EXPLICIT METHODS FOR THE HASSE NORM PRINCIPLE AND APPLICATIONS TO $A_n$ AND $S_n$ EXTENSIONS

ANDRÉ MACEDO AND RACHEL NEWTON

Abstract. Let $K/k$ be an extension of number fields. We describe theoretical results and computational methods for calculating the obstruction to the Hasse norm principle for $K/k$ and the defect of weak approximation for the norm one torus $R^*_K \mathbb{G}_m$. We apply our techniques to give explicit and computable formulae for the obstruction to the Hasse norm principle and the defect of weak approximation when the normal closure of $K/k$ has symmetric or alternating Galois group.

Contents

1. Introduction 1
2. Background 8
3. The $p$-primary parts of $\mathcal{R}(K/k)$ and $H^1(k, \text{Pic} X)$ 15
4. Using subextensions and superextensions 18
5. Applications to $A_n$ and $S_n$ extensions 22
6. Examples 30
Appendix 33
References 38

1. Introduction

In this paper we study a local-global principle known as the Hasse norm principle (HNP). Let $K/k$ be an extension of number fields with associated idèle groups $\mathbb{A}_K^*$ and $\mathbb{A}_k^*$. The norm map $N_{K/k} : K^* \to k^*$ extends to an idèlic norm map $N_{K/k} : \mathbb{A}_K^* \to \mathbb{A}_k^*$. The HNP is said to hold for $K/k$ if the so-called knot group

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

is trivial, i.e. if being a norm everywhere locally is equivalent to being a global norm from $K/k$. For example, if $N/k$ is the normal closure of $K/k$, then the HNP holds for $K/k$ in the following cases:

(I) (The Hasse norm theorem:) $N = K$ and $\text{Gal}(K/k)$ is cyclic [29];
(II) $[K : k]$ is prime [2];
(III) $[K : k] = n$ and $\text{Gal}(N/k) \cong D_n$ is dihedral of order $2n$ [3];
(IV) $[K : k] = n$ and $\text{Gal}(N/k) \cong S_n$ [31];
(V) $[K : k] = n \geq 5$ and $\text{Gal}(N/k) \cong A_n$ [37].
Biquadratic extensions provide the simplest setting in which the HNP can fail. For example, 3 is everywhere locally a norm from $\mathbb{Q}(\sqrt{-3}, \sqrt{13})/\mathbb{Q}$, but not a global norm [29].

The HNP also has a geometric interpretation: the knot group $\mathfrak{A}(K/k)$ is identified with the Tate-Shafarevich group $\mathbb{III}(T)$ of the norm one torus $T = R_{K/k}^1 \mathbb{G}_m$ defined by the following exact sequence of algebraic groups over $k$:

$$1 \rightarrow R_{K/k}^1 \mathbb{G}_m \rightarrow R_{K/k} \mathbb{G}_m \rightarrow \mathbb{G}_{m,k} \rightarrow 1$$

where $R_{K/k} \mathbb{G}_m$ denotes the Weil restriction of $\mathbb{G}_m$ from $K$ to $k$. The HNP holds for $K/k$ if and only if the Hasse principle holds for all principal homogeneous spaces for $R_{K/k}^1 \mathbb{G}_m$.

Weak approximation is said to hold for a torus $T$ over $k$ if its $k$-points are dense in the product of its points over all completions of $k$; in other words if $A(T) = 0$, where $A(T) = \prod_v T(k_v)/\overline{T(k)}$ and $\overline{T(k)}$ denotes the closure of $T(k)$ in $\prod_v T(k_v)$ with respect to the product topology. The following exact sequence, due to Voskresenskiĭ in [50], ties together weak approximation for a torus $T$ and the Hasse principle for principal homogeneous spaces for $T$:

$$0 \rightarrow A(T) \rightarrow \mathbb{H}^1(k, \text{Pic } X)\sim \rightarrow \mathbb{III}(T) \rightarrow 0. \quad (1)$$

Here, $X$ denotes a smooth compactification of $T$ and $\mathbb{H}^1(k, \text{Pic } X)\sim = \text{Hom}(\mathbb{H}^1(k, \text{Pic } X), \mathbb{Q}/\mathbb{Z})$.

Henceforth, let $T = R_{K/k}^1 \mathbb{G}_m$ and let $X$ denote a smooth compactification of $T$. Let $L/k$ be a Galois extension containing $K/k$ and set $G = \text{Gal}(L/k)$ and $H = \text{Gal}(L/K)$. We use $M(p)$ to denote the $p$-primary part of an abelian group $M$. Our first result reduces the calculation of $A(T)$, $\mathbb{H}^1(k, \text{Pic } X)$ and $\mathbb{III}(T)$ to the case where $H$ is a $p$-group.

**Theorem 1.1.** For $p$ prime, let $H_p$ denote a Sylow $p$-subgroup of $H$ and let $K_p$ denote its fixed field. Let $Y_p$ be a smooth compactification of $T_p = R_{K_p/k}^1 \mathbb{G}_m$. Then

$$\mathbb{H}^1(k, \text{Pic } X)_{(p)} \cong \mathbb{H}^1(k, \text{Pic } Y_p)_{(p)},$$

$$A(T)_{(p)} \cong A(T_p)_{(p)}, \quad \text{and}$$

$$\mathbb{III}(T)_{(p)} \cong \mathbb{III}(T_p)_{(p)}.$$  

Our next result deals with the two extremes in terms of the power of $p$ dividing $|H|$.

**Theorem 1.2.** (i) If $p \mid |H|$, then $\mathbb{H}^1(k, \text{Pic } X)_{(p)} \cong \mathbb{H}^3(G, \mathbb{Z})_{(p)}$.

(ii) If $H$ contains a Sylow $p$-subgroup of $G$, then $\mathbb{H}^1(k, \text{Pic } X)_{(p)} = 0$.

In addition to general techniques from the arithmetic of algebraic tori, our work makes use of a quotient of the knot group called the ‘first obstruction to the HNP for $K/k$ corresponding to the tower $L/K/k$’ defined by Drakokhrust and Platonov in [16] as

$$\mathfrak{F}(L/K/k) = (k^* \cap N_{K/k} N_{K/k}^*)/(k^* \cap N_{L/k} N_{L/k}^*) N_{K/k} N_{K/k}^*.$$  

In [16], Drakokhrust and Platonov show that the group $\mathfrak{F}(G, H) = (H \cap [G, G])/\Psi^G(H)$ surjects onto $\mathfrak{F}(L/K/k)$, with equality if $L/k$ is unramified. Here $\Psi^G(H)$ denotes the focal subgroup, see Definition 2.18. As shown in [16], the first obstruction to the HNP in a tower of number fields...
admits a purely group-theoretic description in terms of the relevant local and global Galois groups. Thus our next result allows one to easily compute the \( p \)-primary part of the knot group and the size of the \( p \)-primary part of the defect of weak approximation for all but finitely many primes \( p \).

**Theorem 1.3.** If \( p \) is a prime such that \( H^3(G, \mathbb{Z})_{(p)} = 0 \), then

(i) \( \mathfrak{R}(K/k)_{(p)} \cong \mathfrak{F}(L/K/k)_{(p)} \);

(ii) \( H^1(k, \text{Pic } \overline{X})_{(p)} \cong \mathfrak{F}(G, H)_{(p)} \).

