ARTICLE IN PRESS
JPAA:106906

Journal of Pure and Applied Algebra ••• (••••) ••••••

Contents lists available at ScienceDirect

Journal of Pure and Applied Algebra

www.elsevier.com/locate/jpaa

The Tate-Shafarevich groups of multinorm-one tori

T.-Y. Lee [a,b,*]

[a] *Technische Universität Dortmund, Fakultät für Mathematik, Lehrstuhl LSVI, Vogelpothsweg 87, 44227 Dortmund, Germany*
[b] *NTU-MATH, Astronomy Mathematics Building 5F, No. 1, Sec. 4, Roosevelt Rd., Taipei 10617, Taiwan, ROC*

ARTICLE INFO

Article history:
Received 18 November 2020
Received in revised form 27 July 2021
Available online xxxx
Communicated by V. Suresh

MSC:
11G35; 11R34; 12G05; 14G12; 14G25

Keywords:
Multinorm
Tori
Tate-Shafarevich groups
Local-global principles
Weak approximation
Brauer-Manin obstructions

ABSTRACT

Let k be a global field and L be a product of cyclic extensions of k. Let T be the torus defined by the multinorm equation $N_{L/k}(x) = 1$ and let $\hat{T}$ be its character group. The Tate-Shafarevich group and the algebraic Tate-Shafarevich group of $\hat{T}$ in degree 2 give obstructions to the Hasse principle and weak approximation for rational points on principal homogeneous spaces of T. We give concrete descriptions of these groups and provide several examples.

0. Introduction

Let k be a global field and fix a separable closure k_s of k. In the following all the separable extensions of k are considered as subfields of k_s.

Let K_i be a finite separable extension of k for $i = 0, ..., m$. Set $L = K_0 \times ... \times K_m$. Let $T_{L/k}$ be the torus defined by the multinorm equation:

$$N_{L/k}(t) = 1. \tag{0.1}$$

Denote by $\hat{T}_{L/k}$ the character group of $T_{L/k}$.

* Correspondence to: NTU-MATH, Astronomy Mathematics Building 5F, No. 1, Sec. 4, Roosevelt Rd., Taipei 10617, Taiwan, ROC.
E-mail address: tingyulee@ntu.edu.tw.

https://doi.org/10.1016/j.jpaa.2021.106906

Let Ω_k be the set of all places of k. Define

$$Ш^i(k, T_{L/k}) := \ker(H^i(k, T_{L/k}) \to \prod_{v \in \Omega_k} H^i(k_v, T_{L/k})). \tag{0.2}$$

It is well-known that the elements in $Ш^1(k, T_{L/k})$ are in one-to-one correspondence with the isomorphism classes of $T_{L/k}$-torsors which have k_v-points for all $v \in \Omega_k$. To be precise, let X_c be the variety defined by

$$N_{L/k}(t) = c, \tag{0.3}$$

where $c \in k^\times$. Suppose that X_c has a k_v-point for all $v \in \Omega_k$. Then X_c corresponds to an element $[X_c] \in Ш^1(k, T_{L/k})$. By Poitou-Tate duality, the class $[X_c]$ defines a map $Ш^2(k, \hat{T}_{L/k}) \to \mathbb{Q}/\mathbb{Z}$, which is the Brauer-Manin obstruction to the Hasse principle for the existence of rational points of X_c. Hence the group $Ш^2(k, \hat{T}_{L/k})$ is related to the local-global principle for multinorm equations.

For a Galois module M over k, define

$$Ш^i_\omega(k, M) := \{[C] \in H^i(k, M) \text{ such that } [C]_v = 0 \text{ for almost all } v \in \Omega_k.\}$$

It is clear that $Ш^i(k, \hat{T}_{L/k}) \subseteq Ш^i_\omega(k, \hat{T}_{L/k})$. The case $i = 2$ is the most interesting to us. In fact if $Ш^2_\omega(k, \hat{T}_{L/k}) = Ш^2(k, \hat{T}_{L/k})$, weak approximation holds for $T_{L/k}$ and hence for those X_c with a k-point ([8] Prop. 8.9 and Thm. 8.12).

The local-global principle and weak approximation for multinorm equations (0.3) have been extensively studied. One can see [7], [6], [4], [1] and [5] for recent developments on this topic. In this paper, we are interested in the groups $Ш^2(k, \hat{T}_{L/k})$ and $Ш^2_\omega(k, \hat{T}_{L/k})$ (and hence the group $Ш^2_\omega(k, \hat{T}_{L/k})/Ш^2(k, \hat{T}_{L/k})$). These groups measure the obstruction to the local-global principle for existence of rational points of X_c and the obstruction to weak approximation.

Under the assumption that L is a product of (not necessarily disjoint) cyclic extensions of *prime-power degrees*, we give a formula for $Ш^2_\omega(k, \hat{T}_{L/k})$ and $Ш^2(k, \hat{T}_{L/k})$. Briefly speaking, the group $Ш^2_\omega(k, \hat{T}_{L/k})$ is determined by the "maximal bicyclic field" M generated by subfields of K_i and $Ш^2(k, \hat{T}_{L/k})$ is determined by the "maximal bicyclic and locally cyclic subfield" of M. In combination with [1] Proposition 8.6, one can calculate the group $Ш^2(k, \hat{T}_{L/k})$ for L a product of cyclic extensions of arbitrary degrees. This generalizes the result in [1] §8. Furthermore we compute the bigger group $Ш^2_\omega(k, \hat{T}_{L/k})$ which is related to weak approximation. We give several concrete examples in the final section.

The paper is structured as follows. Section 1 introduces the notation. In Section 2 we give a combinatorial description of $Ш^2(k, \hat{T}_{L/k})$ and $Ш^2_\omega(k, \hat{T}_{L/k})$. In Section 3, we prove some preliminaries about cyclic extensions, which will be the main tools in the following sections. In Section 4-6, we define the *patching degree* and the *degree of freedom* in order to describe the generators of the group $Ш^2(k, \hat{T}_{L/k})$ (resp. $Ш^2_\omega(k, \hat{T}_{L/k})$). We give formulas for $Ш^2(k, \hat{T}_{L/k})$ and $Ш^2_\omega(k, \hat{T}_{L/k})$ in Section 7 and provide several examples in the last section.

Most part of this work is done under the support of Alexander von Humboldt-Stiftung. The author is grateful to the referee for valuable comments.

1. Notation and definitions

For a k-algebra A and a place $v \in \Omega_k$, we denote $A \otimes_k k_v$ by A^v.

A finite Galois extension F of k is said to be *locally cyclic* at v if $F \otimes_k k_v$ is a product of cyclic extensions of k_v. F is said to be locally cyclic if it is locally cyclic at all $v \in \Omega_k$.

A bicyclic extension F/k is a Galois extension with $\mathrm{Gal}(F/k)$ isomorphic to $\mathbb{Z}/n_1\mathbb{Z} \times \mathbb{Z}/n_2\mathbb{Z}$ where n_1, $n_2 > 1$ and $n_2 | n_1$.

Throughout this paper, we assume $\bigcap_{i=0}^{m} K_i = k$.

2. Preliminaries on algebraic tori

For a k-torus T, we denote by $\hat{T}$ its character group as a $\mathrm{Gal}(k_s/k)$-module.

Let A be a field and A' be a finite dimensional A-algebra. For an A'-torus T, we denote by $\mathrm{R}_{A'/A}(T)$ its Weil restriction to A. (For more details on Weil restriction, see [3] A.5.)

Let $N_{A'/A}$ be the norm map and denote by $T_{A'/A}$ the norm one torus $R^{(1)}_{A'/A}(\mathbb{G}_m)$.

We first prove some general facts about multinorm-one tori defined by finite separable extensions of k.

We recall the following well-known fact ([8] Lemma 1.9).

Lemma 2.1. *Let $\mathcal{G} = \mathrm{Gal}(k_s/k)$ and M be a permutation module of $\mathcal{G}$. Then $Ш^2_\omega(k, M) = 0$.*

Recall some notation defined in [1]. Denote the index set by $\mathcal{I} = \{1, ..., m\}$ and $\mathcal{I}' = \{0\} \cup \mathcal{I}$. In the following, we always assume that $m \geq 2$.

Set

- $K' = \prod_{i\in\mathcal{I}} K_i$,
- $L = \prod_{i\in\mathcal{I}'} K_i$,
- $E = K_0 \otimes_k K'$, and
- $E_i = K_0 \otimes_k K_i$.

The norm maps $N_{K_0/k} : K_0 \to k$ and $N_{K'/k} : K' \to k$ induce $N_{E/K'} : E \to K'$ and $N_{E/K_0} : E \to K_0$. Let $\phi : \mathrm{R}_{E/k}(\mathbb{G}_m) \to \mathrm{R}_{L/k}(\mathbb{G}_m)$ be defined by $\phi(x) = (N_{E/K_0}(x)^{-1}, N_{E/K'}(x))$. It is clear that the image of ϕ is contained in $T_{L/k}$. Moreover, ϕ is surjective onto $T_{L/k}$ as a map of algebraic groups (easily checked after base change to the separable closure k_s of k).

Consider the torus $S_{K_0,K'}$ defined by the exact sequence

$$1 \longrightarrow S_{K_0,K'} \longrightarrow \mathrm{R}_{E/k}(\mathbb{G}_m) \xrightarrow{\phi} T_{L/k} \longrightarrow 1 \ . \tag{2.1}$$

Note that $S_{K_0,K'}$ also fits in the exact sequence

$$1 \longrightarrow S_{K_0,K'} \longrightarrow \prod_{i\in I} \mathrm{R}_{K_i/k}(T_{E_i/K_i}) \xrightarrow{N_{E/K_0}} T_{K_0/k} \longrightarrow 1 \ . \tag{2.2}$$

Proposition 2.2. *Let K_0 be a cyclic extension of arbitrary degree. Then $Ш^2_\omega(k, \hat{T}_{K_0/k}) = 0$.*

Proof. Let σ be a generator of $\mathrm{Gal}(K_0/k)$. Consider the exact sequence

$$1 \to \mathbb{G}_m \to \mathrm{R}_{K_0/k}(\mathbb{G}_m) \to T_{K_0/k} \to 1,$$

where the map from $\mathrm{R}_{K_0/k}(\mathbb{G}_m)$ to $T_{K_0/k}$ sends x to $x/\sigma(x)$. Its dual sequence is

$$1 \to \hat{T}_{K_0/K} \to \mathrm{I}_{K_0/k}(\mathbb{Z}) \to \mathbb{Z} \to 1.$$

By Lemma 2.1 we have $Ш^2_\omega(k, \mathrm{I}_{K_0/k}(\mathbb{Z})) = 0$. As $H^1(k, \mathbb{Z}) = 0$, we have $Ш^2_\omega(k, \hat{T}_{K_0/k}) = 0$. $\square$

Please cite this article in press as: T.-Y. Lee, The Tate-Shafarevich groups of multinorm-one tori, J. Pure Appl. Algebra (2022), https://doi.org/10.1016/j.jpaa.2021.106906

Lemma 2.3. *We have*

(1) $Ш^2(k, \hat{T}_{L/k}) \simeq Ш^1(k, \hat{S}_{K_0,K'})$.
(2) $Ш^2_\omega(k, \hat{T}_{L/k}) \simeq Ш^1_\omega(k, \hat{S}_{K_0,K'})$.

Proof. The first statement is [1] Lemma 3.1.

We now prove (2). Consider the dual sequence of (2.1):

$$0 \longrightarrow \hat{T}_{L/k} \longrightarrow \mathrm{I}_{E/k}(\mathbb{Z}) \xrightarrow{\phi} \hat{S}_{K_0,K'} \longrightarrow 0 \ . \tag{2.3}$$

The exact sequence (2.3) gives rise to the following exact sequence:

$$0 \longrightarrow H^1(k, \hat{S}_{K_0,K'}) \xrightarrow{\delta} H^2(k, \hat{T}_{L/k}) \to H^2(k, \mathrm{I}_{E/k}(\mathbb{Z})) \ . \tag{2.4}$$

By Lemma 2.1, we have $Ш^2_\omega(k, \mathrm{I}_{E/k}(\mathbb{Z})) = 0$. Therefore $Ш^2_\omega(k, \hat{T}_{L/k})$ is in the image of δ. Let $[\theta]$ be an element in $H^1(k, \hat{S}_{K_0,K'})$ such that $\delta[\theta] \in Ш^2_\omega(k, \hat{T}_{L/k})$. As $H^1(k_v, \mathrm{I}_{E/k}(\mathbb{Z})) = 0$ for all $v \in \Omega_k$, the element $[\theta]_v = 0$ if $(\delta[\theta])_v = 0$. Hence $[\theta] \in Ш^1_\omega(k, \hat{S}_{K_0,K'})$. The lemma then follows. □

2.1. Combinatorial description of Tate-Shafarevich groups

From now on we assume that K_0 is a cyclic extension of degree p^{ϵ_0} and we denote by $K_0(f)$ the unique subfield of K_0 of degree p^f.

For all $i \in \mathcal{I}$, we set

- $p^{e_{0,i}} = [K_0 \cap K_i : k]$, and
- $e_i = \epsilon_0 - e_{0,i}$.

As K_0 is cyclic, for each $i \in I$, the algebra $K_0 \otimes_k K_i$ is a product of cyclic extensions of degree p^{e_i} of K_i. Without loss of generality, we assume that $e_i \geq e_{i+1}$. Since we assume that $K_0 \cap (\bigcap_i K_i) = k$, we have $e_{0,1} = 0$ and $e_1 = \epsilon_0$.

We can assume further that for any $i \neq j$, $K_j \nsubseteq K_i$. To see this, suppose that there are distinct i, j such that $K_j \subseteq K_i$. Set $J = \{0, 1, ..., m\} \setminus \{i\}$ and set $L' = \prod_{i \in J} K_i$. Then $T_{L/k} \simeq T_{L'/k} \times R_{K_i/k}(\mathbb{G}_m)$. By Lemma 2.1, $Ш^2(k, \hat{T}_{L/k}) \simeq Ш^2(k, \hat{T}_{L'/k})$ and $Ш^2_\omega(k, \hat{T}_{L/k}) \simeq Ш^2_\omega(k, \hat{T}_{L'/k})$.

Recall some definitions from [1]. Let s and t be positive integers. For $s \geq t$, let $\pi_{s,t}$ be the canonical projection $\mathbb{Z}/p^s\mathbb{Z} \to \mathbb{Z}/p^t\mathbb{Z}$. For $x \in \mathbb{Z}/p^s\mathbb{Z}$ and $y \in \mathbb{Z}/p^t\mathbb{Z}$, we say that x *dominates* y if $s \geq t$ and $\pi_{s,t}(x) = y$; if this is the case, we write $x \succeq y$. For $x \in \mathbb{Z}/p^s\mathbb{Z}$ and $y \in \mathbb{Z}/p^t\mathbb{Z}$, let $\delta(x, y)$ be the greatest nonnegative integer $d \leq \min\{s, t\}$ such that $\pi_{s,d}(x) = \pi_{t,d}(y)$. We have $\delta(x, y) = \min\{s, t\}$ if and only if $x \succeq y$ or $y \succeq x$.

Recall that $e_i \geq e_{i+1}$ for $i = 1, ..., m-1$. For $a = (a_1, ..., a_m) \in \bigoplus_{i \in \mathcal{I}} \mathbb{Z}/p^{e_i}\mathbb{Z}$ and $n \in \mathbb{Z}/p^{e_1}\mathbb{Z}$, let $I_n(a)$ be the set $\{i \in \mathcal{I} | \ n \succeq a_i\}$ and let $I(a) = (I_0(a), ..., I_{p^{e_1}-1}(a))$.

Given a positive integer $0 \leq d \leq \epsilon_0$ and $i \in \mathcal{I}$, let Σ^d_i be the set of all places $v \in \Omega_k$ such that at each place w of K_i above v, the following equivalent conditions hold (see [1] Prop. 5.5 and 5.6):

(1) The algebra $K_0 \otimes_k K^w_i$ is isomorphic to a product of isomorphic field extensions of degree at most p^d of K^w_i.

(2) $K_0(\epsilon_0 - d) \otimes_k K_i^w$ is isomorphic to a product of K_i^w.

Let $\Sigma_i = \Sigma_i^0$. In other words, Σ_i is the set of all places $v \in \Omega_k$ where $K_0 \otimes K_i^v$ is isomorphic to a product of copies of K_i^v.

Let $a = (a_1, ..., a_m)$ be an element in $\bigoplus_{i\in\mathcal{I}} \mathbb{Z}/p^{e_i}\mathbb{Z}$ and $I(a) = (I_0, ..., I_{p^{e_1}-1})$. For $I_n \subsetneq \mathcal{I}$, define

$$\Omega(I_n) = \bigcap_{i\notin I_n} \Sigma_i^{\delta(n,a_i)}. \tag{2.5}$$

For $I_n = \mathcal{I}$, we set $\Omega(I_n) = \Omega_k$.

Set

$$G = G(K_0, K') = \{(a_1, ..., a_m) \in \bigoplus_{i\in\mathcal{I}} \mathbb{Z}/p^{e_i}\mathbb{Z} | \bigcup_{n\in\mathbb{Z}/p^{e_1}\mathbb{Z}} \Omega(I_n(a)) = \Omega_k\},$$

and set D to be the diagonal subgroup generated by $(1, 1, ..., 1)$.

