Norm one tori and Hasse norm principle

Akinari Hoshi (joint work with Kazuki Kanai and Aiichi Yamasaki)

Niigata University, Japan

September 1, 2023

Table of contents

A. Hoshi, K. Kanai, A. Yamasaki,
[HKY22] Norm one tori and Hasse norm principle, Math. Comp. (2022).
[HKY23] Norm one tori and Hasse norm principle, II: Degree 12 case, JNT (2023).
[HKY] Hasse norm principle for M_{11} and J_1 extensions, arXiv:2210.09119.

We use GAP. The related algorithms/functions are available from

`https://www.math.kyoto-u.ac.jp/~yamasaki/Algorithm/Norm1ToriHNP/`.

§1 Introduction & Main theorems 1,2,3,4

- k : a global field, i.e. a number field or a finite extension of $\mathbb{F}_q(t)$.

Definition (Hasse norm principle)

Let k be a global field. K/k be a finite extension and $\mathbb{A}_K^\times$ be the idele group of K. We say that the Hasse norm principle holds for K/k if

$$\mathrm{Obs}(K/k) := (N_{K/k}(\mathbb{A}_K^\times) \cap k^\times)/N_{K/k}(K^\times) = 1$$

where $N_{K/k}$ is the norm map.

Theorem (Hasse's norm theorem 1931)

If K/k is a cyclic extension of a number field, then

$$\mathrm{Obs}(K/k) = 1.$$

Example (Hasse [Has31]): $\mathrm{Obs}(\mathbb{Q}(\sqrt{-39}, \sqrt{-3})/\mathbb{Q}) \simeq \mathbb{Z}/2\mathbb{Z}$.
$\mathrm{Obs}(\mathbb{Q}(\sqrt{2}, \sqrt{-1})/\mathbb{Q}) = 1$.

In both cases, Galois group $G \simeq V_4$ (Klein four-group).

Tate's theorem (1967)

For any Galois extension K/k, Tate gave:

Theorem (Tate 1967, *in Alg. Num. Th. ed. by Cassels and Fröhlich*)

Let K/k be a finite Galois extension with Galois group $\mathrm{Gal}(K/k) \simeq G$. Let V_k be the set of all places of k and G_v be the decomposition group of G at $v \in V_k$. Then

$$\mathrm{Obs}(K/k) \simeq \mathrm{Coker}\{\bigoplus_{v \in V_k} \widehat{H}^{-3}(G_v, \mathbb{Z}) \xrightarrow{\text{cores}} \widehat{H}^{-3}(G, \mathbb{Z})\}$$

where $\widehat{H}$ is the Tate cohomology. In particular, In particular, the Hasse norm principle holds for K/k if and only if the restriction map $H^3(G, \mathbb{Z}) \xrightarrow{\text{res}} \bigoplus_{v \in V_k} H^3(G_v, \mathbb{Z})$ is injective.

- If $G \simeq C_n$ is cyclic, then $H^3(C_n, \mathbb{Z}) \simeq H^1(C_n, \mathbb{Z}) = 0$ and hence the Hasse's original theorem follows.
- If $G \simeq V_4$, then $\mathrm{Obs}(K/k) = 0 \iff {}^{\exists}v \in V_k$ such that $G_v = V_4$ $(H^3(V_4, \mathbb{Z}) = \mathbb{Z}/2\mathbb{Z})$ (v: should be ramified).

Known results for HNP (1/2)

The HNP for Galois extensions K/k was investigated by Gerth [Ger77], [Ger78], Gurak [Gur78a], [Gur78b], [Gur80], Morishita [Mor90], Horie [Hor93], Takeuchi [Tak94], Kagawa [Kag95], etc.

- (Gurak 1978; Endo-Miyata 1975 + Ono 1963)
  If all the Sylow subgroups of $\mathrm{Gal}(K/k)$ is cyclic, then $\mathrm{Obs}(K/k) = 0$.

However, for non-Galois extensions K/k, very little is known whether the Hasse norm principle holds:

- (Bartels 1981) $[K : k] = p$; prime $\Rightarrow$ HNP for K/k holds.
- (Bartels 1981) $[K : k] = n$ and Galois closure $\mathrm{Gal}(L/k) \simeq D_n$.
- (Voskresenskii-Kunyavskii 1984) $[K : k] = n$ and $\mathrm{Gal}(L/k) \simeq S_n$
  $\Rightarrow$ HNP for K/k holds.
- (Macedo 2020) $[K : k] = n$ and $\mathrm{Gal}(L/k) \simeq A_n$
  $\Rightarrow$ HNP for K/k holds if $n \geq 5$; $n = 6$ using Hoshi-Yamasaki [HY17].

Ono's theorem (1963)

- T : algebraic k-torus, i.e. $T \times_k \overline{k} \simeq (\mathbb{G}_{m,\overline{k}})^n$.
- $Ш(T) := \mathrm{Ker}\{H^1(k,T) \xrightarrow{\mathrm{res}} \bigoplus_{v \in V_k} H^1(k_v,T)\}$: Shafarevich-Tate gp.
- The norm one torus $R^{(1)}_{K/k}(\mathbb{G}_m)$ of K/k:

$$1 \longrightarrow R^{(1)}_{K/k}(\mathbb{G}_m) \longrightarrow R_{K/k}(\mathbb{G}_{m,K}) \xrightarrow{\mathrm{N}_{K/k}} \mathbb{G}_{m,k} \longrightarrow 1$$

  where $R_{K/k}$ is the Weil restriction.
- $R^{(1)}_{K/k}(\mathbb{G}_m)$ is biregularly isomorphic to the norm hyper surface $f(x_1,\ldots,x_n) = 1$ where $f \in k[x_1,\ldots,x_n]$ is the norm form of K/k.

Theorem (Ono 1963, Ann. of Math.)

Let K/k be a finite extension and $T = R^{(1)}_{K/k}(\mathbb{G}_m)$. Then

$$Ш(T) \simeq \mathrm{Obs}(K/k).$$

Known results for HNP (2/2)

- $T = R^{(1)}_{K/k}(\mathbb{G}_m)$.
- $Ш(T) \simeq \mathrm{Obs}(K/k)$.

