THE HASSE NORM PRINCIPLE FOR $A_n$-EXTENSIONS

ANDRÉ MACEDO

Abstract. 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 $F$ such that $\text{Gal}(F/k) \cong A_n$. 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 $A_K^*$ and $A_k^*$ and let $N_{K/k} : A_K^* \to A_k^*$ be the norm map on the idèles. We can view $K^*$ (respectively, $k^*$) as sitting inside $A_K^*$ (respectively, $A_k^*$) via the diagonal embedding and $N_{K/k}$ 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

$$\mathfrak{R}(K/k) := (k^* \cap N_{K/k}(A_K^*)) / N_{K/k}(K^*)$$

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 1931 by Hasse, who proved that the knot group $\mathfrak{R}(K/k)$ is trivial if $K/k$ is a cyclic extension (the Hasse norm theorem). Since then, much work has been done in the abelian case (see, for instance, [7], [9] or [12]), but results for the non-abelian and non-Galois cases are still limited. For example, if $F$ denotes the normal closure of $K/k$, it is known that the HNP holds for $K/k$ when

- $[K : k]$ is prime ([1]);
- $[K : k] = n$ and $\text{Gal}(F/k) \cong D_n$, the dihedral group of order $2n$ ([2]);
- $[K : k] = n$ and $\text{Gal}(F/k) \cong S_n$, the symmetric group on $n$ letters ([20]).

In this paper, we study the HNP for a degree $n$ extension $K/k$ with normal closure $F$ such that $\text{Gal}(F/k)$ 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 $k$ with respect to $v$. In particular, we examine weak approximation for the norm one torus $T = R^1_{K/k}G_m$ associated to a degree $n$ extension of number fields $K/k$ with $A_n$-normal closure.

The first non-trivial case is $n = 3$. In this case, $K = F$ is a Galois extension of $k$ and the Hasse norm theorem tells us that the HNP holds for $K/k$. Moreover, using a result of Voskresenskiĭ, one can show that weak approximation holds for

2010 Mathematics Subject Classification. 14G05 (primary), 11E72, 11R37, 20D06 (secondary).
the associated norm one torus. In [15] Kunyavski˘ı solved the case \( n = 4 \) by showing that, for a quartic extension \( K/k \) 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 \( T \). In this paper, we use several cohomological results about \( A_n \)-modules to prove the following theorem.

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

The layout of this paper is as follows. In Section 2, we use various cohomological and group-theoretic tools to establish the injectivity of an important restriction map on the cohomology of \( A_n \). In Section 3, we look at the consequences of these results in the arithmetic of number fields. In particular, combining the results of Section 2 with the work of Colliot-Thélène and Sansuc on flasque resolutions and a theorem of Voskresenski˘ı, we prove Theorem 1.1 for \( n \neq 6 \). In Section 4, we exploit a computational method developed by Hoshi and Yamasaki to solve the remaining case \( n = 6 \). All of the code used in Section 4 is provided in the Appendix.

**Notation.** Throughout this paper, we fix the following notation.

- \( k \) a number field;
- \( \overline{k} \) an algebraic closure of \( k \);
- \( v \) a place of \( k \);
- \( k_v \) the completion of \( k \) at \( v \).

For a variety \( X \) over a field \( K \), we use the notation

\[
X_L = X \times_K L \quad \text{the base change of} \ X \ \text{to a field extension} \ L/K;
\]

\[
\overline{X} = X \times_K \overline{K} \quad \text{the base change of} \ X \ \text{to an algebraic closure of} \ K;
\]

\[
\text{Pic} X \quad \text{the Picard group of} \ X.
\]

We define \( \mathbb{G}_{m,K} = \text{Spec}(K[t, t^{-1}]) \) 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 \( \mathbb{G}_m \). Given a \( K \)-torus \( T \), we write \( \hat{T} \) for its character group \( \text{Hom}(T, \mathbb{G}_m) \).

