i_s}} \rangle$.

The next theorem is also essential to compute torsors.

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

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

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

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

where $\det \varphi = \det M$ for the representing matrix $M$, and $\text{Nm} \varphi$ 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

$$0 \rightarrow \mathbb{G}(n)_A \xrightarrow{\varepsilon} \text{Res}_{B/A} \mathbb{G}_{m,B} \xrightarrow{\partial^0} \text{Ker} \partial^1 \rightarrow 0,$$
which is obtained by the cyclotomic resolution in Theorem 3.1, we have a long exact sequence

\[ 0 \to H^0(X, \mathbb{G}(n)_A) \xrightarrow{H^0(X, \varepsilon)} H^0(X, \text{Res}_{B/A} \mathbb{G}_{m,B}) \xrightarrow{H^0(X, \partial^0)} H^0(X, \text{Ker} \partial^1) \]

\[ \partial \to H^1(X, \mathbb{G}(n)_A) \xrightarrow{H^1(X, \varepsilon)} H^1(X, \text{Res}_{B/A} \mathbb{G}_{m,B}) = 0, \]

where \( X = \text{Spec} A \). Hence the correspondence \( f \mapsto \partial f \) gives the isomorphism

\[ \text{Coker} \, H^0(X, \partial^0) \xrightarrow{\sim} H^1(X, \mathbb{G}(n)_A), \]

where \( \partial f \) is given by the diagram

\[
\begin{array}{ccccccc}
\partial f = f^* (\text{Res}_{B/A} \mathbb{G}_{m,B}) & \longrightarrow & X \\
0 & \longrightarrow & \mathbb{G}(n)_A & \xrightarrow{\varepsilon} & \text{Res}_{B/A} \mathbb{G}_{m,B} & \xrightarrow{\partial^0} & \text{Ker} \partial^1 & \longrightarrow & 0.
\end{array}
\]

Let \( p \) 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 \( p \). Then we have an exact sequence

\[ 0 \to \mu_{p,B} \xrightarrow{\epsilon} \mathbb{G}_{m,B} \xrightarrow{\theta} \mathbb{G}_{m,B} \to 0, \]

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

\[ 0 \to (\mu_{p,B})^G \xrightarrow{\epsilon} \mathbb{G}(n)_A \xrightarrow{\theta} \mathbb{G}(n)_A \to 0. \]

By Theorem 1.1, we have that

\[ \mu_{p,B} \cong \text{Spec} B[y]/(y^p - \omega_p y) \]

with the group scheme structure

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

where \( \omega \in A \) with \( \omega_p = p\omega_{p-1} \) and \( \omega_i \equiv i! \pmod{p} \). The Galois group \( G \) acts on \( \text{Spec} B[y]/(y^p - \omega_p y) \) by \( y^g = \zeta^l y \) 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 \( \mu_{p,B} \) is given by \( G_{a,b} \), that is to say, we obtain an exact sequence
\[
0 \rightarrow G_{a,b} \overset{\iota}{\rightarrow} \mathbb{G}(n)_A \overset{\theta}{\rightarrow} \mathbb{G}(n)_A \rightarrow 0.
\]
From this sequence, we obtain a long exact sequence
\[
0 \rightarrow H^0(X, G_{a,b}) \overset{H^0(X, \iota)}{\rightarrow} H^0(X, \mathbb{G}(n)_A) \overset{H^0(X, \theta)}{\rightarrow} H^0(X, \mathbb{G}(n)_A) \\
\overset{\partial}{\rightarrow} H^1(X, G_{a,b}) \overset{H^1(X, \iota)}{\rightarrow} H^1(X, \mathbb{G}(n)_A) \overset{H^1(X, \theta)}{\rightarrow} H^1(X, \mathbb{G}(n)_A) \\
\overset{\partial}{\rightarrow} \ldots,
\]
thus the correspondence
\[
(\mathcal{G}, f^* (\text{Res}_{B/A} \mathbb{G}_{m,B})) \mapsto \partial g + \varphi^{-1} (\{0\} \times X)
\]
gives the non-canonical isomorphism
\[
\text{Coker } H^0(X, \theta) \times \text{Ker } H^1(X, \theta) \cong H^1(X, G_{a,b}),
\]
where \( \varphi^{-1} (\{0\} \times X) \) is given by the diagram
\[
\begin{array}{ccc}
G_{a,b} & \overset{\varphi^{-1}(\{0\} \times X)}{\nearrow} & X \\
\downarrow \iota & & \downarrow \theta \\
\mathbb{G}(n)_A & \overset{f^* (\text{Res}_{B/A} \mathbb{G}_{m,B})}{\nearrow} & X \\
\downarrow \theta & & \downarrow \varphi \\
\mathbb{G}(n)_A & \overset{\theta f^* (\text{Res}_{B/A} \mathbb{G}_{m,B})}{\nearrow} & X.
\end{array}
\]
Note that \( \theta f^* (\text{Res}_{B/A} \mathbb{G}_{m,B}) \cong \mathbb{G}(n)_A \times X. \)
4. The Torsor for the Galois Descent of $\mu_{p^n}, B$