Define $\text{Ш}(K_0, K')$ as $G(K_0, K')/D$.

Theorem 2.4. *([1] Cor. 5.4) The Tate-Shafarevich group $\text{Ш}^2(k, \hat{T}_{L/k})$ is isomorphic to $\text{Ш}(K_0, K')$.*

Proof. This follows from Lemma 2.3 and [1] Thm. 5.3. □

Next we give a combinatorial description of $\text{Ш}^2_\omega(k, \hat{T}_{L/k})$, which is similar to the description of $\text{Ш}^2(k, \hat{T}_{L/k})$.

For $a = (a_1, ..., a_m) \in \bigoplus_{i\in\mathcal{I}} \mathbb{Z}/p^{e_i}\mathbb{Z}$, we define

$$\mathcal{S}_a = \Omega_k \backslash (\bigcup_{n\in\mathbb{Z}/p^{e_1}\mathbb{Z}} \Omega(I_n(a))).$$

Set

$$G_\omega = G_\omega(K_0, K') = \{(a_1, ..., a_m) \in \bigoplus_{i\in\mathcal{I}} \mathbb{Z}/p^{e_i}\mathbb{Z} | \ \mathcal{S}_a \text{ is a finite set}\}.$$

Clearly $G \subseteq G_\omega$. Define $\text{Ш}_\omega(K_0, K')$ as $G_\omega(K_0, K')/D$, where D is the subgroup generated by the diagonal element $(1, ..., 1)$. We prove an analogue of Theorem 2.4.

Theorem 2.5. *Keep the notation above. Then $\text{Ш}^2_\omega(k, \hat{T}_{L/k}) \simeq \text{Ш}_\omega(K_0, K')$.*

Proof. By Lemma 2.3, it is sufficient to show that $\text{Ш}^1_\omega(k, \hat{S}_{K_0,K'}) \simeq \text{Ш}_\omega(K_0, K')$. The proof is similar to the proof of [1] Theorem 5.3. We sketch the proof here. For more details one can refer to [1].

Consider the dual sequence of (2.2),

$$0 \longrightarrow \hat{T}_{K_0/k} \xrightarrow{\iota} \mathrm{I}_{K'/k}(\hat{T}_{E/K'}) \xrightarrow{\rho} \hat{S}_{K_0,K'} \longrightarrow 0\ , \tag{2.6}$$

and the exact sequence induced by (2.6),

$$H^1(k, \hat{T}_{K_0/k}) \xrightarrow{\iota^1} H^1(k, \mathrm{I}_{K'/k}(\hat{T}_{E/K'})) \xrightarrow{\rho^1} H^1(k, \hat{S}_{K_0,K'}) \to H^2(k, \hat{T}_{K_0/k}). \tag{2.7}$$

Please cite this article in press as: T.-Y. Lee, The Tate-Shafarevich groups of multinorm-one tori, J. Pure Appl. Algebra (2022), https://doi.org/10.1016/j.jpaa.2021.106906

By [1] Lemma 1.2 and Lemma 1.3, we can identify $H^1(k, \hat{T}_{K_0/k})$ to $\mathbb{Z}/p^{\epsilon_0}\mathbb{Z}$ and $H^1(k, \mathrm{I}_{K_i/k}(\hat{T}_{E_i/K_i}))$ to $\mathbb{Z}/p^{e_i}\mathbb{Z}$ for $1 \le i \le m$. Under this identification, we can rewrite the exact sequence (2.7) as follows:

$$\mathbb{Z}/p^{\epsilon_0}\mathbb{Z} \xrightarrow{\iota^1} \bigoplus_{i\in\mathcal{I}} \mathbb{Z}/p^{e_i}\mathbb{Z} \xrightarrow{\rho^1} H^1(k, \hat{S}_{K_0,K'}) \to H^2(k, \hat{T}_{K_0/k}), \tag{2.8}$$

where ι^1 is the natural projection from $\mathbb{Z}/p^{\epsilon_0}\mathbb{Z}$ to $\mathbb{Z}/p^{e_i}\mathbb{Z}$ for each i. Note that the image of ι^1 is the subgroup D, and we have the exact sequence

$$0 \to (\bigoplus_{i\in\mathcal{I}} \mathbb{Z}/p^{e_i}\mathbb{Z})/D \xrightarrow{\rho^1} H^1(k, \hat{S}_{K_0,K'}) \to H^2(k, \hat{T}_{K_0/k}). \tag{2.9}$$

By Proposition 2.2 the group $Ш^1_\omega(k, \hat{S}_{K_0,K'})$ is contained in the image of ρ^1. Let $a = (a_1, ..., a_m) \in \bigoplus_{i\in\mathcal{I}} \mathbb{Z}/p^{e_i}\mathbb{Z}$ and $[a]$ be its image in $(\bigoplus_{i\in\mathcal{I}} \mathbb{Z}/p^{e_i}\mathbb{Z})/D$. We claim that $\rho^1([a])$ is in $Ш^1_\omega(k, \hat{S}_{K_0,K'})$ if and only if $a \in G_\omega$.

For $v \in \Omega_k$, we denote by a^v the image of a in $\bigoplus_{i=1}^m H^1(k_v, \mathrm{I}_{K_i^v/k_v}(\hat{T}_{E_i^v/K_i^v}))$, and by D_v the image of D in this sum.

By the exact sequence (2.9) over k_v, we have $\rho^1([a]) \in Ш^1_\omega(k, \hat{S}_{K_0,K'})$ if and only if $a^v \in D_v$ for almost all places $v \in \Omega_k$.

Note that $a^v = (n, ..., n)^v$ if and only if $v \in \Omega(I_n(a))$. Hence $a^v \in D_v$ if and only if $v \in \bigcup_{n\in\mathbb{Z}/p^{e_1}\mathbb{Z}} \Omega(I_n(a))$.

Our claim then follows. □

2.2. Subtori

For $0 \le r \le \epsilon_0$, we set the following:

- $U_r = \{i \in \mathcal{I} |\ e_{0,i} = r\}$.
- $K_{U_r} = \prod_{i\in U_r} K_i$.
- $L_r = K_0 \times K_{U_r}$.
- $E_{U_r} = K_0 \otimes_k K_{U_r}$.

Pick an r such that U_r is nonempty. We define $S_{K_0,K_{U_r}}$ as in (2.1) and (2.2). Namely let ϕ_r : $\mathrm{R}_{E_{U_r}/k}(\mathbb{G}_m) \to \mathrm{R}_{L_r/k}(\mathbb{G}_m)$ be defined by $\phi_r(x) = (N_{E_{U_r}/K_0}(x)^{-1}, N_{E_{U_r}/K_{U_r}}(x))$ and define $S_{K_0,K_{U_r}}$ by the following exact sequence.

$$1 \longrightarrow S_{K_0,K_{U_r}} \longrightarrow \mathrm{R}_{E_{U_r}/k}(\mathbb{G}_m) \xrightarrow{\phi} T_{L_r/k} \longrightarrow 1\ . \tag{2.10}$$

The torus $S_{K_0,K_{U_r}}$ also fits in the exact sequence:

$$1 \longrightarrow S_{K_0,K_{U_r}} \longrightarrow \prod_{i\in U_r} \mathrm{R}_{K_i/k}(T_{E_i/K_i}) \xrightarrow{N_{E_{U_r}/K_0}} T_{K_0/k} \longrightarrow 1\ . \tag{2.11}$$

Write $\mathrm{R}_{K'/k}(\mathbb{G}_m)$ as $\prod_{i\in U_r} \mathrm{R}_{K_i/k}(\mathbb{G}_m) \times \prod_{i\in\mathcal{I}\setminus U_r} \mathrm{R}_{K_i/k}(\mathbb{G}_m)$. There is a natural injective group homomorphism

$$\alpha_r : \prod_{i\in U_r} \mathrm{R}_{K_i/k}(\mathbb{G}_m) \to \prod_{i\in U_r} \mathrm{R}_{K_i/k}(\mathbb{G}_m) \times \prod_{i\in \mathcal{I}\setminus U_r} \mathrm{R}_{K_i/k}(\mathbb{G}_m),$$

which sends x to $(x, 1)$. Then α_r induces an injective homomorphism $\alpha_{E_{U_r}}$ from $\mathrm{R}_{E_{U_r}/k}(\mathbb{G}_m)$ to $\mathrm{R}_{E/k}(\mathbb{G}_m)$, and an injective homomorphism $\mathrm{id}_{K_0} \times \alpha_r$ from $\mathrm{R}_{K_0/k}(\mathbb{G}_m) \times \prod_{i\in U_r} \mathrm{R}_{K_i/k}(\mathbb{G}_m)$ to $\mathrm{R}_{K_0/k}(\mathbb{G}_m) \times \mathrm{R}_{K'/k}(\mathbb{G}_m)$. It is easy to check the following diagram commutes.

$$\begin{array}{ccccccccc} 1 & \longrightarrow & S_{K_0,K'} & \longrightarrow & \mathrm{R}_{E/k}(\mathbb{G}_m) & \xrightarrow{\phi} & T_{L/k} & \longrightarrow & 1 \\ \uparrow & & \uparrow{\scriptstyle \alpha_{U_r}} & & \uparrow{\scriptstyle \alpha_{U_r}} & & \uparrow{\scriptstyle \mathrm{id}_{K_0}\times\alpha_r} & & \uparrow \\ 1 & \longrightarrow & S_{K_0,K_{U_r}} & \longrightarrow & \mathrm{R}_{E_{U_r}/k}(\mathbb{G}_m) & \xrightarrow{\phi_r} & T_{L_r/k} & \longrightarrow & 1 \end{array} \tag{2.12}$$

Together with Lemma 2.3, we have

$$\begin{array}{ccc} Ш^1_\omega(k, \hat{S}_{K_0,K'}) & \xrightarrow{\sim} & Ш^2_\omega(k, \hat{T}_{L/k}) \\ {\scriptstyle \hat{\alpha}_{U_r}}\downarrow & & \downarrow{\scriptstyle \mathrm{id}_{K_0}\times\hat{\alpha}_r} \\ Ш^1_\omega(k, \hat{S}_{K_0,K_{U_r}}) & \xrightarrow{\sim} & Ш^2_\omega(k, \hat{T}_{L_r/k}). \end{array} \tag{2.13}$$

Note that for $i \in U_r$, we have $e_i = \epsilon_0 - r$. We define $G(K_0, K_{U_r})$ and $G_\omega(K_0, K_{U_r})$ by replacing $\mathcal{I}$ with U_r as in Section 2.1 and 2.2. Namely for $a = (a_i)_{i\in U_r} \in \bigoplus_{i\in U_r} \mathbb{Z}/p^{e_i}\mathbb{Z}$, we define $\mathcal{S}_a$ to be the set $\Omega_k \backslash (\bigcup_{n\in \mathbb{Z}/p^{\epsilon_0 - r}\mathbb{Z}} \Omega(I_n(a)))$. Set

$$G_\omega(K_0, K_{U_r}) = \{(a_i)_{i\in U_r} \in \bigoplus_{i\in U_r} \mathbb{Z}/p^{e_i}\mathbb{Z} |\ \mathcal{S}_a \text{ is a finite set}\},$$

and set $G(K_0, K_{U_r})$ to be the subset of $G_\omega(K_0, K_{U_r})$ consisting of all elements a with $\mathcal{S}_a = \emptyset$. Consider the natural projection $\varpi_r : \bigoplus_{i\in I} \mathbb{Z}/p^{e_i}\mathbb{Z} \to \bigoplus_{i\in U_r} \mathbb{Z}/p^{e_i}\mathbb{Z}$. Then the natural projection induces a homomorphism $G_\omega(K_0, K')/D \to G_\omega(K_0, K_{U_r})/D$, which we still denote by ϖ_r. Note that by Theorem 2.5, we have isomorphisms $Ш^2_\omega(k, \hat{T}_{L/k}) \simeq G_\omega(K_0, K')/D$ and $Ш^2_\omega(k, \hat{T}_{L_r/k}) \simeq G_\omega(K_0, K_{U_r})/D$.

Proposition 2.6. *The morphism* $\mathrm{id}_{K_0} \times \hat{\alpha}_r : Ш^2_\omega(k, \hat{T}_{L/k}) \to Ш^2_\omega(k, \hat{T}_{L_r/k})$ *coincides with* ϖ_r.

Proof. It is enough to show that the map induced by $\alpha_{E_{U_r}}$ from $Ш^1_\omega(k, \hat{S}_{K_0,K'}) \to Ш^1_\omega(k, \hat{S}_{K_0,K_{U_r}})$ is equal to ϖ_r.

The map $\alpha_{E_{U_r}}$ gives a map between character groups

$$\hat{\alpha}_{E_{U_r}} : \mathrm{I}_{E/k}(\mathbb{Z}) = \mathrm{I}_{E_{U_r}/k}(\mathbb{Z}) \bigoplus_{i\in\mathcal{I}\setminus U_r} \mathrm{I}_{E_i/k}(\mathbb{Z}) \to \mathrm{I}_{E_{U_r}/k}(\mathbb{Z}),$$

which is the natural projection. Hence the map from $\mathrm{I}_{K'/k}(\hat{T}_{E/K'}) = \mathrm{I}_{K_{U_r}/k}(\hat{T}_{E_{U_r}/K_{U_r}}) \bigoplus_{i\in\mathcal{I}\setminus U_r} \mathrm{I}_{K_i/k}(\hat{T}_{E_i/K_i})$ to $\mathrm{I}_{K_{U_r}/k}(\hat{T}_{E_{U_r}/K_{U_r}})$ induced by $\alpha_{E_{U_r}}$ (restricted to $\mathrm{R}_{K_{U_r}/k}(T_{E_{U_r}/K_{U_r}})$) is the natural projection.

Therefore the map induced by $\hat{\alpha}_{E_{U_r}}$ from $H^1(k, \mathrm{I}_{K'/k}(\hat{T}_{E/K'})) \simeq \bigoplus_{i\in\mathcal{I}} \mathbb{Z}/p^{e_i}\mathbb{Z}$ to $H^1(k, \mathrm{I}_{K_{U_r}/k}(\hat{T}_{E_{U_r}/K_{U_r}})) \simeq \bigoplus_{i\in U_r} \mathbb{Z}/p^{e_i}\mathbb{Z}$ is the natural projection.

By exact sequences (2.8) and (2.9), we have $\hat{\alpha}_{E_{U_r}} : Ш^1_\omega(k, \hat{S}_{K_0,K'}) \to Ш^1_\omega(k, \hat{S}_{K_0,K_{U_r}})$ is equal to ϖ_r. $\square$

3. Preliminaries on cyclic extensions

From now on we assume that K_i are *cyclic extensions* of k.

Let p be a prime which divides $[L : k]$, and let $L(p)$ be the largest subalgebra of L such that $[L(p) : k]$ is a power of p. By [1] Proposition 8.6, to compute $Ш^2(k, \hat{T}_{L/k})$ it is enough to compute $Ш^2(k, \hat{T}_{L(p)/k})$ for each such p. Hence in the following we assume that $[L : k]$ is a *power of* p unless we state otherwise.

By renaming these cyclic extensions, we always assume that the degree of K_0 is minimal. Let $p^{\epsilon_i} = [K_i : k]$ for all $i \in \mathcal{I}'$. For a nonnegative integer $f \leq \epsilon_i$, we denote by $K_i(f)$ the unique subfield of K_i of degree p^f.

For all $i \in \mathcal{I}$, we set $p^{e_{i,j}} = [K_i \cap K_j : k]$. As we assume that $K_j \not\subseteq K_i$ for any i, $j \in \mathcal{I}'$, $e_{i,j} < \min\{\epsilon_i, \epsilon_j\}$ for all $i, j \in \mathcal{I}'$.

Note that for $i, j \in \mathcal{I}$ with $i < j$, we have $e_{i,j} \geq e_{0,i}$. This follows from the assumption in §2.1 that $e_{0,i} \leq e_{0,j}$.

In the following we prove some general facts about cyclic extensions which will be used later.

Lemma 3.1. *Let M/k and N/k be cyclic extensions of p-power degree with $[N : k] \leq [M : k]$. Then $\mathrm{Gal}(MN/k) \simeq \mathrm{Gal}(M/k) \times \mathrm{Gal}(N/N \cap M)$.*

Proof. The nature injection $\mathrm{Gal}(MN/k) \to \mathrm{Gal}(M/k) \times \mathrm{Gal}(N/k)$ shows that each element of $\mathrm{Gal}(MN/k)$ has order at most $[M : k]$. Choose an element in $\mathrm{Gal}(MN/k)$ which projects a generator of $\mathrm{Gal}(M/k)$. Then it generates a subgroup isomorphic to $\mathrm{Gal}(M/k)$. Hence the exact sequence

$$1 \longrightarrow \mathrm{Gal}(MN/M) \longrightarrow \mathrm{Gal}(MN/k) \longrightarrow \mathrm{Gal}(M/k) \longrightarrow 1$$

splits. Note that $\mathrm{Gal}(MN/M)$ is isomorphic to $\mathrm{Gal}(N/N \cap M)$. Therefore $\mathrm{Gal}(MN/k) \simeq \mathrm{Gal}(M/k) \times \mathrm{Gal}(N/N \cap M)$. $\square$

Lemma 3.2. *Let M/k, N/k, and R/k be cyclic extensions of p-power degree and $v \in \Omega_k$. Suppose the following:*

(1) $RM = NM$.
(2) $RN \subseteq RM$.
(3) *RN is locally cyclic at v, i.e. $RN \otimes_k k_v$ is a product of cyclic extensions of k_v.*

Then either $R^v \otimes_{k_v} N^v$ is isomorphic to a product of copies of N^v or $R^v \otimes_{k_v} M^v$ is isomorphic to a product of copies of M^v.