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 \( R_{L/K}^1 \mathbb{G}_m \) 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 \( \hat{H}^q(G, A) \) and the kernel of the restriction map \( \hat{H}^q(G, A) \xrightarrow{\text{Res}} \prod_{g \in G} \hat{H}^q((g), A) \) by \( \mathfrak{H}_q^G(A) \). Since \( \hat{H}^0(G, A) = H^0(G, A) \) for \( q \geq 1 \), we will omit the hat in this case. We also use the notation \( \text{Z}(G), [G, G], G^\sim \) and \( M(G) \) for the center, the derived subgroup, the dual group \( \text{Hom}(G, \mathbb{Q}/\mathbb{Z}) \) and the Schur multiplier \( \hat{H}^{-3}(G, \mathbb{Z}) \) of \( G \), respectively. Given elements \( g, h \in G \), we use the conventions \( [g, h] = ghg^{-1}h^{-1} \) and \( g^h = hgh^{-1} \).
Acknowledgements. I would like to thank my supervisor Rachel Newton for suggesting this problem and for helpful comments on an earlier version of this manuscript. I am also grateful to Prof. Boris Kunyavski˘ı for bringing up the importance of Lemma [2.2]. This work was supported by the FCT doctoral scholarship SFRH/BD/117955/2016.

2. Group cohomology of $A_n$-modules

The goal of this section is to establish several cohomological facts about $A_n$-modules. We start by stating some useful group-theoretic facts.

Remark 2.1. Recall that, for $n \geq 5$, $A_n$ is a non-abelian simple group and hence perfect. Moreover, its Schur multiplier $M(A_n) = \hat{H}^{-3}(A_n, \mathbb{Z})$ is given as follows (see Theorem 2.11 of [11]):

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

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

$$\text{Cor}^H_G : M(H) \to M(G).$$

This map will play an important role for us later, so we begin by establishing the following result.

Lemma 2.2. Let $n \geq 8$ and let $H$ be a copy of $A_{n-1}$ inside $G = A_n$. Then, the corestriction map $\text{Cor}^H_G$ 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 $\text{Cor}^H_G$ given in Lemma 4 of [6]. To put this plan into practice, we need the following concepts.

Definition 2.3. 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 [14]). Additionally, the base normal subgroup $K$ of a Schur covering group $\widetilde{G}$ of $G$ coincides with its Schur multiplier $\hat{H}^{-3}(G, \mathbb{Z})$ (see Section 9.9 of [10]). In [15], 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 2.4. Let $n \geq 4$ and let $U$ be the group with generators $z, t_1, \ldots, t_{n-1}$ and relations

1. $z^2 = 1$;
2. $zt_i = t_iz$, for $1 \leq i \leq n - 1$;
3. $t_i^2 = z$, for $1 \leq i \leq n - 1$;
4. $(t_i^3 + 1)^3 = z$, for $1 \leq i \leq n - 2$;
5. $t_it_j = zt_jt_i$, for $|i - j| \geq 2$ and $1 \leq i, j \leq n - 1$. 


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

$$
\pi : U \to S_n
$$

$$
z \mapsto 1
$$

$$
t_i \mapsto \Gamma_{i}
$$

is surjective and has kernel $K$.

Proof. See Schur’s original paper [18] or Chapter 2 of [11] for a more modern exposition.

Remark 2.5. An immediate consequence of this last proposition is that the Schur multiplier of $S_n$ is isomorphic to $\mathbb{Z}/2$ for $n \geq 4$.

Using the Schur cover of $S_n$ given in Proposition 2.4, one can also construct a Schur covering group of $A_n$ for $n \geq 8$.

Lemma 2.6. In the notation of Proposition 2.4, the group $V := \pi^{-1}(A_n)$ defines a Schur covering group of $A_n$ for every $n \geq 8$.

Proof. It is well-known that $A_n$ is generated by the $n-2$ permutations $\Gamma_i := \Gamma_1\Gamma_{i+1} = (1\ 2)(i+1\ i+2)$ for $1 \leq i \leq n-2$. Hence, $V = \pi^{-1}(A_n)$ is generated by $z, e_1, \ldots, e_{n-2}$, where $e_i := t_it_{i+1}$ for $1 \leq i \leq n-2$. 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 $n \geq 8$, in order to show that $V$ defines a Schur covering group of $A_n$, it suffices to prove that $K \subseteq [V, V]$.

