COMPUTING TATE-SHAFAREVICH GROUPS OF MULTINORM ONE TORI OF KUMMER TYPE

JUN-HAO HUANG, FAN-YUN HUNG, PEI-XIN LIANG, AND CHIA-FU YU

Abstract. A multinorm one torus associated to a commutative étale algebra $L$ over a global field $k$ is of Kummer type if each factor of $L$ is a cyclic Kummer extension. In this paper we compute the Tate-Shafarevich group of such tori based on recent works of Bayer-Fluckiger, T.-Y. Lee and Parimala, and of T.-Y. Lee. We also implement an effective algorithm using SAGE which computes the Tate-Shafarevich groups when each factor of $L$ is contained in a fixed concrete bicyclic extension of $k$.

1. Introduction

Let $k$ be a global field and let $L = \prod_{i=0}^{m} K_i$ be a product of finite separable field extensions $K_i$ of $k$. The norm map $N_{L/k}$ from $L$ to $k$ is defined by $N_{L/k}(x) := \prod_i N_{K_i/k}(x_i)$ for $x = (x_i) \in L$. Let $\mathcal{A}_k$ denote the adele ring of $k$ and $\mathcal{A}_L := L \otimes_k \mathcal{A}_k = \prod_{i=0}^{m} \mathcal{A}_{K_i}$ the adele ring of $L$. We have the norm map $N_{L/k} : \mathcal{A}_L^\times \to \mathcal{A}_k^\times$, sending $(x_i)$ to $\prod_i N_{K_i/k}(x_i)$. We say that the multinorm principle holds for $L/k$ if

$$k^\times \cap N_{L/k}(\mathcal{A}_L^\times) = N_{L/k}(L^\times).$$

The quotient group

$$\text{III}(L/k) := \frac{k^\times \cap N_{L/k}(\mathcal{A}_L^\times)}{N_{L/k}(L^\times)}$$

is called the Tate-Shafarevich group of $L/k$, which measures the deviation of the validity of the multinorm principle.

Hürlimann [3, Proposition 3.3] showed that the multinorm principle holds for $L = K_0 \times K_1$ provided that one of $K_i$ is cyclic and the other is Galois (the second condition is actually superfluous as later proved by [1, Proposition 4.1]). Pollio and Rapinchuk [9, Theorem, p. 803] showed the case when the Galois closures of $K_0$ and $K_1$ are linearly disjoint; the former author proved [3, Theorem 1] that if $K_0$ and $K_1$ are abelian extensions of $k$, then $\text{III}((K_0 \times K_1)/k) = \text{III}((K_0 \cap K_1)/k)$. Demarche and D. Wei [2] constructed a family of examples, showing that the equality $\text{III}((K_0 \times K_1)/k) = \text{III}((K_0 \cap K_1)/k)$ is no longer true when $K_0$ and $K_1$ are non-abelian Galois extensions. Bayer-Fluckiger, T.-Y. Lee and Parimala [1] studied the Tate-Shafarevich group of general multinorm one tori in which $K_0$ is a cyclic extension. Among others, they computed $\text{III}(L/k)$ in the case of products of extensions of prime degree $p$. Very recently T.-Y. Lee [4] computed explicitly $\text{III}(L/k)$ for the cases where every factor is cyclic of degree $p$-power, and by the reduction result of [1], of arbitrary degree. The study of the multinorm principle is also inspired by the work of Prasad and Rapinchuk [11], where they settled the problem of the local-global principle for embeddings of fields with involution into simple algebras with involution.

Date: November 22, 2022.

2010 Mathematics Subject Classification. 11G35, 12G05.

Key words and phrases. Multinorm principles, Tate-Shafarevich groups, Multinorm one tori.
The aim of this article is to compute more examples of the Tate-Shafarevich groups of multiple norm one tori based on T.-Y. Lee’s general formulas. We consider the étale $k$-algebras $L = \prod K_i$, where each $K_i/k$ is a cyclic extension of $p$-power degree and $k$ contains the roots of unity of sufficiently large degree of $p$ (prime to the characteristic of $k$). The idea is to translate all invariants in Lee’s formulas from the number-theoretic description into a combinatorial one. This allows us to compute the Tate-Shafarevich groups much more effectively. The main reason is that computing the decomposition groups of a Galois extension of large degree by computer is extremely time-consuming. We implement an algorithm using SageMath which computes $\text{III}(L)$ for input data where $k = \mathbb{Q}(\zeta_{p^n})$ is the $p^n$-th cyclotomic field and $K_i$ are cyclic subextensions of a bicyclic extension $k(\zeta_{p^{l_1}}, \zeta_{p^{l_2}})$ with primes $l_1, l_2 \neq p$, subject to the condition $\cap_{i=0}^{n} K_i = k$. As our algorithm is based on a combinatorial description, the computing time does not take much longer when $p$ and $n$ are large.

This paper is organized as follows. In Section 2, we organize several results of Bayer-Fluckiger–T.-Y. Lee and Parimala and describe formulas for the Tate-Shafarevich groups due to T.-Y. Lee. Section 3 discusses the assumptions in Theorem 2.13. In Section 4 we translate all invariants in Lee’s formulas from the number-theoretic description into a combinatorial one in the case where $k = \mathbb{Q}(\zeta_{p^n})$ is the $p^n$-th cyclotomic field. Section 5 computes the decomposition groups of any subfield extension of the aforementioned bicyclic extension $k(\zeta_{p^{l_1}}, \zeta_{p^{l_2}})$. Putting all together in the last section, we compute the Tate-Shafarevich group of the multinorm one torus in questions and show examples.

2. THE TATE-SHAFAREVICH GROUPS OF MULTINORM ONE TORI

In this section, we organize several results from Bayer-Fluckiger–Lee–Parimala and describe formulas for the Tate-Shafarevich groups of multinorm one tori due to T.-Y. Lee. Let $k$ be a global field and $k_0$ be a separable field of $k$ whose Galois group is denoted by $\Gamma_k$. Let $\Omega_k$ be the set of all places of $k$. Let $T$ be an algebraic torus over $k$. Denote by $\hat{T} := \text{Hom}_{k_0}(T, \mathbb{G}_m)$ be the character group of $T$; it is a finite free $\mathbb{Z}$-module with a continuous action of $\Gamma_k$. Let $H^i(k, \hat{T})$ denote the $i$-th Galois cohomology group of $\Gamma_k$ with coefficients in $\hat{T}$.

**Definition 2.1.** The $i$-th Tate-Shafarevich group and algebraic Tate-Shafarevich group of $\hat{T}$ are defined by

$$\text{III}^i(k, \hat{T}) := \text{Ker} \left( H^i(k, \hat{T}) \to \prod_{v \in \Omega_k} H^i(k_v, \hat{T}) \right)$$

and

$$\text{III}^i_0(k, \hat{T}) := \left\{ [C] \in H^i(k, \hat{T}) \mid [C]_v = 0 \text{ for almost all } v \in \Omega_k \right\},$$

respectively, where $[C]_v$ is the class of $[C]$ in $H^i(k_v, \hat{T})$ under the restriction map $H^i(k, \hat{T}) \to H^i(k_v, \hat{T})$.

Let $L = \prod_{i=0}^m K_i$ be an étale algebra over $k$, where each $K_i$ is a cyclic extension of $k$ of degree $d_i$ in $k_s$. Let $N_{L/k} : R_{L/k} \mathbb{G}_m,L \to \mathbb{G}_m,k$ be the norm morphism, and let $T_{L/k} = \text{Ker} N_{L/k}$ be the multinorm one torus associated to $L/k$. Put $I = \{1, \ldots, m\}$ and $K' := \prod_{i \in I} K_i$.

Let $E := K_0 \otimes_k K' := \prod_{i \in I} E_i$, where $E_i := K_0 \otimes_k K_i$. We may regard the $k$-étale algebra $E$ as an étale algebra over $K_0$ or over $K'$. Let $N_{E/K_0}$ and $N_{E/K'}$ be the norm maps from $R_{E/k} \mathbb{G}_m,E$ to itself, and define a morphism $f : R_{E/k} \mathbb{G}_m,E \to R_{L/k} \mathbb{G}_m,L$ by $f(x) = (N_{E/K_0}(x)^{-1}, N_{E/K'}(x))$. One easily checks that the image of $f$ is equal to $T_{L/k}$. Let $S_{K_0,K'}$ be the $k$-torus defined by the following exact sequence

$$1 \longrightarrow S_{K_0,K'} \longrightarrow R_{E/k} \mathbb{G}_m,E \overset{f}{\longrightarrow} T_{L/k} \longrightarrow 1.$$
The algebraic torus $S_{K_0,K'}$ also fits in the following exact sequence

$$1 \rightarrow S_{K_0,K'} \rightarrow R_{K'/k}(T_{E/k'}) \xrightarrow{N_{E/K_0}} T_{K_0/k} \rightarrow 1.$$  

Here $R_{K'/k}(T_{E/k'}) = \prod_{i \in I} R_{K_i/k}(T_{E_i/K_i})$.

**Proposition 2.2.** [Lemma 3.1] There is a functorial natural isomorphism

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

It follows from [2.1] that there is a natural isomorphism $H^1(k, T_{L/k}) \simeq H^2(k, S_{K_0,K'})$. Then Proposition 2.2 follows from the Poitou-Tate duality.

Define

$$\Pi(L) := \Pi^2(k, \hat{T}_{L/k}) \quad \text{and} \quad \Pi_L(L) := \Pi^2_2(k, \hat{T}_{L/k}).$$

For any prime number $p$ and any cyclic extension $M$ of $k$, let $M(p)$ denote the largest subfield of $M$ such that $[M(p) : k]$ is a power of $p$. Also, if $p$ divides $[M : k]$, we denote by $M(p)_{\text{prim}}$ the unique subfield of $M(p)$ of degree $p$ over $k$.

