On the Torsors for some Group Schemes

Yohei Toda

Information Security Science Course
Graduate School of Science and Engineering
Chuo University

March 2015

Acknowledgements

I would like to express my sincere gratitude to my advisor Professor Tsutomu Sekiguchi. He has always shown the light in the dark tunnel of mathematics. I would like to express my sincere thanks to Professor Jinhui Chao, Professor Toshiyuki Katsura, Professor Masato Kuwata, and Professor Kanetomo Sato, who helped eradicate misprints and misunderstandings. I would like to express my sincere thanks to Professor Shinji Miura for his warm encouragement.

Contents

Chapter 1

Introduction

Our aim in this thesis is to compute the torsors for some types of finite group schemes. A group scheme is a group object in the category of schemes, which is a generalization of an algebraic group. Computing its torsor can be regarded as solving the inverse Galois problem for group schemes.

Classically, one of the solutions for computing torsors is given by Kummer in the following way:

Let n be an integer greater than one, let k be a field with $\mathrm{ch}\, k \not| n$, and suppose that k contains a primitive n-th root of unity. Under the flat topology, the short exact sequence

$$1 \to \boldsymbol{\mu}_{n,k} \to \mathbb{G}_{m,k} \xrightarrow{\theta_n} \mathbb{G}_{m,k} \to 1,$$

induces the long exact sequence

$$\begin{aligned} 1 &\to H^0\left(X, \boldsymbol{\mu}_{n,k}\right) \to H^0\left(X, \mathbb{G}_{m,k}\right) \xrightarrow{\theta_n} H^0(X, \mathbb{G}_{m,k}) \\ &\xrightarrow{\partial} H^1(X, \boldsymbol{\mu}_{n,k}) \to H^1\left(X, \mathbb{G}_{m,k}\right) \xrightarrow{\theta_n} H^1(X, \mathbb{G}_{m,k}) \\ &\xrightarrow{\partial} \cdots \end{aligned}$$

for a k-scheme X, where θ_n is the n-th power map. Note that $\boldsymbol{\mu}_{n,k} \simeq (\mathbb{Z}/n\mathbb{Z})_k$ by assumption for k, and $H^1(X, \boldsymbol{\mu}_{n,k})$ is the set of isomorphism classes of $(\mathbb{Z}/n\mathbb{Z})$-torsors of X. If B is a local k-algebra and $X = \operatorname{Spec} B$, then we have

$$H^1\left(X, \mathbb{G}_{m,k}\right) = 0.$$

Thus, there exists an isomorphism of groups

$$H^1(X, \boldsymbol{\mu}_{n,k}) \simeq \operatorname{Coker}\left[\,\theta_n : H^0\left(X, \mathbb{G}_{m,k}\right) \to H^0(X, \mathbb{G}_{m,k})\,\right],$$

which determines any cyclic extension of degree n over k under the condition that $\operatorname{ch} k \not| n$ and that k contains a primitive root of unity.

By the classification theorem by Oort and Tate [8], any group scheme of prime order is isomorphic to a group scheme $G_{a,b}$ under a suitable choice of a and b. Roberts [9] gave the torsors for this kind of group scheme $G_{a,b}$ in case where the base ring is a ring of integers of a local number field. Andreatta and Gasbarri [1] gave the torsors in case where the base ring is a complete discrete valuation ring whose residue field has positive characteristic, and that the base ring contains $(p-1)$-st root of b.

We compute torsors for $G_{a,b}$ in a completely different way and under different assumptions, by using the concept of the cyclotomic twisted torus introduced by Koide and Sekiguchi [5]. Mazur, Rubin, and Silverberg [6] treated the cyclotomic twisted torus in a quite general form. Koide and Sekiguchi defined the cyclotomic twisted torus in the following way:

Let n be a positive integer, m the value of the Euler function of n, and ζ a primitive n-th root of unity. Let G be a cyclic group of order n with a generator σ_0, and let $\operatorname{Spec} B/\operatorname{Spec} A$ be a G-torsor. Suppose that B is a free A-module. If I is the representation matrix of the action of ζ on $\mathbb{Z}[\zeta]$ with respect to the $\mathbb{Z}$-basis $\{1, \zeta, \zeta^2, \ldots, \zeta^{m-1}\}$, we define the action of G on $\mathbb{G}_{m,B}^m = \operatorname{Spec} B[x_1, x_2, \ldots, x_m, 1/(x_1 x_2 \cdots x_m)]$ by $(x_1, x_2, \ldots, x_m)^{\sigma_0} = (x_1, x_2, \ldots, x_m)^I$. By this G-action, we obtain a Galois descent of $\mathbb{G}_{m,B}^m$ over A, which we call the cyclotomic twisted torus of degree n, and denote it by $\mathbb{G}(n)_A$.

Koide and Sekiguchi gave an explicit isomorphism from the twisted torus $\mathbb{G}(n)_A$ to the group scheme $\mathcal{T}(n)_A$ given by the intersection of kernels of all norm maps (cf. Thm. 2.6). The isomorphism in a quite general form was given by Mazur, Rubin, and Silverberg in [6].

Here, we extend the isomorphism $\mathbb{G}(n)_A \simeq \mathcal{T}(n)_A$ to a resolution, which we call a cyclotomic resolution, consisting of Weil restrictions of one-dimensional algebraic tori and several norm maps.

Theorem 1 (cf. Thm. 3.4)**.** *Let n be a positive integer and let $n = p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r}$ be its prime decomposition. For integers $1 \le i_0 < i_1 < \cdots < i_s \le r$, we set $n_{i_0 i_1 \cdots i_s} = n / p_{i_0} p_{i_1} \cdots p_{i_s}$, $G_{i_0 i_1 \cdots i_s} = \langle \sigma_0^{n_{i_0 i_1 \cdots i_s}} \rangle$, and $B_{i_0 i_1 \cdots i_s} = B^{G_{i_0 i_1 \cdots i_s}}$. Under this notation, there exists an exact sequence of group schemes over* $\operatorname{Spec} A$*,*

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

where $\operatorname{Res}_{B/A}$ denotes the Weil restriction from B to A.

We have some results on the cyclotomic twisted tori.

Theorem 2 (cf. Thm. 3.5)**.** *There exists a canonical isomorphism of rings*

$$\operatorname{End}\left(\mathbb{G}(n)_A\right) \simeq \mathbb{Z}[\zeta].$$

Theorem 3 (cf. Prop. 3.6)**.** *For a non-zero homomorphism $\varphi \in \operatorname{End}(\mathbb{G}(n)_A)$, we have*

$$\det \varphi = \operatorname{Nm} \varphi = \operatorname{ord}\left(\operatorname{Ker} \varphi\right).$$

By using these results, we compute torsors for $G_{a,b}$ in the following way:

Suppose that A is a local ring. Under the flat topology, the short exact sequence

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

which is obtained by the cyclotomic resolution, induces the long exact sequence

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

Note that $H^1\left(X, \mathrm{Res}_{B/A}\mathbb{G}_{m,B}\right) = 0$ by assumption for A. Therefore, we have the canonical isomorphism of groups

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

Let $\mathfrak{p}$ be the principal prime ideal generated by $\theta \in \mathbb{Z}[\zeta]$, which splits completely over $\mathbb{Q}(\zeta)$ with $\mathfrak{p} \cap \mathbb{Z} = (p)$. We assume that $n = p - 1$. From the exact sequence

$$1 \to \boldsymbol{\mu}_{p,B} \overset{\iota}{\to} \mathbb{G}_{m,B}^m \overset{\theta}{\to} \mathbb{G}_{m,B}^m \to 1,$$

the Galois descent theory gives the exact sequence

$$1 \to (\boldsymbol{\mu}_{p,B})^G \overset{\iota}{\to} \mathbb{G}(n)_A \overset{\theta}{\to} \mathbb{G}(n)_A \to 1.$$

Here, we have $(\boldsymbol{\mu}_{p,B})^G \simeq G_{a,b}$ under some conditions (cf. §4.1). The above short exact sequence induces the long exact sequence

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

Thus, we have the short exact sequence

$$1 \to \mathrm{Coker}\, H^0(X, \theta) \overset{\partial}{\to} H^1(X, G_{a,b}) \xrightarrow{H^1(X,\iota)} \mathrm{Ker}\, H^1(X, \theta) \to 1.$$

Therefore, the elements of $H^1(X, G_{a,b})$ are described by the elements of

$$\mathrm{Coker}\left[\, H^0(X,\theta) : H^0(X, \mathbb{G}(n)_A) \to H^0(X, \mathbb{G}(n)_A)\,\right]$$

and

$$\mathrm{Ker}\left[\, H^1(X,\theta) : H^1(X, \mathbb{G}(n)_A) \to H^1(X, \mathbb{G}(n)_A)\,\right].$$

In Chapter 2, we give a brief survey on the classification theorem by Oort and Tate [8], and the cyclotomic twisted torus introduced by Koide and Sekiguchi [5]. In Chapter 3.1, we give one of our main results, namely, the resolution for cyclotomic twisted tori. In Chapter 3.2, we give results on cyclotomic twisted tori. Combining these results, we give the torsors for $G_{a,b}$ in Chapter 4.1. In Chapter 4.2, we will give some examples. In Chapter 4.3, we generalize the above method.

Chapter 2

Preliminaries

In this chapter, we give a brief survey on the classification theorem by Oort and Tate [8], and the cyclotomic twisted torus introduced by Koide and Sekiguchi [5].

2.1 Classification Theorem of Group Schemes of Prime Order

Let p be a prime number, $\mathbb{Z}_p$ the ring of p-adic integers, and $\chi : \mathbb{F}_p \to \mathbb{Z}_p$ the unique multiplicative section of the natural surjection $\mathbb{Z}_p \to \mathbb{F}_p$. Let A be a Λ_p-algebra, where

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

Example 2.1. *For each prime number $p = 2, 3, 5, 7$, we have*

$$\Lambda_2 = \mathbb{Z}, \quad \Lambda_3 = \mathbb{Z}\left[\frac{1}{2}\right], \quad \Lambda_5 = \mathbb{Z}\left[\zeta_4, \frac{1}{2(2+\zeta_4)}\right], \quad \Lambda_7 = \mathbb{Z}\left[\zeta_6, \frac{1}{6(2+\zeta_6)}\right],$$

where $\zeta_4 = \chi(2)$ is a primitive fourth root of unity with $\zeta_4 \equiv 2 \pmod 5$, and $\zeta_6 = \chi(3)$ is a primitive sixth root of unity with $\zeta_6 \equiv 3 \pmod 7$.

Theorem 2.2 (Oort-Tate [8, Thm. 2]). *An arbitrary finite group A-scheme of order p is isomorphic to a group scheme of the type*

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

with 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 $\omega_i \equiv i! \pmod{p}$.

Example 2.3. *If $p = 5$, then*

$$\omega_1 = 1,\ \ \omega_2 = -\zeta(2+\zeta),\ \ \omega_3 = (2+\zeta)^2,\ \ \omega_4 = -(2+\zeta)^2,\ \ \omega_5 = -5(2+\zeta)^2.$$

These elements are uniquely determined.

If A is a local ring, then $G_{a,b} \simeq G_{a',b'}$ 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 the characteristic of A is p, then

$$G_{0,0} \simeq \boldsymbol{\alpha}_{p,A}, \quad G_{1,0} \simeq (\mathbb{Z}/p\mathbb{Z})_A, \quad \text{and} \quad G_{0,1} \simeq \boldsymbol{\mu}_{p,A}.$$

2.2 Cyclotomic Twisted Torus

Let n be a positive integer greater than one, m the value of the Euler function of n, and ζ a primitive n-th root of unity. Let G be a cyclic group of order n with a generator σ_0, and $\operatorname{Spec} B/\operatorname{Spec} A$ be 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 the representation matrix of the action of ζ on $\mathbb{Z}[\zeta]$ with respect to the $\mathbb{Z}$-basis $\{1, \zeta, \zeta^2, \ldots, \zeta^{m-1}\}$:

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

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

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

Then, we define the action of G 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

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

Example 2.4. *If $n = 6$, then we have $\Phi_6(x) = x^2 - x + 1$ and*

$$I = \begin{pmatrix} 0 & -1 \\ 1 & 1 \end{pmatrix}.$$

Then, the above G-action on $\mathbb{G}_{m,B}^2 = \operatorname{Spec} B[x_1, x_2, 1/x_1x_2]$ is written as

$$(x_1, x_2)^{\sigma_0} = (x_1, x_2)^I = (x_2, x_1^{-1}x_2).$$

By this G-action, we obtain a Galois descent of $\mathbb{G}_{m,B}^m$ over A, which we call *the cyclotomic twisted torus of degree n*, and denote it by $\mathbb{G}(n)_A$. The coordinate ring of the cyclotomic twisted torus is given explicitly as follows.