We now restrict our focus to extensions with normal closure having Galois group isomorphic to \( A_n \) or \( S_n \). Our first main theorem in this setting is the following:

**Theorem 1.4.** (i) For \( G \cong S_n \) the invariant \( H^1(k, \text{Pic } \overline{X}) \) is either trivial or an elementary abelian 2-group. Every possibility is realised for some choice of \( n \) and \( K/k \).

(ii) For \( G \cong A_n \) the invariant \( H^1(k, \text{Pic } \overline{X}) \) is either trivial, isomorphic to \( C_3, C_6 \) or an elementary abelian 2-group. Every possibility is realised for some choice of \( n \) and \( K/k \).

The following corollary of Theorems 1.1 and 1.4 gives a useful shortcut when analyzing the HNP and weak approximation for \( S_n \) extensions, enabling one to reduce to the case where \( H \) is a 2-group.

**Corollary 1.5.** Suppose that \( G \cong S_n \), let \( H_2 \) be a Sylow 2-subgroup of \( H \) and let \( K_2 \) denote its fixed field. Let \( Y_2 \) be a smooth compactification of \( T_2 = \mathbb{R}_{L_2/k}^1 \mathbb{G}_m \). Then

\[
H^1(k, \text{Pic } \overline{X}) \cong H^1(k, \text{Pic } \overline{Y}_2),
\]

\[
A(T) \cong A(T_2), \quad \text{and}
\]

\[
\mathfrak{I}(T) \cong \mathfrak{I}(T_2).
\]

**Remark 1.6.** Corollary 1.5 also holds in the case \( G \cong A_n \) provided \( n \neq 6, 7 \) and \( \mathfrak{F}(G, H)_{(3)} = 0 \). In Proposition 5.9 we show that for most \( n \) we have \( \mathfrak{F}(A_n, H)_{(3)} = 0 \) for all subgroups \( H \).

The proof of Theorem 1.4 uses the following theorem which enables a purely computational analysis of the HNP and weak approximation for \( A_n \) and \( S_n \) extensions.

**Theorem 1.7.** Suppose that \( G \) is isomorphic to \( A_n \) or \( S_n \) for some \( n \geq 4 \) and \( G \not\cong A_6, A_7 \). Then

\[
\mathfrak{R}(K/k) \cong \begin{cases} 
\mathfrak{F}(L/K/k), & \text{if } |H| \text{ is even;} \\
\mathfrak{F}(L/K/k) \times \mathfrak{R}(L/k), & \text{if } |H| \text{ is odd},
\end{cases}
\]

and

\[
H^1(k, \text{Pic } \overline{X}) \cong \begin{cases} 
\mathfrak{F}(G, H), & \text{if } |H| \text{ is even;} \\
\mathfrak{F}(G, H) \times \mathbb{Z}/2, & \text{if } |H| \text{ is odd.}
\end{cases}
\]

A result of Tate (see Theorem 2.11) shows that the knot group of the Galois extension \( L/k \) is dual to \( \text{Ker}(H^1(G, \mathbb{Z}) \to \prod_v H^3(D_v, \mathbb{Z})) \), where \( D_v \) denotes the decomposition group at a place \( v \) of \( k \). Note that this kernel only depends on the decomposition groups at the ramified places, since if \( v \) is unramified then \( D_v \) is cyclic and hence \( H^3(D_v, \mathbb{Z}) = 0 \). This yields the following corollary:
Corollary 1.8. Given an extension $K/k$ satisfying the conditions of Theorem 1.7, there is an algorithm that takes as inputs $G$, $H$ and the decomposition groups at the ramified places of $L/k$ and gives as its outputs the knot group $\mathfrak{r}(K/k)$, the invariant $H^1(k, \text{Pic } X)$, and the defect of weak approximation $A(T)$ for $T = R^1_{K/k} \mathbb{G}_m$.

As an application, one can obtain conditions on the decomposition groups determining whether the HNP and weak approximation hold in $A_n$ and $S_n$ extensions. In Theorems 1.9 and 1.10, we exhibit such a characterization for $n = 4$ or $5$, when these local conditions are particularly simple.

Theorem 1.9. Suppose that $G$ is isomorphic to $A_4, A_5, S_4$ or $S_5$. Then $\mathfrak{r}(K/k) \hookrightarrow C_2$ and

(i) if $|H|$ is odd, then $\mathfrak{r}(K/k) = 1 \iff \exists v$ such that $V_4 \hookrightarrow D_v$;
(ii) if $\exists C \leq H$ generated by a double transposition with $[H : C]$ odd, then $\mathfrak{r}(K/k) = 1 \iff \exists v$ such that $D_v$ contains a copy of $V_4$ generated by two double transpositions;
(iii) in all other cases, $\mathfrak{r}(K/k) = 1$.

Theorem 1.10. Retain the assumptions of Theorem 1.9. Then $H^1(k, \text{Pic } X) \cong \begin{cases} \mathbb{Z}/2 & \text{in cases (i) and (ii) of Theorem 1.9} \\ 0 & \text{otherwise.} \end{cases}$

Therefore, in cases (i) and (ii) of Theorem 1.9, weak approximation holds for $R^1_{K/k} \mathbb{G}_m$ if and only if the HNP fails for $K/k$. In all other cases, weak approximation holds for $R^1_{K/k} \mathbb{G}_m$.

For the sake of completeness, we also provide criteria for the validity of the HNP when $G \cong A_6$ or $A_7$ (the two groups not addressed by Theorem 1.7). The proof uses the first obstruction to the HNP, along with various tricks involving moving between subextensions as detailed in Section 4.

Theorem 1.11. Suppose that $G$ is isomorphic to $A_6$ or $A_7$. Then $\mathfrak{r}(K/k) \hookrightarrow C_6$ and

- $\mathfrak{r}(K/k)(2) = 1 \iff \begin{cases} V_4 \hookrightarrow H; \text{ or} \\ C_4 \hookrightarrow H \text{ and } \exists v \text{ such that } D_4 \hookrightarrow D_v; \text{ or} \\ 4 \nmid |H| \text{ and } \exists v \text{ such that } V_4 \hookrightarrow D_v. \end{cases}$
- $\mathfrak{r}(K/k)(3) = 1 \iff \begin{cases} C_3 \hookrightarrow H; \text{ or} \\ \exists v \text{ such that } C_3 \times C_3 \hookrightarrow D_v. \end{cases}$

Theorem 1.12 below addresses weak approximation in the $A_6$ and $A_7$ cases. The local conditions controlling weak approximation are given in detail in Theorem 5.17; they are a direct consequence of Theorems 1.11 and 1.12 and Voskresenskii’s exact sequence (1).

Theorem 1.12. Retain the assumptions of Theorem 1.11. Then $H^1(k, \text{Pic } X) \hookrightarrow \mathbb{Z}/6$ and

- $H^1(k, \text{Pic } X)(2) = 0$ if and only if $V_4 \hookrightarrow H$;
- $H^1(k, \text{Pic } X)(3) = 0$ if and only if $C_3 \hookrightarrow H$. 
Our motivation for providing explicit local conditions for the failure of the HNP is to enable a statistical analysis of the HNP and weak approximation for norm one tori in families of extensions of number fields. Such an analysis was carried out for extensions of a number field $k$ with fixed abelian Galois group by the second author together with Frei and Loughran in [20] (ordering by discriminant) and [21] (ordering by conductor). One consequence of their results is that the HNP fails for 0% of biquadratic extensions of $k$. In the case $k = \mathbb{Q}$, this was refined to an asymptotic formula for the number of biquadratics failing the HNP (ordered by discriminant) by Rome in [43].