Proof. Let $\tilde{M}$, $\tilde{N}$ and $\tilde{R}$ be cyclic extensions of k_v such that $M^v \simeq \prod \tilde{M}$, $N^v \simeq \prod \tilde{N}$ and $R^v \simeq \prod \tilde{R}$.

Suppose that $R^v \otimes_{k_v} N^v = \prod \tilde{R} \otimes_{k_v} \tilde{N} \not\simeq \prod N^v$. Then $\tilde{R} \cap \tilde{N} \neq \tilde{R}$. We claim that $\tilde{R} \cap \tilde{N} = \tilde{N}$. Suppose not. Then $\tilde{R}\tilde{N}$ is a bicyclic extension of k_v and $\tilde{R} \otimes_{k_v} \tilde{N}$ is a product of bicyclic extensions. As there is a surjective map from $R^v \otimes_{k_v} N^v$ to $RN \otimes_k k_v$ and by assumption the latter is a product of cyclic extensions, the algebra $R^v \otimes_{k_v} N^v = \prod \tilde{R} \otimes_{k_v} \tilde{N}$ is also a product of cyclic extensions, which is a contradiction. Hence $\tilde{N}$ is a proper subfield of $\tilde{R}$.

Now consider the fields $F_R = \tilde{M} \cap \tilde{R}$ and $F_N = \tilde{M} \cap \tilde{N}$. As $RM = NM$, we have $\tilde{R}\tilde{M} = \tilde{N}\tilde{M}$. Therefore $[\tilde{R}\tilde{M} : \tilde{M}] = [\tilde{R} : F_R] = [\tilde{N} : F_N]$.

We claim that $\tilde{N} = F_N$. Suppose not, i.e. $F_N \subsetneq \tilde{N}$. Then we have $\tilde{N} \not\subseteq F_R$. As they are both subfields of $\tilde{R}$, which is cyclic of p-power degree, this implies that $F_R \subseteq \tilde{N}$. Hence $F_N = F_R$. As $[\tilde{R} : F_R] = [\tilde{N} : F_N]$, we have $\tilde{R} = \tilde{N}$, which is a contradiction. Hence $F_N = \tilde{N}$ and $[\tilde{R} : F_R] = [\tilde{N} : F_N] = 1$. Since $\tilde{R} = F_R \subseteq \tilde{M}$, the algebra $R^v \otimes_{k_v} M^v$ is isomorphic to a product of copies of M^v. $\square$

Please cite this article in press as: T.-Y. Lee, The Tate-Shafarevich groups of multinorm-one tori, J. Pure Appl. Algebra (2022), https://doi.org/10.1016/j.jpaa.2021.106906

Lemma 3.3. *Let $i, j \in \mathcal{I}'$ and $i \neq j$. Let R be a cyclic extension of k of degree p^d. Set $F = K_i \cap K_j \cap R$ and $p^h = [F : k]$. Suppose that $R \subseteq K_i K_j$ and $d \leq \min\{\epsilon_i, \epsilon_j\}$. Then $d + e_{i,j} - h \leq \min\{\epsilon_i, \epsilon_j\}$ and $R \subseteq K_i(d + e_{i,j} - h)K_j(d + e_{i,j} - h)$.*

Proof. By the definition of h, we have $h \leq e_{i,j}$. If $h = e_{i,j}$, then $d + e_{i,j} - h \leq \min\{\epsilon_i, \epsilon_j\}$ by assumption. If $h < e_{i,j}$, we claim that $R \cap K_i = R \cap K_j = F$. To see this, first note that $R \cap K_i$ and $K_j \cap K_i$ are both subfields of the cyclic extension K_i. Hence either $R \cap K_i \subseteq K_j \cap K_i$ or $K_j \cap K_i \subsetneq R \cap K_i$. If $K_j \cap K_i \subsetneq R \cap K_i$, then $F = K_j \cap K_i$ which contradicts to the assumption $h < e_{i,j}$. Therefore $R \cap K_i \subseteq K_j \cap K_i$. This implies that $R \cap K_i = F$. Similarly we have $R \cap K_j = F$.

As $RK_i \subseteq K_i K_j$, by comparing the degrees of both sides, we have $\epsilon_i + d - h \leq \epsilon_i + \epsilon_j - e_{i,j}$ and hence $d + e_{i,j} - h \leq \epsilon_j$. One can get $d + e_{i,j} - h \leq \epsilon_i$ by a similar way.

Next we show the second part of the statement. If $h = d$, then by definition $R = K_i(d) = K_j(d)$ and the lemma is clear. Suppose $h < d$. We regard R, K_i and K_j as extensions of F. Let $M = K_i(d + e_{i,j} - h)K_j(d + e_{i,j} - h)$. Without loss of generality, we assume $\epsilon_i \geq \epsilon_j$. By Lemma 3.1, the Galois group $\mathrm{Gal}(K_i K_j/F)$ is isomorphic to $\mathrm{Gal}(K_i/F) \times \mathrm{Gal}(K_j/K_i \cap K_j) \simeq \mathbb{Z}/p^{\epsilon_i - h}\mathbb{Z} \times \mathbb{Z}/p^{\epsilon_j - e_{i,j}}$. Let $(a, b) \in \mathbb{Z}/p^{\epsilon_i - h}\mathbb{Z} \times \mathbb{Z}/p^{\epsilon_j - e_{i,j}}$. If (a, b) fixes M, then a fixes $K_i(d + e_{i,j} - h)$ and b fixes $K_j(d + e_{i,j} - h)$. Hence there are x and y such that $a = p^{d + e_{i,j} - 2h}x$ and $b = p^{d-h}y$.

On the other hand R is a cyclic extension of degree p^{d-h} of F, so for every $\sigma \in \mathrm{Gal}(K_i K_j/F)$, we have $p^{d-h}\sigma \in \mathrm{Gal}(K_i K_j/R)$. Hence we have $\mathrm{Gal}(K_i K_j/M) \subseteq \mathrm{Gal}(K_i K_j/R)$ and $R \subseteq M$. □

For a nonempty subset $C \subseteq \mathcal{I}$ and an integer $d \geq 0$, we define the field $M_C(d)$ to be the composite field $\langle K_i(d) \rangle_{i \in C}$.

Lemma 3.4. *Let d be a positive integer and J be a non-empty subset of $\mathcal{I}'$. Suppose that $M = M_J(d)$ is bicyclic. Then $M = K_i(d)K_j(d)$, for any $i, j \in J$ such that the degree of $K_i(d)K_j(d)$ is maximal.*

Proof. As M is bicyclic, there are at least two elements in J. If $|J| = 2$, then the claim is trivial.

Suppose that $|J| > 2$. Pick $i, j \in J$ such that the degree of $K_i(d)K_j(d)$ is maximal. If $d \leq e_{i,j}$, then $K_i(d)K_j(d) = K_i(d)$ which is of degree p^d. Since for any $s \in J$ the degree of $K_i(d)K_s(d)$ is at least p^d, we have $K_i(d)K_s(d) = K_i(d)$ for all $s \in J$. Hence $M = K_i(d)$ which is a cyclic extension. This contradicts our assumption. Therefore $d > e_{i,j}$.

We claim that for any $s \in J$, the field $K_s(d)$ is contained in $K_i(d)K_j(d)$. As the degree of $K_i(d)K_j(d)$ is maximal, the degree of $K_i(d) \cap K_j(d)$ is minimal. Since K_i is cyclic, this implies that $K_i(d) \cap K_j(d) \subseteq K_i(d) \cap K_s(d)$. Set $N = K_i(d)K_j(d) \cap K_s(d)$. Note that N is a cyclic extension. Let p^l be the degree of $[N : k]$.

We claim that $N = K_s(d)$. Suppose that $N \subsetneq K_s(d)$, i.e. $l < d$. Then $K_i(d)K_j(d)$ is a bicyclic extension of $K_i(l)K_j(l)$. Since $K_i(d) \cap K_j(d) \subseteq K_i(d) \cap K_s(d)$, we have $K_i(d) \cap K_j(d) \subseteq N$. By Lemma 3.3 we have $N \subseteq K_i(l)K_j(l)$. Therefore $K_i(d)K_j(d)/N$ is a bicyclic extension of N.

Note that $\mathrm{Gal}(K_i(d)K_j(d)K_s(d)/N) \simeq \mathrm{Gal}(K_i(d)K_j(d)/N) \times \mathrm{Gal}(K_s(d)/N)$. Since $N \subsetneq K_s(d)$ and $\mathrm{Gal}(K_i(d)K_j(d)/N)$ is bicyclic, the field $K_i(d)K_j(d)K_s(d)$ is not a bicyclic extension of k, which contradicts the fact that M is a bicyclic extension. Hence $N = K_s(d)$ and $K_s(d) \subseteq K_i(d)K_j(d)$. □

Lemma 3.5. *Let $a = (a_1, ..., a_m)$ be an element in $G_\omega(K_0, K') \setminus D$. Set $\epsilon_0 - d = \min\limits_{i \notin I_{a_1}(a)} \{\delta(a_1, a_i)\}$. Choose $j \notin I_{a_1}(a)$ minimal such that $\epsilon_0 - d = \delta(a_1, a_j)$. Set $a' = (a'_1, ..., a'_m) \in \bigoplus\limits_{i \in \mathcal{I}} \mathbb{Z}/p^{e_i}\mathbb{Z}$ as follows:*

$$a'_i = \begin{cases} \pi_{e_j, e_i}(a_j), & \text{if } i \notin I_{a_1}(a) \text{ and } \epsilon_0 - d = \delta(a_1, a_i); \\ \pi_{e_1, e_i}(a_1), & \text{otherwise.} \end{cases} \tag{3.1}$$

Then $a' \notin D$ and $\mathcal{S}_{a'} \subseteq \mathcal{S}_a$.

Proof. First note that $d > e_{0,i}$ for all $i \notin I_{a_1}(a)$. As $j \notin I_{a_1}(a')$, we have $a' \notin D$.

The inclusion $\mathcal{S}_{a'} \subseteq \mathcal{S}_a$ is equivalent to the inclusion $\bigcup_{n \in \mathbb{Z}/p^{e_1}\mathbb{Z}} \Omega(I_n(a)) \subseteq \bigcup_{n \in \mathbb{Z}/p^{e_1}\mathbb{Z}} \Omega(I_n(a'))$, i.e. for $n \in \mathbb{Z}/p^{e_1}\mathbb{Z}$ and for $v \in \Omega(I_n(a))$, there is some $n' \in \mathbb{Z}/p^{e_1}\mathbb{Z}$ such that $v \in \Omega(I_{n'}(a'))$. It is enough to show that for each $n \in \mathbb{Z}/p^{e_1}\mathbb{Z}$, there is some $n' \in \mathbb{Z}/p^{e_1}\mathbb{Z}$ such that $I_n(a) \subseteq I_{n'}(a')$ and $\delta(n, a_i) \leq \delta(n', a'_i)$ for all $i \notin I_{n'}(a')$.

case 1. $\delta(a_1, n) > \epsilon_0 - d$. We claim that $I_n(a) \subseteq I_{a_1}(a')$ in this case. For all $i \in I_n(a)$, we have $\delta(a_1, a_i) = \delta(a_1, \pi_{e_1,e_i}(n)) = \min\{\delta(a_1, n), e_i\}$. Hence we have either $\delta(a_1, a_i) = \delta(a_1, n) > \epsilon_0 - d$ or $i \in I_{a_1}(a)$. Therefore $a'_i = \pi_{e_1,e_i}(a_1)$ and $i \in I_{a_1}(a')$.

By the construction of a', for any $i \notin I_{a_1}(a')$ we have $\delta(a_1, a_i) = \epsilon_0 - d$ and $\delta(a'_1, a'_i) = \delta(a_1, a_j) = \epsilon_0 - d$. Since $\delta(a_1, n) > \epsilon_0 - d$ and $\delta(a_1, a_i) = \epsilon_0 - d$, we have $\delta(n, a_i) = \epsilon_0 - d = \delta(a'_1, a'_i)$.

case 2. $\delta(a_1, n) = \epsilon_0 - d$. Then for all $i \in I_n(a) \setminus I_{a_1}(a)$, we have $\delta(a_1, a_i) = \delta(a_1, n) = \epsilon_0 - d$. If $i \in I_n(a) \cap I_{a_1}(a)$, then $e_i \leq \epsilon_0 - d$ and hence $\pi_{e_1,e_i}(a_1) = \pi_{e_j,e_i}(a_j)$. In both cases, we have $a'_i = \pi_{e_j,e_i}(a_j)$ and $i \in I_{n'}(a')$ for any $n' \in \mathbb{Z}/p^{e_1}\mathbb{Z}$ such that $a_j = \pi_{e_1,e_j}(n')$.

Let $i \notin I_{n'}(a')$. Then we have $e_i > \epsilon_0 - d$ and $a'_i = \pi_{e_1,e_i}(a_1)$. This implies $\delta(n', a'_i) = \delta(a_j, a_1) = \epsilon_0 - d$. On the other hand $\delta(a_1, a_i) > \epsilon_0 - d$ for any $i \notin I_{n'}(a')$. Hence $\delta(n, a_i) = \delta(n, a_1) = \epsilon_0 - d$ and $\delta(n', a'_i) = \delta(n, a_i)$.

case 3. $\delta(a_1, n) < \epsilon_0 - d$. Since $\epsilon_0 - d = \min_{i \notin I_{a_1}(a)} \{\delta(a_1, a_i)\}$, we have $I_n(a) \subseteq I_{a_1}(a) \subseteq I_{a_1}(a')$. For $i \notin I_{a_1}(a')$, we have $\delta(a_1, a_i) = \epsilon_0 - d$ and hence $\delta(n, a_i) = \delta(n, a_1) < \epsilon_0 - d = \delta(a_1, a'_i)$.

From the above three cases we conclude that $\mathcal{S}_{a'} \subseteq \mathcal{S}_a$. □

We immediately have the following corollary.

Corollary 3.6. *Keep notation as above. If $a \in G(K_0, K) \backslash D$ (resp. $G_\omega(K_0, K') \setminus D$), then $a' \in G(K_0, K') \backslash D$ (resp. $G_\omega(K_0, K') \setminus D$).*

Lemma 3.7. *Let $a = (a_1, ..., a_m)$ be an element in $G_\omega(K_0, K') \setminus D$. Set $\epsilon_0 - d = \min_{i \notin I_{a_1}(a)} \{\delta(a_1, a_i)\}$. Choose $s, t \in I$ such that $\delta(a_1, a_s) > \epsilon_0 - d$ and $\delta(a_1, a_t) = \epsilon_0 - d$. Then there is a finite set $\mathcal{S} \subseteq \Omega_k$ such that for all $v \in \Omega_k \setminus \mathcal{S}$ either $K_0(d) \otimes K_s^v$ is a product of copies of K_s^v or $K_0(d) \otimes K_t^v$ is a product of copies of K_t^v. Moreover, if $a \in G(K_0, K') \setminus D$, then we can take $\mathcal{S} = \emptyset$.*

Proof. Let a' be defined as in Lemma 3.5. Then $a' \in G_\omega(K_0, K') \setminus D$. We claim that for all $v \in \Omega_k \setminus \mathcal{S}_{a'}$ either $K_0(d) \otimes K_s^v$ is a product of copies of K_s^v or $K_0(d) \otimes K_t^v$ is a product of copies of K_t^v. Note that if $a \in G(K_0, K') \setminus D$, then $\mathcal{S}_{a'} = \emptyset$.

Let $v \in \Omega_k \setminus \mathcal{S}_{a'}$. By the definition of $\mathcal{S}_{a'}$, there is $n \in \mathbb{Z}/p^{e_1}\mathbb{Z}$ such that $v \in \Omega(I_n(a'))$. We consider the following cases.

case 1: $\delta(a_1, n) \leq \epsilon_0 - d$. Then $s \notin I_n(a')$ and $\delta(a_s, n) \leq \epsilon_0 - d$. By the definition of $\Omega(I_n(a'))$, we have $v \in \Sigma_s^{\epsilon_0 - d}$. Hence $K_0(d) \otimes K_s^v$ is a product of copies of K_s^v.

case 2: $\delta(a_1, n) > \epsilon_0 - d$. If $t \in I_{a_1}(a')$, then $e_t = \epsilon_0 - d$. Hence $K_0(d) \otimes K_t^v$ is a product of copies of K_t^v.