Theorem (Kunyavskii 1984)

Let $[K:k]=4$, $G=\mathrm{Gal}(L/k)\simeq 4Tm$ $(1\le m\le 5)$.
Then $Ш(T)=0$ except for $4T2$ and $4T4$. For $4T2\simeq V_4$, $4T4\simeq A_4$,
(i) $Ш(T)\le \mathbb{Z}/2\mathbb{Z}$;
(ii) $Ш(T)=0 \Leftrightarrow {}^{\exists}v\in V_k$ such that $V_4\le G_v$.

Theorem (Drakokhrust-Platonov 1987)

Let $[K:k]=6$, $G=\mathrm{Gal}(L/k)\simeq 6Tm$ $(1\le m\le 16)$.
Then $Ш(T)=0$ except for $6T4$ and $6T12$. For $6T4\simeq A_4$, $6T12\simeq A_5$,
(i) $Ш(T)\le \mathbb{Z}/2\mathbb{Z}$;
(ii) $Ш(T)=0 \Leftrightarrow {}^{\exists}v\in V_k$ such that $V_4\le G_v$.

Main theorems 1,2,3,4 (1/3)

- $\exists\ 2, 13, 73, 710, 6079$ cases of alg. k-tori T of $\dim(T) = 1, 2, 3, 4, 5$.
- X: a smooth k-compactification of T, $\overline{X} = X \times_k \overline{k}$.

Theorem 1 ([HKY22, Theorem 1.5 and Theorem 1.6])

(i) $\dim(T) = 4$. Among the 216 cases (of 710) of not retract rational T,

$$H^1(k, \operatorname{Pic} \overline{X}) \simeq \begin{cases} 0 & (194 \text{ of } 216), \\ \mathbb{Z}/2\mathbb{Z} & (20 \text{ of } 216), \\ (\mathbb{Z}/2\mathbb{Z})^{\oplus 2} & (2 \text{ of } 216). \end{cases}$$

(ii) $\dim(T) = 5$. Among 3003 cases (of 6079) of not retract rational T,

$$H^1(k, \operatorname{Pic} \overline{X}) \simeq \begin{cases} 0 & (2729 \text{ of } 3003), \\ \mathbb{Z}/2\mathbb{Z} & (263 \text{ of } 3003), \\ (\mathbb{Z}/2\mathbb{Z})^{\oplus 2} & (11 \text{ of } 3003). \end{cases}$$

- Kunyavskii (1984) showed that among the 15 cases (of 73) of not retract ratinal T of $\dim(T) = 3$, $H^1(k, \operatorname{Pic} \overline{X}) = 0$ (13 of 15), $H^1(k, \operatorname{Pic} \overline{X}) \simeq \mathbb{Z}/2\mathbb{Z}$ (2 of 15).

Main theorems 1,2,3,4 (2/3)

- k : a field, K/k : a separable field extension of $[K:k]=n$.
- $T = R^{(1)}_{K/k}(\mathbb{G}_m)$ with $\dim(T) = n-1$.
- X : a smooth k-compactification of T.
- L/k : Galois closure of K/k, $G := \mathrm{Gal}(L/k)$ and $H = \mathrm{Gal}(L/K)$ with $[G:H] = n \Longrightarrow G = nTm \leq S_n$: transitive.
- The number of transitive subgroups nTm of S_n $(2 \leq n \leq 15)$ up to conjugacy is given as follows:

n	2	3	4	5	6	7	8	9	10	11	12	13	14	15
# of nTm	1	2	5	5	16	7	50	34	45	8	301	9	63	104

Theorem 2 ([HKY22, Theorem 1.5], [HKY23, Theorem 1.1])

Let $2 \leq n \leq 15$ be an integer. Then $H^1(k, \mathrm{Pic}\,\overline{X}) \neq 0 \Longleftrightarrow G = nTm$ is given as in [HKY22, Table 1] $(n \neq 12)$ or [HKY23,Table 1] $(n = 12)$.

[HKY22, Table 1]: $H^1(k, \operatorname{Pic}\overline{X}) \simeq H^1(G, [J_{G/H}]^{fl}) \neq 0$ where $G = nTm$ with $2 \leq n \leq 15$ and $n \neq 12$

G	$H^1(k, \operatorname{Pic}\overline{X}) \simeq H^1(G, [J_{G/H}]^{fl})$
$4T2 \simeq V_4$	$\mathbb{Z}/2\mathbb{Z}$
$4T4 \simeq A_4$	$\mathbb{Z}/2\mathbb{Z}$
$6T4 \simeq A_4$	$\mathbb{Z}/2\mathbb{Z}$
$6T12 \simeq A_5$	$\mathbb{Z}/2\mathbb{Z}$
$8T2 \simeq C_4 \times C_2$	$\mathbb{Z}/2\mathbb{Z}$
$8T3 \simeq (C_2)^3$	$(\mathbb{Z}/2\mathbb{Z})^{\oplus 3}$
$8T4 \simeq D_4$	$\mathbb{Z}/2\mathbb{Z}$
$8T9 \simeq D_4 \times C_2$	$\mathbb{Z}/2\mathbb{Z}$
$8T11 \simeq (C_4 \times C_2) \rtimes C_2$	$\mathbb{Z}/2\mathbb{Z}$
$8T13 \simeq A_4 \times C_2$	$\mathbb{Z}/2\mathbb{Z}$
$8T14 \simeq S_4$	$\mathbb{Z}/2\mathbb{Z}$
$8T15 \simeq C_8 \rtimes V_4$	$\mathbb{Z}/2\mathbb{Z}$
$8T19 \simeq (C_2)^3 \rtimes C_4$	$\mathbb{Z}/2\mathbb{Z}$
$8T21 \simeq (C_2)^3 \rtimes C_4$	$\mathbb{Z}/2\mathbb{Z}$
$8T22 \simeq (C_2)^3 \rtimes V_4$	$\mathbb{Z}/2\mathbb{Z}$
$8T31 \simeq ((C_2)^4 \rtimes C_2) \rtimes C_2$	$\mathbb{Z}/2\mathbb{Z}$
$8T32 \simeq ((C_2)^3 \rtimes V_4) \rtimes C_3$	$\mathbb{Z}/2\mathbb{Z}$
$8T37 \simeq \mathrm{PSL}_3(\mathbb{F}_2) \simeq \mathrm{PSL}_2(\mathbb{F}_7)$	$\mathbb{Z}/2\mathbb{Z}$
$8T38 \simeq (((C_2)^4 \rtimes C_2) \rtimes C_2) \rtimes C_3$	$\mathbb{Z}/2\mathbb{Z}$