Theorem 2.5 (Koide-Sekiguchi [5, Thm. 3.2.1])**.** *The cyclotomic twisted torus is written as*

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

where $\xi_1, \xi_2, \ldots, \xi_n$ *are* G*-invariant parameters, and* $\mathfrak{A}$ *is an ideal given explicitly.*

Theorem 2.6 (Koide-Sekiguchi [5, Thm. 3.4.1], Mazur-Rubin-Silverberg [6, Thm. 5.8])**.** *For each positive integer* l *dividing* n*, we set* $G_l = \langle \sigma_0^{n/l} \rangle \subset G$ *and* $B_l = B^{G_l} \subset B$*. Then, the cyclotomic twisted torus is canonically isomorphic to the subgroup scheme of the Weil restriction* $\operatorname{Res}_{B/A}\mathbb{G}_{m,B}$*,*

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

where Nm_l *is the norm map from* B *to* B_l*.*

Example 2.7. *If* $p = 5$ *and* $A = \mathbb{F}_5$*, then computation in MAGMA shows that*

$$\mathbb{G}(4)_{\mathbb{F}_5} = \operatorname{Spec} \mathbb{F}_5[\xi_1, \xi_2, \xi_3, \xi_4]/\mathfrak{A},$$

where the ideal $\mathfrak{A}$ *is generated by*

$$\left\{ \begin{array}{c} 2\xi_1^2 + 3\xi_2\xi_4 + \xi_3^2 + 3, \\ 4\xi_1\xi_3 + 3\xi_2^2 + 4\xi_4^2 \end{array} \right\}.$$

Example 2.8. *If* $p = 7$ *and* $A = \mathbb{F}_7$*, then*

$$\mathbb{G}(6)_{\mathbb{F}_7} = \operatorname{Spec} \mathbb{F}_7[\xi_1, \xi_2, \xi_3, \xi_4, \xi_5, \xi_6]/\mathfrak{A},$$

where the ideal $\mathfrak{A}$ *is generated by*

$$\left\{ \begin{array}{c} 4\xi_1\xi_6 + 6\xi_2\xi_5 + 4\xi_3\xi_4 + 4\xi_6, \\ 6\xi_1\xi_5 + \xi_2\xi_4 + 3\xi_3^2 + 6\xi_6^2, \\ 3\xi_1^2 + 5\xi_2\xi_6 + 2\xi_3\xi_5 + 6\xi_4^2 + 4, \\ 4\xi_1\xi_3 + 3\xi_2^2 + 3\xi_3 + 6\xi_4\xi_6 + \xi_5^2, \\ 6\xi_1\xi_3 + 4\xi_2^2 + 5\xi_4\xi_6 + \xi_5^2, \\ 6\xi_1^2 + 6\xi_1 + 5\xi_2\xi_6 + 5\xi_3\xi_5 + 2\xi_4^2, \\ 2\xi_1\xi_5 + 2\xi_2\xi_4 + 5\xi_3^2 + 5\xi_5 + 4\xi_6^2, \\ 5\xi_1\xi_4 + \xi_2\xi_3 + \xi_4 + 5\xi_5\xi_6, \\ 2\xi_1\xi_2 + 2\xi_2 + \xi_3\xi_6 + 3\xi_4\xi_5 \end{array} \right\}.$$

Chapter 3

Results on Cyclotomic Twisted Torus

3.1 Cyclotomic Resolution

Here, we note the surjectivity of norm maps that will be essential in the following argument.

Lemma 3.1. *Let q be a power of a prime number. The norm map*

$$\mathrm{Nm} : \mathbb{F}_{q^n} \to \mathbb{F}_q$$

is surjective.

Proof. Let α be a primitive element of $\mathbb{F}_{q^n}$. Then, we have

$$\mathrm{Nm}\,\alpha = \alpha^{1+q+q^2+\cdots+q^{l-1}} = \alpha^{(q^n-1)/(q-1)}.$$

This is an element of $\mathbb{F}_q$ of order $q-1$, that is to say, a primitive element of $\mathbb{F}_q$. $\square$

In the rest of this chapter, we denote $k = \mathbb{F}_q$ and $K = \mathbb{F}_{q^n}$. Let n be a positive integer and let $n = p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r}$ be its prime decomposition. For integers $1 \leq i_0 < i_1 < \cdots < i_s \leq r$, we set

$$n_{i_0 i_1 \cdots i_s} = \frac{n}{p_{i_0} p_{i_1} \cdots p_{i_s}} \quad \text{and} \quad M_{i_0 i_1 \cdots i_s} = \mathbb{F}_{q^{n_{i_0 i_1 \cdots i_s}}}.$$

We define the homomorphism

$$\partial^0 : K^\times \to \prod_{i=1}^{r} M_i^\times$$

by

$$\partial^0 x = \left(\mathrm{Nm}_{K^\times / M_1^\times} x, \mathrm{Nm}_{K^\times / M_2^\times} x, \ldots, \mathrm{Nm}_{K^\times / M_r^\times} x \right),$$

and

$$\partial^s : \prod_{1 \leq i_0 < \cdots < i_{s-1} \leq r} M_{i_0 i_1 \cdots i_{s-1}}^\times \to \prod_{1 \leq i_0 < \cdots < i_s \leq r} M_{i_0 i_1 \cdots i_s}^\times$$

by

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

Example 3.2. *If $n = p_1 \cdot p_2 \cdot p_3 = 2 \cdot 3 \cdot 5 = 30$, then we have*

$$\begin{tikzcd}
 & K = \mathbb{F}_{q^{30}} \arrow[dl, dash] \arrow[d, dash] \arrow[dr, dash] & \\
M_1 = \mathbb{F}_{q^{15}} \arrow[d, dash] \arrow[dr, dash] & M_2 = \mathbb{F}_{q^{10}} \arrow[dl, dash] \arrow[dr, dash] & M_3 = \mathbb{F}_{q^6} \arrow[dl, dash] \arrow[d, dash] \\
M_{12} = \mathbb{F}_{q^5} \arrow[dr, dash] & M_{13} = \mathbb{F}_{q^3} \arrow[d, dash] & M_{23} = \mathbb{F}_{q^2} \arrow[dl, dash] \\
 & M_{123} = \mathbb{F}_q &
\end{tikzcd}$$

The homomorphism

$$\partial^0 : K^\times \to M_1^\times \times M_2^\times \times M_3^\times,$$

is defined by

$$\partial^0(x) = \left(\mathrm{Nm}_{K^\times / M_1^\times} x, \mathrm{Nm}_{K^\times / M_2^\times} x, \mathrm{Nm}_{K^\times / M_3^\times} x \right),$$

and the homomorphism

$$\partial^1 : M_1^\times \times M_2^\times \times M_3^\times \to M_{12}^\times \times M_{13}^\times \times M_{23}^\times,$$

is defined by

$$\partial^1(y_1, y_2, y_3) = \left(\frac{\mathrm{Nm}_{M_2^\times/M_{12}^\times} y_2}{\mathrm{Nm}_{M_1^\times/M_{12}^\times} y_1}, \frac{\mathrm{Nm}_{M_3^\times/M_{13}^\times} y_3}{\mathrm{Nm}_{M_1^\times/M_{13}^\times} y_1}, \frac{\mathrm{Nm}_{M_3^\times/M_{23}^\times} y_3}{\mathrm{Nm}_{M_2^\times/M_{23}^\times} y_2} \right).$$

The homomorphism

$$\partial^2 : M_{12}^\times \times M_{13}^\times \times M_{23}^\times \to M_{123}^\times$$

is defined by

$$\partial^2(z_{12}, z_{13}, z_{23}) = \frac{\mathrm{Nm}_{M_{23}^\times/M_{123}^\times} z_{23} \cdot \mathrm{Nm}_{M_{12}^\times/M_{123}^\times} z_{12}}{\mathrm{Nm}_{M_{13}^\times/M_{123}^\times} z_{13}}.$$

In general, we have the following result:

Theorem 3.3. *The following sequence is exact, which we call the cyclotomic resolution:*

$$\begin{aligned} 1 \to \mathbb{G}(n)_k(k) \xrightarrow{\varepsilon} K^\times \xrightarrow{\partial^0} & \prod_{i=1}^{r} M_i^\times \\ \xrightarrow{\partial^1} & \prod_{1 \le i < j \le r} M_{ij}^\times \\ \xrightarrow{\partial^2} & \cdots \\ \xrightarrow{\partial^{r-2}} & \prod_{i=1}^{r} M_{12\cdots\hat{i}\cdots r}^\times \xrightarrow{\partial^{r-1}} M_{12\cdots r}^\times \to 1. \end{aligned}$$

Proof. It is obvious that $\partial^{s+1} \circ \partial^s = 1$. It suffices to show that $\mathrm{Ker}\,\partial^{s+1} \subset \mathrm{Im}\,\partial^s$ since $\mathrm{Ker}\,\partial^0 = \mathrm{Im}\,\varepsilon$ by Theorem 2.6, and ∂^{r-1} is surjective by Lemma 3.1. We use induction on the number r of the prime factors of n.

Firstly, we check the case of $r = 2$, that is to say, $n = p_1^{e_1} p_2^{e_2}$. In this case, the required resolution is as follows:

$$1 \to \mathbb{G}(n)_k(k) \xrightarrow{\varepsilon} K^\times \xrightarrow{\partial^0} M_1^\times \times M_2^\times \xrightarrow{\partial^1} M_{12}^\times \to 1.$$

It suffices to show that $\operatorname{Ker}\partial^1 \subset \operatorname{Im}\partial^0$. Let

$$\boldsymbol{x} = (x_1, x_2) \in \operatorname{Ker}\partial^1 \quad \text{for} \quad \boldsymbol{x} \in M_1^\times \times M_2^\times.$$

By Lemma 3.1, there exists $z_1 \in K^\times$ such that

$$x_1 = \mathrm{Nm}_{K^\times/M_1^\times} z_1.$$

Then, we have

$$\frac{\boldsymbol{x}}{\partial^0 z_1} \in \operatorname{Ker}\partial^1 \quad \text{and} \quad \left(\frac{\boldsymbol{x}}{\partial^0 z_1}\right)_1 = 1.$$

Therefore, we may assume without loss of generality that $\boldsymbol{x} = (1, x_2) \in \operatorname{Ker}\partial^1$, by replacing $\boldsymbol{x}$ with $(\partial^0 z_1)^{-1}\boldsymbol{x}$. Thus, we have

$$\mathrm{Nm}_{M_1^\times/M_{12}^\times} x_2 = 1.$$

Now, we take an element $z_2 \in K^\times$ satisfying

$$x_2 = \mathrm{Nm}_{K^\times/M_2^\times} z_2.$$

Set

$$F(X) = \frac{X^n - 1}{X - 1} \quad \text{and} \quad F_{i_0 i_1 \cdots i_s}(X) = \frac{X^n - 1}{X^{n_{i_0 i_1 \cdots i_s}} - 1}.$$

Then,

$$\mathrm{Nm}_{M^\times_{i_0 i_1 \cdots \hat{i_j} \cdots i_s}/M^\times_{i_0 i_1 \cdots i_s}} z$$

can be written as

$$z^{F_{i_0 i_1 \cdots \hat{i_j} \cdots i_s(\sigma_0)}/F_{i_0 i_1 \cdots i_s(\sigma_0)}}.$$

One can easily see that

$$\left(\frac{F_{12}(X)}{F_1(X)}, \frac{F_{12}(X)}{F_2(X)}\right) = \left(\frac{X^{n_1} - 1}{X^{n_{12}} - 1}, \frac{X^{n_2} - 1}{X^{n_{12}} - 1}\right) = 1.$$

Therefore, there exist polynomials $f_1(X), f_2(X) \in \mathbb{Z}[X]$ such that

$$f_1(X)\frac{F_{12}(X)}{F_1(X)} + f_2(X)\frac{F_{12}(X)}{F_2(X)} = 1$$

(cf. [5, Lem. 10, Prop. 15]). Now we set

$$\gamma = z_2^{f_1(\sigma_0)F_{12}(\sigma_0)/F_1(\sigma_0)}.$$

Then, we have

$$\begin{aligned}
\mathrm{N}_{K^\times/M_1^\times}\gamma &= \mathrm{N}_{K^\times/M_1^\times} z_2^{f_1(\sigma_0)F_{12}(\sigma_0)/F_1(\sigma_0)} \\
&= z_2^{f_1(\sigma_0)F_{12}(\sigma_0)} \\
&= \left(z_2^{F_{12}(\sigma_0)}\right)^{f_1(\sigma_0)} \\
&= 1,
\end{aligned}$$

and

$$\begin{aligned}
\mathrm{N}_{K^\times/M_2^\times}\gamma &= \mathrm{N}_{K^\times/M_2^\times} z_2^{f_1(\sigma_0)F_{12}(\sigma_0)/F_1(\sigma_0)} \\
&= \mathrm{N}_{K^\times/M_2^\times} z_2^{1-f_2(\sigma_0)F_{12}(\sigma_0)/F_2(\sigma_0)} \\
&= x_2 \cdot z_2^{f_2(\sigma_0)F_{12}(\sigma_0)} \\
&= x_2 \left(z_2^{F_{12}(\sigma_0)}\right)^{f_2(\sigma_0)} \\
&= x_2.
\end{aligned}$$

That is to say,

$$\partial^0\gamma = \boldsymbol{x}.$$

Hence, we have $\operatorname{Ker}\partial^1 \subset \operatorname{Im}\partial^0$.