Suppose that $t \notin I_{a_1}(a')$. Then $t \notin I_n(a')$ and $\delta(a_t, n) = \epsilon_0 - d$. By the definition of $\Omega(I_n(a'))$, we have $v \in \Sigma_t^{\epsilon_0 - d}$. Hence $K_0(d) \otimes K_t^v$ is a product of copies of K_t^v. □

Proposition 3.8. *Let $a = (a_1, ..., a_m)$ be an element in $G_\omega(K_0, K') \setminus D$. Set $\epsilon_0 - d = \min_{i \notin I_{a_1}(a)} \{\delta(a_1, a_i)\}$. For any $s, t \in I$ with $\delta(a_1, a_s) > \epsilon_0 - d$ and $\delta(a_1, a_t) = \epsilon_0 - d$, we set $u = \max\{s, t\}$. Let $\beta = \min\{e_{0,s}, e_{0,t}\}$. Then we have the following:*

(1) *The extension* $K_0(d) \subseteq F_{d,s,t} := K_s(d+e_{s,t}-\beta)K_t(d+e_{s,t}-\beta)$. *Moreover, if* $e_{0,s} = e_{0,t}$, *then* $F_{d,s,t} = K_0(d)K_s(d+e_{s,t}-\beta) = K_0(d)K_t(d+e_{s,t}-\beta)$.
(2) *Suppose further that* $a \in G(K_0, K')$. *Then the field* $K_0(d)K_u(d+e_{s,t}-\beta)$ *is locally cyclic*

Proof. Let $s, t \in I$ as above. By Lemma 3.7, there is a finite set $\mathcal{S}$ such that for all $v \in \Omega_k \setminus \mathcal{S}$ either $K_0(d) \otimes K_s^v$ is a product of copies of K_s^v or $K_0(d) \otimes K_t^v$ is a product of copies of K_t^v. Hence $K_0(d) \otimes (K_sK_t)^v$ is a product of copies of $(K_sK_t)^v$ for all $v \notin \mathcal{S}$.

Since $\mathcal{S}$ is a finite set, by Chebotarev's density theorem $K_0(d) \subseteq K_sK_t$. Since $\epsilon_0 - e_{0,s} = e_s \geq \delta(a_1, a_s) > \epsilon_0 - d$, we have $d > \beta$. By Lemma 3.3, we have $K_0(d) \subseteq K_s(d+e_{s,t}-\beta)K_t(d+e_{s,t}-\beta)$.

If $e_{0,s} = e_{0,t}$, then $\beta = e_{0,s} = e_{0,t}$. By dimension reasons we have $K_0(d)K_s(d+e_{s,t}-\beta) = F_{d,s,t} = K_0(d)K_t(d+e_{s,t}-\beta)$. This proves the first statement.

Suppose that $a \in G(K_0, K')$. Since $d > \beta$, the field $F_{d,s,t}$ is bicyclic, and its Galois group is isomorphic to $\mathbb{Z}/p^{d+e_{s,t}-\beta}\mathbb{Z} \times \mathbb{Z}/p^{d-\beta}\mathbb{Z}$ by Lemma 3.1.

We first assume that $e_{0,s} \leq e_{0,t}$. Then $\beta = e_{0,s}$ and $F_{d,s,t} = K_0(d)K_s(d+e_{s,t}-\beta)$ by dimension reasons. Note that the field $K_0(d)K_t(d+e_{s,t}-\beta)$ is contained in $F_{d,s,t}$. By Lemma 3.7, at each place $v \in \Omega_k$ we have either $K_0(d) \otimes_k K_s^v$ splits into a product of K_s^v or $K_0(d) \otimes_k K_t^v$ splits into a product of K_t^v. For a place $v \in \Omega_k$, if $K_0(d) \otimes_k K_s^v$ splits into a product of K_s^v, then $F_{d,s,t}^v$ is a product of cyclic extensions of k_v. As a subalgebra of $F_{d,s,t}^v$, the algebra $(K_0(d)K_t(d+e_{s,t}-\beta))^v$ is a product of cyclic extensions. If $K_0(d) \otimes_k K_t^v$ splits into a product of K_t^v, then $(K_0(d)K_t(d+e_{s,t}-\beta))^v$ is a product of cyclic extensions. Hence $K_0(d)K_t(d+e_{s,t}-\beta)$ is locally cyclic.

For $e_{0,s} \geq e_{0,t}$, a similar argument works. $\square$

4. Patchable subgroups

Recall that for each nonempty subset U_r we define $G_\omega(K_0, K_{U_r})$ and there is a natural projection from $G_\omega(K_0, K')$ to $G_\omega(K_0, K_{U_r})$. (See §2.3 for details.) In view of the combinatorial description of $Ш^2_\omega(k, \hat{T}_{L/k})$ (resp. $Ш^2(k, \hat{T}_{L/k})$), the computation of $Ш^2_\omega(k, \hat{T}_{L/k})$ (resp. $Ш^2(k, \hat{T}_{L/k})$) will be much simpler if the e_i's are equal. Hence we will calculate $G_\omega(K_0, K_{U_r})$ for each nonempty subset U_r and then "patch" them together to get the group $G_\omega(K_0, K')$.

Suppose that an element $x \in G_\omega(K_0, K_{U_r})$ can be patched into an element in $G_\omega(K_0, K')$. Then x must be in the image of $G_\omega(K_0, K')$ under the projection map ϖ_r. (See Section 2.2 for the definition of ϖ_r.)

Let $G^0_\omega(K_0, K')$ (resp. $G^0(K_0, K')$) be the subgroup consisting of elements $(a_1, ..., a_m) \in G_\omega(K_0, K')$ (resp. $G(K_0, K')$) with $a_1 = 0$. Then $G_\omega(K_0, K') = D \oplus G^0_\omega(K_0, K')$. In Section 4.1 we define the *patchable subgroup* $\tilde{G}(K_0, K_{U_r})$, which is in fact the image of $G^0_\omega(K_0, K')$ under the projection map ϖ_r.

We show that there is a section of ϖ_r from $\tilde{G}_\omega(K_0, K_{U_r})$ to $G^0_\omega(K_0, K_{U_r})$ and prove that $G_\omega(K_0, K') = D \oplus \bigoplus_r \tilde{G}_\omega(K_0, K_{U_r})$, where r runs over positive integers with U_r nonempty. We prove similar results for $G(K_0, K')$.

Note that if $\mathcal{I} = U_r$ for some r, then $G_\omega(K_0, K') = G_\omega(K_0, K_{U_r})$ and no patching condition is needed. Hence in the following we fix an integer r such that U_r is not empty and $U_r \neq \mathcal{I}$.

We set $U_{>r} = \{i \in \mathcal{I} | e_{0,i} > r\}$ and $U_{<r} = \{i \in \mathcal{I} | e_{0,i} < r\}$. Recall that we assume $\bigcap_{i \in I'} K_i = k$. Hence U_0 is nonempty.

Recall that for a nonempty subset $C \subseteq \mathcal{I}$ and an integer $d \geq 0$, $M_C(d)$ is the composite field $\langle K_i(d) \rangle_{i \in C}$.

4.1. Algebraic patching degrees

Definition 4.1. Define the *algebraic patching degree* Δ^ω_r of U_r to be the maximum nonnegative integer d satisfying the following:

Please cite this article in press as: T.-Y. Lee, The Tate-Shafarevich groups of multinorm-one tori, J. Pure Appl. Algebra (2022), https://doi.org/10.1016/j.jpaa.2021.106906

(1) If $U_{>r}$ is nonempty, then $M_{U_{>r}}(d) \subseteq \bigcap_{i\in U_r} K_0(d)K_i(d)$.
(2) If $U_{<r}$ is nonempty, then $M_{U_r}(d) \subseteq \bigcap_{i\in U_{<r}} K_0(d)K_i(d)$.

If $U_r = \mathcal{I}$, then we set $\Delta_r^\omega = \epsilon_0$.

Note that $K_0(r) = K_i(r)$ for all $i \in U_{\geq r}$. Hence by definition we have $\Delta_r^\omega \geq r$. By Lemma 3.3 and the definition of Δ_r^ω, all nonnegative integers $d \leq \Delta_r^\omega$ satisfy the conditions (1) and (2) in the above definition.

Lemma 4.2. *Let $d \leq \Delta_r^\omega$ be a nonnegative integer. If $U_{<r}$ is nonempty, then $K_0(d)K_j(d) \subseteq \bigcap_{i\in U_{\leq r}} K_0(d)K_i(d)$ for all $j \in U_r$*

Proof. Suppose that $U_{<r}$ is nonempty. If $d \leq r$, the claim is trivial. Assume $d > r$. By the definition of Δ_r^ω the field $K_0(\Delta_r^\omega)M_{U_r}(\Delta_r^\omega)$ is contained in $K_0(\Delta_r^\omega)K_i(\Delta_r^\omega)$ for all $i \in U_{<r}$. By Lemma 3.4 we have $K_0(d)M_{U_r}(d) = K_0(d)K_j(d)$ for all $j \in U_r$. By Lemma 3.3 we have $K_0(d)K_j(d) \subseteq \bigcap_{i\in U_{<r}} K_0(d)K_i(d)$ for all $j \in U_r$. Hence $K_0(d)K_j(d) \subseteq \bigcap_{i\in U_{\leq r}} K_0(d)K_i(d)$ for all $j \in U_r$. $\square$

Proposition 4.3. *Suppose that $U_{>r}$ is nonempty. Let r' be the smallest positive integer bigger than r such that $U_{r'}$ is nonempty. Then we have the following:*

(1) *If $r = 0$, then $\Delta_r^\omega = \Delta_{r'}^\omega$.*
(2) $\Delta_r^\omega \leq \Delta_{r'}^\omega$.
(3) $\Delta_r^\omega - r \geq \Delta_{r'}^\omega - r'$.

Proof. We first show (2). Note that by our choice of r', we have $U_{<r'} = U_{\leq r}$, which is nonempty. By the definition of Δ_r^ω and by Lemma 4.2, we have $M_{U_{r'}}(\Delta_r^\omega) \subseteq \bigcap_{i\in U_r} K_0(\Delta_r^\omega)K_i(\Delta_r^\omega) \subseteq \bigcap_{i\in U_{<r'}} K_0(\Delta_r^\omega)K_i(\Delta_r^\omega)$.

Suppose that $U_{>r'}$ is nonempty. As $M_{U_{>r}}(\Delta_r^\omega) \subseteq K_0(\Delta_r^\omega)K_i(\Delta_r^\omega)$ for all $i \in U_r$, by Lemma 3.4 we have $K_0(\Delta_r^\omega)M_{U_{>r}}(\Delta_r^\omega) = K_0(\Delta_r^\omega)K_j(\Delta_r^\omega)$ for all $j \in U_{r'}$. Hence $M_{U_{>r'}}(\Delta_r^\omega) \subseteq \bigcap_{i\in U_{r'}} K_0(\Delta_r^\omega)K_i(\Delta_r^\omega)$ and $\Delta_{r'}^\omega \geq \Delta_r^\omega$.

Suppose that $r = 0$. Then $U_{<r'} = U_0$. By the definition of $\Delta_{r'}^\omega$, we have $M_{U_{>r'}}(\Delta_{r'}^\omega) \subseteq \bigcap_{i\in U_{r'}} K_0(\Delta_{r'}^\omega) \times K_i(\Delta_{r'}^\omega)$ and $K_0(\Delta_{r'}^\omega)K_j(\Delta_{r'}^\omega)$ is contained in $\bigcap_{i\in U_0} K_0(\Delta_{r'}^\omega)K_i(\Delta_{r'}^\omega)$ for all $j \in U_{r'}$. Hence $M_{U_{\geq r'}}(\Delta_{r'}^\omega) \subseteq \bigcap_{i\in U_0} K_0(\Delta_{r'}^\omega)K_i(\Delta_{r'}^\omega)$. Therefore $\Delta_{r'}^\omega \leq \Delta_0^\omega$. Combining this with statement (2), we get (1).

Now suppose that $r > 0$. We claim that $\Delta_{r'}^\omega - r' \leq \Delta_r^\omega - r$. By Lemma 4.2, we have $K_0(\Delta_r^\omega)K_i(\Delta_r^\omega) \subseteq \bigcap_{j\in U_{<r'}} K_0(\Delta_r^\omega)K_j(\Delta_r^\omega)$ for all $i \in U_r$.

Let $F = \bigcap_{i\in U_{<r'}} K_0(\Delta_{r'}^\omega)K_i(\Delta_{r'}^\omega)$. By Lemma 4.2 we have $K_0(\Delta_{r'}^\omega)K_i(\Delta_r^\omega) \subseteq F$, for all $i \in U_r$.

Let $i \in U_r$. As $K_0(\Delta_{r'}^\omega)K_i(\Delta_r^\omega) \subseteq F \subseteq K_0(\Delta_{r'}^\omega)K_i(\Delta_{r'}^\omega)$, there is some $\Delta_r^\omega \leq \gamma \leq \Delta_{r'}^\omega$ such that $F = K_0(\Delta_{r'}^\omega)K_i(\gamma)$. As $i \in U_r$, the field F is a cyclic extension of $K_0(\Delta_{r'}^\omega)$ of degree $p^{\gamma-r}$. By the definition of $\Delta_{r'}^\omega$, for all $j \in U_{r'}$ we have $K_0(\Delta_{r'}^\omega)K_j(\Delta_{r'}^\omega) \subseteq F$ and $K_0(\Delta_{r'}^\omega)K_j(\Delta_{r'}^\omega)$ is a cyclic extension of $K_0(\Delta_{r'}^\omega)$ of degree $\Delta_{r'}^\omega - r'$. Hence $\Delta_{r'}^\omega - r' \leq \gamma - r$ for dimension reasons.

Suppose that $\Delta_{r'}^\omega - r' > \Delta_r^\omega - r$. Then $\gamma - r \geq \Delta_{r'}^\omega - r' \geq \Delta_r^\omega + 1 - r$. For dimension reasons $K_0(\Delta_{r'}^\omega)K_i(\Delta_r^\omega + 1) \subseteq F$. Since $K_i(\Delta_r^\omega + 1) \subseteq F \subseteq K_0(\Delta_{r'}^\omega)K_j(\Delta_{r'}^\omega)$ for all $j \in U_{<r'}$, by Lemma 3.3 we have $K_i(\Delta_r^\omega + 1) \subseteq K_0(\Delta_r^\omega + 1)K_j(\Delta_r^\omega + 1)$ for all $j \in U_{<r}$. Hence $\Delta_r^\omega + 1$ satisfies condition (2) in Definition 4.1.

By the choice of r' and the definition of $\Delta_{r'}^\omega$, we have $U_{>r} = U_{\geq r'}$ and $M_{U_{\geq r'}}(\Delta_{r'}^\omega) \subseteq \bigcap_{i\in U_{<r'}} K_0(\Delta_{r'}^\omega) \times K_i(\Delta_{r'}^\omega) \subseteq \bigcap_{i\in U_r} K_0(\Delta_{r'}^\omega)K_i(\Delta_{r'}^\omega)$. Thus $\Delta_{r'}^\omega$ satisfies condition (1) in Definition 4.1. By assumption $\Delta_{r'}^\omega >$

$\Delta_r^\omega + 1$, so we have $\Delta_r^\omega \geq \Delta_r^\omega + 1$, which is a contradiction. Therefore $\Delta_{r'}^\omega - r' \leq \Delta_r^\omega - r$. This proves statement (3). □

Definition 4.4. Suppose that U_r is nonempty. Let $x = (x_i)_{i\in U_r} \in G_\omega(K_0, K_{U_r})$. We say that x is *algebraically patchable* if $\delta(0, x_i) \geq \epsilon_0 - \Delta_r^\omega$ for all $i \in U_r$. Here we regard 0 as an element in $\mathbb{Z}/p^{\epsilon_0}\mathbb{Z}$. We define *the algebraic patchable subgroup* of $G_\omega(K_0, K_{U_r})$ as follows: If $r > 0$, it is the subgroup consisting of all algebraically patchable elements of $G_\omega(K_0, K_{U_r})$; if $r = 0$, it is the subgroup consisting of all algebraically patchable elements of $G_\omega(K_0, K_{U_0})$ with $x_1 = 0$.

For $x = (x_i)_{i\in U_r} \in G_\omega(K_0, K_{U_r})$, define $a_x = (a_1, ..., a_m) \in \bigoplus_{i\in\mathcal{I}} \mathbb{Z}/p^{e_i}\mathbb{Z}$ as follows:

$$a_i = \begin{cases} x_i, & \text{if } i \in U_r, \\ 0, & \text{otherwise.} \end{cases} \tag{4.1}$$

In the following we show that x is algebraically patchable if and only if a_x is in $G_\omega^0(K_0, K')$.

Proposition 4.5. *Let $x \in G_\omega(K_0, K_{U_r})$ and a_x be defined as above. If $a_x \in G_\omega^0(K_0, K')$, then x is algebraically patchable.*

We first prove the following Lemma.