[HKY22, Table 1]: $H^1(k, \operatorname{Pic}\overline{X}) \simeq H^1(G, [J_{G/H}]^{fl}) \neq 0$ where $G = nTm$ with $2 \leq n \leq 15$ and $n \neq 12$

G	$H^1(k, \operatorname{Pic}\overline{X}) \simeq H^1(G, [J_{G/H}]^{fl})$
$9T2 \simeq (C_3)^2$	$\mathbb{Z}/3\mathbb{Z}$
$9T5 \simeq (C_3)^2 \rtimes C_2$	$\mathbb{Z}/3\mathbb{Z}$
$9T7 \simeq (C_3)^2 \rtimes C_3$	$\mathbb{Z}/3\mathbb{Z}$
$9T9 \simeq (C_3)^2 \rtimes C_4$	$\mathbb{Z}/3\mathbb{Z}$
$9T11 \simeq (C_3)^2 \rtimes C_6$	$\mathbb{Z}/3\mathbb{Z}$
$9T14 \simeq (C_3)^2 \rtimes Q_8$	$\mathbb{Z}/3\mathbb{Z}$
$9T23 \simeq ((C_3)^2 \rtimes Q_8) \rtimes C_3$	$\mathbb{Z}/3\mathbb{Z}$
$10T7 \simeq A_5$	$\mathbb{Z}/2\mathbb{Z}$
$10T26 \simeq \mathrm{PSL}_2(\mathbb{F}_9) \simeq A_6$	$\mathbb{Z}/2\mathbb{Z}$
$10T32 \simeq S_6$	$\mathbb{Z}/2\mathbb{Z}$
$14T30 \simeq \mathrm{PSL}_2(\mathbb{F}_{13})$	$\mathbb{Z}/2\mathbb{Z}$
$15T9 \simeq (C_5)^2 \rtimes C_3$	$\mathbb{Z}/5\mathbb{Z}$
$15T14 \simeq (C_5)^2 \rtimes S_3$	$\mathbb{Z}/5\mathbb{Z}$

Main theorems 1,2,3,4 (3/3)

- k : a number field, K/k : a separable field extension of $[K:k]=n$.
- $T = R^{(1)}_{K/k}(\mathbb{G}_m)$, X : a smooth k-compactification of T.

Theorem 3 ([HKY22, Theorem 1.18], [HKY23, Theorem 1.3])

Let $2 \leq n \leq 15$ be an integer. For the cases in [HKY22, Table 1] $(n \neq 12)$ or [HKY23,Table 1] $(n = 12)$,

$$Ш(T) = 0 \iff G = nTm \text{ satisfies } \boxed{\text{some conditions}} \text{ of } G_v$$

where G_v is the decomposition group of G at v.

- By Ono's theorem $Ш(T) \simeq \mathrm{Obs}(K/k)$, Theorem 3 gives a necessary and sufficient condition for HNP for K/k with $[K:k] \leq 15$.

Theorem 4 ([HKY22, Theorem 1.17])

Assume that $G = M_n \leq S_n$ $(n = 11, 12, 22, 23, 24)$ is the Mathieu group of degree n. Then $H^1(k, \mathrm{Pic}\,\overline{X}) = 0$. In particular, $Ш(T) = 0$.

Examples of Theorem 3

Example ($G = 8T4 \simeq D_4$, $8T13 \simeq A_4 \times C_2$, $8T14 \simeq S_4$, $8T37 \simeq \mathrm{PSL}_2(\mathbb{F}_7)$, $10T7 \simeq A_5$, $14T30 \simeq \mathrm{PSL}_2(\mathbb{F}_{13})$)

$Ш(T) = 0 \iff {}^{\exists}v \in V_k$ such that $V_4 \leq G_v$.

Example ($G = 10T26 \simeq \mathrm{PSL}_2(\mathbb{F}_9)$)

$Ш(T) = 0 \iff {}^{\exists}v \in V_k$ such that $D_4 \leq G_v$.

Example ($G = 10T32 \simeq S_6 \leq S_{10}$)

$Ш(T) = 0 \iff {}^{\exists}v \in V_k$ such that
(i) $V_4 \leq G_v$ where $N_{\widetilde{G}}(V_4) \simeq C_8 \rtimes (C_2 \times C_2)$ for the normalizer $N_{\widetilde{G}}(V_4)$ of V_4 in $\widetilde{G}$ with the normalizer $\widetilde{G} = N_{S_{10}}(G) \simeq \mathrm{Aut}(G)$ of G in S_{10} or
(ii) $D_4 \leq G_v$ where $D_4 \leq [G, G] \simeq A_6$.

- $45/165$ subgroups $V_4 \leq G$ satisfy (i).
- $45/180$ subgroups $D_4 \leq G$ satisfy (ii).

Definition of some rationalities

- L/k : f.g. field extension. L is k-rational $\overset{\text{def}}{\Longleftrightarrow} L \simeq k(x_1, \ldots, x_n)$.

Definition (stably rational)

L is called stably k-rational if $L(y_i, \ldots, y_m)$ is k-rational.

Definition (retract rational)

Let k be an infinite field.
L is called retract k-rational if $\exists k$-algebra $R \subset L$ such that
(i) L is the quotient field of R;
(ii) $\exists f \in k[x_1, \ldots, x_n]$, $\exists k$-algebra hom. $\varphi : R \to k[x_1, \ldots, x_n][1/f]$ and $\psi : k[x_1, \ldots, x_n][1/f] \to R$ satisfying $\psi \circ \varphi = 1_R$.

Definition (unirational)

L is called k-unirational if $L \subset k(t_1, \ldots, t_n)$.

- "rational" $\Rightarrow$ "stably rational" $\Rightarrow$ "retract rational" $\Rightarrow$ "unirational".
- algebraic k-torus T is k-unirational.

§2 Rationality problem for algebraic tori (1/3)

Problem (Rationality problem for algebraic tori)

Whether an algebraic torus T is k-rational?

- $\exists 2$ algebraic tori with $\dim(T) = 1$; the trivial torus $\mathbb{G}_m$ and $R^{(1)}_{K/k}(\mathbb{G}_m)$ with $[K : k] = 2$, which are k-rational.
- $\exists 13$ algebraic tori with $\dim(T) = 2$;

Theorem (Voskresenskii 1967)

All the algebraic tori T with $\dim(T) = 2$ are k-rational.

