ARTICLE IN PRESS YJNTH:6429

Journal of Number Theory ••• (••••) •••–•••

Contents lists available at ScienceDirect

Journal of Number Theory

www.elsevier.com/locate/jnt

General Section

The Hasse norm principle for A_n-extensions

André Macedo

Department of Mathematics and Statistics, University of Reading, Reading RG6 6AX, United Kingdom

A R T I C L E I N F O

Article history:
Received 28 November 2018
Received in revised form 30 May 2019
Accepted 2 October 2019
Available online xxxx
Communicated by A. Pal

MSC:
primary 14G05
secondary 11E72, 11R37, 20D06

Keywords:
Local-global principles
Arithmetic of algebraic tori
Group cohomology
Computational methods

A B S T R A C T

We prove that, for every $n \geq 5$, the Hasse norm principle holds for a degree n extension K/k of number fields with normal closure N such that $\mathrm{Gal}(N/k) \cong A_n$. We also show the validity of weak approximation for the associated norm one tori.

1. Introduction

Let K/k be an extension of number fields with associated idèle groups $\mathbb{A}_K^*$ and $\mathbb{A}_k^*$ and let $N_{K/k} : \mathbb{A}_K^* \to \mathbb{A}_k^*$ be the norm map on the idèles. Viewing K^* (respectively, k^*) as sitting inside $\mathbb{A}_K^*$ (respectively, $\mathbb{A}_k^*$) via the diagonal embedding, $N_{K/k}$ naturally extends the usual norm map of the extension K/k. We say that the *Hasse norm principle* (often abbreviated to HNP) holds for K/k if the *knot group*

E-mail address: c.a.v.macedo@pgr.reading.ac.uk.
URL: https://sites.google.com/view/andre-macedo/home.

https://doi.org/10.1016/j.jnt.2019.10.020

$$\mathfrak{K}(K/k) = (k^* \cap N_{K/k}(\mathbb{A}_K^*))/N_{K/k}(K^*)$$

is trivial, i.e. if every nonzero element of k which is a local norm everywhere is a global norm.

The first example of the validity of this principle was established in [16] by Hasse, who proved that the HNP holds if K/k is a cyclic extension (the Hasse norm theorem). This principle can however fail in general, with biquadratic extensions providing the simplest setting where failures are possible. For instance, 5^2 is not a global norm for the extension $\mathbb{Q}(\sqrt{13}, \sqrt{17})/\mathbb{Q}$, despite being the norm of an idèle. In general, the HNP fails for a biquadratic extension if and only if all its decomposition groups are cyclic.

In [26, p. 198], Tate presented an explicit description of the knot group of a Galois extension in terms of the group cohomology of its global and local Galois groups. Using this characterization, many results on the validity of the HNP were obtained in the Galois setting, with a particular emphasis on the abelian case, see e.g. the works of Gerth ([11], [12]), Gurak ([14], [15]) and Razar ([22]). More recently, a focus has also been placed on statistical studies of the HNP in families of extensions, see e.g. [4], [9] and [23].

Nevertheless, results for the non-abelian and non-Galois cases are still limited. For example, if N denotes the normal closure of K/k, it is known that the HNP holds for K/k when

(1) $[K : k]$ is prime ([1, Lemma 4]);
(2) $[K : k] = n$ and $\mathrm{Gal}(N/k) \cong D_n$, the dihedral group of order $2n$ ([2, Satz 1]);
(3) $[K : k] = n$ and $\mathrm{Gal}(N/k) \cong S_n$, the symmetric group on n letters ([28]).

The main underlying theoretical tool used to derive these results is the toric interpretation of the HNP: the knot group $\mathfrak{K}(K/k)$ can be canonically identified with the Tate-Shafarevich group of the norm one torus $R^1_{K/k}\mathbb{G}_m := \ker(N_{K/k} : R_{K/k}\mathbb{G}_m \to \mathbb{G}_m)$, where $R_{K/k}\mathbb{G}_m$ denotes the Weil restriction of $\mathbb{G}_m$ from K to k. This recognition of the knot group implies that the HNP holds for K/k if and only if the Hasse principle holds for every principal homogeneous space under $R^1_{K/k}\mathbb{G}_m$. See Section 2.2 for more details and results concerning this interpretation.

In this paper, we add to the above list of results by studying the HNP for a degree n extension K/k with normal closure N such that $\mathrm{Gal}(N/k)$ is isomorphic to A_n, the alternating group on n letters. We also look at *weak approximation* – recall that this property is said to hold for a variety X/k if $X(k)$ is dense (for the product topology) in $\prod_v X(k_v)$, where the product is taken over all places v of k and k_v denotes the completion of k at v. In particular, we examine weak approximation for the norm one torus $R^1_{K/k}\mathbb{G}_m$ associated to a degree n extension K/k of number fields with A_n-normal closure.