Lemma 4.6. *Keep the notation as in Proposition 4.5. Suppose that $a_x = (a_1, ..., a_m) \in G_\omega(K_0, K') \setminus D$. Set $\epsilon_0 - d = \min_{i\notin I_{a_1}(a_x)} \{\delta(a_1, a_i)\}$ and $U_r' = \{i \in U_r | \epsilon_0 - d = \delta(a_1, a_i)\}$. If U_r' and $U_r \setminus U_r'$ are both nonempty, then $K_0(d)K_s(d) = K_0(d)K_t(d)$ for any $s \in U_r \setminus U_r'$ and any $t \in U_r'$. In particular $K_0(d)M_{U_r}(d) = K_0(d)M_{U_r'}(d) = K_0(d)M_{U\setminus U_r'}(d)$.*

Proof. Suppose that U_r' is nonempty and $U_r' \subsetneq U_r$. Let $t \in U_r'$ and $i \in U_r \setminus U_r'$. By Proposition 3.8, we have $K_0(d) \subseteq K_i(d + e_{i,t} - r)K_t(d + e_{i,t} - r)$, and $K_0(d)K_i(d + e_{i,t} - r) = K_0(d)K_t(d + e_{i,t} - r)$. Regard $K_0(d)K_t(d + e_{i,t} - r)$ as a cyclic extension of $K_0(d)$. Then $K_0(d)K_i(d)$ and $K_0(d)K_t(d)$ are subfields of the same degree of the cyclic extension $K_0(d)K_t(d + e_{i,t} - r)$. Hence $K_0(d)K_i(d) = K_0(d)K_t(d)$ for all $t \in U_r'$ and all $i \in U_r \setminus U_r'$. As a consequence $K_0(d)M_{U_r}(d) = K_0(d)M_{U_r'}(d) = K_0(d)M_{U\setminus U_r'}(d)$. □

Proof of Proposition 4.5. Suppose that $a_x = (a_1, ..., a_m) \in G_\omega^0(K_0, K')$. If $x = 0$, then there is nothing to prove. Hence in the following we assume $x \neq 0$. Note that $a_1 = 0$. Set $\epsilon_0 - d = \min_{i\in U_r}\{\delta(0, a_i)\}$ and $U_r' = \{i \in U_r | \epsilon_0 - d = \delta(0, a_i)\}$.

Since $x \neq 0$, we have $d > r$. It is enough to prove that $\Delta_r^\omega \geq d$, i.e. d satisfies conditions (1) and (2) in Definition 4.1.

Suppose that $U_{<r}$ is nonempty. For any $s \in U_{<r}$ and $t \in U_r'$, we have $e_{s,t} = e_{0,s}$. By Proposition 3.8, we have $K_0(d) \subseteq K_s(d)K_t(d)$. For dimension reasons $K_s(d)K_t(d) = K_0(d)K_s(d)$. Hence $K_0(d)K_t(d) \subseteq K_0(d)K_s(d)$. As s and t are arbitrary, we have $K_0(d)M_{U_r'}(d) \subseteq \bigcap_{s\in U_{<r}} K_0(d)K_s(d)$. If $U_r = U_r'$, then we are done. If not, then by Lemma 4.6 we have $K_0(d)M_{U_r}(d) \subseteq \bigcap_{s\in U_{<r}} K_0(d)K_s(d)$.

Now suppose that $U_{>r}$ is not empty. For $s \in U_{\geq d}$, we have $K_s(d) = K_0(d)$. Suppose that $U_{>r} \setminus U_{\geq d}$ is not empty. Let $s \in U_{>r} \setminus U_{\geq d}$ and $t \in U_r'$. Then $e_{s,t} = e_{0,t}$ and by Proposition 3.8, we have $K_0(d) \subseteq K_s(d)K_t(d) = K_0(d)K_t(d)$. Since s and t are arbitrary, by Lemma 4.6 we have $K_0(d)M_{U_{>r}}(d) \subseteq \bigcap_{t\in U_r} K_0(d)K_t(d)$. Therefore $\Delta_r^\omega \geq d$ and x is algebraically patchable. □

Let $x \in G_\omega(K_0, K_{U_r})$ and denote by $(\overline{I}_0, ..., \overline{I}_{p^{\epsilon_0 - r}-1})$ the partition of U_r defined by x. Recall that $\mathcal{S}_x$ is the finite subset of Ω_k such that $\bigcup_{n \in \mathbb{Z}/p^{\epsilon_0 - r}\mathbb{Z}} \Omega(\overline{I}_n) = \Omega_k \setminus \mathcal{S}_x$. (See §2.)

Definition 4.7. Suppose that U_r is nonempty. For a nonnegative integer $d \leq \Delta_r^\omega$ we define $\mathcal{S}_r(d)$ and $\mathcal{S}_{>r}(d)$ as follows.

(1) Suppose that $U_{>r}$ is nonempty. Define $\mathcal{S}_{>r}(d)$ to be the set of places such that $(K_0(d)M_{U_{>r}}(d))^v$ is not locally cyclic. If $U_{>r}$ is empty, then set $\mathcal{S}_{>r}(d) = \emptyset$.
(2) Define $\mathcal{S}_r(d)$ to be the set of places such that $(K_0(d)M_{U_r}(d))^v$ is not locally cyclic.

Clearly $\mathcal{S}_{>r}(d)$ and $\mathcal{S}_r$ are finite sets.

Proposition 4.8. *Let $x \in \tilde{G}_\omega(K_0, K_{U_r})$ and a_x be defined as in equation (4.1). Denote by $I(a_x) = (I_0, ..., I_{p^{\epsilon_0}-1})$ the partition of $\mathcal{I}$ defined by a_x. Let $d \leq \Delta_r^\omega$ be a nonnegative integer such that $x_i = 0$ (mod $p^{\epsilon_0 - d}$) for all $i \in U_r$. Let $\mathcal{S} = \mathcal{S}_x \cup \mathcal{S}_r(d) \cup \mathcal{S}_{>r}(d)$. Then $\bigcup_{n \in \mathbb{Z}/p^{\epsilon_0}\mathbb{Z}} \Omega(I_n) \supseteq \Omega_k \setminus \mathcal{S}$. As a consequence $a_x \in G_\omega^0(K_0, K')$.*

Proof. If $d = r$, then clearly $a_x = 0 \in G_\omega^0(K_0, K')$. Hence we assume $d > r$.

We claim that $\bigcup_{n \in \mathbb{Z}/p^{\epsilon_0}\mathbb{Z}} \Omega(I_n) \supseteq \Omega_k \setminus \mathcal{S}$. Set $\Omega_S = \Omega_k \setminus \mathcal{S}$. If $\Omega_S \subseteq \Omega(I_0)$, then our claim is clear. Suppose not. Let $v \in \Omega_S \setminus \Omega(I_0)$. Our aim is to find $n \neq 0$ such that $v \in \Omega(I_n)$. Since $v \notin \Omega(I_0)$, there is $t \in U_r \setminus I_0$ such that $v \notin \Sigma_t^{\delta(0, x_t)}$. As $x_t = 0$ (mod $p^{\epsilon_0 - d}$), we have $\delta(0, x_t) \geq \epsilon_0 - d$. Then $K_0(d)^v \otimes_{k_v} K_t(d)^v$ is not a product of copies of $K_t(d)^v$.

Suppose that $U_{>r}$ is nonempty. By the choice of d and $\mathcal{S}$, we have $M_{U_{>r}}(d) \subseteq \bigcap_{i \in U_r} K_0(d)K_i(d)$ and $(K_0(d)M_{U_{>r}}(d))^v$ is a product of cyclic extensions of k_v. Hence for $s \in U_{>r}$ we have $e_{s,t} = e_{0,t}$ and $K_0(d)K_s(d) \subseteq K_0(d)K_t(d) = K_s(d)K_t(d)$. As $(K_0(d)K_s(d))^v$ is a product of cyclic extensions of k_v, by Lemma 3.2 $K_0(d)^v \otimes_{k_v} K_s(d)^v$ is a product of copies of $K_s(d)^v$.

Suppose that $U_{<r}$ is not empty. Let $s \in U_{<r}$. As $K_0(d)K_t(d) \subseteq K_0(d)K_s(d) = K_s(d)K_t(d)$ for all $s \in U_{<r}$, by Lemma 3.2 $K_0(d)^v \otimes_{k_v} K_s(d)^v$ is a product of copies of $K_s(d)^v$. Hence $v \in \bigcap_{s \notin U_r} \Sigma_s^{\epsilon_0 - d}$.

Denote by $(\overline{I}_0, ..., \overline{I}_{p^{\epsilon_0 - r}-1})$ the partition of U_r defined by x. By the definition of $\mathcal{S}_x$, we have $\bigcup_{\overline{n} \in \mathbb{Z}/p^{\epsilon_0 - r}\mathbb{Z}} \Omega(\overline{I}_{\overline{n}}) = \Omega_k \setminus \mathcal{S}_x$. Hence there is $\overline{n} \neq 0$ such that $v \in \Omega(\overline{I}_{\overline{n}})$. Let $n \in \mathbb{Z}/p^{\epsilon_0}\mathbb{Z}$ such that $\pi_{\epsilon_0, \epsilon_0 - r}(n) = \overline{n}$. Then $\delta(n, x_i) = \delta(\overline{n}, x_i)$ for all $i \in U_r$. We claim that $v \in \Omega(I_n)$.

First note that $\delta(n, x_t) > \epsilon_0 - d$. To see this, we first suppose that $t \in I_n$. Then $\delta(n, x_t) = \epsilon_0 - r > \epsilon_0 - d$ by the assumption of d. Suppose that $t \notin I_n$. As $v \notin \Sigma_t^{\epsilon_0 - d}$ and $v \in \Omega(\overline{I}_{\overline{n}})$, we have $\delta(n, x_t) > \epsilon_0 - d$.

As $\delta(n, x_t) > \epsilon_0 - d$ and $\delta(0, x_t) \geq \epsilon_0 - d$, we have $\delta(n, 0) \geq \epsilon_0 - d$. Let $i \notin U_r \cup I_n$. Then $a_i = 0$ and $e_i > \epsilon_0 - d$. Therefore $\delta(n, a_i) = \delta(n, \pi_{e_1, e_i}(0)) \geq \epsilon_0 - d$ for all $i \notin U_r \cup I_n$.

Since $v \in \bigcap_{s \notin U_r} \Sigma_s^{\epsilon_0 - d}$ and $\delta(n, a_i) \geq \epsilon_0 - d$ for all $i \notin U_r \cup I_n$, we have $v \in \bigcap_{s \notin U_r \cup I_n} \Sigma_s^{\delta(a_s, n)}$. Combining this with the fact that $v \in \Omega(\overline{I}_{\overline{n}})$, we have $v \in \Omega(I_n)$.

As $x \in \tilde{G}_\omega(K_0, K_{U_r})$, the set S is finite. Hence $a_x \in G_\omega^0(K_0, K')$. The proposition then follows. □

4.2. Patching degrees

Definition 4.9. Define the patching degree Δ_r of U_r to be the maximum nonnegative integer $d \leq \Delta_r^\omega$ satisfying the following:

(1) If $U_{>r}$ is nonempty, then the field $K_0(d)M_{U_{>r}}(d)$ is locally cyclic.

(2) If $U_{<r}$ is nonempty, then the field $K_0(d)M_{U_r}(d)$ is locally cyclic.

If $U_r = \mathcal{I}$, then we set $\Delta_r = \epsilon_0$.

Note that $K_0(r) = K_i(r)$ for all $i \in U_{\geq r}$. From the definition of Δ_r, we have $\Delta_r^\omega \geq \Delta_r \geq r$.

Proposition 4.10. *Suppose that $U_{>r}$ is nonempty. Let r' be the smallest positive integer bigger than r such that $U_{r'}$ is nonempty. Then we have the following:*

(1) *If $r = 0$, then $\Delta_r = \Delta_{r'}$.*
(2) *$\Delta_r \leq \Delta_{r'}$.*
(3) *$\Delta_{r'} - r' \leq \Delta_r - r$.*

Proof. We first show that $\Delta_r \leq \Delta_{r'}$. Note that by our choice of r', we have $U_{<r'} = U_{\leq r}$, which is nonempty. By Proposition 4.3 (2), we $\Delta_r \leq \Delta_r^\omega \leq \Delta_{r'}^\omega$.

Suppose that $U_{>r'}$ is nonempty. By the definition of Δ_r the field $K_0(\Delta_r)M_{U_{>r}}(\Delta_r)$ is locally cyclic. Hence $K_0(\Delta_r)M_{U_{r'}}(\Delta_r)$ and $K_0(\Delta_r)M_{U_{>r'}}(\Delta_r)$ are locally cyclic. Therefore $\Delta_{r'} \geq \Delta_r$.

If $r = 0$, then $U_{<r'} = U_0$. By Proposition 4.3 (1), we have $\Delta_{r'} \leq \Delta_{r'}^\omega = \Delta_0^\omega$. Since $K_0(\Delta_{r'})M_{U_{>0}}(\Delta_{r'}) = K_0(\Delta_{r'})M_{U_{\geq r'}}(\Delta_{r'}) = K_0(\Delta_{r'})M_{U_{r'}}(\Delta_{r'})$ is locally cyclic, we have $\Delta_{r'} \leq \Delta_0$, which proves statement (1).

Now suppose that $r > 0$. We claim that $\Delta_{r'} - r' \leq \Delta_r - r$. Suppose not. Then $\Delta_{r'} - r' \geq \Delta_r + 1 - r$. Combining with Proposition 4.3 (3) we get $\Delta_r^\omega \geq \Delta_r + 1$.

Let $i \in U_r$ and $j \in U_{r'}$. By the definition of $\Delta_{r'}$ we have $K_0(\Delta_{r'})K_j(\Delta_{r'}) \subseteq K_0(\Delta_{r'})K_i(\Delta_{r'})$. Regard $K_0(\Delta_{r'})K_i(\Delta_{r'})$ as a cyclic extension of $K_0(\Delta_{r'})$. Since $K_0(\Delta_{r'})K_j(\Delta_{r'})$ and $K_0(\Delta_{r'})K_i(\Delta_r + 1)$ are both subfields of $K_0(\Delta_{r'})K_i(\Delta_{r'})$, for dimension reasons $K_0(\Delta_{r'})K_i(\Delta_r + 1) \subseteq K_0(\Delta_{r'})K_j(\Delta_{r'})$.

Since $K_0(\Delta_{r'})M_{U_{r'}}(\Delta_{r'})$ is locally cyclic, its subfield $K_0(\Delta_r + 1)M_{U_r}(\Delta_r + 1)$ is also locally cyclic.

As $K_0(\Delta_{r'})M_{U_{>r}}(\Delta_{r'}) = K_0(\Delta_{r'})M_{U_{r'}}(\Delta_{r'})$ and $K_0(\Delta_{r'})M_{U_{r'}}(\Delta_{r'})$ is locally cyclic, its subfield $K_0(\Delta_r + 1)M_{U_{>r}}(\Delta_r + 1)$ is locally cyclic. Hence $\Delta_r \geq \Delta_r + 1$, which is a contradiction. Therefore $\Delta_{r'} - r' \leq \Delta_r - r$. □

Definition 4.11. Suppose that U_r is nonempty. Let $x \in \tilde{G}_\omega(K_0, K_{U_r})$. We say that x is *patchable* if $x_i = 0 \pmod{p^{\epsilon_0 - \Delta_r}}$ for all $i \in U_r$. The subgroup consisting of all patchable elements of $\tilde{G}_\omega(K_0, K_{U_r})$ is called *the patchable subgroup* of $G(K_0, K_{U_r})$. We denote by $\tilde{G}(K_0, K_{U_r})$ the patchable subgroup of $G(K_0, K_{U_r})$.

Note that if $U_0 = \mathcal{I}$, then by above definition every element of $G^0(K_0, K')$ is *patchable*.

Hence in the rest of this section we fix an r such that U_r is nonempty and $U_r \neq \mathcal{I}$ unless we state otherwise explicitly.

In the following we show that x is patchable if and only if a_x defined in equation (4.1) is in $G^0(K_0, K')$.

Proposition 4.12. *Let a_x be defined as in equation (4.1). If $a_x \in G^0(K_0, K')$, then x is patchable.*

Proof. Suppose that $a_x = (a_1, ..., a_m) \in G^0(K_0, K')$. If $x = 0$, then there is nothing to prove. Hence in the following we assume $x \neq 0$. By the definition of a_x we have $a_1 = 0$ and $\mathcal{I} \setminus U_r \subseteq I_0(a_x)$. Set $\epsilon_0 - d = \min_{i \in U_r}\{\delta(0, a_i)\}$, and $U_r' = \{i \in U_r | \epsilon_0 - d = \delta(0, a_i)\}$. As $x \neq 0$, we have $d > r$ and $a_x \notin D$.

By Proposition 4.5, we have that x is algebraically patchable, i.e. $\Delta_r^\omega \geq d$. Since $\Delta_r^\omega \geq d$, it is enough to prove that d satisfies condition (1) and (2) in Definition 4.9.

Suppose that $U_{<r}$ is nonempty. Let $s \in U_{<r}$ and $t \in U_r'$. Then $e_{s,t} = e_{0,s}$. Since $\Delta_r^\omega \geq d$, the field $K_0(d)M_{U_r}(d)$ is contained in $K_0(d)K_s(d)$. By Lemma 3.4, the field $K_0(d)M_{U_r}(d)$ is equal to $K_0(d)K_t(d)$. By Proposition 3.8, we have $K_0(d)K_t(d)$ is locally cyclic. As $K_0(d)K_t(d)$ is locally cyclic, the field $K_0(d)M_{U_r}(d)$ is locally cyclic.

