TAIWANESE JOURNAL OF MATHEMATICS
Vol. xx, No. x, pp. 1–24, xx 20xx
DOI: 10.11650/tjm/240303

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 general formulas of Lee [4]. Our aim is to illustrate various invariants in Lee's formulas by this class of tori, especially from the computational aspect. We also implement an effective algorithm using SageMath which computes the Tate–Shafarevich groups when each factor of L is contained in a fixed concrete bicyclic extension of a cyclotomic field 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 $\mathbb{A}_k$ denote the adele ring of k and $\mathbb{A}_L := L \bigotimes_k \mathbb{A}_k = \prod_{i=0}^{m} \mathbb{A}_{K_i}$ the adele ring of L. We have the norm map $N_{L/k} \colon \mathbb{A}_L^\times \to \mathbb{A}_k^\times$, sending elements $(x_i) \in \mathbb{A}_L^\times$ to $\prod_i N_{K_i/k}(x_i)$. We say that *the multinorm principle* holds for L/k if

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

where $k^\times$ is viewed as a subgroup of $\mathbb{A}_k^\times$ through the diagonal map. The quotient group

$$Ш(L/k) := \frac{k^\times \cap N_{L/k}(\mathbb{A}_L^\times)}{N_{L/k}(L^\times)}$$

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 Bayer-Fluckiger, Lee and Parimala [1, Proposition 4.1]). Pollio and Rapinchuk [9, Theorem, p. 803] and Wei [11, Corollary 3.3] showed the case when the respect Galois closures of K_0 and K_1 are linearly disjoint. Moreover, Pollio

Received June 15, 2023; Accepted March 6, 2024.
Communicated by Liang-Chung Hsia.
2020 *Mathematics Subject Classification.* 11G35, 12G05.
Key words and phrases. multinorm principle, Tate–Shafarevich groups, multinorm one tori.
*Corresponding author.

proved [8, Theorem 1] that if K_0 and K_1 are abelian extensions of k, then $Ш((K_0 \times K_1)/k) = Ш((K_0 \cap K_1)/k)$ and asked whether the equality holds for more general K_0 and K_1. This question was answered by Demarche and Wei [2] who constructed a family of examples, showing that the equality $Ш((K_0 \times K_1)/k) = Ш((K_0 \cap K_1)/k)$ is no longer true when K_0 and K_1 are non-abelian Galois extensions. The study of the multinorm principle is also inspired by the work of Prasad and Rapinchuk [10], where the authors settled the problem of the local-global principle for embeddings of field extensions with involution into simple algebras with involution. This provides a useful method of constructing maximal tori with given properties in a classical group over k.

Some earlier studies were focus to determine whether the multinorm principle holds true. In [1], Bayer-Fluckiger, Lee and Parimala made a breakthrough and gave a general method for computing $Ш(L/k)$ provided one of factors of L is cyclic over k. Moreover, under the condition that every factor of L is cyclic over k, they gave a necessary and sufficient condition for $Ш(L/k) = 0$ (by combining Theorem 8.1 and Propositions 8.5 and 8.6 of loc. cit.). Extending works of [1], Lee [4] gave a general formula for the group $Ш(L/k)$ when L is of p-power degree. Her formulas together with [1, Proposition 8.6] solve the computational problem of $Ш(L/k)$ completely.

The aim of this article is to compute more examples of the Tate–Shafarevich groups of multiple norm one tori based on Lee's general formulas. We consider the étale k-algebras $L = \prod_i K_i$, where each K_i/k is a cyclic extension of p-power degree and k contains the roots of unity of degree high power of p (prime to the characteristic of k). Therefore, each K_i/k is a Kummer extension. Lee introduced several invariants for describing $Ш(L/k)$ explicitly. However, some of these invariants are still rather technical and are not yet easily computable. Our main task is to illustrate these invariants introduced in [4] in this particular class of tori.

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 Tate–Sharafevich groups much more effectively. Using the combinatorial description, we implement an algorithm using SageMath which computes $Ш(L)$ 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 $k(\ell_1^{1/p^n}, \ell_2^{1/p^n})$ with primes $\ell_1, \ell_2 \neq p$, subject to the condition $\bigcap_{i=0}^{m} K_i = k$. As our algorithm is based on a combinatorial description, the computing time does not take much longer when either p or n goes large.

Note that Lee's formulas are already algorithmic. The invariants are carefully defined upon structural recursive relations. However, in the practical issue, a direct implementing the program using existing number theoretic packages has not yet worked so well (for example, for a case where $p = 3$, $n = 2$ and $m = 2$, the computer does not give an output

after 5 hours). A major obstruction is that computing the decomposition groups of a Galois extension of large degree by computer is extremely time-consuming (in that case, one needs to compute decomposition groups of a few abelian extensions of degree 54). For this reason, we study decomposition groups in this particular case for our program (see Section 5). We remark that [1, Theorem 8.1] is incorrect as stated; a counterexample can be found in [4, Example 7.7]; see Remark 2.6. We state a necessary and sufficient condition for $Ш(L/k) = 0$ based on Lee's formulas (see Corollary 2.17).

This paper is organized as follows. In Section 2, we present several results of Bayer-Fluckiger, Lee and Parimala and describe Lee's formulas for the Tate–Shafarevich groups. 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 cyclomotic field. Section 5 computes the decomposition groups of any subfield extension of the aforementioned bicyclic extension $k(\ell_1^{1/p^n}, \ell_2^{1/p^n})$. Putting everything together in the last section, we compute the Tate–Shafarevich group of the multinorm one torus in question and show examples.

2. The Tate–Shafarevich groups of multinorm one tori

In this section, we organize several results from Bayer-Fluckiger–Lee–Parimala [1] and describe formulas for the Tate–Shafarevich groups of multinorm one tori due to Lee [4].

2.1.

Let k be a global field and k_s a separable field extension of k whose Galois group is denoted by Γ_k. Let Ω_k be the set of all places of k. Let T be an algebraic torus over k. Denote by $\widehat{T} := \mathrm{Hom}_{k_s}(T, \mathbb{G}_m)$ the character group of T; it is a finite free $\mathbb{Z}$-module with a continuous action of Γ_k. Let $H^i(k, \widehat{T})$ denote the i-th Galois cohomology group of Γ_k with coefficients in $\widehat{T}$.

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

$$Ш^i(k, \widehat{T}) := \mathrm{Ker}\left(H^i(k, \widehat{T}) \to \prod_{v \in \Omega_k} H^i(k_v, \widehat{T})\right)$$

and

$$Ш^i_\omega(k, \widehat{T}) := \left\{[C] \in H^i(k, \widehat{T}) : [C]_v = 0 \text{ for almost all } v \in \Omega_k\right\},$$

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

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 $N_{L/k}\colon R_{L/k}\mathbb{G}_{m,L} \to \mathbb{G}_{\mathrm{m},k}$ be the norm morphism, and denote by

$$T_{L/k} := \operatorname{Ker} N_{L/k}$$

the multinorm one torus associated to L/k. Put $\mathcal{I} = \{1, \dots, m\}$ and $K' := \prod_{i\in\mathcal{I}} K_i$.