As in the previous section, we denote by $p$ an odd prime number, by $m = \phi(p-1)$ the value of the Euler function $\phi$, by $\zeta$ a primitive $(p-1)$-st root of the unity, by $G$ a cyclic group of order $p-1$ generated by $\sigma_0$, and by $\text{Spec} \ B/\text{Spec} \ A$ a $G$-torsor. We assume that the base scheme lies over $\text{Spec} \Lambda_p$, where

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

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

$$0 \to \mu_{p^n}, B \to \mathbb{G}^m_{m,B} \xrightarrow{p^n} \mathbb{G}^m_{m,B} \to 0,$$

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

$$\mu_{p^n}, B = \text{Spec} \ B[z]/(z^{p^n}-1).$$

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 $\left( \mathbb{Z}/p^n\mathbb{Z} \right)^\times$ is cyclic and

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

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

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

and

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

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

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

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

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

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

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

Since

$$\text{ord}_p\left(\frac{p^l}{k}\right) = \text{ord}_p\left(p^l \cdot \frac{p^l - 1}{1} \cdot \frac{p^l - 2}{2} \cdots \frac{p^l - (k-1)}{k-1} \cdot \frac{1}{k}\right)$$

$$= \text{ord}_p\left(p^l\right) + \text{ord}_p\left(\frac{1}{k}\right)$$

$$= l - \text{ord}_p k,$$

we have that

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

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 $k - \text{ord}_p k \geq 2$ for $k \geq 2$, and

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

Hence

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

and we obtain that

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

\qed
Remark. In case \( p = 2 \), we have the isomorphisms
\[
(Z/4\mathbb{Z})^\times \cong \mathbb{Z}/2\mathbb{Z}, \quad \text{and} \quad (Z/2^n\mathbb{Z})^\times \cong \mathbb{Z}/2\mathbb{Z} \times Z/2^{n-2}\mathbb{Z} \quad \text{for} \ n \geq 3,
\]
thus \((Z/2^n\mathbb{Z})^\times\) is not cyclic for \( n \geq 3 \). In fact, we can define group homomorphism
\[
\varphi : Z/2\mathbb{Z} \times Z/2^{n-2}\mathbb{Z} \to (Z/2^n\mathbb{Z})^\times
\]
by \( \varphi(a, b) = (-1)^a b \). We show that 3 is of order 2 in \((Z/2^n\mathbb{Z})^\times\). It is clear that 3 is of order 2 in \((Z/8\mathbb{Z})^\times\). Suppose \( n \geq 4 \). By the same argument in Lemma 4.2, we have that
\[
\text{ord}_2 \left( \binom{2l}{k} 2^k \right) = l + k - \text{ord}_2(k) \begin{cases} 
= l + 1 & \text{for} \ k = 1, 2, \\
= l + 2 & \text{for} \ k = 4, \\
\geq l + 3 & \text{for} \ k = 3 \text{ or } k \geq 5,
\end{cases}
\]
where \( l \geq 2 \). Hence
\[
(1 + 2)^2^l = 1 + \binom{2^l}{1} 2 + \binom{2^l}{2} 2^2 + \cdots + \binom{2^l}{k} 2^k + \cdots + 2^{2^l}
= 1 + 2^{l+1} \left( 1 + (2^l - 1) + 2s + 2^2t \right)
= 1 + 2^{l+1} \left( 2^l + 2s + 2^2t \right)
= 1 + 2^{l+2} \left( s + 2^{l-1} + 2t \right),
\]
where \( s, t \in \mathbb{Z} \) with \((s, 2) = 1\). Therefore we have that
\[
3^{p^l} \begin{cases} 
\equiv 1 \pmod{2^n} & \text{if} \ l < n - 2, \\
\equiv 1 \pmod{2^n} & \text{if} \ l = n - 2.
\end{cases}
\]
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 \((Z/2^n\mathbb{Z})^\times\). If \( 3^b \equiv -1 \) \pmod{8} for \( l \in \mathbb{Z} \). Hence \( \varphi \) is injective. By comparing the orders of the groups, we see that \( \varphi \) is isomorphism.