**Proposition 2.3.** [Propositions 5.16 and 8.6] Let $L = \prod_{i=0}^{m} K_i$ be a product of cyclic extensions of degree $d_i$ over $k$. Set $L(p) := K_0(p) \times K' \times L^*(p) := \prod_{i=0}^{m} K_i(p)$. Then we have isomorphisms

$$\Pi(L) = \bigoplus_{p \mid d} \Pi(L(p)),$$

and

$$\Pi(L) = \bigoplus_{p \nmid d} \Pi(L^*(p)),$$

where $d = \gcd(d_0, \ldots, d_m)$.

Note that if $K_i(p) = k$ for some $i$, then $\Pi(L^*(p)) = 0$. Thus, if $p \nmid d$, then $\Pi(L^*(p)) = 0$.

**Theorem 2.4.** Let the notation be as Proposition 2.3. Assume that the field extensions $K_{i}(p)$ are linearly disjoint over $k$. Then

$$\Pi(L^*(p)) = 0 \iff \Pi(L^*(p)_{\text{prim}}) = 0,$$

where $L^*(p)_{\text{prim}} := \prod_{i=0}^{m} K_i(p)_{\text{prim}}$.

**Proof.** This is [Theorem 8.1]. Note that we add an additional condition that $\{K_i(p)\}$ are linearly disjoint over $k$. This is because that the proof relies on [Proposition 5.13], which should be modified by adding this condition; see also Remark 2.6.

By Theorem 2.4, it is important to compute $\Pi(L)$ in the case where $L$ is a product of cyclic extensions of degree $p$. More generally we have the following result [Proposition 8.5].

**Proposition 2.5.** Let $p$ be a prime number, and $L = \prod_{i=0}^{m} K_i$ a product of distinct field extensions of degree $p$ such that $K_0/k$ is cyclic. Then $\Pi(L) \neq 0$ only if every field $K_i$ is contained a field extension $F/k$ of degree $p^2$ and all local degrees of $F$ are $\leq p$. Moreover, if the above condition is satisfied, then $\Pi(L) \simeq (\mathbb{Z}/p\mathbb{Z})^{n-1}$.

**Remark 2.6.** Theorem 8.1 of [I] is incorrect as stated. Lee gave a counterexample to it (Example 7.7): Let $k = \mathbb{Q}(i), K_0 = k(\sqrt{3}), K_1 = k(\sqrt{17})$ and $k(\sqrt{13} \cdot 17^2)$. We have $\Pi(L) = \mathbb{Z}/2\mathbb{Z}$, while $L_{\text{prim}} = k(\sqrt{13}) \times k(\sqrt{17}) \times k(\sqrt{3})$ and $\Pi(L_{\text{prim}}) = 0$. 


2.2. In what follows, we let \( L = \prod_{i=0}^{m} K_i \), where \( K_i \) are cyclic extensions of \( k \) of degree \( p^{e_i} \). Assume \( \cap_{i=0}^{m} K_i = k \) and \( e_0 = \min_{0 \leq i \leq m} \{e_i\} \). For any \( i, j \in I \), we set
\[
\begin{align*}
(i) & \quad p^{e_{i,j}} = [K_i \cap K_j : k], \\
(ii) & \quad e_i = e_0 - e_{0,i}.
\end{align*}
\]
Without loss of generality, we assume that \( e_i \geq e_{i+1} \), and notice that \( e_1 = e_0 \) since \( K_0 \cap K_1 = k \). Note that \( p^{e_i} = [M_i : K_i] \), where \( M_i = K_0 K_i \) and one has \( H^1(k, \hat{T}_{E_i/K_i}) \simeq \mathbb{Z}/p^{e_i} \mathbb{Z} \).

For any \( 0 \leq d \leq e_i \), let \( K_i(d) \) denote the subfield of \( K_i \) of degree \( p^d \) over \( k \). For a nonempty subset \( c \subseteq I \) and an integer \( d > 0 \), set \( M_c(d) := \langle K_i(d) \rangle_{i \in c}, \) the composite of \( K_i(d) \) for \( i \in c \). For \( 0 \leq r \leq e_0 \), set
\[
U_r := \{ i \in I \mid e_{0,i} = r \}, \quad U_{r>} := \{ i \in I \mid e_{0,i} > r \}, \quad \text{and} \quad U_{r<} := \{ i \in I \mid e_{0,i} < r \}.
\]
In order to describe formulas for the Tate-Shafarevich group of multinorm one tori due to T.-Y. Lee, we need to introduce the following invariants.

**Definition 2.7.** For a nonempty set \( U_r \), the algebraic patching degree \( \Delta^*_{p,r} \) of \( U_r \) is the largest nonnegative integer \( d \leq e_0 \) satisfying the following two conditions:
\[
\begin{align*}
(i) & \quad \text{If } U_{r>} \text{ is nonempty, then } M_{U_{r>}}(d) \subseteq \bigcap_{i \in U_r} K_0(d) K_i(d), \\
(ii) & \quad \text{If } U_{r<} \text{ is nonempty, then } M_{U_{r<}}(d) \subseteq \bigcap_{i \in U_r} K_0(d) K_i(d).
\end{align*}
\]
If \( U_r = I \) (so \( r = 0 \)), then we set \( \Delta^*_{0} = e_0 \).

We say that a field extension \( M \) of \( k \) is locally cyclic if its completion \( M \otimes_k k_v \) at \( v \) is a product of cyclic extensions of \( k_v \) for all places \( v \in \Omega_k \). Moreover, if \( M \) is a finite Galois extension of \( k \), then \( M/k \) is locally cyclic if and only if every decomposition group of \( M \) over \( k \) is cyclic.

**Definition 2.8.** The patching degree \( \Delta_r \) of \( U_r \) is the largest nonnegative integer \( d \leq \Delta^*_{p,r} \) satisfying the following two conditions:
\[
\begin{align*}
(i) & \quad \text{If } U_{r>} \text{ is nonempty, then } K_0(d) M_{U_{r>}}(d) \text{ is locally cyclic}, \\
(ii) & \quad \text{If } U_{r<} \text{ is nonempty, then } K_0(d) M_{U_{r<}}(d) \text{ is locally cyclic}.
\end{align*}
\]
If \( U_0 = I \), then we set \( \Delta_0 = e_0 \).

**Definition 2.9.** Let \( i, j \in I \) and \( l \) be a nonnegative integer. We say that \( i \sim j \) if \( e_{i,j} \geq l \) or \( i = j \). For any nonempty subset \( c \subseteq I \), let \( n_l(c) \) be the number of \( l \)-equivalence classes of \( c \).

**Definition 2.10.** For each \( c \subseteq I \) with \( |c| \geq 1 \), the level of \( c \) is defined by
\[
L(c) := \min\{e_{i,j} : i, j \in c \}.
\]

**Definition 2.11.** (1) For a nonempty set \( U_r \), let \( l_r = L(U_r) \) and let \( f_{\omega,U}^r \) be the largest nonnegative integer \( f \leq \Delta^*_{p,r} \) satisfying the following two conditions:
\[
\begin{align*}
(i) & \quad \text{The field } M_{U_r}(f + l_r - r) \text{ is a subfield of a bicyclic extension}, \\
(ii) & \quad K_0(f) \subseteq M_{U_r}(f + l_r - r).
\end{align*}
\]
We call \( f_{\omega,U}^r \) the algebraic degree of freedom of \( U_r \).

(2) Similarly, for any \( h \)-equivalence class \( c \subseteq U_r \) with \( h \geq L(U_r) \), the algebraic degree of freedom of \( c \), denoted by \( f_{\omega,c}^r \), is the largest nonnegative integer \( f \leq \Delta^*_{p,r} \) satisfying the following two conditions:
\[
\begin{align*}
(i) & \quad \text{The field } M_c(f + L(c) - r) \text{ is a subfield of a bicyclic extension}, \\
(ii) & \quad K_0(f) \subseteq M_c(f + L(c) - r).
\end{align*}
\]
According to the definition one has \( r \leq f_{\omega,c}^r \leq f_{\omega,U}^r \leq \Delta^*_{p,r} \).

\(^{1}\)Do not confuse this with the notation \( K_i(p) \) in Section 2.1.
**Definition 2.12.** Let \( c \subset U_r \) be an \( h \)-equivalence class for some \( h \geq L(U_r) \). The degree of freedom \( f_c \) of \( c \) is defined to be the largest nonnegative integer \( f \leq f_c^\omega \) such that \( M_c(f + L(c) - r) \) is locally cyclic.

**Theorem 2.13.** [4, Theorem 6.5] Let \( T_{L/k} \) be the multinorm one torus associated to a \( k \)-étale algebra \( L = \prod_{i=0}^n K_i \). We have

\[
\begin{align*}
\Pi_i^2(k, \hat{T}_{L/k}) &\cong \bigoplus_{r \in R \setminus \{0\}} \mathbb{Z}/p^\Delta_{i} \mathbb{Z} \bigoplus_{c \in \text{Adm}} (\mathbb{Z}/p^\Delta_{c} \mathbb{Z})^\nu_{L(c)+1}(c)^{-1}, \\
\Pi_i^2(k, \hat{T}_{L/k}) &\cong \bigoplus_{r \in R \setminus \{0\}} \mathbb{Z}/p^\Delta_{i} \mathbb{Z} \bigoplus_{c \in \text{Adm}} (\mathbb{Z}/p^\Delta_{c} \mathbb{Z})^\nu_{L(c)+1}(c)^{-1},
\end{align*}
\]

where \( R = \{0 \leq r \leq \epsilon_0 \mid U_r \neq \emptyset\} \).

2.3. We use Theorem 2.13 to revisit the criterion for the vanishing of the groups \( \Pi_i^2(k, \hat{T}_{L/k}) \) and \( \Pi_i^2(k, \hat{T}_{L/k}) \) [4, Theorem 8.1].