The first non-trivial case is $n = 3$. In this case, $K = N$ is a cyclic extension of k and the Hasse norm theorem implies that the HNP holds for K/k. Moreover, using a result of Voskresenskiĭ, one can show that weak approximation holds for the associated norm one torus. In [20], Kunyavskiĭ solved the case $n = 4$ by showing that, for a quartic extension

Please cite this article in press as: A. Macedo, The Hasse norm principle for A_n-extensions, J. Number Theory (2019), https://doi.org/10.1016/j.jnt.2019.10.020

K/k with A_4-normal closure, $\mathfrak{K}(K/k)$ is either 0 or $\mathbb{Z}/2$ and both cases can occur. Additionally, he proved that the HNP holds for K/k if and only if weak approximation fails for $R^1_{K/k}\mathbb{G}_m$. We complete the picture for this family of extensions by proving the following theorem.

Theorem 1.1 *(Main Theorem). Let $n \geq 5$ be an integer. Let K/k be a degree n extension of number fields and let N be its normal closure. If* $\mathrm{Gal}(N/k) \cong A_n$*, then the Hasse norm principle holds for K/k and weak approximation holds for the norm one torus $R^1_{K/k}\mathbb{G}_m$.*

Our strategy to establish this result is twofold. First, we combine the toric interpretation of the HNP with several cohomological facts about A_n-modules to prove the aforementioned result for $n \geq 8$. Next, we use a computational method developed by Hoshi and Yamasaki to solve the case $n = 6$. The remaining cases $n = 5$ and 7 follow from the remark below.

Remark 1.2. We note that when $n = p$ is a prime number, Theorem 1.1 was already known. Indeed, in this case the HNP always holds by fact (1) above and a result of Colliot-Thélène and Sansuc on the rationality of the norm one torus of an extension with prime degree also shows the validity of weak approximation (see Proposition 9.1 and Remark 9.3 of [7]).

The layout of this paper is as follows. In Section 2, we recall some basic group cohomology constructions and results on the arithmetic of algebraic tori. In Section 3, we use various group-theoretic tools to establish the surjectivity of an important map on the cohomology of A_n. We then make use of this result to prove Theorem 1.1 for $n \geq 8$. In Section 4, we exploit a computational method developed by Hoshi and Yamasaki to solve the case $n = 6$.

Notation

Throughout this paper, we fix the following notation.

k	a number field
$\overline{k}$	an algebraic closure of k
Ω_k	the set of all places of k
k_v	the completion of k at $v \in \Omega_k$
$\mathbb{A}_k^*$	the idèle group of k

For a variety X defined over a field K, we use the notation

$X_L = X \times_K L$	the base change of X to a field extension L/K
$\overline{X} = X \times_K \overline{K}$	the base change of X to an algebraic closure of K
$\operatorname{Pic} X$	the Picard group of X

We define $\mathbb{G}_{m,K} = \mathrm{Spec}(K[t, t^{-1}])$ to be the multiplicative group over a field K and, if K is apparent from the context, we omit it from the subscript and simply write $\mathbb{G}_m$.

Please cite this article in press as: A. Macedo, The Hasse norm principle for A_n-extensions, J. Number Theory (2019), https://doi.org/10.1016/j.jnt.2019.10.020

Given an algebraic K-torus T, we write $\widehat{T}$ for its character group $\mathrm{Hom}(\overline{T}, \mathbb{G}_{m,\overline{K}})$. If L/K is a finite extension of fields and T is an L-torus, we denote the Weil restriction of T from L to K by $R_{L/K}T$. We use the notation $R^1_{L/K}\mathbb{G}_m$ for the norm one torus, defined as the kernel of the norm map $N_{L/K} : R_{L/K}\mathbb{G}_m \to \mathbb{G}_m$.

Let G be a finite group. The label 'G-module' shall always mean a free $\mathbb{Z}$-module of finite rank equipped with a right action of G. For a G-module A and $q \in \mathbb{Z}$, we denote the Tate cohomology groups by $\hat{\mathrm{H}}^q(G, A)$. Since $\hat{\mathrm{H}}^q(G, A) = \mathrm{H}^q(G, A)$ for $q \geq 1$, we will omit the hat in this case. We use the notation $Z(G)$, $[G, G]$ and $M(G)$ for the center, the derived subgroup and the Schur multiplier $\hat{\mathrm{H}}^{-3}(G, \mathbb{Z})$ of G, respectively. If G is abelian, we denote its Pontryagin dual $\mathrm{Hom}(G, \mathbb{Q}/\mathbb{Z})$ by $G^{\sim}$. Given elements $g, h \in G$, we use the conventions $[g, h] = ghg^{-1}h^{-1}$ and $g^h = hgh^{-1}$.

