Kummer Theory for Cyclotomic Twisted Tori

Yu KOIDE

Course of *Information Security Science*

Graduate School of Science and Engineering

Chuo University

March 2013

Acknowledgements

I would like to give my sincere gratitude to my supervisor, Professor Tsutomu Sekiguchi for his useful advices, discussions and his continuous warm encouragement. I could not complete my thesis without his support.

I would like to express my sincere thanks to Professors Jinhui Chao, Masato Kuwata, Kanetomo Sato and Toshiyuki Katsura for kindly accepting to be a member of the jury, for carefully reading a draft of this thesis and for giving useful comments on it. In particular, Professor Kanetomo Sato gave me useful advices for my presentations of the results of my study and opportunities for me to participate in his Seminar.

I would like to express my sincere thanks to Professor Noriyuki Suwa for his advices and his valuable support.

I would like to express my sincere thanks to Professor Shinji Miura for his advices and warm encouragement.

I would like to express my sincere thanks to Professors Yoshihiko Mitsumatsu and Tatsuru Takakura for their financial support.

I would like to express my thanks to Doctors Kazuyoshi Tsuchiya, Mitsuaki Yato, Yasuhiro Niitsuma, Michio Amano, Yuji Tsuno and Nobuhiro Aki for their kind advices. In particular, Doctor Kazuyoshi Tsuchiya often supported me and encouraged me sincerely, and Doctor Michio Amano read a draft of this thesis carefully and gave me warm encouragement.

I would like to thank all my colleagues and the staff of the department for providing me the excellent working atmosphere. Special thanks to Doctors Taro Suzuki, Noboru Ogawa, Tomohiro Horiuchi and Yohei Toda for stimulative discussions in the

graduate student room, and Doctor Heewon Park and Ms. Junko Kannauchi for their continuous and sincere encouragement.

Last but not least, I would like to give my gratitude to my family. I can not have led my excellent student life without their support and encouragement.

Contents

Notation

- A ring means a commutative ring with unity.
- n : a positive integer
- $m = \phi(n)$: the value of the Euler function ϕ
- G : a cyclic group of order n with a generator σ_0
- $\operatorname{Spec} B / \operatorname{Spec} A$: a G-torsor
- ζ : a primitive n-th root of unity
- R^* : the group of inverse elements in a ring R
- $\mathbb{G}_{m,R}$: the multiplicative group scheme over a ring R
- $\boldsymbol{\mu}_{n,R}$: the group scheme over a ring R of the n-th root of unity

Chapter 1

Introduction

The aim of this thesis is to determine the torsors for the finite group schemes $G_{a,b}$ of order p, which were classified by John Tate and Frans Oort. Roughly speaking, X is a torsor for $G_{a,b}$ if X is locally isomorphic to $G_{a,b}$ with respect to the flat topology on the base scheme of $G_{a,b}$.

The concept of torsors has its origin in Galois theory. The ideas of Galois theory have been developed by many mathematisians such as Newton, Lagrange, Galois, Kronecker, Artin and Grothendieck. In classical Galois theory, the fundamental result is the Galois correspondence between the intermidiate fields of a finite Galois extension K/k and the subgroups of its Galois group $\mathrm{Gal}(K/k)$. The Galois correspondence was developed to the one between the intermidiate separable extensions of k and the closed subgroups of $\mathrm{Gal}(k^{sep}/k)$ with the profinite topology. From the viewpoint of geometry, Galois theory gives the correspondece between the covering spaces of a topological manifold V and the foundamental groups of V. Galois theory for schemes classifies the finite étale coverings of a connected scheme X in terms of the fundamental group $\pi(X)$. Furthermore, this concept is generalized to the notion of torsors for group schemes.

The description of torsors can be regarded as the inverse problem of Galois theory for group schemes. The inverse Galois problem asks whether or not a finite group G occurs as a Galois group of some extensions K over k. The inverse Galois problem for schemes asks whether a group scheme G occurs as a torsor over a scheme X.

One of the excellent solutions to the inverse Galois problem is given by Kummer theory. Let X be a scheme and n a positive integer that is coprime to the characteristic of the residue field $k(x)$ for all $x \in X$. We denote by $\mathbb{G}_{m,X}$ the multiplicative group scheme over X. We have an exact sequence of abelian sheaves on $X_{\text{ét}}$

$$1 \longrightarrow \boldsymbol{\mu}_{n,X} \longrightarrow \mathbb{G}_{m,X} \xrightarrow{n} \mathbb{G}_{m,X} \longrightarrow 1,$$

where the morphism $n : \mathbb{G}_{m,X} \to \mathbb{G}_{m,X}$ is given by raising to the n-th power and $\boldsymbol{\mu}_{n,X}$ is its kernel of the morphism $n : \mathbb{G}_{m,X} \to \mathbb{G}_{m,X}$. This is called the Kummer sequence. If X is a scheme over a strictly local ring A such that $n \in A$ is invertible, then $\boldsymbol{\mu}_{n,X}$ is (noncanonically) isomorphic to the constant sheaf $\mathbb{Z}/n\mathbb{Z}$ on X. Hence the Kummer sequence yields the long exact sequence

$$\begin{array}{ccccccc} 0 & \longrightarrow & \Gamma(X, \mathbb{Z}/n\mathbb{Z}) & \longrightarrow & \Gamma(X, \mathbb{G}_{m,X}) & \xrightarrow{n} & \Gamma(X, \mathbb{G}_{m,X}) \\ & \longrightarrow & \mathrm{H}^1_{\text{ét}}(X, \mathbb{Z}/n\mathbb{Z}) & \longrightarrow & \mathrm{H}^1_{\text{ét}}(X, \mathbb{G}_{m,X}) & \xrightarrow{n} & \mathrm{H}^1_{\text{ét}}(X, \mathbb{G}_{m,X}) \\ & \longrightarrow & \mathrm{H}^2_{\text{ét}}(X, \mathbb{Z}/n\mathbb{Z}) & \longrightarrow & \cdots . & & \end{array}$$

Note that $\Gamma(X, \mathbb{G}_{m,X}) = \Gamma(X, \mathcal{O}_X^*)$ and $\mathrm{H}^1_{\text{ét}}(X, \mathbb{G}_{m,X}) = \mathrm{Pic}(X)$. Then we obtain an exact sequence

$$0 \longrightarrow \Gamma(X, \mathcal{O}_X^*)/\Gamma(X, \mathcal{O}_X^*)^n \longrightarrow \mathrm{H}^1_{\text{ét}}(X, \mathbb{Z}/n\mathbb{Z}) \longrightarrow \mathrm{Pic}(X)[n] \longrightarrow 0.$$

In particular, we consider the case that $X = \mathrm{Spec}k$, where k is a field containing a primitive n-th root ζ of unity. By Hilbert theorem 90, we get an isomorpism

$$k^*/(k^*)^n \cong \mathrm{H}^1_{\text{ét}}(X, \mathbb{Z}/n\mathbb{Z}),$$

which explicitly describes the cyclic extensions of degree n over k.

In this thesis, 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 $\mathrm{Spec}\, B/\,\mathrm{Spec}\, A$ 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 the representation matrix of the action of ζ on $\mathbb{Z}[\zeta]$ by the multiplication for the standard basis of a $\mathbb{Z}$-module $\mathbb{Z}^m$. Then we can define the canonical G-action on $B\,[x_1, \ldots, x_m, 1/\prod_{i=1}^m x_i]$ by $(x_1, \ldots, x_m)^{\sigma_0} := (x_1, \ldots, x_m)^I$ and on B by the Galois action. (See Definition 5 for details.) Galois descent theory for $\mathbb{G}^m_{m,B}$ yields a group scheme over A, which we call a cyclotomic twisted torus of degree n and denote it by $\mathbb{G}(n)_A$. Then the cyclotomic twisted torus can be written explicitly:

Assertion 1. *(Theorem 3.2.1.) There exist an ideal $\mathfrak{A}$ given explicitly and G-invariant parameters $\xi_1, \ldots, \xi_n$ such that*

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

A cyclotomic twisted torus is canonically isomorphic to the intersection of the kernel of norm maps. We denote by $\mathrm{Res}_{B/A}\mathbb{G}_{m,B}$ the Weil restriction of the group scheme $\mathbb{G}_{m,B}$ to A. For each positive integer ℓ dividing n, we define $B_\ell = B^{\left\langle \sigma_0^{n/\ell} \right\rangle} \subset B$ and denote by $\mathrm{Nm}_\ell : \mathrm{Res}_{B/A}\mathbb{G}_{m,B} \to \mathrm{Res}_{B_\ell/A}\mathbb{G}_{m,B_\ell}$ the norm map from B to B_ℓ. The group scheme $\mathcal{T}(n)_A := \cap_{\ell | n} \mathrm{Ker}(\mathrm{Nm}_\ell) \subset \mathrm{Res}_{B/A}\mathbb{G}_{m,B}$ is introduced to cryptologists by K. Rubin and A. Silverberg [13, 14]. They pointed out that this group scheme $\mathcal{T}(n)_A$ is a twisted torus. However, it is curious that any explicit expression of such twisted tori can not be found in literature. Our second assertion is that the group scheme $\mathcal{T}(n)_A$ is nothing but the cyclotomic twisted torus $\mathbb{G}(n)_A$.

Assertion 2. *(Theorem 3.4.1.) There exists the canonical isomorphism* $\mathbb{G}(n)_A \cong \mathcal{T}(n)_A$.

Note that the assertion above is relative to consequences by B. Mazur, K. Rubin and A. Silverberg [9].

We assume that n is greater than or equal to 2. Let $p \in \mathbb{Z}$ be a prime number with $n|(p-1)$. By $n|(p-1)$, p is completely decomposed in the number field $\mathbb{Q}(\zeta)/\mathbb{Q}$. We suppose that prime ideals $\mathfrak{p}$ lying above p are principal, namely, there exists $\theta \in \mathbb{Z}[\zeta]$ such that $\mathfrak{p} = (\theta)$ for each $\mathfrak{p} \subset \mathbb{Z}[\zeta]$. By $\mathbb{Z}[\zeta] \subset \mathrm{End}(\mathbb{G}_{m,B})$, we can regard θ as an endomorphism on $\mathbb{G}_{m,B}$. Hence we have

$$1 \longrightarrow \operatorname{Ker}\theta \longrightarrow \mathbb{G}_{m,B}^m \xrightarrow{\theta} \mathbb{G}_{m,B}^m \longrightarrow 1.$$

The Galois descent yields an exact sequence

$$1 \longrightarrow \overline{\operatorname{Ker}\theta} \longrightarrow \mathbb{G}(n)_A \xrightarrow{\theta} \mathbb{G}(n)_A \longrightarrow 1, \tag{1.1}$$

where $\overline{\operatorname{Ker}\theta}$ is the Galois descent of $\operatorname{Ker}\theta$ from B to A. Then we obtain a long exact sequence as cohomology groups

$$\begin{aligned} 1 \longrightarrow \mathrm{H}^0(X, \overline{\operatorname{Ker}\theta}) &\longrightarrow \mathrm{H}^0(X, \mathbb{G}(n)_A) \xrightarrow{\mathrm{H}^0(\theta)} \mathrm{H}^0(X, \mathbb{G}(n)_A) \\ \xrightarrow{\partial^0} \mathrm{H}^1(X, \overline{\operatorname{Ker}\theta}) &\longrightarrow \mathrm{H}^1(X, \mathbb{G}(n)_A) \xrightarrow{\mathrm{H}^1(\theta)} \mathrm{H}^1(X, \mathbb{G}(n)_A) \\ \xrightarrow{\partial^1} \cdots . \end{aligned}$$

From the long exact sequence above, T. Sekiguchi and Y. Toda [16] described torsors for $\overline{\operatorname{Ker}\theta}$ in terms of the first cohomology group $\mathrm{H}^1(\operatorname{Spec} A, \overline{\operatorname{Ker}\theta})$.

In particular, we consider the case of $n = p - 1$. Assume that there exists an n-th root $u \in B$ of $b \in A$. Let $B = A[u]$. Then T. Sekiguchi and Y. Toda pointed out that

$$(\boldsymbol{\mu}_{p,B})^G \cong G_{a,b},$$

where $G_{a,b}$ is a finite group scheme of order p classified by F. Oort and J. Tate [11]. Note that $\operatorname{Ker} \theta \cong \boldsymbol{\mu}_{p,B}$. We have a short exact sequence by the sequence (1.1):

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

which we call the Kummer sequence for cyclotomic twisted tori. Then using the exact sequence above, T. Sekiguchi and Y. Toda described torsors for $G_{a,b}$ in the paper [16]. We call their consequence Kummer theory for cyclotomic twisted tori in the principal case.

In this thesis, we consider torsors for the finite group scheme $G_{a,b}$ of order p. We need not assume that the prime ideal $\mathfrak{p}$ is principal. We consider homomorphisms defined by ideals of the endomorphism ring on $G(n)_A$. T. Sekiguchi and Y. Toda proved that $\mathbb{Z}[\zeta] \cong \operatorname{End}(\mathbb{G}(n)_A)$ in [16]. Let $\mathfrak{a} \subset \mathbb{Z}[\zeta]$ be a non-zero ideal. There exists $\xi, \eta \in \mathbb{Z}[\zeta]$ such that $\mathfrak{a} = (\xi, \eta)$. We define a homomorphism $\psi_{\mathfrak{a}}$ from $\mathbb{G}(n)_A$ to $\mathbb{G}(n)_A \times \mathbb{G}(n)_A$ by the ideal $\mathfrak{a} \subset \mathbb{Z}[\zeta]$. We denote by $\mathbb{G}(n)_A[\mathfrak{a}]$ the kernel of the homomorphism $\psi_{\mathfrak{a}}$. Then we have the assertion of the order of $\mathbb{G}(n)_A[\mathfrak{a}]$:

Assertion 3. *(Theorem 5.1.1) For each unramified ideal $\mathfrak{a} \subset \mathbb{Z}[\zeta]$, we have*

$$|\mathbb{G}(n)_A[\mathfrak{a}]| = \operatorname{Nm}_{\mathbb{Q}[\zeta]/\mathbb{Q}} \mathfrak{a}.$$

Note that $\mathbb{G}(n)_A[\mathfrak{a}]$ is independent of the choice of the generators of the ideal $\mathfrak{a}$ (see Lemma 11). We provide the following exact sequence, which plays a key role to describe torsors. Here, let θ' be an element of $\mathbb{Z}[\zeta]$ such that $\mathfrak{p} = (p, \theta')$.

Assertion 4. *(cf. Theorem 5.2.1) For $\mathfrak{p} = (p, \theta')$, there exists a homomorphism ψ such that the following sequence is exact as sheaves of groups on $(\operatorname{Spec} B)_{flat}$:*

$$1 \longrightarrow \operatorname{Ker} \psi_{\mathfrak{p}} \longrightarrow \mathbb{G}_{m,B}^m \xrightarrow{\psi_{\mathfrak{p}}} \mathbb{G}_{m,B}^m \times \mathbb{G}_{m,B}^m \xrightarrow{\psi} \mathbb{G}_{m,B}^m \times \mathbb{G}_{m,B}^m.$$

Therefore we obtain the exact sequence

$$1 \to \operatorname{Ker} \psi_{\mathfrak{p}} \to \mathbb{G}_{m,B}^m \xrightarrow{\psi_{\mathfrak{p}}} \operatorname{Ker} \psi \to 1.$$

We will give the defining equations of $\operatorname{Ker} \psi$ (see Appendix A.2). Here, we denote by $\overline{\operatorname{Ker} \psi_{\mathfrak{p}}}$ and $\overline{\operatorname{Ker} \psi}$ the Galois descent of $\operatorname{Ker} \psi_{\mathfrak{p}}$ and $\operatorname{Ker} \psi$ respectively. The Galois descent yields the exact sequence

$$1 \to \overline{\operatorname{Ker} \psi_{\mathfrak{p}}} \to \mathbb{G}(n)_A \xrightarrow{\psi_{\mathfrak{p}}} \overline{\operatorname{Ker} \psi} \to 1.$$

Then we describe torsors for $\overline{\operatorname{Ker} \psi_{\mathfrak{p}}}$ by computing the first cohomology group $\mathrm{H}^1(\operatorname{Spec} A, \operatorname{Ker} \psi_{\mathfrak{p}})$. In particular, when $n = p - 1$, we have

$$\overline{\operatorname{Ker} \psi_{\mathfrak{p}}} = (\boldsymbol{\mu}_{p,B})^G = G_{a,b}.$$

Then we get the exact sequence

$$1 \to G_{a,b} \to \mathbb{G}(n)_A \to \overline{\operatorname{Ker} \psi} \to 1,$$

which we call the Kummer sequence for cyclotomic twisted tori in the general case. Thus we obtain the description of $G_{a,b}$-torsors in the non-principal case. We call the consequence above Kummer theory for cyclotomic twisted tori in the general case.

This thesis consists of five chapters.

In Chapter 2, we give a short review of the Galois descent for affine group schemes and the Weil restriction.

In Chapter 3, we define the cyclotomic twisted torus. We give its coordinate ring explicitly and some examples. Finally we prove the second assertion, namely, we give the canonical isomorphism between $\mathbb{G}(n)_A$ and $\mathcal{T}(n)_A$.

In Chapter 4, we briefly review the description of $G_{a,b}$-torsors by T. Sekiguchi and Y. Toda [16].