Secondly, we check that $\operatorname{Ker}\partial^1 \subset \operatorname{Im}\partial^0$ in the general number r of the prime factors of n. Take

$$\boldsymbol{x} = (x_1, x_2, \ldots, x_r) \in \operatorname{Ker}\partial^1 \quad \text{for} \quad \boldsymbol{x} \in \prod_{i=1}^{r} M_i^\times,$$

and set

$$n' = p_1^{e_1}p_2^{e_2}\cdots p_{r-1}^{e_{r-1}}, \quad q' = q^{p_r^{e_r}}, \quad \boldsymbol{x}' = (x_1, x_2, \ldots, x_{r-1}),$$

and consider a sequence

$$\begin{aligned} 1 \to \mathbb{G}(n')_k(k) \xrightarrow{\varepsilon} K^\times &\xrightarrow{(\partial')^0} \prod_{i=1}^{r-1} M_i^\times \\ &\xrightarrow{(\partial')^1} \prod_{1\le i<j\le r-1} M_{ij}^\times \\ &\xrightarrow{(\partial')^2} \cdots \\ &\xrightarrow{(\partial')^{r-3}} \prod_{i=1}^{r-1} M^\times_{12\cdots\hat{i}\cdots r-1} \xrightarrow{(\partial')^{r-2}} M^\times_{12\cdots r-1} \to 1, \end{aligned}$$

where the morphisms ∂' are induced naturally by ∂. Then, we have $\boldsymbol{x}' \in \operatorname{Ker}(\partial')^1$. By the induction hypothesis, there exists an element $z' \in K^\times$ such that

$$(\partial')^0 z' = \boldsymbol{x}'.$$

Then, we have

$$\frac{\boldsymbol{x}}{\partial^0 z'} \in \operatorname{Ker}\partial^1, \quad \text{and} \quad \left(\frac{\boldsymbol{x}}{\partial^0 z'}\right)_i = 1 \quad \text{for} \quad 1 \le i \le r-1.$$

Therefore, we may assume without loss of generality that $\boldsymbol{x} = (1, \ldots, 1, x_r) \in \operatorname{Ker}\partial^1$, by replacing $\boldsymbol{x}$ with $(\partial^0 z')^{-1}\boldsymbol{x}$. By the same argument, there exists $z \in K^\times$ such that

$$\left(\frac{\boldsymbol{x}}{\partial^0 z}\right)_i = 1 \quad \text{for} \quad 2 \le i \le r,$$

and polynomials $f_1(X), f_r(X) \in \mathbb{Z}[X]$ such that

$$f_1(X)\frac{F_{1r}(X)}{F_1(X)} + f_r(X)\frac{F_{1r}(X)}{F_r(X)} = 1.$$

By setting

$$\gamma = z^{f_1(\sigma_0)F_{14}(\sigma_0)/F_1(\sigma_0)},$$

we have

$$\partial^0 \gamma = \boldsymbol{x}.$$

Hence, we have $\operatorname{Ker}\partial^1 \subset \operatorname{Im}\partial^0$.

Thirdly, we verify that $\operatorname{Ker}\partial^{s+1} \subset \operatorname{Im}\partial^{s}$, where $s \neq 0$ and $s+1 \neq r-1$. For simplicity, we always assume that $1 \leq i_0 < i_1 < \cdots < i_s$. Take

$$\boldsymbol{x} = (x_{i_0 i_1 \cdots i_s})_{i_s \leq r} \in \operatorname{Ker}\partial^{s+1} \quad \text{for} \quad \boldsymbol{x} \in \prod_{i_s \leq r} M^{\times}_{i_0 i_1 \cdots i_s},$$

and set

$$n' = p_1^{e_1} p_2^{e_2} \cdots p_{r-1}^{e_{r-1}}, \quad q' = q^{p_r^{e_r}}, \quad \boldsymbol{x}' = (x_{i_0 i_1 \cdots i_s})_{i_s \leq r-1}.$$

Consider the sequence

$$\begin{aligned} 1 \to \mathbb{G}(n')_k(k) \xrightarrow{\varepsilon} K^{\times} &\xrightarrow{(\partial')^0} \prod_{i=1}^{r-1} M_i^{\times} \\ &\xrightarrow{(\partial')^1} \prod_{1 \leq i < j \leq r-1} M_{ij}^{\times} \\ &\xrightarrow{(\partial')^2} \cdots \\ &\xrightarrow{(\partial')^{r-3}} \prod_{i=1}^{r-1} M^{\times}_{12\cdots\hat{i}\cdots r-1} \xrightarrow{(\partial')^{r-2}} M^{\times}_{12\cdots r-1} \to 1, \end{aligned}$$

where the morphisms ∂' are induced naturally by ∂. Then, we have $\boldsymbol{x}' \in \operatorname{Ker}(\partial')^{s+1}$. By the induction hypothesis, there exists an element $\boldsymbol{u}' = (u_{i_0 i_1 \cdots i_{s-1}})_{i_{s-1} \leq r-1}$ such that

$$(\partial')^s \boldsymbol{u}' = \boldsymbol{x}'.$$

We set

$$u_{i_0 i_1 \cdots i_{s-2} r} = 1 \quad \text{and} \quad \boldsymbol{u} = \left(u_{i_0 i_1 \cdots i_{s-1}}\right)_{i_{s-1} \leq r}.$$

Then, we have

$$\frac{\boldsymbol{x}}{\partial^s \boldsymbol{u}} \in \operatorname{Ker}\partial^{s+1}, \quad \text{and} \quad \left(\frac{\boldsymbol{x}}{\partial^s \boldsymbol{u}}\right)_{i_0 i_1 \cdots i_s} = 1 \quad \text{for} \quad i_s \leq r-1.$$

Therefore, we may assume without loss of generality that $\boldsymbol{x} = \left(x_{i_0 i_1 \cdots i_s}\right)_{i_s \leq r} \in \operatorname{Ker}\partial^{s+1}$ with $x_{i_0 i_1 \cdots i_s} = 1$ for $i_s \leq r-1$, by replacing $\boldsymbol{x}$ with $(\partial^s \boldsymbol{u})^{-1}\boldsymbol{x}$. Next we set

$$
\begin{aligned}
y_{i_0 i_1 \cdots i_{s-1}} &= x_{i_0 i_1 \cdots i_{s-1} r}, \\
\boldsymbol{y} &= \left(y_{i_0 i_1 \cdots i_{s-1}}\right)_{i_{s-1} \leq r-1}, \\
n' &= p_1^{e_1} p_2^{e_2} \cdots p_{r-1}^{e_{r-1}}, \\
q' &= q^{p_r^{e_r - 1}}, \\
K' &= M_r = \mathbb{F}_{(q')^{n'}}, \\
M'_{i_0 i_1 \cdots i_s} &= M_{i_0 i_1 \cdots i_s r},
\end{aligned}
$$

and consider the sequence

$$
\begin{aligned}
1 \to \mathbb{G}(n')_k(k) \xrightarrow{\varepsilon'} (K')^{\times} &\xrightarrow{(\partial')^0} \prod_{i=1}^{r-1} (M'_i)^{\times} \\
&\xrightarrow{(\partial')^1} \prod_{1 \leq i < j \leq r-1} (M'_{ij})^{\times} \\
&\xrightarrow{(\partial')^2} \cdots \\
&\xrightarrow{(\partial')^{r-3}} \prod_{i=1}^{r-1} (M'_{12 \cdots \hat{i} \cdots r-1})^{\times} \xrightarrow{(\partial')^{r-2}} (M'_{12 \cdots r-1})^{\times} \to 1,
\end{aligned}
$$

where the morphisms ∂' are induced naturally by ∂. Then, we have

$$
((\partial')^s \boldsymbol{y})_{i_0 i_1 \cdots i_s} = \left(\partial^{s+1} \boldsymbol{x}\right)_{i_0 i_1 \cdots i_s r} = 1.
$$

Hence, there exists $\boldsymbol{v}' = (v'_{i_0 i_1 \cdots i_{s-2}})_{i_{s-2} \leq r-1}$ such that

$$
\left((\partial')^{s-1} \boldsymbol{v}'\right)_{i_0 i_1 \cdots i_{s-1}} = y_{i_0 i_1 \cdots i_{s-1}} = x_{i_0 i_1 \cdots i_{s-1} r}.
$$

Set

$$
v_{i_0 i_1 \cdots i_{s-1}} = \begin{cases} 1 & \text{for} \quad i_{s-1} \leq r-1, \\ v'_{i_0 i_1 \cdots i_{s-2}} & \text{for} \quad i_{s-1} = r, \end{cases}
$$

and

$$
\boldsymbol{v} = \left(v_{i_0 i_1 \cdots i_{s-1}}\right)_{i_{s-1} \leq r}.
$$

Then, we have

$$(\partial^s \boldsymbol{v})_{i_0 i_1 \cdots i_s} = \begin{cases} 1 & \text{for} \quad i_s \leq r-1, \\ x_{i_0 i_1 \cdots i_{s-1} r} & \text{for} \quad i_s = r. \end{cases}$$

That is to say,

$$\partial^s \boldsymbol{v} = \boldsymbol{x}.$$

Hence, we see that $\operatorname{Ker} \partial^{s+1} \subset \operatorname{Im} \partial^s$.

Lastly, we check that $\operatorname{Ker} \partial^{r-1} \subset \operatorname{Im} \partial^{r-2}$. We set

$$\hat{i} = (1, \ldots, \hat{i}, \ldots, r) \quad \text{and} \quad \widehat{ij} = (1, \ldots, \hat{i}, \ldots, \hat{j}, \ldots, r).$$

Fix

$$\boldsymbol{x} = (x_{\hat{1}}, x_{\hat{2}}, \ldots, x_{\hat{r}}) \in \operatorname{Ker} \partial^{r-1} \quad \text{for} \quad x_{\hat{i}} \in M_{\hat{i}}^{\times}.$$

We choose elements $z_2, z_3, \ldots, z_r \in K^{\times}$ satisfying

$$x_{\hat{i}} = \operatorname{Nm}_{K^{\times}/M_{\hat{i}}^{\times}} z_i \quad \text{for} \quad i = 2, 3, \ldots, r.$$

Now we set

$$n' = p_1^{e_1} p_2^{e_2}, \quad q' = q^{p_3^{e_3 - 1} \cdots p_r^{e_r - 1}}, \quad K' = M_{\widehat{12}} = \mathbb{F}_{(q')^{n'}},$$

and

$$\boldsymbol{x}' = \left(x_{\hat{1}}, \prod_{j=2}^{r} \left(\operatorname{Nm}_{K^{\times}/M_{\hat{2}}^{\times}} z_j \right)^{(-1)^j} \right) \in (M_2')^{\times} \times (M_1')^{\times} = M_{\hat{1}}^{\times} \times M_{\hat{2}}^{\times},$$

and consider the sequence

$$1 \to \mathbb{G}(n')_k(k) \xrightarrow{\varepsilon'} (K')^{\times} \xrightarrow{(\partial')^0} (M_1')^{\times} \times (M_2')^{\times} \xrightarrow{(\partial')^1} (M_{12}')^{\times} \to 1.$$

Then, we have

$$(\partial')^1 \boldsymbol{x}' = \partial^{r-1} \boldsymbol{x} = 1.$$

By the induction hypothesis, there exists $u_{\widehat{12}} \in (K')^{\times} = M_{\widehat{12}}^{\times}$ such that

$$(\partial')^0 u_{\widehat{12}} = \boldsymbol{x}'.$$

By setting

$$u_{\widehat{ij}} = 1 \quad \text{for} \quad \widehat{ij} \neq \widehat{12}, \quad \text{and} \quad \boldsymbol{u} = (u_{\widehat{ij}})_{1 \leq i < j \leq r},$$

we have

$$\left(\frac{\boldsymbol{x}}{\partial^{r-2}\boldsymbol{u}}\right)_{\hat{1}} = 1 \quad \text{and} \quad \frac{\boldsymbol{x}}{\partial^{r-2}\boldsymbol{u}} \in \operatorname{Ker}\partial^{r-1}.$$

