The Hasse norm principle for some non-Galois extensions of square-free degree

Yasuhiro Oki

March 05, 2024

Waseda Number Theory Workshop 2024

Faculty of Science, Department of Mathematics, Hokkaido University

Contents

1. Introduction

- k: a number field.

Definition

Let K/k be a finite extension, and denote by $\mathbb{A}_K^\times$ the idèle group of K. Set

$$Ш(K/k) := (k^\times \cap \mathrm{N}_{K/k}(\mathbb{A}_K^\times))/\,\mathrm{N}_{K/k}(K^\times).$$

We say that the Hasse norm principle (HNP) holds for K/k if

$$Ш(K/k) = 0.$$

The Hasse norm principle for abelian extensions

Examples (Hasse (1931)):

1. If K/k is cyclic, then $\text{Ш}(K/k) = 0$.
2. One has $\text{Ш}(\mathbb{Q}(\sqrt{-39}, \sqrt{-3})/\mathbb{Q}) \cong \mathbb{Z}/2$.

The assertion 2 is generalized as follows.

Fact 1 (Tate (1967)+ε)

Let $d = p^2 d'$, where p is a prime and $d' \in \mathbb{Z}_{>0}$.

1. There is an abelian extension K/k with group $\mathbb{Z}/p \times \mathbb{Z}/pd'$ ($\Longrightarrow [K : k] = d$) in which all decomposition groups are cyclic.
2. Let K/k be as in 1. Then there is an isomorphism

$$\text{Ш}(K/k) \cong \mathbb{Z}/p.$$

The question (1/2)

Question

Let d be a square-free positive integer. Is there a finite extension K/k of degree d so that $Ш(K/k) \neq 0$?

Remarks:

1. The question is weaker than the classification of the failure of the HNP for extensions of fixed degree (explain later).
2. If $Ш(K/k) \neq 0$, then we can construct a unirational projective variety over k of which the "unramified Brauer group" of the function field does not coincide with the Brauer group of k (Saltman, Colliot-Thélène–Sansuc etc.).

The question (2/2)

Question

Let d be a square-free positive integer. Is there a finite extension K/k of degree d so that $\text{Ш}(K/k) \neq 0$?

We must consider the HNP for non-Galois extensions.

Fact 2 (Gurak (1978), Endo–Miyata (1975))

One has $\text{Ш}(K/k) = 0$ if K/k is Galois of square-free degree.

The question has settled negatively in the case that d is a prime.

Fact 3 (Bartels (1981))

We have $\text{Ш}(K/k) = 0$ if $[K : k]$ is a prime number.

Known results on the question

There exist a number field k and an extension K/k of degree d so that $Ш(K/k) \neq 0$ if d is one of the following:

1. $d = 6$: Drakokhrust–Platonov (1987)
2. $d \leq 15$: Hoshi–Kanai–Yamasaki (2022)

Remark:

- The above studies also give a complete classification of the failure of the HNP for extensions of degree ≤ 15.
- The existence of k above are not explicit.

Today

Find a new positive answer to the question for any number field.

Main theorem

Theorem (O.)

Let d be a square-free composite number satisfying the following:

- there are prime divisors p and ℓ of d so that $2 < \ell \mid p^2 - 1$.

Then, for any number field k, there is a finite extension K/k of degree d which admits an isomorphism

$$Ш(K/k)[p^\infty] \cong \mathbb{Z}/p.$$

If $p \neq 3$ and $\ell = 3$ ($\Longrightarrow 2 < \ell \mid p^2 - 1$ is true), then we obtain

Corollary (O.)

Let d be a square-free composite number that is a multiple of 3. For any number field k, there is a finite extension K/k of degree d for which the HNP fails.

2. Norm one tori and their Tate–Shafarevich groups

Norm one tori

- k: a number field.

A k-torus is an algebraic group scheme T over k satisfying $T \otimes_k \overline{k} \cong \mathbb{G}_{m,\overline{k}}^N$ for some $N \in \mathbb{Z}_{\geq 0}$, where $\mathbb{G}_m := \operatorname{Spec} \mathbb{Z}[X^{\pm 1}]$.

Definition

For a finite extension K of k, put

$$T_{K/k} := \operatorname{Ker}(\mathrm{N}_{K/k} \colon \operatorname{Res}_{K/k} \mathbb{G}_m \to \mathbb{G}_m),$$

which is said to be the norm one torus associated to K/k.