Let $E := K_0 \bigotimes_k K' = \prod_{i\in\mathcal{I}} E_i$, where $E_i := K_0 \bigotimes_k K_i$. 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 $f\colon R_{E/k}\mathbb{G}_{m,E} \to R_{L/k}\mathbb{G}_{m,L}$ 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

$$1 \longrightarrow S_{K_0,K'} \longrightarrow R_{E/k}(\mathbb{G}_{m,E}) \xrightarrow{f} T_{L/k} \longrightarrow 1. \tag{2.1}$$

The algebraic torus $S_{K_0,K'}$ also fits in the following exact sequence

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

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

Proposition 2.2. [1, Lemma 3.1] *There is a functorial natural isomorphism*

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

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

Define

$$Ш(L) := Ш^2(k, \widehat{T}_{L/k}) \quad \text{and} \quad Ш_\omega(L) := Ш^2_\omega(k, \widehat{T}_{L/k}).$$

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 $M(p)_{\mathrm{prim}}$ the unique subfield of $M(p)$ of degree p over k.

Proposition 2.3. [1, Propositions 5.16 and 8.6] *Let $L = \prod_{i=0}^{m} K_i$ be a product of cyclic extensions of respective degree d_i over k. Set $L(p) := \prod_{i=0}^{m} K_i(p)$. Then we have isomorphisms*

$$Ш(L) = \bigoplus_{p|d_0} Ш(K_0(p) \times K'), \quad \textit{and} \quad Ш(L) = \bigoplus_{p|d} Ш(L(p)),$$

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

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

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

$$Ш(L(p)) = 0 \quad \Longleftrightarrow \quad Ш(L(p)_{\mathrm{prim}}) = 0,$$

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

Proof. This is [1, Theorem 8.1]. Note that we add an additional condition that $\{K_i(p)\}$ are linearly disjoint over k. This is because the proof relies on [1, 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 $Ш(L)$ in the case where L is a product of cyclic extensions of degree p. More generally we have the following result [1, 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* $Ш(L) \neq 0$ *only if every field* K_i *is contained in 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* $Ш(L) \simeq (\mathbb{Z}/p\mathbb{Z})^{m-1}$.

Remark 2.6. Theorem 8.1 of [1] is incorrect as stated. Let $k = \mathbb{Q}(i)$, $K_0 = k(\sqrt[4]{13})$, $K_1 = k(\sqrt[4]{17})$ and $k(\sqrt[4]{13 \cdot 17^2})$. We have $Ш(L) = \mathbb{Z}/2\mathbb{Z}$, while $L_{\mathrm{prim}} = k(\sqrt{13}) \times k(\sqrt{17}) \times k(\sqrt{13})$ and $Ш(L_{\mathrm{prim}}) = 0$; see [4, Example 7.7]. This gives a counterexample.

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^{ϵ_i} for a positive integer ϵ_i. Assume $\bigcap_{i=0}^{m} K_i = k$ and $\epsilon_0 = \min_{0 \leq i \leq m}\{\epsilon_i\}$. For any $i, j \in \mathcal{I}$, we set

(i) $p^{e_{i,j}} = [K_i \cap K_j : k]$, and

(ii) $e_i = \epsilon_0 - e_{0,i}$.

Without loss of generality, we assume that $e_i \geq e_{i+1}$, and notice that $e_1 = \epsilon_0$ 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 $H^1(k, \widehat{T}_{E_i/K_i}) \simeq \mathbb{Z}/p^{e_i}\mathbb{Z}$.

For any $0 \leq d \leq \epsilon_i$, let $K_i(d)$ denote the subfield of K_i of degree p^d over k.[1] For a nonempty subset $c \subseteq \mathcal{I}$ and an integer $d > 0$, set $M_c(d) := \langle K_i(d) \rangle_{i \in c}$, the compositum of $K_i(d)$ for $i \in c$. For $0 \leq r \leq \epsilon_0$, set

$$U_r := \{i \in \mathcal{I} \mid e_{0,i} = r\}, \quad U_{>r} := \{i \in \mathcal{I} \mid e_{0,i} > r\}, \quad \text{and} \quad U_{<r} := \{i \in \mathcal{I} \mid e_{0,i} < r\}.$$

[1] Not to be confused this with the notation $K_i(p)$ in Section 2.1.

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* Δ_r^ω of U_r is the largest nonnegative integer $d \leq \epsilon_0$ satisfying the following two conditions:

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

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

If $U_r = \mathcal{I}$ (so $r = 0$), then we set $\Delta_0^\omega = \epsilon_0$.

We say that a field extension M of k is *locally cyclic* if its completion $M \bigotimes_k k_v$ 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* Δ_r of U_r is the largest nonnegative integer $d \leq \Delta_r^\omega$ satisfying the following two conditions:

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

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

If $U_0 = \mathcal{I}$, then we set $\Delta_0 = \epsilon_0$.

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

Definition 2.10. For each $c \subseteq \mathcal{I}$ 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 $f_{U_r}^\omega$ be the largest nonnegative integer $f \leq \Delta_r^\omega$ satisfying the following two conditions:

(i) The field $M_{U_r}(f + l_r - r)$ is a subfield of a bicyclic extension.

(ii) $K_0(f) \subseteq M_{U_r}(f + l_r - r)$.

We call $f_{U_r}^\omega$ the *algebraic degree of freedom* of U_r.

(2) Similarly, for any h-equivalence class $c \subset U_r$ with $h \geq L(U_r)$, the *algebraic degree of freedom* of c, denoted by f_c^ω, is the largest nonnegative integer $f \leq \Delta_r^\omega$ satisfying the following two conditions:

(i) The field $M_c(f + L(c) - r)$ is a subfield of a bicyclic extension.

(ii) $K_0(f) \subseteq M_c(f + L(c) - r)$.

According to the definition one has $r \leq f_c^\omega \leq f_{U_r}^\omega \leq \Delta_r^\omega$.

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 $L = \prod_{i=0}^m K_i$. We have*

$$Ш^2_\omega(k, \widehat{T}_{L/k}) \cong \bigoplus_{r \in \mathcal{R}\setminus\{0\}} \mathbb{Z}/p^{\Delta_r^w - r}\mathbb{Z} \bigoplus_{r \in \mathcal{R}} \bigoplus_{l \geq L(U_r)} \bigoplus_{c \in U_r/\sim_l} (\mathbb{Z}/p^{f_c^w - r}\mathbb{Z})^{n_{l+1}(c)-1},$$
$$Ш^2(k, \widehat{T}_{L/k}) \cong \bigoplus_{r \in \mathcal{R}\setminus\{0\}} \mathbb{Z}/p^{\Delta_r - r}\mathbb{Z} \bigoplus_{r \in \mathcal{R}} \bigoplus_{l \geq L(U_r)} \bigoplus_{c \in U_r/\sim_l} (\mathbb{Z}/p^{f_c - r}\mathbb{Z})^{n_{l+1}(c)-1},$$

where $\mathcal{R} = \{0 \leq r \leq \epsilon_0 \mid U_r \neq \emptyset\}$.

2.3.

We use Theorem 2.13 to revisit the criterion for the vanishing of the groups $Ш^2_\omega(k, \widehat{T}_{L/k})$ and $Ш^2(k, \widehat{T}_{L/k})$ [1, Theorem 8.1].