- $\exists 73$ algebraic tori with $\dim(T) = 3$;

Theorem (Kunyavskii 1990)

(i) $\exists 58$ algebraic tori T with $\dim(T) = 3$ which are k-rational;
(ii) $\exists 15$ algebraic tori T with $\dim(T) = 3$ which are not k-rational;
(iii) T is k-rational $\Leftrightarrow$ T is stably k-rational $\Leftrightarrow$ T is retract k-rational.

- $\exists 710$ algebraic tori with $\dim(T) = 4$;

Theorem (Hoshi-Yamasaki 2017)

(i) $\exists 487$ algebraic tori T with $\dim(T) = 4$ which are stably k-rational;
(ii) $\exists 7$ algebraic tori T with $\dim(T) = 4$ which are not stably k-rational but retract k-rational;
(iii) $\exists 216$ algebraic tori T with $\dim(T) = 4$ which are not retract k-rational.

- $\exists 6079$ algebraic tori with $\dim(T) = 5$;

Theorem (Hoshi-Yamasaki 2017)

(i) $\exists 3051$ algebraic tori T with $\dim(T) = 5$ which are stably k-rational;
(ii) $\exists 25$ algebraic tori T with $\dim(T) = 5$ which are not stably k-rational but retract k-rational;
(iii) $\exists 3003$ algebraic tori T with $\dim(T) = 5$ which are not retract k-rational.

- We do not know "k-rationality".
- Voskresenskii's conjecture: any stably k-rational torus is k-rational (Zariski problem).

Rationality problem for algebraic tori T (2/3)

- T: algebraic k-torus
  $\Longrightarrow \exists$ finite Galois extension L/k such that $T \times_k L \simeq (\mathbb{G}_{m,L})^n$.
- $G = \mathrm{Gal}(L/k)$ where L is the minimal splitting field.

Category of algebraic k-tori which split$/L$ $\overset{\text{duality}}{\longleftrightarrow}$ Category of G-lattices (i.e. finitely generated $\mathbb{Z}$-free $\mathbb{Z}[G]$-module)

- $T \mapsto$ the character group $X(T) = \mathrm{Hom}(T, \mathbb{G}_m)$: G-lattice.
- $T = \mathrm{Spec}(L[M]^G)$ which splits$/L$ with $X(T) \simeq M \leftarrow\!\shortmid M$: G-lattice.
- Tori of dimension $n \overset{1:1}{\longleftrightarrow}$ elements of the set $H^1(\mathcal{G}, \mathrm{GL}(n, \mathbb{Z}))$ where $\mathcal{G} = \mathrm{Gal}(\overline{k}/k)$ since $\mathrm{Aut}(\mathbb{G}_m^n) = \mathrm{GL}(n, \mathbb{Z})$.
- k-torus T of dimension n is determined uniquely by the integral representation $h : \mathcal{G} \to \mathrm{GL}(n, \mathbb{Z})$ up to conjugacy, and the group $h(\mathcal{G})$ is a finite subgroup of $\mathrm{GL}(n, \mathbb{Z})$.
- The function field of T $\overset{\text{identified}}{\longleftrightarrow}$ $L(M)^G$: invariant field.

Rationality problem for algebraic tori T (3/3)

- L/k: Galois extension with $G = \mathrm{Gal}(L/k)$.
- $M = \bigoplus_{1 \le j \le n} \mathbb{Z} \cdot u_j$: G-lattice with a $\mathbb{Z}$-basis $\{u_1, \ldots, u_n\}$.
- G acts on $L(x_1, \ldots, x_n)$ by

$$\sigma(x_i) = \prod_{j=1}^{n} x_j^{a_{i,j}}, \quad 1 \le i \le n$$

  for any $\sigma \in G$, when $\sigma(u_i) = \sum_{j=1}^{n} a_{i,j} u_j$, $a_{i,j} \in \mathbb{Z}$.
- $L(M) := L(x_1, \ldots, x_n)$ with this action of G.
- $\boxed{\text{The function field of algebraic } k\text{-torus } T \overset{\text{identified}}{\longleftrightarrow} L(M)^G}$

Rationality problem for algebraic tori T (2nd form)

Whether $L(M)^G$ is k-rational?
($=$ purely transcendental over k?; $L(M)^G = k(\exists t_1, \ldots, \exists t_n)$?)

Flabby (Flasque) resolution (1/3)

- M: G-lattice, i.e. f.g. $\mathbb{Z}$-free $\mathbb{Z}[G]$-module.

Definition

(i) M is permutation $\overset{\text{def}}{\Longleftrightarrow} M \simeq \oplus_{1 \leq i \leq m} \mathbb{Z}[G/H_i]$;
(ii) M is stably permutation $\overset{\text{def}}{\Longleftrightarrow} M \oplus \exists P \simeq P'$, P, P' : permutation;
(iii) M is invertible $\overset{\text{def}}{\Longleftrightarrow} M \oplus \exists M' \simeq P$: permutation;
(iv) M is coflabby $\overset{\text{def}}{\Longleftrightarrow} H^1(H, M) = 0$ $(\forall H \leq G)$;
(v) M is flabby $\overset{\text{def}}{\Longleftrightarrow} \widehat{H}^{-1}(H, F) = 0$ $(\forall H \leq G)$.

- "permutation" $\Rightarrow$ "stably permutationl" $\Rightarrow$ "invertible"
  $\Rightarrow$ "flabby and coflabby".

Definition (Commutative monoid of G-lattices mod. permutation)

$M_1 \sim M_2 \overset{\text{def}}{\Longleftrightarrow} M_1 \oplus P_1 \simeq M_2 \oplus P_2$ $(\exists P_1, \exists P_2$: permutation)
$\Longrightarrow$ commutative monoid $\mathcal{L}$: $[M_1] + [M_2] := [M_1 \oplus M_2], 0 = [P]$.

Flabby (Flasque) resolution (2/3)

Theorem (Endo-Miyata 1975, Colliot-Thélène and Sansuc 1977)

For any G-lattice M, there exists a short exact sequence of G-lattices

$$0 \to M \to P \to F \to 0$$

where P is permutation and F is flabby.