We often use '=' to indicate a canonical isomorphism between two objects.

2. Preliminaries

2.1. Chevalley modules

Let G be a finite group and H a subgroup of G. Recall that we have the augmentation map $\varepsilon : \mathbb{Z}[G/H] \to \mathbb{Z}$ defined by mapping $Hg \mapsto 1$ for any $Hg \in G/H$. This map produces the exact sequence of G-modules

$$0 \to I_{G/H} \to \mathbb{Z}[G/H] \xrightarrow{\varepsilon} \mathbb{Z} \to 0, \tag{2.1}$$

where $I_{G/H} = \ker(\varepsilon)$ is the augmentation ideal. Dually, we have a norm map $\eta : \mathbb{Z} \to \mathbb{Z}[G/H]$ defined by $\eta : 1 \mapsto N_{G/H}$, where $N_{G/H} = \sum_{Hg \in G/H} Hg$. This produces the exact sequence of G-modules

$$0 \to \mathbb{Z} \xrightarrow{\eta} \mathbb{Z}[G/H] \to J_{G/H} \to 0, \tag{2.2}$$

where $J_{G/H} = \mathrm{coker}(\eta)$ (called the *Chevalley module* of G/H) is the dual module $\mathrm{Hom}(I_{G/H}, \mathbb{Z})$ of $I_{G/H}$.

For any $g \in G$, we can consider the restriction maps

$$\mathrm{Res}_g : \mathrm{H}^2(G, J_{G/H}) \to \mathrm{H}^2(\langle g \rangle, J_{G/H})$$

and aggregate all of these functions together in order to get a homomorphism of G-modules

$$\mathrm{Res} : \mathrm{H}^2(G, J_{G/H}) \to \prod_{g \in G} \mathrm{H}^2(\langle g \rangle, J_{G/H}).$$

It turns out that the kernel of this map is of extreme importance in the arithmetic of norm one tori, as we will see later on.

2.2. Arithmetic of algebraic tori

Let T be an algebraic k-torus. We introduce the *defect of weak approximation* for T

$$A(T) = (\prod_{v \in \Omega_k} T(k_v))/\overline{T(k)},$$

where $\overline{T(k)}$ denotes the closure (with respect to the product topology) of $T(k)$ in $\prod\limits_{v \in \Omega_k} T(k_v)$. We say that *weak approximation* holds for T if and only if $A(T) = 0$. We will also work with the Tate-Shafarevich group of T, defined as

$$Ш(T) = \ker(\mathrm{H}^1(k, T) \to \prod_{v \in \Omega_k} \mathrm{H}^1(k_v, T_{k_v})).$$

The following result remarkably connects weak approximation for T with the Hasse principle for principal homogeneous spaces under T by combining the two groups $A(T)$ and $Ш(T)$ into an exact sequence.

Theorem 2.1 *(Voskresenskiĭ). Let T be a torus defined over a number field k and let X/k be a smooth projective model of T. Then there exists an exact sequence*

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

Proof. See Theorem 6 of [27]. □

Remark 2.2. In the framework of the well-known *Brauer-Manin obstruction*, the birational invariant $\mathrm{H}^1(k, \operatorname{Pic} \overline{X})$ in the previous theorem can be identified with $\operatorname{Br} X / \operatorname{Br} k$, where $\operatorname{Br} X = \mathrm{H}^2_{\text{ét}}(X, \mathbb{G}_m)$ is the cohomological Brauer-Grothendieck group of X. Furthermore, work of Sansuc [24] implies that this obstruction is the only one to the Hasse principle and weak approximation for principal homogeneous spaces of T.

Let us now specialize T to be the norm one torus $R^1_{K/k}\mathbb{G}_m$ of an extension K/k of number fields, defined via the exact sequence of algebraic groups

$$1 \to T \to R_{K/k}\mathbb{G}_m \xrightarrow{N_{K/k}} \mathbb{G}_m \to 1.$$

Taking the $\mathrm{Gal}(\overline{k}/k)$-cohomology of this exact sequence, we obtain

$$K^* \xrightarrow{N_{K/k}} k^* \to \mathrm{H}^1(k, T) \to \mathrm{H}^1(k, R_{K/k}\mathbb{G}_m).$$

By Shapiro's lemma and Hilbert's Theorem 90, we have $\mathrm{H}^1(k, R_{K/k}\mathbb{G}_m) = \mathrm{H}^1(K, \mathbb{G}_m) = 1$. It follows that $\mathrm{H}^1(k, T) \cong k^*/N_{K/k}(K^*)$. Analogously, for every $v \in \Omega_k$ we have $\mathrm{H}^1(k_v, T_{k_v}) \cong k_v^*/\prod_{w|v} N_{K_w/k_v}(K_w^*)$, where the product runs over all places w of K above v. Hence, we conclude that

Please cite this article in press as: A. Macedo, The Hasse norm principle for A_n-extensions, J. Number Theory (2019), https://doi.org/10.1016/j.jnt.2019.10.020

$$\ker(\mathrm{H}^1(k,T) \to \prod_{v\in\Omega_k} \mathrm{H}^1(k_v, T_{k_v})) \cong (k^* \cap N_{K/k}(\mathbb{A}_K^*))/N_{K/k}(K^*),$$

i.e. the Tate-Shafarevich group $\text{Ш}(T)$ is isomorphic to the knot group $\mathfrak{K}(K/k)$.