Now suppose that $U_{>r}$ is not empty. For $s \in U_{\geq d}$, we have $K_s(d) = K_0(d)$. If $U_{>r} \neq U_{\geq d}$, then there is $s \in U_{>r} \setminus U_{\geq d}$ such that $K_0(d)M_{U_{>r}}(d) = K_0(d)K_s(d)$. Let $t \in U'_r$. Then $e_{s,t} = e_{0,t}$. Again by Proposition 3.8, we have $K_0(d)K_s(d)$ is locally cyclic. Hence $K_0(d)M_{U_{>r}}(d)$ is locally cyclic. Therefore $\Delta_r \geq d$ and x is patchable. □

Now we prove the converse.

Proposition 4.13. *Let $x \in \tilde{G}(K_0, K_{U_r})$ and a_x be defined as in the equation (4.1). Then $a_x \in G^0(K_0, K')$.*

Proof. If $\Delta_r = r$, then clearly $a_x = 0 \in G(K_0, K')$. Hence we can assume $\Delta_r > r$.

As $x \in \tilde{G}(K_0, K_{U_r})$, we have $S_x = \emptyset$. Since $S_r(\Delta_r)$ and $S_{>r}(\Delta_r)$ are also empty, by Proposition 4.8 we have $a_x \in G^0(K_0, K')$. □

Lemma 4.14. *Let $a = (a_1, ..., a_m) \in G^0_\omega(K_0, K')$ be a nonzero element. Let r be the maximum integer with the following property:*

(1) *There is some $t \in U_r \setminus I_0(a)$ such that $\delta(a_t, 0) = \min_{i \notin I_0(a)} \{\delta(a_i, 0)\}$.*

Set $x = \varpi_r(a) \in \bigoplus_{i \in U_r} \mathbb{Z}/p^{\epsilon_0 - r}\mathbb{Z}$. Then $x \in \tilde{G}_\omega(K_0, K_{U_r})$. Moreover if $a \in G^0(K_0, K')$, then $x \in \tilde{G}(K_0, K_{U_r})$.

Proof. Clearly $x \in G_\omega(K_0, K_{U_r})$. By the choice of t, we have $x \neq 0$. Set $\epsilon_0 - d = \delta(a_t, 0)$. Then $d > r$ as $x \neq 0$. To prove that x is algebraically patchable, it is enough to show that $d \leq \Delta^\omega_r$.

Set $U'_r = \{i \in U_r | \ \epsilon_0 - d = \delta(0, a_i)\}$. By the choice of r we have $U'_r \neq \emptyset$.

Suppose that $U_{>r}$ is nonempty. By the choice of U_r, for all $s \in U_{>r}$ we have either $\delta(0, a_s) > \epsilon_0 - d$ or $s \in I_0(a)$. Let $s \in U_{>r}$. Suppose $\delta(0, a_s) \leq \epsilon_0 - d$. Then $s \in I_0(a)$ and $e_{0,s} \geq d$. As $e_{0,s} \geq d$, we have $K_s(d) = K_0(d) \subseteq K_0(d)K_i(d)$ for all i in U_r.

Suppose that $\delta(0, a_s) > \epsilon_0 - d$. By Proposition 3.8, we have $K_0(d)K_s(d) \subseteq K_0(d)K_i(d)$ for all i in U'_r. Hence by Lemma 4.6 we have $K_0(d)M_{U_{>r}}(d) \subseteq \bigcap_{i \in U_r} K_0(d)K_i(d)$.

Suppose that $U_{<r}$ is nonempty. Let $s \in U_{<r}$. Then $\delta(0, a_s) \geq \epsilon_0 - d$. If $\delta(0, a_s) > \epsilon_0 - d$, then by Proposition 3.8 we have $K_0(d)K_i(d) \subseteq K_0(d)K_s(d)$ for all i in U'_r.

If $\delta(0, a_s) = \epsilon_0 - d$, then by Proposition 3.8 we have $K_0(d)K_s(d) \subseteq K_0(d)K_1(d)$. As $e_{0,s} < r$, we have $[K_0(d)K_i(d) : K_0(d)] < [K_0(d)K_s(d) : K_0(d)]$ for all $i \in U'_r$. Since they are both subfields of the cyclic extension $K_0(d)K_1(d)$ of $K_0(d)$, we have $K_0(d)K_i(d) \subset K_0(d)K_s(d)$ for all $i \in U'_r$.

By Lemma 4.6 we have $K_0(d)M_{U_r}(d) = K_0(d)M_{U'_r}(d) \subseteq \bigcap_{s \in U_{<r}} K_0(d)K_s(d)$. Therefore $d \leq \Delta^\omega_r$ and x is algebraically patchable.

Now suppose further that $a \in G^0(K_0, K')$. Clearly $x \in G(K_0, K_{U_r})$. Suppose that $U_{>r}$ is nonempty. Then as $K_0(d)M_{U>r}(d)$ is contained in a bicyclic extension, by Lemma 3.4 we have $K_0(d)M_{U>r}(d) = K_0(d)K_s(d)$ for some $s \in U_{>r}$. By the choice of r and by Proposition 3.8 (2), we have either $K_0(d) = K_s(d)$ or $K_0(d)K_s(d)$ is locally cyclic.

Suppose that $U_{<r}$ is nonempty. By the same argument we have $K_0(d)M_{U_r}(d) = K_0(d)K_i(d)$ for some $i \in U'_r$. As $a_1 = 0$, by Proposition 3.8 (2) we have $K_0(d)K_i(d)$ is locally cyclic. Hence $d \leq \Delta_r$. □

Proposition 4.15. *We have*

(1) $G_\omega(K_0, K') \simeq D \oplus \bigoplus_r \tilde{G}_\omega(K_0, K_{U_r})$, *where r runs over nonnegative integers such that U_r is nonempty.*
(2) $G(K_0, K') \simeq D \oplus \bigoplus_r \tilde{G}(K_0, K_{U_r})$, *where r runs over nonnegative integers such that U_r is nonempty.*

Please cite this article in press as: T.-Y. Lee, The Tate-Shafarevich groups of multinorm-one tori, J. Pure Appl. Algebra (2022), https://doi.org/10.1016/j.jpaa.2021.106906

Proof. To prove (1), it is sufficient to show that $G^0_\omega(K_0, K') \simeq \bigoplus_r \tilde{G}_\omega(K_0, K_{U_r})$. By Proposition 4.8, we have $G^0_\omega(K_0, K') \supseteq \bigoplus_r \tilde{G}_\omega(K_0, K_{U_r})$.

Let $a \in G^0_\omega(K_0, K')$ and $J(a) = \mathcal{I} \setminus I_0(a)$. We prove that $a \in \bigoplus_r \tilde{G}_\omega(K_0, K_{U_r})$ by induction on $|J(a)|$.

If $|J(a)| = 0$, then $a = 0 \in \bigoplus_r \tilde{G}_\omega(K_0, K_{U_r})$. Suppose that the result holds when $|J(a)| < h$.

Let $|J(a)| = h$ and let r satisfy the condition (1) in Lemma 4.14. By Lemma 4.14, we have $\varpi_r(a) \in \tilde{G}_\omega(K_0, K_{U_r})$. Set $x = \varpi_r(a)$. Then $a_x \in G^0_\omega(K_0, K')$ by Proposition 4.8. Hence $(a'_i)_{i\in\mathcal{I}} = a - a_x \in G^0_\omega(K_0, K')$ and $|J(a')| < h$. By induction hypothesis $a' \in \bigoplus_r \tilde{G}_\omega(K_0, K_{U_r})$. Hence $a \in \bigoplus_r \tilde{G}_\omega(K_0, K_{U_r})$.

Assertion (2) can be proved similarly by using Lemma 4.14 and Proposition 4.13. □

5. The degree of freedom

In this section, we define the *algebraic degree of freedom* (resp. the *degree of freedom*) to describe the generators of the subgroups $\tilde{G}_\omega(K_0, K_{U_r})$'s (resp. $\tilde{G}(K_0, K_{U_r})$'s).

5.1. *l-equivalence relations and levels*

Let $i, j \in \mathcal{I}'$ and l be a nonnegative integer. We say that i, j are l-equivalent and we write $i \underset{l}{\sim} j$ if $e_{i,j} \geq l$ or $i = j$. As K_i are cyclic, it is clear that "$\underset{l}{\sim}$" defines an equivalence relation on any nonempty subset of $\mathcal{I}'$.

For a nonempty subset C of $\mathcal{I}'$, denote by $n_l(C)$ the number of l-equivalence classes of C. In particular $n_0(C) = 1$.

For each $C \subseteq \mathcal{I}'$ with cardinality bigger than 1, we define the *level* of C to be the smallest integer l such that $n_{l+1}(C) > 1$. For each $C = \{i\}$, we define the *level* of C to be ϵ_i. Denote by $L(C)$ the level of C.

5.2. *The degree of freedom of $U_0 = \mathcal{I}$*

Lemma 5.1. *Assume that $U_0 = \mathcal{I}$. Let $l = L(\mathcal{I})$ and c be an equivalence class of $\mathcal{I}/\underset{l+1}{\sim}$. Let $0 \leq f \leq d$ be integers satisfying the following:*

- *(1) $M_{U_0}(d)$ is a subfield of a bicyclic extension.*
- *(2) $K_0(f) \subseteq M_{U_0}(d)$.*

For $i \in \mathcal{I}$, set $x = (x_1, ..., x_m)$ as follows:

$$x_j = \begin{cases} p^{\epsilon_0 - f}, & \text{if } j \in c \\ 0, & \text{otherwise.} \end{cases} \tag{5.1}$$

Then $x \in G_\omega(K_0, K')$.

Proof. By the definition of l, the field $M_{U_0}(d)$ is cyclic if and only if $d \leq l$. In this case we have $f = 0$ and $x = 0 \in G_\omega(K_0, K')$. Hence we assume $M_{U_0}(d)$ is bicyclic in the following.

As there are more than one equivalence classes in $\mathcal{I}/\underset{l+1}{\sim}$, the set $\mathcal{I} \setminus c$ is non-empty and $I_0(x) = \mathcal{I} \setminus c$. Since $L(\mathcal{I}) = l$, we have $e_{s,t} \geq l$ for any s, $t \in \mathcal{I}$. Moreover for $s \in c$ and $t \in \mathcal{I} \setminus c$ we have $e_{s,t} = l$. By Lemma 3.4 we have $M_\mathcal{I}(d) = K_s(d)K_t(d)$ for any $s \in c$ and $t \in \mathcal{I} \setminus c$.

Let s, t be as above. Let $v \in \Omega$ be a place where $M_\mathcal{I}(d)^v$ is locally cyclic at v. We claim that either $K_0(f) \otimes_k K_s(d)^v$ is a product of copies of $K_s(d)^v$ or $K_0(f) \otimes_k K_t(d)^v$ is a product of copies of $K_t(d)^v$.

Please cite this article in press as: T.-Y. Lee, The Tate-Shafarevich groups of multinorm-one tori, J. Pure Appl. Algebra (2022), https://doi.org/10.1016/j.jpaa.2021.106906

Let γ (resp. γ_i's) be the integer such that $K_0(f)^v$ (resp. $K_i(d)^v$) is a product of extensions of degree p^γ (resp. p^{γ_i}) of k^v. Suppose that $K_0(f)^v \otimes_{k^v} K_s(d)^v$ is not a product of copies of $K_s(d)^v$. Then since $M_{\mathcal{I}}(d)^v$ is a product of cyclic extensions, we have $\gamma > \gamma_s$. If $\gamma > \gamma_t$, then $M_{\mathcal{I}}(d)^v = (K_s(d)K_t(d))^v$ is a product of fields of degree less than γ, which is a contradiction as $K_0(f) \subseteq M_{\mathcal{I}}(d)$. Hence $\gamma < \gamma_t$ and $K_0(f)^v \otimes_{k^v} K_t(d)^v$ is a product of copies of $K_t(d)^v$ by the cyclicity of $M_{\mathcal{I}}(d)^v$.

Since $M_{\mathcal{I}}(d)^v$ is locally cyclic at almost all $v \in \Omega_k$, we have $x \in G_\omega(K_0, K')$. □

Remark 5.2. If $M_{\mathcal{I}}(d)$ in Lemma 5.1 is locally cyclic, then by the above proof we have $x \in G(K_0, K')$.

Keep the notation defined as above. The element x has order p^f. Suppose that $f > 0$. Then $d > L(U_0)$ by the above proof. As $K_0(f)K_i(d) \subseteq M_{U_0}(d)$, for dimension reasons $f \leq d - L(U_0)$. On the other hand, by Lemma 3.3 if $K_0(f) \subseteq M_{U_0}(d)$, then $K_0(f) \subseteq M_{U_0}(f + L(U_0))$. Hence we can choose $d = f + L(U_0)$ and define *the algebraic degree of freedom* $f^\omega_{U_0}$ *of* U_0 to be the largest f such that f and $d = f + L(U_0)$ satisfy the conditions in Lemma 5.1. By Proposition 3.8 *the algebraic degree of freedom* $f^\omega_{U_0}$ is the maximal possible order of a class function on $U_0/\underset{l+1}{\sim}$ which lies in $G_\omega(K_0, K')$.

5.3. General cases

Inspired by the definition of $f^\omega_{U_0}$, for U_r nonempty we define the algebraic degree of freedom of U_r to describe the generators of $\tilde{G}_\omega(K_0, K_{U_r})$. Briefly speaking, the group $\tilde{G}_\omega(K_0, K_{U_r})$ is generated by class functions on $U_r/\underset{l}{\sim}$ for $l > L(U_r)$. The order of such a generator is called *the degree of freedom*.

Definition 5.3. For a nonempty U_r, let $l_r = L(U_r)$. Let $f \leq \Delta^\omega_r$ be a nonnegative integer satisfying the following:

(1) The field $M_{U_r}(f + l_r - r)$ is a subfield of a bicyclic extension.
(2) $K_0(f) \subseteq M_{U_r}(f + l_r - r)$.

Then we set $f^\omega_{U_r}$ to be the largest $f \leq \Delta^\omega_r$ satisfying above conditions. We call $f^\omega_{U_r}$ *the algebraic degree of freedom* of U_r.

Remark 5.4. Note that $f = r$ always satisfies the conditions in Definition 5.3. Hence we have $\Delta^\omega_r \geq f^\omega_{U_r} \geq r$.

For $h \geq L(U_r)$ and a class c_0 of $U_r/\underset{h}{\sim}$, we define by recursion *the algebraic degree of freedom of* $c \in c_0/\underset{h+1}{\sim}$ as follows.

Definition 5.5. Keep the notation defined as above. Let $f \leq f^\omega_{c_0}$ be a nonnegative integer satisfying the following:

(1) The field $M_c(f + L(c) - r)$ is a subfield of a bicyclic extension.
(2) $K_0(f) \subseteq M_c(f + L(c) - r)$.

Then we set f^ω_c to be the largest $f \leq f^\omega_{c_0}$ satisfying above conditions. We call f^ω_c *the algebraic degree of freedom* of c.

Inspired by Remark 5.2 we define similarly *the degree of freedom*.

Definition 5.6. For a nonempty U_r, let $h \geq L(U_r)$ and $c \in U_r/\underset{h}{\sim}$. We define *the degree of freedom* f_c of c to be the maximum integer $f \leq f^\omega_c$ such that $M_c(f + L(c) - r)$ is locally cyclic.

Please cite this article in press as: T.-Y. Lee, The Tate-Shafarevich groups of multinorm-one tori, J. Pure Appl. Algebra (2022), https://doi.org/10.1016/j.jpaa.2021.106906

Remark 5.7. From the above definition, we see that $f_c = f_c^\omega$ if $M_c(f_c^\omega + L(c) - r)$ is locally cyclic (e.g. unramified) over k.

Proposition 5.8. *For a nonempty U_r, let $h \geq L(U_r)$ and $c \in U_r/\underset{h}{\sim}$. For all integers $r \leq f \leq f_c^\omega$ and $i \in c$, we have $M_c(f + L(c) - r) = K_0(f)K_i(f + L(c) - r)$.*

Proof. For $f = r$, it is trivial. Hence we assume $f > r$ in the following. This means that $|c| > 1$ and $M_c(f + L(c) - r)$ is not cyclic. By the definition of f_c^ω and Lemma 3.4, there are $i, j \in c$ such that $e_{i,j} = L(c)$ and $M_c(f_c^\omega + L(c) - r) = K_i(f_c^\omega + L(c) - r)K_j(f_c^\omega + L(c) - r)$. As $K_0(f) \subseteq M_c(f_c^\omega + L(c) - r)$, by Lemma 3.3 we have $K_0(f) \subseteq K_i(f + L(c) - r)K_j(f + L(c) - r)$. By dimension reasons $K_0(f)K_i(f + L(c) - r) = K_i(f + L(c) - r)K_j(f + L(c) - r)$.

Since $M_c(f + L(c) - r)$ is contained in $K_i(f_c^\omega + L(c) - r)K_j(f_c^\omega + L(c) - r)$, by Lemma 3.4 we have $M_c(f + L(c) - r) = K_i(f + L(c) - r)K_j(f + L(c) - r)$. Hence $M_c(f + L(c) - r) = K_0(f)K_i(f + L(c) - r)$. □

In the following we assume that U_r is nonempty. We prove a generalization of Lemma 5.1.