Having dealt with the $V_4$ case and noting that the HNP holds for all $C_4, D_4$ and $S_4$ quartics (see (I), (III) and (IV)), if one wants to fully understand the frequency of failure of the HNP for quartics with fixed Galois group, there is one remaining family to tackle: namely $A_4$ quartics. Counting $A_4$ quartics may be beyond current capabilities but the following corollary of Theorem 1.9 gives hope that one may be able to exploit results about biquadratic extensions to bound the number of $A_4$ quartics for which the HNP fails.

**Corollary 1.13.** Let $K/k$ be a quartic extension of number fields with normal closure $L/k$ such that $G = \text{Gal}(L/k)$ is isomorphic to $A_4$. Let $F$ be the fixed field of the copy of $V_4$ in $G$. Then

$$\mathcal{R}(K/k) \cong \mathcal{R}(L/k) \cong \mathcal{R}(L/F).$$

In particular, the HNP holds for $K/k$ if and only if it holds for the biquadratic extension $L/F$. Likewise, weak approximation holds for $K/k$ if and only if it holds for $L/F$.

The first statistical study of the HNP in a family of extensions with fixed non-abelian Galois group is carried out by the first author in [38], where he shows that the HNP fails for 0% of $D_4$ octics ordered by an Artin conductor. The present paper provides the algebraic input required to study the statistics of the HNP and weak approximation in several more families of non-abelian, and even non-Galois, number fields – such as $S_4$ octics, for example. This future work will capitalize on recent advances in counting within families of number fields, see e.g. [1, 4, 5, 8, 17, 22, 31, 40, 52], and contribute to the ongoing rapid progress in the area of rational points and failures of local-global principles in families of varieties. See [11] for a survey of recent developments in this area.

Although counting degree $n > 4$ extensions of number fields with bounded discriminant may be out of reach at present, there are very precise conjectures for the number of such extensions. Namely, the weak Malle conjecture on the distribution of number fields (see [39]) predicts that the number $N(k, G, X)$ of degree $n$ extensions $K$ of a number field $k$ with Galois group $G$ and $|N_{k/\mathbb{Q}}(\text{Disc}_K/k)| \leq X$ satisfies

$$X^{\alpha(G)} \ll N(k, G, X) \ll X^{\alpha(G)+\epsilon},$$

where $\alpha(G) = \min_{g \in G \setminus \{1\}} \{\text{ind}(g)\}$ and $\text{ind}(g)$ equals $n$ minus the number of orbits of $g$ on $\{1, \ldots, n\}$. Using a computational method developed by Hoshi and Yamasaki (see Section 5.2), we obtain the following consequence of this conjecture:
Theorem 1.14. Fix a number field \( k \) and an integer \( n \leq 15 \) with \( n \neq 8, 12 \). Suppose that Conjecture (2) holds for every transitive subgroup \( G \leq S_n \). Then

(i) the HNP holds for 100% of degree \( n \) extensions over \( k \), when ordered by discriminant;
(ii) weak approximation holds for 100% of norm one tori of degree \( n \) extensions over \( k \), when ordered by discriminant of the associated extension\(^1\).

In fact, the assertions of Theorem 1.14 remain true if one only assumes Conjecture (2) for a few transitive subgroups of \( S_n \), see Remark 5.11(iii).

In order to obtain asymptotic formulae for the number of extensions satisfying certain conditions, it is often necessary to first show the existence of at least one such extension, see [20, Theorem 1.7], for example. Our next result addresses this issue. We call an extension of number fields \( K/k \) a \((G,H)\)-extension if there exists a Galois extension \( L/k \) containing \( K/k \) such that \( \text{Gal}(L/k) \cong G \) and \( \text{Gal}(L/K) \cong H \). We write \( F_{G/H} \) for a flasque module in a flasque resolution of the Chevalley module \( J_{G/H} \), see Section 2.2.

Theorem 1.15. Let \( G \) be a finite group and \( H \) a subgroup of \( G \). Then

(i) there exists a \((G,H)\)-extension satisfying the HNP;
(ii) if \( H^1(G, F_{G/H}) \neq 0 \), then there exists a \((G,H)\)-extension failing the HNP.

The condition \( H^1(G, F_{G/H}) \neq 0 \) in (ii) is necessary because for a \((G,H)\)-extension \( K/k \) with \( X \) a smooth compactification of \( R^1_{K/k} \mathbb{G}_m \), one has \( H^1(k, \text{Pic} X) = H^1(G, F_{G/H}) \). This is due to Colliot-Thélène and Sansuc (see Theorem 2.8).

It is interesting to compare Theorem 1.15 with [20, Theorem 1.3], where the authors prove existence of Galois extensions failing the HNP with prescribed solvable Galois group \( G \) and base field \( k \). Here we avoid the restriction on \( G \) but lose control of the base field which, in both cases of Theorem 1.15 may be of quite large degree over \( \mathbb{Q} \). In Section 6 we give explicit examples of extensions of number fields illustrating all cases of Theorems 1.9 and 1.11. The examples of field extensions for which the HNP holds all have base field \( \mathbb{Q} \), and the examples for which the HNP fails have base fields that are at most quadratic extensions of \( \mathbb{Q} \).

1.1. Structure of the paper. Section 2 contains the relevant background material. In Section 3 we prove Theorems 1.1 – 1.3. Section 4 gathers results that allow one to transfer information regarding the HNP from a field extension to its subextensions and vice versa. We also give analogues of these results for weak approximation on the associated norm one tori. In Section 5 we apply our results to extensions whose normal closure has Galois group \( A_n \) or \( S_n \), proving Theorems 1.4 – 1.12, Corollary 1.13 and Theorem 1.14. In Section 6 we prove Theorem 1.15 and give examples of successes and failures of the HNP in all cases covered by Theorems 1.9 and 1.11.

\(^1\)Note that the isomorphism class of a number field is determined by the isomorphism class of its norm one torus.
1.2. **Notation.** Given a number field $k$ and a Galois extension $L/k$, we use the following notation:

- $\overline{k}$ an algebraic closure of $k$
- $\mathbb{A}_k^*$ the idèle group of $k$
- $\mathcal{O}_k$ the ring of integers of $k$
- $\Omega_k$ the set of all places of $k$
- $L_v$ the completion of $L$ at some choice of place above $v \in \Omega_k$
- $D_v$ the Galois group of $L_v/k_v$

Given a field $K$, a variety $X$ over $K$ and an algebraic $K$-torus $T$, we use the following notation:

- $\mathbb{G}_{m,K}$ the multiplicative group $\text{Spec}(K[t,t^{-1}])$ of $K$ (if $K$ is clear from the context, we omit it from the subscript)
- $X_L$ the base change $X \times_K L$ of $X$ to a field extension $L/K$
- $\overline{X}$ the base change of $X$ to an algebraic closure of $K$
- $\text{Pic} X$ the Picard group of $X$
- $\hat{T}$ the character group $\text{Hom}(T, \mathbb{G}_{m,K})$ of $T$
- $R_{K/k}T$ the Weil restriction of $T$ to a subfield $k$ of $K$
- $R_{1/K/k}^1 \mathbb{G}_m$ the kernel of the norm map $N_{K/k} : R_{K/k}^1 \mathbb{G}_m \to \mathbb{G}_{m,k}$

For an algebraic torus $T$ defined over a number field $k$, we denote its Tate-Shafarevich group and defect of weak approximation by

$$\text{III}(T) := \text{Ker} \left( H^1(k, T) \to \prod_{v \in \Omega_k} H^1(k_v, T) \right)$$
and
$$A(T) := \left( \prod_{v \in \Omega_k} T(k_v) \right) / T(k),$$
respectively.