The group $\mathrm{H}^1(k, \operatorname{Pic}\overline{X})$ in Theorem 2.1 is therefore pivotal in the study of the HNP for K/k and weak approximation for T. A very useful tool to deal with this cohomology group is flasque resolutions, as introduced in the work of Colliot-Thélène and Sansuc. We recall here the main definitions and refer the reader to [6] and [7] for more details on this topic.

Flasque resolutions

Let G be a finite group and let A be a G-module. The module A is said to be *flasque* if $\hat{\mathrm{H}}^{-1}(G', A) = 0$ for every subgroup G' of G and *coflasque* if $\mathrm{H}^1(G', A) = 0$ for every subgroup G' of G. We say that A is a *permutation* module if it admits a $\mathbb{Z}$-basis permuted by G. A *flasque resolution* of A is an exact sequence of G-modules

$$0 \to A \to P \to F \to 0$$

where P is a permutation module and F is flasque. Dually, a *coflasque resolution* of A is an exact sequence of G-modules

$$0 \to C \to Q \to A \to 0$$

where Q is a permutation module and C is coflasque. Two G-modules A_1 and A_2 are said to be *similar* if $A_1 \oplus P_1 \cong A_2 \oplus P_2$ for some permutation G-modules P_1, P_2. We denote the similarity class of A by $[A]$.

There is a very direct relation between the invariant $\mathrm{H}^1(k, \operatorname{Pic}\overline{X})$ and flasque resolutions of the G-module $\widehat{T}$, as the following result shows.

Theorem 2.3 *(Colliot-Thélène and Sansuc). Let T be a torus defined over a number field k and split by a finite Galois extension N/k with $G = \mathrm{Gal}(N/k)$. Let*

$$0 \to \widehat{T} \to P \to F \to 0$$

be a flasque resolution of the G-module $\widehat{T}$ and let X/k be a smooth projective model of T. Then the similarity class $[F]$ and the group $\mathrm{H}^1(G, F)$ are determined uniquely and

$$\mathrm{H}^1(k, \operatorname{Pic}\overline{X}) = \mathrm{H}^1(G, \operatorname{Pic} X_N) = \mathrm{H}^1(G, F).$$

Proof. See Lemme 5 and Proposition 6 of [6]. □

In [7], Colliot-Thélène and Sansuc further presented a very useful description of the group $\mathrm{H}^1(G, F)$ in the conclusion of the previous theorem.

Proposition 2.4. $\mathrm{H}^1(G, F) = \ker(\mathrm{H}^2(G, \widehat{T}) \xrightarrow{\mathrm{Res}} \prod_{g \in G} \mathrm{H}^2(\langle g \rangle, \widehat{T}))$.

Proof. See Proposition 9.5(ii) of [7]. □

3. Group cohomology of A_n-modules

The goal of this section is to prove Theorem 1.1 for $n \geq 8$. We start out by establishing several group-theoretic and cohomological facts about A_n-modules. We then exploit the consequences of these results in the arithmetic of norm one tori associated to A_n-extensions.

Recall that, for $n \geq 5$, A_n is a non-abelian simple group and hence perfect. Moreover, its Schur multiplier $M(A_n) = \hat{\mathrm{H}}^{-3}(A_n, \mathbb{Z})$ is given as follows (see Theorem 2.11 of [17]):

$$M(A_n) = \begin{cases} 0 & \text{if } n \leq 3; \\ \mathbb{Z}/2 & \text{if } n \in \{4, 5\} \text{ or } n \geq 8; \\ \mathbb{Z}/6 & \text{if } n \in \{6, 7\}. \end{cases}$$

Given a copy H of A_{n-1} inside $G = A_n$, we have a corestriction map on cohomology

$$\mathrm{Cor}_G^H : M(H) \to M(G).$$

This map will play an important role in the proof of Theorem 1.1, so we begin by establishing the following result.

Lemma 3.1. *Let $n \geq 8$ and let H be a copy of A_{n-1} inside $G = A_n$. Then the corestriction map Cor_G^H is surjective.*

In order to prove this lemma, we will use multiple results about covering groups of S_n and A_n together with the characterization of the image of Cor_G^H given in Lemma 4 of [8]. To put this plan into practice, we need the following concepts.