**Definition 2.14.** A subset \( c \subset I \) with \( |c| > 1 \) is said to be admissible if \( c \) is an \( l \)-equivalence class in \( U_r \) for some \( r \geq 0 \). The integer \( r \), denoted \( \text{supp}(c) \), is called the support of \( c \). Let \( \text{Adm} \) be the set of admissible subsets of \( I \).

Theorem 2.13 can be reformulated as follows.

**Theorem 2.15.** We have

\[
\begin{align*}
\Pi_i^2(k, \hat{T}_{L/k}) &\cong \bigoplus_{r \in R \setminus \{0\}} \mathbb{Z}/p^\Delta_{i} \mathbb{Z} \bigoplus_{c \in \text{Adm}} (\mathbb{Z}/p^\Delta_{c} \mathbb{Z})^\nu_{L(c)+1}(c)^{-1}, \\
\Pi_i^2(k, \hat{T}_{L/k}) &\cong \bigoplus_{r \in R \setminus \{0\}} \mathbb{Z}/p^\Delta_{i} \mathbb{Z} \bigoplus_{c \in \text{Adm}} (\mathbb{Z}/p^\Delta_{c} \mathbb{Z})^\nu_{L(c)+1}(c)^{-1},
\end{align*}
\]

**Proposition 2.16.** Let \( r_0 > 0 \) be the smallest integer such that \( U_r \) is nonempty.

1. We have \( \Pi_i^2(k, \hat{T}_{L/k}) = 0 \) if and only if \( \Delta_{i}^{\omega} = r_0 \) and \( f_{U_0}^c = 0 \).

2. We have \( \Pi_i^2(k, \hat{T}_{L/k}) = 0 \) if and only if \( \Delta_{c}^{\omega} = r_0 \) and \( f_{U_0}^c = 0 \).

**Proof.** By Theorem 2.15, \( \Pi_i^2(k, \hat{T}_{L/k}) = 0 \) if and only if \( \Delta_{i}^{\omega} = r \) for all \( r \in R \setminus \{0\} \) and \( f_{c}^\omega = r \) for all admissible subsets \( c \) of support \( r \). Since \( r \leq f_{c}^\omega \leq \Delta_{i}^{\omega} \), the first condition \( \Delta_{i}^{\omega} = r \) implies that \( f_{c}^\omega = r \) for all admissible subsets \( c \) of support \( r \geq 1 \). Also one has \( 0 \leq f_{a}^\omega \leq \Delta_{i}^{\omega} \) if \( c \subset U_0 \), so that the above condition is equivalent to that \( \Delta_{i}^{\omega} = r \) for all \( r \in R \setminus \{0\} \) and \( f_{U_0}^c = 0 \). By [4, Proposition 4.3], we have \( \Delta_{i}^{\omega} - r_0 \geq \Delta_{i}^{\omega} - r \). This proves the first statement.

We now show \( r \leq f_{c} \leq f_{U_0}^c \leq \Delta_{i} \). By [4, Proposition 5.8], if \( r \leq f \leq f_{U_0}^c \) and \( i \in c \), then

\[
M_c(f + L(c) - r) = K_0(f)K_i(f + L(c) - r).
\]

Since \( f \leq f_{U_0}^c \), one also has

\[
M_{U_r}(f + L(U_r) - r) = K_0(f)K_i(f + L(U_r) - r).
\]

Therefore, \( M_{U_r}(f + L(U_r) - r) \subset M_c(f + L(c) - r) \). Hence if \( M_c(f + L(c) - r) \) is locally cyclic then \( M_{U_r}(f + L(U_r) - r) \) is locally cyclic. It follows that \( f_{c} \leq f_{U_0}^c \).

For \( r \leq f \leq f_{U_0}^c \leq \Delta_{i}^{\omega} \) and \( i \in U_r \), one has

\[
K_0(f)K_i(f) \subset K_0(f)K_i(f + L(U_r) - r) = M_{U_r}(f + L(U_r) - r)
\]

and hence \( K_0(f)K_{U_r}(f) \subset M_{U_r}(f + L(U_r) - r) \). Since \( f \leq \Delta_{i}^{\omega} \), one also has

\[
K_0(f)K_{U_r}(f) \subset \bigcap_{i \in U_r} K_0(f)K_i(f) \subset K_0(f)K_i(f) \subset M_{U_r}(f + L(U_r) - r).
\]
Therefore, if $M_{U_i}(f + L(U_i) - r)$ is locally cyclic, then both $K_0(f)K_{U_{\geq r_i}}(f)$ and $K_0(f)K_{U_i}(f)$ are locally cyclic. It follows that $f_{U_i} \leq \Delta_r$. This shows $r \leq f_{U_i} \leq \Delta_r$.

The second statement then follows from the same argument and [3, Proposition 4.10].

We can look further the conditions for nonvanishing of the groups $\Omega^2_L(k, \hat{T}_L/k)$ and $\Delta^2(k, \hat{T}_L/k)$. Note that if $U_{\geq r} \neq \emptyset$, then $M_{U_{\geq r}}(r + 1) = K_0(r + 1)$ and hence the condition

$$M_{U_{\geq r}}(r + 1) \subset \bigcap_{\sigma \in \mathcal{G}_{r_0}} K_0(r + 1)K_i(r + 1)$$

always holds. Thus, we have

$$\Delta^\omega_{r_0} \geq r_0 + 1 \iff M_{U_{\geq r_0}}(r_0 + 1) \subset \bigcap_{\sigma \in \mathcal{G}_{r_0}} K_0(r_0 + 1)K_i(r_0 + 1).$$

By definition, we have $\Delta^\omega_{r_0} \geq r_0 + 1$ if and only if the following three conditions hold

(i) $\Delta^\omega_{r_0} \geq r_0 + 1$;

(ii) $K_0(r_0 + 1)M_{U_{\geq r_0}}(r_0 + 1)$ is locally cyclic;

(iii) If $U_{r_0}$ is nonempty, then $K_0(r_0 + 1)M_{U_{\geq r_0}}(r_0 + 1)$ is locally cyclic.

Similarly, we have

$$f_{U_0}^c \geq 1 \iff M_{U_0}(1 + L(U_0)) \text{ is a subfield of a bicyclic extension of } k$$

and it contains $K_0(1)$,

and

$$f_{U_0} \geq 1 \iff f_{U_0} \geq 1 \text{ and } M_{U_0}(1 + L(U_0)) \text{ is locally cyclic.}$$

In the special case where $K_i$ are distinct cyclic extensions of degree $p$ over $k$, one obtains from (2.6) that $\Omega^2(L) \neq 0$ if and only if (i) $K_0 \subset M_{U_0}(1)$, (ii) $M_{U_0}(1)$ is a subfield of a bicyclic extension, and (iii) $M_{U_0}(1)$ is locally cyclic. This is the same as Proposition 2.5 in this special case.

3. Remarks on the conditions for Theorem 2.13

3.1. Note that the assumption $e_1 \geq e_2 \geq \cdots \geq e_m$ is unnecessary. We can choose some permutation $\sigma \in S_m$ such that $e_{\sigma(i)} \geq e_{\sigma(i + 1)}$. The invariants $e_{i,j}$ are identical up to $\sigma$. From the definition of $\ell$-equivalence, $U_r$, $\epsilon_r$ (algebraic) patching degrees $\Delta^\omega_r$, (algebraic) degrees of freedom $f_r^c$, etc., we see that they are identical after the action of $\sigma$. Therefore the Tate-Shafarevich groups $\Omega^2(L)$ and $\Delta^2(L)$ given by the formula without the assumption are the same as those given by the formula with the assumption. Thus, for implementing an algorithm, we do not need to rearrange our input data so that this assumption holds.

3.2. In this subsection, we discuss whether we have the same results without the condition $\cap_{i=0}^m K_i = K$. That is, setting $F = \cap_{i=0}^m K_i$ and considering $L/F$ as an étale $F$-algebra, we compare the groups $\Omega^2(k, \hat{T}_L/k)$ and $\Omega^2(F, \hat{T}_L/F)$.

First we denote

$$T^L_F = R_{L/F}\mathbb{G}_{m,L}, \quad T_L^L := R_{L/k}\mathbb{G}_{m,L} = R_{F/k}T^L_F, \quad T^F = R_{F/k}\mathbb{G}_{m,F},$$

and let $T_{L/F} = \text{Ker}\; N_{L/F}$ and $T_{L/k} = \text{Ker}\; N_{L/k}$, where $N_{L/F} = \prod_{i=0}^m N_{K_i/F}$ and $N_{L/k} = \prod_{i=0}^m N_{K_i/k}$ are the norm maps. Let $\hat{k} = K_0K_1\cdots K_m$ be the composition of $K_i$, and set

$G = \text{Gal}(\hat{k}/k), \quad H_i = \text{Gal}(\hat{k}/K_i), \quad \text{and } H = \text{Gal}(\hat{k}/F)$.

Lemma 3.1. (1) We have $H^1(F, \hat{T}_{L/F}) = H^1(H, \hat{T}_{L/F}) = 0$. 
Lemma 3.2. Let $T$ be an algebraic torus over $k$ and $K/k$ a Galois splitting field for $T$ with Galois group $G$.