Note: Let $K/K_0/k$ a tower of finite extensions.

$$\operatorname{Res}_{K/k} \mathbb{G}_m(k) = K^\times, \quad T_{K/k}(k) = \{x \in K^\times \mid \mathrm{N}_{K/k}(x) = 1\},$$

$$\operatorname{Res}_{K_0/k} T_{K/K_0}(k) = T_{K/K_0}(K_0).$$

Character groups of tori

Definition

Let T be a torus over k. The character group of T is defined as

$$X^*(T) := \mathrm{Hom}_{\overline{k}\text{-group}}(T, \mathbb{G}_m).$$

It is a finite free abelian group equipped with a continuous action of $\mathrm{Gal}(\overline{k}/k)$ (with respect to discrete topology).

Example: Let $\widetilde{K}/K/k$ be a tower of finite extension, where $\widetilde{K}/k$ is Galois. Put $G := \mathrm{Gal}(\widetilde{K}/k)$ and $H := \mathrm{Gal}(\widetilde{K}/K)$. Then

$$X^*(\mathbb{G}_m) \cong \mathbb{Z}, \quad X^*(\mathrm{Res}_{K/k}\,\mathbb{G}_m) \cong \mathbb{Z}[G/H],$$
$$X^*(T_{K/k}) \cong \mathrm{Coker}(\mathbb{Z} \to \mathbb{Z}[G/H]).$$

Tate–Shafarevich groups (1/2)

Let A be a $\mathrm{Gal}(\overline{k}/k)$-module, and $i \in \mathbb{Z}_{>0}$. Put

$$Ш^i(k, A) := \mathrm{Ker}\left(H^i(k, A) \xrightarrow{\mathrm{Res}} \prod_v H^i(k_v, A) \right),$$

which is said to be the *i-th Tate–Shafarevich group* of A.

Theorem 1 (Ono (1963))

Let K be a finite extension of k. Then we have

$$Ш(K/k) \cong Ш^1(k, T_{K/k}).$$

Theorem 2 (Poitou–Tate duality)

For a torus T over k, there is an isomorphism

$$Ш^1(k, T) \cong Ш^2(k, X^*(T))^\vee,$$

where $(-)^\vee$ denotes the Pontryagin dual.

Tate–Shafarevich groups (2/2)

By Theorems 1 and 2, we obtain

Corollary 3

Let K/k be a finite extension. Then there is an isomorphism

$$\text{Ш}(K/k) \cong \text{Ш}^2(k, X^*(T_{K/k}))^\vee.$$

Remark: Let T be a torus over k. Assume that $\mathrm{Gal}(\overline{k}/k)$ acts on $X^*(T)$ via its finite quotient G. Denote by $\mathcal{D}$ the set of decomposition subgroups of G. Then we have

$$\text{Ш}^2(k, X^*(T)) = \mathrm{Ker}\left(H^2(G, X^*(T)) \xrightarrow{\mathrm{Res}} \bigoplus_{D \in \mathcal{D}} H^2(D, X^*(T)) \right).$$

3. Sketch of proof

Review of main theorem

Theorem (O.)

Let d be a square-free composite number satisfying the following:

- there are prime divisors p and ℓ of d so that $2 < \ell \mid p^2 - 1$.

Then, for any number field k, there is a finite extension K/k of degree d which admits an isomorphism

$$\text{Ш}(K/k)[p^\infty] \cong \mathbb{Z}/p.$$

Recall: $\text{Ш}(K/k) \cong \text{Ш}^2(k, X^*(T_{K/k}))^\vee$ (Corollary 3).

2-dimensional representation over $\mathbb{F}_p$

We only prove the case where $d = p\ell$, where $2 < \ell \mid p^2 - 1$.

Lemma 4

Let p and ℓ be prime numbers satisfying $2 < \ell \mid p^2 - 1$. Put $G' := \mathbb{Z}/\ell$. Then there is a 2-dimensional $\mathbb{F}_p$-representation S_p of G' satisfying the following:

(1) $S_p^{G'} = 0$,

(2) there is a line L in S_p which is unstable under G'.

Proof: We may define S_p by the homomorphism

$$G' = \mathbb{Z}/\ell \to \mathrm{GL}_2(\mathbb{F}_p);\ 1 \mapsto \begin{cases} \mathrm{diag}(\zeta_\ell, \zeta_\ell^{-1}) & \text{if } p \equiv 1 \bmod \ell, \\ \begin{pmatrix} 0 & -1 \\ 1 & \zeta_\ell + \zeta_\ell^p \end{pmatrix} & \text{if } p \equiv -1 \bmod \ell. \end{cases}$$

Lemma 5

Let ℓ, $G' := \mathbb{Z}/\ell$ and S_p be as in Lemma 4, and set

$$G := S_p \rtimes G'.$$

Then, for any number field k, there is a Galois extension $\widetilde{K}/k$ with Galois group G in which all decomposition groups are cyclic.

Proof: Since G' and S_p are abelian, the group G must be solvable. Hence the assertion follows from the proof of the inverse Galois problem (Shafarevich; see also Neukirch–Schmidt–Wingberg).

