CHUO MATH NO.100(2013)

On the cyclotomic twisted torus and some torsors

by
Tsutomu Sekiguchi and Yohei Toda

DEPARTMENT OF MATHEMATICS
CHUO UNIVERSITY
BUNKYOKU TOKYO JAPAN

JAN.11 , 2013

On the cyclotomic twisted torus and some torsors

Tsutomu Sekiguchi, Yohei Toda

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

---

Abstract

Our aim in this paper is to compute the first cohomology of some type of finite group schemes. L. G. Roberts [7] gave the first cohomology of group schemes in certain conditions. We compute it by completely different way and under circumstances, by using the concept of cyclotomic twisted tori. The concept was introduced by Y. Koide and T. Sekiguchi [4], and they showed that such a twisted torus is isomorphic to a subgroup scheme in a Weil restriction of 1-dimensional algebraic torus given by the intersection of whole norm maps. Here we extend the isomorphism to a resolution of the cyclotomic twisted torus, consisting of Weil restriction of 1-dimensional algebraic tori and several norm maps. And we describe the endomorphism ring of a cyclotomic twisted torus. Moreover, we show that by using the resolution, one can compute that first cohomology of a cyclotomic twisted torus, and that one can describe the torsors of some type of finite group schemes by using the concept of cyclotomic twisted tori.

Email addresses: `sekiguti@math.chuo-u.ac.jp` (Tsutomu Sekiguchi), `yoyo@gug.math.chuo-u.ac.jp` (Yohei Toda)

1. Introduction

F. Oort and J. Tate [6] gave the complete classification of finite group schemes of order prime p in the following way: Let A be a Λ_p-algebra, where

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

ζ being a primitive $(p-1)$-st root of unity in the ring of p-adic integers $\mathbb{Z}_p$. Then any finite A-group schemes of order p are classified by triples (M, a, b) consisting of a projective module M of rank 1 (cf. [1, Chap. II, p.141]), together with $a \in M^{\otimes(p-1)}$ and $b \in M^{\otimes(1-p)}$ such that $a \otimes b = \omega_p$ where ω_p is the product of p and of an invertible element of Λ_p (cf. [6] for details). The group scheme corresponding to triples (M, a, b) is given by

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

with the group scheme structure

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

where $U(i)$ is an invertible element of A.

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 the multiplicative group of the invertible elements of A. If A has characteristic p, then

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

If u is a $(p-1)$-st root of $b \in A$ with $a = b^{-1}\omega_p \in A$ and $B = A[u]$, then $G_{a,b}$ is the Galois descent of $\boldsymbol{\mu}_{p,B}$. Our aim is to compute the torsors for this kind of group schemes $G_{a,b}$.

As all the symbols used in [4], we denote by n a positive integer, by $m = \phi(n)$ the value of the Euler function and by G a cyclic group of order n

with a generator σ_0, unless otherwise stated throughout this paper. Let B/A be a G-torsor. We suppose that B is a free A-module. Let ζ be a primitive n-th root of unity, and I be the representation matrix of the action of ζ on $\mathbb{Z}[\zeta]$ by the multiplication. Then we can define an action of G on $\mathbb{G}_{m,B}^m$ by $(x_1, x_2, \ldots, x_m)^{\sigma_0} = (x_1, x_2, \ldots, x_m)^I$, and on B by the Galois action (cf. §2). By this G-action, we can descent the torus $\mathbb{G}_{m,B}^m$ to over A, which we call *a cyclotomic twisted torus of degree* n, and we denote it by $\mathbb{G}(n)_A$. Y. Koide and T. Sekiguchi [4] showed that the cyclotomic twisted torus is canonically isomorphic to the subgroup scheme

$$\mathcal{T}(n)_A := \bigcap_{\ell | n} \operatorname{Ker}(\operatorname{Nm}_\ell) \subset \prod_{B/A} \mathbb{G}_{m,B},$$

where Nm_ℓ is the norm map from B to $B_\ell = B^{\langle \sigma_0^{n/\ell} \rangle}$ (cf. [4, Th. 6.1.]). We extend the isomorphism to a resolution of the cyclotomic twisted torus, which we call *a cyclotomic resolution*, as follows.