1. There is a natural isomorphism $\mathfrak{III}^2(G, \hat{T}) \cong \mathfrak{III}^2(k, \hat{T})$.

2. There is a natural isomorphism $\mathfrak{III}^2_G(G, \hat{T}) \cong \mathfrak{III}^2_G(k, \hat{T})$.

Proof. These are well-known results. The statement (1) follows from the fact that the group $\mathfrak{III}^1(G, T)$ is independent of the choice of the splitting field $K$; see [6] Sections 3.3 and 3.4] and the Poitou-Tate duality ([7] Theorem 6.10] and [5] Theorem 8.6.8}). We give a proof of (2) for the reader’s convenience. Let $K'$ be another Galois splitting field for $T$ containing $K$ with Galois groups $G' = \text{Gal}(K'/k)$ and $H = \text{Gal}(K'/K)$. Since $\hat{T}$ is a trivial $H$-module, $H^1(H, \hat{T}) = \text{Hom}(H, \hat{T}) = 0$. By Hochschild-Serre’s spectral sequence, we have the exact sequence

$$0 \longrightarrow H^2(G, \hat{T}) \longrightarrow H^2(G', \hat{T}) \longrightarrow H^2(H, \hat{T}).$$

Thus, to show $\mathfrak{III}^2_G(G, \hat{T}) \cong \mathfrak{III}^2_G(G', \hat{T})$, it suffices to show $\mathfrak{III}^2_G(H, \hat{T}) = 0$. Since $\hat{T}$ is a trivial $H$-module, it is the same to show $\mathfrak{III}^2_G(H, \hat{T}) = 0$. As $H^2(H, \hat{T}) \simeq H^1(H, \hat{T})$, this follows from that

$$\text{Ker} \left( \text{Hom}(H, \hat{T}) \longrightarrow \prod_C \text{Hom}(C, \hat{T}) \right) = 0,$$

where $C$ runs through all cyclic subgroups of $H$. \hfill $\blacksquare$
Proposition 3.3. There is a natural injective map \( \tilde{\tau} : \mathbb{III}^2_\omega(k, \widehat{T}_{L/k}) \mapsto \mathbb{III}^2_\omega(F, \widehat{T}_{L/F}) \).

Proof. From the commutative diagram

\[
\begin{array}{cccccc}
1 & \rightarrow & R_{F/k}(T_{L/k}) & \rightarrow & T_L & \stackrel{N_{L/F}}{\rightarrow} & T^F & \rightarrow & 1 \\
\downarrow & & \downarrow & & \downarrow & & \downarrow \\
1 & \rightarrow & T_{L/k} & \rightarrow & T_L & \stackrel{N_{L/k}}{\rightarrow} & \mathbb{G}_{m,k} & \rightarrow & 1
\end{array}
\]

where the two rows are exact, we obtain the following commutative diagram

\[
\begin{array}{cccccc}
1 & \rightarrow & R_{F/k}T_{L/F} & \rightarrow & T_{L/k} & \stackrel{\iota}{\rightarrow} & T_L & \stackrel{N_{L/F}}{\rightarrow} & T^F & \rightarrow & 1 \\
\downarrow & & \downarrow & & \downarrow & & \downarrow & & \downarrow \\
1 & \rightarrow & R_{F/k}T_{L/F} & \rightarrow & T_{L/k} & \stackrel{\iota}{\rightarrow} & T_L & \stackrel{N_{L/F}}{\rightarrow} & T^F & \rightarrow & 1 \\
\end{array}
\]

whose rows and columns are exact. Taking the dual of the first row yields an exact sequence

(3.2)

\[
0 \rightarrow \widehat{T}_{F/k} \rightarrow \widehat{\mathbb{G}}_{L/F} \rightarrow \widetilde{T}_{L/F} \rightarrow \text{Ind}^G_H \widehat{T}_{L/F} \rightarrow 0.
\]

This gives the following commutative diagram

(3.3)

\[
\begin{array}{cccccc}
H^1(H, \widehat{T}_{L/F}) & \rightarrow & H^2(G, \widehat{T}_{F/k}) & \stackrel{\mathbb{S}_{L/F}}{\rightarrow} & H^2(G, \widehat{T}_{L/k}) & \rightarrow & H^2(H, \widehat{T}_{L/F}) \\
\downarrow & & \downarrow & & \downarrow & & \downarrow \\
\prod_{w \mid v} H^1(H_w, \widehat{T}_{L/F}) & \rightarrow & H^2(G_v, \widehat{T}_{F/k}) & \stackrel{\mathbb{S}_{L/F,v}}{\rightarrow} & H^2(G_v, \widehat{T}_{L/k}) & \rightarrow & \prod_{w \mid v} H^2(H_w, \widehat{T}_{L/F}) \\
\end{array}
\]

for every decomposition group \( G_v \) of \( G \), where \( w \) runs through places of \( F \) above \( v \). By Lemma 3.1 we have \( H^1(H, \widehat{T}_{L/F}) = 0 \) and \( H^1(H_w, \widehat{T}_{L/F}) = 0 \), so the maps \( \tilde{\mathbb{N}}_{L/F} \) and \( \tilde{\mathbb{N}}_{L/F,v} \) are injective.

Suppose an element \( x \in H^2(G, \widehat{T}_{L/k}) \) lies in \( \text{Ker} \tilde{\tau} \) satisfying \( r_{L/k}(x) = 0 \). Let \( y \in H^2(G, \widehat{T}_{F/k}) \) be the unique element with \( \tilde{\mathbb{N}}_{L/F}(y) = x \). Then \( r_{F/k}(y) = 0 \) as the map \( \tilde{\mathbb{N}}_{L/F,v} \) is injective. It follows that \( \mathbb{III}^2_\omega(G, \widehat{T}_{L/k}) \cap \text{Ker} \tilde{\tau} \simeq \mathbb{III}^2_\omega(G, \widehat{T}_{F/k}) \), which is zero from [3] Proposition 2.2 if \( F/k \) is cyclic. Thus, the map

\[
\tilde{\tau} : \mathbb{III}^2_\omega(k, \widehat{T}_{L/k}) \rightarrow \mathbb{III}^2_\omega(G, \widehat{T}_{L/k}) \rightarrow \mathbb{III}^2_\omega(H, \widehat{T}_{L/F}) = \mathbb{III}^2_\omega(F, \widehat{T}_{L/F})
\]

is injective. \( \blacksquare \)

Corollary 3.4. Notation being as above, if \( \mathbb{III}^2_\omega(F, \widehat{T}_{L/F}) = 0 \), then \( \mathbb{III}^2_\omega(F, \widehat{T}_{L/k}) = 0 \).

4. Multinorm one tori of Kummer type

4.1. Kummer extensions. For a moment, let \( k \) be a field which contains a primitive \( N \)-th root of unity, where \( N \geq 2 \) is a positive integer prime to the characteristic of \( k \). Recall that a Kummer extension \( L/k \) of exponent \( N \) is a finite abelian field extension, whose Galois group \( \text{Gal}(L/k) \) is of exponent \( N \), that is, \( \sigma^N = 1 \) for any \( \sigma \in \text{Gal}(L/k) \). For example, if \( \text{char} \ k \neq 2 \) then a quadratic extension \( L = k(\sqrt{a}) \), where \( a \in k \) is not a square, is a Kummer extension. Biquadratic
extensions and multiquadratic extensions are also Kummer extensions. More generally, for any
nonzero element $a \in k$, $k(a^{1/N})$ is a Kummer extension whose degree $m$ divides $N$.

Kummer theory establishes the following one-to-one correspondence
\[(4.1) \quad \{ \text{Kummer extensions over } k \text{ of exponent } N \} \leftrightarrow \{ \text{finite subgroups of } k^{\times}/(k^{\times})^N \}.
\]
For any finite subgroup $W$ of $k^{\times}/(k^{\times})^N$, we define
\[K_W := k \left( w^{1/N} : w \in W \right)\]
and associate $K_W$ to $W$. Conversely, let $W$ be a Kummer extension of $k$. Since $L$ is of exponent
$N$, $L$ can be written as a composition of cyclic extensions $k(a_1^{1/N}) \cdots k(a_m^{1/N})$, where $a_i \in k^{\times}$.

We associate it to the subgroup
\[W_L = \langle \overline{a_i} : i = 1, \ldots, m \rangle\]
where $\overline{a_i}$ denotes the image of $a_i$ in $k^{\times}$.

Let $\mu_N$ be the group of $N$-th roots of unity in $k$. There is a perfect pairing
\[\text{Gal}(K_W/k) \times W \to \mu_N \quad (\sigma, w) \mapsto \sigma(w^{1/p^n}).\]
This gives a natural identification $\text{Gal}(K_W/k) = \text{Hom}(W, \mu_N)$. If $W_1 \subset W_2$ are two subgroups
of $k^{\times}/(k^{\times})^{p^n}$, the natural projection $\text{Gal}(K_{W_2}/k) \to \text{Gal}(K_{W_1}/k)$ is the restriction to $W_1$:
\[\text{Hom}(W_2, \mu_N) \to \text{Hom}(W_1, \mu_N).\]

Inclusion, composition, and intersection of groups $W_i$ correspond to those of Kummer extensions.

**Proposition 4.1.** Let $W$ and $W_i$ ($i = 1, 2$) be subgroups of $k^{\times}/(k^{\times})^N$ and $K_W$ and $K_{W_i}$ be the
corresponding Kummer extensions. Then
\begin{enumerate}
\item $K_{W_1} \subset K_{W_2}$ if and only if $W_1 \subset W_2$.
\item $W = W_1W_2$ if and only if $K_W = K_{W_1}K_{W_2}$.
\item $W = W_1 \cap W_2$ if and only if $K_W \cap K_{W_1} = K_{W_2}$.
\end{enumerate}

**4.2. Group theoretic description for $\text{III}_2^2(k, \hat{T}_{L/k})$ and $\text{III}_2^2(k, \hat{T}_{L/k})$.** For the rest of this
section, let $k$ be a global field in which $p^{-1} \in k$ and $L = \prod_{i=0}^m K_i$ an étale $k$-algebra as in Section
2.2. Let $N = p^n$ be a power of $p$ such that $[K_1 : k]$ divides $N$ for all $i$. Suppose that $k$ contains a
primitive $N$-th root of unity. We further assume that each $K_i$ can be written as $k(a_i)$, where
$a_i = a_i^{1/p^n}$ for some $a_i \in \mathbb{Q}^{\times}$. We may assume $a_i \in \mathbb{Z}$: if $a_i = \frac{a}{b}$, we can set $a'_i = a_ib^{p^n}$ so that
$k(a_i^{1/p^n}) = k(a_i^{1/p^n})$.