- called a flabby resolution of the G-lattice M.
- $[M]^{fl} := [F]$: flabby class of M (well-defined).

Theorem (Endo-Miyata 1973, Voskresenskii 1974, Saltman 1984)

(EM73) $[M]^{fl} = 0 \iff L(M)^G$ is stably k-rational.
(Vos74) $[M]^{fl} = [M']^{fl} \iff L(M)^G(x_1, \ldots, x_m) \simeq L(M')^G(y_1, \ldots, y_n)$.
(Sal84) $[M]^{fl}$ is invertible $\iff L(M)^G$ is retract k-rational.

Flabby (Flasque) resolution (3/3)

Theorem (Voskresenskii 1969)

Let k be a field and $\mathcal{G} = \mathrm{Gal}(\overline{k}/k)$. Let T be an algebraic k-torus, X be a smooth k-compactification of T and $\overline{X} = X \times_k \overline{k}$. Then

$$0 \to \widehat{T} \to \widehat{Q} \to \mathrm{Pic}\,\overline{X} \to 0$$

is an exact seq. of $\mathcal{G}$-lattice where $\widehat{Q}$ is permutation and $\mathrm{Pic}\ \overline{X}$ is flabby.

- $[\widehat{T}]^{fl} = [\mathrm{Pic}\,\overline{X}]$; flabby class of $\widehat{T}$.

Theorem (Endo-Miyata 1973, Voskresenskii 1974, Saltman 1984)

(EM73) $[\mathrm{Pic}\,\overline{X}] = 0 \iff T$ is stably k-rational.
(Vos74) $[\mathrm{Pic}\,\overline{X}] = [\mathrm{Pic}\,\overline{X'}] \iff T$ and T' are stably bir. k-equivalent.
(Sal84) $[\mathrm{Pic}\,\overline{X}]$ is invertible $\iff T$ is retract k-rational.

Voskresenskii's theorem (1969) (1/2)

Theorem (Voskresenskii 1969)

Let k be a global field, T be an algebraic k-torus and X be a smooth k-compactification of T. Then there exists an exact sequence

$$0 \to A(T) \to H^1(k, \operatorname{Pic} \overline{X})^\vee \to Ш(T) \to 0$$

where $M^\vee = \operatorname{Hom}(M, \mathbb{Q}/\mathbb{Z})$ is the Pontryagin dual of M.

- The group $A(T) := \left(\prod_{v \in V_k} T(k_v)\right) \Big/ \overline{T(k)}$ is called the kernel of the weak approximation of T.
- T : retract rational $\iff$ $[\widehat{T}]^{fl} = [\operatorname{Pic} \overline{X}]$ is invertible
  $\implies$ $\operatorname{Pic} \overline{X}$ is flabby and coflabby
  $\implies$ $H^1(k, \operatorname{Pic} \overline{X})^\vee = 0 \quad \implies A(T) = Ш(T) = 0.$
- when $T = R^{(1)}_{K/k}(\mathbb{G}_m)$, by Ono's theorem $Ш(T) \simeq \operatorname{Obs}(K/k)$,
  T : retract k-rational $\implies \operatorname{Obs}(K/k) = 0$ (HNP for K/k holds).

Voskresenskii's theorem (1969) (2/2)

- when $T = R^{(1)}_{K/k}(\mathbb{G}_m)$, by Ono's theorem $Ш(T) \simeq \mathrm{Obs}(K/k)$, T : retract k-rational $\Longrightarrow \mathrm{Obs}(K/k) = 0$ (HNP for K/k holds).
- when $T = R^{(1)}_{K/k}(\mathbb{G}_m)$, $\widehat{T} = J_{G/H}$ where $J_{G/H} = (I_{G/H})^\circ = \mathrm{Hom}(I_{G/H}, \mathbb{Z})$ is the dual lattice of $I_{G/H} = \mathrm{Ker}(\varepsilon)$ and $\varepsilon : \mathbb{Z}[G/H] \to \mathbb{Z}$ is the augmentation map.
- (Hoshi-Yamasaki, 2018, Hasegawa-Hoshi-Yamasaki, 2020) For $[K : k] = n \leq 15$ except $9T27 \simeq \mathrm{PSL}_2(\mathbb{F}_8)$, the classificasion of stably/retract rational $R^{(1)}_{K/k}(\mathbb{G}_m)$ was given.
- when $T = R^{(1)}_{K/k}(\mathbb{G}_m)$, T : retract k-rational $\Longrightarrow H^1(k, \mathrm{Pic}\,\overline{X}) = 0$ (use this to get Theorem 2).
- $H^1(k, \mathrm{Pic}\,\overline{X}) \simeq \mathrm{Br}(X)/\mathrm{Br}(k) \simeq \mathrm{Br}_{\mathrm{nr}}(k(X)/k)/\mathrm{Br}(k)$ where $\mathrm{Br}(X)$ is the étale cohomological/Azumaya Brauer group of X by Colliot-Thélène-Sansuc 1987.

§3 Proof of Theorem 3

- We use Drakokhrust-Platonov's method :

Definition (first obstruction to the HNP)

Let $L \supset K \supset k$ be a tower of finite extensions where L is normal over k. We call the group

$$\mathrm{Obs}_1(L/K/k) = \left(N_{K/k}(\mathbb{A}_K^\times) \cap k^\times\right) / \left((N_{L/k}(\mathbb{A}_L^\times) \cap k^\times) N_{K/k}(K^\times)\right)$$

the first obstruction to the HNP for K/k corresponding to the tower $L \supset K \supset k$.

- $\mathrm{Obs}_1(L/K/k) = \mathrm{Obs}(K/k) \,/\, (N_{L/k}(\mathbb{A}_L^\times) \cap k^\times)$.
- $\mathrm{Obs}_1(L/K/k)$ is easier than $\mathrm{Obs}(K/k)$.
- We use GAP. The related algorithms/functions we made are available from

`https://www.math.kyoto-u.ac.jp/~yamasaki/Algorithm/Norm1ToriHNP/`.