Definition 3.2. Let G be a finite group. A *stem extension* of G is a group $\widetilde{G}$ containing a normal subgroup K such that $\widetilde{G}/K \cong G$ and $K \subseteq Z(\widetilde{G}) \cap [\widetilde{G}, \widetilde{G}]$. A *Schur covering group* of G is a stem extension of G of maximal size.

It is a well-known fact that a stem extension of a finite group G always exists (see Theorem 2.1.4 of [19]). Additionally, the base normal subgroup K of a Schur covering group of G coincides with its Schur multiplier $\hat{\mathrm{H}}^{-3}(G, \mathbb{Z})$ (see Section 9.9 of [13]). In [25], Schur completely classified the Schur covering groups of S_n and A_n. He also gave an explicit presentation of a cover of S_n, as follows.

Proposition 3.3. *Let $n \geq 4$ and let U be the group with generators $z, t_1, \ldots, t_{n-1}$ and relations*

Please cite this article in press as: A. Macedo, The Hasse norm principle for A_n-extensions, J. Number Theory (2019), https://doi.org/10.1016/j.jnt.2019.10.020

(1) $z^2 = 1$;
(2) $zt_i = t_i z$, for $1 \le i \le n-1$;
(3) $t_i^2 = z$, for $1 \le i \le n-1$;
(4) $(t_i t_{i+1})^3 = z$, for $1 \le i \le n-2$;
(5) $t_i t_j = z t_j t_i$, for $|i-j| \ge 2$ and $1 \le i, j \le n-1$.

Then U is a Schur covering group of S_n with base normal subgroup $K = \langle z \rangle$. Moreover, if $\overline{t_i}$ denotes the transposition $(i, i+1)$ in S_n, then the map

$$\begin{aligned} \pi \colon U &\longrightarrow S_n \\ z &\longmapsto 1 \\ t_i &\longmapsto \overline{t_i} \end{aligned}$$

is surjective and has kernel K.

Proof. See Schur's original paper [25] or Chapter 2 of [17] for a more modern exposition. □

Remark 3.4. An immediate consequence of this last proposition is that the Schur multiplier $M(S_n)$ of S_n is isomorphic to $\mathbb{Z}/2$ for $n \ge 4$.

Using the Schur cover of S_n given in Proposition 3.3, one can also construct a Schur covering group of A_n for $n \ge 8$.

Lemma 3.5. *In the notation of Proposition 3.3, the group $V := \pi^{-1}(A_n)$ defines a Schur covering group of A_n for every $n \ge 8$.*

Proof. It is well-known that A_n is generated by the $n-2$ permutations $\overline{e_i} := \overline{t_1}.\overline{t_{i+1}} = (1,2)(i+1, i+2)$ for $1 \le i \le n-2$. Hence, $V = \pi^{-1}(A_n)$ is generated by $z, e_1, \dots, e_{n-2}$, where $e_i := t_1 t_{i+1}$ for $1 \le i \le n-2$. Clearly, we have $K \subseteq Z(V)$ and $V/K \cong A_n$. As the Schur multiplier of A_n is also $\mathbb{Z}/2$ for $n \ge 8$, in order to show that V defines a Schur covering group of A_n it suffices to prove that $K \subseteq [V, V]$.

Claim: $z = [e_1^{-1} e_2 e_1, e_2]$.

Proof of claim: This follows from a standard computation using the identities $(e_1 e_2)^3 = z$, $e_1^3 = z$ and $e_i^2 = z$ for $2 \le i \le n-2$, which result directly from the relations satisfied by t_i. From the claim, it follows that $K = \langle z \rangle$ is contained in $[V, V]$, as desired. □

Given a copy H of A_{n-1} inside A_n, one can subsequently repeat the same procedure of this last lemma and further restrict π to $W := \pi^{-1}(H)$ to seek a Schur covering group of H. The same argument works, but with two small caveats.

First, it is necessary to assure that we still have $z \in [W, W]$. This is indeed the case since, for $n \ge 7$, any subgroup $H \le A_n$ isomorphic to A_{n-1} is conjugate to the point stabilizer $(A_n)_n$ of the letter n in A_n (this is a consequence of Lemma 2.2 of [29]). Therefore, we have $H = {(A_n)_n}^{\pi(x)}$ for some $x \in U$ and hence $z = z^x = [e_1^{-1}e_2e_1, e_2]^x = [(e_1^{-1}e_2e_1)^x, e_2^x]$ is in $[W, W]$, as clearly $\overline{e_1}, \overline{e_2} \in (A_n)_n$.

Second, note that we are making use of the fact that the Schur multipliers of A_{n-1} and S_n coincide, which does not hold for $n = 8$ (recall that $M(A_7) = \mathbb{Z}/6$). However, it is still true that $\pi^{-1}(A_7)$ gives a (non-maximal) stem extension of A_7, by the same reasoning as above. We have thus established the following result.