The correspondence [4.1] enables us to describe $\text{III}_2^2(k, \hat{T}_{L/k})$ and $\text{III}_2^2(k, \hat{T}_{L/k})$ in terms of
information in the group $k^{\times}/(k^{\times})^{p^n}$. First, we set $W_i = \langle \overline{a_i} \rangle$ to be the subgroup corresponding to $K_i$.
For any nonempty subset $I$ of $\mathcal{I} = \{1, \ldots, m\}$, we let $W_I = \langle \overline{a_i} \rangle : i \in I \rangle$ be the group corresponding to $M_I$.
We define $W_i(d), W_I(d)$ as groups corresponding to $K_i(d)$ and $M_I(d)$, respectively. Note that the order of $\overline{a_i}$ in $k^{\times}/(k^{\times})^{p^n}$ is $p^n$, so $K_i(d) = k(a_i^{p^{n-d}/p^n})$ and $W_i(d) = \langle a_i^{p^n-d/p^n} \rangle$.

We translate the first definitions in Section 2 as follows.
\begin{enumerate}
\item For $i, j \in I$, $i$ and $j$ are $\ell$-equivalent if and only if $W_i(\ell) = W_j(\ell)$.
\item The set $U_0 = \{ i \in I \mid W_0(r) = W_0 \cap W_i = W_i(r) \}$.
\item For any subset $c \subset I$, $L(c) = \min \{ \ell \mid W_i(\ell) = W_i \cap W_j = W_j(\ell) \text{ for any } i, j \in c \}$.
\end{enumerate}
With the above language, we can rewrite the definitions of algebraic patching degrees and algebraic degrees of freedom. If \( U_0 = \mathcal{I} \), then we set the algebraic patching degree \( \Delta^\omega \) for nonempty \( U_r \) is the maximal positive integer \( d \) satisfying two conditions:

(i) If \( U_{>r} \) is nonempty, then \( W_{U_{>r}}(d) \subset \bigcap_{i \in U_{>r}} W_0(d) W_i(d) \).

(ii) If \( U_{<r} \) is nonempty, then \( W_{U_{<r}}(d) \subset \bigcap_{i \in U_{<r}} W_0(d) W_i(d) \).

Now the algebraic degree of freedom \( f^c_r \) for an admissible set \( c \subset U_r \) can be defined as the largest nonnegative integer \( f \leq \Delta^c_r \) satisfying two conditions:

(i) \( W_c(f + L(c) - r) \) is a cyclic group or a bicyclic group.

(ii) \( W_0(f) \subset W_c(f + L(c) - r) \).

Before we rewrite the definition of patching degrees and degrees of freedom, recall that we have to check whether a field is locally cyclic in the definition of patching degrees \( \Delta_r \). We need to describe whether a Kummer extension is locally cyclic in terms of groups, too. Let \( K/k \) be a Kummer extension and \( v \) a place of \( k \). Let \( w \) be a place of \( K \) lying over \( v \). The decomposition group \( G_v = \Gal(K_w/k_w) \) corresponds to a subgroup \( W_v \) of \( k_v^\times/(k_v^\times)^p \) through the duality between \( \Gal(K/k) \) and \( W \).

\[
\begin{align*}
\Gal(K_w/k_w) &= G_v 
\hookrightarrow W_v \subset k_v^\times/(k_v^\times)^p^n \\
\Gal(K/k) &\hookrightarrow W \subset k^\times/(k^\times)^p^n 
\end{align*}
\]

The map \( \pi_v : W \to W_v \) is induced by the map \( k^\times \to k_v^\times \) whose image is dense in \( k_v^\times \). \( W_v \) is a finite set and hence \( \pi_v \) is surjective. Recall that \( K/k \) is locally cyclic at \( v \) means that \( K_w/k_w \) is cyclic for any \( w \mid v \), and this is equivalent to saying that \( \pi_v(W_v) \) is cyclic for any \( v \).

Now we can redefine the patching degree \( \Delta_v \) to be the maximal positive integer \( d \leq \Delta^\omega_r \) satisfying two conditions:

(i) If \( U_{>r} \) is nonempty then \( \pi_v(W_0(d) W_{U_{>r}}(d)) \) is cyclic for all places \( v \) in \( k \).

(ii) If \( U_{<r} \) is nonempty then \( \pi_v(W_0(d) W_{U_{<r}}(d)) \) is cyclic for all places \( v \) in \( k \).

On the other hand, for an admissible set \( c \subset U_r \) the degree of freedom \( f_c \) is the largest nonnegative integer \( f \leq f^c_r \) such that \( \pi_v(W_c(f + L(c) - r)) \) is a cyclic group for any place \( v \) of \( K \).

### 4.3. Cyclotomic cases: combinatorial description for \( \Pi_2^c(k, \hat{T}_L/k) \) and \( \Pi_2(k, \hat{T}_L/k) \).

In this subsection we define

\[ W = \{ \pi : a \in \mathbb{Q}^\times \} \subset k^\times/(k^\times)^p^n, \]

that is, the image of \( \iota : \mathbb{Q}^\times/(\mathbb{Q}^\times)^p^n \to k^\times/(k^\times)^p^n \). Because each component \( K_i \) of \( L \) is of the form \( k(a_i^1/p^n) \) where \( a_i \) is an integer, the group \( W_i \) corresponding to \( K_i \) is contained in \( W \). We shall investigate the structure of \( W \). Let \( \mathbb{P} \) denote the set of prime numbers in \( \mathbb{Q} \).

**Proposition 4.2.**

1. If \( p \) is odd, then \( W \simeq \mathbb{Q}_{>0}/(\mathbb{Q}_{>0})^{p^n} \simeq \bigoplus_{\ell \in \mathbb{P}} \mathbb{Z}/p^n \mathbb{Z} \).

2. Suppose \( p = 2 \) and we denote \( \mathbb{P} \) the set of prime integers.
   - (a) If \( N = 2 \), then \( W \simeq \bigoplus_{\ell \in \mathbb{P} \cup \{-1\}} \mathbb{Z}/2 \mathbb{Z} \).
   - (b) If \( N = 4 \), then \( W \simeq \mathbb{Z}/2 \mathbb{Z} \times \bigoplus_{\ell \in \mathbb{P}} \mathbb{Z}/4 \mathbb{Z} \).
   - (c) If \( N \geq 8 \), then \( W \simeq \mathbb{Z}/2 \mathbb{Z} \times \mathbb{Z}/2^{n-1} \mathbb{Z} \times \bigoplus_{\ell \in \mathbb{P} \setminus \{2\}} \mathbb{Z}/2^n \mathbb{Z} \).

**Proof.**
(1) Suppose \( a \) is an integer such that \( a = \alpha p^n \) for some \( \alpha \in k^\times \). Let \( \ell \) be a prime integer not equal to \( p \), then \( \ell \) is unramified in \( k \) and hence the valuation \( v_\ell \) sends each element of \( k^\times \) to an integer. Therefore, \( v_\ell(a) = p^n v_\ell(\alpha) \in p^n\mathbb{Z} \), i.e., \( p^n \mid n_\ell \) for all \( i \). We may then assume that \( a = \pm p^r \) for some \( r \in \mathbb{Z}_{\geq 0} \). Because \( \iota(-1) = 1 \), we may further assume \( a = p^r \). If \( r > 0 \), without loss of generality, we can write \( p^r = \alpha p^{n_\ell} \), i.e., \( p = \alpha p^{n_\ell - 1} \) where \( \alpha \in k = \mathbb{Q}(\zeta_p^n) \). This shows that \( \sqrt[p^n-1]{p} \in \mathbb{Q}(\zeta_p^n) \). On the other hand, we consider the Galois group of \( k(p^{1/r}) = \mathbb{Q}(\zeta_p^n, p^{1/r}) \). In this group we have automorphisms

\[
\tau_a : \zeta_p^n \mapsto \zeta_p^n, \quad \sqrt[p^n-1]{a} \mapsto \sqrt[p^n-1]{a}.
\]

for \( a \in (Z/p^nZ)^\times \). Also we have

\[
\sigma : \zeta_p^n \mapsto \zeta_p^n, \quad \sqrt[p^n-1]{\alpha} \mapsto \sqrt[p^n-1]{\alpha}.
\]

But \( \tau_a \sigma \tau_a^{-1} \neq \sigma \), so the Galois group is not abelian. This contradicts the above conclusion \( \mathbb{Q}(\sqrt[p^n-1]{p}, \zeta_p^n) = \mathbb{Q}(\zeta_p^n) \). Therefore, the integer \( a \) must be 1, and hence we conclude that \( \ker(\iota) = \{ 1 \} \).