Assertion 1. (cf. Th. 3.2, 3.3) *Let* $n = p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r}$ *be the prime decomposition of a positive integer* n*. For integers* $1 \leq i_0 < i_1 < \cdots < i_s \leq r$*, we set* $n_{i_0 i_1 \cdots i_s} = n/p_{i_0} p_{i_1} \cdots p_{i_s}$ *and* $B_{i_0 i_1 \cdots i_s} = B^{\langle \sigma_0^{n_{i_0 i_1 \cdots i_s}} \rangle}$*. Under these notations, there is a following exact sequence of sheaves of groups on* $(\operatorname{Spec} A)_{\mathrm{flat}}$*;*

$$\begin{aligned} 0 \to \mathbb{G}(n)_A \xrightarrow{\varepsilon} \prod_{B/A} \mathbb{G}_{m,B} \xrightarrow{\partial^0} & \prod_{i=1}^{r} \left(\prod_{B_i/A} \mathbb{G}_{m,B_i} \right) \\ & \xrightarrow{\partial^1} \prod_{1 \leq i_0 < i_1 \leq r} \left(\prod_{B_{i_0 i_1}/A} \mathbb{G}_{m,B_{i_0 i_1}} \right) \xrightarrow{\partial^2} \cdots \\ & \xrightarrow{\partial^{r-1}} \prod_{B_{12\cdots r}/A} \mathbb{G}_{m,B_{12\cdots r}} \to 0. \end{aligned}$$

In §2, we quickly review the cyclotomic twisted torus $\mathbb{G}(n)$. In §3, we give the cyclotomic resolution above. In §4, we give explicitly the endomorphism ring of $\mathbb{G}(n)_A$ and the isomorphism as follows.

Assertion 2. (cf. Th. 4.1) *There exists the canonical isomorphism*

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

Assertion 3. (cf. Prop. 4.2) *For* $\varphi \in \mathrm{End}(\mathbb{G}(n)_A)$ $(\varphi \neq 0)$,

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

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

In §5, we compute the first cohomology of $\mathbb{G}(n)_A$ and the Galois descent of the kernel of an isogeny $\theta : \mathbb{G}^m_{m,B} \to \mathbb{G}^m_{m,B}$, where $\theta \in \mathbb{Z}[\zeta]$.

2. Review on $\mathbb{G}(n)$: the cyclotomic twisted tori

From now on, as in the introduction, we denote by n a positive integer, by $m = \phi(n)$ the value of the Euler function and by G a cyclic group of order n with a generator σ_0. Let B/A be a G-torsor. We suppose that B is a free A-module. Let ζ be a primitive n-th root of unity. Let

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

be the cyclotomic polynomial, and I be the representation matrix of the action of ζ on $\mathbb{Z}[\zeta]$ by the multiplication, that is to say,

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

It is well-known that the coefficients of $\Phi_n(x)$ are rational integers. In particular, we can easily see that $a_m = 1$. In general, for a vector $\boldsymbol{x} = (x_1, x_2, \ldots, x_m)$ and a matrix $A = (a_{ij}) \in \mathrm{M}_{m\times\ell}(\mathbb{Z})$, we define the matrix power $\boldsymbol{x}^A$ by

$$\boldsymbol{x}^A = \left(\prod_{j=1}^{m} x_j^{a_{j1}}, \prod_{j=1}^{m} x_j^{a_{j2}}, \ldots, \prod_{j=1}^{m} x_j^{a_{j\ell}} \right).$$

Now we consider the algebraic torus

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

over B. It is well-known that $\operatorname{Aut}(\mathbb{G}_{m,B}^m) \cong \mathrm{GL}_m(\mathbb{Z})$. We define an action of G on $\mathbb{G}_{m,B}^m$ by

$$\sigma_0 : \begin{cases} B[x_1, \ldots, x_m, 1/\prod_{i=1}^m x_i] & \xrightarrow{\sigma_0} & B[x_1, \ldots, x_m, 1/\prod_{i=1}^m x_i]; \\ \boldsymbol{x} = (x_1, \ldots, x_m) & \mapsto & \boldsymbol{x}^{\sigma_0} = (x_1^{\sigma_0}, \ldots, x_m^{\sigma_0}) = \boldsymbol{x}^I, \\ b \in B & \mapsto & b^{\sigma_0}. \end{cases}$$