Lemma 3.6. *Let $n \geq 8$ and let H be a copy of A_{n-1} inside A_n. Then the restriction to $W = \pi^{-1}(H)$ of the Schur cover V of A_n given in Lemma 3.5 defines a stem extension of H.*

We can now prove the surjectivity of Cor_G^H for $n \geq 8$.

Proof of Lemma 3.1. Let V be the Schur covering group of G constructed in Lemma 3.5. We then have a central extension

$$1 \to M(G) \to V \xrightarrow{\pi} G \to 1,$$

where we identified the base normal subgroup K of V with the Schur multiplier $M(G)$ of G. Since $M(G) \subset [V, V]$ by the definition of a Schur cover, V is a *generalized representation group* of G, as defined on p. 310 of [8]. Therefore, by Lemma 4 of [8] we have an isomorphism $\mathrm{Cor}_G^H(M(H)) \cong M(G) \cap [W, W]$, where $W = \pi^{-1}(H)$. Hence, it is enough to show that $M(G) \cap [W, W] = M(G)$. By Lemma 3.6, W defines a stem extension of H for $n \geq 8$, so that we immediately get $M(G) \subset [W, W]$. It follows that $M(G) \cap [W, W] = M(G)$, as desired. □

Using this lemma we show the vanishing of $\mathrm{H}^2(G, J_{G/H})$ and prove Theorem 1.1 for $n \geq 8$.

Proposition 3.7. *Let $n \geq 8$ and H be a copy of A_{n-1} inside $G = A_n$. Then $\mathrm{H}^2(G, J_{G/H}) = 0$.*

Proof. Taking the G-cohomology of the exact sequence (2.2) gives the exact sequence of abelian groups

$$\mathrm{H}^2(G, \mathbb{Z}[G/H]) \to \mathrm{H}^2(G, J_{G/H}) \to \mathrm{H}^3(G, \mathbb{Z}) \xrightarrow{\overline{\eta}} \mathrm{H}^3(G, \mathbb{Z}[G/H]),$$

where $\overline{\eta}$ is the map induced on the degree 3 cohomology groups by the norm map η. Applying Shapiro's lemma and using the fundamental duality theorem in the cohomology of finite groups (see, for example, Section VI.7 of [3]), we have $\mathrm{H}^2(G, \mathbb{Z}[G/H]) \cong \mathrm{H}^2(H, \mathbb{Z}) \cong \hat{\mathrm{H}}^{-2}(H, \mathbb{Z}) \cong H/[H, H] = 0$, as H is perfect. Therefore, this last exact sequence becomes

Please cite this article in press as: A. Macedo, The Hasse norm principle for A_n-extensions, J. Number Theory (2019), https://doi.org/10.1016/j.jnt.2019.10.020

$$0 \to \mathrm{H}^2(G, J_{G/H}) \to \mathrm{H}^3(G, \mathbb{Z}) \xrightarrow{\overline{\eta}} \mathrm{H}^3(G, \mathbb{Z}[G/H]),$$

which shows that $\mathrm{H}^2(G, J_{G/H}) = 0$ if $\overline{\eta}$ is injective. Since the composition of the map $\overline{\eta}$ with the isomorphism of Shapiro's lemma

$$\mathrm{H}^3(G, \mathbb{Z}) \xrightarrow{\overline{\eta}} \mathrm{H}^3(G, \mathbb{Z}[G/H]) \xrightarrow{\cong} \mathrm{H}^3(H, \mathbb{Z})$$

gives the restriction map (see Example 1.27(b) of [21]), it suffices to prove that the restriction

$$\mathrm{Res}^G_H : \mathrm{H}^3(G, \mathbb{Z}) \to \mathrm{H}^3(H, \mathbb{Z})$$

is injective. Again, by the duality in the cohomology of finite groups, this is the same as proving that the corestriction map (dual to Res^G_H)

$$\mathrm{Cor}^H_G : \hat{\mathrm{H}}^{-3}(H, \mathbb{Z}) \to \hat{\mathrm{H}}^{-3}(G, \mathbb{Z})$$

is surjective. But this is the content of Lemma 3.1 and so it follows that $\mathrm{H}^2(G, J_{G/H}) = 0$. □

Proof of Theorem 1.1 for $n \geq 8$. Set $G = \mathrm{Gal}(N/k) \cong A_n$, $H = \mathrm{Gal}(N/K)$ and observe that H is isomorphic to A_{n-1}, since it has index n in A_n. By Theorems 2.1 and 2.3 and Proposition 2.4, it is enough to establish that the group $\mathrm{H}^2(G, \widehat{T})$ is trivial, where $T = R^1_{K/k}\mathbb{G}_m$ is the norm one torus associated to the extension K/k. It is a well-known fact that $\widehat{T} \cong J_{G/H}$ as G-modules, so the result follows from Proposition 3.7. □