(2) When \( N = p = 2 \), \( k \) is simply \( \mathbb{Q} \) and thus

\[
W = \mathbb{Q}^2/(\mathbb{Q}^2)^2 \simeq \bigoplus_{\ell \in \mathbb{F}_2 \cup \{-1\}} \mathbb{Z}/2\mathbb{Z}.
\]

Now suppose \( N = 2^n \geq 4 \). Observe that \( \sqrt{2} \in \mathbb{Q}(\zeta_8) \) and \( -1 \in (k^\times)^2 \). If \( \ell \) is a prime integer other than 2, then the argument in part (1) applies, so \( \ker(\iota) = \ker(\iota|_{\mathbb{Q}(\zeta_2)}) \). It suffices to study the restriction of \( \iota \) to \( (\mathbb{Q}(\zeta_2), -1) \). First, the restriction of \( \iota \) to \( (\mathbb{Q}(\zeta_2), -1) \) is injective: if \( -1 = \alpha^{2^n} \) for some \( \alpha \in k \), then \( k \) must contain primitive \( 2n+1 \)-roots of unity, which is absurd. Next, we turn to the restriction of \( \iota \) to \( (\mathbb{Q}(\zeta_2), 2) \). Note that \( \sqrt{2} \in \mathbb{Q}(\zeta_8) \), while \( \sqrt{2} \) is not contained in \( \mathbb{Q}(\zeta_N) \) since \( \mathbb{Q}(\sqrt{2})/\mathbb{Q} \) is not an abelian extension. From this, we deduce that if \( N = 4 \), then the restriction of \( \iota \) to \( (\mathbb{Q}(\zeta_2), 2) \) is injective. We also deduce that if \( N \geq 8 \), then the kernel of the restriction is \( (\mathbb{Z}/2^{2n-1})^\times \). In conclusion, if \( N = 4 \), then \( \ker \iota \) is trivial and

\[
W \simeq \mathbb{Z}/2\mathbb{Z} \times \bigoplus_{\ell \in \mathbb{F}_2} \mathbb{Z}/4\mathbb{Z};
\]

if \( N = 2^n \geq 8 \), then \( \ker \iota = \ker(\iota|_{\mathbb{Q}(\zeta_2)}) \) and

\[
W \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2^{n-1}\mathbb{Z} \times \bigoplus_{\ell \in \mathbb{F}_2 \setminus \{2\}} \mathbb{Z}/2^{n}\mathbb{Z}.
\]

The structure of \( W \) determined, we may describe the corresponding groups \( W_i \) of the cyclic fields \( K_i \) in combinatorial terms. Note that each \( W_i \) is a finite cyclic subgroup of \( W \) for \( 0 \leq i \leq m \), so we can use only finitely many generators to describe the groups \( W_i \). For example, suppose \( N = 2^n \geq 8 \) and \( K = k(a^{1/N}) \) for some integer \( a \neq 0 \). If

\[
a = (-1)^{n-1} \cdot 2^{2^t} \cdot \prod_{\ell \in \mathbb{F}_2 \setminus \{2\}} \ell^{n_t}
\]

for a finite subset \( \mathbb{F}_2 \subset \mathbb{F}_2 \), then the corresponding finite subgroup is the cyclic subgroup of \( W \) generated by \( (\pi_{-1}, \pi_2, (\pi_t)_{\ell \in \mathbb{F}_2 \setminus \{2\}}) \).

Using Proposition 3.1, one can compute effectively algebraic patching degrees \( \Delta_e \) and algebraic degrees of freedom \( f_e \). However, to compute patching degrees \( \Delta_e \) and \( f_e \), we will need to analyze further the image of a subgroup \( W \) in \( k^e/(k^e)^{p\mathbb{Z}} \). We shall do this when each \( K_i \) is in a fixed concrete bicyclic extension in the next section.
5. Computing decomposition groups: the case of subfields contained in a bicyclic extension

In the following sections, we shall further restrict to a special case. Fix a prime integer \( p \) and a positive integer \( n \). Let \( k := \mathbb{Q}(\zeta) \) be the \( p^n \)-th cyclotomic field, where \( \zeta \) is a primitive \( p^n \)-th root of unity in \( \mathbb{Q} \), the algebraic closure of \( \mathbb{Q} \) in \( \mathbb{C} \). We fix an algebraic closure \( \overline{\mathbb{Q}}_\ell \) of \( \mathbb{Q}_\ell \) and an embedding \( \overline{\mathbb{Q}} \hookrightarrow \overline{\mathbb{Q}}_\ell \).

Let \( \ell_1 \) and \( \ell_2 \) be two distinct prime integers with \( \ell_1 \neq p \), and let \( F := k(\alpha_1, \alpha_2) \), where \( \alpha_1 = \ell_1^{s_1}/p^n \) and \( \alpha_2 = \ell_2^{s_2}/p^n \). Let \( m \geq 1 \) be a positive integer. We assume that each component \( K_j \) of the étale \( k \)-algebra \( L = \prod_{i=0}^{\ell-2} K_i \) is of the form \( K_i = k(\alpha_1^{a_i} \alpha_2^{b_i}) \), that is, a cyclic subextension of \( F/k \), where \( a_i \) and \( b_i \) are integers satisfying \( 0 \leq a_i, b_i < p^n \). The Galois group \( G = \text{Gal}(F/k) \) is cyclic of order \( p^m \), generated by two elements \( \tau_1, \tau_2 \),

\[
\tau_1(\alpha_1) = \alpha_1 \zeta, \quad \tau_2(\alpha_1) = \alpha_1, \quad \tau_2(\alpha_2) = \alpha_2 \zeta.
\]

Therefore, any subfield of the form \( M_\ell(d) \), which appears in the definition of algebraic degrees of freedom, is automatically a subfield of the bicyclic extension \( F \).

5.1. Decomposition groups and local cyclicity. Set \( F_i = k(\alpha_i) \) for \( i = 1, 2 \). Write \( G_i = \text{Gal}(F_i/k) \) and we have a natural isomorphism

\[
G \cong G_1 \times G_2, \quad \sigma \mapsto (\sigma|_{F_1}, \sigma|_{F_2}).
\]

For any prime \( \ell \), write \( w, w_1, w_2, \) and \( v \) for the places of \( F, F_1, F_2 \) and \( k \), respectively, lying over \( \ell \) with respect to the embedding \( \overline{\mathbb{Q}} \hookrightarrow \overline{\mathbb{Q}}_\ell \). If \( \ell \nmid \ell_1 \ell_2 \), then \( \ell \) is unramified in both \( F_1 \) and \( F_2 \) and hence \( \ell \) is unramified in \( F \). Let \( G_v, G_{1,v} \) and \( G_{2,v} \) be the decomposition groups of \( v \) in \( G, G_1 \) and \( G_2 \), respectively.

For any integers \( m_1 \neq 0 \) and \( r \), denote by \([r]_{m_1}\) the residue class of \( r \) in \( \mathbb{Z}/m_1 \mathbb{Z} \). If \( m_1 \) and \( r \) are coprime, let \( \text{ord}([r]_{m_1}) \) denote the order of \([r]_{m_1}\) in \((\mathbb{Z}/m_1 \mathbb{Z})^\times\). In the following lemma we investigate the ramification after we add a \( p^n \)-th root of an integer to \( \mathbb{Q}_\ell(\zeta) \).

Lemma 5.1. Let \( \ell \neq p \) be a prime number.

1. For any positive integer \( s \), the field extension \( \mathbb{Q}_\ell(\zeta, \ell^s/p^n)/\mathbb{Q}_\ell(\zeta) \) is totally ramified of degree \( p^{\text{ord}_p(s)} \), where \( \text{ord}_p \) is the normalized valuation at \( p \).

2. For any positive integer \( r \) not divisible by \( \ell \), the field extension \( \mathbb{Q}_\ell(\zeta, r^{1/p^n})/\mathbb{Q}_\ell(\zeta) \) is unramified of degree

\[
(5.1) \quad p^{\max\{\min\{n,s_1\}, (s_1 - s_2)\}, 0}
\]

where \( s_1 = v_p(\ell - 1) \) and \( s_2 = v_p(\text{ord}([r]_{\ell})) \).

Proof. (1) We first consider the case where \( s = 1 \). As \( \mathbb{Q}_\ell(\zeta, \ell^{1/p^n}) \) is the splitting field of the polynomial \( f(X) = X^{p^n} - \ell \) over \( \mathbb{Q}_\ell(\zeta) \), it suffices to show that \( f(X) \) is irreducible. Since \( \ell \) is unramified in \( \mathbb{Q}_\ell(\zeta) \), the element \( \ell \) is a uniformizer of the complete discrete valuation ring \( \mathbb{Z}[\zeta] \).

By Eisenstein’s criterion, \( f(X) \) is irreducible in \( \mathbb{Z}[\zeta][X] \). Therefore, \( \mathbb{Q}_\ell(\zeta, \ell^{1/p^n})/\mathbb{Q}_\ell(\zeta) \) is totally ramified of degree \( p^n \).

For general \( s \), write \( s = p^{v_p(s)} s' \). Then \( \mathbb{Q}_\ell(\zeta, \ell^{s/p^n}) = \mathbb{Q}_\ell(\zeta, \ell^{s'}/p^{n'}) \) with \( n' = n - v_p(s) \). Since \( s' \) is prime to \( p \), \( \mathbb{Q}_\ell(\zeta, \ell^{s'}/p^{n'}) \) is a totally ramified extension of has degree \( p^n \) over \( \mathbb{Q}_\ell(\zeta) \) of degree \( p^{n-v_p(s)} \).

(2) Since \( \ell \nmid r \), the prime \( \ell \) is unramified in both \( \mathbb{Q}(\zeta) \) and \( \mathbb{Q}(r^{1/p^n}) \), and therefore \( \mathbb{Q}_\ell(\zeta, r^{1/p^n}) \) is an unramified extension over \( \mathbb{Q}_\ell(\zeta) \). Denote the residue fields of \( \mathbb{Q}_\ell(\zeta) \) and \( \mathbb{Q}_\ell(\zeta, r^{1/p^n}) \) by \( \mathbb{F}_{\ell^1} \) and \( \mathbb{F}_{\ell^2} \), respectively. Then

\[
[\mathbb{Q}_\ell(\zeta, r^{1/p^n}) : \mathbb{Q}_\ell(\zeta)] = \frac{f_2}{f_1}
\]
We have $f_1 = \text{ord}([\ell]_{p^n})$, the smallest positive integer $f$ such that $\ell^f \equiv 1 \pmod{p^n}$. Put $s_1 = v_p(\ell - 1)$, the smallest positive integer $s$ such that $\ell \equiv 1 \pmod{p^s}$. If $s_1 = 0$, let $f_0$ be the smallest positive integer such that $p$ divides $\ell^{f_0} - 1$. If $s_1 > 0$, then $f_1 = p^{\min\{n-s_1,0\}}$.

We know $F_{\ell^r}$ is the splitting field of the polynomial $f(X) = X^{p^n} - r$ over $F_\ell$. Let $G$ be the finite abelian group in $\mathbb{F}_\ell^\times$ generated by all roots $\alpha$ of $f(X)$. Since $p$ divides the cardinality of $G$, every root $\alpha$ has order $p^n\text{ord}([\alpha]_\ell)$ by the fundamental theorem of abelian groups. Thus, $f_2$ is the smallest positive integer such that $p^n\text{ord}([\alpha]_\ell)$ divides $\ell^{f_2} - 1$. Put $s_2 = v_p(\text{ord}([\alpha]_\ell))$.