By this G-action, we can descent the torus $\mathbb{G}_{m,B}^m$ to over A, which we call a *cyclotomic twisted torus of degree* n, and we denote it by $\mathbb{G}(n)_A$. Then the cyclotomic twisted torus can be 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 the ideal $\mathfrak{A}$ is given explicitly (cf. [4, Th. 4.1.]).

Example 2.1. In case $p = 5$ and $A = \mathbb{F}_5$, 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

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

If $p = 7$ and $A = \mathbb{F}_7$ then

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

with the ideal $\mathfrak{A}$ generated by

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

The cyclotomic twisted torus is canonically isomorphic to the intersection of the kernels of norm maps. In fact, for each positive integer ℓ dividing n, we denote $B_\ell = B^{\langle \sigma_0^{n/\ell} \rangle} \subset B$, and

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

the norm map from B to B_ℓ. Then the group scheme

$$\mathcal{T}(n)_A = \bigcap_{\ell | n} \mathrm{Ker}\,(\mathrm{Nm}_\ell) \subset \prod_{B/A} \mathbb{G}_{m,B}$$

is nothing but the cyclotomic twisted torus $\mathbb{G}(n)_A$ (cf. [4, Th. 6.1.]).

3. Cyclotomic resolution

Here we note the surjectivity of the norm map

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

for later use.

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

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

is surjective.

Proof. Let $\overline{a}$ be a primitive element of $\mathbb{F}_{q^n}$. Then

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

This is an element of $\mathbb{F}_q$ of order $q-1$. $\square$

The rest of this section, we denote $k=\mathbb{F}_q$ and $K=\mathbb{F}_{q^n}$. Now we have the following theorem.

Theorem 3.2. *Let $n=p_1^{e_1}p_2^{e_2}\cdots p_r^{e_r}$ be the prime decomposition of a positive integer n. For integers $1\le i_0<i_1<\cdots<i_s\le r$, we set $n_{i_0i_1\cdots i_s}=n/p_{i_0}p_{i_1}\cdots p_{i_s}$ and $M_{i_0i_1\cdots i_s}=\mathbb{F}_{q^{n_{i_0i_1\cdots i_s}}}$. Under these notations, there is a following exact sequence which we call a cyclotomic resolution;*

$$0\to\mathbb{G}(n)_k(k)\xrightarrow{\varepsilon}K^\times\xrightarrow{\partial^0}\prod_{i=1}^{r}M_i^\times\xrightarrow{\partial^1}\prod_{1\le i_0<i_1\le r}M_{i_0i_1}^\times\xrightarrow{\partial^2}\cdots$$
$$\cdots\xrightarrow{\partial^{r-2}}\prod_{i=1}^{r}M_{12\cdots\hat{i}\cdots r}^\times\xrightarrow{\partial^{r-1}}M_{12\cdots r}^\times\to 0,$$

where the morphisms ∂^i are defined as

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

for $x\in K$, and

$$(\partial^s\boldsymbol{x})_{i_0i_1\cdots i_s}=\prod_{j=0}^{s}\left(\mathrm{Nm}_{M^\times_{i_0i_1\cdots\hat{i_j}\cdots i_s}/M^\times_{i_0i_1\cdots i_s}}x_{i_0i_1\cdots\hat{i_j}\cdots i_s}\right)^{(-1)^j}$$

for $\boldsymbol{x}=(x_{i_0i_1\cdots i_{s-1}})_{1\le i_0<i_1<\cdots<i_{s-1}\le r}\in\prod_{1\le i_0<\cdots<i_{s-1}\le r}M^\times_{i_0i_1\cdots i_{s-1}}$.

Proof. Clearly, $\partial^{s+1}\partial^{s} = 1$. The case of $r = 1$ is proved by Lemma 3.1. We use induction on the number r of the prime factors of n.