Claim: $z = [e_1^{-1}e_2^3, e_2]$. 

Proof of claim: This follows from a standard computation using the identities $(e_1e_2)^3 = z$, $e_1^3 = z$ and $e_2^2 = z$ for $2 \leq i \leq n-2$, which follow directly from the relations satisfied by the $t_i$.

Given 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 $\pi$ 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 $n \geq 7$, any subgroup $H \leq A_n$ 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 [21]). 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 $e_1, e_2 \in (A_n)_n$.

Second, note that we are making use of the fact that the Schur multipliers of $A_{n-1}$ and $S_n$ coincide, which is only true for $n \geq 9$ (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 2.7. 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 2.6 defines a stem extension of $H$.

We can now prove Lemma 2.2.

Proof of Lemma 2.2. Let $V$ be the Schur covering group of $G$ constructed in Lemma 2.6. 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 [6]. Therefore, by Lemma 4 of [6], we have an isomorphism $\text{Cor}_{H}^{H}(M(H)) \cong M(G) \cap [W, W]$, where $W = \pi^{-1}(H)$. Hence, it is enough to show that $M(G) \cap [W, W] = M(G)$. By Lemma 2.7, $W$ 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. □

In order to proceed with our cohomological analysis, we need to recollect some group-theoretic objects. Let $H$ be a subgroup of a finite group $G$. Recall that we have the augmentation map $\epsilon : \mathbb{Z}[G/H] \to \mathbb{Z}$ defined by $\epsilon : Hg \mapsto 1$ for any $Hg \in G/H$. This map produces the exact sequence of $G$-modules

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

where $I_{G/H} = \ker(\epsilon)$ is the augmentation ideal. Dually, we also have a 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

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

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

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

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

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

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

It turns out that the kernel of this map (denoted by $\Pi H^2(G, J_{G/H})$) is of extreme importance in the arithmetic of number fields, as we will see in the next section. We describe this kernel for our case of interest $G = A_n$, $H \cong A_{n-1}$ and $n \geq 8$ (the cases $n \leq 7$ will be treated separately).
Proposition 2.8. Let $n \geq 8$ and let $H$ be a copy of $A_{n-1}$ inside $G = A_n$. Then, we have $\III^2_\omega(G, J_{G/H}) = 0$.

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

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

where $\overline{\eta}$ is the map induced on the degree 3 cohomology groups by the norm map $\eta$. 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 $H^2(G, \mathbb{Z}[G/H]) \cong H^2(H, \mathbb{Z}) \cong \hat{H}^{-2}(H, \mathbb{Z}) \cong H/[H, H] = 0$, as $H$ is perfect. Therefore, this last exact sequence becomes

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

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

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

gives the restriction map (see Example 1.27(b) of [16]), it is enough to prove that the restriction

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

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

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

is surjective. But this is the content of Lemma 2.2, so it follows that $H^2(G, J_{G/H})$ is trivial and therefore $\III^2_\omega(G, J_{G/H}) = 0$, as desired. 

\[ \square \]

3. Arithmetic consequences

In this section, we delve into the consequences of the cohomological results of Section 2 in the arithmetic of number fields. In particular, we will recall how the group $\III^2_\omega(G, J_{G/H})$ governs two important local-global principles, the Hasse norm principle and weak approximation. Specifying to the case $G = A_n$, $H \cong A_{n-1}$ and using Proposition 2.8, we will prove Theorem 1.1 for $n \geq 8$. The remaining cases ($n \leq 7$) will be solved using a result of Colliot-Thélène and Sansuc and a computational method adapted from work of Hoshi and Yamasaki.