Key Proposition

Let $\widetilde{K}/k$ be the Galois extension in Lemma 5, i.e.

$$\mathrm{Gal}(\widetilde{K}/k) \cong G := S_p \rtimes G'.$$

Put $H := L \rtimes \{0\}$, where L is a line which is unstable under G' (see the condition (2) in Lemma 4), and set $K := \widetilde{K}^H$.

(1) The Galois closure of K/k coincides with $\widetilde{K}/k$.

(2) There is an isomorphism

$$Ш^2(k, X^*(T_{K/k}))[p^\infty] \cong \mathbb{Z}/p.$$

Key Proposition $\Longrightarrow$ Theorem (O.): Use Corollary 3.

Proof of Key Proposition (1/2)

Proof of (1): By the non-stability of L under G' (the condition (2) in Lemma 4).

Proof of (2): Put $K_0 := \widetilde{K}^{S_p \rtimes \{0\}}$, which is contained in K. Then we obtain an exact sequence of k-tori

$$1 \to \mathrm{Res}_{K_0/k} T_{K/K_0} \xrightarrow{i} T_{K/k} \xrightarrow{\mathrm{N}_{K/K_0}} T_{K_0/k} \to 1.$$

This induces an exact sequence of G-cohomology groups

$$H^1(X^*(T_{K/k})) \xrightarrow{i^*} H^1(X^*(\mathrm{Res}_{K_0/k} T_{K/K_0})) \xrightarrow{\delta} H^2(X^*(T_{K_0/k}))$$
$$\xrightarrow{\mathrm{N}^*_{K/K_0}} H^2(X^*(T_{K/k})) \xrightarrow{i^*} H^2(X^*(\mathrm{Res}_{K_0/k} T_{K/K_0})).$$

Recall: We have $Ш^2(k, X^*(T_{K/k})) \subset H^2(X^*(T_{K/k}))$ (Remark after Corollary 3).

Proof of Key Proposition (2/2)

Define H' by the Cartesian product

$$\begin{array}{ccc} H' & \longrightarrow & Ш^2(k, X^*(T_{K/k})) \\ \downarrow & & \downarrow \\ H^2(X^*(T_{K_0/k})) & \xrightarrow{\mathrm{N}^*_{K/K_0}} & H^2(X^*(T_{K/k})). \end{array}$$

Lemma 6

Keep the notations in Key Lemma.

(1) There is an exact sequence

$$0 \to \mathbb{Z}/p \to H' \xrightarrow{\mathrm{N}^*_{K/k}} Ш^2(X^*(T_{K/k})) \to 0.$$

(2) We have $H'[p^\infty] \cong S_p^\vee \cong (\mathbb{Z}/p)^2$.

Lemma 6 $\Longrightarrow$ **Key Proposition:** Not so difficult.

Proof of Lemma 6 (1/2)

Proof of (1): By the definition of H', one has an exact sequence

$$H^1(X^*(T_{K/k})) \xrightarrow{i^*} H^1(X^*(\operatorname{Res}_{K_0/k} T_{K/K_0})) \xrightarrow{\delta} H'$$
$$\xrightarrow{\mathrm{N}^*_{K/K_0}} Ш^2(k, X^*(T_{K/k})) \to Ш^2(k, X^*(\operatorname{Res}_{K_0/k} T_{K/K_0})).$$

The following implies that the map δ induces the desired injection:

- $H^1(X^*(T_{K/k}))[p^\infty] = 0$,
- $H^1(X^*(\operatorname{Res}_{K_0/k} T_{K/K_0})) \cong \mathbb{Z}/p$.

On the other hand, Fact 3 (Bartels) and Shapiro's lemma imply

$$Ш^2(k, X^*(\operatorname{Res}_{K_0/k} T_{K/K_0})) = 0.$$

This completes the proof.

Proof of Lemma 6 (2/2)

Proof of (2): By the condition (1) in Lemma 4, we have

$$H^2(X^*(T_{K_0/k}))[p^\infty] \cong S_p^\vee/(S_p/[S_p, G])^\vee = S_p^\vee.$$

Hence it suffices to prove $H'[p^\infty] = H^2(X^*(T_{K_0/k}))[p^\infty]$. This follows from direct computation of the homomorphism

$$\delta\colon H^1(X^*(\mathrm{Res}_{K_0/k} T_{K/K_0})) \to H^2(X^*(T_{K_0/k})),$$

where we use Mackey's decomposition for G-modules $X^*(T_{K_0/k})$ and $X^*(\mathrm{Res}_{K_0/k} T_{K/K_0})$ (the assumption $S_p = (\mathbb{Z}/p)^2$ is essential).

Remark: Lemma 8 is inspired by the previous work on $Ш^2$ of "CM tori" (Liang–O.–Yang–Yu (2024)).

Thank you for your attention!