Therefore, we may assume that $\boldsymbol{x} = (1, x_{\hat{2}}, \ldots, x_{\hat{r}}) \in \operatorname{Ker}\partial^{r-1}$. Assume without loss of generality that $\boldsymbol{x} = (x_{\hat{1}}, \ldots, x_{\widehat{r-1}}, 1)$. Next we set

$$\begin{aligned}
n'' &= p_1^{e_1} \cdots p_{r-1}^{e_{r-1}}, \\
q'' &= q^{p_r^{e_r - 1}}, \\
K'' &= M_r = \mathbb{F}_{(q'')^{n''}}, \\
M''_{i_0 \cdots i_s} &= M_{i_0 \cdots i_s r}, \\
\boldsymbol{x}'' &= (x_{\hat{1}}, \ldots, x_{\widehat{r-1}}),
\end{aligned}$$

and consider the sequence

$$\begin{aligned}
1 \to \mathbb{G}(n'')_k(k) \xrightarrow{\varepsilon''} (K'')^\times &\xrightarrow{(\partial'')^0} \prod_{i=1}^{r-1} (M''_i)^\times \\
&\xrightarrow{(\partial'')^1} \cdots \\
&\xrightarrow{(\partial'')^{r-3}} \prod_{i=1}^{r-1} (M''_{\hat{i}})^\times \xrightarrow{(\partial'')^{r-2}} (M''_{12\cdots r-1})^\times \to 1.
\end{aligned}$$

Then, we have

$$(\partial'')^{r-2}\boldsymbol{x}'' = \partial^{r-1}\boldsymbol{x} = 1.$$

Again by the induction hypothesis, there exists $\boldsymbol{v}' = (v_{\widehat{ij}})_{1 \leq i < j \leq r-1}$ such that

$$(\partial'')^{r-3}\boldsymbol{v}'_{\widehat{ij}} = \boldsymbol{x}''.$$

By setting

$$v_{\widehat{ir}} = 1 \quad \text{and} \quad \boldsymbol{v} = (v_{\widehat{ij}})_{1 \leq i < j \leq r},$$

we have

$$(\partial^{r-2}\boldsymbol{v})_{\hat{i}} = \begin{cases} x_{\hat{i}} & \text{for} \quad 1 \leq i \leq r-1, \\ 1 & \text{for} \quad i = r. \end{cases}$$

That is to say,

$$\partial^{r-2}\boldsymbol{v} = \boldsymbol{x}.$$

Hence, we see that $\operatorname{Ker} \partial^{r-1} \subset \operatorname{Im} \partial^{r-2}$. □

The essential point of the proof of Theorem 3.3 is the surjectivity of the norm map

$$\mathrm{Nm} : \mathbb{F}_{q^n} \to \mathbb{F}_q.$$

We easily see the surjectivity of the norm map of sheaves on the flat site $(\operatorname{Spec} A)_{\mathrm{flat}}$;

$$\mathrm{Nm} : \mathrm{Res}_{B/A}\mathbb{G}_{m,B} \to \mathbb{G}_{m,A},$$

where the notation is as in the previous chapter. In fact, for any A-algebra R and any element $a \in \mathbb{G}_{m,A}(R) = R^\times$, set $S = R[T]/(T^n - a)$. Then, the morphism $\operatorname{Spec} S \to \operatorname{Spec} R$ is surjective and flat, and we get the following commutative diagram:

$$\begin{tikzcd}
\left(\mathrm{Res}_{B/A}\mathbb{G}_{m,B}\right)(R) = (R \otimes_A B)^\times \arrow[r, "\mathrm{Nm}(R)"] \arrow[d, "\mathrm{rest}"] & \mathbb{G}_{m,A}(R) = R^\times \arrow[d, "\mathrm{rest}"] \\
\left(\mathrm{Res}_{B/A}\mathbb{G}_{m,B}\right)(S) = (S \otimes_A B)^\times \arrow[r, "\mathrm{Nm}(S)"] & \mathbb{G}_{m,A}(S) = S^\times.
\end{tikzcd}$$

Thus, we see that $\mathrm{Nm}(S)(\overline{T} \otimes 1) = \mathrm{rest}(a)$. Therefore, by the same argument as in the proof of Theorem 3.3, we have the following:

Theorem 3.4. *The following sequence of group schemes over* $\operatorname{Spec} A$ *is exact:*

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

where $B_{i_0 i_1 \cdots i_s} = B^{G_{i_0 i_1 \cdots i_s}}$ *and* $G_{i_0 i_1 \cdots i_s} = \langle \sigma_0^{n_{i_0 i_1 \cdots i_s}} \rangle$.

3.2 Endomorphism Ring of Cyclotomic Twisted Torus

Under the notation in the previous section, we determine the endomorphism ring of group A-scheme $\mathbb{G}(n)_A$ as follows:

Theorem 3.5. *There exists a canonical isomorphism of rings*

$$\mathrm{End}\left(\mathbb{G}(n)_A\right) \simeq \mathbb{Z}[\zeta].$$

Proof. Suppose that φ is a G-equivariant endomorphism of $\mathbb{G}_{m,B}^m$. Then, the morphism φ is represented by some matrix $M = (b_{ij}) \in \mathrm{M}_m(\mathbb{Z})$ satisfying the equality $MI = IM$. By calculating IMI^{-1}, we have the relations

$$
\begin{cases}
b_{ij} = b_{i-1,j-1} - a_{m-i+1} b_{m,j-1} & \text{for} \quad i, j \geq 2,\\
b_{1j} = -b_{m,j-1} & \text{for} \quad j \geq 2.
\end{cases}
$$

Set $c_i = b_{i1}$ for $i = 1, 2, \cdots, m$. Our assertion is that

$$M = \sum_{k=1}^{m} c_k I^{k-1}.$$

In fact, we have

$$b_{1k} = \sum_{l=1}^{k-1} \alpha_l c_{m-k+1+l}$$

by the above relations, where

$$\alpha_1 = -1, \quad \text{and} \quad \alpha_k = -\sum_{i=1}^{k-1} \alpha_i a_{k-i} \quad \text{for} \quad k \geq 2.$$

Then, we have

$$b_{ij} = c_{i-j+1} + \sum_{k=m-j+2}^{m} \left(c_k \sum_{l=1}^{i} a_{m-l+1} \alpha_{k-m+j-i-1+l} \right),$$

where $\alpha_l = c_l = 0$ for $l \leq 0$. On the other hand, since the (i, m)-entry of the matrix I^k is given by

$$\sum_{l=k-i+1}^{k} \alpha_l a_{m-l+k-i+1},$$

and the (i, j)-entry of the matrix

$$\sum_{k=1}^{m} c_k I^{k-1}$$

is given by

$$c_{i-j+1} + \sum_{k=m-j+2}^{m} \left(c_k \sum_{l=1}^{i} \alpha_{k-1+j-m-i+l} a_{m-l+1} \right).$$

This proves the theorem. □

By Theorem 3.5, we have the following proposition.

Proposition 3.6. *For non-zero homomorphism $\varphi \in \operatorname{End}(\mathbb{G}(n)_A)$, we have*

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

where $\det \varphi$ is the determinant of the representing matrix M, and $\operatorname{Nm} \varphi$ means the norm of φ regarded as an element of $\mathbb{Z}[\zeta]$.

Proof. Let

$$M = \sum_{i=1}^{m} c_i I^{i-1}$$

be the representing matrix of non-zero homomorphism $\varphi \in \operatorname{End}(\mathbb{G}(n)_A)$. Set

$$f(x) = \sum_{i=1}^{m} c_i x^{i-1}.$$

Then, the eigenvalues of $M = f(I)$ are given by $\{\, f(\zeta^k) \mid \overline{k} \in (\mathbb{Z}/n\mathbb{Z})^\times \,\}$ by Frobenius' theorem. Therefore, we have

$$\det M = \prod_{\overline{k} \in (\mathbb{Z}/n\mathbb{Z})^\times} f(\zeta^k) = \operatorname{Nm} f(\zeta).$$

Note that $\det M > 0$ since

$$\operatorname{Nm}_{\mathbb{Q}(\zeta)/\mathbb{Q}(\zeta+\zeta^{-1})} \varphi = \varphi\overline{\varphi} = |\varphi|^2 > 0.$$

Hence, there exist $J, J' \in \mathrm{GL}_m(\mathbb{Z})$ such that

$$JMJ' = \begin{pmatrix} d_1 & & & \\ & d_2 & & \\ & & \ddots & \\ & & & d_m \end{pmatrix},$$

where $d_1, d_2, \ldots, d_m$ are positive integers such that $d_1 | d_2 | \cdots | d_m$, and $\det M = d_1 d_2 \cdots d_m$ since $\det M > 0$. Therefore, we see that $\det M = \operatorname{ord}(\operatorname{Ker} \varphi)$ since

$$\begin{aligned} \operatorname{Ker} \varphi &\simeq \operatorname{Ker} \varphi_{JMJ'} \\ &= \operatorname{Spec} B[x_1, x_2, \ldots, x_m]/\bigl(x_1^{d_1} - 1, x_2^{d_2} - 1, \ldots, x_m^{d_m} - 1\bigr) \\ &= \boldsymbol{\mu}_{d_1} \times_{\operatorname{Spec} B} \boldsymbol{\mu}_{d_2} \times_{\operatorname{Spec} B} \cdots \times_{\operatorname{Spec} B} \boldsymbol{\mu}_{d_m}. \end{aligned}$$

□

Chapter 4

Computations on Torsors

4.1 Torsors for $G_{a,b}$

As in previous chapter, let G be a cyclic group of order n and B/A be a G-torsor. We denote $X = \operatorname{Spec} A$ and $Y = \operatorname{Spec} B$. We assume that the base scheme lies over $\operatorname{Spec} \Lambda_p$, where

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

where ζ is a primitive $(p-1)$-st root of unity in the ring of p-adic integers $\mathbb{Z}_p$. Since the morphism $Y \to X$ is étale, and $\operatorname{Res}_{B/A}\mathbb{G}_{m,B}$ is a smooth X-group scheme, we have

$$H^q\left(X_{\text{ét}}, \operatorname{Res}_{B/A}\mathbb{G}_{m,B}\right) = H^q\left(X_{\text{fl}}, \operatorname{Res}_{B/A}\mathbb{G}_{m,B}\right)$$

for $q \geq 0$. In general, we have

$$H^q\left(X_{\text{ét}}, \operatorname{Res}_{B/A}\mathbb{G}_{m,B}\right) = \check{H}^q\left(X_{\text{ét}}, \operatorname{Res}_{B/A}\mathbb{G}_{m,B}\right).$$

For any étale open covering $\{U_\lambda \to X\}_{\lambda\in\Lambda}$, we have an étale open covering $\{U_\lambda \cap Y \to X\}_{\lambda\in\Lambda}$. Then, we have

$$\begin{aligned} C^q\left(\{U_\lambda\}_{\lambda\in\Lambda}, \mathrm{Res}_{B/A}\mathbb{G}_{m,B}\right) &= \prod_{\lambda_0,\lambda_1,\ldots,\lambda_q\in\Lambda} \Gamma\left(U_{\lambda_0\lambda_1\cdots\lambda_q}, \mathrm{Res}_{B/A}\mathbb{G}_{m,B}\right) \\ &= \prod_{\lambda_0,\lambda_1,\ldots,\lambda_q\in\Lambda} \Gamma\left(U_{\lambda_0\lambda_1\cdots\lambda_q}\cap Y, \mathbb{G}_{m,B}\right) \\ &= C^q\left(\{U_\lambda\cap Y\}_{\lambda\in\Lambda}, \mathbb{G}_{m,B}\right). \end{aligned}$$

We obtain

$$\check{H}^q\left(\{U_\lambda\}_{\lambda\in\Lambda}, \mathrm{Res}_{B/A}\mathbb{G}_{m,B}\right) = \check{H}^q\left(\{U_\lambda\cap Y\}_{\lambda\in\Lambda}, \mathbb{G}_{m,B}\right).$$

Therefore, we have the following equalities:

$$\begin{aligned} H^1\left(X_{\mathrm{fl}}, \mathrm{Res}_{B/A}\mathbb{G}_{m,B}\right) &= H^1\left(X_{\text{ét}}, \mathrm{Res}_{B/A}\mathbb{G}_{m,B}\right) \\ &= H^1\left(Y_{\text{ét}}, \mathbb{G}_{m,B}\right) \\ &= H^1\left(Y_{\mathrm{Zar}}, \mathbb{G}_{m,B}\right) \\ &= H^1\left(Y_{\mathrm{fl}}, \mathbb{G}_{m,B}\right), \end{aligned}$$

since

$$\check{H}^q\left(X_{\text{ét}}, \mathrm{Res}_{B/A}\mathbb{G}_{m,B}\right) = \check{H}^q\left(Y_{\text{ét}}, \mathbb{G}_{m,B}\right) = H^q\left(Y_{\text{ét}}, \mathbb{G}_{m,B}\right).$$

In particular if A is local, then B is semi-local and

$$H^1\left(Y_{\mathrm{Zar}}, \mathbb{G}_{m,B}\right) = \mathrm{Pic}\, Y = 0.$$

Consider the exact sequence

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

which is obtained by the cyclotomic resolution

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

Under the flat topology, we have an exact sequence

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

Here, we have $H^1(X, \mathrm{Res}_{B/A}\mathbb{G}_{m,B}) = 0$ by assumption for A and B. Thus, we have the canonical isomorphism of groups

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

and the explicit correspondence is given as follows:

For $\overline{f} \in \mathrm{Coker}\, H^0(X, \partial^0)$ that is represented by $f \in H^0(X, \mathrm{Ker}\,\partial^1)$, we have the diagram

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

by taking pull-back, i.e., fiber product (cf. Appendix).