In Chapter 5, we show Assertion 3, which is the claim of the order of the kernel of a homomorphism defined by an ideal of $\mathbb{Z}[\zeta] \cong \operatorname{End} \mathbb{G}(n)_A$. Then we prove Assertion 4 and we compute $G_{a,b}$-torsors explicitly using Assertion 4.

As Appendix A.1, we give an elementary proof of a result on a cyclotomic polynomial, which is crucial in our proof of the second assertion. Let $n = p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r}$ be the factorization of n into prime numbers. For each p_i, we set $F_i(X) = (X^n - 1)/(X^{n/p_i} - 1)$. Then the greatest common divisor of F_i's is obviously the cyclotomic polynomial $\Phi_n(X)$:

Assertion 5. *(Lemma 10, Proposition 15.) There exist polynomials $A_i(X) \in \mathbb{Z}[X]$ for $i = 1, \ldots, r$ such that $\Phi_n(X) = \sum_{i=1}^{r} A_i(X) F_i(X)$.*

Note that this fact is already given by N. G. de Bruijn [3] in a completely different way. At the end of this thesis, we describe the defining equations of the subgroup scheme $\operatorname{Ker} \psi$ of $\mathbb{G}_{m,B}^m \times \mathbb{G}_{m,B}^m$.

Finally, we add a few comments. L. G. Roberts [12] considers $G_{a,b}$-torsors in the case where the base ring of $G_{a,b}$ is the ring of integers of a local number field. And

F. Andreatta and C. Gasbarri [2] describe $G_{a,b}$-torsors in the case where the base ring of the finite group scheme $G_{a,b}$ is a complete discrete valuation ring of the residue characteristic p, and b admits a $(p-1)$-th root in $\mathbb{F}_p$.

Chapter 2

Preliminaries

In this chapter, we recall the Galois descent for affine group schemes and the Weil restriction. We give the Galois descent theory in the case of affine group schemes. Next we define the Weil restriction. We consider the one of an affine group scheme and give some examples. For details of the faithfully flat descent and the Galois descent, one can refer to U. Görtz and T. Wedhorn [6] and W. C. Waterhouse [21]. For details of the Weil restriction, one can refer to A. Weil [22], M. Demazur and P. Gabriel [5] and W. C. Waterhouse [21].

2.1 Galois descent

Let G be a finite group of order n. We let $\mathrm{Spec}B/\mathrm{Spec}A$ be a G-torsor. We denote the G-action on B by $x \mapsto x^\sigma$ for any $x \in B$ and any $\sigma \in G$. Then we know that B is a faithfully flat A-algebra and B has a G-action over A such that $\varphi : B \otimes_A B \overset{\simeq}{\to} B \otimes_A \prod_G A$; $b_1 \otimes b_2 \mapsto \sum_\sigma b_1 b_2^\sigma \otimes e_\sigma$, where e_σ is the element of $\prod_G A$ whose entries are zero except 1 at σ.

Furthermore we suppose that B is a free A-module. Note that if A is a principal ideal normal domain, then B is automatically a free A-module (see [4], Chap. 5, § 1, n$^{\mathrm{o}}$ 7, Cor. 2 to Prop. 18). Let $\{\omega_1, \dots, \omega_n\}$ be a free basis of A-module B. Then $\varphi(1 \otimes \omega_i) = (\omega_i^\sigma)_{\sigma \in G}$. Therefore $\Delta = \Delta(\omega_1, \dots, \omega_n) := \det(\omega_i^\sigma)_{i,\sigma}$ is an invertible element of B. Note that $B \supset B^G := \{x \in B \mid x^\sigma = x \quad \forall \sigma \in G\} = A$. Let C and C' be B-algebras. For any element $\sigma \in G$ and any morphism $\varphi : \operatorname{Spec} C \to \operatorname{Spec} C'$ over B, we denote by

$$\varphi^\sigma : \left\{\operatorname{Spec} C \xrightarrow{\varphi} \operatorname{Spec} C'\right\} \times_{\operatorname{Spec} B} \left\{\operatorname{Spec} B \xrightarrow{\operatorname{Spec} \sigma} \operatorname{Spec} B\right\}$$

the morphism induced from φ by taking the base change $\operatorname{Spec} B \xrightarrow{\operatorname{Spec} \sigma} \operatorname{Spec} B$.

Now let $\mathcal{G} = \operatorname{Spec} C$ be an affine group scheme over B. We assume that for any element $\sigma \in G$, $\rho_\sigma : \mathcal{G} \to \mathcal{G}^\sigma$ is a B-isomorphism of B-group schemes. If these isomorphisms satisfy the condition

$$\rho_\tau^\sigma \circ \rho_\sigma = \rho_{\sigma\tau} \quad \forall \sigma, \tau \in G,$$

then there exists uniquely, up to isomorphism, a group scheme $\mathcal{G}_0$ over A such that $\mathcal{G}_0 \times_{\operatorname{Spec} A} \operatorname{Spec} B \cong \mathcal{G}$. This group scheme $\mathcal{G}_0$ is called the Galois descent of $\mathcal{G}$ by G.

In fact, $\mathcal{G}_0$ is given as follows: For any $\sigma \in G$, we denote the composition $C \to C \otimes_B (\sigma, B) \xrightarrow{(\rho_\sigma)^*} C$ again by $(\rho_\sigma)^* : C \to C$. Then this gives a G-action on C, and the G-invariant subring $C^G \subset C$ yields the Galois descent $\mathcal{G}_0 = \operatorname{Spec} C^G$ of $\mathcal{G}$. In the sequel, abusing the terminology, we denote $(\rho_\sigma)^*$ simply by σ. For an A-algebra C, we also denote the automorphism $\mathrm{id}_C \otimes \sigma$ of $C \otimes_A B$ simply by σ.

2.2 Weil restriction

We recall the Weil restriction. An useful tool of "realification" of a complex linear space is generalized to an operation in the theory of schemes, calling the Weil restriction.

Let S be a scheme and S_{fl} be the flat site $((\mathrm{Sch}\,/S), \mathrm{cov}(\mathrm{Sch}\,/S)_{fppf})$. Moreover, we let X be an S-scheme. For each S-scheme U, we define $\mathcal{F}(U)$ by

$$\mathcal{F}(U) = X(U) = \mathrm{Hom}_S(U, X).$$

Then $\mathcal{F}$ is a sheaf on S_{fl}, and it is called representable by X.

Let $f : S \to T$ be a morphism of schemes and $\mathcal{F}$ a presheaf on S_{fl}. Then we define a presheaf $f_*\mathcal{F}$ on T_{fl} by

$$(f_*\mathcal{F})(V) = \mathcal{F}(f^{-1}(V)) \qquad \text{for each } T\text{-scheme } V.$$

Here, the presheaf $f_*\mathcal{F}$ has the restriction maps, which is induced by them for $\mathcal{F}$. We call $f_*\mathcal{F}$ the direct image of $\mathcal{F}$ under f. Then we immediately check that if $\mathcal{F}$ is a sheaf on S, the direct image $f_*\mathcal{F}$ is a sheaf on T.

Proposition 1. *Let K and k be rings and $f : \mathrm{Spec}\, K \to \mathrm{Spec}\, k$ a morphism of affine schemes. Let X be a K-scheme and $\mathcal{F}$ the sheaf on $(\mathrm{Spec}\, K)_{fl}$ represented by X. Suppose that the k-module K is projective and finitely generated. Then we have*

(1) if X is an affine K-scheme, then the sheaf $f_*\mathcal{F}$ on $\mathrm{Spec}\, k$ is represented by an affine k-scheme.

(2) if X a K-scheme and for each finite subset P of X, there exists an affine open subscheme U of X such that $P \subset U$, then the sheaf $f_*\mathcal{F}$ on $\mathrm{Spec}\, k$ is represented by a k-scheme.

We denote by $\operatorname{Res}_{K/k} X$ the scheme representing $f_*\mathcal{F}$. We call it the Weil restriction of X to k. Then, by the definition we have

$$\left(\operatorname{Res}_{K/k} X\right)(L) = X(L \times_k K)$$

for each k-algebra L.

Example 2. *Let $k_1, k_2, \ldots, k_d$ be d copies of k. We set $K = k_1 \times k_2 \times \cdots \times k_d$. For each $i = 1, 2, \ldots, d$, we assign k_i the K-algebra structure induced by the i-th canonical projection $p_i : K = k^d \to k$. Let $u_i : \operatorname{Spec} k \to \operatorname{Spec} K$ be the immersion corresponding to p_i and we set $X_i = X \times_{\operatorname{Spec} K} (\operatorname{Spec} k, u_i)$. Then we have the isomorphism $\operatorname{Res}_{K/k} X \cong \prod_{i=1}^{d} X_i$.*

Example 3. *Let K be a finite extension field over k of degree n and a group scheme $X = \operatorname{Spec} R$ over $\operatorname{Spec} K$ of finite type. We give the defining equations of $\operatorname{Res}_{K/k} X$. There are $\alpha_1, \alpha_2, \ldots, \alpha_n \in K$ such that*

$$K = k\alpha_1 \oplus k\alpha_2 \oplus \cdots \oplus k\alpha_n.$$

Since $X = \operatorname{Spec} R$ is of finite type over K, there exists an ideal $(F_1, F_2, \ldots, F_r) \subset K[T_1, T_2, \ldots, T_d]$ such that

$$R = K[T_1, T_2, \ldots, T_d]/(F_1, F_2, \ldots, F_r).$$

For any k-algebra L, we have the equalities

$$\begin{aligned}\left(\operatorname{Res}_{K/k} X\right)(L) &= X(L \otimes_k K)\\ &= \operatorname{Hom}_K(R, L \otimes_k K)\\ &= \operatorname{Hom}_K(K[T_1, T_2, \ldots, T_d]/(F_1, F_2, \ldots, F_r), L \otimes_k K)\\ &= \{\psi : K[T_1, T_2, \ldots, T_d] \to L \otimes_k K : K\text{-}\mathit{alg.\ homo.} \mid\\ &\qquad\qquad \psi(F_i(T_1, T_2, \ldots, T_d)) = 0 \ \ \mathit{for}\ i = 1, 2, \ldots, r\}\\ &= \{(t_1, t_2, \ldots, t_d) \in (L \otimes_k K)^d \mid F_i(t_1, t_2, \ldots, t_d) = 0\\ &\qquad\qquad\qquad\qquad \mathit{for\ any}\ i = 1, 2, \ldots, r\},\end{aligned}$$

where we set $t_i = \psi(T_i)$ for each $i = 1, 2, \ldots, d$. Note that $L \otimes_k K = \bigoplus_{i=1}^n L \otimes_k k\alpha_i$. We set

$$\begin{aligned}t_1 &= t_{11} \otimes \alpha_1 + t_{12} \otimes \alpha_2 + \cdots + t_{1n} \otimes \alpha_n\\ t_2 &= t_{21} \otimes \alpha_1 + t_{22} \otimes \alpha_2 + \cdots + t_{2n} \otimes \alpha_n\\ &\vdots\\ t_d &= t_{d1} \otimes \alpha_1 + t_{d2} \otimes \alpha_2 + \cdots + t_{dn} \otimes \alpha_n,\end{aligned}$$

where $t_{ij} \in L$ for all $i = 1, 2, \ldots, d$ and $j = 1, 2, \ldots, n$. For $i = 1, 2, \ldots, r$ we define

$$f_{ij}(\boldsymbol{t}) \in k[t_{11}, t_{12}, \ldots, t_{1n}, t_{21}, t_{22}, \ldots, t_{2n}, \ldots, t_{d1}, t_{d2}, \ldots, t_{dn}]$$

by

$$F_i(t_1, t_2, \ldots, t_d) = f_{i1}(\boldsymbol{t}) \otimes \alpha_1 + f_{i2}(\boldsymbol{t}) \otimes \alpha_2 + \cdots + f_{in}(\boldsymbol{t}) \otimes \alpha_n.$$

Then we have the equalities

$$\begin{aligned}\left(\operatorname{Res}_{K/k} X\right)(L) &= \{\boldsymbol{t} = (t_{ij})_{i,j} \in L^{dn} \mid f_{ij}(\boldsymbol{t}) = 0 \\ &\qquad\qquad \textit{for } i = 1,2,\ldots,r \textit{ and } j = 1,2,\ldots,n\} \\ &= \operatorname{Hom}_{k-algebra}(k[\boldsymbol{x}]/(f_{ij}(\boldsymbol{x}), L) \\ &= \operatorname{Spec}(k[\boldsymbol{x}]/(f_{ij}(\boldsymbol{x}))(L).\end{aligned}$$

Therefore we obtain the following defining equations of $\operatorname{Res}_{K/k} X$*:*

$$\begin{aligned}0 &= f_{11}(x_{11}, x_{12}, \ldots, x_{1n}, x_{21}, x_{22}, \ldots, x_{2n}, x_{d1}, x_{d2}, \ldots, x_{dn}) \\ 0 &= f_{21}(x_{11}, x_{12}, \ldots, x_{1n}, x_{21}, x_{22}, \ldots, x_{2n}, x_{d1}, x_{d2}, \ldots, x_{dn}) \\ &\vdots \\ 0 &= f_{r1}(x_{11}, x_{12}, \ldots, x_{1n}, x_{21}, x_{22}, \ldots, x_{2n}, x_{d1}, x_{d2}, \ldots, x_{dn}) \\ 0 &= f_{12}(x_{11}, x_{12}, \ldots, x_{1n}, x_{21}, x_{22}, \ldots, x_{2n}, x_{d1}, x_{d2}, \ldots, x_{dn}) \\ 0 &= f_{22}(x_{11}, x_{12}, \ldots, x_{1n}, x_{21}, x_{22}, \ldots, x_{2n}, x_{d1}, x_{d2}, \ldots, x_{dn}) \\ &\vdots \\ 0 &= f_{r2}(x_{11}, x_{12}, \ldots, x_{1n}, x_{21}, x_{22}, \ldots, x_{2n}, x_{d1}, x_{d2}, \ldots, x_{dn}) \\ &\vdots \\ 0 &= f_{1n}(x_{11}, x_{12}, \ldots, x_{1n}, x_{21}, x_{22}, \ldots, x_{2n}, x_{d1}, x_{d2}, \ldots, x_{dn}) \\ 0 &= f_{2n}(x_{11}, x_{12}, \ldots, x_{1n}, x_{21}, x_{22}, \ldots, x_{2n}, x_{d1}, x_{d2}, \ldots, x_{dn}) \\ &\vdots \\ 0 &= f_{rn}(x_{11}, x_{12}, \ldots, x_{1n}, x_{21}, x_{22}, \ldots, x_{2n}, x_{d1}, x_{d2}, \ldots, x_{dn}).\end{aligned}$$

Example 4. *We have the isomorphism*

$$\operatorname{Res}_{\mathbb{C}/\mathbb{R}} \mathbb{P}^1_{\mathbb{C}} \cong \operatorname{Proj} \mathbb{R}[x, y, z, w]/(x^2 + y^2 + z^2 - w^2).$$

Chapter 3

Cyclotomic twisted tori

We introduce a concept of cyclotomic twisted tori along [8]. It is a main object of this thesis. We describe the coordinate ring of a cyclotomic twisted torus of degree n. Furthermore, we prove that the cyclotomic twisted torus is canonically isomorphic to an intersection of all kernels of norm maps between the Weil restrictions of the algebraic torus (cf. B. Mazur, K. Rubin and A. Silverberg [9] Remark 5.11).

3.1 Cyclotomic twisted tori

We give the definition of cyclotomic twisted tori of degree n. Let $\Phi_n(x) = x^m + a_1x^{m-1} + \cdots + a_m$ be the cyclotomic polynomial, namely,

$$\Phi_n(x) = \prod_{\bar{k} \in (\mathbb{Z}/n\mathbb{Z})^*} (x - \zeta^k).$$

It is well-known that the coefficients of $\Phi_n(x)$ are rational integers. In particular, we can easily see that $a_m = 1$. We take $\{1, \zeta, \zeta^2, \ldots, \zeta^{m-1}\}$ as a $\mathbb{Z}$-basis of $\mathbb{Z}[\zeta]$. Now we consider the representation of ζ with respect to the standard $\mathbb{Z}$-basis of a $\mathbb{Z}$-module

$\mathbb{Z}^m$:

$$\begin{aligned}
&(1,\zeta,\zeta^2,\ldots,\zeta^{m-1})\zeta \\
&\qquad = (\zeta,\zeta^2,\ldots,\zeta^{m-1}, -a_m - a_{m-1}\zeta - \cdots - a_1\zeta^{m-1}) \\
&\qquad = (1,\zeta,\zeta^2,\ldots,\zeta^{m-1}) \begin{pmatrix} 0 & 0 & \cdots & 0 & -a_m \\ 1 & 0 & \cdots & 0 & -a_{m-1} \\ 0 & 1 & \cdots & 0 & -a_{m-2} \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & -a_1 \end{pmatrix}
\end{aligned}$$

and

$$\begin{aligned}
&(1,\zeta,\zeta^2,\ldots,\zeta^{m-1})\zeta^{-1} \\
&\qquad = (-a_{m-1} - a_{m-2}\zeta - \cdots - a_1\zeta^{m-2} - \zeta^{m-1}, 1, \ldots, \zeta^{m-2}) \\
&\qquad = (1,\zeta,\zeta^2,\ldots,\zeta^{m-1}) \begin{pmatrix} -a_{m-1} & 1 & 0 & \cdots & 0 \\ -a_{m-2} & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ -a_1 & 0 & 0 & \cdots & 1 \\ -1 & 0 & 0 & \cdots & 0 \end{pmatrix}.
\end{aligned}$$

Therefore ζ and ζ^{-1} are represented by the matrices

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

and

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

respectively.