Definition 2.14. A subset $c \subset \mathcal{I}$ 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 $\mathrm{supp}(c)$, is called the support of c. Let Adm be the set of admissible subsets of $\mathcal{I}$, which depends only on the set $\{e_{i,j}\}_{1 \leq i \leq m, 1 \leq j \leq m}$.

Theorem 2.13 can be reformulated as follows.

Theorem 2.15. *We have*

$$Ш^2_\omega(k, \widehat{T}_{L/k}) \cong \bigoplus_{r \in \mathcal{R}\setminus\{0\}} \mathbb{Z}/p^{\Delta_r^w - r}\mathbb{Z} \oplus \bigoplus_{c \in \mathrm{Adm}} (\mathbb{Z}/p^{f_c^w - r}\mathbb{Z})^{n_{L(c)+1}(c)-1},$$
$$Ш^2(k, \widehat{T}_{L/k}) \cong \bigoplus_{r \in \mathcal{R}\setminus\{0\}} \mathbb{Z}/p^{\Delta_r - r}\mathbb{Z} \oplus \bigoplus_{c \in \mathrm{Adm}} (\mathbb{Z}/p^{f_c - r}\mathbb{Z})^{n_{L(c)+1}(c)-1}.$$

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

(1) *We have $Ш^2_\omega(k, \widehat{T}_{L/k}) = 0$ if and only if $\Delta_{r_0}^\omega = r_0$ and $f_{U_0}^\omega = 0$.*

(2) *We have $Ш^2(k, \widehat{T}_{L/k}) = 0$ if and only if $\Delta_{r_0} = r_0$ and $f_{U_0} = 0$.*

Proof. By Theorem 2.15, $Ш^2_\omega(k, \widehat{T}_{L/k}) = 0$ if an only if $\Delta^\omega_r = r$ for all $r \in \mathcal{R} \setminus \{0\}$ and $f^\omega_c = r$ for all admissible subsets c of support r. Since $r \le f^\omega_c \le \Delta^\omega_r$, the first condition $\Delta^\omega_r = r$ implies that $f^\omega_c = r$ for all admissible subsets c of support $r \ge 1$. Also one has $0 \le f^\omega_c \le f^\omega_{U_0}$ if $c \subset U_0$, so that the above condition is equivalent to $\Delta^\omega_r = r$ for all $r \in \mathcal{R} \setminus \{0\}$ and $f^\omega_{U_0} = 0$. By [4, Proposition 4.3], we have $\Delta^\omega_{r_0} - r_0 \ge \Delta^\omega_r - r$. This proves the first statement.

We now show $r \le f_c \le f_{U_r} \le \Delta_r$. By [4, Proposition 5.8], if $r \le f \le f^\omega_c$ and $i \in c$, then

$$M_c(f + L(c) - r) = K_0(f)K_i(f + L(c) - r).$$

Since $f \le f^\omega_{U_r}$, 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 $f_c \le f_{U_r}$.

For $r \le f \le f^\omega_{U_r} \le \Delta^\omega_r$ 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 $f \le \Delta^\omega_r$, 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 $M_{U_r}(f + L(U_r) - r)$ is locally cyclic, then $K_0(f)K_{U_{>r}}(f)$ and $K_0(f)K_{U_r}(f)$ are both locally cyclic. It follows that $f_{U_r} \le \Delta_r$. This shows $r \le f_c \le f_{U_r} \le \Delta_r$.

The second statement follows from the same argument and [4, Proposition 4.10]. □

We spread out the conditions in Proposition 2.16 and have the following result.

Corollary 2.17. *Consider the following five conditions:*

(a) $M_{U_{r_0}}(r_0 + 1) \subset \bigcap_{i \in U_{<r_0}} K_0(r_0 + 1)K_i(r_0 + 1)$;

(b) $M_{U_0}(1 + L(U_0))$ *is a subfield of a bicyclic extension of* k *and it contains* $K_0(1)$;

(c) $K_0(r_0 + 1)M_{U_{r_0}}(r_0 + 1)$ *is locally cyclic;*

(d) *If* $U_{>r_0}$ *is nonempty, then* $K_0(r_0 + 1)M_{U_{>r_0}}(r_0 + 1)$ *is locally cyclic;*

(e) $M_{U_0}(1 + L(U_0))$ *is locally cyclic.*

Then we have

(1) $Ш^2_\omega(k, \widehat{T}_{L/k}) \neq 0$ *if and only if either condition* (a) *or condition* (b) *holds.*

(2) $Ш^2(k, \widehat{T}_{L/k}) = 0$ *if and only if either the conditions* (a), (c) *and* (d) *hold, or the conditions* (b) *and* (e) *hold.*

Proof. (1) By Proposition 2.16(1), we have $Ш^2_\omega(k, \widehat{T}_{L/k}) \neq 0$ if and only if either $\Delta^\omega_{r_0} \geq r_0 + 1$ or $f^\omega_{U_0} \geq 1$. Note that if $U_{>r} \neq \emptyset$, then $M_{U_{>r}}(r+1) = K_0(r+1)$ and hence the condition

$$M_{U_{>r}}(r+1) \subset \bigcap_{i \in U_r} K_0(r+1)K_i(r+1)$$

always holds. Therefore, we have $\Delta^\omega_{r_0} \geq r_0 + 1$ if and only if condition (a) holds. On the other hand, the condition $f^\omega_{U_0} \geq 1$ holds if and only if condition (b) holds. This proves (1).

(2) By Proposition 2.16(2), we have $Ш^2(k, \widehat{T}_{L/k}) \neq 0$ if and only if either $\Delta_{r_0} \geq r_0 + 1$ or $f_{U_0} \geq 1$. By definition, we have $\Delta_{r_0} \geq r_0 + 1$ if and only if $\Delta^\omega_{r_0} \geq r_0 + 1$ and both conditions (c) and (d) hold. The first condition holds if and only if condition (a) holds.

On the other hand, we have

$$f_{U_0} \geq 1 \quad \Longleftrightarrow \quad f^\omega_{U_0} \geq 1 \text{ and condition (e) holds.} \tag{2.2}$$

Again, $f^\omega_{U_0} \geq 1$ holds if and only if condition (b). □

Remark 2.18. Assume that K_i are distinct cyclic extensions of degree p over k. We see from (2.2) that $Ш(L) \neq 0$ 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 σ. From the definition of ℓ-equivalence, U_r, ϵ_i, (algebraic) patching degrees $\Delta^{(\omega)}_r$, (algebraic) degrees of freedom f^ω_c, etc., we see that they are identical after the action of σ. Therefore the Tate–Shafarevich groups $Ш(L)$ and $Ш_\omega(L)$ given by the formula without the assumption are the same as those given by the formula with the assumption. As a result, for implementing an algorithm, we do not need to rearrange of our input data so that this assumption for ordering $\{e_i\}$ holds.

3.2.

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

First we denote

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

and let $T_{L/F} = \operatorname{Ker} N_{L/F}$ and $T_{L/k} = \operatorname{Ker} N_{L/k}$, 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 $\widetilde{k} = K_0K_1\cdots K_m$ be the composition of K_i, and set

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

Lemma 3.1. (1) *We have* $H^1(F, \widehat{T}_{L/F}) = H^1(H, \widehat{T}_{L/F}) = 0$.