Given a finite group $G$, a subgroup $H$ of $G$, a $G$-module $A$, an integer $q$ and a prime number $p$, we use the notation:

- $|G|$ the order of $G$
- $\exp(G)$ the exponent of $G$
- $[G,G]$ the derived subgroup of $G$
- $G^\sim$ the $\mathbb{Q}/\mathbb{Z}$-dual $\text{Hom}(G, \mathbb{Q}/\mathbb{Z})$ of $G$
- $G_p$ a Sylow $p$-subgroup of $G$
- $\hat{H}^q(G, A)$ the Tate cohomology group
- $\text{III}^q(G, A)$ the kernel of the restriction map $\hat{H}^q(G, A) \xrightarrow{\text{Res}} \prod_{g \in G} \hat{H}^q(\langle g \rangle, A)$

For $x, y \in G$ we adopt the convention $[x, y] = x^{-1}y^{-1}xy$ and $x^y = y^{-1}xy$. If $G$ is abelian and $d \in \mathbb{Z}_{>0}$, we denote:

- $G[d]$ the $d$-torsion of $G$
- $G_{(d)}$ the $d$-primary part of $G$
We often use ‘=’ to indicate a canonical isomorphism between two objects.

1.3. Acknowledgements. We are grateful to Manjul Bhargava for conversations that motivated our work on this topic and to Jean-Louis Colliot-Thélène for very useful discussions which led to a cleaner proof of Theorem 1.1. We thank Levent Alpoge, Henri Cohen, Valentina Grazian, Samir Siksek, Anitha Thillaisundaram and Rishi Vyas for helpful conversations. André Macedo is supported by the Portuguese Foundation of Science and Technology (FCT) via the doctoral scholarship SFRH/BD/117955/2016. Rachel Newton is supported by EPSRC grant EP/S004696/1.

2. Background

2.1. Group cohomology. The following well-known fact will be useful.

Proposition 2.1. Let $G$ be a finite group and $G_p$ a Sylow $p$-subgroup of $G$. For any $G$-module $A$ and any $n \in \mathbb{Z}_{>0}$, the restriction map

$$\text{Res}^G_{G_p} : H^n(G, A) \to H^n(G_p, A)$$

maps $H^n(G, A)_{(p)}$ injectively into $H^n(G_p, A)$.

Proof. See, for example, [10, Theorem III.10.3]. □

In order to study restriction and corestriction maps, we will also need a few results from the theory of covering groups.

Definition 2.2. Let $G$ be a finite group. A finite group $\overline{G}$ is called a generalized representation group of $G$ if there exists a central extension

$$1 \to K \to \overline{G} \xrightarrow{\lambda} G \to 1,$$

with $K \cap [\overline{G}, \overline{G}] \cong \hat{H}^{-3}(G, \mathbb{Z})$, the Schur multiplier of $G$. We call $K$ the base normal subgroup of $\overline{G}$.

Lemma 2.3. [16] Lemma 4] Let $G$ be a finite group, $H$ a subgroup of $G$ and $\overline{G}$ a generalized representation group of $G$ with projection map $\lambda$ and base normal subgroup $K$. Then

$$\text{Im} \left( \text{Cor} : \hat{H}^{-3}(H, \mathbb{Z}) \to \hat{H}^{-3}(G, \mathbb{Z}) \right) \cong K \cap [\lambda^{-1}(H), \lambda^{-1}(H)].$$

It is well known that every finite group has a generalized representation group (see [33 Theorem 2.1.4]). The following result of Schur, giving presentations of generalized representation groups of $A_n$ and $S_n$, will be useful when investigating the Hasse norm principle for $A_n$ and $S_n$ extensions.

Proposition 2.4. Let $n \geq 4$ and let $U$ be the group with generators $z, \overline{t_1}, \ldots, \overline{t_{n-1}}$ and relations

(i) $z^2 = 1$;
(ii) $z \overline{t}_i = \overline{t}_i z$, for $1 \leq i \leq n - 1$;
(iii) $\overline{t}_i^2 = z$, for $1 \leq i \leq n - 1$;
(iv) $(\overline{t}_i \overline{t}_{i+1})^3 = z$, for $1 \leq i \leq n - 2$;
(v) $\overline{t}_i \overline{t}_j = z \overline{t}_j \overline{t}_i$, for $|i - j| \geq 2$ and $1 \leq i, j \leq n - 1$. 
Then $U$ is a generalized representation group of $S_n$ with base normal subgroup $K = \langle z \rangle$. Moreover, if $t_i$ denotes the transposition $(i \ i + 1)$ in $S_n$, then the map

$$\lambda: U \to S_n$$

$$z \mapsto 1$$

$$t_i \mapsto t_i$$

is surjective and has kernel $K$. Additionally, if $n \neq 6, 7$, then a generalized representation group of $A_n$ is given by $V = \lambda^{-1}(A_n) = \langle z, t_1, t_2, t_1, t_3, \ldots, t_1, t_{n-1} \rangle \leq U$.

Proof. See Schur’s original paper [46] or [32, Chapter 2] for a more modern exposition regarding generalized representation groups of $S_n$. The $A_n$ case is dealt with in [37, §2]. □

2.2. Arithmetic of algebraic tori. Let $T$ be a torus over a number field $k$. As mentioned in the introduction, Voskresenski˘ı’s exact sequence ties together the Tate-Shafarevich group $X(T)$ and the defect of weak approximation $A(T)$:

**Theorem 2.5** (Voskresenski˘ı). Let $T$ be a torus defined over a number field $k$ and let $X/k$ be a smooth compactification of $T$. Then there exists an exact sequence

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

**Proof.** See [50, Theorem 6]. □

Note that the Hochschild-Serre spectral sequence gives an isomorphism $\text{Br} X/\text{Br}_0 X \cong H^1(k, \text{Pic} \overline{X})$, where $\text{Br}_0 X = \text{Im}(\text{Br} k \to \text{Br} X)$. Furthermore, $\text{Br} X = \text{Br}_{nr}(k(T)/k)$ is known as the unramified Brauer group of $T$.

In the case of the norm one torus $T = R_{K/k}^1 \mathbb{G}_m$ associated to an extension of number fields $K/k$, $\text{III}(T) = \mathfrak{M}(K/k)$ (see [11, p. 307]). Hence, Theorem 2.5 gives a necessary and sufficient condition for the validity of both the HNP for $K/k$ and weak approximation for $T$, namely the vanishing of $H^1(k, \text{Pic} \overline{K})$.