In general, for $k, \ell \in \mathbb{Z}$, any vector $\boldsymbol{x} = (x_1, x_2, \ldots, x_k)$ and any matrix $M = (m_{ij}) \in \mathrm{M}_{k,\ell}(\mathbb{Z})$, we define the vector $\boldsymbol{x}^M$ obtained by raising to the power of the matrix M by

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

Now we consider the algebraic torus

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

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

$$\sigma_0 : \begin{cases} B[x_1, x_2, \ldots, x_m, 1/\prod_{i=1}^m x_i] & \xrightarrow{\sigma_0} B[x_1, x_2, \ldots, x_m, 1/\prod_{i=1}^m x_i]; \\ x = (x_1, x_2, \ldots, x_m) & \longmapsto x^{\sigma_0} = (x_1^{\sigma}, \ldots, x_m^{\sigma}) := x^I \\ b \in B & \longmapsto b^{\sigma_0}. \end{cases}$$

Definition 5. *The Galois descent of $\mathbb{G}_{m,B}^m$ by G is called a cyclotomic twisted torus of degree n and denoted by $\mathbb{G}(n)_A$:*

$$\mathbb{G}(n)_A := \mathbb{G}_{m,B}^m / G = \operatorname{Spec} B \left[x_1, x_2, \ldots, x_m, \frac{1}{\prod_{i=1}^m x_i} \right]^G.$$

3.2 The coordinate ring of a cyclotomic twisted torus

We suppose that B is free over A of rank n. Let $B = A\cdot\omega_1 + \cdots + A\cdot\omega_n$ and $\mathbb{G}(n)_A = \operatorname{Spec} B\left[x_1, x_2, \ldots, x_m, \frac{1}{\prod_{i=1}^m x_i}\right]^G$ be the cyclotomic twisted torus as Section 3.1.

Now we define the elements $\xi_i \in B[x_1, x_2, \ldots, x_m, 1/\prod_{i=1}^m x_i]$ for $i = 1, \ldots, n$ by

$$\xi_i := \sum_{\sigma\in G} \omega_i^\sigma x_1^\sigma.$$

Then since $\Delta = \Delta(\omega_1, \ldots, \omega_n) = \det(\omega_i^\sigma)_{i,\sigma}$ is invertible in B, the linear equations above can be solved in x_1^σ's over B:

$$x_1^{\sigma_0^i} = f_{i+1}(\xi_1, \ldots, \xi_n) \in \sum_{j=1}^n B\xi_j \quad \text{for} \quad i = 0, \ldots, n-1.$$

For each $i = 1, \ldots, n-m$, we set $x_1^{\sigma_0^{m+i-1}} = x_1^{A_{1i}} x_2^{A_{2i}} \cdots x_m^{A_{mi}}$. Note that $A_{11} = -a_m, A_{21} = -a_{m-1}, \ldots, A_{m1} = -1$ and $A_{ij} \in \mathbb{Z}$.

Now we prepare more notation. For any integer a, we set $a' := \dfrac{1}{2}(|a| - a)$ and $a'' := \dfrac{1}{2}(|a| + a)$. Then we define some equations in $B[\xi_1, \ldots, \xi_n]$:

$$F_i(\xi_1, \ldots, \xi_n) := f_{m+i} f_1^{A'_{1i}} f_2^{A'_{2i}} \cdots f_m^{A'_{mi}} - f_1^{A''_{1i}} f_2^{A''_{2i}} \cdots f_m^{A''_{mi}}$$

for $i = 1, \ldots, n-m$.

For each polynomial $F \in B[\xi_1, \ldots, \xi_n]$, we denote the isotropic subgroup at F by $G_F := \{\sigma \in G \mid F^\sigma = F\} \subset G$. Under these notation, we have the theorem:

Theorem 3.2.1. *The coordinate ring of the cyclotomic twisted torus $\mathbb{G}(n)_A$ is described as*

$$B\left[x_1, x_2, \ldots, x_m, \frac{1}{\prod_{i=1}^m x_i}\right]^G = A[\xi_1, \ldots, \xi_n]/\mathfrak{A},$$

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

$$\tilde{F}_{ki} := \sum_{\overline{\sigma} \in G/G_{\omega_k F_i}} (\omega_k F_i)^\sigma$$

for $k = 1, \ldots, n$ *and* $i = 0, \ldots, n-m-1$.

Proof. First, we check the equality

$$B\left[x_1, x_1^{\sigma_0}, \ldots, x_1^{\sigma_0^{n-1}}\right] = B[x_1, \ldots, x_m, 1/(x_1 \cdots x_m)].$$

Since $B\left[x_1, x_1^{\sigma_0}, \ldots, x_1^{\sigma_0^{n-1}}\right]$ is G-stable, we have only to check that $1/x_1$ belong to it. Note that $\mathrm{End}(\mathbb{G}_{m,B}^m) \cong \mathrm{M}_m(\mathbb{Z})$, and the correspondence $\mathbb{Z}[\zeta] \to \mathrm{M}_m(\mathbb{Z})$ defined by $\sum_{k=0}^{n-1} c_k \zeta^k \mapsto \sum_{k=0}^{n-1} c_k I^k$ is an injective ring homomorphism. Since $\sum_{k=0}^{n-1} \zeta^k = 0$, we have $\sum_{k=0}^{n-1} I^k = O \in \mathrm{M}_m(\mathbb{Z})$ and $\sum_{k=0}^{n-1} \sigma_0^k = 0 \in \mathrm{End}(\mathbb{G}_{m,B}^m)$. Then we have the equality $x_1^{\sigma_0} x_1^{\sigma_0^2} \cdots x_1^{\sigma_0^{n-1}} = x_1^{-1}$. Hence we have the equalities

$$B\left[x_1, x_1^{\sigma_0}, \ldots, x_1^{\sigma_0^{n-1}}\right] = B[x_1, \ldots, x_m, 1/(x_1 \cdots x_m)] = B[\xi_1, \ldots, \xi_n].$$

In the ring $B[x_1, x_2, \ldots, x_m, 1/\prod_{i=1}^m x_i]$, the ideals $(F_0, \ldots, F_{n-m-1})$ and $(\{\tilde{F}_{ki} \mid k = 1, \ldots, n;\ i = 0, \ldots, n-m-1\})$ are equal to each other. We denote by $\mathfrak{A}$ these ideals. Therefore we see that

$$B\left[x_1, x_2, \ldots, x_m, \frac{1}{\prod_{i=1}^m x_i}\right] \cong B[\xi_1, \ldots, \xi_n]/(\mathfrak{A} B[\xi_1, \ldots, \xi_n])$$

and

$$(A[\xi_1, \ldots, \xi_n]/\mathfrak{A}) \otimes_A B \cong B\left[x_1, x_2, \ldots, x_m, \frac{1}{\prod_{i=1}^m x_i}\right].$$

Note that we recognize ξ_i's as variables. Since B is faithfully flat over A and $(A[\xi_1, \ldots, \xi_n]/\mathfrak{A}) \otimes_A B \cong B[x_1, x_2, \ldots, x_m, 1/\prod_{i=1}^m x_i]$ is flat over B, we know that $A[\xi_1, \ldots, \xi_n]/\mathfrak{A}$ is flat over A. Hence from the exact sequence

$$0 \to A = \mathrm{Ker}(\sigma_0 - \mathrm{id}) \to B \xrightarrow{\sigma_0 - \mathrm{id}} \mathrm{Im}(\sigma_0 - \mathrm{id}) \to 0,$$

we have the exact sequence

$$0 \to (A[\xi]/\mathfrak{A}) \otimes_A A \to (A[\xi]/\mathfrak{A}) \otimes_A B$$
$$\xrightarrow{\mathrm{id}\otimes(\sigma_0-\mathrm{id})} (A[\xi]/\mathfrak{A}) \otimes_A \mathrm{Im}(\sigma_0 - \mathrm{id}) \to 0,$$

where $\xi = (\xi_1, \ldots, \xi_n)$. Note that $\mathrm{Im}(\sigma_0 - \mathrm{id}) \subset B$ and $(A[\xi]/\mathfrak{A}) \otimes_A \mathrm{Im}(\sigma_0 - \mathrm{id}) \subset (A[\xi]/\mathfrak{A}) \otimes_A B$. This implies that

$$B\left[x_1, x_2, \ldots, x_m, \frac{1}{\prod_{i=1}^m x_i}\right]^G = A[\xi_1, \ldots, \xi_n]/\mathfrak{A}.$$

□

3.3 Example

In this section, we provide some examples of cyclotomic twisted tori.

Example 6. *Suppose that $n = p^e$ is a power of a prime number p. Then $m = \phi(n) = p^{e-1}(p-1)$,*

$$\Phi_n(X) = \Phi_p(X^{p^{e-1}}) = X^m + X^{m-p^{e-1}} + \cdots + X^{p^{e-1}} + 1,$$

and

$$a_k = \begin{cases} 1 & \textit{if} \quad k = ip^{e-1} \\ 0 & \textit{otherwise,} \end{cases}$$

where $k = 1, \ldots, m$ and $i = 1, \ldots, p-1$. Hence we have $x_1^{\sigma_0^m} = x_1^{-1}x_{(p-2)p^{e-1}+1}^{-1} \cdots x_{p^{e-1}+1}^{-1}$ and

$$B[x_1, \ldots, x_m, 1/(x_1 \cdots x_m)]^G = A[\xi_1. \ldots, \xi_n]/\mathfrak{A},$$

where

$$\mathfrak{A} = (\{\tilde{F}_{ki} \mid k = 1, \ldots, n;\ i = 1, \ldots, n-m-1\}).$$

Example 7. *Let $B = \mathbb{F}_{7^6}$, $A = \mathbb{F}_7$ and $n = 6$. Then $m = \phi(n) = 2$ and $\Phi_6(X) = X^2 - X + 1$. Note that $\mathbb{F}_{7^6} = \mathbb{F}_7[X]/(X^6 - 3)$ and we set $\alpha = \overline{X} \in \mathbb{F}_{7^6}$. Then $\mathbb{F}_{7^6} = \mathbb{F}_7 \cdot 1 + \mathbb{F}_7 \cdot \alpha + \cdots + \mathbb{F}_7 \cdot \alpha^5$. Let $\sigma_0(x) = x^7$ for any $x \in \mathbb{F}_{7^6}$. In this case, we obtain*

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

and $x_1^{\sigma_0} = x_2$, $x_2^{\sigma_0} = x_1^{-1}x_2$. Therefore we have $x_1^{\sigma_0^3} = x_1^{-1}$ and

$$\mathbb{F}_{7^6}[x_1, x_2, 1/(x_1x_2)]^G = \mathbb{F}_7[\xi_1, \ldots, \xi_6]/\mathfrak{A}.$$

Here

$$\begin{aligned}
\xi_1 &= x_1 + x_2 + x_1^{-1}x_2 + x_1^{-1} + x_2^{-1} + x_1x_2^{-1} \\
\xi_2 &= \alpha x_1 + 3\alpha x_2 + 2\alpha x_1^{-1}y - \alpha x_1^{-1} - 3\alpha y^{-1} - 2\alpha x_1x_2^{-1} \\
\xi_3 &= \alpha^2 x_1 + 2\alpha^2 x_2 - 3\alpha^2 x_1^{-1}x_2 - \alpha^2 x_1^{-1} + 2\alpha^2 x_2^{-1} - 3\alpha 2x_1x_2^{-1} \\
\xi_4 &= \alpha^3 x_1 - \alpha^3 x_2 + \alpha^3 x_1^{-1}x_2 - \alpha^3 x_1^{-1} + \alpha^3 x_2^{-1} - \alpha^3 x_1x_2^{-1} \\
\xi_5 &= \alpha^4 x_1 - 3\alpha 4x_2 + 2\alpha 4x_1^{-1}x_2 - \alpha^4 x_1^{-1} - 3\alpha^3 x_2^{-1} - 2\alpha^4 x_1x_2^{-1} \\
\xi_6 &= \alpha^5 x_1 - 2\alpha^5 x_2 - 3\alpha^5 x_1^{-1}x_2 - \alpha^5 x_1^{-1} + 3\alpha^5 x_2^{-1} + x_1x_2^{-1},
\end{aligned}$$

$$\begin{aligned}
x_1 = f_1 &= -\xi_1 + 2\alpha^5\xi_2 + 2\alpha^4\xi_3 + 2\alpha^3\xi_4 + 2\alpha^2\xi_5 + 2\alpha\xi_6 \\
x_1^{\sigma_0} = f_2 &= -\xi_1 + 3\alpha^5\xi_2 + \alpha^4\xi_3 - 2\alpha^3\xi_4 - 3\alpha^2\xi_5 - \alpha\xi_6 \\
x_1^{\sigma_0^2} = f_3 &= -\xi_1 + \alpha^5\xi_2 - 3\alpha^4\xi_3 + 2\alpha^3\xi_4 + \alpha^2\xi_5 - 3\alpha\xi_6 \\
x_1^{\sigma_0^3} = f_4 &= -\xi_1 - 2\alpha^5\xi_2 + 2\alpha^4\xi_3 - 2\alpha^3\xi_4 + 2\alpha^2\xi_5 - 2\alpha\xi_6 \\
x_1^{\sigma_0^4} = f_5 &= -\xi_1 - 3\alpha^5\xi_2 + \alpha^4\xi_3 + 2\alpha^3\xi_4 - 3\alpha^2\xi_5 + \alpha\xi_6 \\
x_1^{\sigma_0^5} = f_6 &= -\xi_1 - \alpha^5\xi_2 - 3\alpha^4\xi_3 - 2\alpha^3\xi_4 + \alpha^2\xi_5 + 3\alpha\xi_6
\end{aligned}$$

and

$$F_1 = f_3 f_1 - f_2, \quad F_2 = f_4 f_1 - 1$$
$$F_3 = f_5 f_2 - 1, \quad F_4 = f_6 f_2 - 1.$$

Note that $F_1^{\sigma_0^5} = F_4$, $F_2^{\sigma_0} = F_3$ *and* $G_{F_2} = G_{\alpha^2 F_2} = G_{\alpha^4 F_2} = \langle \sigma_0^3 \rangle$. *Hence we have*

$$\begin{aligned}
\tilde{F}_{i1} &= \sum_{\sigma \in G} (\alpha^{i-1} F_1)^\sigma \quad \textit{for} \quad i = 1, \ldots, 6 \\
\tilde{F}_{12} &= \sum_{\sigma \in G/\langle \sigma_0^3 \rangle} F_2^\sigma \\
\tilde{F}_{22} &= \sum_{\sigma \in G} (\alpha F_2)^\sigma = 0 \\
\tilde{F}_{32} &= \sum_{\sigma \in G/\langle \sigma_0^3 \rangle} (\alpha^2 F_2)^\sigma \\
\tilde{F}_{42} &= \sum_{\sigma \in G} (\alpha^3 F_2)^\sigma = 0 \\
\tilde{F}_{52} &= \sum_{\sigma \in G/\langle \sigma_0^3 \rangle} (\alpha^4 F_2)^\sigma
\end{aligned}$$

and

$$\mathfrak{A} = (\{\tilde{F}_{i1}, \tilde{F}_{12}, \tilde{F}_{32}, \tilde{F}_{52} \mid i = 1, \ldots, 6\}).$$

3.4 A cyclotomic twisted torus as kernel of norm maps

In this section, we prove that we can regard the cyclic twisted torus as the intersection of all kernels of norm maps between the Weil restrictions of the algebraic torus. The theorem in this section indicates the generalization of discussions on twisting commutative algebraic groups in [9]. In [9], B. Mazur, K. Rubin and A. Silverberg consider twists of commutative algebraic groups over a field. The following theorem gives a example of their consequences over a ring.

For each positive integer ℓ dividing n, we set $G_\ell = \left\langle \sigma_0^{n/\ell} \right\rangle \subset G$ and $B_\ell = B^{G_\ell} \subset B$. For any group scheme $\mathcal{G}$ over B, we denote by $\operatorname{Res}_{B/A} \mathcal{G}$ the Weil restriction of $\mathcal{G}$ to over A. For each positive integer ℓ with $\ell | n$, let

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

be the norm map from B to B_ℓ. We define the subgroup scheme $\mathcal{T}(n)_A$ of $\operatorname{Res}_{B/A} \mathbb{G}_{m,B}$ by the intersection of all kernels of norm maps:

$$\mathcal{T}(n)_A := \operatorname{Ker}\left((\mathrm{Nm}_\ell)_{\ell|n} : \operatorname{Res}_{B/A}(\mathbb{G}_{m,B}) \to \prod_{\ell|n} \operatorname{Res}_{B_\ell/A}(\mathbb{G}_{m,B_\ell}) \right).$$

The follwing theorem is our main result of this section.