Let $k$ be a number field and let $T$ be a $k$-torus. We introduce the defect to weak approximation for $T$

$$A(T) = \left( \prod_v T(k_v) \right) / T(k),$$

where the product is taken over all places \( v \) of \( k \) and \( \overline{T(k)} \) denotes the closure (with respect to the product topology) of \( T(k) \) in \( \prod_v T(k_v) \). We say that weak approximation holds for \( T \) if and only if \( A(T) = 0 \).

We also define the Tate-Shafarevich group of \( T \) as

\[
X(T) = \ker(H^1(k, T) \to \prod_v H^1(k_v, T_{k_v}))
\]

where the product runs over all places \( v \) of \( k \). It is known that this group controls the validity of the Hasse principle for every principal homogeneous space under \( T \). In fact, the Hasse principle holds for every such space if and only if \( X(T) = 0 \).

The following result remarkably connects weak approximation with the Hasse principle by combining the two groups \( A(T) \) and \( X(T) \) in an exact sequence.

**Theorem 3.1** (Voskresenski˘ı). 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

\[
0 \to A(T) \to H^1(k, \text{Pic } \overline{X}) \to X(T) \to 0.
\]

**Proof.** See Theorem 6 of [19]. \( \square \)

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. In this case, we have \( \mathfrak{H}(K/k) \cong \Pi(T) \) (see p. 307 of [17]). Therefore, the cohomology group \( H^1(k, \text{Pic } \overline{X}) \) in the previous theorem is pivotal in the study of the HNP for \( K/k \) and weak approximation for \( T \). A very useful tool to deal with this object is flasque resolutions, as introduced in the work of Colliot-Thélène and Sansuc. We recall here the main definitions and refer the reader to [4] and [5] 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 \( \check{H}^{-1}(G', A) = 0 \) for every subgroup \( G' \) of \( G \) and coflasque if \( H^1(G', A) = 0 \) for every subgroup \( G' \) of \( G \). Moreover, \( A \) is called a permutation module if it admits a \( \mathbb{Z} \)-basis permuted by \( G \) and an invertible module if it is a direct summand of a permutation module. A flasque resolution of \( A \) is an exact sequence of \( G \)-modules

\[
0 \to A \to P \to M \to 0
\]

where \( P \) is a permutation module and \( M \) is flasque. Dually, a coflasque resolution of \( A \) is an exact sequence of \( G \)-modules

\[
0 \to N \to Q \to A \to 0
\]

where \( Q \) is a permutation module and \( N \) is coflasque.

It turns out that there is a very direct relation between the group \( H^1(k, \text{Pic } \overline{X}) \) and flasque resolutions of the \( G \)-module \( \check{T} \), as the following result shows.
Theorem 3.2 (Colliot-Thélène & Sansuc). Let $T$ be a torus defined over a number field $k$ and split by a finite Galois extension $F/k$ with $G = \text{Gal}(F/k)$. Suppose that

$$0 \to \hat{T} \to P \to M \to 0$$

is a flasque resolution of the $G$-module $\hat{T}$ and let $X/k$ be a smooth projective model of $T$. Then, we have

$$H^1(k, \text{Pic} X) = H^1(G, \text{Pic} X_F) = H^1(G, M).$$

Proof. See Lemme 5 and Proposition 6 of [4]. □

We proceed by presenting a very useful description of the group $H^1(G, M)$ in the conclusion of the previous theorem.

Proposition 3.3. $H^1(G, M) = \text{III}_2^2(G, \hat{T})$.

Proof. See Proposition 9.5(ii) of [5]. □

Using this characterization, we can now prove Theorem 1.1 for $n \neq 6$ (the case $n = 6$ will be treated separately in the next section).

Proof of Theorem 1.1 for $n \neq 6$. Set $G = \text{Gal}(F/k) \cong A_n$ and $H = \text{Gal}(F/K)$. Observe that such a group $H$ is necessarily isomorphic to $A_{n-1}$, since it has index $n$ in $A_n$. We have two cases:

Case $n \geq 8$: By Theorems 3.1 and 3.2 and Proposition 3.3 it is enough to establish that the group $\text{III}_2^2(G, \hat{T})$ is trivial, where $\hat{T} = R_{K/k}^{1}G_m$ is the norm one torus associated to the extension $K/k$. Moreover, it is a well-known fact that $\hat{T} = J_{G/H}$ as $G$-modules, so it is sufficient to prove that $\text{III}_2^2(G, J_{G/H}) = 0$. But this was shown in Proposition 2.8 of Section 2, so the result follows.