(2) *We have* $H^1(F_w, \widehat{T}_{L^w/F_w}) = H^1(H_w, \widehat{T}_{L/F}) = 0$, *where* w *is any place of* F, H_w *is the decomposition group, and* $L^w = L \bigotimes_F F_w$.

Proof. (1) The first equality follows from that the group $H^1(F, \widehat{T}_{L/F})$ is independent of the choice of the splitting field. Using the short exact sequence of H-modules

$$0 \longrightarrow \mathbb{Z} \longrightarrow \widehat{T_F^L} = \bigoplus_{i=0}^m \operatorname{Ind}_{H_i}^H \mathbb{Z} \longrightarrow \widehat{T}_{L/F} \longrightarrow 0,$$

we have the long exact sequence

$$0 = H^1(H, \widehat{T_F^L}) \longrightarrow H^1(H, \widehat{T}_{L/F}) \longrightarrow H^2(H, \mathbb{Z}) \longrightarrow H^2(H, \widehat{T_F^L}).$$

Using the canonical isomorphism $H^2(H, \mathbb{Z}) \simeq \operatorname{Hom}(H, \mathbb{Q}/\mathbb{Z})$ we get

$$H^1(H, \widehat{T}_{L/F}) \simeq \operatorname{Ker}\left(\operatorname{Hom}(H, \mathbb{Q}/\mathbb{Z}) \to \bigoplus_{i=0}^m \operatorname{Hom}(H_i, \mathbb{Q}/\mathbb{Z})\right).$$

Since $\bigcap_i K_i = F$, one has $H = H_0 \cdots H_m$ and hence $H^1(H, \widehat{T}_{L/F}) = 0$.

(2) By the construction, we have $T_{L/F} \bigotimes_F F_v = T_{L^w/F_v}$. Thus, the Γ_{F_v}-module $\widehat{T}_{L^w/F_w}$ is equal to $\widehat{T}_{L/F}$ when viewed as a Γ_{F_v} by an inclusion $\Gamma_{F_v} \hookrightarrow \Gamma_F$. As its first Galois cohomology is independent of the choice of a splitting field, one gets

$$H^1(F_w, \widehat{T}_{L^w/F_w}) \simeq H^1(H_w, \widehat{T}_{L^w/F_w}) \simeq H^1(H_w, \widehat{T}_{L/F}).$$

By the same argument as (1), one obtains $H^1(F_w, \widehat{T}_{L^w/F_w}) = 0$. This completes the proof of the lemma. □

Lemma 3.2. *Let T be an algebraic torus over k and K/k a Galois splitting field for T with Galois group G. There is a natural isomorphism $Ш^2_\bullet(G, \widehat{T}) \xrightarrow{\sim} Ш^2_\bullet(k, \widehat{T})$, where $\bullet \in \{\omega, \emptyset\}$.*

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

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

Thus, to show $Ш^2_\omega(G, \widehat{T}) \xrightarrow{\sim} Ш^2_\omega(G', \widehat{T})$, it suffices to show $Ш^2_\omega(H', \widehat{T}) = 0$. Since $\widehat{T}$ is a trivial H'-module, it is equivalent to show $Ш^2_\omega(H', \mathbb{Z}) = 0$. As $H^2(H', \mathbb{Z}) \simeq H^1(H', \mathbb{Q}/\mathbb{Z})$, this follows from that

$$\mathrm{Ker}\left(\mathrm{Hom}(H', \mathbb{Q}/\mathbb{Z}) \longrightarrow \prod_C \mathrm{Hom}(C, \mathbb{Q}/\mathbb{Z})\right) = 0,$$

where C runs through all cyclic subgroups of H'. □

Proposition 3.3. *There is a natural injective map $\widehat{\iota}\colon Ш^2_\bullet(k, \widehat{T}_{L/k}) \to Ш^2_\bullet(F, \widehat{T}_{L/F})$, where $\bullet \in \{\omega, \emptyset\}$.*

Proof. First we relate the tori $T_{L/F}$ and $T_{L/k}$ by the following exact sequence, which can be checked directly at their k_s-points

$$1 \longrightarrow R_{F/k}(T_{L/F}) \xrightarrow{\iota} T^L \xrightarrow{N_{L/F}} T^F \longrightarrow 1.$$

Taking the dual yields an exact sequence

$$0 \longrightarrow \widehat{T}_{F/k} \xrightarrow{\widehat{N}_{L/F}} \widehat{T}_{L/k} \xrightarrow{\widehat{\iota}} \mathrm{Ind}_H^G \widehat{T}_{L/F} \longrightarrow 0.$$

This gives the following commutative diagram

$$\begin{array}{ccccccc}
H^1(H, \widehat{T}_{L/F}) & \longrightarrow & H^2(G, \widehat{T}_{F/k}) & \xrightarrow{\widehat{N}_{L/F}} & H^2(G, \widehat{T}_{L/k}) & \xrightarrow{\widehat{\iota}} & H^2(H, \widehat{T}_{L/F}) \\
\downarrow & & \downarrow{\scriptstyle r_{F/k}} & & \downarrow{\scriptstyle r_{L/k}} & & \downarrow{\scriptstyle r_{L/F}} \\
\prod_{w|v} H^1(H_w, \widehat{T}_{L/F}) & \longrightarrow & H^2(G_v, \widehat{T}_{F/k}) & \xrightarrow{\widehat{N}_{L/F,v}} & H^2(G_v, \widehat{T}_{L/k}) & \xrightarrow{\widehat{\iota}_v} & \prod_{w|v} H^2(H_w, \widehat{T}_{L/F})
\end{array}$$

for every decomposition group G_v of G, where w runs through places of F over 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 $\widehat{N}_{L/F}$ and $\widehat{N}_{L/F,v}$ are injective. Suppose an element $x \in H^2(G, \widehat{T}_{L/k})$ lies in $\operatorname{Ker}\widehat{\iota}$ satisfying $r_{L/k}(x) = 0$. Let $y \in H^2(G, \widehat{T}_{F/k})$ be the unique element with $\widehat{N}_{L/F}(y) = x$. Then $r_{F/k}(y) = 0$ as the map $\widehat{N}_{L/F,v}$ is injective. It follows that $Ш^2_\bullet(G, \widehat{T}_{L/k}) \cap \operatorname{Ker}\widehat{\iota} \simeq Ш^2_\bullet(G, \widehat{T}_{F/k})$. Since F/k is cyclic, the group $Ш^2_\omega(G, \widehat{T}_{F/k}) = 0$ by [4, Proposition 2.2] and hence $Ш^2(G, \widehat{T}_{F/k}) = 0$. Since $Ш^2_\bullet(G, \widehat{T}_{L/k}) \cap \operatorname{Ker}\widehat{\iota} = 0$, by Lemma 3.2 the map

$$\widehat{\iota}\colon Ш^2_\bullet(k, \widehat{T}_{L/k}) = Ш^2_\bullet(G, \widehat{T}_{L/k}) \hookrightarrow Ш^2_\bullet(H, \widehat{T}_{L/F}) = Ш^2_\bullet(F, \widehat{T}_{L/F})$$

is injective. □

Corollary 3.4. *Notation being as above, if* $Ш^2_\bullet(F, \widehat{T}_{L/F}) = 0$*, then* $Ш^2_\bullet(k, \widehat{T}_{L/k}) = 0$.