First, we check that $\operatorname{Ker}\partial^1 \subset \operatorname{Im}\partial^0$ in the case $r = 2$, that is to say, $n = p_1^{e_1}p_2^{e_2}$. In this case, the required resolution is as follows;

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

Set

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

By Lemma 3.1, we can take an element $z_1 \in K^\times$ satisfying $x_1 = \mathrm{Nm}_{K^\times/M_1^\times} z_1$. Then

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

Therefore we may assume that $\boldsymbol{x} = (1, x_2) \in \operatorname{Ker}\partial^1$. Now we can take an element $z_2 \in K^\times$ satisfying $x_2 = \mathrm{Nm}_{K^\times/M_2^\times} z_2$, and prepare more notations. 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

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

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

$$f_1(X)\frac{X^{n_1} - 1}{X^{n_{12}} - 1} + f_2(X)\frac{X^{n_2} - 1}{X^{n_{12}} - 1} = 1$$

(cf. [4, Lem. 6.4., Prop. 7.4.]). Now we set

$$\gamma = z_2^{f_1(\sigma_0)(\sigma_0^{n_1} - 1)/(\sigma_0^{n_{12}} - 1)}.$$

Then

$$\mathrm{N}_{K^\times/M_1^\times}\gamma = 1 \quad \text{and} \quad \mathrm{N}_{K^\times/M_2^\times}\gamma = x_2.$$

That is to say, $\partial^0\gamma = \boldsymbol{x}$. Hence we prove that $\operatorname{Ker}\partial^1 \subset \operatorname{Im}\partial^0$.

Second, we will verify that $\operatorname{Ker}\partial^{s+1} \subset \operatorname{Im}\partial^{s}$, where $s+1 \neq r-1$. For simplicity, we suppose that $1 \leq i_0 < i_1 < \cdots < i_s$ always. Set

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

and

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

and consider a sequence

$$0 \to \mathbb{G}(n)_k(k) \xrightarrow{\varepsilon} K^{\times} \xrightarrow{\partial'^0} \prod_{i=1}^{r-1} M_i^{\times} \xrightarrow{\partial'^1} \prod_{1 \leq i_0 < i_1 \leq r-1} M^{\times}_{i_0 i_1} \xrightarrow{\partial'^2} \cdots$$
$$\cdots \xrightarrow{\partial'^{r-2}} M^{\times}_{12 \cdots r-1} \to 0,$$

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

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

and

$$(\partial^s \boldsymbol{u})^{-1} \boldsymbol{x} \in \operatorname{Ker}\partial^{s+1}.$$

Therefore we may assume that $\boldsymbol{x} = (x_{i_0 i_1 \cdots i_s})_{i_s \leq r} \in \operatorname{Ker}\partial^{s+1}$ with $x_{i_0 i_1 \cdots i_s} = 1$ for $i_s \leq r-1$. Then we have

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

We set

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

and consider a sequence

$$0 \to \mathbb{G}(n')_k(k) \xrightarrow{\varepsilon'} (K')^\times \xrightarrow{(\partial')^0} \prod_{i=1}^{r-1} (M'_i)^\times$$
$$\xrightarrow{(\partial')^1} \prod_{1 \le i_0 < i_1 \le r-1} (M'_{i_0 i_1})^\times \xrightarrow{(\partial')^2} \cdots \xrightarrow{(\partial')^{r-2}} (M'_{12\cdots r-1})^\times \to 0,$$

where the morphisms $(\partial')^i$ are naturally induced by ∂^i. Then

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

Then we choose an element $\boldsymbol{v}' = \left(v'_{i_0 i_1 \cdots i_{s-2}}\right)_{i_{s-2} \le r-1}$ 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

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

and

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

Then we have

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

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 prepare more notations. We set

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

Fixed

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

Then

$$\partial^{r-1}\boldsymbol{x} = \prod_{j=1}^{r} (\mathrm{Nm}_{M_{\hat{j}}^{\times}/M_{1\cdots r}^{\times}} x_{\hat{j}})^{(-1)^{j-1}} = 1.$$