Let $\mathfrak{p}$ be a principal prime ideal with a generator $\theta \in \mathbb{Z}[\zeta]$, which splits completely over $\mathbb{Q}(\zeta)$ with $\mathfrak{p} \cap \mathbb{Z} = (p)$. In fact, $\mathfrak{p}$ splits completely if and only if $p \equiv 1 \pmod{n}$ (cf. [15, Prop. 2.14]). We assume that $n = p-1$. Then, we have an exact sequence

$$1 \to \boldsymbol{\mu}_{p,B} \xrightarrow{\iota} \mathbb{G}_{m,B}^m \xrightarrow{\theta} \mathbb{G}_{m,B}^m \to 1,$$

where we regard θ as an element of $\mathrm{End}(\mathbb{G}(n)_A)$. Then, the Galois descent theory gives an exact sequence

$$1 \to (\boldsymbol{\mu}_{p,B})^G \xrightarrow{\iota} \mathbb{G}(n)_A \xrightarrow{\theta} \mathbb{G}(n)_A \to 1.$$

We describe the torsors for $(\boldsymbol{\mu}_{p,B})^G$ in the following way:

By Oort-Tate's classification theorem, we have

$$\boldsymbol{\mu}_{p,B} \simeq \operatorname{Spec} B[z]/(z^p - \omega_p z)$$

with group scheme structure

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

where ω_p is the product of p and of an invertible element of Λ_p, and ω_k for $1 \leq k \leq p-1$ is an invertible element of A satisfying $\omega_k \equiv k! \pmod{p}$ (cf. [8, §2, Prop.]). The Galois group $G = \langle \sigma_0 \rangle$ acts on $\boldsymbol{\mu}_{p,B} = \operatorname{Spec} B[x]/(x^p - 1)$ by $x^{\sigma_0} = x^l$ with some integer l, and on $\operatorname{Spec} B[z]/(z^p - \omega_p z)$ by $z^{\sigma_0} = \zeta^l z$, where ζ is a primitive n-th root of unity (cf. [8, §2, Prop.]). Now we assume that $x^n - b$ is irreducible in $A[x]$, $ab = \omega_p \in A$, and $B = A[u]$, where u is an n-th root of b. Then, $G_{a,b}$ is isomorphic to the Galois descent of $\boldsymbol{\mu}_{p,B}$. In fact, we may assume without loss of generality that $u^{\sigma_0} = \zeta^l u$ since

$$F_{u/A}(X) = X^n - b = (X-u)(X-\zeta u)\cdots(X-\zeta^{l-1}u).$$

Hence, $u^{-1}z$ is G-invariant, and we have

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

and

$$m^*\left(\frac{z}{u}\right) = \left(\frac{z}{u}\right) \otimes 1 + 1 \otimes \left(\frac{z}{u}\right) - \frac{b}{p-1} \sum_{i=1}^{p-1} \frac{(z/u)^i}{\omega_i} \otimes \frac{(z/u)^{p-i}}{\omega_{p-i}}.$$

Thus, the Galois descent of $\boldsymbol{\mu}_{p,B}$ is isomorphic to $G_{a,b}$, i.e., we obtain the exact sequence

$$1 \to G_{a,b} \xrightarrow{\iota} \mathbb{G}(n)_A \xrightarrow{\theta} \mathbb{G}(n)_A \to 1.$$

From this sequence, we obtain a long exact sequence

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

then, we have the exact sequence

$$1 \to \operatorname{Coker} H^0(X,\theta) \overset{\partial}{\to} H^1(X, G_{a,b}) \xrightarrow{H^1(X,\iota)} \operatorname{Ker} H^1(X,\theta) \to 1.$$

Therefore, the elements of $H^1(X, G_{a,b})$ are described by the elements of

$$\operatorname{Coker} \left[H^0(X, \mathbb{G}(n)_A) \xrightarrow{H^0(X,\theta)} H^0(X, \mathbb{G}(n)_A) \right]$$

and

$$\operatorname{Ker} \left[H^1(X, \mathbb{G}(n)_A) \xrightarrow{H^1(X,\theta)} H^1(X, \mathbb{G}(n)_A) \right].$$

In fact, for $\overline{g} \in \operatorname{Coker} H^0(X,\theta)$ and $f^*(\mathrm{Res}_{B/A}\mathbb{G}_{m,B}) \in \operatorname{Ker} H^1(X,\theta)$, we obtain an element of $H^1(X, G_{a,b})$ as follows:

We have the diagram

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

where the morphism $\tilde{\theta}$ is defined by θ, and we have

$$\iota_*(\tilde{\theta}^{-1}(\{1\} \times X)) \simeq f^*(\mathrm{Res}_{B/A}\mathbb{G}_{m,B})$$

(cf. Appendix). Therefore, we have

$$\partial\, g + \tilde{\theta}^{-1}(\{1\} \times X) \in H^1(X, G_{a,b}),$$

where the operation "+" is the group law of $H^1(X, G_{a,b})$.

Note that we only considered the case where prime ideals lying over p are principal. The non-principal case is treated by Koide [4].

4.2 Examples

Let A be a local $\mathbb{F}_p$-algebra, and $\bar{b} \in \mathbb{F}_p$ be a primitive element of $\mathbb{F}_p$. Set $B = A[u]$, where u is an n-th root of b, and $n = p - 1$. Then, the ideal $(p, b - \zeta)$ of $\mathbb{Z}[\zeta]$ is one of the prime ideals lying over p (cf. [15, Prop. 2.14]). We consider the case where $(p, b - \zeta)$ is principal. Computation in MAGMA for $p < 100$ shows that $(p, b - \zeta)$ is principal if p is one of the numbers

$$5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 61, 67, 71.$$

In fact, we have the equalities

$$\begin{aligned}
5 &= \mathrm{Nm}(2 + \zeta_4), & 31 &= \mathrm{Nm}(1 + \zeta_{30} - \zeta_{30}^2), \\
7 &= \mathrm{Nm}(2 + \zeta_6), & 37 &= \mathrm{Nm}(1 + \zeta_{36} - \zeta_{36}^3), \\
11 &= \mathrm{Nm}(2 - \zeta_{10}), & 41 &= \mathrm{Nm}(1 + \zeta_{40} - \zeta_{40}^4), \\
13 &= \mathrm{Nm}(2 + \zeta_{12}), & 43 &= \mathrm{Nm}(1 - \zeta_{42} + \zeta_{42}^3), \\
17 &= \mathrm{Nm}(1 + \zeta_{16} + \zeta_{16}^3), & 61 &= \mathrm{Nm}(1 + \zeta_{60}^2 + \zeta_{60}^5), \\
19 &= \mathrm{Nm}(1 + \zeta_{18} - \zeta_{18}^2), & 67 &= \mathrm{Nm}(1 + \zeta_{66} - \zeta_{66}^3), \\
23 &= \mathrm{Nm}(1 - \zeta_{22} + \zeta_{22}^3), & 71 &= \mathrm{Nm}(1 - \zeta_{70}^2 - \zeta_{70}^5), \\
29 &= \mathrm{Nm}(1 + \zeta_{28} + \zeta_{28}^4), & &
\end{aligned}$$

where ζ_n is a primitive n-th root of unity. Let $\theta \in \mathbb{Z}[\zeta]$ denote a generator of the ideal $(p, b - \zeta)$. Then, we have an exact sequence

$$1 \to \boldsymbol{\mu}_{p,B} \xrightarrow{\iota} \mathbb{G}_{m,B}^m \xrightarrow{\theta} \mathbb{G}_{m,B}^m \to 1.$$

By the same argument as in the previous section, the Galois descent theory gives an exact sequence

$$1 \to G_{0,b} \xrightarrow{\iota} \mathbb{G}(n)_A \xrightarrow{\theta} \mathbb{G}(n)_A \to 1,$$

and one can compute the torsors for $G_{0,b}$. In particular, if $A = \mathbb{F}_p$, then $H^0(X, G_{0,b}) = 0$. Hence, we have $H^1(X, G_{0,b}) = 0$ since

$$H^0(X,\theta) : H^0(X, \mathbb{G}(n)_A) \to H^0(X, \mathbb{G}(n)_A)$$

is an isomorphism of groups.

4.3 Torsors for Galois Descent of $\boldsymbol{\mu}_{p^l,B}$

In this section, let p be an odd prime number. Let n be a positive integer greater than one, m the value of the Euler function of n, and ζ a primitive n-th root of unity. Let G be the multiplicative group $(\mathbb{Z}/p^l\mathbb{Z})^\times$, and $\operatorname{Spec} B/\operatorname{Spec} A$ 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 $\mathbb{Z}_p$ is the ring of p-adic integers. Here we obtain an exact sequence

$$1 \to \boldsymbol{\mu}_{p^l,B} \to \mathbb{G}_{m,B}^m \xrightarrow{\mathfrak{p}^l} \mathbb{G}_{m,B}^m \to 1,$$

where $\mathfrak{p}$ is a prime ideal lying over p with $\mathfrak{p} \cap \mathbb{Z} = (p)$. We now study the group scheme

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

by extending the method of Oort-Tate. For simplicity, we assume that the ideal $\mathfrak{p}$ is principal. However, this argument can be generalized to non-principal case by using the concept of the homomorphisms defined by ideals, which is introduced by Koide [4].

We fix elements $\alpha, \beta \in (\mathbb{Z}/p^l\mathbb{Z})^\times$, whose orders are p^{l-1} and $p-1$ respectively. Indeed, we have the isomorphism

$$\left(\mathbb{Z}/p^l\mathbb{Z}\right)^\times \simeq \mathbb{Z}/p^{l-1}\mathbb{Z} \times \mathbb{Z}/(p-1)\mathbb{Z}$$

since we assume p is an odd prime number. Using α and β, we define the actions of $\langle 1\rangle \in \mathbb{Z}/p^{l-1}\mathbb{Z}$ and $[1] \in \mathbb{Z}/(p-1)\mathbb{Z}$ on $\boldsymbol{\mu}_{p^l,B}$ by

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

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

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

and has a B-basis $\{\, 1 - z^k \mid 1 \le k \le p^l - 1 \,\}$. 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 $J_j = e_j J$. Clealy e_j and J_j depend only on $j \pmod{p-1}$.

Lemma 4.1. *We have*

$$J = \sum_{j=1}^{p-1} J_j \quad \textit{and} \quad J_j = \left\{\, f \in B[z]/(z^{p^l}-1) \mid [k]f = \zeta^{kj} f \,\right\},$$

thus $J_i J_j \subset J_{i+j}$.