Proposition 3.3 shows the inclusion relation $Ш^2_\bullet(k, \widehat{T}_{L/k}) \hookrightarrow Ш^2_\bullet(F, \widehat{T}_{L/F})$. However, we do not know whether they are actually isomorphic. If so, we could replace k by F and assume $\bigcap_i K_i = k$ without loss of generality in Lee's formulas.

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 $\operatorname{Gal}(L/k)$ is of exponent N, that is, $\sigma^N = 1$ for any $\sigma \in \operatorname{Gal}(L/k)$. For example, if $\operatorname{char} k \neq 2$ 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)

$$\big\{\text{Kummer extensions over } k \text{ of exponent } N\big\} \longleftrightarrow \big\{\text{finite subgroups of } k^\times/(k^\times)^N\big\}.$$

For any finite subgroup W of $k^\times/(k^\times)^N$, we define

$$K_W := k\big(w^{1/N} : w \in W\big)$$

and associate K_W to W. Conversely, let L be a Kummer extension of k. Since L is of exponent N, L can be written as a compositum 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

$$W_L = \langle \overline{a_i} \mid i = 1, \ldots, m \rangle,$$

where $\overline{a_i}$ denotes the image of a_i in $k^\times/(k^\times)^N$.

Let μ_N be the group of N-th roots of unity in $k^\times$. There is a perfect pairing

$$\begin{array}{ccc} \mathrm{Gal}(K_W/k) \times W & \longrightarrow & \mu_N \\ (\sigma, w) & \longmapsto & \frac{\sigma(w^{1/N})}{w^{1/N}}. \end{array}$$

This gives a natural identification $\mathrm{Gal}(K_W/k) = \mathrm{Hom}(W, \mu_N)$. If $W_1 \subset W_2$ are two subgroups of $k^\times/(k^\times)^N$, the natural projection $\mathrm{Gal}(K_{W_2}/k) \to \mathrm{Gal}(K_{W_1}/k)$ is the restriction to W_1:

$$\mathrm{Hom}(W_2, \mu_N) \longrightarrow \mathrm{Hom}(W_1, \mu_N).$$

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*

(1) *$K_{W_1} \subset K_{W_2}$ if and only if $W_1 \subset W_2$.*

(2) *$W = W_1 W_2$ if and only if $K_W = K_{W_1} K_{W_2}$.*

(3) *$W = W_1 \cap W_2$ if and only if $K_{W_1} \cap K_{W_2} = K_W$.*

4.2. Group theoretic description for $Ш^2_\omega(k, \widehat{T}_{L/k})$ and $Ш^2(k, \widehat{T}_{L/k})$

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 $[K_i : k]$ 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 $k(\alpha_i)$, where $\alpha_i = a_i^{1/p^n}$ 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 $a_i' = a_i b^{p^n}$ so that $k(a_i^{1/p^n}) = k(a_i'^{1/p^n})$.

The correspondence (4.1) enables us to describe $Ш^2_\omega(k, \widehat{T}_{L/k})$ and $Ш^2(k, \widehat{T}_{L/k})$ in terms of information on 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 $W_I = \langle \overline{a_i} \mid i \in I \rangle$ 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^{ϵ_i}, so $K_i(d) = k(a_i^{p^{\epsilon_i - d}/p^n})$ and $W_i(d) = \big\langle \overline{a_i^{p^{\epsilon_i - d}/p^n}} \big\rangle$.

We translate the first definitions in Section 2 as follows.

(1) For $i, j \in I$, i and j are ℓ-equivalent if and only if $W_i(\ell) = W_j(\ell)$.

(2) The set $U_r = \{i \in \mathcal{I} \mid W_0(r) = W_0 \cap W_i = W_i(r)\}$.

(3) For any subset $c \subset \mathcal{I}'$, $L(c) = \min\big\{\ell \mid W_i(\ell) = W_i \cap W_j = W_j(\ell) \text{ for any } i, j \in c\big\}$.

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 $\Delta_0^\omega = \epsilon_0$. Otherwise, the algebraic patching degree of freedom Δ_r^ω 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^ω for an admissible set $c \subset U_r$ can be defined as the largest nonnegative integer $f \leq \Delta_r^\omega$ 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 Δ_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 $G_v = \mathrm{Gal}(K_w/k_v)$ corresponds to a subgroup W_v of $k_v^\times/(k_v^\times)^{p^n}$ through the duality between $\mathrm{Gal}(K/k)$ and W.

$$\begin{array}{ccc} \mathrm{Gal}(K_w/k_v) = G_v & \longleftrightarrow & W_v \subset k_v^\times/(k_v^\times)^{p^n} \\ \big\downarrow & & \big\uparrow{\scriptstyle \pi_v} \\ \mathrm{Gal}(K/k) & \longleftrightarrow & W \subset k^\times/(k^\times)^{p^n} \end{array}$$

The natural map $\pi_v\colon k^\times/(k^\times)^{p^n} \to k_v^\times/(k_v^\times)^{p^n}$ is surjective as $k^\times$ is dense in $k_v^\times$ and $(k_v^\times)^{p^n}$ is open in $k_v^\times$. By the duality, π_v maps W onto W_v. Recall that K/k being locally cyclic at v means that K_w/k_v is cyclic for any $w \mid v$, and this is equivalent to saying that $\pi_v(W)$ is cyclic for any v.

Now we can redefine the patching degree Δ_r to be the maximal positive integer $d \leq \Delta_r^\omega$ 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 $f \leq f_c^\omega$ such that $\pi_v(W_c(f + L(c) - r))$ is a cyclic group for any place v of k.

4.3. Cyclotomic cases: the combinatorial description for $Ш^2_\omega(k\widehat{T}_{L/k})$ and $Ш^2(k,\widehat{T}_{L/k})$

In this subsection we define

$$\mathcal{W} = \langle \overline{a} : a \in \mathbb{Q}^\times \rangle \subset k^\times/(k^\times)^{p^n},$$

that is, the image of $\iota\colon \mathbb{Q}^\times/(\mathbb{Q}^\times)^{p^n} \to k^\times/(k^\times)^{p^n}$. 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 $\mathcal{W}$. We shall investigate the structure of $\mathcal{W}$. Let $\mathbb{P}$ denote the set of prime numbers in $\mathbb{Q}$.