Drakokhrust-Platonov's method (1/3)

Theorem (Drakokhrust-Platonov 1987)

Let $L \supset K \supset k$ be a tower of finite extensions where L is Galois over k. Let $G = \mathrm{Gal}(L/k)$ and $H = \mathrm{Gal}(L/K)$. Then

$$\mathrm{Obs}_1(L/K/k) \simeq \mathrm{Ker}\,\psi_1 \,/\, \varphi_1(\mathrm{Ker}\,\psi_2)$$

where

$$\begin{tikzcd}
H/[H,H] \arrow[r, "\psi_1 : H \hookrightarrow G"] & G/[G,G] \\
\bigoplus_{v \in V_k} \left(\bigoplus_{w|v} H_w/[H_w,H_w] \right) \arrow[u, "\varphi_1 : H_w \hookrightarrow H"] \arrow[r, "\psi_2"] & \bigoplus_{v \in V_k} G_v/[G_v,G_v] \arrow[u, "\varphi_2 : G_v \hookrightarrow G"]
\end{tikzcd}$$

and ψ_2 is defined by

$$\psi_2(h[H_w,H_w]) = x_i^{-1} h x_i [G_v,G_v]$$

for $h \in H_w = H \cap x_i^{-1} h x_i [G_v,G_v]$ $(x_i \in G)$.

Drakokhrust-Platonov's method (2/3)

- ψ_2^v : the restriction of the map ψ_2 to $\bigoplus_{w|v} H_w/[H_w, H_w]$.
- $\mathrm{Obs}_1(L/K/k) = \mathrm{Ker}\,\psi_1/\varphi_1(\mathrm{Ker}\,\psi_2^{\mathrm{nr}})\varphi_1(\mathrm{Ker}\,\psi_2^r)$.

Proposition (Drakokhrust-Platonov 1987)

(i) $G_{v_1} \leq G_{v_2} \Longrightarrow \varphi_1(\mathrm{Ker}\,\psi_2^{v_1}) \subset \varphi_1(\mathrm{Ker}\,\psi_2^{v_2})$;
(ii) $\varphi_1(\mathrm{Ker}\,\psi_2^{\mathrm{nr}}) = \langle [h, x] \mid h \in H \cap xHx^{-1}, x \in G\rangle/[H, H]$;
(iii) Let $H_i \leq G_i \leq G$ $(1 \leq i \leq m)$, $H_i \leq H \cap G_i$, $k_i = L^{G_i}$ and $K_i = L^{H_i}$. If $\mathrm{Obs}(K_i/k_i) = 1$ for any $1 \leq i \leq m$ and

$$\bigoplus_{i=1}^{m} \widehat{H}^{-3}(G_i, \mathbb{Z}) \xrightarrow{\text{cores}} \widehat{H}^{-3}(G, \mathbb{Z})$$

is surjective, then $\mathrm{Obs}(K/k) = \mathrm{Obs}_1(L/K/k)$. In particular,

$$[K : k] = n \text{ is square-free} \Longrightarrow \mathrm{Obs}(K/k) = \mathrm{Obs}_1(L/K/k).$$

Drakokhrust-Platonov's method (3/3)

Theorem (Drakokhrust 1989; Opolka 1980)

Let $\widetilde{L} \supset L \supset k$ be a tower of Galois extensions with $\widetilde{G} = \mathrm{Gal}(\widetilde{L}/k)$ and $\widetilde{H} = \mathrm{Gal}(\widetilde{L}/K)$ which correspond to a central extension

$$1 \to A \to \widetilde{G} \to G \to 1 \text{ with } A \cap [\widetilde{G}, \widetilde{G}] \simeq M(G) = H^2(G, \mathbb{C}^\times);$$

the Schur multiplier of G. Then

$$\mathrm{Obs}(K/k) = \mathrm{Obs}_1(\widetilde{L}/K/k).$$

In particular, if $\widetilde{G}$ is a Schur cover of G, i.e. $A \simeq M(G)$, then $\mathrm{Obs}(K/k) = \mathrm{Obs}_1(\widetilde{L}/K/k)$.

- This theorem is useful, but $\widetilde{G}$ may become large!
- We use GAP. The related algorithms/functions we made are available from

`https://www.math.kyoto-u.ac.jp/~yamasaki/Algorithm/Norm1ToriHNP/`.

Example : $G = 12T261 \simeq (S_3)^4 \rtimes V_4 \simeq S_3 \wr V_4$ (1/2)

Example ($G = 12T261 \simeq (S_3)^4 \rtimes V_4 \simeq S_3 \wr V_4$)

$Ш(T) = 0 \iff$ there exists a place v of k such that
(i) $V_4 \leq G_v$ where $V_4 \cap D(G) = 1$ for the unique characteristic subgroup $D(G) \simeq (C_3)^4 \rtimes (C_2)^3 \lhd G$,
(ii) $C_4 \times C_2 \leq G_v$ where $(C_4 \times C_2) \cap D(G1) \simeq C_2$ with $D(G) \simeq (C_3)^4 \rtimes (C_2)^3 \lhd G$,
(iii) $D_4 \leq G_v$ where $D_4 \cap (S_3)^4 \simeq C_2$ with $(S_3)^4 \lhd G$,
(iv) $Q_8 \leq G_v$, or
(v) $(C_2)^3 \rtimes C_3 \leq G_v$.

- $H^1(k, \operatorname{Pic} \overline{X}) \simeq \mathbb{Z}/2\mathbb{Z}$.
- $|G| = 6^4 \times 4 = 5184$.
- $H^3(G, \mathbb{Z}) \simeq M(G) \simeq (\mathbb{Z}/2\mathbb{Z})^{\oplus 4}$: Schur multiplier of G.

  $\widetilde{G} \leftarrow$ too large ! $|\widetilde{G}| = 6^4 \times 4 \times 2^4 = 82944$.