Proof. In fact, we have the equalities

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

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

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

□

Set

$$q = \frac{p^l-1}{p-1} = \sum_{k=1}^{l}p^{l-k},$$

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

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

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

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

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

for $k \in \mathbb{Z}$, therefore we have

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

for $j \in \mathbb{Z}$. Note that $\langle 1 \rangle \in \mathbb{Z}/p^{l-1}\mathbb{Z}$ acts on $y_{i,j}$'s by

$$y_{1,j}^{\langle 1 \rangle} = y_{2,j}, \quad y_{2,j}^{\langle 1 \rangle} = y_{3,j}, \quad \ldots, \quad y_{p^{l-1},j}^{\langle 1 \rangle} = y_{1,j},$$

$$y_{p^{l-1}+1,j}^{\langle 1 \rangle} = y_{p^{l-1}+2,j}, \ y_{p^{l-1}+2,j}^{\langle 1 \rangle} = y_{p^{l-1}+3,j}, \ \ldots, \ y_{p^{l-1}+p^{l-2},j}^{\langle 1 \rangle} = y_{p^{l-1}+1,j},$$

and so on. Thus, $y_{q,j}$ is invariant for the action of $\mathbb{Z}/p^{l-1}\mathbb{Z}$ for $j \in \mathbb{Z}$. Furthermore, we have

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

thus

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

By setting $y_i = y_{i,1}$, we have especially that

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

We define elements $\omega_{i,j,k} \in B$ by

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

that is to say, we have the equality

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

Setting $M_{p^l,k} = (\omega_{i,j,k})_{1 \leq i,j \leq q}$, we have the following:

Lemma 4.2. *The matrix $M_{p^l,k}$ is formed of*

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

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

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

Proof. Set

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

where

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

Let z', e'_j and y'_i be the z, e_j and y_i in the case of replacing l by $l-1$, respectively. For $1 \leq i \leq p^{l-j}$, we have the equalities

$$\begin{aligned} y^k_{r+i} &= \sum_{s=1}^{q} \omega_{r+i,s,k} y_{s,k} \\ &= \sum_{s=1}^{p^{l-j}} \omega_{r+i,r+s,k} y_{r+s,k} + \left(\text{terms of } z^{p^j}, z^{2p^j}, \ldots\right), \end{aligned} \tag{4.1}$$

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

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

and

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

where $z^{p^l} = 1$, $(z')^{p^{l-1}} = 1$. Setting $Z = z^p$, we have $Z^{p^{l-1}} = 1$. Therefore, we 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

$$\omega_{r+i,r+j,k} = \omega'_{r'+i,r'+j,k} \quad \text{for} \quad 1 \le i,j \le p^{l-j}.$$

Furthermore, by the relation (4.1), we have

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

□

Lemma 4.3. *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 unity. Setting $\Omega = \left(\omega^{(i-1)(j-1)}\right)_{1 \leq i,j \leq p^l}$, we see that

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

Since

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

we obtain

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

□

Proposition 4.4. *We have* $\det M_{p^l,k,j} \equiv k! \pmod{p}$*, thus* $\det M_{p^l,k} \equiv (k!)^l \pmod{p}$*, and* $M_{p^l,k}$ *is invertible for* $1 \leq k \leq p-1$*.*

Proof. By Lemma 4.2, it suffices to show that $M_{p^l,k,1} \equiv k! \pmod{p}$. By setting $Z = z^{p^{l-1}}$, we have

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

with $Z^p = 1$. Hence, it can be reduced to the Oort-Tate case, thus $\omega_{q,q,k} \equiv k!$

(mod p). On the other hand,

$$\begin{aligned}
\omega_{q,q,k} &= -\bigl(\text{the coefficient of } Z \text{ of } y_q^k\bigr) \\
&= - \sum_{\substack{0 \le n_1, n_2, \dots, n_k \le p-2 \\ 1 \equiv \beta^{n_1} + \beta^{n_2} + \cdots + \beta^{n_k} \pmod{p}}} \zeta^{-(n_1+n_2+\cdots+n_k)} \\
&= - \sum_{j=1}^{p^{l-1}} \sum_{\substack{0 \le n_1, n_2, \dots, n_k \le p-2 \\ \alpha^{j-1} \equiv \beta^{n_1} + \beta^{n_2} + \cdots + \beta^{n_k} \pmod{p^l}}} \zeta^{-(n_1+n_2+\cdots+n_k)} \\
&= - \sum_{j=1}^{p^{l-1}} \Bigl(\text{the coefficient of } z^{\alpha^{j-1}} \text{ of } y_q^k\Bigr) \\
&= \sum_{j=1}^{p^{l-1}} \omega_{1,j,k}.
\end{aligned}$$

Therefore, we have

$$\det M_{p^l,k,j} \equiv \sum_{j=1}^{p^{l-1}} \omega_{1,j,k} = \omega_{q,q,k} \equiv k! \pmod{p}.$$

□

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

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

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

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

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 $\mathfrak{A}$ is given by

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

The group $\mathbb{Z}/(p-1)\mathbb{Z}$ acts on $\operatorname{Spec} B[y_1, y_2, \ldots, y_q]/\mathfrak{A}$ by $y_i^{\sigma_0} = \zeta y_i$ under the suitable choice of β. Now we assume that $x^l - b$ is irreducible in $A[x]$, and $ab = \omega_p \in A$. Set $B_1 = A[u]$, where u is n-th root of b. We may assume without loss of generality that $u^{\sigma_0} = \zeta u$. Hence, $u^{-1}y_i$ is G-invariant. By the equalities

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

and

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

we obtain the Galois descent of $\boldsymbol{\mu}_{p^l,B_1}$ by the action of $\mathbb{Z}/(p-1)\mathbb{Z}$.

In the rest of this section, we assume that $l = 2$ for simplicity, i.e., consider the group scheme $\boldsymbol{\mu}_{p^2,B}$. In this case, we have $q = p+1$. Let ζ_p be a primitive p-th root of unity. Set $\lambda = \zeta_p - 1$ and $A = \mathbb{Z}_{(p)}[\lambda]$. Now we consider the group scheme

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

with group scheme structure

$$m^*(X) = X \otimes 1 + 1 \otimes X + \lambda X \otimes X.$$

The group scheme $\mathcal{G}^{(\lambda)}$ gives the deformation of the additive group $\mathbb{G}_a$ to the multiplicative group $\mathbb{G}_m$, and it is introduced by Sekiguchi, Oort and Suwa [10], and also by Waterhouse [16] independently.

Define a group scheme homomorphism

$$\alpha^{(\lambda)} : \mathcal{G}^{(\lambda)} \to \mathbb{G}_{m,A} \quad \text{by} \quad \alpha^{(\lambda)}(x) = \lambda x + 1.$$

Consider the diagram

$$\begin{tikzcd}
\mathcal{G}^{(\lambda)} \arrow[r, "\alpha^{(\lambda)}"] \arrow[d, "\psi"] & \mathbb{G}_{m,A} \arrow[d, "p"] . \\
\mathcal{G}^{(\lambda^p)} \arrow[r, "\alpha^{(\lambda^p)}"] & \mathbb{G}_{m,A}
\end{tikzcd}$$

We define the group scheme homomorphism ψ which makes the above diagram commutative, that is to say,

$$\psi(x) = \frac{1}{\lambda^p}\left\{(\lambda x + 1)^p - 1\right\}.$$

Then, we have

$$\begin{aligned}
\psi(x) &= \frac{1}{\lambda^p}\left\{(\lambda x)^p + p(\lambda x)^{p-1} + \binom{p}{2}(\lambda x)^{p-2} + \cdots + \binom{p}{p-2}(\lambda x)^2 + p\lambda x\right\} \\
&= x^p + c_1 x^{p-1} + c_2 x^{p-2} + \cdots + c_{p-2}x^2 + \frac{p}{\lambda^{p-1}}x \qquad (\mathrm{ord}_\lambda(c_i) \geq 1) \\
&\equiv x^p - x \pmod{\lambda}.
\end{aligned}$$

Thus, we obtain an exact sequence

$$1 \to \mathbb{Z}/p\mathbb{Z} \to \mathcal{G}^{(\lambda)} \xrightarrow{\psi} \mathcal{G}^{(\lambda^p)} \to 1.$$

For an A-scheme X, under the flat topology, we have a long exact sequence

$$\begin{aligned}
1 &\to H^0\left(X, (\mathbb{Z}/p\mathbb{Z})_X\right) \to H^0\left(X, \mathcal{G}^{(\lambda)}\right) \xrightarrow{H^0(X,\psi)} H^0\left(X, \mathcal{G}^{(\lambda^p)}\right) \\
&\xrightarrow{\partial} H^1\left(X, (\mathbb{Z}/p\mathbb{Z})_X\right) \to H^1\left(X, \mathcal{G}^{(\lambda)}\right) \xrightarrow{H^1(X,\psi)} H^1\left(X, \mathcal{G}^{(\lambda^p)}\right) \\
&\xrightarrow{\partial} \cdots,
\end{aligned}$$

where

$$\begin{aligned}
H^0\left(X, \mathcal{G}^{(\lambda)}\right) &= \left\{f \in \mathcal{O}_X(X) \mid \lambda f + 1 \in \mathcal{O}_X(X)^\times\right\}, \\
H^0\left(X, \mathcal{G}^{(\lambda^p)}\right) &= \left\{g \in \mathcal{O}_X(X) \mid \lambda^p g + 1 \in \mathcal{O}_X(X)^\times\right\}, \\
H^1\left(X, (\mathbb{Z}/p\mathbb{Z})_X\right) &= \left\{\text{the isomorphism class of } (\mathbb{Z}/p\mathbb{Z})\text{-torsors over } X\right\}.
\end{aligned}$$

If $X = \operatorname{Spec} A$ with a local ring A, then we have $H^1(X, \mathcal{G}^{(\lambda)}) = 0$, and the isomorphism of groups

$$\partial : \operatorname{Coker} H^0\left(X, \psi\right) \xrightarrow{\sim} H^1\left(X, (\mathbb{Z}/p\mathbb{Z})_X\right),$$

where the explicit correspondence is given as follows:

For $\overline{g} \in \operatorname{Coker} H^0\left(X, \psi\right)$, which is represented by $g \in H^0(X, \mathcal{G}^{(\lambda^p)})$, we have the diagram

$$\begin{tikzcd}
 & & \partial g = g^*\left(\mathcal{G}^{(\lambda)}\right) \arrow[r] \arrow[d] \arrow[dr, phantom, "\square"] & X \arrow[d, "g"] & \\
0 \arrow[r] & \mathbb{Z}/p\mathbb{Z} \arrow[r] & \mathcal{G}^{(\lambda)} \arrow[r, "\psi"] & \mathcal{G}^{(\lambda^p)} \arrow[r] & 0
\end{tikzcd}$$

by taking fiber product. Thus, we have

$$\begin{aligned}
\partial g &= \operatorname{Spec} A \otimes_{A\left[X, \frac{1}{\lambda X+1}\right]} A\left[X, \frac{1}{\lambda X + 1}\right] \\
&= \operatorname{Spec} A[X] / \left(\frac{1}{\lambda^p}\left\{(\lambda x + 1)^p - 1\right\} - g \right).
\end{aligned}$$

Let ω denote the solution for

$$\frac{1}{\lambda^p}\left\{(\lambda x + 1)^p - 1\right\} = g.$$

Set $B_2 = A[\omega]$. The group $\mathbb{Z}/p\mathbb{Z}$ acts on B_1 by $\langle 1 \rangle \omega = \zeta_p \omega + 1$. We define $\tilde{y_1}, \tilde{y}_2, \ldots, \tilde{y}_p$ by

$$\begin{pmatrix} \tilde{y_1} \\ \tilde{y}_2 \\ \tilde{y}_3 \\ \vdots \\ \tilde{y}_p \end{pmatrix} = \begin{pmatrix} 1 & 1 & 1 & \cdots & 1 \\ \omega & \langle 1 \rangle \omega & \langle 2 \rangle \omega & \cdots & \langle p-1 \rangle \omega \\ \omega^2 & \langle 1 \rangle \omega^2 & \langle 2 \rangle \omega^2 & \cdots & \langle p-1 \rangle \omega^2 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ \omega^{p-1} & \langle 1 \rangle \omega^{p-1} & \langle 2 \rangle \omega^{p-1} & \cdots & \langle p-1 \rangle \omega^{p-1} \end{pmatrix} \begin{pmatrix} y_1 \\ y_2 \\ y_3 \\ \vdots \\ y_p \end{pmatrix}.$$

Since the matrix $(\langle j-1 \rangle \omega^{i-1})_{1 \leq i,j \leq p}$ is invertible, the above equation is solved in y_i's. Thus, we obtain the Galois descent of $\boldsymbol{\mu}_{p^2, B_2}$ by the action of $\mathbb{Z}/p\mathbb{Z}$.