If $s_1 = 0$, then $s_2 = 0$ and $f_2 = f_0p^{n+s_2-1} = f_0p^{n-1}$. If $s_1 > 1$, then $f_2 = p^{\min\{n+s_2-s_1,0\}}$.

Thus, if $s_1 = 0$, then $f_2/f_1 = 1$. If $s_1 \geq 1$, then

$$
\frac{f_2}{f_1} = \begin{cases} 
p^{s_2} & \text{if } s_1 \leq n; 
\frac{p^{n-(s_1-s_2)}}{f_0} & \text{if } s_1 - s_2 \leq n \leq s_1; 
1 & \text{if } n \leq s_1 - s_2.
\end{cases}
$$

This gives the degree in (5.1).

Now we investigate the structure of the decomposition group $G_v$, where $v$ is a place of $k$ lying over the prime $\ell$.

**Lemma 5.2.** Let $\ell$ be a prime and $v$ a place of $k$ lying over $\ell$. Let $G_v$, $G_{1,v}$ and $G_{2,v}$ be the decomposition groups of $v$ in $G$, $G_1$ and $G_2$, respectively.

1. If $\ell = p$, then $G_v$ is a cyclic group.
2. If $\ell = \ell_1$ or $\ell_2$, then $G_v \simeq G_{1,v} \times G_{2,v}$. Moreover, if $\ell = \ell_1$, then $G_{1,v} \simeq \mathbb{Z}/p^n\mathbb{Z}$ and $G_{2,v} \simeq \mathbb{Z}/p^{m_{12}}\mathbb{Z}$, where

$$
m_{12} = \max\{\min\{n, s_1\} - (s_1 - s_2), 0\}, \quad s_1 := v_p(\ell_1 - 1), \quad s_2 := v_p(\text{ord}([\ell_2]_{\ell_1})).
$$

If $\ell = \ell_2$, then $G_{1,v} \simeq \mathbb{Z}/p^{2n}\mathbb{Z}$ and $G_{2,v} \simeq \mathbb{Z}/p^n\mathbb{Z}$, where

$$
m_{21} = \max\{\min\{n, s_1\} - (s_1 - s_2), 0\}, \quad s_1 := v_p(\ell_2 - 1), \quad s_2 := v_p(\text{ord}([\ell_1]_{\ell_2})).
$$

**Proof.** (1) By Kummer theory, it suffices to show that the group $W = \langle \ell_1, \ell_2 \rangle$ generated by $\ell_1$ and $\ell_2$ in $k^p/(k^p)^p$ is cyclic. Note that $W$ is a finite $p$-group contained in the image of $\mathbb{Z}_p^\times$ and hence in the image of $1 + p\mathbb{Z}_p$. As a profinite group $1 + p\mathbb{Z}_p$ is isomorphic to $\mathbb{Z}_p$, and any finite quotient of $1 + p\mathbb{Z}_p$ is isomorphic to $(1 + p\mathbb{Z}_p)/(1 + p^{i+1}\mathbb{Z}_p) \simeq \mathbb{Z}_p/p^i\mathbb{Z}_p$ for some $r \geq 0$, which is a cyclic group. Therefore, $W$ is cyclic and $k_p((\alpha_1, \alpha_2))$ is a cyclic extension over $k_p$.

(2) If $\ell = \ell_1$, then $F_{1,w_1} = Q_{\ell_1}(\zeta, \alpha_1)$ is totally ramified of degree $p^n$ over $k_v = Q_{\ell_1}(\zeta)$ and $F_{2,w_2} = Q_{\ell_1}(\zeta, \alpha_2)$ is unramified of degree $p^{m_{12}}$ over $k_v$ by Lemma 5.1. Since $F_{1,w_1}F_{2,w_2} = F_w$ and $F_{1,w_1} \cap F_{2,w_2} = k_v$, we have $G_v \simeq G_{1,v} \times G_{2,v} \simeq \mathbb{Z}/p^n\mathbb{Z} \times \mathbb{Z}/p^{m_{12}}\mathbb{Z}$. Similarly, we have the same result for $\ell = \ell_2$.

Let $W = \langle \ell_1, \ell_2 \rangle$ be the subgroup of $k^x/(k^x)^p$ generated by $\ell_1$ and $\ell_2$. With these generators, we shall write $W = \mathbb{Z}/p^n\mathbb{Z} \times \mathbb{Z}/p^n\mathbb{Z}$. Each subgroup $K_i = k(\alpha_i^a \beta_i^b) \subset F$ then corresponds to the cyclic subgroup of $W$ generated by the element $(a_i, b_i)$. Recall that $[K_i : k] = p^e_i$ and we assume $e_0 = \min\{e_i \mid 0 \leq i \leq m\}$. We can write $(a_i, b_i) = p^{n-e}(a'_i, b'_i)$ such that $p$ does not divide both $a'_i$ and $b'_i$. For any subset $c \subset \mathcal{I} = \{1, \ldots, m\}$ and any positive integer $d \leq \min\{e_i \mid i \in c\}$, the composition field $M_c(d)$ corresponds to the subgroup $W_c(d) = p^{n-d}(a'_i, b'_i) : i \in c$.

We have identified the Galois group $G = \text{Gal}(F/k)$ with $\text{Hom}(W, \mu)$, where $\mu$ denotes the cyclic group $(\zeta)$. For the basis $(1,0), (0,1)$ of $W$, we have a dual basis $\tau_1, \tau_2$ for $\text{Hom}(W, \mu)$:

$$
\tau_1((1,0)) = \tau_2((0,1)) = \zeta, \quad \tau_1((0,1)) = \tau_2((1,0)) = 1.
$$
We set $H := \text{Gal}(M_c(d)/k)$ and write $\pi : G \to H$ for the natural projection, which can be represented as the restriction map

$$\pi : \text{Hom}(W, \mu) \to \text{Hom}(W_c(d), \mu).$$

The condition that $M_c(d)/k$ is locally cyclic is equivalent to that for any finite place $v$ of $K$, the decomposition group $H_v$ at $v$ is cyclic. If $G_v$ is the decomposition group at $v$, then $H_v = \pi(G_v).$

This provides a method to check whether $M_c(d)$ is locally cyclic.

**Lemma 5.3.** Let $c \subset I$ be a subset and $d$ be a positive integer with $d \leq \epsilon_0$. Write

$$W_c(d) = p^{n-d}((c_1(c), d_1(c)), (0, d_2(c)))$$

as a subgroup of $\mathbb{Z}/p^n\mathbb{Z} \times \mathbb{Z}/p^n\mathbb{Z}$ for some $c_1(c), d_1(c), d_2(c) \in \mathbb{Z}/p^n\mathbb{Z}$ using row reduction. Let $m_{12}$ and $m_{21}$ be the integers as in Lemma 5.2. Then $M_c(d)$ is locally cyclic if and only if

$$p^{n-d}c_1(c) \in p^{m_{12}}\mathbb{Z} \quad \text{and} \quad p^{n-d}d_2(c) \in p^{m_{21}}\mathbb{Z}.$$

**Proof.** Let $\ell$ be a prime integer and $v$ a place of $k$ over $\ell$. If $\ell \nmid p(k_1k_2)$, then $v$ is unramified in $F$ and $G_v$ is cyclic. If $v = p$, then $G_v$ is cyclic by Lemma 5.2. Thus, it suffices to check the cyclicity of $H_v$ at $\ell = \ell_1$ or $\ell = \ell_2$. Let $W_0 \subset W$ be the subgroup such that $G_v = \text{Hom}(W/W_v, \mu)$. Then $G_v$ is cyclic if and only if the quotient $W_c(d)/W_v$ is cyclic.

If $\ell = \ell_1$, then $G_v = \mathbb{Z}/p^{m_{12}}\mathbb{Z} \times \mathbb{Z}/p^{m_{12}}\mathbb{Z}$ and $W_v = \{0\} \times p^{m_{12}}\mathbb{Z}/p^{m_{12}}\mathbb{Z}$ by Lemma 5.2. Thus, the quotient group $W_c(d)/W_v$ is cyclic if and only if

$$p^{n-d}c_1(c) = 0 \quad \text{or} \quad p^{n-d}d_2(c) \equiv 0 \pmod{p^{m_{12}}}.$$

If $\ell = \ell_2$, then $G_v = \mathbb{Z}/p^{m_{21}}\mathbb{Z} \times \mathbb{Z}/p^{m_{21}}\mathbb{Z}$ and $W_v = p^{m_{21}}\mathbb{Z}/p^{m_{21}}\mathbb{Z} \times \{0\}$ by Lemma 5.2. Thus, the quotient group $W_c(d)/W_v$ is cyclic if and only if

$$p^{n-d}c_1(c) \equiv 0 \pmod{p^{m_{21}}} \quad \text{or} \quad p^{n-d}d_2(c) = 0.$$

To sum up, $M_c(d)$ is locally cyclic if and only if $p^{n-d}c_1(c) \in p^{m_{21}}\mathbb{Z}$ and $p^{n-d}d_2(c) \in p^{m_{12}}\mathbb{Z}$. 