We now continue our discussion in case \( p \neq 2 \). We fix elements \( \alpha, \beta \in (Z/p^n\mathbb{Z})^\times \) with \( \beta \equiv \zeta \pmod{p} \), whose orders are \( p^{n-1} \) and \( p - 1 \) respectively. Using \( \alpha \) and \( \beta \), we define the actions of \( \langle 1 \rangle \in Z/p^n\mathbb{Z} \) and \([1] \in Z/(p - 1)\mathbb{Z}\) on \( \mu_{p^n, B} \) 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 \( \{1 - z^k \mid 1 \leq k \leq p^n - 1\} \). For \( j \in \mathbb{Z} \), we set
\[
e_j = \frac{1}{p-1} \sum_{k=1}^{p-1} \zeta^{-(k-1)j} [k-1] \in B[\mathbb{Z}/(p-1)\mathbb{Z}]
\]
and \( J_j = e_j J \). Clearly \( e_j \), hence also \( J_j \), depends only on \( j \) (mod \( p - 1 \)).

**Lemma 4.3.** \( J \) is the direct sum of \( J_j \) for \( 1 \leq j \leq p - 1 \). Furthermore, we have that
\[
J_j = \left\{ f \in B[z]/(z^{p^n} - 1) \mid [k]f = \zeta^{kj} f \right\},
\]
and \( J_i J_j \subset J_{i+j} \) for \( i, j \in \mathbb{Z} \).

**Proof.** The elements \( e_1, e_2, \ldots, e_{p-1} \) are orthogonal idempotents in the group ring \( B[\mathbb{Z}/(p-1)\mathbb{Z}] \), whose sum is 1, since
\[
e_i e_j = \left( \frac{1}{p-1} \right)^2 \sum_{1 \leq s, t \leq p-1} \zeta^{-(s-1)i-(t-1)j} [(s + t - 1) - 1]
\]
\[
= \left( \frac{1}{p-1} \right)^2 \sum_{1 \leq s, k \leq p-1} \zeta^{-(s-1)i-(k-1)j} [k - 1]
\]
\[
= \left( \frac{1}{p-1} \right)^2 \sum_{k=1}^{p-1} \zeta^{-kj+i} \left( \sum_{s=1}^{p-1} \zeta^{-(i-j)s} \right) [k - 1]
\]
\[
= \begin{cases} 
\frac{1}{p-1} \sum_{k=1}^{p-1} \zeta^{-(k-1)j} [k - 1] & \text{if } i = j, \\
0 & \text{if } i \neq j,
\end{cases}
\]
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 $1 \leq j \leq p-1$, and $J_j$ consists of $f \in J$ such that $[k]f = \zeta^{k_j}f$ for $k \in \mathbb{Z}/(p-1)\mathbb{Z}$. Then we see that $J_iJ_j \subset J_{i+j}$ for $f \in J_i$ and $g \in J_j$, since

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

We set

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

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

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

$$y_{i,j} = \sum_{k=1}^{p-1} \zeta^{-(k-1)j} (1 - [k-1] \langle i-1 \rangle z^{p_i})$$

$$= \begin{cases} (p-1) - \sum_{k=1}^{p-1} z^{a_{i,k}} & \text{if } j \equiv 0 \pmod{p-1}, \\ -\sum_{k=1}^{p-1} \zeta^{-(k-1)j} z^{a_{i,k}} & \text{otherwise}, \end{cases}$$

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

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

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

$$m^*(y_{i,j}) - y_{i,j} \otimes 1 - 1 \otimes y_{i,j}$$

$$= -\sum_{k=1}^{p-1} \zeta^{-(k-1)j} ([1 - z^{a_{i,k}}] \otimes (1 - z^{a_{i,k}}))$$
\[- \frac{1}{(p-1)^2} \sum_{k=1}^{p-1} \zeta^{-(k-1)} \sum_{s=1}^{p-1} \sum_{t=1}^{p-1} \zeta^{(k-1)s} \zeta^{(k-1)t} y_{i,s} \otimes y_{i,t} \]
\[- \frac{1}{p-1} \sum_{s+t \equiv j \pmod{p-1}} y_{i,s} \otimes y_{i,t}.\]

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

\[J = \sum_{i=1}^{q} \sum_{j=1}^{p-1} B y_{i,j},\]

hence

\[J_j = \sum_{i=1}^{q} B y_{i,j}\]

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

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

\[
M_{p^n,k} = \begin{pmatrix}
M_{p^n,k,1} & * \\
M_{p^n,k,2} & \ddots \\
O & & \ddots \\
& & & M_{p^n,k,n}
\end{pmatrix},
\]
ON THE TORSOS FOR SOME GROUP SCHEMES...