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

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

Now we set

$$n' = p_1^{e_1} p_2^{e_2}, \quad q' = q^{p_3^{e_3-1} \cdots p_r^{e_r-1}}, \quad K' = M_{\widehat{12}} = \mathbb{F}_{(q')^{n'}},$$
$$\boldsymbol{x}' = \left(x_{\hat{1}}, \prod_{j=2}^{r} \left(\mathrm{Nm}_{K^{\times}/M_{\hat{2}}^{\times}} z_j \right)^{(-1)^j} \right) \in (M_2')^{\times} \times (M_1')^{\times} = M_{\hat{1}}^{\times} \times M_{\hat{2}}^{\times},$$

and consider a sequence

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

Then

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

By the induction hypothesis, we can choose an element $u_{\widehat{12}} \in (K')^{\times} = M_{\widehat{12}}^{\times}$ such that $(\partial')^0 u_{\widehat{12}} = \boldsymbol{x}'$. By setting $u_{\widehat{ij}} = 1$ for $\widehat{ij} \neq \widehat{12}$ and $\boldsymbol{u} = (u_{\widehat{ij}})_{1 \le i < j \le r}$, we have

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

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

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

and consider a sequence

$$0 \to \mathbb{G}(n'')_k(k) \xrightarrow{\varepsilon''} (K'')^\times \xrightarrow{(\partial'')^0} \prod_{i=1}^{r-1} (M''_i)^\times \xrightarrow{(\partial'')^1} \prod_{1\le i_0,i_1\le r-1} (M''_{i_0 i_1})^\times$$
$$\xrightarrow{(\partial'')^2} \cdots \xrightarrow{(\partial'')^{r-3}} \prod_{i=1}^{r-1} (M''_{\hat{i}})^\times \xrightarrow{(\partial'')^{r-2}} (M''_{12\cdots r-1})^\times \to 0.$$

Then

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

Again by the induction hypothesis, we can choose an element $\boldsymbol{v}' = (v_{\widehat{ij}})_{1\le i<j\le r-1}$ such that $(\partial'')^{r-3}\boldsymbol{v}'_{\widehat{ij}} = \boldsymbol{x}''$. By setting $v_{\widehat{ir}} = 1$ and $\boldsymbol{v} = (v_{\widehat{ij}})_{1\le i<j\le r}$, we have

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

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 3.2 is the surjectivity of the norm map

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

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

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

where the notations are as in the previous section, namely, G is a cyclic group of order n and B/A is a G-torsor. 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;

$$\begin{array}{ccc}\left(\prod_{B/A}\mathbb{G}_{m,B}\right)(R)=(R\otimes_A B)^\times & \xrightarrow{\mathrm{Nm}(R)} & \mathbb{G}_{m,A}(R)=R^\times \\ \Big\downarrow \text{rest.} & & \Big\downarrow \text{rest.} \\ \left(\prod_{B/A}\mathbb{G}_{m,B}\right)(S)=(S\otimes_A B)^\times & \xrightarrow{\mathrm{Nm}(S)} & \mathbb{G}_{m,A}(S)=S^\times .\end{array}$$

Thus we see that $\mathrm{Nm}(S)(\overline{T}\otimes 1)=\mathrm{rest}(a)$. Therefore by the same argument in the proof of Theorem 3.2, we have the following.

Theorem 3.3. *The sequence of sheaves of groups on* $(\operatorname{Spec} A)_{\mathsf{flat}}$:

$$\begin{aligned}0\to\mathbb{G}(n)_A \xrightarrow{\varepsilon} \prod_{B/A}\mathbb{G}_{m,B} \xrightarrow{\partial^0} \prod_{i=1}^{r}\left(\prod_{B_i/A}\mathbb{G}_{m,B_i}\right) \\ \xrightarrow{\partial^1} \prod_{1\le i_0<i_1\le r}\left(\prod_{B_{i_0i_1}/A}\mathbb{G}_{m,B_{i_0i_1}}\right)\xrightarrow{\partial^2}\cdots \\ \xrightarrow{\partial^{r-1}} \prod_{B_{12\cdots r}/A}\mathbb{G}_{m,B_{12\cdots r}}\to 0,\end{aligned}$$

where $B_{i_0i_1\cdots i_s}=B^{\langle\sigma_0^{n_{i_0i_1\cdots i_s}}\rangle}$, *is exact.*

4. Endomorphism ring of cyclotomic twisted torus

Under the notations in the previous section, we determine the endomorphism ring of $\mathbb{G}(n)_A$ as follows.