**Corollary 5.4.** Let $F = k(\alpha_1, \alpha_2)$ be the bicyclic field extension as above. Then $F$ is locally cyclic if and only if

$$n \leq \min \{v_p(\ell_1 - 1) - v_p(\text{ord}[\ell_2|\ell_1]), v_p(\ell_2 - 1) - v_p(\text{ord}[\ell_1|\ell_2])\}.$$

6. Computing Tate-Shafarevich groups and examples

In view of Sections 5, we have made some assumptions on $k$ and $K_i$. Our aim is to compute the Tate-Shafarevich groups $\Sha^2(k, \tilde{T}_{L/k})$ and $\Sha^2(k, \tilde{T}_{L/k})$ using Theorem 2.13. We implemented several computer programs that computed all the invariants mentioned in the theorem. The programs use the mathematical software SageMath and can be found on https://github.com/hfy880916/Tate-Shafarevich-groups-of-multinorm-one-torus

There are some advantages to make the assumptions above. First, each $K_i$ is contained in the bicyclic extension $k(\sqrt[n]{\alpha_1}, \sqrt[n]{\alpha_2})$, so we do not have to check whether a field $M_c(d)$ is a subfield when we compute the algebraic degree of freedom of an equivalence class $c$. Furthermore, the conditions “$M_c(d)$ is locally cyclic” and “$K_0(f)$ is contained in $M_c(d)$” that appear in the definitions can be converted into problems in finite abelian groups. With these advantages, we can calculate (algebraic) patching degrees and (algebraic) degrees of freedom of examples in reasonable time. Below we illustrate the results by showing two examples.
Example 6.1. We put $p = 3$ and $n = 3$, so $k = \mathbb{Q}(\zeta_{27})$. Let the primes $\ell_1 = 5$ and $\ell_2 = 19$. We consider the tori consisting of the following extensions over $k$: $K_0 = k(\sqrt[5]{5})$, $K_1 = k(\sqrt[19]{19})$, $K_2 = k(\sqrt[5]{5^3 \times 19^5})$, $K_3 = k(\sqrt[5]{5^4 \times 19^9})$, $K_4 = k(\sqrt[5]{5^4 \times 19^{15}})$. We list $a_i$ and $b_i$ as follows:

\[
\begin{align*}
  a_0 &= 1, & a_1 &= 1, & a_2 &= 2, & a_3 &= 3, & a_4 &= 5, \\
  b_0 &= 0, & b_1 &= 1, & b_2 &= 3, & b_3 &= 5, & b_4 &= 11.
\end{align*}
\]

We see that the $K_i$’s are linearly disjoint. Now we list the $e_{ij}$’s,

\[
e_{ij} = \begin{pmatrix}
  3 & 0 & 0 & 0 \\
  0 & 3 & 0 & 0 \\
  0 & 0 & 3 & 0 \\
  0 & 0 & 0 & 3
\end{pmatrix}.
\]

In this case the only nonempty $U_r$ is $U_0 = \{1, 2, 3, 4\} = \mathbb{Z}$, and it has four $1$-equivalence classes $\{1\}, \{2\}, \{3\}, \{4\}$. We compute that $L(U_0) = 0$, the algebraic patching degree $\Delta^0 = 3$, and the patching degree $\Delta_0 = 3$. We compute and list the algebraic degrees of freedom $f^\omega_c$ and degrees of freedom $f_c$ for equivalence classes $c = U_0$, $\{1\}$, $\{2\}$, $\{3\}$, $\{4\}$.

| $c$   | $U_0$ | $\{1\}$ | $\{2\}$ | $\{3\}$ | $\{4\}$ |
|------|-------|---------|---------|---------|---------|
| $f^\omega_c$ | 3     | 0       | 0       | 0       | 0       |
| $f_c$   | 1     | NE      | NE      | NE      | NE      |

**Table 1.** The algebraic degrees of freedom and degrees of freedom in Example 6.1

In the table above, “NE” stands for “does not exist”. Using Theorem 2.13 we compute the Tate-Shafarevich groups,

\[
\begin{align*}
\varPi^2(k, \overline{\mathbb{T}}_{L/k}) &\simeq (\mathbb{Z}/p^{(3-0)}\mathbb{Z})^{(4-1)} = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}, \\
\varPi^2(k, \overline{\mathbb{T}}_{L/k}) &\simeq (\mathbb{Z}/p^{(1-0)}\mathbb{Z})^{(4-1)} = \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}.
\end{align*}
\]

Example 6.2. Let $p, n, k, \ell_1, \ell_2, m$ be the same. Consider a different tori consisting of $K_0 = k(\sqrt[5]{5})$, $K_1 = k(\sqrt[19]{19})$, $K_2 = k(\sqrt[5]{5^3 \times 19^5})$, $K_3 = k(\sqrt[5]{5^4 \times 19^9})$, $K_4 = k(\sqrt[5]{5^4 \times 19^{15}})$. We list $a_i$ and $b_i$ as follows:

\[
\begin{align*}
  a_0 &= 1, & a_1 &= 1, & a_2 &= 2, & a_3 &= 4, & a_4 &= 10, \\
  b_0 &= 0, & b_1 &= 1, & b_2 &= 3, & b_3 &= 9, & b_4 &= 19.
\end{align*}
\]

The $K_i$’s are no longer linearly disjoint so we expect the components of the Tate-Shafarevich groups to be less regular. We list the $e_{ij}$’s,

\[
e_{ij} = \begin{pmatrix}
  3 & 0 & 0 & 1 & 0 \\
  0 & 3 & 0 & 0 & 2 \\
  0 & 0 & 3 & 0 & 0 \\
  1 & 0 & 0 & 3 & 0 \\
  0 & 2 & 0 & 0 & 3
\end{pmatrix}.
\]

In this case we have two nonempty $U_r$’s, $U_0 = \{1, 2, 4\}$ and $U_1 = \{3\}$. We present the $\ell$-equivalence relations that need to be considered as follows.
(a) $\ell = 0$
(b) $\ell = 1, 2$
(c) $\ell = 3$

Figure 1. For $i, j \in U_r$, they are connected by a line iff. $i \sim_{\ell} j$.

The set $R = \{0, 1\}$, and we compute that $L(U_0) = 0$, $L(U_1) = 3$. We compute the algebraic patching degrees $\Delta_\omega^c$ and patching degrees $\Delta_r$,

$$\Delta_\omega^0 = 3, \quad \Delta_\omega^1 = 3, \quad \Delta_0 = 1, \quad \Delta_1 = 1.$$ 

We compute and list the algebraic degrees of freedom $f_\omega^c$ and degrees of freedom $f_c$ for equivalence classes $c = U_0, \{1, 4\}, \{1\}, \{4\}, \{2\}$, and $U_1$.

| $c$   | $U_0$ | $\{1, 4\}$ | $\{1\}$ | $\{4\}$ | $\{2\}$ | $U_1$ |
|-------|-------|------------|---------|---------|---------|-------|
| $f_\omega^c$ | 3     | 0          | 0       | 0       | 0       | 1     |
| $f_c$     |       | NE         | NE      | NE      | NE      | NE    |

Table 2. The algebraic degrees of freedom and degrees of freedom in Example 6.2:

Hence the Tate-Shafarevich groups are

$$\text{III}^2(k, \hat{T}_{L/k}) \simeq \mathbb{Z}/p^{3-1}\mathbb{Z} \oplus (\mathbb{Z}/p^{3-0}\mathbb{Z})^{2-1} = \mathbb{Z}/9\mathbb{Z} \times \mathbb{Z}/27\mathbb{Z};$$

$$\text{III}^2(k, \hat{T}_{L/k}) \simeq (\mathbb{Z}/p^{1-0}\mathbb{Z})^{2-1} = \mathbb{Z}/3\mathbb{Z}.$$ 

**Acknowledgments**

The authors are grateful to Ting-Yu Lee for her helpful discussions and generously sharing the ideas of her work [4]. Thanks also go to Dasheng Wei for his expertise and helpful discussions. The present paper grows up through the authors’ participating an undergraduate research program (URP) held by the National Center for Theoretical Sciences. They acknowledge the NCTS for the stimulating environment. Liang and Yu are partially supported by the NSTC grant 109-2115-M-001-002-MY3.

**References**

[1] E. Bayer-Fluckiger, T.-Y. Lee, and R. Parimala. Hasse principles for multinorm equations. *Adv. Math.*, 356:106818, 35, 2019.
[2] Cyril Demarche and Dasheng Wei. Hasse principle and weak approximation for multinorm equations. *Israel J. Math.*, 202(1):275–293, 2014.
[3] W. Hürlimann. On algebraic tori of norm type. *Comment. Math. Helv.*, 59(4):539–549, 1984.
[4] T-Y Lee. The Tate-Shafarevich groups of multinorm-one tori. *Journal of Pure and Applied Algebra*, 226(7):106906, 2022.
[5] Jürgen Neukirch, Alexander Schmidt, and Kay Wingberg. *Cohomology of number fields*, volume 323 of *Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]*. Springer-Verlag, Berlin, 2000.
[6] Takashi Ono. On the Tamagawa number of algebraic tori. *Ann. of Math. (2)*, 78:47–73, 1963.
[7] Vladimir Platonov and Andrei Rapinchuk. *Algebraic groups and number theory*, volume 139 of *Pure and Applied Mathematics*. Academic Press, Inc., Boston, MA, 1994. Translated from the 1991 Russian original by Rachel Rowen.

[8] Timothy P. Pollio. On the multinorm principle for finite abelian extensions. *Pure Appl. Math. Q.*, 10(3):547–566, 2014.

[9] Timothy P. Pollio and Andrei S. Rapinchuk. The multinorm principle for linearly disjoint Galois extensions. *J. Number Theory*, 133(2):802–821, 2013.

[10] Gopal Prasad and Andrei S. Rapinchuk. Local-global principles for embedding of fields with involution into simple algebras with involution. *Comment. Math. Helv.*, 85(3):583–645, 2010.

(Huang) Department of Mathematics, National Taiwan Normal University, Taipei, Taiwan, 116059
Email address: junhao20150115@gmail.com

(Hung) Institute of Mathematics, Academia Sinica, Taipei, Taiwan, 10617
Email address: fanyunhung@gate.sinica.edu.tw

(Liang) Department of Mathematics, National Tsing-Hua University, Hsin-Chu, Taiwan, 300044
Email address: cindy11420@gmail.com

(Yu) Institute of Mathematics, Academia Sinica and the National Center for Theoretical Sciences, Taipei, Taiwan, 10617
Email address: chiafu@math.sinica.edu.tw