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

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

**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

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

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

\[
y'^k_{r+i} = \sum_{s=1}^{q} b'_{r+i,s,k} y_{s,k}
\]

\[
= \sum_{s=1}^{p^{n-j}} b'_{r+i,r+s,k} y_{r+s,k} + \left( \text{terms of } z^{p^j}, z^{2p^j}, \ldots \right) \quad (2)
\]

and

\[
(y'^{k}_{r'+i})^k = \sum_{s=1}^{q} b'_{r'+i,s,k} y'^k_{s,k}
\]

\[
= \sum_{s=1}^{p^{s-j}} b'_{r'+i,r'+s,k} y'^{k}_{r'+s,k} + \left( \text{terms of } (z')^{p^{j-1}}, (z')^{2p^{j-1}}, \ldots \right),
\]

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 $1 \leq i, j \leq p^n - j$. Furthermore, by the relation (2), we have that

$$b_{r+i,r+j,k} = - \left(\text{the coefficient of } z^{\alpha r+j-1} \text{ of } y^k_{r+i}\right)$$

$$= - \sum_{0 \leq \epsilon_1, \epsilon_2, \ldots, \epsilon_k \leq p-2, \atop \alpha r+j-1 \equiv \alpha r+i (\beta \epsilon_2 + \ldots + \beta \epsilon_k)} \zeta^{-(\epsilon_1 + \cdots + \epsilon_k)}$$

$$= - \sum_{0 \leq \epsilon_1, \epsilon_2, \ldots, \epsilon_k \leq p-2, \atop \alpha r+j \equiv \alpha r+i (\beta \epsilon_2 + \ldots + \beta \epsilon_k)} \zeta^{-(\epsilon_1 + \cdots + \epsilon_k)}$$

$$= \left(\text{the coefficient of } z^{\alpha r+j} \text{ of } y^k_{r+i+1}\right)$$

$$= b_{r+i+1,r+j+1,k}.$$

\[ \square \]

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

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

is given by

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

**Proof.** Let $\omega$ be a primitive $p^l$-th root of the unity. Setting

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

...
we see that

\[
M \Omega = \Omega \begin{pmatrix}
\sum_{i=1}^{p^l} m_i \\
\sum_{i=1}^{p^l} \omega^{i-1} m_i \\
\vdots \\
\sum_{i=1}^{p^l} \omega^{(p^l-1)(i-1)} m_i
\end{pmatrix}.
\]

Since

\[
\det \Omega = \sum_{1 \leq i < j \leq p^l} (\omega^i - \omega^j) \neq 0,
\]

we obtain

\[
\det M = \sum_{j=1}^{p^l} \sum_{i=1}^{p^l} \omega^{(i-1)(j-1)} m_i \equiv \sum_{i=1}^{p^l} m_i \quad \text{(mod } p\text{)}.
\]

\[\square\]

**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 \(1 \leq k \leq p-1\).

**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,

\[
b_{q,q,k} = - \left(\text{the coefficient of } Z\text{ of } y_q^k\right)
\]

\[
= - \sum_{\substack{0 \leq n_1, n_2, \ldots, n_k \leq p-2 \\
1 \equiv \beta^{n_1} + \beta^{n_2} + \cdots + \beta^{n_k} \pmod{p}}}
\zeta^{-(n_1 + n_2 + \cdots + n_k)}
\]
\[
= - \sum_{j=1}^{p^{n-1}} \sum_{0 \leq n_1, n_2, \ldots, n_k \leq p-2, \alpha^{-1} \equiv \beta n_1 + \beta n_2 + \cdots + \beta n_k \pmod{p^n}} \zeta^{-(n_1 + n_2 + \cdots + n_k)}
\]

\[
= - \sum_{j=1}^{p^{n-1}} \left( \text{the coefficient of } z^{\alpha^{-1}} \text{ of } y_q^k \right)
\]

\[
= \sum_{j=1}^{p^{n-1}} b_{1,j,k}.
\]

Therefore we have that

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

\[\square\]

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

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

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

\[
A = \left( \{ F_{ij} \mid 1 \leq i < j \leq q \}, \{ F_i \mid 1 \leq i \leq q \} \right).
\]