Proposition 5.9. *Let $l \geq L(U_r)$ and $c \in U_r/\underset{l}{\sim}$. Let $r \leq f \leq f_c^\omega$ be an integer. Set $l_1 = L(c)$, $c_1 \in c/\underset{l_1+1}{\sim}$, and*

$$\mathcal{S}_c = \{v \in \Omega_k | M_c(f + L(c) - r)^v \text{ is not locally cyclic at } v\}.$$

Then $\Omega_k \setminus \mathcal{S}_c \subseteq (\bigcap_{j \in c_1} \Sigma_j^{\epsilon_0 - f}) \cup (\bigcap_{j \in U_r \setminus c_1} \Sigma_j^{\epsilon_0 - f})$.

Proof. If $f = r$, then clearly $v \in \Sigma_j^{\epsilon_0 - r}$ for all $j \in U_r$ and all $v \in \Omega_k$. Hence in the following we assume that $f > r$, which implies that $|U_r| > 1$. Note that for any equivalence class $c_0 \in U_r/\underset{h}{\sim}$ with $L(U_r) \leq h \leq l$ and $c_0 \supseteq c$, we have $f \leq f_c^\omega \leq f_{c_0}^\omega$.

We prove the statement by induction on l. Consider the case where $l = L(U_r)$. By definition $c = U_r$. As there are more than one equivalence class in $U_r/\underset{l+1}{\sim}$, the set $U_r \setminus c_1$ is non-empty. By Lemma 3.4 we have $M_{U_r}(f + l - r) = K_s(f + l - r)K_t(f + l - r)$ for any $s \in c_1$ and $t \in U_r \setminus c_1$. By Proposition 5.8 we have $K_0(f)K_s(f + l - r) = M_{U_r}(f + l - r) = K_0(f)K_t(f + l - r)$.

By Lemma 3.2 for all $v \in \Omega_k \setminus \mathcal{S}_{U_r}$, either $K_0(f) \otimes_k K_s(f + l - r)^v$ is a product of copies of $K_s(f + l - r)^v$ or $K_0(f) \otimes_k K_t(f + l - r)^v$ is a product of copies of $K_t(f + l - r)^v$. Hence $\Omega_k \setminus \mathcal{S}_{U_r} \subseteq (\bigcap_{j \in c_1} \Sigma_j^{\epsilon_0 - f}) \cup (\bigcap_{j \in U_r \setminus c_1} \Sigma_j^{\epsilon_0 - f})$, and the statement is true for $l = L(U_r)$.

Suppose that the statement is true for $l = h > L(U_r)$. Let $l = h + 1$. If c is also an equivalence class of $U_r/\underset{h}{\sim}$, then the statement is true by the induction hypothesis.

Now suppose that $c \notin U_r/\underset{h}{\sim}$. Let $v \in \Omega_k \setminus \mathcal{S}_c$. It suffices to show that if $v \notin \bigcap_{j \in c_1} \Sigma_j^{\epsilon_0 - f}$, then $v \in \bigcap_{j \in U_r \setminus c_1} \Sigma_j^{\epsilon_0 - f}$. Suppose that $v \notin (\bigcap_{j \in c_1} \Sigma_j^{\epsilon_0 - f})$. We first prove that $v \in (\bigcap_{j \in c \setminus c_1} \Sigma_j^{\epsilon_0 - f})$.

Let $s \in c_1$ such that $v \notin \Sigma_s^{\epsilon_0 - f}$. By Lemma 3.4 the field $M_c(f + l_1 - r)$ is equal to $K_s(f + l_1 - r) \times K_j(f + l_1 - r)$ for any $j \in c \setminus c_1$. Hence $M_c(f + l_1 - r) = K_0(f)K_j(f + l_1 - r) = K_0(f)K_s(f + l_1 - r)$. Since $M_c(f + l_1 - r)^v$ is a product of cyclic extensions of k_v and $v \notin \Sigma_s^{\epsilon_0 - f}$, by Lemma 3.2 we have $K_0(f) \otimes_k K_j(f + l_1 - r)^v$ is a product of copies of $K_j(f + l_1 - r)^v$. This implies $v \in (\bigcap_{j \in c \setminus c_1} \Sigma_j^{\epsilon_0 - f})$.

Next we show that $v \in (\bigcap_{j \in U_r \setminus c} \Sigma_j^{\epsilon_0 - f})$. As $c \notin U_r/\underset{h}{\sim}$, there is some $c_o \in U_r/\underset{h}{\sim}$ such that $c \subsetneq c_0$. This implies that $L(c_0) = h$ and $c \in c_0/\underset{h+1}{\sim}$. By induction hypothesis $\Omega_k \setminus \mathcal{S}_{c_0} \subseteq (\bigcap_{j \in U_r \setminus c} \Sigma_j^{\epsilon_0 - f}) \cup (\bigcap_{j \in c} \Sigma_j^{\epsilon_0 - f})$.

As $h < l_1$, by Proposition 5.8 we have $M_{c_0}(f + h - r) \subseteq M_c(f + l_1 - r)$. Hence $\Omega_k \setminus \mathcal{S}_c \subseteq \Omega_k \setminus \mathcal{S}_{c_0}$, which implies that $v \in \Omega_k \setminus \mathcal{S}_{c_0}$.

Since $c_1 \subseteq c$ and $v \notin (\bigcap_{j\in c_1} \Sigma_j^{\epsilon_0-f})$, $v \notin (\bigcap_{j\in c} \Sigma_j^{\epsilon_0-f})$. Hence $v \in \bigcap_{j\in U_r\setminus c} \Sigma_j^{\epsilon_0-f}$ by induction hypothesis. Combining this with the fact that $v \in (\bigcap_{j\in c\setminus c_1} \Sigma_j^{\epsilon_0-f})$, we have $v \in (\bigcap_{j\in U_r\setminus c_1} \Sigma_j^{\epsilon_0-f})$. □

Corollary 5.10. *Let $l \geq L(U_r)$ and $c \in U_r/\underset{l}{\sim}$. Set $l_1 = L(c)$, $c_1 \in c/\underset{l_1+1}{\sim}$ and $x_{c_1}^{\omega} = (x_i)_{i\in U_r} \in \bigoplus_{i\in U_r} \mathbb{Z}/p^{\epsilon_0-r}\mathbb{Z}$ as follows:*

$$x_j = \begin{cases} p^{\epsilon_0-f_c^{\omega}}, & \text{for all } j \in c_1, \\ 0, & \text{otherwise.} \end{cases} \tag{5.2}$$

Then $x_{c_1}^{\omega} \in G_{\omega}(K_0, K_{U_r})$.

Proof. It is a direct consequence of Proposition 5.9. □

Corollary 5.11. *Keep the notation as in Corollary 5.10. Set $x_{c_1} = (x_i)_{i\in U_r} \in \bigoplus_{i\in U_r} \mathbb{Z}/p^{\epsilon_0-r}\mathbb{Z}$ as follows:*

$$x_j = \begin{cases} p^{\epsilon_0-f_c}, & \text{for all } j \in c_1, \\ 0, & \text{otherwise.} \end{cases} \tag{5.3}$$

Then $x_{c_1} \in G(K_0, K_{U_r})$.

Proof. It is a direct consequence of Proposition 5.9. □

6. The computation of $Ш_{\omega}^2(k, \hat{T}_{L/k})$ and $Ш^2(k, \hat{T}_{L/k})$

In this section we use the (algebraic) patching degrees and the (algebraic) degrees of freedom to describe the groups $Ш^2(k, \hat{T}_{L/k})$ and $Ш_{\omega}^2(k, \hat{T}_{L/k})$.

6.1. Generators of algebraic patchable subgroups and patchable subgroups

For U_r nonempty, set

$$x_{U_r}^{\omega} = (p^{\epsilon_0-\Delta_r^{\omega}})_{i\in U_r} \in G_{\omega}(K_0, K_{U_r});$$

and

$$x_{U_r} = (p^{\epsilon_0-\Delta_r})_{i\in U_r} \in G(K_0, K_{U_r}).$$

In the following we show that the elements x_{c_1}'s (resp. $x_{c_1}^{\omega}$) defined in Corollary 5.11 (resp. Corollary 5.10) are generators of $\tilde{G}(K_0, K_{U_r})$ (resp. $\tilde{G}_{\omega}(K_0, K_{U_r})$).

Proposition 6.1. *For a nonempty U_r, we have the following:*

(1) *The algebraic patchable subgroup $\tilde{G}_{\omega}(K_0, K_{U_r})$ is generated by x_c^{ω} for all $l \geq L(U_r)$ and $c \in U_r/\underset{l}{\sim}$.*
(2) *The patchable subgroup $\tilde{G}(K_0, K_{U_r})$ is generated by x_c for all $l \geq L(U_r)$ and $c \in U_r/\underset{l}{\sim}$.*

Proof. Let $x = (x_i)_{i\in U_r} \in \tilde{G}_{\omega}(K_0, K_{U_r}) \subseteq \bigoplus_{i\in U_r} (\mathbb{Z}/p^{\epsilon_0-r}\mathbb{Z})$. Let t be the smallest index in U_r. After modifying x by a multiple of x_{U_r}, we can assume $x_t = 0$.

Let $I(x) = (I_0(x), ..., I_{p^{\epsilon_0 - r}-1}(x))$ be the partition of U_r associated to x. Set $J = U_r \setminus I_0(x)$. We prove the proposition by induction on $|J|$. If $|J| = 0$, then it is clear that $x = 0 \in \langle x_c^\omega \rangle$. Let h be a positive integer, and suppose that the statement is true for all $|J| < h$.

For $|J| = h$, let $\epsilon_0 - d = \min_{i \in J}\{\delta(0, x_i)\}$. As x is patchable, we have $d \le \Delta_r^\omega$. Let $J' = \{i \in J|\ \delta(0, x_i) = \epsilon_0 - d\}$. Let l be the smallest integer such that there is $c \in U_r/\underset{l}{\sim}$ contained in J'. Pick $i \in c$. We claim that for all $r \le l_0 < l$ and $c_0 \in U_r/\underset{l_0}{\sim}$ containing c, the field $M_{c_0}(d + L(c_0) - r)$ is a subfield of a bicyclic extension.

By the choice of l_0, we have $c_0 \nsubseteq J'$. Set $J_0 = J' \cap c_0$. Pick $j \in J_0$ and $i \in c_0 \setminus J_0$ such that

$$e_{i,j} = \max\{e_{s,t}|\ s \in J_0, t \in c_0 \setminus J_0\}.$$

By Lemma 3.8 we have $F_{d,i,j} = K_0(d)K_i(d + e_{i,j} - r) = K_0(d)K_j(d + e_{i,j} - r)$. Again by Lemma 3.8 for any $s \in c_0 \setminus J_0$, we have $F_{d,s,j} = K_0(d)K_j(d + e_{s,j} - r) \subseteq F_{d,i,j}$. Similarly $F_{d,i,s} \subseteq F_{d,i,j}$ for all $s \in J_0$.

Note that by definition $L(c_0) = \min\{e_{t,t'}|\ t, t' \in c_0\}$. Since $L(c_0) \le e_{s,j} \le e_{i,j}$, we have $K_s(d + L(c_0) - r)K_j(d + L(c_0) - r) \subseteq F_{d,s,j}$ for all $s \in c_0 \setminus J_0$.

By a similar argument, we have $K_s(d + L(c_0) - r)K_i(d + L(c_0) - r) \subseteq F_{d,i,s}$ for all $s \in J_0$. Hence $M_{c_0}(d + L(c_0) - r) \subseteq F_{d,i,j}$.

Next we show that $d \le f_{c_0}^\omega$. As $M_{c_0}(d + L(c_0) - r)$ is a subfield of a bicyclic extension, by Lemma 3.4 there are s and t such that $M_{c_0}(d + L(c_0) - r) = K_s(d + L(c_0) - r)K_t(d + L(c_0) - r)$. Moreover we can choose s, $t \in c_0$ such that $s \notin J_0$ and $t \in J_0$.

To see this, first suppose that J_0 is contained in some $c' \in c_0/\underset{L(c_0)+1}{\sim}$. Then we can pick $s \in c_0 \setminus c'$ and pick $t \in J_0$.

Suppose that $J_0 \nsubseteq c'$ for any $c' \in c_0/\underset{L(c_0)+1}{\sim}$. Then pick $s \in c_0 \setminus J_0$. Let c' be the class of $c_0/\underset{L(c_0)+1}{\sim}$ containing s. Since J_0 is not contained in c', $J_0 \setminus c'$ is nonempty. Pick $t \in J_0 \setminus c'$. Then $e_{s,t} = L(c_0)$. By Lemma 3.4, we have $M_{c_0}(d + L(c_0) - r) = F_{d,s,t}$.

By Lemma 3.8 $K_0(d) \subseteq M_{c_0}(d + L(c_0) - r)$, so we have $d \le f_{c_0}^\omega$. In particular for $c_0 \in U_r/\underset{l-1}{\sim}$ containing c, we have $d \le f_{c_0}^\omega$. By Corollary 5.10, there is an integer n such that the i-th coordinate of nx_c^ω is x_i. Since $c \subseteq J'$, the number of non-zero coordinates of $x - nx_c^\omega$ decreases by at least one. By the induction hypothesis, the element $x - nx_c^\omega$ is generated by patchable diagonal elements and $x_{c'}^\omega$ for $l' \ge L(U_r)$ and $c' \in U_r/\underset{l'}{\sim}$. Statement (1) then follows.

Suppose further that $x \in \tilde{G}(K_0, K_{U_r})$. Then by Lemma 3.8 $M_{c_0}(d + L(c_0) - r) = F_{d,s,t}$ is locally cyclic. Hence $d \le f_{c_0}$. By similar argument we get statement (2). $\square$

Theorem 6.2. *Suppose that U_r is nonempty. Then*

(1) $\tilde{G}_\omega(K_0, K_{U_r}) \simeq \mathbb{Z}/p^{\Delta_r^\omega - r}\mathbb{Z} \oplus \bigoplus_{l \ge L(U_r)} \bigoplus_{c \in U_r/\underset{l}{\sim}} (\mathbb{Z}/p^{f_c^\omega - r}\mathbb{Z})^{n_{l+1}(c)-1}$.

(2) $\tilde{G}(K_0, K_{U_r}) \simeq \mathbb{Z}/p^{\Delta_r - r}\mathbb{Z} \oplus \bigoplus_{l \ge L(U_r)} \bigoplus_{c \in U_r/\underset{l}{\sim}} (\mathbb{Z}/p^{f_c - r}\mathbb{Z})^{n_{l+1}(c)-1}$.

Proof. By Proposition 6.1, the group $\tilde{G}_\omega(K_0, K_{U_r})$ is generated by the x_c^ω for $l \ge L(U_r)$ and $c \in U_r/\underset{l}{\sim}$.

It is clear that the cyclic group $\langle x_{U_r}^\omega \rangle \simeq \mathbb{Z}/p^{\Delta_r^\omega - r}\mathbb{Z}$. For $l \ge L(U_r)$, $c \in U_r/\underset{l}{\sim}$, and $c_1 \in c/\underset{L(c)+1}{\sim}$, the group $\langle x_{c_1}^\omega \rangle$ is isomorphic to $\mathbb{Z}/p^{f_c^\omega - r}\mathbb{Z}$.

For U_r we have

$$\sum_{c \in U_r/\underset{L(U_r)+1}{\sim}} x_c^\omega = p^{\Delta_r^\omega - f_{U_r}^\omega} x_{U_r}^\omega.$$

Let $c_0 \in U_r/\underset{l_0}{\sim}$ and $c \in c_0/\underset{L(c_0)+1}{\sim}$. Set $l = L(c_0) + 1$. If $n_{l+1}(c) > 1$, then we have the relation

$$\sum_{c_1 \in c/\underset{l+1}{\sim}} x^{\omega}_{c_1} = p^{f^{\omega}_{c_0} - f^{\omega}_c} x^{\omega}_c.$$

We choose $n_{l+1}(c)$-1 distinct classes in $c/\underset{l+1}{\sim}$. Let c_i for $1 \le i < n_{l+1}(c)$ be these classes. Then $x^{\omega}_{c_i}$'s generate a group isomorphic to $(\mathbb{Z}/p^{f^{\omega}_c - r}\mathbb{Z})^{n_{l+1}(c)-1}$ and this group is disjoint from the group generated by $x^{\omega}_{c'}$ for $L(U_r) \le h \le l$ and $c' \in U_r/\underset{h}{\sim}$ and by $x^{\omega}_{c'}$ for $c' \in U_r/\underset{l+1}{\sim}$ for $c' \not\subseteq c$.

Hence $\tilde{G}(K_0, K_{U_r}) \simeq \mathbb{Z}/p^{\Delta^{\omega}_r - r}\mathbb{Z} \bigoplus_{l \ge L(U_r)} \bigoplus_{c \in U_r/\underset{l}{\sim}} (\mathbb{Z}/p^{f^{\omega}_c - r}\mathbb{Z})^{n_{l+1}(c)-1}$.

One can prove (2) by a similar argument. □

For $U_0 = \mathcal{I}$, we get the group structure of $\text{Ш}^1(k, T_{L/k})$ immediately from the above theorem.