Proposition 4.2. (1) *If p is odd, then $\mathcal{W} \simeq \mathbb{Q}_{>0}/(\mathbb{Q}_{>0})^{p^n} \simeq \bigoplus_{\ell\in\mathbb{P}} \mathbb{Z}/p^n\mathbb{Z}$.*

(2) *Suppose $p = 2$.*

(a) *If $N = 2$, then $\mathcal{W} \simeq \bigoplus_{\ell\in\mathbb{P}\cup\{-1\}} \mathbb{Z}/2\mathbb{Z}$.*

(b) *If $N = 4$, then $\mathcal{W} \simeq \mathbb{Z}/2\mathbb{Z} \times \bigoplus_{\ell\in\mathbb{P}} \mathbb{Z}/4\mathbb{Z}$.*

(c) *If $N \geq 8$, then $\mathcal{W} \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2^{n-1}\mathbb{Z} \times \bigoplus_{\ell\in\mathbb{P}\setminus\{2\}} \mathbb{Z}/2^n\mathbb{Z}$.*

Proof. (1) The second isomorphism follows from the unique factorization property for positive integers and we show the first isomorphism. Write $\mathbb{Q}^\times = \{\pm 1\} \times \mathbb{Q}_{>0}$. As p is odd, we have

$$\mathbb{Q}^\times/(\mathbb{Q}^\times)^{p^n} = \{\pm 1\}/\{\pm 1\}^{p^n} \times \mathbb{Q}_{>0}/(\mathbb{Q}_{>0})^{p^n} = \mathbb{Q}_{>0}/(\mathbb{Q}_{>0})^{p^n}.$$

Thus, it suffices to show that the induced map $\iota\colon \mathbb{Q}_{>0}/(\mathbb{Q}_{>0})^{p^n} \to k^\times/(k^\times)^{p^n}$ is injective. Suppose a is a positive integer such that $a = \alpha^{p^n}$ for some $\alpha \in k^\times$. Let ℓ be a prime integer not equal to p, then ℓ is unramified in k and hence the valuation v_ℓ sends each element of $k^\times$ to an integer. Therefore, $v_\ell(a) = p^n v_\ell(\alpha) \in p^n\mathbb{Z}$. Replacing a by ab^{p^n} for a suitable $b \in \mathbb{Q}_{>0}$, we may assume that $v_\ell(a) = 0$ for all primes $\ell \neq p$ and thus $a = p^r$ for some $r \in \mathbb{Z}_{\geq 0}$. We need to show $p^n \mid r$. Again replacing a by some ab^{p^n}, we may assume that $0 \leq r < p^n$. Suppose that $0 < r < p^n$, then p^{r/p^n} is not contained in $\mathbb{Q}$. The Galois closure of $\mathbb{Q}(p^{r/p^n})$ is $\mathbb{Q}(p^{r/p^n}, \zeta_{p^m})$ for some $1 \leq m \leq n$ and is non-abelian. However, $p^{r/p^n} = \alpha \in k$ and $k = k(p^{r/p^n})$ contains a non-abelian extension $\mathbb{Q}(p^{r/p^n}, \zeta_{p^m})$, a contradiction. Therefore, $r = 0$ and the integer a must be 1, and hence we conclude that $\ker(\iota) = \{\overline{1}\}$.

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

$$\mathcal{W} = \mathbb{Q}^\times/(\mathbb{Q}^\times)^2 \simeq \bigoplus_{\ell\in\mathbb{P}\cup\{-1\}} \mathbb{Z}/2\mathbb{Z}.$$

Now suppose $N = 2^n \geq 4$. Observe that $\sqrt{2} \in \mathbb{Q}(\zeta_8)$ and $-1 \in (k^\times)^2$. If ℓ is a prime integer other than 2, then the argument in part (1) applies, so $\ker(\iota) = \ker(\iota|_{\langle\overline{-1},\overline{2}\rangle})$. It

suffices to study the restriction of ι to $\langle\overline{-1},\overline{2}\rangle$. First, the restriction of ι to $\langle\overline{-1}\rangle$ is injective: if $-1=\alpha^{2^n}$ for some $\alpha\in k$, then k must contain primitive 2^{n+1}-roots of unity, which is absurd. Next, we turn to the restriction of ι to $\langle\overline{2}\rangle$. Note that $\sqrt{2}\in\mathbb{Q}(\zeta_8)$, while $\sqrt[4]{2}$ is not contained in $\mathbb{Q}(\zeta_N)$ since $\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q}$ is not an abelian extension. From this, we deduce that if $N=4$, then the restriction of ι to $\langle\overline{2}\rangle$ is injective. We also deduce that if $N\geq 8$, then the kernel of the restriction is $\langle\overline{2^{2^{n-1}}}\rangle$. In conclusion, if $N=4$, then $\ker\iota$ is trivial and

$$\mathcal{W}\simeq\mathbb{Z}/2\mathbb{Z}\times\bigoplus_{\ell\in\mathbb{P}}\mathbb{Z}/4\mathbb{Z};$$

if $N=2^n\geq 8$, then $\ker\iota=\ker(\iota|_{\langle\overline{2}\rangle})$ and

$$\mathcal{W}\simeq\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2^{n-1}\mathbb{Z}\times\bigoplus_{\ell\in\mathbb{P}\setminus\{2\}}\mathbb{Z}/2^n\mathbb{Z}. \qquad \square$$

The structure of $\mathcal{W}$ 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 $\mathcal{W}$ for $0\leq i\in m$, 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

$$a=(-1)^{n_{-1}}\cdot 2^{n_2}\cdot\prod_{\ell\in\mathbb{P}'\setminus\{2\}}\ell^{n_\ell}$$

for a finite subset $\mathbb{P}'\subset\mathbb{P}$, then the corresponding finite subgroup is the cyclic subgroup of $\mathcal{W}$ generated by $(\overline{n_{-1}},\overline{n_2},(\overline{n}_\ell)_{\ell\in\mathbb{P}'\setminus\{2\}})$.

Using Proposition 4.1, one can compute effectively algebraic patching degrees Δ_r^ω and algebraic degrees of freedom f_c^ω. However, to compute patching degrees Δ_r and f_c, we will need to analyze further the image of a subgroup W in $k_v^\times/(k_v^\times)^{p^n}$. 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 ζ is a primitive p^n-th root of unity in $\overline{\mathbb{Q}}$, 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 ℓ_1 and ℓ_2 be two distinct prime integers with $\ell_i\neq p$, and let $F:=k(\alpha_1,\alpha_2)$, where $\alpha_1=\ell_1^{1/p^n}$ and $\alpha_2=\ell_2^{1/p^n}$. Let $m\geq 1$ be a positive integer. We assume that each component K_i of the étale k-algebra $L=\prod_{i=0}^m K_i$ 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 $G = \mathrm{Gal}(F/k)$ is bicyclic of order p^{2n} generated by two elements τ_1, τ_2,

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

Therefore, any subfield of the form $M_c(d)$, 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 $F_i = k(\alpha_i)$ with Galois group $G_i = \mathrm{Gal}(F_i/k)$ for $i = 1, 2$. We have a natural isomorphism

$$G \xrightarrow{\sim} G_1 \times G_2, \quad \sigma \mapsto (\sigma|_{F_1}, \sigma|_{F_2}).$$

For any prime ℓ, write w, w_1, w_2, and v for the places of F, F_1, F_2 and k, respectively, lying over ℓ with respect to the embedding $\overline{\mathbb{Q}} \hookrightarrow \overline{\mathbb{Q}}_\ell$. If $\ell \nmid p\ell_1\ell_2$, then ℓ is unramified in both F_1 and F_2 and hence ℓ 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 $\mathrm{ord}([r]_{m_1})$ 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 $p^{n-v_p(s)}$, where v_p is the normalized valuation at p.*

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

$$p^{\max\{\min\{n,s_1\}-(s_1-s_2),0\}}, \tag{5.1}$$

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

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 ℓ is unramified in $\mathbb{Q}(\zeta)$, the element ℓ is a uniformizer of the complete discrete valuation ring $\mathbb{Z}_\ell[\zeta]$. By Eisenstein's criterion, $f(X)$ is irreducible in $\mathbb{Z}_\ell[\zeta][X]$. 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, $\mathbb{Q}_\ell(\zeta, \ell^{s'/p^{n'}}) = \mathbb{Q}_\ell(\zeta, \ell^{1/p^{n'}})$ is a totally ramified extension over $\mathbb{Q}_\ell(\zeta)$ of degree $p^{n-v_p(s)}$.