The Galois group \(G\) acts on \(\text{Spec } B[y_1, y_2, \ldots, y_q]/A\) by \(y_i^{p^n} = \zeta y_i\) under the suitable choice of \(\beta\). 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
\[
m^* \left(\left(\frac{y_i}{u}\right)\right) = \left(\frac{y_i}{u}\right) \otimes 1 + 1 \otimes \left(\frac{y_i}{u}\right) - \frac{b}{p-1} \sum_{k=1}^{q} d_{i,s,k} \left(\frac{y_s}{u}\right)^k \otimes \sum_{t=1}^{q} d_{i,t,p-k} \left(\frac{y_t}{u}\right)^{p-k},
\]
we obtain the Galois descent $(\mathbb{F}_{p^n}, B)_G$ and the exact sequence
\[
0 \to (\mathbb{F}_{p^n}, B)_G \to G(p-1)_A \xrightarrow{p^n} G(p-1)_A \to 0,
\]
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 $(\mathbb{F}_{p^n}, B)^G$.

**Example 4.7.** If $p = 5$, then $p = (2 + \zeta) \subset \mathbb{Z}[\zeta]$ is one of the prime ideals lying over 5, where $\zeta$ is a primitive 4th root of the unity. Set $\theta = (2 + \zeta)^2 = 3 + 4\zeta \in \mathbb{Z}[\zeta]$.

The endomorphism corresponding $\theta$ 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
\[
\text{Ker } \Theta \cong \text{Spec } B[x, y, 1/xy]/(x - y^7, y^{5^2} - 1) \cong \text{Spec } B[z]/(z^{5^2} - 1) \cong \mathbb{F}_{5^2, B}
\]
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 $\mathbb{F}_{5^2, B}$ by $\langle 1 \rangle z = z^6$ and $[1] z = z^{18}$. The group scheme $\mathbb{F}_{5^2, B}$ is isomorphic to $\text{Spec } B[y_1, y_2, y_3, y_4, y_5, y_6]/\mathbb{A}$ with co-multiplication
\[
m^*(y_i) = y_i \otimes 1 + 1 \otimes y_i - \frac{1}{4} \sum_{k=1}^{6} \left( \sum_{s=1}^{6} d_{i,s,k} y_s^k \otimes \sum_{t=1}^{6} d_{i,t,5-k} y_t^{5-k} \right).
\]
$G$ acts on $\text{Spec } B[y_1, y_2, y_3, y_4, y_5, y_6]/A$ by
\[
y_i^{\sigma_0} = -\sum_{l=1}^{4} \zeta^{-(l-1)}(z^{\sigma_0})^{a_i,l}
\]
\[
= -\sum_{l=1}^{4} \zeta^{-(l-1)}z^{a_i,l+1}
\]
\[
= -\zeta\sum_{l=1}^{4} \zeta^{-l}z^{a_i,l+1}
\]
\[
= \zeta y_i.
\]

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 $p = (2 + \zeta) \subset \mathbb{Z}[\zeta]$ is one of the prime ideals lying over 7, where $\zeta$ is a primitive 6th root of the unity. Set
\[
\theta = (2 + \zeta)^3 = 1 + 18\zeta \in \mathbb{Z}[\zeta].
\]
The endomorphism corresponding $\theta$ 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
\[
\text{Ker } \Theta \cong \text{Spec } B[x, y, 1/xy]/(x - y^{-18}, y^{7^3} - 1)
\]
\[
\cong \text{Spec } B[z]/(z^{7^3} - 1)
\]
\[
\cong \mathfrak{m}^{7^3, B}
\]
with the $G$-action $z^{\sigma_0} = z^{19}$. We can define actions of $\langle 1 \rangle \subset \mathbb{Z}/5\mathbb{Z}$ and $[1] \subset \mathbb{Z}/4\mathbb{Z}$ on $\mathfrak{m}^{7^3, B}$ by $\langle 1 \rangle z = z^8$ and $[1]z = z^{19}$. The group scheme $\mathfrak{m}^{7^3, B}$ is isomorphic to $\text{Spec } B[y_1, y_2, \ldots, y_{57}]/A$ with co-multiplication
\[
m^*(y_i) = y_i \otimes 1 + 1 \otimes y_i - \frac{1}{6} \sum_{k=1}^{57} \left(\sum_{i=1}^{57} d_{i,s,k}y_s^k \otimes \sum_{t=1}^{57} d_{i,t,7-k}y_t^{7-k}\right).
\]

$G$ acts on $\text{Spec } B[y_1, y_2, \ldots, y_{57}]/A$ 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