Recall that if $T$ is split by a Galois subextension $L/k$ of $\overline{K}/k$, then $\text{Gal}(\overline{K}/L)$ acts trivially on the character group $\widehat{T} = \text{Hom}(T, \mathbb{G}_m, \overline{K})$ and thus $\widehat{T}$ is a $\text{Gal}(L/k)$-module. Implicit in much of our work is the fact that the norm one torus $R_{K/k}^1 \mathbb{G}_m$ is split by any Galois extension of $k$ containing $K$.

**Lemma 2.6.** Let $K/k$ be a finite extension and let $X$ be a smooth compactification of $T = R_{K/k}^1 \mathbb{G}_m$. Then $T \times_k K$ is stably rational. Consequently, $H^1(k, \text{Pic} \overline{X})$ is killed by $[K : k]$.

**Proof.** Write $T_K = T \times_k K$. Applying base change to the exact sequence defining $T$ gives

$$1 \to T_K \to (R_{K/k}^1 \mathbb{G}_m) \times_k K \xrightarrow{N_{K/k}} \mathbb{G}_{m,K} \to 1. \quad (3)$$

Let $L/k$ be a Galois extension containing $K$. Let $G = \text{Gal}(L/k)$ and let $H = \text{Gal}(L/K)$. Taking character groups gives an exact sequence of $H$-modules

$$0 \to \mathbb{Z} \to \mathbb{Z}[G/H] \to \widehat{T}_K \to 0 \quad (4)$$
As an $H$-module, $\mathbb{Z}[G/H]$ decomposes as $\mathbb{Z}[G/H] = \mathbb{Z} \oplus M$ for some $H$-module $M$, whereby the exact sequence (1) splits and hence so does (3). Therefore,

$$T_K \times \mathbb{G}_{m,K} \cong (R_{K/k}\mathbb{G}_m) \times_k K.$$ 

Hence, $T_K$ is $K$-stably rational, whereby $H^1(K, \text{Pic} \bar{X}) = H^1(H, \text{Pic} X_L) = 0$. Now recall that $\text{Cor}^G_H \circ \text{Res}^G_H$ is multiplication by $[G : H] = [K : k]$ and $\text{Res}^G_H : H^1(G, \text{Pic} X_L) \to H^1(H, \text{Pic} X_L) = 0$. This completes the proof that $[K : k]$ kills $H^1(G, \text{Pic} X_L) = H^1(k, \text{Pic} \bar{X})$.

The corollary below is an immediate consequence of Theorem 2.5 and Lemma 2.6.

**Corollary 2.7.** Let $T = R^1_{K/k}\mathbb{G}_m$. If $p \nmid [K : k]$, then $A(T)_{(p)} = 0 = \mathcal{R}(K/k)_{(p)}$.

One approach to understanding the group $H^1(k, \text{Pic} \bar{X})$ is via flasque resolutions of the Galois module $\hat{T}$. We explain this approach below (see [12] and [13] for more details).

Let $G$ be a finite group and let $A$ be a $G$-module. We say that $A$ is a permutation module if it has a $\mathbb{Z}$-basis permuted by $G$. We say that $A$ is flasque if $H^1(G', A) = 0$ for all subgroups $G'$ of $G$. 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. We say two $G$-modules $A_1$ and $A_2$ are similar if $A_1 \oplus P_1 \cong A_2 \oplus P_2$ for permutation modules $P_1, P_2$ and denote the similarity class of $A$ by $[A]$.

**Theorem 2.8** (Colliot-Thélène and Sansuc). Let $T$ be a torus defined over a number field $k$ and split by a finite Galois extension $L/k$ with $G = \text{Gal}(L/k)$. Let

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

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

$$H^1(k, \text{Pic} \bar{X}) = H^1(G, \text{Pic} X_L) = H^1(G, F).$$

Additionally, $H^1(G, F) = \Xi^2_0(G, \hat{T}) := \text{Ker} \left( H^2(G, \hat{T}) \xrightarrow{\text{Res}} \prod_{g \in G} H^2(\langle g \rangle, \hat{T}) \right)$.

**Proof.** See [12] Lemme 5 and Proposition 6], and [13] Proposition 9.5(ii)] for the final assertion. □

Let us return to the case where $T$ is the norm one torus $R^1_{K/k}\mathbb{G}_m$ of an extension $K/k$ of number fields. In the special case where $K/k$ is a Galois extension the invariant $H^1(G, F)$ of Theorem 2.8 takes a particularly simple form, as the following result shows.

**Proposition 2.9.** If $T = R^1_{K/k}\mathbb{G}_m$ and $K/k$ is Galois with $G = \text{Gal}(K/k)$, then the invariant $H^1(G, F)$ of Theorem 2.8 is canonically isomorphic to $H^3(G, \mathbb{Z})$.

**Proof.** See [12] Proposition 7]. □

Let $L/k$ be a Galois extension containing $K/k$ and set $G = \text{Gal}(L/k), H = \text{Gal}(L/K)$. It is a well-known fact that the module $\hat{T}$ is isomorphic to the $G$-module $J_{G/H}$, defined as follows:
**Definition 2.10** (Chevalley module). Let $G$ be a finite group and $H$ a subgroup of $G$. The map $\eta : \mathbb{Z} \to \mathbb{Z}[G/H]$ defined by $\eta : 1 \mapsto N_{G/H} = \sum_{gH \in G/H} gH$ produces the exact sequence of $G$-modules

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

where $J_{G/H} = \text{coker} \eta$ is called the Chevalley module of $G/H$.

By Theorem 2.8 we see that in order to compute the middle group of Voskresenski˘ı’s exact sequence in Theorem 2.5, it suffices to construct a flasque module $F_{G/H}$ in a flasque resolution of the $G$-module $\hat{T}$ and then calculate the cohomology group $\text{H}^1(G,F_{G/H})$. The Tate-Shafarevich group $X(T)$ also has a description in terms of the cohomology of $\hat{T}$, as follows:

**Theorem 2.11** (Tate). Let $T$ be a torus defined over a number field $k$ and split by a finite Galois extension $L/k$ with $G = \text{Gal}(L/k)$. There is a canonical isomorphism

$$ \Pi(T)^\sim = \text{Ker} \left( \text{H}^2(G,\hat{T}) \xrightarrow{\text{Res}} \prod_{v \in \Omega_k} \text{H}^2(D_v,\hat{T}) \right) $$

where $D_v = \text{Gal}(L_v/k_v)$ is the decomposition group at $v$. In the special case where $T = R^1_{L/k} \mathbb{G}_m$, $\Pi(T)^\sim = \mathfrak{R}(L/k)^\sim = \text{Ker} \left( \text{H}^3(G,\mathbb{Z}) \xrightarrow{\text{Res}} \prod_{v \in \Omega_k} \text{H}^3(D_v,\mathbb{Z}) \right)$.

**Proof.** This is the case $i = 1$ of [111, Theorem 6.10]. For the case $T = R^1_{L/k} \mathbb{G}_m$, see [113, p. 198]. □

**2.3. The first obstruction to the Hasse norm principle.** Throughout this section, we fix a tower of number fields $L/K/k$ such that $L/k$ is Galois.

**Definition 2.12.** [16, Definition 1] The group

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

is called the first obstruction to the HNP for $K/k$, corresponding to the tower $L/K/k$.