Now, we assume that $B = A[u, \omega]$, i.e.,

$$\begin{tikzcd}
& B = A[u,\omega] \arrow[dl, dash] \arrow[dr, dash] & \\
B_1 = A[u] \arrow[dr, dash, "p-1"'] & & B_2 = A[\omega] \arrow[dl, dash, "p"] \\
& A &
\end{tikzcd},$$

$$\begin{tikzcd}
& \mathbb{Z}/(p-1)\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z} \arrow[dl, dash] \arrow[dr, dash] & \\
\mathbb{Z}/(p-1)\mathbb{Z} \arrow[dr, dash] & & \mathbb{Z}/p\mathbb{Z} \arrow[dl, dash] \\
& \{1\} &
\end{tikzcd}.$$

We obtain the Galois descent of $\boldsymbol{\mu}_{p^2,B}$ by the action of G, and the exact sequence

$$1 \to \left(\boldsymbol{\mu}_{p^2,B}\right)^G \to \mathbb{G}(n)_A \xrightarrow{\mathfrak{p}^2} \mathbb{G}(n)_A \to 1,$$

where $\mathfrak{p}$ is a prime ideal of $\mathbb{Z}[\zeta]$ lying over p. Therefore, using the same argument as in the previous section, one can compute the torsors for $(\boldsymbol{\mu}_{p^2,B})^G$.

One can compute the $(\boldsymbol{\mu}_{p^l,B})^G$-torsors for general $l \in \mathbb{Z}$, by considering the Kummer-Artin-Schreier-Witt exact sequence

$$1 \to \mathbb{Z}/p^{l-1}\mathbb{Z} \to \mathcal{W}_{l-1} \to \mathcal{V}_{l-1} \to 1,$$

which is given by Sekiguchi and Suwa [11].

4.4 Examples

Example 4.5 (In case $p^l = 3^2$)**.** Let the notation be as in the previous section, and consider the group scheme

$$\boldsymbol{\mu}_{3^2,B} = \operatorname{Spec} B[z]/(z^{3^2} - 1).$$

In this case, we have $(\mathbb{Z}/3^2\mathbb{Z})^\times \cong \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. In the multiplicative group $(\mathbb{Z}/3^2\mathbb{Z})^\times$, 4 is of order 3, and 8 is of order 2. Then, we define the action of $\langle 1\rangle \in \mathbb{Z}/3\mathbb{Z}$ and $[1] \in \mathbb{Z}/2\mathbb{Z}$ by

$$\langle 1\rangle z = z^4 \quad \text{and} \quad [1]z = z^8.$$

The values of q and p_i are given by $q = 8/2 = 4$, $p_1 = p_2 = p_3 = 1$, and $p_4 = 3$, thus we have

$$\begin{aligned} y_{1,1} &= -z + z^8, & y_{1,2} &= -z - z^8 + 2, \\ y_{2,1} &= -z^4 + z^5, & y_{2,2} &= -z^4 - z^5 + 2, \\ y_{3,1} &= -z^7 + z^2, & y_{3,2} &= -z^7 - z^2 + 2, \end{aligned}$$

and

$$y_{4,1} = -z^3 + z^6, \qquad y_{4,2} = -z^3 - z^6 + 2,$$

and we decompose the augmentation ideal J of $B[z]/(z^{3^2} - 1)$ into eigenspaces J_1 and J_2 by the action of $\mathbb{Z}/2\mathbb{Z}$, where J_1 is generated by $y_{1,1}, y_{2,1}, y_{3,1}, y_{4,1}$ over B with eigenvalue -1, and J_2 is generated by $y_{1,2}, y_{2,2}, y_{3,2}, y_{4,2}$ over B with eigenvalue 1. Matrices $M_{3^2,2}$ and $M_{3^2,3}$ are given by

$$\begin{pmatrix} y_1^2 \\ y_2^2 \\ y_3^2 \\ y_4^2 \end{pmatrix} = \begin{pmatrix} 0 & 0 & -1 & 0 \\ -1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix} \begin{pmatrix} y_{1,2} \\ y_{2,2} \\ y_{3,2} \\ y_{4,2} \end{pmatrix},$$

and

$$\begin{pmatrix} y_1^3 \\ y_2^3 \\ y_3^3 \\ y_4^3 \end{pmatrix} = \begin{pmatrix} -3 & 0 & 0 & 1 \\ 0 & -3 & 0 & 1 \\ 0 & 0 & -3 & 1 \\ 0 & 0 & 0 & -3 \end{pmatrix} \begin{pmatrix} y_1 \\ y_2 \\ y_3 \\ y_4 \end{pmatrix},$$

respectively. Note that $M_{3^2,1}$ is the identity matrix. Thus, we have

$$\boldsymbol{\mu}_{3^2,B} = \operatorname{Spec} B[y_1, y_2, y_3, y_4],$$

with relations

$$y_1y_2 = y_3^2 - y_4^2, \quad y_1y_4 = y_3^2 - y_1^2, \quad y_1^3 = -3y_1 + y_4, \quad y_4^3 = -3y_4, \tag{4.2}$$

and

$$\begin{aligned} y_2y_3 &= y_1^2 - y_4^2, \quad y_2y_4 = y_1^2 - y_2^2, \quad y_2^3 = -3y_2 + y_4, \\ y_3y_1 &= y_2^2 - y_4^2, \quad y_3y_4 = y_2^2 - y_3^2, \quad y_3^3 = -3y_3 + y_4, \end{aligned} \tag{4.3}$$

with group scheme structure

$$\begin{aligned} m^*(y_1) &= y_1 \otimes 1 + 1 \otimes y_1 + \frac{1}{2}\left(y_1 \otimes y_2^2 + y_2^2 \otimes y_1\right), \\ m^*(y_2) &= y_2 \otimes 1 + 1 \otimes y_2 + \frac{1}{2}\left(y_2 \otimes y_3^2 + y_3^2 \otimes y_2\right), \\ m^*(y_3) &= y_3 \otimes 1 + 1 \otimes y_3 + \frac{1}{2}\left(y_3 \otimes y_1^2 + y_1^2 \otimes y_3\right), \\ m^*(y_4) &= y_4 \otimes 1 + 1 \otimes y_4 + \frac{1}{2}\left(y_4 \otimes y_4^2 + y_4^2 \otimes y_4\right). \end{aligned}$$

Note that the latter six relations (4.3) are obtained by the first four relations (4.2) by action of $\mathbb{Z}/3\mathbb{Z}$. For example, the relation $y_2y_3 = y_1^2 - y_4^2$ is obtained by $y_1^{\langle 1\rangle}y_2^{\langle 1\rangle} = (y_3^2)^{\langle 1\rangle} - (y_4^2)^{\langle 1\rangle}$. Thus, the first four relations (4.2) are essential. Formulas for $m^*(y_2)$ and $m^*(y_3)$ are also obtained by $m^*(y_1)$.

Example 4.6 (In case $p^l = 3^3$)**.** Consider the group scheme

$$\boldsymbol{\mu}_{3^3,B} = \operatorname{Spec} B[z]/(z^{3^3} - 1).$$

In this case, we have $(\mathbb{Z}/3^3\mathbb{Z})^\times \cong \mathbb{Z}/3^2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. In the multiplicative group $(\mathbb{Z}/3^3\mathbb{Z})^\times$, 4 is of order 3^2, and 26 is of order 2. Then, we define the action of $\langle 1\rangle \in \mathbb{Z}/3^2\mathbb{Z}$ and $[1] \in \mathbb{Z}/2\mathbb{Z}$ by

$$\langle 1\rangle z = z^4 \quad \text{and} \quad [1]z = z^{26}.$$

The values of q and p_i are given by $q = 26/2 = 13$, $p_1 = p_2 = \cdots = p_9 = 1$, $p_{10} = p_{11} = p_{12} = 3$, and $p_{13} = 9$. Then, $y_{i,j}$'s are given by

$$\begin{aligned}
y_{1,1} &= -z + z^{26}, & y_{1,2} &= -z - z^{26} + 2,\\
y_{2,1} &= -z^4 + z^{23}, & y_{2,2} &= -z^4 - z^{23} + 2,\\
y_{3,1} &= -z^{16} + z^{11}, & y_{3,2} &= -z^{16} - z^{11} + 2,\\
y_{4,1} &= -z^{10} + z^{17}, & y_{4,2} &= -z^{10} - z^{17} + 2,\\
y_{5,1} &= -z^{13} + z^{14}, & y_{5,2} &= -z^{13} - z^{14} + 2,\\
y_{6,1} &= -z^{25} + z^{2}, & y_{6,2} &= -z^{25} - z^{2} + 2,\\
y_{7,1} &= -z^{19} + z^{8}, & y_{7,2} &= -z^{19} - z^{8} + 2,\\
y_{8,1} &= -z^{22} + z^{5}, & y_{8,2} &= -z^{22} - z^{5} + 2,\\
y_{9,1} &= -z^{7} + z^{20}, & y_{9,2} &= -z^{7} - z^{20} + 2,
\end{aligned}$$

and

$$\begin{aligned}
y_{10,1} &= -z^3 + z^{24}, & y_{10,2} &= -z^3 - z^{24} + 2,\\
y_{11,1} &= -z^{12} + z^{15}, & y_{11,2} &= -z^{12} - z^{15} + 2,\\
y_{12,1} &= -z^{21} + z^{6}, & y_{12,2} &= -z^{21} - z^{6} + 2,
\end{aligned}$$

and

$$y_{13,1} = -z^9 + z^{18}, \qquad y_{13,2} = -z^9 - z^{18} + 2,$$

and we decompose J into eigenspaces J_1 and J_2 by the action of $\mathbb{Z}/2\mathbb{Z}$, where J_1 is generated by $y_{1,1}, y_{2,1}, \ldots, y_{13,1}$ over B with eigenvalue -1, and J_2 is generated by $y_{1,2}, y_{2,2}, \ldots, y_{13,2}$ over B with eigenvalue 1. Matrices $M_{3^3,2}$ and $M_{3^3,3}$ are given by

$$\begin{pmatrix}
0 & 0 & 0 & 0 & 0 & -1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & -1 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & -1 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & -1 & 0 & 0 & 0 & 0 \\
-1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & -1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & -1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & -1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & -1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & -1 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & -1 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & -1 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & -1
\end{pmatrix}$$

and

$$\begin{pmatrix}
-3 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\
0 & -3 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\
0 & 0 & -3 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\
0 & 0 & 0 & -3 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & -3 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & -3 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & -3 & 0 & 0 & 1 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & -3 & 0 & 0 & 1 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & -3 & 0 & 0 & 1 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & -3 & 0 & 0 & 1 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & -3 & 0 & 1 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & -3 & 1 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & -3
\end{pmatrix},$$

respectively. Thus, we have

$$\boldsymbol{\mu}_{3^3,B} = \operatorname{Spec} B[y_1, y_2, \dots, y_{13}],$$

with relations

$$\begin{array}{llll}
y_1y_2 = y_3^2 - y_{11}^2, & y_2y_3 = y_4^2 - y_{12}^2, & \dots, & y_9y_1 = y_2^2 - y_{10}^2, \\
y_1y_3 = y_8^2 - y_{12}^2, & y_2y_4 = y_9^2 - y_{10}^2, & \dots, & y_9y_2 = y_7^2 - y_{11}^2, \\
y_1y_4 = y_7^2 - y_{13}^2, & y_2y_5 = y_8^2 - y_{13}^2, & \dots, & y_9y_3 = y_6^2 - y_{13}^2, \\
y_1y_5 = y_9^2 - y_{12}^2, & y_2y_6 = y_1^2 - y_{10}^2, & \dots, & y_9y_4 = y_8^2 - y_{11}^2, \\
y_1y_{10} = y_6^2 - y_1^2, & y_2y_{11} = y_7^2 - y_2^2, & \dots, & y_9y_{12} = y_5^2 - y_9^2, \\
y_1y_{11} = y_9^2 - y_7^2, & y_2y_{12} = y_1^2 - y_8^2, & \dots, & y_9y_{10} = y_2^2 - y_6^2, \\
y_1y_{12} = y_3^2 - y_4^2, & y_2y_{10} = y_4^2 - y_5^2, & \dots, & y_9y_{11} = y_2^2 - y_3^2,
\end{array}$$

$$y_1y_{13} = y_8^2 - y_2^2, \quad y_2y_{13} = y_9^2 - y_3^2, \quad \ldots, \quad y_9y_{13} = y_7^2 - y_1^2,$$

$$y_{10}y_{11} = y_{12}^2 - y_{13}^2, \quad y_{11}y_{12} = y_{10}^2 - y_{13}^2, \quad y_{12}y_{10} = y_{11}^2 - y_{13}^2,$$

$$y_{10}y_{13} = y_{12}^2 - y_{10}^2, \quad y_{11}y_{13} = y_{10}^2 - y_{11}^2, \quad y_{12}y_{13} = y_{11}^2 - y_{12}^2,$$