Example : $G = 12T261 \simeq (S_3)^4 \rtimes V_4 \simeq S_3 \wr V_4$ (2/2)

We can take a minimal stem ext. $\overline{G} = \widetilde{G}/A'$ (i.e. $\overline{A} \leq Z(\overline{G}) \cap [\overline{G}, \overline{G}]$) of G in the commutative diagram

$$\begin{tikzcd}
1 \arrow[r] & A = M(G) \arrow[r] \arrow[d] & \widetilde{G} \arrow[r, "\pi"] \arrow[d] & G \arrow[r] \arrow[d, equal] & 1 \\
1 \arrow[r] & \overline{A} = A/A' \arrow[r] & \overline{G} = \widetilde{G}/A' \arrow[r, "\overline{\pi}"] & G \arrow[r] & 1
\end{tikzcd}$$

with $\overline{A} \simeq \mathbb{Z}/2\mathbb{Z}$. There exists 15 minimal stem extensions. Then we can find exactly one (1/15) minimal stem extension which satisfies that

$$\oplus_{i=1}^{m'} \widehat{H}^{-3}(G_i, \mathbb{Z}) \xrightarrow{\text{cores}} \widehat{H}^{-3}(\overline{G}, \mathbb{Z})$$

is surjective. By Drakorust-Platonov's Proposition (iii), we have

$$\mathrm{Obs}(K/k) = \mathrm{Obs}_1(\overline{L}_j/K/k).$$

- $\mathrm{Ker}\,\psi_1 = (\mathbb{Z}/2\mathbb{Z})^{\oplus 4}$.
- $\varphi_1^{\mathrm{nr}}(\mathrm{Ker}\,\psi_2^{\mathrm{nr}}) = (\mathbb{Z}/2\mathbb{Z})^{\oplus 3}$.
- $\varphi_1^{\mathrm{r}}(\mathrm{Ker}\,\psi_2^{\mathrm{r}}) = \mathbb{Z}/2\mathbb{Z}$ ($819/891$ cases) or 0 ($72/891$ cases).

Sketch of the proof of Theorem 3 (1/2)

Step 1

• For $G = \mathrm{Gal}(L/k) = nTm \leq S_n$ and $H = \mathrm{Gal}(L/K) \leq G$ with $[G : H] = n$, determine $T = R^{(1)}_{K/k}(\mathbb{G}_m)$ satisfying $H^1(k, \mathrm{Pic}\,\overline{X}) \neq 0$.
(Make Table 1)

- We shoud treat $n = (4, 6), 8, 9, 10, 12, 14, 15$ because $H^1(k, \mathrm{Pic}\,\overline{X}) = 0$ when $n = p$: prime.

Step 2

• For the cases in Table1, determine $Ш(T) \simeq \mathrm{Obs}(K/k)$.
(2-1)

(a) $n = pq$ ($p \neq q$: primes) $\longrightarrow$ $\mathrm{Obs}(K/k) \simeq \mathrm{Obs}_1(L/K/k)$.

(b) otherwise $\longrightarrow$ Find a Schur cover $\widetilde{G}$.

Then we get $\widetilde{L}/k$ s.t. $\mathrm{Obs}(K/k) \simeq \mathrm{Obs}_1(\widetilde{L}/K/k)$.

(2-2) Calculation $\mathrm{Obs}_1(\overline{L}/K/k)$ for suitable $\overline{L} \subset \widetilde{L}$.

Sketch of the proof of Theorem 3 (2/2)

(2-2) Calculation $\mathrm{Obs}_1(\overline{L}/K/k)$.

By Drakokhrust-Platonov's Thmeorem,

$$\mathrm{Obs}_1(\overline{L}/K/k) \simeq \mathrm{Ker}\,\psi_1/\varphi_1(\mathrm{Ker}\,\psi_2^{\mathrm{nr}})\varphi_1(\mathrm{Ker}\,\psi_2^{\mathrm{r}}),$$

$$\begin{tikzcd}
H/[H,H] \arrow[r, "\psi_1"] & G/[G,G] \\
\bigoplus_{v\in V_k}\left(\bigoplus_{w|v} H_w/[H_w,H_w]\right) \arrow[u, "\varphi_1"'] \arrow[r, "\psi_2"] & \bigoplus_{v\in V_k} G_v/[G_v,G_v]. \arrow[u, "\varphi_2"']
\end{tikzcd}$$

We compute the following:

(i) $\mathrm{Ker}\,\psi_1$;

(ii) $\varphi_1(\mathrm{Ker}\,\psi_2^{\mathrm{nr}}) = \langle [h,x] \mid h \in H \cap xHx^{-1}, x \in G\rangle/[H,H]$;
(by Drakokhrust-Platonov's Proposition (ii))

(iii) $\varphi_1(\mathrm{Ker}\,\psi_2^{\mathrm{r}})$ (in terms of G_v).

§4 Application 1: R-equivalence in algebraic k-tori (1/2)

Definition (R-equivalence, Manin 1974, *in Cubic Forms*)

- $f : Z \to X$: rational map of k-varieties covers a point $x \in X(k)$.
  $\overset{\text{def}}{\Longleftrightarrow}$ there exists a point $z \in Z(k)$ such that f is defined at z and $f(z) = x$.
- $x, y \in X(k)$ are R-equivalent.
  $\overset{\text{def}}{\Longleftrightarrow}$ there exist a fin. seq. of points $x = x_1, \ldots, x_r = y$ and rational maps $f_i : \mathbb{P}^1 \to X$ $(1 \leq i \leq r-1)$ such that f_i covers x_i, x_{i+1}.

Theorem (Colliot-Thélène and Sansuc 1977)

Let k be a field, T be an algebraic k-torus and $1 \to S \to Q \to T \to 1$ be a flabby resolution of T. Then $T(k) = H^0(k, T) \xrightarrow{\delta} H^1(k, S)$ induces

$$T(k)/R \simeq H^1(k, S).$$

Application 1: R-equivalence in algebraic k-tori (2/2)

- Let k be a local field. Using Tate-Nakayama duality, we have

$$T(k)/R \simeq H^1(k, S) \simeq H^1(k, \widehat{S}) \simeq H^1(k, \operatorname{Pic} \overline{X})$$

for norm one tori $T = R^{(1)}_{K/k}(\mathbb{G}_m)$ where $[K : k] = n \leq 15$.

Theorem ([HKY22], [HKY23])

Let $2 \leq n \leq 15$ be an integer. Let k be a local field, K/k be a separable field extension of degree n, and $T = R^{(1)}_{K/k}(\mathbb{G}_m)$ be the norm one torus of K/k. Then, $T(k)/R \simeq H^1(k, \operatorname{Pic} \overline{X}) \neq 0 \iff G$ is given as in [HKY22, Table 1] of [HKY23, Table 1].

Application 2: Tamagawa number of k-tori (1/2)

Theorem (Ono 1963)

Let k be a global field, T be an algebraic k-torus and $\tau(T)$ be the Tamagawa number of T. Then

$$\tau(T) = \frac{|H^1(k, \widehat{T})|}{|Ш(T)|}.$$

In particular, if T is retract k-rational, then $\tau(T) = |H^1(k, \widehat{T})|$.