Clearly the knot group $\mathfrak{K}(K/k)$ (which is sometimes called the total obstruction to the HNP) subjects onto $\mathfrak{F}(L/K/k)$ and $\mathfrak{F}(L/K/k)$ equals $\mathfrak{K}(K/k)$ if the HNP holds for $L/k$. In [16], Drakokhrust and Platonov give another very useful sufficient criterion for this equality to hold, as follows:

**Theorem 2.13.** [16, Theorem 3] Set $G = \text{Gal}(L/k), H = \text{Gal}(L/K)$. Let $G_1, \ldots, G_r$ be subgroups of $G$ and let $H_1, \ldots, H_r$ be subgroups of $H$ such that $H_i \subset H \cap G_i$ for each $i$. Let $K_i = L^{H_i}$ and $k_i = L^{G_i}$. Suppose that the HNP holds for the extensions $K_i/k_i$ and that the map

$$ \bigoplus_{i=1}^r \text{Cor}_{G_i}^G : \bigoplus_{i=1}^r \hat{H}^{-3}(G_i,\mathbb{Z}) \to \hat{H}^{-3}(G,\mathbb{Z}) $$

is surjective. Then $\mathfrak{F}(L/K/k) = \mathfrak{K}(K/k)$. 

In order to compute $\mathfrak{g}(L/K/k)$, Drakokhrust and Platonov give some explicit results relating this object to the local and global Galois groups of the tower $L/K/k$. We present their results here in a slightly more general setting. Let $G$ be a finite group, let $H \leq G$, and let $S$ be a set of subgroups of $G$. Consider the following commutative diagram:

$$
H/[H,H] \xrightarrow{\psi_1} G/[G,G] \xrightarrow{\varphi_1} \bigoplus_{D \in S} \left( H_i/[H_i,H_i] \right) \xrightarrow{\psi_2} \bigoplus_{D \in S} D/[D,D]
$$

where the $x_i$’s are a set of representatives of the $H-D$ double cosets of $G$, the sum over $D$ is a sum over all subgroups in $S$, and $H_i := H \cap x_i D x_i^{-1}$. The maps $\psi_1, \varphi_1$ and $\varphi_2$ are induced by the natural inclusions $H \hookrightarrow G$, $H_i \hookrightarrow H$ and $D \hookrightarrow G$, respectively. If $h \in H_i$, then

$$
\psi_2(h[H_i,H_i]) = x_i^{-1} h x_i [D,D] \in D/[D,D].
$$

Given a subgroup $D \in S$, we denote by $\psi_2^D$ the restriction of the map $\psi_2$ in diagram (5) to the subgroup $\bigoplus_{Hx_iD \in H \setminus G/D} H_i/[H_i,H_i]$.

**Lemma 2.14.** In diagram (5), $\varphi_1(\operatorname{Ker} \psi_2^D) \subset \varphi_1(\operatorname{Ker} \psi_2^{D'})$ whenever $D \subset D'$.

**Proof.** The proof follows in the same manner as the proof of [16, Lemma 2].

**Lemma 2.15.** [16, Lemma 1] Set $G = \operatorname{Gal}(L/k)$ and $H = \operatorname{Gal}(L/K)$. Given a place $v$ of $k$, the set of places $w$ of $K$ above $v$ is in one-to-one correspondence with the set of double cosets in the decomposition $G = \bigcup_{i=1}^r H x_i D_v$. If $w$ corresponds to $H x_i D_v$, then the decomposition group $H_w$ of the extension $L/K$ at $w$ equals $H \cap x_i D_v x_i^{-1}$.

Set $G = \operatorname{Gal}(L/k)$, $H = \operatorname{Gal}(L/K)$ and $S = \{D_v \mid v \in \Omega_k\}$. Lemma 2.15 shows that, with these choices, diagram (5) takes the form

$$
H/[H,H] \xrightarrow{\psi_1} G/[G,G] \xrightarrow{\varphi_1} \bigoplus_{v \in \Omega_k} \left( \bigoplus_{w \mid v} H_w/[H_w,H_w] \right) \xrightarrow{\psi_2} \bigoplus_{v \in \Omega_k} D_v/[D_v,D_v]
$$

where the sum over $w \mid v$ is a sum over all places $w$ of $K$ above $v$ and $H_w$ is the decomposition group of $L/K$ at $w$.

**Theorem 2.16.** [16, Theorem 1] In the notation of diagram (6), we have

$$
\mathfrak{g}(L/K/k) \cong \operatorname{Ker} \psi_1/\varphi_1(\operatorname{Ker} \psi_2).
$$
For $v \in \Omega_k$ we denote by $\psi^v_2$ the restriction of the map $\psi_2$ in diagram $[5]$ to $\bigoplus_{w|v} H_w/[H_w, H_w]$. If $v_1, v_2 \in \Omega_k$ are such that their decomposition groups satisfy $D_{v_1} \subset D_{v_2}$, Lemma 2.14 gives $\varphi_1(\text{Ker} \psi^v_2) \subset \varphi_1(\text{Ker} \psi^{v_2}_2)$. We write $\psi^r_2$ for the restriction of the map $\psi_2$ to the subgroup

\[ \bigoplus_{v \text{ unramified in } L/k} H_w/[H_w, H_w] \]

and define $\psi^r_2$ similarly using the ramified places.

**Lemma 2.17.** Set $G = \text{Gal}(L/k)$ and $H = \text{Gal}(L/K)$. Let $C$ be the set of all cyclic subgroups of $G$ and let $\varphi^C_1$ and $\psi^C_2$ denote the relevant maps in diagram $[5]$ with $S = C$. Then

\[ \varphi_1(\text{Ker} \psi^nr_2) = \varphi^C_1(\text{Ker} \psi^C_2) \]

where the maps in the expression on the left are the ones in diagram $[6]$.

**Proof.** This follows from the Chebotarev density theorem and Lemma 2.14. □

**Definition 2.18.** Let $H$ be a subgroup of a finite group $G$. The focal subgroup of $H$ in $G$ is

\[ \Phi^G(H) = \langle h_1^{-1}h_2 \mid h_1, h_2 \in H \text{ and } h_2 \text{ is } G\text{-conjugate to } h_1 \rangle = \langle [h, x] \mid h \in H \cap xHx^{-1}, x \in G \rangle \leq H. \]

**Theorem 2.19.** [16, Theorem 2] In the notation of diagram $[6]$, we have

\[ \varphi_1(\text{Ker} \psi^nr_2) = \Phi^G(H)/[H, H]. \]

Theorem 2.19 is very useful – quite often one can show that $\Phi^G(H) = H \cap [G, G]$ and hence the first obstruction $\mathcal{F}(L/K/k)$ is trivial. In fact, since $[N_G(H), H] \subset \Phi^G(H)$, if one can show that $[N_G(H), H] = H \cap [G, G]$, then $\mathcal{F}(L/K/k) = 1$. This criterion generalizes [28, Theorem 3].

**Remark 2.20.** The group $\text{Ker} \psi_1/\varphi_1(\text{Ker} \psi_2)$ featured in Theorem 2.16 can be computed in finite time. Indeed, $\text{Ker} \psi_1$ is given in terms of the relevant Galois groups, and by [16, p. 307] we have

\[ \varphi_1(\text{Ker} \psi_2) = \varphi_1(\text{Ker} \psi^nr_2)\varphi_1(\text{Ker} \psi^r_2). \]

Hence, Theorem 2.19 and the fact that only finitely many places of $k$ ramify in $L/k$ show that $\varphi_1(\text{Ker} \psi_2)$ can be obtained by a finite computation. We combined these facts to assemble a function $1\text{obs}(G, H, 1)$ in GAP [23] that, given the groups $G = \text{Gal}(L/k)$, $H = \text{Gal}(L/K)$ and the list $l$ of decomposition groups $D_v$ at the ramified places $v$, returns the group $\text{Ker} \psi_1/\varphi_1(\text{Ker} \psi_2)$ isomorphic to the first obstruction $\mathcal{F}(L/K/k)$. The code for this function is available at [36].