Cases $n = 5$ and $n = 7$: Since $n$ is a prime number, these cases follow from a direct application of Proposition 9.1 of [3]. In this proposition, the authors show that there exists a $k$-torus $T_1$ such that the variety $T \times_k T_1$ is $k$-rational, where $T = R_{K/k}^{1}G_m$ is the norm one torus associated to $K/k$. This result is in its turn equivalent to the fact that any flasque module $M$ in a flasque resolution of $\hat{T}$ is invertible (see Proposition 9.5(i) of [5]), which is a stronger property than being coflasque. Therefore, the group $H^1(G, M)$ vanishes and so, by Theorem 3.2 the middle group of Voskresenskii's exact sequence in Theorem 3.1 is trivial. Hence, we conclude that $A(T) = 0 = \text{III}(T)$, as desired. □

4. The case $n = 6$

In this section, we finish the proof of Theorem 1.1 by using the computer algebra system GAP to establish the remaining case $n = 6$. More precisely, we devise an algorithm that, given a finite group $G$ and a non-normal subgroup $H$ such that $\text{Core}_G(H) := \bigcap_{g \in G} g^{-1}Hg$ is trivial (for example, this is always the case
if \( G \) is simple), outputs the invariant \( H^1(G, M) \) of Theorem 3.2 for the norm one torus. We use two ingredients to achieve this: First, we construct a routine in GAP that computes the matrix representation of the action of \( G \) on the Chevalley module \( J_{G/H} \). Second, we make use of the GAP algorithms developed by Hoshi and Yamasaki in [13] to construct flasque resolutions. Before we present our method, we need a few preliminaries.

**Definition 4.1** (Definition 1.26 of [13]). Let \( G \) be a finite subgroup of \( \text{GL}(n, \mathbb{Z}) \). The \( G \)-lattice \( M \) is defined to be the \( G \)-lattice with a \( \mathbb{Z} \)-basis \( \{u_1, \ldots, u_n\} \) and right action of \( G \) given by \( u_i.g = \sum_{j=1}^{n} a_{i,j} u_j \), where \( g = [a_{i,j}]_{i,j=1}^{n} \in G \).

In [13] the authors study the rationality of low-dimensional algebraic tori via the properties of the corresponding group modules, for which they create multiple algorithms. In particular, given a finite subgroup \( G \) of \( \text{GL}(n, \mathbb{Z}) \), they design the functions \( H^1 \) and \( \text{FlabbyResolution} \) (see Sections 5.0 and 5.1 of [13], respectively) computing the cohomology group \( H^1(G, M) \) and producing a flasque resolution of the \( G \)-module \( M \), respectively. For instance, by invoking the command
\[
gap> \text{FlabbyResolution}(G).\text{actionF};
\]
in GAP, one can access the matrix representation of the action of \( G \) on a flasque module in a flasque resolution of \( M \).

Let \( G \) be a finite group and \( H \) a non-normal subgroup of \( G \) with trivial normal core \( \text{Core}_{G}(H) \). Set \( d = |G/H| \) and fix a set of right-coset representatives \( L = \{Hg_1, \ldots, Hg_d\} \) of \( H \) in \( G \). In this way, we have \( \mathbb{Z}[G/H] = \sum_{i=1}^{d} Hg_i \mathbb{Z} \) and \( N_{G/H} = \sum_{i=1}^{d} Hg_i \in \mathbb{Z}[G/H] \).