Theorem 3.4.1. *The cyclotomic twisted torus $\mathbb{G}(n)_A$ is canonically isomorphic to the group scheme $\mathcal{T}(n)_A$ over A:*

$$\mathbb{G}(n)_A \cong \mathcal{T}(n)_A.$$

Though the way of B. Mazur, K. Rubin and A. Silverberg in [9] makes a proof of this theorem easier, we provide another one (cf. B. Mazur, et al. [9] Remark 5.11).

Proof. Let C be any A-algebra. We will define a functorial group isomorphism $\rho(C) : \mathbb{G}(n)_A(C) \cong \mathcal{T}(n)_A(C)$. Note that

$$\mathbb{G}(n)_A = \operatorname{Spec} B[x_1, \ldots, x_m, 1/(x_1 \cdots x_m)]^G$$

and

$$B[x_1, \ldots, x_m, 1/(x_1 \cdots x_m)]^G \otimes_A B \cong B[x_1, \ldots, x_m, 1/(x_1 \cdots x_m)].$$

Therefore we have a correspondence

$$\begin{aligned}\mathbb{G}(n)_A(C) &= \mathrm{Hom}_A\left(B[x_1,\ldots,x_m,1/(x_1\cdots x_m)]^G, C\right)\\ &\subset \mathrm{Hom}_B\left(B[x_1,\ldots,x_m,1/(x_1\cdots x_m)]^G\otimes_A B, C\otimes_A B\right)\\ &= \mathrm{Hom}_B(B[x_1,\ldots,x_m,1/(x_1\cdots x_m)], C\otimes_A B);\\ \varphi &\mapsto \varphi\otimes \mathrm{id}_B\,.\end{aligned}$$

We define a G-action on $\mathrm{Hom}_B(B[x_1,\ldots,x_m,1/(x_1\cdots x_m)], C\otimes_A B)$ by $\psi^\sigma := (\mathrm{id}_C\otimes\sigma)\circ\psi\circ\sigma^{-1}$ for any $\psi\in\mathrm{Hom}_B(B[x_1,\ldots,x_m,1/(x_1\cdots x_m)], C\otimes_A B)$. By this G-action, we obtain the Lemma:

Lemma 8. *We have the equality*

$$\begin{aligned}&(\mathrm{Hom}_B(B[x_1,\ldots,x_m,1/(x_1\cdots x_m)], C\otimes_A B)^G\\ &= \mathrm{Hom}_A\left(B[x_1,\ldots,x_m,1/(x_1\cdots x_m)]^G, C\right).\end{aligned}$$

In fact, if $\psi\in\mathrm{Hom}_B(B[x_1,\ldots,x_m,1/(x_1\cdots x_m)], C\otimes_A B)$ is of the type $\psi = \varphi\otimes\mathrm{id}_B$ for some $\varphi\in\mathrm{Hom}_A\left(B[x_1,\ldots,x_m,1/(x_1\cdots x_m)]^G, C\right)$, then $\psi^\sigma = \sigma\circ\psi\circ\sigma^{-1} = \sigma\circ(\varphi\otimes\mathrm{id}_B)\sigma^{-1} = (\mathrm{id}_C\otimes\sigma)(\varphi\otimes\mathrm{id}_B)(\mathrm{id}\otimes\sigma^{-1}) = \varphi\otimes\mathrm{id}_B = \psi$. Conversely, if $\sigma_0\circ\psi\circ\sigma_0^{-1} = \psi$, then the restriction map $\varphi := \psi|_{B[x_1,\ldots,x_m,1/(x_1\cdots x_m)]^G} : B[x_1,\ldots,x_m,1/(x_1\cdots x_m)]^G\to C\otimes_A B$ satisfies $\sigma\varphi\sigma^{-1} = \sigma\varphi = \varphi$. Therefore we have $\mathrm{Im}(\varphi)\subset C = (C\otimes_A B)^G$. Since ψ is B-algebra homomorphism, we have $\psi = \varphi\otimes\mathrm{id}_B$, which proves Lemma 8.

Moreover we define an action of $G = \langle \sigma_0 \rangle$ on $((C \otimes_A B)^\times)^m$ by

$$\begin{aligned}(u_1, \ldots, u_m)^{\sigma_0} &= (u_1^{\sigma_0}, \ldots, u_m^{\sigma_0}) \\ &:= (\mathrm{id}_C \otimes \sigma_0)(u_1, \ldots, u_m)^{I^{-1}} \\ &= (\mathrm{id}_C \otimes \sigma_0)(u_1^{-1} u_2^{-a_{m-1}} \cdots u_m^{-a_1}, u_1, u_2, \ldots, u_{m-1})\end{aligned}$$

for $(u_1, \ldots, u_m) \in ((C \otimes_A B)^\times)^m$. Then we obtain

Lemma 9. *The canonical correspondence*

$$\begin{aligned}\mathrm{Hom}_B(B[x_1, \ldots, x_m, 1/(x_1 \cdots x_m)], C \otimes_A B) &\rightarrow ((C \otimes_A B)^\times)^m \\ \psi &\mapsto (\psi(x_1), \ldots, \psi(x_m))\end{aligned}$$

is G-equivariant.

In fact, for $\psi \in \mathrm{Hom}_B(B[x_1, \ldots, x_m, 1/(x_1 \cdots x_m)], C \otimes_A B)$, we have

$$\begin{aligned}(\mathrm{id}_C \otimes \sigma_0) \circ \psi \circ \sigma_0^{-1} \mapsto& (\mathrm{id}_C \otimes \sigma_0)(\psi \sigma_0^{-1}(x_1), \ldots, \psi \sigma_0^{-1}(x_m)) \\ &= (\mathrm{id}_C \otimes \sigma_0) \psi(x_1, \ldots, x_m)^{I^{-1}} \\ &= (\mathrm{id}_C \otimes \sigma_0)(\psi(x_1), \ldots, \psi(x_m))^{I^{-1}} \\ &= (\psi(x_1), \ldots, \psi(x_m))^{\sigma_0},\end{aligned}$$

which gives the proof of Lemma 9.

By using these lemmas, we obtain the canonical correspondence

$$\mathbb{G}(n)_A(C) \cong \left(\left((C \otimes_A B)^\times\right)^m\right)^G .$$

Furthermore, for any $u = (u_1, \ldots, u_m) \in ((C \otimes_A B)^\times)^m$, we have the equivalences

$$
\begin{aligned}
u \text{ is } G\text{-invariant} &\Longleftrightarrow (\mathrm{id}_C \otimes \sigma_0) u^{I^{-1}} = u \\
&\Longleftrightarrow \begin{cases} (\mathrm{id}_C \otimes \sigma_0)(u_1^{-a_{m-1}} u_2^{-a_{m-2}} \cdots u_{m-1}^{-a_1} u_m^{-1}) = u_1 \\ (\mathrm{id}_C \otimes \sigma_0) u_i = u_{i+1} \quad \text{for} \quad i = 1, \ldots, m-1 \end{cases} \\
&\Longleftrightarrow \begin{cases} u_1^{\sigma_0^i} = u_{i+1} \quad (i = 1, \ldots, m-1) \\ u_1^{1 + a_{m-1}\sigma_0 + \cdots + a_1 \sigma_0^{m-1} + \sigma_0^m} = 1 \end{cases} \\
&\Longleftrightarrow \begin{cases} u_1^{\sigma_0^i} = u_{i+1} \quad (i = 1, \ldots, m-1) \\ u_1^{\Phi_n(\sigma_0)} = 1. \end{cases}
\end{aligned}
$$

Therefore we have the canonical isomorphism

$$\begin{tikzcd}
 & \mathrm{Res}_{B/A}\left(\mathbb{G}_{m,B}\right)(C) \arrow[d, phantom, "||"] \\
 & (C \otimes_A B)^\times \arrow[d, phantom, "\bigcup"] \\
\mathbb{G}(n)_A(C) \cong (((C \otimes_A B)^\times)^m)^G \arrow[r, "\sim"] & \{u \mid u^{\Phi_n(\sigma_0)} = 1\} \\
(u_1, u_2, \ldots, u_m) \arrow[r, mapsto] & u_1.
\end{tikzcd}$$

On the other hand, let $n = p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r}$ be the prime decomposition of n. We set $n_i = n/p_i$ and

$$F_i(X) = X^{(p_i-1)n_i} + X^{(p_i-2)n_i} + \cdots + X^{n_i} + 1 = \frac{X^n - 1}{X^{n_i} - 1}$$

for $i = 1, \ldots, r$. We readily see that $(F_1(X), \ldots, F_r(X)) = \Phi_n(X)$. By the transitivity of the norm maps, we have

$$\mathcal{T}(n)_A = \mathrm{Ker}\left((\mathrm{Nm}_{n_i})_{i=1,\ldots,r} : \mathrm{Res}_{B/A}(\mathbb{G}_{m,B}) \to \prod_{i=1}^{r} \mathrm{Res}_{B_{n_i}/A}\left(\mathbb{G}_{m,B_{n_i}}\right) \right)$$

and for any $u \in (C \otimes_A B)^*$

$$\mathrm{Nm}_{n_i}(u) = \prod_{k=0}^{p_i-1} u^{\sigma_0^{kn_i}} = u^{F_i(\sigma_0)}$$

for $i = 1, \ldots, r$. Therefore we have the inclusion

$$\{u \mid u^{\Phi_n(\sigma_0)} = 1\} \subseteq \mathcal{T}(n)_A(C).$$

To prove the converse relation, we will use the following lemma, whose proof can be seen in N. G. de Bruijn [3]. However in Appendix A.1 to this thesis, we will give an elementary proof of it. According to Lemma 10 or Proposition 15, there exist polynomials $A_1(X), \ldots, A_r(X)$ with integral coefficients such that $\Phi_n(X) = \sum_{i=1}^r A_i(X)F_i(X)$. Hence for any $v \in \mathcal{T}(n)_A(C)$, we have

$$\begin{aligned} v^{\Phi_n(\sigma_0)} &= v^{\sum_{i=1}^r A_i(\sigma_0)F_i(\sigma_0)} \\ &= \prod \left(v^{F_i(\sigma_0)}\right)^{A_i(\sigma_0)} = 1 \end{aligned}$$

and $v \in \{u \mid u^{\Phi_n(\sigma_0)} = 1\}$. □

Lemma 10. *There exist polynomials $A_1(X), \ldots, A_r(X)$ with integral coefficients such that $\Phi_n(X) = \sum_{i=1}^r A_i(X)F_i(X)$.*

Proof. See Appendix A.1 in this thesis. □

Chapter 4

Review : Torsors for $G_{a,b}$ in the case of principal ideals

In this chapter, we review the description of torsors for $G_{a,b}$ by T. Sekiguchi and Y. Toda [16] in the case of the principal ideals.

Suppose that n is a positive integer with $n \geq 2$. Let $p \in \mathbb{Z}$ be a prime number with $n|(p-1)$. Note that $p \geq 3$. We assume that A is a local ring. We consider the number field $\mathbb{Q}(\zeta)/\mathbb{Q}$ of degree $m = \phi(n)$. By $n|(p-1)$, p is completely decomposed in $\mathbb{Q}(\zeta)$, namely, $(p) = \mathfrak{p}\mathfrak{p}_1 \cdots \mathfrak{p}_{m-1}$. Suppose that the ideal $\mathfrak{p}$ is principal in this section. Let $\theta \in \mathbb{Z}[\zeta]$ with $(\theta) = \mathfrak{p}$.

We recall the definition of the vector $\boldsymbol{x}^M$ obtained by raising to the power of the matrix M:

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

for $k, \ell \in \mathbb{Z}$, any vector $\boldsymbol{x} = (x_1, x_2, \ldots, x_k)$ and any matrix $M = (m_{ij}) \in \mathrm{M}_{k,\ell}(\mathbb{Z})$ (see Section 3.1).

We denote by I the representing matrix of ζ with respect to the standard basis of a $\mathbb{Z}$-module $\mathbb{Z}^m$. (See Section 3.1.) Then we have an exact sequence

$$1 \longrightarrow \operatorname{Ker}\theta \longrightarrow \mathbb{G}_{m,B}^m \xrightarrow{\theta} \mathbb{G}_{m,B}^m \longrightarrow 1, \tag{4.1}$$

where we regard θ as an endomorphism on $\mathbb{G}_{m,B}^m$ by $\mathbb{Z}[\zeta] \subset \operatorname{End}(\mathbb{G}_{m,B}^m)$ (see Section 3.2 or [8]). The morphism θ is precisely defined by

$$\theta(\boldsymbol{u}) = \boldsymbol{u}^{\theta(I)},$$

where $\theta(I)$ is the representing matrix of θ with respect to the standard basis of $\mathbb{Z}^m$. Note that $\det\theta(I) = p$. We denote by $\mathbb{G}(n)_A$ the Galois descent of $\mathbb{G}_{m,B}^m$ from B to A, called a cyclotomic twisted torus. See Chapter 3 or [8] for details. The Galois descent yields an exact sequence

$$1 \longrightarrow \overline{\operatorname{Ker}\theta} \longrightarrow \mathbb{G}(n)_A \xrightarrow{\theta} \mathbb{G}(n)_A \longrightarrow 1,$$

where $\overline{\operatorname{Ker}\theta}$ is the Galois descent of $\operatorname{Ker}\theta$ from B to A. Therefore we get the following long exact sequence as cohomology groups on $X_{fl} = (\operatorname{Spec} A)_{flat}$

$$\begin{aligned}
1 \longrightarrow \mathrm{H}^0_{\mathrm{fl}}(X, \overline{\operatorname{Ker}\theta}) &\longrightarrow \mathrm{H}^0_{\mathrm{fl}}(X, \mathbb{G}(n)_A) \xrightarrow{\mathrm{H}^0(\theta)} \mathrm{H}^0_{\mathrm{fl}}(X, \mathbb{G}(n)_A) \\
\xrightarrow{\partial^0} \mathrm{H}^1_{\mathrm{fl}}(X, \overline{\operatorname{Ker}\theta}) &\longrightarrow \mathrm{H}^1_{\mathrm{fl}}(X, \mathbb{G}(n)_A) \xrightarrow{\mathrm{H}^1(\theta)} \mathrm{H}^1_{\mathrm{fl}}(X, \mathbb{G}(n)_A) \\
\xrightarrow{\partial^1} \cdots .&
\end{aligned}$$

Thus we have the non-canonical isomorphism

$$\begin{aligned}
\mathrm{H}^1_{\mathrm{fl}}(X, \overline{\operatorname{Ker}\theta}) \cong \operatorname{Coker}[&\mathrm{H}^0_{\mathrm{fl}}(X, \mathbb{G}(n)_A) \overset{\mathrm{H}^0(\theta)}{\to} \mathrm{H}^0_{\mathrm{fl}}(X, \mathbb{G}(n)_A)] \\
&\times \operatorname{Ker}[\mathrm{H}^1_{\mathrm{fl}}(X, \mathbb{G}(n)_A) \overset{\mathrm{H}^1(\theta)}{\to} \mathrm{H}^1_{\mathrm{fl}}(X, \mathbb{G}(n)_A)].
\end{aligned} \tag{4.2}$$

Let $n = p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r}$ be the factorization of n into prime numbers. T. Sekiguchi and Y. Toda [16] computed the first cohomology group $\mathrm{H}^1_{\mathrm{fl}}(X, \mathbb{G}(n)_A)$ by a cyclotomic resolution

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

where $n_{i_0i_1\cdots i_s} = \dfrac{n}{p_{i_1}p_{i_2}\cdots p_{i_s}}$ and $B_{i_0i_1\cdots i_s} = B^{<\sigma^{n_{i_0i_1\cdots i_s}}>}$ for integers $0 \le i_0 < i_1 < \cdots < i_s \le r$. Then we have the short exact sequence

$$1 \longrightarrow \mathbb{G}(n)_A \longrightarrow \operatorname{Res}_{B/A}\mathbb{G}_{m,B} \xrightarrow{\delta^0} \operatorname{Ker}\delta^1 \longrightarrow 1.$$

Then we have the long exact sequence

$$\begin{aligned} 1 &\longrightarrow \mathrm{H}^0_{\mathrm{fl}}(X, \mathbb{G}(n)_A) \longrightarrow \mathrm{H}^0_{\mathrm{fl}}(X, \operatorname{Res}_{B/A}\mathbb{G}_{m,B}) \xrightarrow{\mathrm{H}(\delta^0)} \mathrm{H}^0_{\mathrm{fl}}(X, \operatorname{Ker}\delta^1) \\ &\xrightarrow{\partial} \mathrm{H}^1_{\mathrm{fl}}(X, \mathbb{G}(n)_A) \longrightarrow \mathrm{H}^1_{\mathrm{fl}}(X, \operatorname{Res}_{B/A}\mathbb{G}_{m,B}) = 0. \end{aligned}$$

Therefore there is the canonical isomorphism

$$\mathrm{H}^1_{\mathrm{fl}}(X, \mathbb{G}(n)_A) \cong \operatorname{Coker}\left[\mathrm{H}^0_{\mathrm{fl}}(X, \operatorname{Res}_{B/A}\mathbb{G}_{m,B}) \xrightarrow{\mathrm{H}(\delta^0)} \mathrm{H}^0_{\mathrm{fl}}(X, \operatorname{Ker}\delta^1)\right].$$

We have the explicit correspondence in the isomorphism above as follows: for any $\overline{s} \in \operatorname{Coker}\left[\mathrm{H}^0_{\mathrm{fl}}(X, \operatorname{Res}_{B/A}\mathbb{G}_{m,B}) \xrightarrow{\mathrm{H}(\delta^0)} \mathrm{H}^0_{\mathrm{fl}}(X, \operatorname{Ker}\delta^1)\right]$, $s^*(\operatorname{Res}_{B/A}\mathbb{G}_{m,B})$, which is the pull-back of $\operatorname{Res}_{B/A}\mathbb{G}_{m,B}$ by $s : X \to \operatorname{Ker}\delta^1$, is in $\mathrm{H}^1_{\mathrm{fl}}(X, \mathbb{G}(n)_A)$.