$$y_1^3 = -3y_1 + y_{10}, \quad y_2^3 = -3y_2 + y_{11}, \quad \ldots, \quad y_9^3 = -3y_9 + y_{12},$$

$$y_{10}^3 = -3y_{10} + y_{13}, \quad y_{11}^3 = -3y_{11} + y_{13}, \quad \ldots, \quad y_{12}^3 = -3y_{12} + y_{13},$$

$$y_{13}^3 = -3y_{13},$$

with group scheme structure

$$\begin{aligned}
m^*(y_1) &= y_1 \otimes 1 + 1 \otimes y_1 + \frac{1}{2}\left(y_1 \otimes y_5^2 + y_5^2 \otimes y_1\right), \\
m^*(y_2) &= y_2 \otimes 1 + 1 \otimes y_2 + \frac{1}{2}\left(y_2 \otimes y_6^2 + y_6^2 \otimes y_2\right), \\
&\vdots \\
m^*(y_1) &= y_9 \otimes 1 + 1 \otimes y_9 + \frac{1}{2}\left(y_9 \otimes y_4^2 + y_4^2 \otimes y_9\right), \\
m^*(y_{10}) &= y_3 \otimes 1 + 1 \otimes y_3 + \frac{1}{2}\left(y_{10} \otimes y_{11}^2 + y_{11}^2 \otimes y_{10}\right), \\
m^*(y_{11}) &= y_3 \otimes 1 + 1 \otimes y_3 + \frac{1}{2}\left(y_{11} \otimes y_{12}^2 + y_{12}^2 \otimes y_{11}\right), \\
m^*(y_{12}) &= y_3 \otimes 1 + 1 \otimes y_3 + \frac{1}{2}\left(y_{12} \otimes y_{10}^2 + y_{10}^2 \otimes y_{12}\right), \\
m^*(y_{13}) &= y_{13} \otimes 1 + 1 \otimes y_{13} + \frac{1}{2}\left(y_{13} \otimes y_{13}^2 + y_{13}^2 \otimes y_{13}\right).
\end{aligned}$$

Example 4.7 (In case $p^l = 5^2$)**.** Consider the group scheme

$$\boldsymbol{\mu}_{5^2,B} = \operatorname{Spec} B[z]/(z^{5^2} - 1).$$

In this case, we have $(\mathbb{Z}/5^2\mathbb{Z})^\times \cong \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$. In the multiplicative group $(\mathbb{Z}/5^2\mathbb{Z})^\times$, 6 is of order 5, and 7 is of order 4. Then, we define the action of $\langle 1 \rangle \in \mathbb{Z}/5\mathbb{Z}$ and $[1] \in \mathbb{Z}/4\mathbb{Z}$ by

$$\langle 1 \rangle z = z^6 \quad \text{and} \quad [1]z = z^7.$$

The values of q and p_i are given by $q = 24/4 = 6$, $p_1 = p_2 = p_3 = p_4 = p_5 = 1$, and $p_6 = 5$. Then, $y_{i,j}$'s are given by

$$y_{1,1} = -z + \zeta z^7 + z^{24} - \zeta z^{18}, \qquad y_{1,2} = -z + z^7 - z^{24} + z^{18},$$
$$y_{1,3} = -z - \zeta z^7 + z^{24} + \zeta z^{18}, \qquad y_{1,4} = -z - z^7 - z^{24} - z^{18} + 4,$$
$$y_{2,1} = -z^6 + \zeta z^{17} + z^{19} - \zeta z^8, \qquad y_{2,2} = -z^6 - z^{19} + z^{17} + z^8,$$
$$y_{2,3} = -z^6 - \zeta z^{17} + z^{19} + \zeta z^8, \qquad y_{2,4} = -z^6 - z^{17} - z^{19} - z^8 + 4,$$
$$y_{3,1} = -z^{11} + \zeta z^2 + z^{14} - \zeta z^{23}, \qquad y_{3,2} = -z^{11} + z^2 - z^{14} + z^{23},$$
$$y_{3,3} = -z^{11} - \zeta z^2 + z^{14} + \zeta z^{23}, \qquad y_{3,4} = -z^{11} - z^2 - z^{14} - z^{23} + 4,$$
$$y_{4,1} = -z^{16} + \zeta z^{12} + z^9 - \zeta z^{13}, \qquad y_{4,2} = -z^{16} + z^{12} - z^9 + z^{13},$$
$$y_{4,3} = -z^{16} - \zeta z^{12} + z^9 + \zeta z^{13}, \qquad y_{4,4} = -z^{16} - z^{13} - z^{12} - z^9 + 4,$$
$$y_{5,1} = -z^{21} + \zeta z^{22} + z^4 - \zeta z^3, \qquad y_{5,2} = -z^{21} + z^{22} - z^4 + z^3,$$
$$y_{5,3} = -z^{21} - \zeta z^{22} + z^4 + \zeta z^3, \qquad y_{5,4} = -z^{21} - z^{22} - z^4 - z^3 + 4,$$

and

$$y_{6,1} = -z^5 + \zeta z^{10} + z^{20} - \zeta z^{15}, \qquad y_{6,2} = -z^5 + z^{10} - z^{20} + z^{15},$$
$$y_{6,3} = -z^5 - \zeta z^{10} + z^{20} + \zeta z^{15}, \qquad y_{6,4} = -z^5 - z^{10} - z^{20} - z^{15} + 4.$$

where ζ is a primitive fourth root of unity. We decompose J into eigenspaces J_1, J_2, J_3, J_4 by the action of $\mathbb{Z}/4\mathbb{Z}$, where J_k is generated by $y_{i,k}$'s for $1 \leq i \leq 6$ over B, with eigenvalue ζ^k. Matrices $M_{5^2,2}, M_{5^2,3}, M_{5^2,4}, M_{5^2,5}$ are given by

$$M_{5^2,2} = \begin{pmatrix} 0 & -2\zeta & 1 & 0 & 0 & 0 \\ 0 & 0 & -2\zeta & 1 & 0 & 0 \\ 0 & 0 & 0 & -2\zeta & 1 & 0 \\ 1 & 0 & 0 & 0 & -2\zeta & 0 \\ -2\zeta & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & -2\zeta + 1 \end{pmatrix},$$

$$M_{5^2,3} = \begin{pmatrix} 3 & 0 & 0 & 3\zeta & \zeta & -3\zeta \\ \zeta & 3 & 0 & 0 & 3\zeta & -3\zeta \\ 3\zeta & \zeta & 3 & 0 & 0 & -3\zeta \\ 0 & 3\zeta & \zeta & 3 & 0 & -3\zeta \\ 0 & 0 & 3\zeta & \zeta & 3 & -3\zeta \\ 0 & 0 & 0 & 0 & 0 & 4\zeta+3 \end{pmatrix},$$

$$M_{5^2,4} = \begin{pmatrix} 0 & 0 & -8 & 6 & -4\zeta-1 & 4\zeta \\ -4\zeta-1 & 0 & 0 & -8 & 6 & 4\zeta \\ 6 & -4\zeta-1 & 0 & 0 & -8 & 4\zeta \\ -8 & 6 & -4\zeta-1 & 0 & 0 & 4\zeta \\ 0 & -8 & 6 & -4\zeta-1 & 0 & 4\zeta \\ 0 & 0 & 0 & 0 & 0 & -4\zeta-3 \end{pmatrix},$$

$$M_{5^2,5} = \begin{pmatrix} -20 & -10\zeta & -5\zeta+10 & 10\zeta & -15\zeta-5 & -10\zeta+1 \\ -15\zeta-5 & -20 & -10\zeta & -5\zeta+10 & 10\zeta & -10\zeta+1 \\ 10\zeta & -15\zeta-5 & -20 & -10\zeta & -5\zeta+10 & -10\zeta+1 \\ -5\zeta+10 & 10\zeta & -15\zeta-5 & -20 & -10\zeta & -10\zeta+1 \\ -10\zeta & -5\zeta+10 & 10\zeta & -15\zeta-5 & -20 & -10\zeta+1 \\ 0 & 0 & 0 & 0 & 0 & -20\zeta-15 \end{pmatrix},$$

respectively. One can give explicit relations among $y_{i,j}$'s and group scheme structure.

Appendix

In this appendix, we give an outline of a proof which we apply the push-down and the pull-back theory to the torsors of schemes.

Push-Down of Torsors

Let G be a commutative group scheme over X, and Y/X a G-torsor. For a group homomorphism $\varphi : G \to G'$, we obtain the G'-torsor on X as follows, by the same argument with the push-down in extensions of groups: Consider the diagram

$$\begin{tikzcd}
G \arrow[d, "\varphi"] & \curvearrowright & Y \arrow[r, "\pi"] \arrow[d, "\tilde{\varphi}"] & X \arrow[d, equal] \ , \\
G' & \curvearrowright & \varphi_* Y \arrow[r, "\tilde{\pi}"] & X
\end{tikzcd}$$

where we assume that there exists the quotient

$$\varphi_* Y = G' \times Y / \{\, (\varphi g, -g) \mid g \in G \,\}$$

as a scheme, and the morphisms $\tilde{\varphi}$ and $\tilde{\pi}$ are defined by

$$\tilde{\varphi}(y) = \overline{(0, y)} \quad \text{and} \quad \tilde{\pi}\left(\overline{(g', y)}\right) = \pi(y)$$

for any local sections $y \in Y$, $g' \in G'$, and G' acts on $\varphi_* Y$ by

$$g'\left(\overline{(g'', y)}\right) = \overline{(g' + g'', y)}.$$

Then, one can check that $\tilde{\pi}$ is well defined and the diagram is commutative, i.e.,

$$\tilde{\varphi}(gy) = \varphi g(\tilde{\varphi} y) \quad \text{and} \quad \tilde{\pi} \circ \tilde{\varphi} = \pi.$$

Moreover, we have

$$(\tilde{\pi})^{-1}(\pi y) = \overline{(G', Gy)} = \overline{(\varphi(G) + G', y)} = \overline{(G', y)} \simeq G'.$$

Therefore, we see that $\varphi_* Y$ is a G'-torsor on X.

Pull-Back of Torsors

Let G be a group, and Y/X a G-torsor. For a morphism $f : X' \to X$, we obtain the G-torsor on X' as follows, as in the same argument as the pull-back in extensions of groups: Consider the diagram

$$\begin{tikzcd}
G \arrow[d, equal] & \curvearrowright & f^*Y \arrow[r, "p_2"] \arrow[d, "p_1"] \arrow[dr, phantom, "\square"] & X' \arrow[d, "f"] \, , \\
G & \curvearrowright & Y \arrow[r, "\pi"] & X
\end{tikzcd}$$

where $f^*Y = Y \times_X X'$, the morphisms p_1 and p_2 are projections, and G acts on f^*Y by

$$g(y, x') = (gy, x').$$

Then, we see that the action of G commutes with the projection p_1, and f^*Y is a G-torsor on X'.

Bibliography

[1] F. Andreatta and C. Gasbarri, *Torsors under some group schemes of order p^n*, Journal of Algebra **318** (2007), 1057–1067.

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

[3] A. Grothendieck, M. Artin and J. L. Verdier, *Théorie des topos et cohomologie étale des schémas*, Lecture Notes in Mathematics **269**, **270**, **305**, Springer-Verlag, Heidelberg, 1972–73.

[4] Y. Koide, *On Torsors for General Twisted Finite Group Schemes of Prime Order*, JP Journal of Algebra, Number Theory and Applications **28** (2013), 107–127.

[5] Y. Koide and T. Sekiguchi, *On the Cyclotomic Twisted Torus*, Far East Journal of Mathematical Sciences **72** (2013), 201–224.

[6] B. Mazur, K. Rubin and A. Silverberg, *Twisting Commutative Algebraic groups,* Journal of Algebra **314** (2007), 419–438.

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

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

[9] L. G. Roberts, *The Flat Cohomology of Group Schemes of Rank p*, American Journal of Mathematics **95** (1973), 688–702.

[10] T. Sekiguchi, F. Oort and N. Suwa, *On the deformation of Artin-Schreier to Kummer*, Ann. Scient. École Norm. Sup. **22** (1989), 345–375.

[11] T. Sekiguchi and N. Suwa, *On the unified Kummer-Artin-Schreier-Witt theory*, Prépublication n^{o}111 (1999), Mathématiques Pures de Bordeaux C.N.R.S.

[12] T. Sekiguchi and Y. Toda, *On the cyclotomic twisted torus and some torsors*, International Journal of Pure and Applied Mathematics **89** (2013), 461–482.

[13] Y. Toda, *On the torsors for group schemes of prime-power order*, International Journal of Pure and Applied Mathematics **96** (2014), 407–425.

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

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

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