Theorem 2.19 also motivates the following definition.

**Definition 2.21.** Let $G$ be a finite group and let $H \leq G$. Define the group $\mathcal{F}(G, H)$ by

\[ \mathcal{F}(G, H) = (H \cap [G, G])/\Phi^G(H). \]
Returning to the situation of a tower of number fields $L/K/k$ with $L/k$ Galois, $G = \text{Gal}(L/k)$ and $H = \text{Gal}(L/K)$ and employing the notation of diagram (5), we have

$$\mathfrak{F}(G, H) \cong \text{Ker} \psi_1/\varphi_1(\text{Ker} \psi_2^{\text{nr}}).$$

(8)

Note that $\mathfrak{F}(G, H)$ is an abelian group since $[H, H] \subset \Phi^G(H)$. Furthermore, $\mathfrak{F}(G, H)$ surjects onto the first obstruction $\mathfrak{F}(L/K/k)$ and $\mathfrak{F}(G, H) \cong \mathfrak{F}(L/K/k)$ when $L/k$ is unramified. In [15], Drakokhrust used $\mathfrak{F}(G, H)$ to calculate the middle group of Voskresenskiǐ’s exact sequence in terms of generalized representation groups of the Galois groups involved.

**Theorem 2.22.** Let $T$ be the norm one torus $R^1_{K/k} \mathbb{G}_m$ and let $X/k$ be a smooth compactification of $T$. Set $G = \text{Gal}(L/k), H = \text{Gal}(L/K)$. Let $\overline{G}$ be a generalized representation group of $G$ with projection map $\lambda$ and for any subgroup $B \leq G$ let $\overline{B} = \lambda^{-1}(B)$. Then

$$\mathbb{H}^1(k, \text{Pic} X) \cong \mathfrak{F}(\overline{G}, \overline{H}).$$

**Proof.** For any $v \in \Omega_k$, define

$$S_v = \begin{cases} 
\lambda^{-1}(D_v), & \text{if } v \text{ is ramified in } L/k; \\
\text{a cyclic subgroup of } \lambda^{-1}(D_v) \text{ with } \lambda(S_v) = D_v, & \text{otherwise.} 
\end{cases}$$

Consider the version of diagram (5) with respect to the groups $\overline{G}, \overline{H}$ and $S = \{S_v \mid v \in \Omega_k\}$. In this setting, Drakokhrust shows in [15, Theorem 2] that

$$\mathbb{H}^1(k, \text{Pic} X) \cong \text{Ker} \psi_1/\varphi_1(\text{Ker} \psi_2^{\text{nr}}),$$

where $\psi_2^{\text{nr}}$ denotes the restriction of $\psi_2$ to the subgroup

$$\bigoplus_{v \text{ unramified in } L/k} \left( \bigoplus_{i=1}^{r_v} \overline{H} \cap x_i S_v x_i^{-1} \right)$$

and the $x_i$’s are a set of representatives for the double coset decomposition $\overline{G} = \bigcup_{i=1}^{r_v} \overline{H} x_i S_v$.

By the Chebotarev density theorem we can choose the subgroups $S_v$ for $v$ unramified in such a way that every cyclic subgroup of $\overline{G}$ is in $S$. For this choice, we obtain

$$\text{Ker} \psi_1/\varphi_1(\text{Ker} \psi_2^{\text{nr}}) = \mathfrak{F}(\overline{G}, \overline{H}).$$

Indeed, we clearly have $\text{Ker} \psi_1 = (\overline{H} \cap [\overline{G}, \overline{G}])/[\overline{H}, \overline{H}]$ and the equality $\varphi_1(\text{Ker} \psi_2^{\text{nr}}) = \Phi^G(\overline{H})/[\overline{H}, \overline{H}]$ follows from Lemma 2.17 and an argument similar to the proof of [16, Theorem 2].

We finish this section by summarizing the relation between some of the objects introduced so far.

**Proposition 2.23.** Retain the notation of Theorem 2.22. There is a diagram of surjections

$$\mathfrak{F}(\overline{G}, \overline{H}) \twoheadrightarrow \mathfrak{F}(K/k) \twoheadrightarrow \mathfrak{F}(L/K/k).$$
Furthermore,

(i) $\mathfrak{g}(\overline{G}, \overline{H}) \cong \mathfrak{g}(K/k)$ if and only if weak approximation holds for $R_{K/k}^1 \mathbb{G}_m$;

(ii) $\mathfrak{g}(\overline{G}, \overline{H}) \cong \mathfrak{g}(G, H)$ if and only if $\text{Ker} \lambda \cap (\overline{G}, \overline{G}) \subset \Phi(\overline{G}, \overline{H})$;

(iii) $\mathfrak{g}(K/k) = \mathfrak{g}(L/K/k)$ if the HNP holds for $L/k$;

(iv) $\mathfrak{g}(G, H) \cong \mathfrak{g}(L/K/k)$ if every decomposition group of $L/k$ is cyclic.

Proof. The existence of a surjection $\mathfrak{g}(\overline{G}, \overline{H}) \to \mathfrak{g}(K/k)$ follows from Theorems 2.5 and 2.22. The surjection $\mathfrak{g}(\overline{G}, \overline{H}) \to \mathfrak{g}(G, H)$ is induced by the projection map $\lambda : \overline{G} \to G$. The other surjections have been covered earlier in this section. We now prove statements (i) to (iv).

(i) Follows from Theorems 2.5 and 2.22.

(ii) Easy exercise.

(iii) Immediate from the definitions.

(iv) Follows from Theorem 2.16 Lemma 2.17 and facts (7) and (8) above. \(\square\)

3. The $p$-primary parts of $\mathfrak{g}(K/k)$ and $H^1(k, \text{Pic} \overline{X})$

In this section, we prove Theorems 1.1, 1.2 and 1.3. In what follows, $K/k$ denotes an extension of number fields, $X$ denotes a smooth compactification of $R_{K/k}^1 \mathbb{G}_m$, $L/k$ denotes a Galois extension containing $K/k$, $G = \text{Gal}(L/k)$ and $H = \text{Gal}(L/K)$.