Since we explicitly give the correspondence in the isomorphism (4.2) in [16], we provide $(\overline{\operatorname{Ker}\theta})$-torsors in terms of the cohomology groups of $\mathbb{G}(n)_A$. In the case of $n = p-1$, we get $G_{a,b}$-torsors under the assumption that the ideal $\mathfrak{p} \subset \mathbb{Z}[\zeta]$ is principal.

In fact, let $\operatorname{Spec}\Lambda_p$ be the base scheme of $\operatorname{Spec} A$ and $\operatorname{Spec} B$, where

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

Note that ζ is a primitive $(p-1)$-st root of unity in the ring $\mathbb{Z}_p$ of p-adic integers. First, we explain the Oort-Tate group schemes $G_{a,b}$. F. Oort and J. Tate completely classified the finite A-group schemes of order p. Let (M, a, b) be a tuple consisting of a projective A-module M of rank one together with $a \in M^{\otimes(p-1)}$ and $b \in M^{\otimes(1-p)}$ satisfying $a \otimes b = \omega_p$, where ω_p is the product of p and an invertible element of Λ_p. The finite group scheme corresponding to (A, a, b) is given by

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

with the comultiplication

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

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

Now, we describe $G_{a,b}$-torsors in the case where the ideal $\mathfrak{p}$ is principal i.e. $\mathfrak{p} = (\theta)$ for some $\theta \in \mathbb{Z}[\zeta]$. We assume that $B = A[u]$, where we denote by u an n-th root of a non-zero divisor $b \in A$. In other words, we assume that there exists an n-th root $u \in B$ of a non-zero divisor $b \in A$. From the exact sequence (4.1), we have an exact sequence

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

Note that deg $\theta = p$. The Galois descent makes it the exact sequence

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

T. Sekiguchi and Y. Toda confirmed that

$$\left(\boldsymbol{\mu}_{p,B}\right)^G \cong G_{a,b}$$

by choosing suitable elements $a, b \in A$ in [16]. Therefore we obtain the Kummer sequence for the cyclotomic twisted torus $\mathbb{G}(n)_A$:

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

Then we have a long exact sequence

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

We have the explicit correspondence in the noncanonical isomorphism

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

for any $\overline{g} \in \operatorname{Coker} \mathrm{H}^0(\theta)$ and any $s^*(\mathrm{Res}_{B/A}\, \mathbb{G}_{m,B}) \in \operatorname{Ker} \mathrm{H}^1(\theta)$, we have the commutative diagram

$$\begin{tikzcd} \rho^{-1}(\{1\} \times X) \arrow[r] \arrow[d] & s^*(\mathrm{Res}_{B/A}\, \mathbb{G}_{m,B}) \arrow[r, "\rho"] \arrow[d] & \theta_* s^*(\mathrm{Res}_{B/A}\, \mathbb{G}_{m,B}) \arrow[d] \\ X \arrow[r, equal] & X \arrow[r, equal] & X. \end{tikzcd}$$

Note that $\theta_* s^*(\mathrm{Res}_{B/A}\, \mathbb{G}_{m,B}) \cong \mathbb{G}(n)_A \times X$ and $\iota_*(\rho^{-1}(\{1\} \times X)) \cong s^*(\mathrm{Res}_{B/A}\, \mathbb{G}_{m,B})$. See [16] for details. Furthermore $G_{a,b}$, $\mathbb{G}(n)_A$ and $\mathbb{G}(n)_A$ act on $\rho^{-1}(\{1\} \times X)$, $s^*(\mathrm{Res}_{B/A}\, \mathbb{G}_{m,B})$ and $\theta_* s^*(\mathrm{Res}_{B/A}\, \mathbb{G}_{m,B})$ respectively. Then we have

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

where the operation "+" is on $\mathrm{H}^1_{\mathrm{fl}}(X, G_{a,b})$.

Chapter 5

$G_{a,b}$-torsors in the general conditions

In this chapter, we introduce Kummer theory for cyclotomic twisted tori in the general case along [7]. This is the main chapter in this thesis. First, we consider the homomorphisms defined by ideals of $\mathrm{End}(\mathbb{G}(n)_A)$. Second, we provide the exact sequence inducing the Kummer sequence for cyclotomic twisted tori in the non-principal case. Finally, we describe torsors for $G_{a,b}$ in the general case.

5.1 Homomorphisms defined by ideals of $\mathrm{End}(\mathbb{G}(n)_A)$

Suppose that n is an integer with $n \geq 2$. Let $p \in \mathbb{Z}$ be prime with $n|(p-1)$. We provide the claim of an order of the kernel of a homomorphism on $\mathbb{G}(n)_A$ corresponding to an ideal in $\mathbb{Z}[\zeta]$. This plays a key role when we consider finite subgroup schemes of the cyclotomic twisted torus.

Let $\mathfrak{a} \subset \mathbb{Z}[\zeta]$ be a non-zero ideal. It is well-known that there exist $\xi, \eta \in \mathbb{Z}[\zeta]$

such that $\mathfrak{a} = (\xi, \eta)$. Note that $\mathbb{Z}[\zeta] \cong \mathrm{End}(\mathbb{G}(n)_A)$ (see [16] Theorem 4.1). We denote by I the representing matrix of ζ with respect to the standard $\mathbb{Z}$-basis of $\mathbb{Z}^m$ (see Section 3.1). We define a homomorphism $\psi_{\mathfrak{a}} : \mathbb{G}(n)_A \to \mathbb{G}(n)_A \times \mathbb{G}(n)_A$ corresponding to the ideal $\mathfrak{a} = (\xi, \eta)$ by

$$\psi_{\mathfrak{a}}(\boldsymbol{x}) = (\boldsymbol{x}^{\xi(I)}, \boldsymbol{x}^{\eta(I)}),$$

where $\xi(I)$ and $\eta(I)$ are the representing matrixes of ξ and η respectively. For simplicity, we may denote a vector $\boldsymbol{x}^{\alpha(I)}$ obtained by raising to the power of a matrix $\alpha(I)$ by $\boldsymbol{x}^{\alpha}$ for any $\alpha \in \mathbb{Z}[\zeta]$. We set $\mathbb{G}(n)_A[\mathfrak{a}] = \mathrm{Ker}(\psi_{\mathfrak{a}} : \mathbb{G}(n)_A \to \mathbb{G}(n)_A \times \mathbb{G}(n)_A)$. The following lemma indicates that this construction of $\mathbb{G}(n)_A[\mathfrak{a}]$ is independent of the choice of the generators of $\mathfrak{a}$.

Lemma 11. *Suppose that an ideal $\mathfrak{a}$ admits a pair of generators*

$$\mathfrak{a} = (\xi, \eta) = (\xi', \eta').$$

Then we have

$$\mathbb{G}(n)_A[(\xi, \eta)] = \mathbb{G}(n)_A[(\xi', \eta')].$$

Proof. It suffices to show that $\mathbb{G}(n)_A[(\xi, \eta)] \supset \mathbb{G}(n)_A[(\xi', \eta')]$. Fix a local section $\boldsymbol{x} \in \mathbb{G}(n)_A[(\xi', \eta')]$. Therefore the local section $\boldsymbol{x}$ satisfies $1 = \boldsymbol{x}^{\xi'} = \boldsymbol{x}^{\eta'}$. By the assumption, there is the matrix $M = \begin{pmatrix} m_1 & m_2 \\ m_3 & m_4 \end{pmatrix} \in \mathrm{GL}_2(\mathbb{Z}[\zeta])$ such that

$$\begin{pmatrix} m_1 & m_2 \\ m_3 & m_4 \end{pmatrix} \begin{pmatrix} \xi \\ \eta \end{pmatrix} = \begin{pmatrix} \xi' \\ \eta' \end{pmatrix}.$$

Then we have

$$\begin{cases} \boldsymbol{x}^{m_1\xi} = \boldsymbol{x}^{-m_2\eta} \\ \boldsymbol{x}^{m_3\xi} = \boldsymbol{x}^{-m_4\eta}. \end{cases}$$

Hence we get the equalities

$$\begin{aligned}\boldsymbol{x}^{m_1 m_4 \xi} &= \boldsymbol{x}^{-m_2 m_4 \eta} \\ &= \left(\boldsymbol{x}^{-m_4 \eta}\right)^{m_2} \\ &= \left(\boldsymbol{x}^{m_3 \xi}\right)^{m_2} \\ &= \boldsymbol{x}^{m_2 m_3 \xi}.\end{aligned}$$

Since $\det \begin{pmatrix} m_1 & m_2 \\ m_3 & m_4 \end{pmatrix} \in \mathbb{Z}[\zeta]^*$, we obtain $\boldsymbol{x}^{\xi} = 1$. Similarly, we have $\boldsymbol{x}^{\eta} = 1$. □

Theorem 5.1.1. *For each unramified ideal $\mathfrak{a} \subset \mathbb{Z}[\zeta]$, we have*

$$|\mathbb{G}(n)_A[\mathfrak{a}]| = \mathrm{Nm}_{\mathbb{Q}(\zeta)/\mathbb{Q}}\, \mathfrak{a}.$$

Proof. If two unramified ideals $\mathfrak{a}$ and $\mathfrak{b}$ are coprime, we easily see that $\mathbb{G}(n)_A[\mathfrak{a}\mathfrak{b}] = \mathbb{G}(n)_A[\mathfrak{a}] \oplus \mathbb{G}(n)_A[\mathfrak{b}]$. Hence we may assume that $\mathfrak{a} = \mathfrak{p}^{\ell}$, where $\mathfrak{p}$ is an unramified prime ideal and $\ell \in \mathbb{Z}$. Let $p \in \mathbb{Z}$ be a prime number with $(p) = \mathbb{Z} \cap \mathfrak{p}$. There exists $\theta \in \mathbb{Z}[\zeta]$ such that $\mathfrak{p} = (p,\ \theta)$. Then we have $\mathfrak{p}^{\ell} = (p^{\ell},\ \theta^{\ell})$ by the factorization into prime ideals. Let $f \in \mathbb{Z}$ be the degree of $\mathfrak{p}$ i.e. $f = [\mathbb{Z}[\zeta]/\mathfrak{p} : \mathbb{Z}/p\mathbb{Z}]$. Therefore, we obtain $\mathrm{Nm}_{\mathbb{Q}[\zeta]/\mathbb{Q}}\, \mathfrak{p}^{\ell} = p^{f\ell}$.

In the rest of the proof, we see that $|\mathbb{G}(n)_A[\mathfrak{p}^{\ell}]| = p^{f\ell}$ by induction on ℓ. It suffices to check that the p-part of $\mathbb{Z}[\zeta]/\theta^{\ell}\mathbb{Z}[\zeta]$ is isomorphic to $(\mathbb{Z}/p^{\ell}\mathbb{Z})^f$. In the case of $\ell = 1$, since $\mathfrak{p}$ is lying above p we have the isomorphisms

$$\begin{aligned}(\mathbb{Z}[\zeta]/\theta\mathbb{Z}[\zeta])_p &\cong \mathbb{Z}[\zeta]/\mathfrak{p} \\ &= \mathbb{F}_{p^f} \\ &\cong \bigoplus_{i=1}^{f} \mathbb{Z}/p\mathbb{Z} \qquad \text{as } \mathbb{Z}/p\mathbb{Z}\text{-modules,}\end{aligned}$$

where we denote the p-part of $\mathbb{Z}[\zeta]/\theta\mathbb{Z}[\zeta]$ by $(\mathbb{Z}[\zeta]/\theta\mathbb{Z}[\zeta])_p$. Suppose that our claim is true for ℓ, namely, we have

$$(\mathbb{Z}[\zeta]/\theta^\ell\mathbb{Z}[\zeta])_p \cong (\mathbb{Z}/p^\ell\mathbb{Z})^f.$$

Note that we have the isomorphism

$$(\mathbb{Z}[\zeta]/\theta^\ell\mathbb{Z}[\zeta])_p \cong \mathbb{Z}[\zeta]/\mathfrak{p}^\ell$$

in the same way as above. We get the exact sequence

$$0 \longrightarrow \mathfrak{p}^\ell/\mathfrak{p}^{\ell+1} \longrightarrow \mathbb{Z}[\zeta]/\mathfrak{p}^{\ell+1} \xrightarrow{\pi} \mathbb{Z}[\zeta]/\mathfrak{p}^\ell \longrightarrow 0.$$

Let $\boldsymbol{x}_i = (0, \ldots, 1, \ldots, 0) \in (\mathbb{Z}/p^\ell\mathbb{Z})^f$ for $i = 1, \ldots, f$. Then we have the isomorphism

$$\mathbb{Z}[\zeta]/\mathfrak{p}^\ell \cong \bigoplus_{i=1}^{f}(\mathbb{Z}/p^\ell\mathbb{Z})\boldsymbol{x}_i.$$

Let $\xi_i \in \mathbb{Z}[\zeta]/\mathfrak{p}^{\ell+1}$ satisfying $\pi(\xi_i) = \boldsymbol{x}_i$ for $i = 1, \ldots, f$. Hence we obtain a basis $\{[\overline{\boldsymbol{x}_1}], \ldots, [\overline{\boldsymbol{x}_f}]\}$ of $\mathbb{Z}[\zeta]/\mathfrak{p} \cong \mathbb{F}_{p^f}$, where $[\overline{\boldsymbol{x}_i}]$'s are the images of $\overline{\boldsymbol{x}_i}$'s under the isomorphism $(\mathbb{Z}[\zeta]/\mathfrak{p}^\ell)/(\mathfrak{p}/\mathfrak{p}^\ell) \tilde{\to} \mathbb{Z}[\zeta]/\mathfrak{p} \cong \mathbb{F}_{p^f}$. Since $\mathbb{Z}[\zeta]/\mathfrak{p}^\ell$ is an Artin local ring, all $\boldsymbol{x}_i$'s are in $(\mathbb{Z}[\zeta]/\mathfrak{p}^\ell)^*$. Therefore since $\boldsymbol{x}_i = \pi(\xi_i)$, we have $\xi_i \in (\mathbb{Z}[\zeta]/\mathfrak{p}^{\ell+1})^*$ for any $i = 1, \ldots, f$. We take any $a_1, \ldots, a_f \in \mathbb{Z}$ satisfying $\pi(\sum_{i=1}^{f} a_i\xi_i) = 0$. Since $\boldsymbol{x}_1, \ldots, \boldsymbol{x}_f$ are generators of $\mathbb{Z}[\zeta]/\mathfrak{p}^\ell$, $a_1 = \cdots = a_f \in p^\ell\mathbb{Z}$. On the other hand, we have the equivalences

$$\begin{aligned} a\xi_i = 0 \quad \text{in } \mathbb{Z}[\zeta]/\mathfrak{p}^{\ell+1} &\Longleftrightarrow v_\mathfrak{p}(a\xi_i) \geq \ell + 1 \\ &\Longleftrightarrow p^{\ell+1} | a. \end{aligned}$$

In fact, the first equivalence is true by the definition of a $\mathfrak{p}$-exponent. We know that $v_\mathfrak{p}(a\xi_i) = v_\mathfrak{p}(a) + v_\mathfrak{p}(\xi_i)$. Since $a \in \mathbb{Z}$ and $(p) = \mathbb{Z} \cap \mathfrak{p}$, we have $v_\mathfrak{p}(a) = v_p(a)$. Since

$\xi_i \in (\mathbb{Z}[\zeta]/\mathfrak{p}^{\ell+1})^*$, $v_{\mathfrak{p}}(\xi_i) = 0$. Therefore we get $v_{\mathfrak{p}}(a\xi_i) = v_p(a) \geq \ell + 1$ by which we check the last equivalence. Let $\mathbb{Z}[\zeta]_{\mathfrak{p}}$ be the local ring of $\mathbb{Z}[\zeta]$ at $\mathfrak{p}$ and t a generator of the maximal ideal $\mathfrak{p}\mathbb{Z}[\zeta]_{\mathfrak{p}}$. Then we have the isomorphisms

$$\begin{aligned}
\mathfrak{p}^\ell/\mathfrak{p}^{\ell+1} &\cong (\mathbb{Z}[\zeta]/\mathfrak{p})\bar{t}^\ell && \text{as } \mathbb{Z}[\zeta]/\mathfrak{p}\text{-modules} \\
&\supset \sum_{i=1}^{f} p^\ell(\mathbb{Z}/p^{\ell+1})\xi_i \\
&\cong \bigoplus_{i=1}^{f} \mathbb{F}_p\xi_i && \text{as } \mathbb{F}_p\text{-modules} \\
&\cong \mathbb{F}_{p^f}.
\end{aligned}$$

Note that $\sum_{i=1}^{f}(\mathbb{Z}/p^{\ell+1}\mathbb{Z})\xi_i \subset \mathbb{Z}[\zeta]/\mathfrak{p}^{\ell+1}$. We see that the homomorphism π restricted to $\sum_{i=1}^{f}(\mathbb{Z}/p^{\ell+1}\mathbb{Z})\xi_i$ is surjective. In fact, we have the isomorphism $\mathbb{Z}[\zeta]/\mathfrak{p}^\ell \cong (\mathbb{Z}/p^\ell\mathbb{Z})\boldsymbol{x}_1 \oplus \cdots \oplus (\mathbb{Z}/p^\ell\mathbb{Z})\boldsymbol{x}_f$ as $\mathbb{Z}/p^\ell\mathbb{Z}$-modules. Let $a_1\boldsymbol{x}_1 + \cdots + a_f\boldsymbol{x}_f$ be fixed. Since the map $\mathbb{Z}/p^{\ell+1}\mathbb{Z} \to \mathbb{Z}/p^\ell\mathbb{Z}$ is surjective, there is α_i such that its image is a_i for each $i = 1, \ldots f$. Thus $\pi(\sum_{i=1}^{f}\alpha_i\xi_i) = \sum_{i=1}^{f} a_i\boldsymbol{x}_i$, as desired. Therefore we have a commutative diagram

$$\begin{tikzcd}
0 \arrow[r] & \mathfrak{p}^\ell/\mathfrak{p}^{\ell+1} \arrow[r] \arrow[d, "\wr"'] & \mathbb{Z}[\zeta]/\mathfrak{p}^{\ell+1} \arrow[r] & \mathbb{Z}[\zeta]/\mathfrak{p}^\ell \arrow[r] \arrow[d, equal] & 0 \\
0 \arrow[r] & \mathbb{F}_{p^f} \arrow[r] & \sum_{i=1}^{f}(\mathbb{Z}/p^{\ell+1}\mathbb{Z})\xi_i \arrow[r] \arrow[u] & \mathbb{Z}[\zeta]/\mathfrak{p}^\ell \arrow[r] & 0.
\end{tikzcd}$$

By the snake lemma, we have $\mathbb{Z}[\zeta]/\mathfrak{p}^{\ell+1} \cong \sum_{i=1}^{f}(\mathbb{Z}/p^{\ell+1}\mathbb{Z})\xi_i$, which completes the proof.