(2) Since $\ell \nmid pr$, the prime ℓ 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 of $\mathbb{Q}_\ell(\zeta)$. Denote the residue fields of $\mathbb{Q}_\ell(\zeta)$ and $\mathbb{Q}_\ell(\zeta, r^{1/p^n})$ by $\mathbb{F}_{\ell^{f_1}}$ and $\mathbb{F}_{\ell^{f_2}}$, respectively. Then

$$\big[\mathbb{Q}_\ell(\zeta, r^{1/p^n}) : \mathbb{Q}_\ell(\zeta)\big] = \frac{f_2}{f_1}.$$

We have $f_1 = \mathrm{ord}([\ell]_{p^n})$, 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 $\ell^{f_0} - 1$, then we have $f_1 = f_0 p^{n-1}$. If $s_1 > 0$, then $f_1 = p^{\min\{n-s_1,0\}}$.

We know $\mathbb{F}_{\ell^{f_2}}$ is the splitting field of the polynomial $f(X) = X^{p^n} - r$ over $\mathbb{F}_\ell$. Let G be the finite abelian group in $\overline{\mathbb{F}}_\ell^\times$ generated by all roots α of $f(X)$. Since p divides the cardinality of G, every root α has order $p^n \,\mathrm{ord}([r]_\ell)$ by the fundamental theorem of abelian groups. Thus, f_2 is the smallest positive integer such that $p^n \,\mathrm{ord}([r]_\ell)$ divides $\ell^{f_2} - 1$. Put $s_2 = v_p(\mathrm{ord}([r]_\ell))$. If $s_1 = 0$, then $s_2 = 0$ and $f_2 = f_0 p^{n+s_2-1} = f_0 p^{n-1}$. 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

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

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 ℓ.

Lemma 5.2. *Let ℓ be a prime and v a place of k lying over ℓ. 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 ℓ is ℓ_1 or ℓ_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*

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

If $\ell = \ell_2$, then $G_{1,v} \simeq \mathbb{Z}/p^{m_{21}}\mathbb{Z}$ and $G_{2,v} \simeq \mathbb{Z}/p^n\mathbb{Z}$, where

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

Proof. (1) By Kummer theory, it suffices to show that the group $W = \langle \ell_1, \ell_2 \rangle$ generated by ℓ_1 and ℓ_2 in $k_p^\times/(k_p^\times)^{p^n}$ 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 $(1 + p\mathbb{Z}_p)/(1 + p^{r+1}\mathbb{Z}_p) \simeq \mathbb{Z}_p/p^r\mathbb{Z}_p$ 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 $F_{1,w_1} = \mathbb{Q}_{\ell_1}(\zeta, \alpha_1)$ is totally ramified of degree p^n over $k_v = \mathbb{Q}_{\ell_1}(\zeta)$ and $F_{2,w_2} = \mathbb{Q}_{\ell_1}(\zeta, \alpha_2)$ 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 $k^\times/(k^\times)^{p^n}$ generated by ℓ_1 and ℓ_2. With these generators, we shall write $W = \mathbb{Z}/p^n\mathbb{Z} \times \mathbb{Z}/p^n\mathbb{Z}$. Each subfield $K_i = k(\alpha_1^{a_i}\alpha_2^{b_i}) \subset F$ then corresponds to the cyclic subgroup of W generated by the element (a_i, b_i). Recall that $[K_i : k] = p^{\epsilon_i}$ and we assume $\epsilon_0 = \min\{\epsilon_i \mid 0 \leq i \leq m\}$. We can write $(a_i, b_i) = p^{n-\epsilon_i}(a_i', b_i')$ 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 $d \leq \min\{\epsilon_i \mid i \in c\}$, the composition field $M_c(d)$ corresponds to the subgroup $W_c(d) = p^{n-d}\langle (a_i', b_i') : i \in c \rangle$.

We have identified the Galois group $G = \mathrm{Gal}(F/k)$ with $\mathrm{Hom}(W, \mu)$, where μ denotes the cyclic group $\langle \zeta \rangle$. For the basis $(1, 0)$, $(0, 1)$ of W, we have a dual basis τ_1, τ_2 for $\mathrm{Hom}(W, \mu)$:

$$\tau_1((1,0)) = \tau_2((0,1)) = \zeta, \quad \tau_1((0,1)) = \tau_2((1,0)) = 1.$$

We set $H := \mathrm{Gal}(M_c(d)/k)$ and write $\pi\colon G \to H$ for the natural projection, which can be represented as the restriction map

$$\pi\colon \mathrm{Hom}(W, \mu) \to \mathrm{Hom}(W_c(d), \mu).$$

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 $c \subset \mathcal{I}$ be a subset and d be a positive integer with $d \leq \epsilon_0$. Write*

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

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

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

Proof. Let ℓ be a prime integer and v a place of k over ℓ. If $\ell \nmid p\ell_1\ell_2$, 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 $W_v \subset W$ be the subgroup such that $G_v = \mathrm{Hom}(W/W_v, \mu)$. Then H_v is cyclic if and only if the quotient $W_c(d)/W_v$ is cyclic.

If $\ell = \ell_1$, then $G_v = \mathbb{Z}/p^n\mathbb{Z} \times \mathbb{Z}/p^{m_{12}}\mathbb{Z}$ and $W_v = \{0\} \times p^{m_{12}}\mathbb{Z}/p^n\mathbb{Z}$ 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 $G_v = \mathbb{Z}/p^{m_{21}}\mathbb{Z} \times \mathbb{Z}/p^n\mathbb{Z}$ and $W_v = p^{m_{21}}\mathbb{Z}/p^n\mathbb{Z} \times \{0\}$ 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 bicylic field extension as above. Then F is locally cyclic if and only if*

$$n \leq \min\left\{v_p(\ell_1 - 1) - v_p(\mathrm{ord}[\ell_2]_{\ell_1}), v_p(\ell_2 - 1) - v_p(\mathrm{ord}[\ell_1]_{\ell_2})\right\}.$$

6. Computing Tate–Shafarevich groups and examples

In view of Section 5, we have made some assumptions on k and K_i. Our aim is to compute the Tate–Shafarevich groups $Ш^2_\omega(k, \widehat{T}_{L/k})$ and $Ш^2(k, \widehat{T}_{L/k})$ 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 at

`https://github.com/hfy880916/Tate-Shafarevich-groups-of-multinorm-one-torus`.

There are some advantages to making the assumptions above. First, each K_i is contained in the bicyclic extension $k(\sqrt[p^n]{\ell_1}, \sqrt[p^n]{\ell_2})$, 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 to problems in finite abelian groups. With these advantages, we can calculate (algebraic) patching degrees and (algebraic) degrees of freedom of examples in reasonable time: the most time-consuming invariant is degree of freedoms f_c, where it took 8.96 and 12 seconds to compute $\{f_c\}$ in Examples 6.1 and 6.2, respectively. Below we illustrate the results by showing two examples.