Theorem 4.1. *There exists the following canonical isomorphism*;

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

Proof. Suppose that φ is a G-equivariant endomorphism of $\mathbb{G}^m_{m,B}$. 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

$$b_{1k} = \sum_{\ell=1}^{k-1} \alpha_\ell c_{m-k+1+\ell}$$

by the relations above, where $\alpha_1 = -1$ and

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

Then

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

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

$$\sum_{\ell=k-i+1}^{k} \alpha_\ell a_{m-\ell+k-i+1},$$

(i, j)-entry of the matrix $\sum_{k=1}^{m} c_k I^{k-1}$ is

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

This proves the theorem. □

By Theorem 4.1, we have the following proposition.

Proposition 4.2. *For* $\varphi \in \mathrm{End}(\mathbb{G}(n)_A)$ $(\varphi \neq 0)$,

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

where $\det \varphi = \det M$ *for the representing matrix* M*, and* $\mathrm{Nm}\, \varphi$ *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 $\varphi \in \mathrm{End}(\mathbb{G}(n)_A)$ $(\varphi \neq 0)$. Set

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

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

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

Note that $\det M > 0$ since

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

Then we can choose $J, J' \in \mathrm{GL}_m(\mathbb{Z})$ 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 $\det M = \mathrm{ord}\,(\mathrm{Ker}\, \varphi)$ since

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

$\square$

5. $G_{a,b}$-torsors

As previous section, 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

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

ζ being 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 $\prod_{B/A} \mathbb{G}_{m,B}$ is a smooth X-group scheme,

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

for $q \geq 0$. In general,

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

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

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

We obtain,

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

Therefore we have the following equalities;

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

since

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

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

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

Consider the exact sequence

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

which is obtained by the cyclotomic resolution,

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

Under flat topology, we have an exact sequence,

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

Then we have the canonical isomorphism,

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

and the explicit correspondence is given as follows: For $\overline{f} \in \mathrm{Coker}\, H^0(X, \partial^0)$ which is represented by $f \in H^0(X, \mathrm{Ker}\, \partial^1)$, we have the following diagram

$$\begin{array}{ccccccccc}
 & & & & \partial f = f^* \left(\prod_{B/A} \mathbb{G}_{m,B} \right) & \longrightarrow & X & & \\
 & & & & \downarrow & \square & \downarrow{\scriptstyle f} & & \\
0 & \longrightarrow & \mathbb{G}(n)_A & \xrightarrow{\varepsilon} & \prod_{B/A} \mathbb{G}_{m,B} & \xrightarrow{\partial^0} & \mathrm{Ker}\, \partial^1 & \longrightarrow & 0
\end{array}$$

by taking pull-back i.e. fiber product (cf. §7).

Let $\mathfrak{p}$ be a principal prime ideal 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. [9, Prop. 2.14.]). We assume that $n = p - 1$. Set $\mathfrak{p} = (\theta)$. Then we have an exact sequence

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

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

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

We can describe the torsors for $(\boldsymbol{\mu}_{p,B})^G$ in the following way: By Oort-Tate's classification theorem, we have

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

with comultiplication

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

where ω_p is the product of p and of an invertible element of Λ_p, and $U(i)$ is an invertible element of A (cf. [6] for details). The Galois group $G = \langle \sigma_0 \rangle$ acts on $\boldsymbol{\mu}_{p,B} = \operatorname{Spec} B[x]/(x^p - 1)$ by $x^{\sigma_0} = x^\ell$ with some integer ℓ, and on $\operatorname{Spec} B[z]/(z^p - \omega_p z)$ by $z^{\sigma_0} = \zeta^\ell z$ where ζ is a primitive n-th root of unity (cf. [6, Section 2, Prop.]). Now we assume that there exists $u \in B$ a n-th root of some non-zero divisor $b \in A$ with $a = b^{-1}\omega_p \in A$ and $B = A[u]$. Then $G_{a,b}$ is the Galois descent of $\boldsymbol{\mu}_{p,B}$. In fact, we may assume without loss of generality that $u^{\sigma_0} = \zeta^\ell u$ since