□

5.2 The key exact sequence for calculating $G_{a,b}$-torsors

Here we show an exact sequence, which induces the short exact sequence like the Kummer sequence. This will play a key role to consider $G_{a,b}$-torsors in terms of the first cohomology group of $G_{a,b}$ in Section 5.3.

Suppose that n is an integer with $n \geq 2$. Let $p \in \mathbb{Z}$ be a prime number with $n|(p-1)$ and hence $p \geq 3$. We consider an algebraic number field $\mathbb{Q}(\zeta)/\mathbb{Q}$. Let $\mathfrak{p} \subset \mathbb{Z}[\zeta]$ be one of the prime ideals lying above $p \in \mathbb{Z}$. We know that there exists $\theta \in \mathbb{Z}[\zeta]$ such that $\mathfrak{p} = (p, \theta)$. Then we have the theorem for the key exact sequence:

Theorem 5.2.1. *For the ideal $\mathfrak{p} = (p, \theta)$ above, we can choose a homomorphism ψ such that the following sequence is exact as sheaves of groups on $(\operatorname{Spec} B)_{flat}$:*

$$1 \longrightarrow \operatorname{Ker} \psi_{\mathfrak{p}} \longrightarrow \mathbb{G}_{m,B}^m \xrightarrow{\psi_{\mathfrak{p}}} \mathbb{G}_{m,B}^m \times \mathbb{G}_{m,B}^m \xrightarrow{\psi} \mathbb{G}_{m,B}^m \times \mathbb{G}_{m,B}^m,$$

where we set $\psi_{\mathfrak{p}}(\boldsymbol{x}) = (\boldsymbol{x}^p, \boldsymbol{x}^\theta)$ and $\psi(\boldsymbol{u}, \boldsymbol{v}) = (\boldsymbol{u}^\beta \boldsymbol{v}^{-\alpha}, \boldsymbol{u}^{\beta'} \boldsymbol{v}^{-\alpha'})$.

First, we explain the morphisms $\psi_{\mathfrak{p}}$ and ψ in the theorem above. Recall the definition of a homomorphism $\psi_{\mathfrak{a}}$ corresponding to the ideal $\mathfrak{a} \subset \mathbb{Z}[\zeta]$ in Section 5, 5.1. Then we have the morphism

$$\psi_{\mathfrak{p}}(\boldsymbol{x}) = (\boldsymbol{x}^{pE_m}, \boldsymbol{x}^{\theta(I)}),$$

where E_m is the identity element of $M_m(\mathbb{Z})$, I the representing matrix of ζ with respect to the standard basis of a $\mathbb{Z}$-module $\mathbb{Z}^m$ and $\theta(I)$ the representing matrix of θ.

Now we give the definition of the morphism ψ. We have

$$(p) = \mathfrak{p}\mathfrak{p}_1 \cdots \mathfrak{p}_{m-1},$$

$$(\theta) = \mathfrak{p}\mathfrak{q}_1^{e_1} \cdots \mathfrak{q}_r^{e_r}$$

by the factorization into prime ideals with $\mathfrak{p}_i + \mathfrak{q}_j = (1)$ for any $i = 1, \ldots, m-1$ and $j = 1, \ldots, r$. We denote an uniformizing parameter at a prime ideal $\mathfrak{q}$ by $x_{\mathfrak{q}} \in \mathbb{Z}[\zeta]_{\mathfrak{q}}$. By the approximation theorem, there exists $\alpha \in \mathbb{Q}[\zeta]$ such that

$$\begin{cases} v_{\mathfrak{p}_i}(\alpha - x_{\mathfrak{p}_i}) \geq 2 & (i = 1, \ldots, m-1) \\ v_{\mathfrak{q}_j}(\alpha - 1 + x_{\mathfrak{q}_j}^{e_j}) \geq e_j + 1 & (j = 1, \ldots, r) \\ v_{\mathfrak{q}}(\alpha) \geq 0 & (\mathfrak{q} \neq \mathfrak{p}_i, \mathfrak{q}_j), \end{cases}$$

where $v_{\mathfrak{q}}$ is a $\mathfrak{q}$-exponent for each prime ideal $\mathfrak{q}$. Then we easily see that α belongs to $\mathbb{Z}[\zeta]$ satisfying $\alpha \in \mathfrak{p}_1 \cdots \mathfrak{p}_{m-1} = (p)\mathfrak{p}^{-1}$. There exists an ideal $\mathfrak{a}$ to be coprime to all $\mathfrak{p}_i$ and $\mathfrak{q}_j$ such that $(\alpha) = \mathfrak{p}_1 \cdots \mathfrak{p}_{m-1}\mathfrak{a}$. Moreover for each prime ideal $\mathfrak{q}_j$, we have the equations

$$\alpha = 1 - x_{\mathfrak{q}_j}^{e_j} + (\text{terms of higher degree in } x_{\mathfrak{q}_j}).$$

Then there exists an ideal $\mathfrak{b}$ to be coprime to all $\mathfrak{p}_i$ and $\mathfrak{q}_j$ such that $(1-\alpha) = \mathfrak{q}_1^{e_1} \cdots \mathfrak{q}_r^{e_r}\mathfrak{b}$. We have the equation

$$(p(1-\alpha)) = \mathfrak{p}\mathfrak{p}_1 \cdots \mathfrak{p}_{m-1}\mathfrak{q}_1^{e_1} \cdots \mathfrak{q}_r^{e_r}\mathfrak{b}.$$

Note that $\mathfrak{b}$ is coprime to $\mathfrak{p}$ by $1 - \alpha \in (\theta)\mathfrak{p}^{-1}$. And we have the equality $(\theta\alpha) = \mathfrak{p}\mathfrak{p}_1 \cdots \mathfrak{p}_{m-1}\mathfrak{q}_1^{e_1} \cdots \mathfrak{q}_r^{e_r}\mathfrak{a}$. Note that the ideal $\mathfrak{a}$ satisfies that $(\mathfrak{p}, \mathfrak{a}) = (\mathfrak{b}, \mathfrak{a}) = 1$ by $1-\alpha \in (\theta)\mathfrak{p}^{-1}$. Hence we see that $\theta\alpha \in \mathfrak{p}\mathfrak{p}_1 \cdots \mathfrak{p}_{m-1} = (p)$ and $p(1-\alpha) \in \mathfrak{p}\mathfrak{q}_1^{e_1} \cdots \mathfrak{q}_r^{e_r} = (\theta)$. Then there exists $\beta \in \mathbb{Z}[\zeta]$ such that $\theta\alpha = p\beta$ and $\alpha' \in \mathbb{Z}[\zeta]$ such that $p(1-\alpha) = \theta\alpha'$. We set $\beta' = 1 - \alpha$. We define a morphism ψ by

$$\psi(\boldsymbol{u}, \boldsymbol{v}) = (\boldsymbol{u}^{\beta(I)}\boldsymbol{v}^{-\alpha(I)}, \boldsymbol{u}^{\beta'(I)}\boldsymbol{v}^{-\alpha'(I)}),$$

where $\alpha(I), \beta(I), \alpha'(I)$ and $\beta'(I)$ are the repsresenting matrixes of α, β, α' and β' respectively.

Second, we give a proof of Theorem 5.2.1.

Proof. It suffices to show that $\operatorname{Im}\psi_{\mathfrak{p}} = \operatorname{Ker}\psi$. By the definitions of homomorphisms $\psi_{\mathfrak{p}}$ and ψ, we immediately see that $\operatorname{Im}\psi_{\mathfrak{p}} \subset \operatorname{Ker}\psi$. Conversely, for any B-algebra R, let a local section $(\boldsymbol{u}, \boldsymbol{v}) \in \operatorname{Ker}[\psi_R : (\mathbb{G}_{m,B}^m \times \mathbb{G}_{m,B}^m)(R) \to \mathbb{G}_{m,B}^m \times \mathbb{G}_{m,B}^m)(R)]$ be fixed. Since $\mathbb{G}_{m,B}$ is a sheaf of group on the flat topology, we choose $\boldsymbol{x} \in \mathbb{G}_{m,B}(R')$ such that $\boldsymbol{x}^p = \boldsymbol{u}$ for some suitable flat extension R' of R. Then we have $\boldsymbol{x}^{p\beta}\boldsymbol{v}^{-\alpha} = 1$ and $\boldsymbol{x}^{p\beta'}\boldsymbol{v}^{-\alpha'} = 1$. Since $\theta\alpha = p\beta$ and $p\beta' = \theta\alpha'$, we get

$$\begin{cases} \left(\dfrac{\boldsymbol{v}}{\boldsymbol{x}^\theta}\right)^\alpha = 1 \\ \left(\dfrac{\boldsymbol{v}}{\boldsymbol{x}^\theta}\right)^{\alpha'} = 1. \end{cases}$$

We set $\xi = \dfrac{\boldsymbol{v}}{\boldsymbol{x}^\theta}$. Hence we have $\xi^\alpha = 1 = \xi^{\alpha'}$. Since we know that

$$\begin{cases} (\alpha) = \mathfrak{p}_1 \cdots \mathfrak{p}_{m-1}\mathfrak{a} \\ (\alpha') = \mathfrak{p}_1 \cdots \mathfrak{p}_{m-1}\mathfrak{b}, \end{cases}$$

we have

$$(\alpha, \alpha') = \mathfrak{p}_1 \cdots \mathfrak{p}_{m-1} \supset \mathfrak{p}\mathfrak{p}_1 \cdots \mathfrak{p}_{m-1} = (p).$$

There exist $x, y \in \mathbb{Z}[\zeta]$ such that $p = x\alpha + y\alpha'$. Then we have $\xi^p = 1$, since $\xi^\alpha = \xi^{\alpha'} = 1$. We easily see that $(\theta) + (\alpha) = 1$. Then there exist $z, w \in \mathbb{Z}[\zeta]$ such that $\theta z + \alpha w = 1$. Hence we get $\xi = \xi^{\theta z + \alpha w} = \xi^{\theta z}$. Therefore, we have equations

$$\begin{cases} \boldsymbol{u} = \boldsymbol{x}^p = (\xi^z \boldsymbol{x})^p \\ \boldsymbol{v} = \xi \boldsymbol{x}^\theta = (\xi^z \boldsymbol{x})^\theta. \end{cases}$$

This completes the proof. □

5.3 On the general $G_{a,b}$-torsors

In this section, we provide the description of $G_{a,b}$-torsors in terms of elements in the first cohomology group of $\mathbb{G}(n)_A$ in the case of non-principal ideals.

Let $p \in \mathbb{Z}$ be a prime number with $p \geq 3$. We let $n = p - 1$. Let $\mathfrak{p} \subset \mathbb{Z}[\zeta]$ be an ideal lying above p. We assume that A is a local ring. Now we describe the $G_{a,b}$-torsors in the general case. In this section, we do not assume that the ideal $\mathfrak{p}$ is principal. Suppose that $B = A[u]$, where u is an n-th root of a non-zero divisor $b \in A$. By Theorem 5.2.1, we have the exact sequence

$$1 \to \boldsymbol{\mu}_{p,B} \to \mathbb{G}_{m,B}^m \xrightarrow{\psi_{\mathfrak{p}}} \operatorname{Ker}(\psi : \mathbb{G}_{m,B}^m \times \mathbb{G}_{m,B}^m \to \mathbb{G}_{m,B}^m \times \mathbb{G}_{m,B}^m) \to 1. \tag{5.1}$$

We will give the defining equations of $\operatorname{Ker}\psi$ explicitly in Appendix A.2.

The Galois descent for the exact sequence (5.1) yields an exact sequence

$$1 \longrightarrow G_{a,b} \longrightarrow \mathbb{G}(n)_A \xrightarrow{\psi_{\mathfrak{p}}} \overline{\operatorname{Ker}\psi} \longrightarrow 1,$$

where $\overline{\operatorname{Ker}\psi}$ is the Galois descent of $\operatorname{Ker}\psi$ to A. We call the exact sequence above the Kummer sequence for cyclotomic twisted tori in the general case. Then we have a long exact sequence as cohomology groups on $X_{fl} = (\operatorname{Spec}A)_{flat}$

$$\begin{aligned} 0 \longrightarrow \mathrm{H}^0_{\mathrm{fl}}(X, G_{a,b}) &\longrightarrow \mathrm{H}^0_{\mathrm{fl}}(X, \mathbb{G}(n)_A) \xrightarrow{\mathrm{H}^0(\psi_{\mathfrak{p}})} \mathrm{H}^0_{\mathrm{fl}}(X, \overline{\operatorname{Ker}\psi}) \\ \xrightarrow{\partial^0} \mathrm{H}^1_{\mathrm{fl}}(X, G_{a,b}) &\longrightarrow \mathrm{H}^1_{\mathrm{fl}}(X, \mathbb{G}(n)_A) \xrightarrow{\mathrm{H}^1(\psi_{\mathfrak{p}})} \mathrm{H}^1_{\mathrm{fl}}(X, \overline{\operatorname{Ker}\psi}) \\ \xrightarrow{\partial^1} \cdots . & \end{aligned}$$

We have the noncanonical isomorphism

$$\begin{aligned} \mathrm{H}^1_{\mathrm{fl}}(X, G_{a,b}) \cong \operatorname{Coker} &\left[\mathrm{H}^0_{\mathrm{fl}}(X, \mathbb{G}(n)_A) \xrightarrow{\mathrm{H}^0(\psi_{\mathfrak{p}})} \mathrm{H}^0_{\mathrm{fl}}(X, \overline{\operatorname{Ker}\psi})\right] \\ &\times \operatorname{Ker}\left[\mathrm{H}^1_{\mathrm{fl}}(X, \mathbb{G}(n)_A) \xrightarrow{\mathrm{H}^1(\psi_{\mathfrak{p}})} \mathrm{H}^1_{\mathrm{fl}}(X, \overline{\operatorname{Ker}\psi})\right]. \end{aligned}$$

The explicit correspondence on the isomorphism above is obtained as follows: for any

$$\overline{g} \in \operatorname{Coker}\left[\mathrm{H}^0_{\mathrm{fl}}(X, \mathbb{G}(n)_A) \overset{\mathrm{H}^0(\psi_{\mathfrak{p}})}{\longrightarrow} \mathrm{H}^0_{\mathrm{fl}}(X, \overline{\operatorname{Ker}\psi})\right]$$

and any

$$s^*(\operatorname{Res}_{B/A}\mathbb{G}_{m,B}) \in \operatorname{Ker}\left[\mathrm{H}^1_{\mathrm{fl}}(X, \mathbb{G}(n)_A) \overset{\mathrm{H}^1(\psi_{\mathfrak{p}})}{\longrightarrow} \mathrm{H}^1_{\mathrm{fl}}(X, \overline{\operatorname{Ker}\psi})\right]$$

(see Section 4), we have the commutative diagram

$$\begin{tikzcd}
\rho^{-1}(\{1\} \times X) \arrow[r] \arrow[d] & s^*(\operatorname{Res}_{B/A}\mathbb{G}_{m,B}) \arrow[r, "\rho"] \arrow[d] & \psi_{\mathfrak{p}*}s^*(\operatorname{Res}_{B/A}\mathbb{G}_{m,B}) \arrow[d] \\
X \arrow[r, equal] & X \arrow[r, equal] & X.
\end{tikzcd}$$

Note that $\psi_{\mathfrak{p}*}s^*(\operatorname{Res}_{B/A}\mathbb{G}_{m,B}) \cong \overline{\operatorname{Ker}\psi} \times X$ and $\iota_*(\rho^{-1}(\{1\} \times X)) \cong s^*(\operatorname{Res}_{B/A}\mathbb{G}_{m,B})$ (cf. See [16] for details). Furthermore $G_{a,b}$, $\mathbb{G}(n)_A$ and $\overline{\operatorname{Ker}\psi}$ act on $\rho^{-1}(\{1\} \times X)$, $s^*(\operatorname{Res}_{B/A}\mathbb{G}_{m,B})$ and $\psi_{\mathfrak{p}*}s^*(\operatorname{Res}_{B/A}\mathbb{G}_{m,B})$ respectively. Then we have

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

where the operation "+" is on $\mathrm{H}^1_{\mathrm{fl}}(X, G_{a,b})$.