Our first goal is to establish an isomorphism between the \( G \)-module \( J_{G/H} \) and the \( R_G \)-module \( M_{R_G} \), where \( R_G \leq \text{GL}(d-1, \mathbb{Z}) \) is a group (to be defined below) isomorphic to \( G \). We accomplish this by using the representation of \( G \) associated to its right action on \( J_{G/H} \). More precisely, consider the \( \mathbb{Z} \)-basis
\[
B = \{Hg_1 + N_{G/H} \mathbb{Z}, \ldots, Hg_{d-1} + N_{G/H} \mathbb{Z}\}
\]
of \( J_{G/H} \). Since the submodule \( N_{G/H} \mathbb{Z} \) is fixed by the action of any element of \( G \), we will omit it when working with elements of \( B \). Given \( g \in G \), we build a matrix \( R_g \in \text{GL}(d-1, \mathbb{Z}) \) as follows.

For any \( Hg_i \in B \), we have \( (Hg_i).g = Hg_{\sigma(i)} \) for some \( 1 \leq \sigma(i) \leq d \). There are two cases:

1) If \( \sigma(i) < d \), then the \( k \)-th entry of the \( i \)-th row of \( R_g \) is set to be equal to 1 if \( k = \sigma(i) \) and 0 otherwise.

2) If \( \sigma(i) = d \), then the \( k \)-th entry of the \( i \)-th row of \( R_g \) is set to be equal to \(-1 \) for every \( k \).

1The code for these algorithms is available on the web page [https://www.math.kyoto-u.ac.jp/~yamasaki/Algorithm/RatProbAlgTori/](https://www.math.kyoto-u.ac.jp/~yamasaki/Algorithm/RatProbAlgTori/).
Let $R_G$ be the group $\langle R_g \mid g \in G \rangle \leq \text{GL}(d-1, \mathbb{Z})$. It is easy to see that the map 

$$\rho_G : G \rightarrow R_G$$

$$g \mapsto R_g$$

is the representation of $G$ corresponding to its action on $J_{G/H}$. Clearly we have $\ker \rho_G = \text{Core}_G(H)$, which we are assuming is trivial. Hence, $\rho_G$ is faithful and thus it yields an isomorphism $G \cong R_G$. Moreover, identifying $R_g \in R_G$ with the corresponding element $g \in G$, it is straightforward to check that the map

$$\psi : M_{R_G} \rightarrow J_{G/H}$$

$$\sum_{i=1}^{d-1} \lambda_i u_i \mapsto \sum_{i=1}^{d-1} \lambda_i Hg_i + N_{G/H} \mathbb{Z}$$

defines an isomorphism of group modules.

With the tools introduced so far, we are now able to construct the function \texttt{FlasqCoho}(G,H) (presented in the Appendix) in GAP that computes the cohomology group $H^1(G,M)$, where $M$ is a flasque module in a flasque resolution of the Chevalley module $J_{G/H}$. The necessary steps to assemble this function are the following.

**Step 1)** Fix a set \texttt{gens} of generators of $G$ and construct the matrix group $R_G = \langle R_g \mid g \in \text{gens} \rangle$ using the following two functions

- \texttt{row(s,d)} (an auxiliary routine to \texttt{action}), returning the $i$-th row of the matrix $R_g$ as explained on page 9;
- \texttt{action}(G,H), constructing the matrices $R_g$ for $g \in \text{gens}$ and returning the group $R_G$.

The code for these two functions is also provided in the Appendix. The group $R_G = \text{action}(G,H)$ is then a subgroup of $\text{GL}(d-1, \mathbb{Z})$ isomorphic to $G$ such that $M_{R_G} \cong J_{G/H}$.

**Step 2)** Create a flasque resolution of the $R_G$-module $M_{R_G}$ and access its flasque module $M'$ using the commands

```gap
gap> FR:=FlabbyResolution(RG);
gap> FM:=FR.actionF;
```

The object \texttt{FM} is the matrix representation group of the action of $R_G$ on $M'$. Note that, by the inflation-restriction exact sequence, we have $H^1(R_G,M') \cong H^1(\text{FM},M_{\text{FM}})$.

**Step 3)** Obtain the group $H^1(\text{FM},M_{\text{FM}}) \cong H^1(G,M)$ using the function \texttt{H1}.

```gap
gap> H1(FM);
```

The result of this line is the final output of the algorithm.
Using this computational method, we can now establish the remaining case of Theorem 1.1.