- Let k be a number field, K/k be a field extension of degree n, $T = R^{(1)}_{K/k}(\mathbb{G}_m)$ be the norm one torus of K/k. By Ono's formula, we can calculate Tamagawa number of T explicitly.
- Example. $G = 15T9 \Rightarrow \tau(T) = \dfrac{3}{5}$ or 3 because $Ш(T) \leq \mathbb{Z}/5\mathbb{Z}$.

Application 2: Tamagawa number of k-tori (2/2)

- $\tau(T) = |H^1(k, \widehat{T})|/|Ш(T)|$.

Theorem ([HKY22, Theorem 8.2])

Let k be a global field and T be an algebraic k-torus of dimension 4 (resp. 5). Among 710 (reps. 6079) cases of algebraic k-tori T, if T is one of the 688 (resp. 5805) cases with $H^1(k, \operatorname{Pic} \overline{X}) = 0$, then $\tau(T) = |H^1(k, \widehat{T})|$.

Theorem ([HKY22, Theorem 8.3], [HKY23, Remark 1.4])

Let $2 \leq n \leq 15$ be an integer. Let k be a number field, K/k be a field extension of degree n, L/k be the Galois closure of K/k, and $T = R^{(1)}_{K/k}(\mathbb{G}_m)$ be the norm one torus of K/k. Then $\tau(T) = |H^1(k, \widehat{T})|$ except for the cases in [HKY22, Table 1] and [HKY23, Table 1]. For the exceptional cases, we have $\tau(T) = |H^1(G, J_{G/H})|/|Ш(T)|$.

Sporadic simple group cases: M_{11} and J_1 (1/3)

- k : a numberl field.
- K/k : a separable field extension of $[K:k]=n$ (not fixed).
- L/k : Galois closure of K/k with $G=\mathrm{Gal}(L/k)$ and $H=\mathrm{Gal}(L/K)\lneq G$ with $[G:H]=n$.
- $T=R^{(1)}_{K/k}(\mathbb{G}_m)$ with $\dim(T)=n-1$.
- X : a smooth k-compactification of T.
- $G\simeq M_{11}$ with $|G|=7920=2^4\cdot 3^2\cdot 5\cdot 11$ or $G\simeq J_1$ with $|G|=175560=2^3\cdot 3\cdot 5\cdot 7\cdot 11\cdot 19$

  $\Rightarrow M(G)\simeq H^3(G,\mathbb{Z})=0$: Schur multiplier of G.

Theorem ([HKY, Theorem 1.6]) $G\simeq M_{11}$

Asume that $G\simeq M_{11}$ and $H=\mathrm{Gal}(L/K)\lneq G$.

$$H^1(k,\mathrm{Pic}\,\overline{X})=\begin{cases}0 & \text{if } \mathrm{Syl}_2(H)\not\simeq C_2,C_4,C_8,\\ \mathbb{Z}/2\mathbb{Z} & \text{if } \mathrm{Syl}_2(H)\simeq C_2,C_4,C_8.\end{cases}$$

Sporadic simple group cases: M_{11} and J_1 (2/3)

Theorem ([HKY, Theorem 1.8]) $G \simeq M_{11}$

Asume that $G \simeq M_{11}$ and $H = \mathrm{Gal}(L/K) \lneq G$.
(1) If $\mathrm{Syl}_2(H) \not\simeq C_2, C_4, C_8$, then $A(T) \simeq Ш(T) \simeq H^1(k, \mathrm{Pic}\,\overline{X}) = 0$.
(2) If $\mathrm{Syl}_2(H) \simeq C_2, C_4, C_8$, then either
(a) $A(T) = 0$ and $Ш(T) \simeq H^1(k, \mathrm{Pic}\,\overline{X}) \simeq \mathbb{Z}/2\mathbb{Z}$ or
(b) $A(T) \simeq H^1(k, \mathrm{Pic}\,\overline{X}) \simeq \mathbb{Z}/2\mathbb{Z}$ and $Ш(T) = 0$,
and the condition (b) is equivalent to:
(c) there exists a place v of k such that

$$\begin{cases} V_4 \leq G_v \text{ or } Q_8 \leq G_v & \text{if } \mathrm{Syl}_2(H) \simeq C_2, \\ D_4 \leq G_v \text{ or } Q_8 \leq G_v & \text{if } \mathrm{Syl}_2(H) \simeq C_4, \\ QD_8 \leq G_v & \text{if } \mathrm{Syl}_2(H) \simeq C_8 \end{cases}$$

where G_v is the decomposition group of G at a place v of k.

- $0 \to A(T) \to H^1(k, \mathrm{Pic}\,\overline{X})^\vee \to Ш(T) \to 0$ (Voskresenskii 1969).

Sporadic simple group cases: M_{11} and J_1 (3/3)

Theorem ([HKY, Theorem 1.7]) $G \simeq J_1$

Asume that $G \simeq J_1$ and $H = \mathrm{Gal}(L/K) \lneq G$.

$$H^1(k, \mathrm{Pic}\,\overline{X}) = \begin{cases} 0 & \text{if } \mathrm{Syl}_2(H) \not\simeq C_2, \\ \mathbb{Z}/2\mathbb{Z} & \text{if } \mathrm{Syl}_2(H) \simeq C_2. \end{cases}$$

Theorem ([HKY, Theorem 1.9]) $G \simeq J_1$

Asume that $G \simeq J_1$ and $H = \mathrm{Gal}(L/K) \lneq G$.

(1) If $\mathrm{Syl}_2(H) \not\simeq C_2$, then $A(T) \simeq Ш(T) \simeq H^1(k, \mathrm{Pic}\,\overline{X}) = 0$.

(2) If $\mathrm{Syl}_2(H) \simeq C_2$, then either

(a) $A(T) = 0$ and $Ш(T) \simeq H^1(k, \mathrm{Pic}\,\overline{X}) \simeq \mathbb{Z}/2\mathbb{Z}$ or

(b) $A(T) \simeq H^1(k, \mathrm{Pic}\,\overline{X}) \simeq \mathbb{Z}/2\mathbb{Z}$ and $Ш(T) = 0$,

and the condition (b) is equivalent to:

(c) there exists a place v of k such that $V_4 \leq G_v$ where G_v is the decomposition group of G at a place v of k.