The discussion above can be generalized to the case of $n|(p-1)$. In other words, we have torsors for $\overline{\operatorname{Ker}\psi_{\mathfrak{p}}}$.

Bibliography

[1] M. Artin, A. Grothendieck and J. L. Verdier, *Théorie des Topes et Cohomologie Étale des Schémas(SGA4)*, Tome 1-3, Lecture Notes in Mathematics, vol. 269, 270, 305, Springer, Berlin Heidellberg New York, 1972, 1973.

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

[3] N. G. de Bruijn, *On the factorization of cyclic groups*, Nederl. Akad. Wetensch. Proc. Ser. A 56(=Indagationes Math. 15)(1953), pp.370-377.

[4] N. Bourbaki, *Algèbre Commutative, Eléments de Math, 27, 28, 30, 31*, Hermann, Paris, 1961-65.

[5] M. Demazure and P. Gabriel, *Groupes Algébriques, tomeI: Géométrie Algébrique, Généralités, Groupes Commutatifs*, Masson & Cie, North-Holland, 1970.

[6] U. Görtz and T. Wedhorn, *Algebraic Geometry I: Schemes With Examples and Exercises*, Vieweg+Teubner Verlag, Germany, 2010.

[7] Y. Koide, *On the Torsors for General Twisted Finite Group Schemes of Prime Order*, Preprint, 2012. (to appear in Journal of Algebra, Number Theory and Applications.)

[8] Y. Koide and T. Sekiguchi, *On the Cyclotomic Twisted Torus*, Far East Journal of Mathematical Sciences, vol.72, No. 2(2013), pp.201-224.

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

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

[11] F. Oort and J. Tate, *Group Schemes of Prime Order*, Annales Scientifiques de l'É.N.S., 4^e série, tome3, 1970, pp.1-21.

[12] L. G. Roberts, *The Flat Cohomology of Group Schemes of Rank p*, American Journal of Mathematics, Vol.95, No.3(Autumn, 1973), pp.688-702.

[13] K. Rubin and A. Silverberg, *Torus-based cryptography*, in *Advances in Cryptography-CRYPTO 2003*. Lect. Notes in Comp. Sci. vol.2729(Springer, Berlin, 2003), pp.349-365.

[14] K. Rubin and A. Silverberg, *Algebraic tori in cryptoraphy*, in High Primes and Misdemeanours: lectures in honour of the 60th birthday of Hugh Cowie Williams, Fields Institute Communications Series 41, American Mathematical Society, Providence, RI (2004), pp.317-326.

[15] K. Rubin and A. Silverberg, *Using abelian vaieties to improve pairing-based cryptography*, J. Cryptol.(2009)22 pp.330-364.

[16] T. Sekiguchi and Y. Toda, *On the cyclotomic twisted torus and some torsors*, Preprint, 2012.

[17] J.P. Serre, *Local Fields*, Graduate Texts in Mathematics, No.67, Springer-Verlag, New York, 1979.

[18] V. E. Voskresenskii, *Algebraic groups and their birational invariatns*, Translations of Mathematical Monographs 179, American Mathematical Society. Providence, RI, 1998.

[19] B. L. van der Waerden, *Algebra, I/II*, Heidelberger Taschenbücher 12/23, Springer Verlag, Berlin, Heidelberg andNew York, 1966/67; (English translation), Fredelick Unger, New York, 1970.

[20] L. C. Washington, *Introduction to Cyclotomic Fields*, 2nd ed., Graduate Texts in Mathematics, No.83, Springer-Verlag, New York, 1997.

[21] W. C. Waterhouse, *Introduction to affine group schemes*, Graduate Texts in Mathematics, No.66, Springer-Verlag, New York, 1979.

[22] A. Weil, *Adeles and Algebraic Groups*, 2nd ed., Progr. Math., Vol. 23, Birkhäuser, Boston, 1982.

Appendix A

A.1 On the cyclotomic polynomial

In this section, we prove that for each positive integer n the cyclotomic polynomial $\Phi_n(X)$ can be written down as a linear combination of $F_i(X)$ over $\mathbb{Z}[X]$. There are two key facts in our proof. The first one is the well-known fact that $\mathcal{O} \cap \mathbb{Q} = \mathbb{Z}$, where $\mathcal{O}$ is the set of algebraic integers. The second one is Newton's interpolation formula. We summarize these things as the following three lemmas to prove our main result.

Lemma 12. *Suppose that $\alpha_0, \ldots, \alpha_n \in \mathcal{O}$. Let $f(X) = a_0 + a_1(X - \alpha_0) + a_2(X - \alpha_0)(X - \alpha_1) + \cdots + a_n(X - \alpha_0)\cdots(X - \alpha_{n-1})$ and b_i the coefficients of X^i of $f(X)$ for each $i = 0, 1, \ldots, n$. Then all a_i belong to the set of algebraic integers $\mathcal{O}$ if and only if all b_i belong to the set of algebraic integers $\mathcal{O}$.*

Proof. Assume that $b_0, \ldots, b_n$ belong to $\mathcal{O}$. Dividing $f(X)$ by $X - \alpha_0$ we have

$$\begin{aligned} f(X) = \{&a_1 + a_2(X - \alpha_1) + a_3(X - \alpha_1)(X - \alpha_2) + \cdots \\ &\cdots + a_n(X - \alpha_1)\cdots(X - \alpha_{n-1})\}(X - \alpha_0) + a_0. \end{aligned}$$

Thus a_0 is represented by b_i's and α_i's , so a_0 is in $\mathcal{O}$. Moreover the quotient $a_1 + a_2(X - \alpha_1) + a_3(X - \alpha_1)(X - \alpha_2) + \cdots + a_n(X - \alpha_1)\cdots(X - \alpha_{n-1})$ belongs to $\mathcal{O}[X]$.

Continuing such process, we can easily prove that $a_i \in \mathcal{O}$. Conversely if all b_i are $\mathcal{O}$ then all a_i are $\mathcal{O}$ clearly. □

Now we briefly review Newton's interpolation formula. For details, one can refer to B. L. van der Waerden [19]. Given $n+1$ distinct elements $\alpha_0, \ldots, \alpha_n$ and $n+1$ elements $\beta_0, \ldots, \beta_n$ belonging to some field, we can construct the unique polynomial f of degree at most n such that $f(\alpha_i) = \beta_i$ for $i = 0, \ldots, n$. Let $f(X) = a_0 + a_1(X - \alpha_0) + a_2(X - \alpha_0)(X - \alpha_1) + \cdots + a_n(X - \alpha_0) \cdots (X - \alpha_{n-1})$. We set $f_1(X_0) = f(X_0)$. For each $k > 0$, we define a polynomial $f_{k+1}(X_k, \ldots, X_0)$ inductively by

$$f_{k+1}(X_k, \ldots, X_0) := \frac{f_k(X_k, \ldots, X_1) - f_{k-1}(X_{k-1}, \ldots, X_0)}{X_k - X_0}.$$

Then $a_0, \ldots, a_n$ are determined by

$$a_k = f_{k+1}(\alpha_k, \ldots, \alpha_0)$$

for $k = 0, \ldots, n$. We call the right side of the above equation the k-th difference quotient. Note that the k-th difference quotient is independent of the order of $\alpha_0, \ldots, \alpha_k$.

The following lemma plays an important role to prove Proposition 15.

Lemma 13. *Let $n+1$ distinct elements $\xi_0, \xi_1, \ldots, \xi_n \in \mathcal{O}$ and $A(X)$ be a polynomial of degree n with the form: $A(X) = a_0 + a_1(X - \xi_0) + a_2(X - \xi_0)(X - \xi_1) + \cdots + a_n(X - \xi_0) \cdots (X - \xi_{n-1})$. If there exists $G_1(X) \in \mathcal{O}[X]$ such that $G_1(\xi_i) = A(\xi_i)$ for all $i = 0, 1, \ldots, n$, then the k-th difference quotient $A_{k+1}(\xi_k, \xi_{k-1}, \ldots, \xi_0)(= a_k) \in \mathcal{O}$ for all $i = 0, 1, \ldots, n$.*

Proof. We are going to give a proof by induction on $i = 1, 2, \ldots, n$. By Newton's interpolation formula, We have

$$A_2(\xi_i, \xi_{i-1}) = \frac{A(\xi_i) - A(\xi_{i-1})}{\xi_i - \xi_{i-1}} = \frac{G_1(\xi_i) - G_1(\xi_{i-1})}{\xi_i - \xi_{i-1}}$$

for $i = 1, \cdots, n$. Replacing ξ_j with ξ_{j-1}, the numerator of $A_2(\xi_j, \xi_{j-1})$ equals to 0. Thus $G_1(\xi_j) - G_1(\xi_{j-1})$ has the factor $\xi_j - \xi_{j-1}$ for all $j = 1, 2, \ldots, n$, so we can write $A_2(\xi_j, \xi_{j-1})$ as a polynomial in ξ_j and ξ_{j-1} for all $j = 1, 2, \ldots, n$. It is that for all $j = 1, 2, \ldots, n$, there exists a polynomial $G_2(X_1, X_0)$ such that $G_2(\xi_j, \xi_{j-1}) = A_2(\xi_j, \xi_{j-1})$. In particular, the first difference quotient $A_2(\xi_1, \xi_0) \in \mathcal{O}$. Suppose that we have verified our claim for $k-1$, that is, we suppose there exists $G_k(X_{k-1}, X_{k-2}, \ldots, X_0)$ such that $G_k(\xi_{k+j-1}, \xi_{k+j-2}, \ldots, \xi_j) = A_k(\xi_{k+j-1}, \xi_{k+j-2}, \ldots, \xi_j)$ for all $j = 0, 1, \ldots, n-k+1$. By Newton's interpolation formula, we obtain

$$\begin{aligned} & A_{k+1}(\xi_{k+i+1}, \xi_{k+i}, \ldots, \xi_i) \\ & \quad = \frac{A_k(\xi_{k+i}, \xi_{k+i-1}, \ldots, \xi_{i+1}) - A_k(\xi_{k+i-1}, \xi_{k+i-2}, \ldots, \xi_i)}{\xi_{k+i} - \xi_i} \\ & \quad = \frac{G_k(\xi_{k+i}, \xi_{k+i-1}, \ldots, \xi_{i+1}) - G_k(\xi_{k+i-1}, \xi_{k+i-2}, \ldots, \xi_i)}{\xi_{k+i} - \xi_i} \end{aligned}$$

for $i = 0, 1, \ldots, n-k$. Replacing ξ_{k+j-1} with ξ_{j-1}, the numerator of $A_{k+1}(\xi_{k+j-1}, \xi_{k+j-2}, \ldots, \xi_{j-1})$ equals to 0. Thus

$$G_k(\xi_{k+j-1}, \xi_{k+j-2}, \ldots, \xi_j) - G_k(\xi_{k+j-2}, \xi_{k+j-3}, \ldots, \xi_{j-1})$$

has the factor $\xi_{k+j-1} - \xi_{j-1}$ for all $j = 1, 2, \ldots, n-k+1$, so we can write $A_{k+1}(\xi_{k+j-1}, \xi_{k+j-2}, \ldots, \xi_{j-1})$ as a polynomial in $\xi_{k+j-1}, \ldots, \xi_j$ and ξ_{j-1} for all $j = 1, 2, \ldots, n-k+1$. We easily see that for all $j = 1, 2, \ldots, n-k+1$ there exists a polynomial $G_{k+1}(X_k, X_{k-1}, \ldots, X_0)$ such that $G_{k+1}(\xi_{k+j}, \xi_{k+j-1}, \ldots, \xi_j) = A_{k+1}(\xi_{k+j}, \xi_{k+j-1}, \ldots, \xi_j)$. In particular the k-th difference quotient $A_{k+1}(\xi_k, \xi_{k-1}, \ldots, \xi_0) \in \mathcal{O}$, which completes the proof. □

Lemma 14. *Let $f(X)$ and $g(X)$ be polynomials with coefficients in $\mathbb{Q}$. We denote by $d(X)$ the greatest common divisor of $f(X)$ and $g(X)$. By the extended Euclidian* *algorithm, there exist polynomials $A(X)$ and $B(X)$ such that $d(X) = A(X)f(X) + B(X)g(X)$. Then we have the following inequalities*

$$\deg A(X) < \deg g(X) - \deg d(X),$$

$$\deg B(X) < \deg f(X) - \deg d(X).$$

Proof. Since the proof is straightforward, we omit it. □

Let n be a positive integer, $n = p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r}$ with distinct primes $p_1, p_2, \ldots, p_r$ and positive integers $e_1, e_2, \ldots, e_r$, and $n_i = \dfrac{n}{p_i}$ for each $i = 1, 2, \ldots, r$. Set $F_i(X) = \dfrac{X^n - 1}{X^{n_i} - 1}$ for each $i = 1, 2, \ldots, r$. In the last section, we know that for all n, the cyclotomic polynomial $\Phi_n(X)$ is a $\mathbb{Q}[X]$-linear combination of $F_i(X)$'s.

Proposition 15. *Notations are as above. For each n, the cyclotomic polynomial $\Phi_n(X)$ is a $\mathbb{Z}[X]$-linear combination of $F_i(X)$'s.*

Proof. Let ζ_n be a primitive n-th root of unity. For simplicity, we denote ζ_n by ζ. Then we can write down $F_i(X) = \dfrac{\prod_{a \in \mathbb{Z}/n\mathbb{Z}} (X - \zeta^a)}{\prod_{b \in \mathbb{Z}/n_i\mathbb{Z}} (X - \zeta^{p_i b})}$ for each $i = 1, 2, \ldots, n$. We denote by $F_{k!}(X)$ the greatest common divisor of $F_1(X), \ldots, F_{k-1}(X)$ and $F_k(X)$, that is, $(F_1(X), F_2(X), \ldots, F_k(X))$
$= F_{k!}(X)$. If $k = r$, then $F_{r!}(X)$ is equal to $\Phi_n(X)$.