Proof of the case $n = 6$ in Theorem 1.1. Set $G = \text{Gal}(F/k) \cong A_6$ and $H = \text{Gal}(F/K)$. By Theorems 3.1 and 3.2, it is enough to prove that the cohomology group $H^1(G, M)$ is trivial, where $M$ is a flasque module in a flasque resolution of the $G$-module $\hat{T} = J_{G/H}$ and $T = R^1_{K/k} \mathbb{G}_m$ is the norm one torus associated to the extension $K/k$.

As in the case $n \neq 6$, we have $H \cong A_5$. Notice that, up to conjugation, there are exactly two distinct subgroups of $A_6$ isomorphic to $A_5$, namely $H_1 = \langle (1 \ 2 \ 3 \ 4 \ 5), (1 \ 2 \ 3) \rangle$ and $H_2 = \langle (1 \ 2 \ 3 \ 4 \ 5), (1 \ 4)(5 \ 6) \rangle$. Moreover, it suffices to check the vanishing of $H^1(G, M)$ for one subgroup $H$ in each conjugacy class (this follows from the fact that two subgroups $H_1$ and $H_2$ are conjugate if and only if the two $G$-sets $G/H_1$ and $G/H_2$ are isomorphic). Using the above algorithm, we obtained $H^1(G, M) = 0$ in both cases, as desired.

\begin{remark}
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 $H^1(A_4, M) = \mathbb{Z}/2$ for $n = 4$, as computed by Kunyavskii in [15].

The authors of [13] also pay special attention to the case $n = 5$ (see Example 8.1 of [13]). In this case, they establish that the torus $T = R^1_{K/k} \mathbb{G}_m$ is stably $k$-rational (see Corollary 1.11 of [13]), i.e. that there exists $n \in \mathbb{N}$ such that $T \times_k \mathbb{G}_m^n$ is $k$-rational. In the language of group modules, this is equivalent to any flasque module $M$ in a flasque resolution of $\hat{T}$ being a permutation module, which is a stronger property than being coflasque.

The computational method developed in this section might be of independent interest, as it can often be used to compute the birational invariant $H^1(G, M)$ for low-degree field extensions and, in this way, deduce consequences about the groups $A(T)$ and $\mathcal{R}(K/k)$.
Appendix

Remark 4.3. The code for all the functions below can also be found at [https://sites.google.com/view/andre-macedo/code](https://sites.google.com/view/andre-macedo/code). Additionally, in order to successfully run the function `FlasqCoho`, the user will need the GAP programs for the functions `ConjugacyClassesSubgroups2`, `H1` and `FlabbyResolution` (see Sections 4.1, 5.0 and 5.1 of [13], respectively).

```plaintext
row:=function(s,d)
    local r,k;
    r:=[];  // i-th row of \( R_g \)
    if s = d then  // Case 2 of page 9
        r:=List([1..d−1],x−>−1);
    else
        for k in [1..d−1] do
            if k = s then
                r:=Concatenation(r,1);
            else
                r:=Concatenation(r,0);
            fi;
        od;
    fi;
    return r;
end;
```

```plaintext
action:=function(G,H)
    local d,gens,RT,L,S,j,Rg,i,s;
    d:=Order(G)/Order(H);
    gens:=GeneratorsOfGroup(G);
    RT:=RightTransversal(G,H);
    L:=List(RT,i−>CanonicalRightCosetElement(H,i));  // List of right-coset representatives of \( H \) in \( G \)
    S:=[[]];  // List of matrices \( R_g \) for \( g \in \text{gens} \)
    for j in [1..Size(gens)] do
        Rg:=List([1..d−1],x−>0);  // Create a matrix with \( d−1 \) lines
        for i in [1..d−1] do
            s:=PositionCanonical(RT,L[i]∗gens[j]);  // Obtain the index \( s = \sigma(i) \) of the right-coset \( (H ∗ L[i]) \cdot \text{gens}[j] \) in \( RT \) as explained on page 9
            Rg[i]:=row(s,d);  // Produce the \( i \)-th row of \( R_{\text{gens}[j]} \)
        od;
        S:=Concatenation(S,[Rg]);  // Append the matrix \( R_{\text{gens}[j]} \) to \( S \)
    od;
    return GroupByGenerators(S);  // Return the group \( R_G \)
end;
```
FlasqCoho:=function(G,H)
    local RG,FR,FM;
    RG:=action(G,H); // Matrix group \( R_G \)
    FR:=FlabbyResolution(RG); // Flasque resolution of \( R_G \)
    FM:=FR.actionF; // Flasque module in FR
    return H1(FM); // Return the cohomology group \( H^1(G,M) \)
end;