Example 6.1. We put $p = 3$ and $n = 3$, so $k = \mathbb{Q}(\zeta_{27})$. Choose the primes $\ell_1 = 5$ and $\ell_2 = 19$. We consider the multinorm one torus defined by the following extensions over k: $K_0 = k(\sqrt[27]{5})$, $K_1 = k(\sqrt[27]{5 \times 19})$, $K_2 = k(\sqrt[27]{5^2 \times 19^3})$, $K_3 = k(\sqrt[27]{5^3 \times 19^5})$, $K_4 = k(\sqrt[27]{5^5 \times 19^{11}})$. We list a_i and b_i as follows:

$$a_0 = 1, \quad a_1 = 1, \quad a_2 = 2, \quad a_3 = 3, \quad a_4 = 5,$$
$$b_0 = 0, \quad b_1 = 1, \quad b_2 = 3, \quad b_3 = 5, \quad b_4 = 11.$$

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

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

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

Table 6.1: The algebraic degrees of freedom and degrees of freedom in Example 6.1.

c	U_0	$\{1\}$	$\{2\}$	$\{3\}$	$\{4\}$
f_c^ω	3	0	0	0	0
f_c	1	NE	NE	NE	NE

In Table 6.1, "NE" stands for "does not exist". Using Theorem 2.13 we compute the Tate–Shafarevich groups,

$$Ш^2_\omega(k, \widehat{T}_{L/k}) \simeq (\mathbb{Z}/p^{(3-0)}\mathbb{Z})^{(4-1)} = \mathbb{Z}/27\mathbb{Z} \times \mathbb{Z}/27\mathbb{Z} \times \mathbb{Z}/27\mathbb{Z},$$
$$Ш^2(k, \widehat{T}_{L/k}) \simeq (\mathbb{Z}/p^{(1-0)}\mathbb{Z})^{(4-1)} = \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}.$$

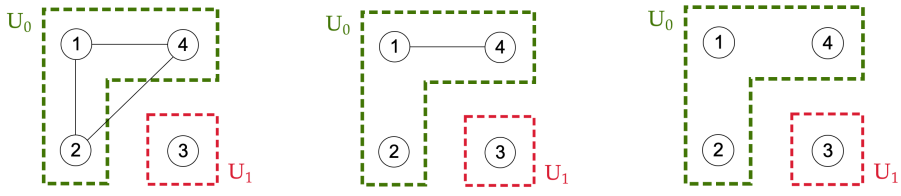
Example 6.2. Let p, n, k, ℓ_1, ℓ_2, m be the same as in Example 6.1. Consider a different mutlinorm one torus defined by the following field extensions: $K_0 = k(\sqrt[27]{5})$, $K_1 = k(\sqrt[27]{5 \times 19})$, $K_2 = k(\sqrt[27]{5^2 \times 19^3})$, $K_3 = k(\sqrt[27]{5^4 \times 19^9})$, $K_4 = k(\sqrt[27]{5^{10} \times 19^{19}})$. We list a_i and b_i as follows:

$$a_0 = 1, \quad a_1 = 1, \quad a_2 = 2, \quad a_3 = 4, \quad a_4 = 10,$$
$$b_0 = 0, \quad b_1 = 1, \quad b_2 = 3, \quad b_3 = 9, \quad b_4 = 19.$$

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 ℓ-equivalence relations that need to be considered as follows.



(a) $\ell = 0$ (b) $\ell = 1, 2$ (c) $\ell = 3$

Figure 6.1: For $i, j \in U_r$, they are connected by a line if $i \sim_\ell j$.

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

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

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

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

c	U_0	$\{1,4\}$	$\{1\}$	$\{4\}$	$\{2\}$	U_1
f_c^ω	3	0	0	0	0	1
f_c	1	NE	NE	NE	NE	NE

Hence the Tate–Shafarevich groups are

$$Ш^2_\omega(k, \widehat{T}_{L/k}) \simeq \mathbb{Z}/p^{3-1}\mathbb{Z} \oplus (\mathbb{Z}/p^{3-0}\mathbb{Z})^{2-1} = \mathbb{Z}/9\mathbb{Z} \times \mathbb{Z}/27\mathbb{Z},$$
$$Ш^2(k, \widehat{T}_{L/k}) \simeq (\mathbb{Z}/p^{1-0}\mathbb{Z})^{2-1} = \mathbb{Z}/3\mathbb{Z}.$$

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 and thank Valentijn Karemaker for helpful comments on an earlier version. Liang and Yu were partially supported by the NSTC grant 109-2115-M-001-002-MY3. The authors thank the referee for careful reading and helpful comments.

References

[1] E. Bayer-Fluckiger, T.-Y. Lee and R. Parimala, *Hasse principles for multinorm equations*, Adv. Math. **356** (2019), 106818, 35 pp.

[2] C. Demarche and D. Wei, *Hasse principle and weak approximation for multinorm equations*, Israel J. Math. **202** (2014), no. 1, 275–293.

[3] W. Hürlimann, *On algebraic tori of norm type*, Comment. Math. Helv. **59** (1984), no. 4, 539–549.

[4] T.-Y. Lee, *The Tate–Shafarevich groups of multinorm-one tori*, J. Pure Appl. Algebra **226** (2022), no. 7, Paper No. 106906, 25 pp.

[5] J. Neukirch, A. Schmidt and K. Wingberg, *Cohomology of Number Fields*, Grundlehren Math. Wiss. **323**, [Fundamental Principles of Mathematical Sciences], Springer-Verlag, Berlin, 2000.

[6] T. Ono, *On the Tamagawa number of algebraic tori*, Ann. of Math. (2) **78** (1963), 47–73.

[7] V. Platonov and A. Rapinchuk, *Algebraic Groups and Number Theory*, Pure Appl. Math. **139**, Academic Press, Boston, MA, 1994.

[8] T. P. Pollio, *On the multinorm principle for finite abelian extensions*, Pure Appl. Math. Q. **10** (2014), no. 3, 547–566.

[9] T. P. Pollio and A. S. Rapinchuk, *The multinorm principle for linearly disjoint Galois extensions*, J. Number Theory **133** (2013), no. 2, 802–821.

[10] G. Prasad and A. S. Rapinchuk, *Local-global principles for embedding of fields with involution into simple algebras with involution*, Comment. Math. Helv. **85** (2010), no. 3, 583–645.

[11] D. Wei, *On the equation* $N_{K/k}(\Xi) = P(t)$, Proc. Lond. Math. Soc. (3) **109** (2014), no. 6, 1402–1434.

Jun-Hao Huang
Department of Mathematics, National Taiwan Normal University, Taipei 116059, Taiwan
E-mail address: junhao20150115@gmail.com

Fan-Yun Hung
Department of Mathematics, UCLA, 520 Portola Plaza, Los Angeles, CA 90095-1555, USA
E-mail address: fanyunhung@gate.sinica.edu.tw

Pei-Xin Liang
Institute of Mathematics, Academia Sinica, Taipei 10617, Taiwan
E-mail address: cindy11420@gmail.com

Chia-Fu Yu
Institute of Mathematics, Academia Sinica and the National Center for Theoretical Sciences, Taipei 10617, Taiwan
E-mail address: chiafu@math.sinica.edu.tw