Corollary 6.3. *Suppose that $U_0 = \mathcal{I}$. Then*

(1) $\text{Ш}^2_{\omega}(k, \hat{T}_{L/k}) \simeq \bigoplus_{l \ge L(\mathcal{I})} \bigoplus_{c \in \mathcal{I}/\underset{l}{\sim}} (\mathbb{Z}/p^{f^{\omega}_c}\mathbb{Z})^{n_{l+1}(c)-1}$.

(2) $\text{Ш}^2(k, \hat{T}_{L/k}) \simeq \bigoplus_{l \ge L(\mathcal{I})} \bigoplus_{c \in \mathcal{I}/\underset{l}{\sim}} (\mathbb{Z}/p^{f_c}\mathbb{Z})^{n_{l+1}(c)-1}$.

Proof. The arguments for (1) and (2) are similar. We show (2) here.

As $U_0 = \mathcal{I}$, we have $\Delta_0 = \epsilon_0$ and $G(K_0, K') = \tilde{G}(K_0, K_{U_0})$. By Theorem 6.2 the group $G(K_0, K') \simeq \mathbb{Z}/p^{\epsilon_0}\mathbb{Z} \bigoplus_{l \ge L(\mathcal{I})} \bigoplus_{c \in \mathcal{I}/\underset{l}{\sim}} (\mathbb{Z}/p^{f_c}\mathbb{Z})^{n_{l+1}(c)-1}$. As the diagonal group D is isomorphic to $\mathbb{Z}/p^{\epsilon_0}\mathbb{Z}$, we have

$$\text{Ш}^2(k, \hat{T}_{L/k}) \simeq \bigoplus_{l \ge L(\mathcal{I})} \bigoplus_{c \in \mathcal{I}/\underset{l}{\sim}} (\mathbb{Z}/p^{f_c}\mathbb{Z})^{n_{l+1}(c)-1}. \quad \square$$

6.2. The Tate-Shafarevich groups

For $i \in U_r$ and $l \ge L(U_r)$, set $a^{\omega}_c = (a_j)_{j \in \mathcal{I}}$ to be the embedding of $x^{\omega}_c = (x_j)_{j \in U_r}$ in $G_{\omega}(K_0, K')$ as follows:

$$a_j = \begin{cases} x_j, & \text{for all } j \in U_r, \\ 0, & \text{otherwise.} \end{cases} \tag{6.1}$$

We define $a_c = (a_j)_{j \in \mathcal{I}}$ to be the embedding of $x_c = (x_j)_{j \in U_r}$ in $G(K_0, K')$ in the same way.

Proposition 6.4. *We have the following:*

(1) *The group $G_{\omega}(K_0, K')$ is generated by the diagonal group D and the a^{ω}_c's defined as above.*
(2) *The group $G(K_0, K')$ is generated by the diagonal group D and the a_c's defined as above.*

Proof. Let $a = (a_i)_{i \in \mathcal{I}} \in G_{\omega}(K_0, K')$. After modifying by a diagonal element, we can assume that $a_1 = 0$. By Proposition 4.15 we have $a \in \bigoplus_r \tilde{G}_{\omega}(K_0, K_{U_r})$. Then a is generated by D and x^{ω}_c's by Proposition 6.1.

A similar argument proves (2). □

Theorem 6.5. *Keep the notations as above. Then we have*

$$G_\omega(K_0,K')\simeq \mathbb{Z}/p^{\epsilon_0}\mathbb{Z}\bigoplus_{r\in\mathcal{R}\setminus\{0\}}\mathbb{Z}/p^{\Delta_r^\omega-r}\mathbb{Z}\bigoplus_{r\in\mathcal{R}}\bigoplus_{l\geq L(U_r)}\bigoplus_{c\in U_r/\underset{l}{\sim}}(\mathbb{Z}/p^{f_c^\omega-r}\mathbb{Z})^{n_{l+1}(c)-1};$$

and

$$G(K_0,K')\simeq \mathbb{Z}/p^{\epsilon_0}\mathbb{Z}\bigoplus_{r\in\mathcal{R}\setminus\{0\}}\mathbb{Z}/p^{\Delta_r-r}\mathbb{Z}\bigoplus_{r\in\mathcal{R}}\bigoplus_{l\geq L(U_r)}\bigoplus_{c\in U_r/\underset{l}{\sim}}(\mathbb{Z}/p^{f_c-r}\mathbb{Z})^{n_{l+1}(c)-1}.$$

As a consequence, we have

$$Ш^2_\omega(k,\hat{T}_{L/K})\simeq \bigoplus_{r\in\mathcal{R}\setminus\{0\}}\mathbb{Z}/p^{\Delta_r^\omega-r}\mathbb{Z}\bigoplus_{r\in\mathcal{R}}\bigoplus_{l\geq L(U_r)}\bigoplus_{c\in U_r/\underset{l}{\sim}}(\mathbb{Z}/p^{f_c^\omega-r}\mathbb{Z})^{n_{l+1}(c)-1};$$

and

$$Ш^1(k,T_{L/K})\simeq \bigoplus_{r\in\mathcal{R}\setminus\{0\}}\mathbb{Z}/p^{\Delta_r-r}\mathbb{Z}\bigoplus_{r\in\mathcal{R}}\bigoplus_{l\geq L(U_r)}\bigoplus_{c\in U_r/\underset{l}{\sim}}(\mathbb{Z}/p^{f_c-r}\mathbb{Z})^{n_{l+1}(c)-1}.$$

Proof. By Proposition 6.4, the group $G_\omega(K_0,K')$ is generated by the diagonal group D and the group $\bigoplus_{r\in\mathcal{R}}\tilde{G}_\omega(K_0,K_{U_r})$. If $U_0=\mathcal{I}$, then it is Theorem 6.2.

Suppose that $U_0\neq\mathcal{I}$. Set $a_\mathcal{I}=(1,...,1)$, which is a generator of D. Then we have the relation

$$\sum_{r\in\mathcal{R}}p^{\Delta_r^\omega-\Delta_0^\omega}a^\omega_{U_r}=p^{\epsilon_0-\Delta_0^\omega}a_\mathcal{I}.$$

Note that by Proposition 4.3 (1) and (2), we have $\Delta_0^\omega>0$ and $\Delta_r^\omega-\Delta_0^\omega\geq 0$. Hence $p^{\epsilon_0-\Delta_0^\omega}a_\mathcal{I}$ and $a^\omega_{U_0}$ are nonzero. It is clear that the element $p^{\epsilon_0-\Delta_0^\omega}a_\mathcal{I}$ generates the intersection $D\cap\bigoplus_{r\in\mathcal{R}}\tilde{G}_\omega(K_0,K_{U_r})$. Hence

$$G_\omega(K_0,K')\simeq D\bigoplus_{l\geq L(U_0)}\bigoplus_{c\in U_0/\underset{l}{\sim}}(\mathbb{Z}/p^{f_c^\omega}\mathbb{Z})^{n_{l+1}(c)-1}\bigoplus_{r\in\mathcal{R}\setminus\{0\}}\tilde{G}_\omega(K_0,K_{U_r}).$$

Applying Proposition 4.10 (1) and (2) instead of Proposition 4.3, one proves in a similar way the statement of $G(K_0,K')$. □

Remark 6.6. Let $\mathcal{K}$ be a minimal Galois extension of k which splits $T_{L/k}$ and denote its Galois group by $\mathcal{G}$. An alternative way to calculate $Ш^2_\omega(\mathcal{G},\hat{T}_{L/k})$ is to express the degree of freedom and patching degree in terms of the group structure of $\mathcal{G}$. Then one can use the method in [2] to get $Ш^2_\omega(\mathcal{G},\hat{T}_{L/k})$ from $Ш^2(l,M)$ for some finite extension l and some $\mathrm{Gal}(k_s/k)$-module M.

7. Examples

In this section, we give some examples where more explicit descriptions of the groups $Ш^2(k,\hat{T}_{L/k})$ and $Ш^2_\omega(k,\hat{T}_{L/k})$ are obtained. We first note the following case.

Proposition 7.1. *If* $\bigcap_{i\in U_0}K_0K_i=K_0$, *then* $Ш^2(k,\hat{T}_{L/k})=Ш^2_\omega(k,\hat{T}_{L/k})=0$.

Proof. It is enough to show that $Ш^2_\omega(k,\hat{T}_{L/k})=0$. Let $l=L(U_0)$. If $f^\omega_{U_0}\neq 0$, then $K_0(f^\omega_{U_0})M_{U_0}(f^\omega_{U_0}+l)$ is bicyclic and by Proposition 5.8 it is contained in $\bigcap_{i\in U_0}K_0K_i$, which is a contradiction. Therefore $f^\omega_{U_0}=0$. If $U_0=\mathcal{I}$, then $Ш^2_\omega(k,\hat{T}_{L/k})=0$ by Corollary 6.3.

Suppose that $U_0 \neq \mathcal{I}$. Choose $r > 0$ such that U_r is nonempty. Since $\bigcap_{i \in U_0} K_0 K_i = K_0$, we have $\Delta_r^\omega = r$. Hence $f_c^\omega = r$ for all $c \in U_r / \underset{l}{\sim}$. By Theorem 6.5 $Ш_\omega^2(k, \hat{T}_{L/k}) = 0$. $\square$

Example 7.2. Let $k = \mathbb{Q}$ and ζ_n be a primitive n-th root of unity. Let $p_0, ..., p_m$ be distinct odd primes and n_i be positive integers. Set $K_i = \mathbb{Q}(\zeta_{p_i{}^{n_i}})$ for $0 \leq i \leq m$. Then K_i are cyclic extensions. Since $\bigcap_{i \in \mathcal{I}} K_0 K_i = K_0$, by Proposition 7.1 the group $Ш_\omega^2(k, \hat{T}_{L/k}) = 0$.

Proposition 7.3. *Suppose that K_i are linearly disjoint extensions of k for all $i \in \mathcal{I}'$. Let f be the maximum integer such that $M_{\mathcal{I}'}(f)$ is a subfield of a bicyclic extension; and f' be the maximum integer such that $M_{\mathcal{I}'}(f')$ is bicyclic and locally cyclic. Then $Ш_\omega^2(k, \hat{T}_{L/k}) \simeq (\mathbb{Z}/p^f\mathbb{Z})^{m-1}$ and $Ш^2(k, \hat{T}_{L/k}) \simeq (\mathbb{Z}/p^{f'}\mathbb{Z})^{m-1}$.*

Proof. Since K_i are disjoint extensions for all $i \in \mathcal{I}'$, we have $U_0 = \mathcal{I}$, $L(U_0) = 0$ and $n_1(U_0) = m$. Then by definition we have $f_{U_0}^\omega = f$ and $f_{U_0} = f'$. The proposition follows from Corollary 6.3. $\square$

Example 7.4. Let $k = \mathbb{Q}(i)$. Let $K_0 = k(\sqrt[4]{17})$, $K_1 = k(\sqrt[4]{17 \times 13})$ and $K_2 = k(\sqrt[4]{13})$. Then $M_{\mathcal{I}'}(2)$ is a bicyclic extension of k with Galois group $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$. Hence $Ш_\omega^2(k, \hat{T}_{L/k}) \simeq \mathbb{Z}/4\mathbb{Z}$.

It is clear that $M_{\mathcal{I}'}(2)_v$ is a product of cyclic extensions if v is an unramified place. Let $\mathcal{P}$ be the prime ideal associated to v. If $M_{\mathcal{I}'}(2)$ is ramified at v, then $\mathcal{P} \cap \mathbb{Z} \in \{(2), (13), (17)\}$. Since 17 is not a 4-th power root in $\mathbb{Q}_{13}$, the field $M_{\mathcal{I}'}(2)_{17}$ is not cyclic.

It is easy to check that $M_{\mathcal{I}'}(1)$ is locally cyclic. Hence by Proposition 7.3 we have $Ш^2(k, \hat{T}_{L/k}) \simeq \mathbb{Z}/2\mathbb{Z}$.

Example 7.5. Let $k = \mathbb{Q}(i)$. Let $K_0 = k(\sqrt[4]{17})$, $K_1 = k(\sqrt[4]{17 \times 409})$ and $K_2 = k(\sqrt[4]{409})$. Then $M_{\mathcal{I}'}(2)$ is a bicyclic extension of k with Galois group $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$. Hence $Ш_\omega^2(k, \hat{T}_{L/k}) \simeq \mathbb{Z}/4\mathbb{Z}$.

We claim that $M_{\mathcal{I}'}(2)$ is locally cyclic. Let $v \in \Omega_k$. It is clear that $M_{\mathcal{I}'}(2)_v$ is a product of cyclic extensions if v is an unramified place. Let $\mathcal{P}$ be the prime ideal associated to v. If $M_{\mathcal{I}'}(2)$ is ramified at v, then $\mathcal{P} \cap \mathbb{Z} \in \{(2), (17), (409)\}$. However 409 and 17 are quartic residues of each other, and 17 has a 4-th root in $\mathbb{Q}_2$. Therefore $M_{\mathcal{I}'}(2)$ is locally cyclic and $f_{U_0} = 2$. By Proposition 7.3 we have $Ш^2(k, \hat{T}_{L/k}) \simeq \mathbb{Z}/4\mathbb{Z}$. In this case weak approximation holds for $T_{L/k}$-torsors with a k-point.

Proposition 7.6. *Let F be a bicyclic extension of k with Galois group $\mathbb{Z}/p^n\mathbb{Z} \times \mathbb{Z}/p^n\mathbb{Z}$. Let K_i be distinct cyclic subfields of F with degree p^n. Then*

$$Ш_\omega^2(k, \hat{T}_{L/k}) \simeq \bigoplus_{r \in \mathcal{R} \setminus \{0\}} \mathbb{Z}/p^{n-r}\mathbb{Z} \bigoplus_{r \in \mathcal{R}} \bigoplus_{l \geq L(U_r)} \bigoplus_{c \in U_r / \underset{l}{\sim}} (\mathbb{Z}/p^{n-l}\mathbb{Z})^{n_{l+1}(c)-1}.$$

Proof. Regard F as a cyclic extension of K_0.

For a nonempty U_r and all $i \in U_r$, the field $K_0 K_i$ is the unique degree p^{n-r} extension of K_0 contained in F. Hence $\Delta_r^\omega = n$ for all $r \in \mathcal{R}$.

For $l \geq L(U_r)$, the field $M_c(n)$ is contained in F and its Galois group is isomorphic to $\mathbb{Z}/p^n\mathbb{Z} \times \mathbb{Z}/p^{n-L(c)}$. We claim that $f_c^\omega = n - L(c) + r$. Regard F as a cyclic field extension of K_i. As subfields of F, both $K_0(n-L(c)+r)K_i$ and $M_c(n)$ are cyclic extensions of K_i of degree $p^{n-L(c)}$. Hence $K_0(n-L(c)+r)K_i = M_c(n)$ and $f_c^\omega = n - L(c) + r$.

For a class $c \in U_r / \underset{l}{\sim}$, we have $n_{l+1}(c) > 1$ if and only if $L(c) = l$. The proposition then follows. $\square$

Example 7.7. Let $k = \mathbb{Q}(i)$. Let $K_0 = k(\sqrt[4]{13})$, $K_1 = k(\sqrt[4]{17})$, $K_2 = k(\sqrt[4]{13 \times 17^2})$. Then $1 \in U_0$ and $2 \in U_1$. By Proposition 7.6, we have $Ш_\omega^2(k, \hat{T}_{L/k}) \simeq \mathbb{Z}/2\mathbb{Z}$. As the field K_0K_2 is locally cyclic, we have $\Delta_1 = 2$. Hence $Ш^1(k, T_{L/k}) \simeq \mathbb{Z}/2\mathbb{Z}$. In this case weak approximation holds for $T_{L/k}$-torsors with a k-point.

Please cite this article in press as: T.-Y. Lee, The Tate-Shafarevich groups of multinorm-one tori, J. Pure Appl. Algebra (2022), https://doi.org/10.1016/j.jpaa.2021.106906

References

[1] E. Bayer-Fluckiger, T.-Y. Lee, R. Parimala, Hasse principles for multinorm equations, Adv. Math. 356 (2019).

[2] E. Bayer-Fluckiger, R. Parimala, On unramified Brauer groups of torsors over tori, Doc. Math. 25 (2020) 1263–1284.

[3] B. Conrad, O. Gabber, G. Prasad, Pseudo Reductive Groups, 2nd ed., New Mathematical Monographs, vol. 26, Cambridge University Press, 2015.

[4] C. Demarche, D. Wei, Hasse principle and weak approximation for multinorm equations, Isr. J. Math. 202 (1) (2014) 275–293.

[5] A. Macedo, On the obstruction to the Hasse principle for multinorm equations, arXiv:1912.11941.

[6] T. Pollio, On the multinorm principle for finite Abelian extensions, Pure Appl. Math. Q. 10 (2014) 547–566.

[7] T. Pollio, A.S. Rapinchuk, The multinorm principle for linearly disjoint Galois extensions, J. Number Theory 133 (2013) 802–821.

[8] J.-J. Sansuc, Groupe de Brauer et arithmétique des groupes algébriques linéaires sur un corps de nombres, J. Reine Angew. Math. 327 (1981) 12–80.

Please cite this article in press as: T.-Y. Lee, The Tate-Shafarevich groups of multinorm-one tori, J. Pure Appl. Algebra (2022), https://doi.org/10.1016/j.jpaa.2021.106906