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

Hence $u^{-1}z$ is G-invariant. Therefore we have the following equalities

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

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

and that the Galois descent of $\boldsymbol{\mu}_{p,B}$ is given by $G_{a,b}$, i.e., we obtain an exact sequence

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

From this sequence, we obtain a long exact sequence

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

Then we have the non-canonical isomorphism

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

and the explicit correspondence is given as follows: For $\overline{g} \in \operatorname{Coker} H^0(X, \theta)$ and $f^*\left(\prod_{B/A} \mathbb{G}_{m,B}\right) \in \operatorname{Ker} H^1(X, \theta)$, we have the diagram,

$$
\begin{array}{ccccc}
G_{a,b} & \curvearrowright & \varphi^{-1}(\{0\} \times X) & \longrightarrow & X \\
\downarrow{\scriptstyle \iota} & & \downarrow & & \| \\
\mathbb{G}(n)_A & \curvearrowright & f^*\left(\displaystyle\prod_{B/A} \mathbb{G}_{m,B}\right) & \longrightarrow & X \\
\downarrow{\scriptstyle \theta} & & \downarrow{\scriptstyle \varphi} & & \| \\
\mathbb{G}(n)_A & \curvearrowright & \theta_* f^*\left(\displaystyle\prod_{B/A} \mathbb{G}_{m,B}\right) & \longrightarrow & X \\
 & & \wr\| & & \\
 & & \mathbb{G}(n)_A \times X & &
\end{array}
$$

where $\iota_*\left(\varphi^{-1}\left(\{1\} \times X\right)\right) \cong f^*\left(\prod_{B/A} \mathbb{G}_{m,B}\right)$ (cf. §7). Therefore we have

$$\partial\, g + \varphi^{-1}(\{0\} \times X) \in H^1(X, G_{a,b}),$$

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

Note that we only considered the case that prime ideals lying over p are principal. The non-principal case is studied by Y. Koide in his forthcoming paper [3].

6. Examples

Example 6.1 (cf. [6] for details)**.** In case $p = 7$, $n = 6$, $m = 2$. The base ring Λ_7 is given by

$$\Lambda_7 = \mathbb{Z}\left[\zeta, \frac{1}{6(2+\zeta)}\right],$$

where ζ is the unique element of $\mathbb{Z}_7$ such that $\zeta^3 = -1$ and $\zeta \equiv 3 \pmod 7$. The representation matrix of the action of ζ on $\mathbb{Z}[\zeta]$ is given by

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

i.e., $G = \langle \sigma_0 \rangle$ acts on $\mathbb{G}^2_{m,B} = \operatorname{Spec} B[x, y, 1/xy]$ by $(x, y)^{\sigma_0} = (y, x^{-1}y)$. Set $\theta = 3 - 2\zeta \in \mathbb{Z}[\zeta]$ which corresponds to an endomorphism

$$\begin{pmatrix} 3 & 2 \\ -2 & 1 \end{pmatrix} \in \operatorname{End}\left(\mathbb{G}(6)_A\right).$$

Note that $\det \theta = 7$. Then we see that

$$\begin{pmatrix} 1 & 0 \\ 3 & 1 \end{pmatrix} \begin{pmatrix} 3 & 2 \\ -2 & 1 \end{pmatrix} \begin{pmatrix} 1 & -2 \\ -1 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 7 \end{pmatrix}$$

and

$$\operatorname{Ker} \theta \cong \operatorname{Spec} B[x, y, 1/xy]/(x - y^3, y^7 - 1) \cong \operatorname{Spec} B[y]/(y^7 - 1) \cong \boldsymbol{\mu}_{7,B}$$

with the G-action $y^{\sigma_0} = y^5$. By Oort-Tate's theorem, the group scheme $\boldsymbol{\mu}_{7,B}$ is isomorphic to the group scheme $\operatorname{Spec} B[z]/(z^7 - \omega_7 z)$ with comultiplication