We are going to give a proof by induction on k. If $k = 2$, we have that $F_{2!}(X) = \dfrac{(X^n - 1)(X^{n_{12}} - 1)}{(X^{n_1} - 1)(X^{n_2} - 1)}$, where we set $n_{12} = \dfrac{n}{p_1 p_2}$. By the extended Euclidian algorithm and Lemma 14, there exist $A_2(X)$ and $B_2(X)$ belonging to $\mathbb{Q}[X]$ such that

$$A_2(X)F_1(X) + B_2(X)F_2(X) = F_{2!}(X), \tag{A.1}$$

$\deg A_2(X) < \deg F_2(X) - \deg F_{2!}(X) = n_1 - n_{12}$ and $\deg B_2(X) < \deg F_1(X) - \deg F_{2!}(X)$. Note that $A_2(X)$ belongs to $\mathbb{Z}[X]$ if and only if $B_2(X)$ belongs to $\mathbb{Z}[X]$, and so to give a proof we have only to verify just that the coefficients of $A_2(X)$ are in $\mathbb{Z}$. We substitute $\zeta^{p_1 b}$ to X of (A.1), where b is in $\mathbb{Z}/n_1\mathbb{Z}$ and it is coprime to p_2 and so the number of b's is $n_1 - n_{12}$. Then we have

$$A_2(\zeta^{p_1 b}) = \frac{\zeta^{p_1 b n_{12}} - 1}{\zeta^{p_1 b n_2} - 1}.$$

We denote the primitive p_i-th root of unity by ζ_{p_i}, that is $\zeta_{p_i} = \zeta^{n_i}$. Then we have

$$\begin{aligned} A_2(\zeta^{p_1 b}) &= \frac{\zeta_{p_2}^{b} - 1}{\zeta_{p_2}^{p_1 b} - 1} \\ &= \frac{\zeta_{p_2}^{p_1' p_1 b} - 1}{\zeta_{p_2}^{p_1 b} - 1} \\ &= \zeta^{p_1 b n_2 (p_1' - 1)} + \zeta^{p_1 b n_2 (p_1' - 2)} + \cdots + 1 \in \mathcal{O}, \end{aligned}$$

since there exists p_1' such that $p_1' p_1 \equiv 1 \mod p_2$. We recall that the number of $A_2(\zeta^{p_2 b})$'s is greater than the degree of $A_2(X)$. Therefore by Newton's interpolation formula, we uniquely determine the coefficients of $A_2(X)$. Since all $A_2(\zeta^{p_1 b})$ are polynomials in $\zeta^{p_1 b}$ respectively we prove that the coefficients of $A_2(X)$ are in $\mathcal{O}$ by Lemma 13. Next suppose that we have verified our claim for every $i \leq k - 1$. By the extended Euclidian algorithm, there exist $A_k(X)$ and $B_k(X)$ belonging to $\mathbb{Q}[X]$ such that

$$A_k(X)F_k(X) + B_k(X)F_{(k-1)!}(X) = F_{k!}(X), \tag{A.2}$$

$$\begin{aligned} \deg A_k(X) &< \deg F_{(k-1)!}(X) - \deg F_{k!}(X) \\ &= \phi(p_1^{e_1} \cdots p_{k-1}^{e_{k-1}}) p_k^{e_k - 1} p_{k+1}^{e_{k+1}} \cdots p_r^{e_r} \end{aligned}$$

and $\deg B_k(X) < \deg F_k(X) - \deg F_{k!}(X)$, where ϕ is the Euler function. Note that $A_k(X)$ belongs to $\mathbb{Z}[X]$ if and only if $B_k(X)$ belongs to $\mathbb{Z}[X]$, and so to give a proof we have only to verify just that the coefficients of $A_k(X)$ are in $\mathbb{Z}$. We substitute $\zeta^{p_k b}$

to X of (A.2), where b is in $\mathbb{Z}/n_k\mathbb{Z}$ and it is coprime to $p_1 \cdots p_{k-1}$ and so the number of b's is $\phi(p_1^{e_1} \cdots p_{k-1}^{e_{k-1}}) p_k^{e_k - 1} p_{k+1}^{e_{k+1}} \cdots p_r^{e_r}$. Then we have the following equation

$$A_k(\zeta^{bp_k}) p_k = F_{k!}(\zeta^{bp_k}).$$

We set $n_{i_1 i_2 \cdots i_s} = \dfrac{n}{p_{i_1} p_{i_2} \cdots p_{i_s}}$. Since we describe

$$\begin{aligned} F_{k!}(X) =& (X^n - 1) \prod_{i=1,\cdots,k} (X^{n_i} - 1)^{-1} \prod_{i<j} (X^{n_{ij}} - 1) \cdots \\ & \cdots \prod_{i_1 < \cdots < i_{k-1}} (X^{n_{i_1 \cdots i_{k-1}}} - 1)^{(-1)^{k-1}} (X^{n_{1 \cdots k}} - 1)^{(-1)^k}, \end{aligned}$$

we consider the values of $\dfrac{X^n - 1}{X^{n_k} - 1}$, $\dfrac{X^{n_{i_1 \cdots i_s}} - 1}{X^{n_{i_1 \cdots i_s k}} - 1}$ and $\dfrac{X^{n_{i_1 \cdots i_t k}} - 1}{X^{n_{i_1 \cdots i_t}} - 1}$, where s is even and t is odd. Since $F_k(X) = \dfrac{X^n - 1}{X^{n_k} - 1} = X^{n_k(p_k - 1)} + X^{n_k(p_k - 2)} + \cdots + 1$, for $\dfrac{X^n - 1}{X^{n_k} - 1}$ we get $F_k(\zeta^{bp_k}) = p_k$. The values of $\dfrac{X^{n_{i_1 \cdots i_s}} - 1}{X^{n_{i_1 \cdots i_s k}} - 1}$ and $\dfrac{X^{n_{i_1 \cdots i_t k}} - 1}{X^{n_{i_1 \cdots i_t}} - 1}$ substituting ζ^{bp_k} to X are represented by the polynomials on ζ^{bp_k} respectively as follows

$$\begin{aligned} \frac{(\zeta^{bp_k})^{n_{i_1 \cdots i_s}} - 1}{(\zeta^{bp_k})^{n_{i_1 \cdots i_s k}} - 1} &= \frac{(\zeta^{bp_k})^{p_k n_{i_1 \cdots i_s k}} - 1}{(\zeta^{bp_k})^{n_{i_1 \cdots i_s k}} - 1} \\ &= (\zeta^{bp_k})^{n_{i_1 \cdots i_s k}(p_k - 1)} + (\zeta^{bp_k})^{n_{i_1 \cdots i_s k}(p_k - 2)} + \cdots + 1 \end{aligned}$$

and

$$\begin{aligned} \frac{(\zeta^{bp_k})^{n_{i_1 \cdots i_t k}} - 1}{(\zeta^{bp_k})^{n_{i_1 \cdots i_t}} - 1} &= \frac{\zeta_{p_{i_1} \cdots p_{i_t}}^{b} - 1}{\zeta_{p_{i_1} \cdots p_{i_t}}^{bp_k} - 1} \\ &= \frac{\zeta_{p_{i_1} \cdots p_{i_t}}^{bp_k p'_k} - 1}{\zeta_{p_{i_1} \cdots p_{i_t}}^{bp_k} - 1} \\ &= (\zeta^{bp_k})^{n_{i_1 \cdots i_t}(p'_k - 1)} + (\zeta^{bp_k})^{n_{i_1 \cdots i_t}(p'_k - 2)} + \cdots + 1 \end{aligned}$$

since there exists p'_k such that $p_k p'_k \equiv 1 \mod p_{i_1} \cdots p_{i_t}$. Thus we obtain $A_k(\zeta^{bp_k})$ represented by the polynomial of ζ^{bp_k} and so it is in $\mathcal{O}$. Therefore we can verify that the coefficients of $A_k(X)$ belong to $\mathbb{Z}$ by Lemma 13, which completes the proof. □

A.2 Defining equations of some subgroup scheme of $\mathbb{G}_{m,B}^m \times \mathbb{G}_{m,B}^m$

In this section, we give the explicit defining equations of the subgroup scheme $\operatorname{Ker}\psi \subset \mathbb{G}_{m,B}^m \times \mathbb{G}_{m,B}^m$. We recall that $\psi : \mathbb{G}_{m,B}^m \times \mathbb{G}_{m,B}^m \to \mathbb{G}_{m,B}^m \times \mathbb{G}_{m,B}^m$; $(\boldsymbol{u}, \boldsymbol{v}) \mapsto (\boldsymbol{u}^\beta \boldsymbol{v}^{-\alpha}, \boldsymbol{u}^{\beta'} \boldsymbol{v}^{-\alpha'})$ (see Section 5.3).

Since α, β, α' and β' are in $\mathbb{Z}[\zeta]$, we set

$$\alpha = \alpha(\zeta) := a_{m-1}\zeta^{m-1} + a_{m-2}\zeta^{m-2} + \cdots + a_1\zeta + a_0$$

$$\beta = \beta(\zeta) := b_{m-1}\zeta^{m-1} + b_{m-2}\zeta^{m-2} + \cdots + b_1\zeta + b_0$$

and α', β' replacing a_j's, b_j's for a'_j's, b'_j's respectively. Let $\Phi_n(X) = X^m + p_{m-1}X^{m-1} + \cdots + p_1X + p_0$ be the cyclotomic polynomial, satisfied by ζ. The matrix I representing of ζ forms

$$\begin{pmatrix} 0 & \cdots & 0 & -p_{m-1} \\ 1 & \ddots & \vdots & -p_{m-2} \\ & \ddots & 0 & \vdots \\ & & 1 & -p_0 \end{pmatrix}$$

with respect to the standard $\mathbb{Z}$-basis of $\mathbb{Z}^m$. (See Section 3.) For $k \in \mathbb{Z}$, we denote by $\boldsymbol{i}_k$ the last column of $I^k \in \mathrm{GL}_m(\mathbb{Z})$ and for $j = 1, 2, \ldots, m$, by i_k^j the j-th entry of $\boldsymbol{i}_k$. We know that $i_1^j = -p_{m-j}$ for each $j = 0, \ldots, m-1$ and $\boldsymbol{i}_1 = \begin{pmatrix} -p_{m-1} \\ -p_{m-2} \\ \vdots \\ -p_0 \end{pmatrix}$. We set $\boldsymbol{e}_j = \begin{pmatrix} 0 \\ \vdots \\ 1 \\ \vdots \\ 0 \end{pmatrix}$ of which the j-th entry is one but the others are zero. Then we have

$I = (\boldsymbol{e}_2\ \boldsymbol{e}_3\ \cdots\ \boldsymbol{e}_m\ \boldsymbol{i}_1)$. By straightforward calculating $I^k = I^{k-1}I$, we have

$$i_k^j = \begin{cases} \sum_{l=1}^{k-1} i_l^j \cdot i_1^{k-1-l} & m-k+1 \leq j \leq m-1 \\ i_1^{j+k-1} + \sum_{l=1}^{k-1} i_l^j \cdot i_1^{k-1-l} & 1 \leq j \leq m-k. \end{cases}$$

Or by straightforward calculating $I^k = II^{k-1}$, we have

$$i_k^j = \begin{cases} i_1^{m-1} \cdot i_{k-1}^0 & j = m-1 \\ i_{k-1}^{j+1} + i_1^j \cdot i_{k-1}^0 & 1 \leq j \leq m-2. \end{cases}$$

Note that these recurrent formulas are equal to each others. Thus we have $I^k = (\boldsymbol{e}_{k+1}\ \boldsymbol{e}_{k+2}\ \cdots\ \boldsymbol{e}_m\ \boldsymbol{i}_1\ \boldsymbol{i}_2\ \cdots\ \boldsymbol{i}_k)$ for each $k = 1, \ldots, m-1$. So we obtain the matrix $\alpha(I)$ corresponding to $\alpha(\zeta)$ as follows,

$$\alpha(I) = \left(\sum_{l=0}^{m-1} a_l \boldsymbol{e}_{l+1} \quad a_{m-1}\boldsymbol{i}_1 + \sum_{l=2}^{m} a_{l-2}\boldsymbol{e}_l \quad \cdots \quad \sum_{l=1}^{m-1} a_l \boldsymbol{i}_l + a_0 \boldsymbol{e}_m \right)$$

in which the k-th column is $\sum_{l=1}^{k-1} a_{m-k+l}\boldsymbol{i}_l + \sum_{l=k}^{m} a_{l-k}\boldsymbol{e}_l$ for $k = 2, \ldots, m$. We see that the first column and the k-th column are respectively

$$\begin{pmatrix} a_0 \\ a_1 \\ \vdots \\ a_{m-1} \end{pmatrix} \text{ and } \begin{pmatrix} \sum_{l=1}^{k-1} a_{m-l} \cdot i_{k-l}^{m-1} \\ \vdots \\ \sum_{l=1}^{k-1} a_{m-l} \cdot i_{k-l}^{m-k+1} \\ \sum_{l=1}^{k-1} a_{m-l} \cdot i_{k-l}^{m-k} + a_0 \\ \vdots \\ \sum_{l=1}^{k-1} a_{m-l} \cdot i_{k-l}^{0} + a_{m-k} \end{pmatrix}.$$

And we obtain the matrices corresponding the others by substituting a_j's for the coefficients of them. Fix any $(\boldsymbol{u}, \boldsymbol{v}) \in (\operatorname{Ker} \psi)(R)$ for A-algebra R. We have

$$\begin{cases} \boldsymbol{v}^{\alpha(I)} = \boldsymbol{u}^{\beta(I)}, \\ \boldsymbol{v}^{\alpha'(I)} = \boldsymbol{u}^{\beta'(I)}. \end{cases}$$

We set $\boldsymbol{u} = (u_1, u_2, \ldots, u_m)$ and $\boldsymbol{v} = (v_1, v_2, \ldots, v_m)$. Comparing the two sides of

$\boldsymbol{v}^{\alpha(I)} = \boldsymbol{u}^{\beta(I)}$, we have the equations

$$\left\{\begin{aligned}
\prod_{j=1}^{m} v_j^{a_{j-1}} &= \prod_{j=1}^{m} u_j^{b_{j-1}}\\
v_1^{a_{m-1}i_1^{m-1}} \prod_{j=2}^{m} v_j^{a_{m-1}i_1^{m-j}+a_{j-2}} &= u_1^{b_{m-1}i_1^{m-1}} \prod_{j=2}^{m} u_j^{b_{m-1}i_1^{m-j}+b_{j-2}}\\
&\vdots\\
\prod_{j=1}^{k-1} v_j^{\sum_{l=1}^{k-1} a_{m-l}i_{k-l}^{m-j}} \prod_{j=k}^{m} v_j^{\sum_{l=1}^{k-1} a_{m-l}i_{k-l}^{m-j}+a_{j-k}} &\\
&= \prod_{j=1}^{k-1} u_j^{\sum_{l=1}^{k-1} b_{m-l}i_{k-l}^{m-j}} \prod_{j=k}^{m} u_j^{\sum_{l=1}^{k-1} b_{m-l}i_{k-l}^{m-j}+b_{j-k}}\\
&\vdots\\
\left(\prod_{j=1}^{m-1} v_j^{\sum_{l=1}^{m-1} a_{m-l}i_{m-1}^{m-j}}\right) v_m^{\sum_{l=1}^{m-1} a_{m-l}i_{m-l}^{0}+a_0} &\\
&= \left(\prod_{j=1}^{m-1} u_j^{\sum_{l=1}^{m-1} b_{m-l}i_{m-1}^{m-j}}\right) u_m^{\sum_{l=1}^{m-1} b_{m-l}i_{m-l}^{0}+b_0}.
\end{aligned}\right.$$

Similarly, from $\boldsymbol{v}^{\alpha'(I)} = \boldsymbol{u}^{\beta'(I)}$ we have the equations of u_j's and v_j's by substituting a_j's and b_j's for a'_j's and b'_j's respectively. We set

$$f_1(X_1,\dots,X_m,Y_1,\dots,Y_m) = \prod_{j=1}^{m} Y_j^{a_{j-1}} - \prod_{j=1}^{m} X_j^{b_{j-1}},$$

and

$$\begin{aligned}
f_k(X_1,\dots,X_m,Y_1,\dots,Y_m) &= \prod_{j=1}^{k-1} Y_j^{\sum_{l=1}^{k-1} a_{m-l}i_{k-l}^{m-j}} \prod_{j=k}^{m} Y_j^{\sum_{l=1}^{k-1} a_{m-l}i_{k-l}^{m-j}+a_{j-k}}\\
&\quad - \prod_{j=1}^{k-1} X_j^{\sum_{l=1}^{k-1} b_{m-l}i_{k-l}^{m-j}} \prod_{j=k}^{m} X_j^{\sum_{l=1}^{k-1} b_{m-l}i_{k-l}^{m-j}+b_{j-k}}
\end{aligned}$$

for each $k = 2,\dots,m$, and substituting a_j's and b_j's for a'_j's and b'_j's respectively gives the definitions of $f'_1(X_1,\dots,X_m,Y_1,\dots,Y_m)$ and $f'_k(X_1,\dots,X_m,Y_1,\dots,Y_m)$ for each $k = 2, \ldots, m$. Then we have the equalities

$$\begin{aligned}(\operatorname{Ker}\psi)(R) &= \left\{(\boldsymbol{u}, \boldsymbol{v}) \in \mathbb{G}_{m,B}^m(R) \times \mathbb{G}_{m,B}^m(R) \mid \boldsymbol{v}^{\alpha} = \boldsymbol{u}^{\beta}, \boldsymbol{v}^{\alpha'} = \boldsymbol{u}^{\beta'}\right\} \\ &= \left\{(\boldsymbol{u}, \boldsymbol{v}) \in \mathbb{G}_{m,B}^m(R) \times \mathbb{G}_{m,B}^m(R) \mid 0 = f_j(\boldsymbol{u}, \boldsymbol{v}) = f'_j(\boldsymbol{u}, \boldsymbol{v}) \ \forall j\right\} \\ &\cong \operatorname{Hom}_{B\text{-alg}}\left(B\left[X_1, \ldots, X_m, Y_1, \ldots, Y_m, \frac{1}{\prod_{j=1}^m X_j Y_j}\right]/\boldsymbol{F}, R\right),\end{aligned}$$

where the ideal $\boldsymbol{F}$ is generated by $f_j(X_1, \ldots, X_m, Y_1, \ldots, Y_m)$ and $f'_j(X_1, \ldots, X_m, Y_1, \ldots, Y_m)$ for $j = 1, 2, \ldots, m$. Thus the defining equations of $\operatorname{Ker}\psi$ are $f_1(X_1, \ldots, X_m, Y_1, \ldots, Y_m)$, $f_k(X_1, \ldots, X_m, Y_1, \ldots, Y_m)$'s, $f'_1(X_1, \ldots, X_m, Y_1, \ldots, Y_m)$ and $f'_k(X_1, \ldots, X_m, Y_1, \ldots, Y_m)$'s, namely,

$$\operatorname{Ker}\psi = \operatorname{Spec}\left(B\left[X_1, \ldots, X_m, Y_1, \ldots, Y_m, \frac{1}{\prod_{j=1}^m X_j}, \frac{1}{\prod_{j=1}^m Y_j}\right]/\boldsymbol{F}\right),$$

where $\boldsymbol{F}$ is the ideal generated by $f_1(X_1, \ldots, X_m, Y_1, \ldots, Y_m)$, $f_k(X_1, \ldots, X_m, Y_1, \ldots, Y_m)$'s, $f'_1(X_1, \ldots, X_m, Y_1, \ldots, Y_m)$ and $f'_k(X_1, \ldots, X_m, Y_1, \ldots, Y_m)$'s.