Remark 3.8. Note that in the proof of Proposition 3.7 we actually showed that

$$\mathrm{H}^2(G, J_{G/H}) \cong \ker(\mathrm{Res}^G_H : \mathrm{H}^3(G, \mathbb{Z}) \to \mathrm{H}^3(H, \mathbb{Z}))$$

for every $n \geq 6$. Using this fact and an approach similar to the one carried out in the proof of Lemma 3.1, one can show that $\mathrm{H}^2(G, J_{G/H}) = \mathbb{Z}/3$ when $n = 6$. Therefore the statement of Proposition 3.7 does not hold in this case and hence the proof of Theorem 1.1 for $n = 6$ requires a different strategy.

4. The case $n = 6$

In this section, we conclude the proof of Theorem 1.1 by using the computer algebra system GAP [10] to establish the remaining case $n = 6$. For this, we make use of the algorithms[1] developed by Hoshi and Yamasaki in [18]. In this work, the authors study

[1] The code for these algorithms is available in the web page: https://www.math.kyoto-u.ac.jp/~yamasaki/Algorithm/RatProbAlgTori/, accessed May, 2019.

the rationality of low-dimensional algebraic tori via the properties of the corresponding group modules, which they analyze using various computational methods. In particular, they create the following GAP algorithms:

- `Norm1TorusJ(d,m)` (Algorithm N1T in [18, Section 8]), computing the action of G on $J_{G/H}$, where G is the transitive subgroup of S_d with GAP index number m (cf. [5] and [10]) and H is the stabilizer of one of the letters in G;
- `FlabbyResolution(G)` (Algorithm F1 in [18, Section 5.1]), computing a flasque resolution of the G-lattice M_G (see [18, Definition 1.26]);
- `H1(G)` (Algorithm F0 in [18, Section 5.0]), computing the cohomology group $\mathrm{H}^1(G, M_G)$ of the G-lattice M_G.

Using these algorithms, we can easily prove the A_6 case of Theorem 1.1 as follows:

Proof of the case $n = 6$ of Theorem 1.1. Set $G = \mathrm{Gal}(N/k) \cong A_6$, $H = \mathrm{Gal}(N/K) \cong A_5$ and $T = R^1_{K/k}\mathbb{G}_m$. By Theorems 2.1 and 2.3, it is enough to prove that $\mathrm{H}^1(G, F) = 0$, where F is a flasque module in a flasque resolution of the G-module $\widehat{T} \cong J_{G/H}$. Writing $K = N^H = k(\alpha_1)$ and $N = k(\alpha_1, \dots, \alpha_6)$ for some $\alpha_i \in \overline{k}$, we see that H is the stabilizer of α_1 and so the above algorithm `Norm1TorusJ` to compute $J_{G/H}$ applies. Finally, observing that A_6 is the transitive subgroup of S_6 with GAP index number 15, one can conclude that the desired cohomology group is trivial by running the following code in GAP:

```
gap> Read("FlabbyResolution.gap");
gap> J:=Norm1TorusJ(6,15);
<matrix group with 2 generators>
gap> F:=FlabbyResolution(J).actionF;
<matrix group with 2 generators>
gap> Product(H1(F));
1
```
$\square$

Remark 4.1. The computation used for the case $n = 6$ in the previous proof can be reproduced for other small values of n. We have checked that for $n \leq 11$ the algorithm confirms our results, giving the trivial group for $n \neq 4$ and producing the counterexample $\mathrm{H}^1(A_4, F) = \mathbb{Z}/2$ for $n = 4$, as computed by Kunyavskiĭ in [20].

Although the primary goal of this section was to establish the case $n = 6$ of Theorem 1.1, the computer algorithms of Hoshi and Yamasaki employed here might be of independent interest. Indeed, this computational method can consistently be used to compute the birational invariant $\mathrm{H}^1(G, F)$ for low-degree field extensions and, in this way, deduce consequences about the validity of the Hasse norm principle and weak approximation for norm one tori.

Please cite this article in press as: A. Macedo, The Hasse norm principle for A_n-extensions, J. Number Theory (2019), https://doi.org/10.1016/j.jnt.2019.10.020

Acknowledgments

The author would like to warmly thank his supervisor, Rachel Newton, for suggesting this problem and for continuous encouragement and advice; Prof. Boris Kunyavskiĭ for bringing up the importance of Lemma 3.1; the anonymous referee for useful comments and suggestions that greatly improved the exposition of the paper. This work was completed as part of the author's PhD and was supported by the doctoral scholarship SFRH/BD/117955/2016 provided by the Foundation of Science and Technology (FCT) of Portugal.