$$m^*(z) = z \otimes 1 + 1 \otimes z - \frac{1}{6} \sum_{i=1}^{6} U(i) z^i \otimes z^{7-i},$$

where

$$\begin{aligned} U(1) = U(6) &= \frac{1}{\zeta(2+\zeta)^4}, \\ U(2) = U(5) &= \frac{1}{\zeta(2+\zeta)^5}, \\ U(3) = U(4) &= \frac{1}{-(2+\zeta)^5}, \end{aligned}$$

and

$$z = -y + \zeta y^2 + \zeta^2 y^3 - \zeta^2 y^4 - \zeta y^5 + y^6.$$

Hence G acts on $\operatorname{Spec} B[z]/(z^7 - \omega_7 z)$ by

$$z^{\sigma_0} = -y^5 + \zeta y^3 + \zeta^2 y - \zeta^2 y^6 - \zeta y^4 + y^2 = \zeta^5 z.$$

Now we assume that there exists $u \in B$ a 6-th root of some non-zero divisor $b \in A$ with $a = b^{-1}\omega_7 \in A$ and $B = A[u]$. We may assume without loss of generality that $u^{\sigma_0} = \zeta^5 u$. Then $u^{-1}z$ is G-invariant. Therefore $G_{a,b}$ is the Galois descent of $\boldsymbol{\mu}_{7,B}$ since

$$z^7 - \omega_7 z = u^7 \left(\left(\frac{z}{u}\right)^7 - a\left(\frac{z}{u}\right) \right) \in B\left[\frac{z}{u}\right]$$

and

$$m^*\left(\frac{z}{u}\right) = \left(\frac{z}{u}\right) \otimes 1 + 1 \otimes \left(\frac{z}{u}\right) - \frac{b}{6}\sum_{i=1}^{6} U(i)\left(\frac{z}{u}\right)^i \otimes \left(\frac{z}{u}\right)^{7-i}.$$

Example 6.2. In case that A is a local $\mathbb{F}_p$-algebra. Let $\bar{b} \in \mathbb{F}_p$ be a primitive element of $\mathbb{F}_p$. Set $B = A[u]$ where u is a n-th root of b, and $n = p - 1$. Then an ideal $(p, b - \zeta)$ of $\mathbb{Z}[\zeta]$ is one of the prime ideals lying over p (cf. [9, Prop. 2.14.]). We consider the case that $(p, b - \zeta)$ is principal. Computation in MAGMA for $p \le 100$ shows that $(p, b - \zeta)$ is principal if p is one of the numbers

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

and a prime ideal lying over p is given as follows:

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

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

$$0 \to \boldsymbol{\mu}_{p,B} \xrightarrow{\iota} \mathbb{G}^m_{m,B} \xrightarrow{\theta} \mathbb{G}^m_{m,B} \to 0.$$

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

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

and we can compute the torsor for $G_{0,b}$.

In particular if $A = \mathbb{F}_p$ then $H^0(X, G_{0,b}) = 0$. Hence $H^1(X, G_{0,b}) = 0$ since

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

is an isomorphism.

7. Appendix : push-down and pull-back of torsors

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

7.1. Push-down of torsors

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

$$\begin{array}{ccccc} G & \curvearrowright & Y & \xrightarrow{\pi} & X \\ \downarrow{\scriptstyle\varphi} & & \downarrow{\scriptstyle\tilde{\varphi}} & & \| \\ G' & \curvearrowright & \varphi_* Y & \xrightarrow{\tilde{\pi}} & X, \end{array}$$

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 we can check that $\tilde{\pi}$ is well defined and the diagram is commutative, that is to say,

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

Moreover,

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

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

7.2. Pull-back of torsors

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

$$\begin{array}{ccccc} G & \curvearrowright & f^*Y & \xrightarrow{p_2} & X' \\ \| & & \downarrow{\scriptstyle p_1} & \square & \downarrow{\scriptstyle f} \\ G & \curvearrowright & Y & \xrightarrow{\pi} & X, \end{array}$$

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'.

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

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

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

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

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

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

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

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

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