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 87, Springer-Verlag, 1982.
[4] J.-L. Colliot-Thélène, J.-J. Sansuc, La R-équivalence sur les tores. Ann. Sc. E.N.S. 10 (1977), 175–229.
[5] J.-L. Colliot-Thélène, J.-J. Sansuc, Principal homogeneous spaces under flasque tori: Applications, J. Algebra 106 (1987), 148–205.
[6] Y. A. Drakokhrust, V. P. Platonov, The Hasse norm principle for algebraic number fields, Math. USSR-Izv. 29 (1987), 299-322.
[7] C. Frei, D. Loughran, R. Newton, The Hasse norm principle for abelian extensions, Amer. J. Math, to appear.
[8] The GAP Group, GAP – Groups, Algorithms, and Programming, Version 4.8.10 (2018), available at https://www.gap-system.org
[9] F. Gerth, The Hasse norm principle for abelian extensions of number fields, Bulletin of the AMS, Vol. 83 (1977), 264-266.
[10] K. W. Gruenberg, Cohomological Topics in Group Theory, Lecture Notes in Mathematics 143, Springer-Verlag, 1970.
[11] P. N. Hoffman, J. F. Humphreys, Projective representations of the symmetric groups, Oxford Mathematical Monographs, Clarendon Press, Oxford, 1992.
[12] M. Horie, The Hasse norm principle for elementary abelian extensions, Proc. Amer. Math. Soc. 118(1) (1993), 47–56.
[13] A. Hoshi, A. Yamasaki, Rationality problem for algebraic tori, Memoirs of the American Mathematical Society 248 (2017), no. 1176.
[14] G. Karpilovsky, The Schur Multiplier, Clarendon Press, Oxford, 1987.
[15] B. Kunyavskiĭ, Arithmetic properties of three-dimensional algebraic tori, Zap. Nauch. Sem. LOMI Akad. Nauk SSSR 16 (1982), 102-107.
[16] J. S. Milne, Class Field Theory, Version 4.02 (2013), available at http://www.jmilne.org/math/CourseNotes/CFT.pdf
[17] V. Platonov, A. Rapinchuk, Algebraic groups and number theory, Pure and Applied Mathematics, 139, Academic Press, Inc., Boston, MA, 1994.
[18] J. Schur, Über die Darstellung der symmetrischen und der alternierenden Gruppe durch gebrochene lineare Substitutionen, J. reine angew. Math. 139 (1911), 155–250.
[19] V. Voskresenskiĭ, Birational properties of linear algebraic groups, Izv. Akad. Nauk SSSR Ser. Mat. 34 (1970) 3–19. English translation: Math. USSR-Izv. Vol. 4 (1970), 1-17.
[20] V. Voskresenskiĭ, B. Kunyavskiĭ, Maximal tori in semisimple algebraic groups, Manuscript deposited at VINITI 15.03.84, no. 1269-84, 28pp. (in Russian).
[21] R. A. Wilson, The finite simple groups, Graduate Texts in Mathematics 251, Springer-Verlag, 2009.
ANDRÉ MACEDO

ANDRÉ MACEDO, DEPARTMENT OF MATHEMATICS AND STATISTICS, UNIVERSITY OF READING, WHITEKNIGHTS, PO BOX 220, READING RG6 6AX, UK

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