References

[1] H.-J. Bartels, Zur Arithmetik von Konjugationsklassen in algebraischen Gruppen, J. Algebra 70 (1981) 179–199.
[2] H.-J. Bartels, Zur Arithmetik von Diedergruppenerweiterungen, Math. Ann. 256 (1981) 465–473.
[3] K. Brown, Cohomology of Groups, Graduate Texts in Mathematics, vol. 87, Springer-Verlag, 1982.
[4] T. Browning, R. Newton, The proportion of failures of the Hasse norm principle, Mathematika 62 (2016) 337–347.
[5] G. Butler, J. McKay, The transitive groups of degree up to eleven, Comm. Algebra 11 (1983) 863–911.
[6] J.-L. Colliot-Thélène, J.-J. Sansuc, La R-équivalence sur les tores, Ann. Sci. Éc. Norm. Supér. 10 (1977) 175–229.
[7] J.-L. Colliot-Thélène, J.-J. Sansuc, Principal homogeneous spaces under flasque tori: applications, J. Algebra 106 (1987) 148–205.
[8] Y.A. Drakokhrust, V.P. Platonov, The Hasse norm principle for algebraic number fields, Math. USSR, Izv. 29 (1987) 299–322.
[9] C. Frei, D. Loughran, R. Newton, The Hasse norm principle for abelian extensions, Amer. J. Math. 140 (6) (2018) 1639–1685.
[10] The GAP Group, GAP – Groups, Algorithms, and Programming, available at https://www.gap-system.org, Version 4.8.10, 2018. (Accessed May 2019).
[11] F. Gerth, The Hasse norm principle in metacyclic extensions of number fields, J. Lond. Math. Soc. (2) 16 (1977) 203–208.
[12] F. Gerth, The Hasse norm principle in cyclotomic number fields, J. Reine Angew. Math. 303/304 (1978) 249–252.
[13] K.W. Gruenberg, Cohomological Topics in Group Theory, Lecture Notes in Mathematics, vol. 143, Springer-Verlag, 1970.
[14] S. Gurak, On the Hasse norm principle, J. Reine Angew. Math. 299/300 (1978) 16–27.
[15] S. Gurak, The Hasse norm principle in non-abelian extensions, J. Reine Angew. Math. 303/304 (1978) 314–318.
[16] H. Hasse, Beweis eines Satzes und Wiederlegung einer Vermutung über das allgemeine Normenrestsymbol, Nachr. Ges. Wiss. Göttingen Math.-Phys. Kl. (1931) 64–69.
[17] P.N. Hoffman, J.F. Humphreys, Projective Representations of the Symmetric Groups, Oxford Mathematical Monographs, Clarendon Press, Oxford, 1992.
[18] A. Hoshi, A. Yamasaki, Rationality problem for algebraic tori, Mem. Amer. Math. Soc. 248 (1176) (2017).
[19] G. Karpilovsky, The Schur Multiplier, Clarendon Press, Oxford, 1987.
[20] B. Kunyavskiĭ, Arithmetic properties of three-dimensional algebraic tori, Zap. Nauchn. Sem. S.-Peterburg. Otdel. Mat. Inst. Steklov. (POMI) 16 (1982) 102–107.
[21] J.S. Milne, Class Field Theory, available at http://www.jmilne.org/math/CourseNotes/CFT.pdf, Version 4.02, 2013. (Accessed May 2019).
[22] M.J. Razar, Central and genus class fields and the Hasse norm theorem, Compos. Math. 35 (1977) 281–298.
[23] N. Rome, The Hasse norm principle for biquadratic extensions, J. Théor. Nombres Bordeaux 30 (3) (2018) 947–964.

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

[25] J. Schur, Über die Darstellung der symmetrischen und der alternierenden Gruppe durch gebrochene lineare Substitutionen, J. Reine Angew. Math. 139 (1911) 155–250.

[26] J.T. Tate, Global class field theory, in: J.W.S. Cassels, A. Fröhlich (Eds.), Algebraic Number Theory, Academic Press, London, 1967, pp. 162–203.

[27] V. Voskresenskiĭ, Birational properties of linear algebraic groups, Izv. Ross. Akad. Nauk Ser. Mat. 34 (1970) 3–19, English translation: Math. USSR, Izv. 4 (1970) 1–17.

[28] V. Voskresenskiĭ, B. Kunyavskiĭ, Maximal tori in semisimple algebraic groups, Manuscript deposited at VINITI 15.03.84, no. 1269-84, 28pp. (in Russian).

[29] R.A. Wilson, The Finite Simple Groups, Graduate Texts in Mathematics, vol. 251, Springer-Verlag, 2009.

Please cite this article in press as: A. Macedo, The Hasse norm principle for A_n-extensions, J. Number Theory (2019), https://doi.org/10.1016/j.jnt.2019.10.020