Lemma 3.1. Let $\phi : T_1 \to T_2$ be an isogeny of algebraic tori over $k$ giving rise to an exact sequence

$$1 \longrightarrow \mu \longrightarrow T_1 \overset{\phi}{\longrightarrow} T_2 \longrightarrow 1$$

of algebraic groups over $k$ such that $\mu$ is finite. Then for any prime $p$ such that $p \nmid |\mu(k)|$,

$$H^1(k, \text{Pic} \overline{X}_1)(p) \cong H^1(k, \text{Pic} \overline{X}_2)(p),$$

$$A(T_1)(p) \cong A(T_2)(p), \quad \text{and}$$

$$\text{III}(T_1)(p) \cong \text{III}(T_2)(p).$$

Proof. Let $d = |\mu(k)|$ and let $p$ be a prime such that $p \nmid d$. Then $\phi$ induces an injection of function fields $\phi^* : k(T_2) \hookrightarrow k(T_1)$ with $[k(T_1) : \phi^*k(T_2)] = d$ and hence a restriction map $\text{Br}_{nr}(k(T_2)/k) \to \text{Br}_{nr}(k(T_1)/k)$. The fact that $\text{Cor} \circ \text{Res} = [d]$ shows that the kernel of this map is killed by $d$. Thus we obtain an injection of finite groups $H^1(k, \text{Pic} \overline{X}_2)(p) \hookrightarrow H^1(k, \text{Pic} \overline{X}_1)(p)$. The dual isogeny $\psi$ yields an injection in the opposite direction, showing that the groups are isomorphic. Similarly, we have homomorphisms of finite groups

$$A(T_1) \overset{\phi}{\longrightarrow} A(T_2) \overset{\psi}{\longrightarrow} A(T_1) \overset{\phi}{\longrightarrow} A(T_2)$$

where $\psi \circ \phi$ is the map $x \mapsto x^d$ on $A(T_1)$ and $\phi \circ \psi$ is the map $x \mapsto x^d$ on $A(T_2)$. Therefore, the induced injections $A(T_1)(p) \hookrightarrow A(T_2)(p)$ and $A(T_2)(p) \hookrightarrow A(T_1)(p)$ are isomorphisms. Likewise, $\phi$ and $\psi$ induce maps $\text{III}(T_1) \to \text{III}(T_2)$ and $\text{III}(T_2) \to \text{III}(T_1)$ whose kernels are killed by $d$. \(\square\)
Proof of Theorem 1.1. Let $S$ be the kernel of $N_{K_p/K}: R_{K_p/k}G_m \to R_{K/k}G_m$ and let $i: S \to R_{K_p/k}G_m$ be the inclusion. Then the following diagram with exact rows commutes:

$$
\begin{array}{cccccc}
1 & \rightarrow & S & \overset{i}{\rightarrow} & R_{K_p/k}G_m & \overset{N_{K_p/K}}{\rightarrow} & R_{K/k}G_m & \rightarrow & 1 \\
1 & \rightarrow & S & \overset{i}{\rightarrow} & R_{K_p/k}G_m & \overset{N_{K_p/K}}{\rightarrow} & R_{K/k}G_m & \rightarrow & 1.
\end{array}
$$

Let $d = [K_p : K]$ and let $[d]$ denote the map $x \mapsto x^d$. The natural inclusion $j: R_{K/k}G_m \to R_{K_p/k}G_m$ satisfies $N_{K_p/K} \circ j = [d]$. Using $i$ and $j$, we obtain a surjective morphism

$$S \times R_{K/k}G_m \to R_{K_p/k}G_m$$

whose kernel $\mu$ is finite for dimension reasons. Moreover, since $N_{K_p/K} \circ j = [d]$, $\mu$ is killed by $d$. Let $Z$, $W$ and $W_p$ be smooth compactifications of $S$, $R_{K/k}G_m$ and $R_{K_p/k}G_m$, respectively. Since $Z$ and $W$ are $k$-rational, $\text{Pic}(Z \times W) = \text{Pic}Z \oplus \text{Pic}W$. Thus, Lemma 3.1 yields

$$H^1(k, \text{Pic}Z(p)) \oplus H^1(k, \text{Pic}W(p)) = H^1(k, \text{Pic}W_p(p)).$$

Furthermore, $R_{K/k}G_m$ and $R_{K_p/k}G_m$ are $k$-rational so $H^1(k, \text{Pic}W) = H^1(k, \text{Pic}W_p) = 0$ and hence $H^1(k, \text{Pic}Z(p)) = 0$. Now the result follows from applying Lemma 3.1 to the surjective morphism

$$S \times R_{K/k}G_m \to R_{K_p/k}G_m$$

whose finite kernel is killed by $d$. 

We can now prove Theorem 1.2.

Proof of Theorem 1.2. (i) Follows from Theorem 1.1 and Proposition 2.9

(ii) Follows from Lemma 2.6

Corollary 3.2. If $H$ is a Hall subgroup of $G$, then

$$H^1(k, \text{Pic}X) \cong \prod_{p \mid |H|} H^3(G, Z(p)),
\mathfrak{R}(K/k) \cong \prod_{p \mid |H|} \mathfrak{R}(L/k)(p), \quad \text{and}
A(T) \cong \prod_{p \mid |H|} A(T_0)(p),$$

where $T = R_{K/k}G_m$ and $T_0 = R_{L/k}G_m$.

Proof. Follows immediately from Theorems 1.1 and 1.2 and Lemma 2.6

Proposition 3.3. If $H$ is a Hall subgroup of $G$ then $\mathfrak{F}(L/K/k) = \mathfrak{F}(G, H) = 0$.

Proof. The focal subgroup theorem [30] shows that for a Hall subgroup $H$ of $G$, we have $\mathfrak{F}(G, H) = 0$. Now recall that $\mathfrak{F}(G, H) \to \mathfrak{F}(L/K/k)$.
Taking the $G$-cohomology of the exact sequence
\[ 0 \to \mathbb{Z} \to \mathbb{Z}[G/H] \to J_{G/H} \to 0 \]
gives a long exact sequence, from which one can form the following commutative diagram of abelian groups (wherein the vertical maps are restriction maps and $S \subset \Omega_k$ is a set of places of $k$):

\[
\begin{array}{cccc}
\text{H}^2(G, \mathbb{Z}) & \xrightarrow{\psi_1} & \text{H}^2(G, \mathbb{Z}[G/H]) & \xrightarrow{\psi_2} & \text{H}^2(G, J_{G/H}) & \xrightarrow{\psi_3} & \text{H}^3(G, \mathbb{Z}) \\
\alpha_1 \downarrow & & \alpha_2 \downarrow & & \alpha_3 \downarrow & & \\
\prod_{v \in S} \text{H}^2(D_v, \mathbb{Z}) & \xrightarrow{\psi_1} & \prod_{v \in S} \text{H}^2(D_v, \mathbb{Z}[G/H]) & \xrightarrow{\psi_2} & \prod_{v \in S} \text{H}^2(D_v, J_{G/H}) & & \\
\end{array}
\] (9)

Our final task in this section is the proof of Theorem 1.3. We will need the following lemma:

**Lemma 3.4.** In the notation of diagram (9), we have

(i) $\alpha_2^{-1}(\text{Im} \psi_1)/\text{Im} \varphi_1 \cong \mathfrak{f}(L/K/k)$, if $S = \Omega_k$;

(ii) $\alpha_2^{-1}(\text{Im} \psi_1)/\text{Im} \varphi_1 \cong \mathfrak{f}(G, H)$, if $S$ is the set of unramified places of $L/k$.

**Proof.** In [41, Theorem 6.12] and pages leading to it, the authors show that the first square in (9) is dual to diagram (6) of Section 2.3, reproduced below:

\[
\begin{array}{cccc}
H/[H, H] & \xrightarrow{\psi_1} & G/[G, G] \\
\varphi_1 \downarrow & & \varphi_2 \downarrow \\
\bigoplus_{v \in S} (\bigoplus_{\pi \in G} H_v/[H_v, H_v]) & \xrightarrow{\psi_2} & \bigoplus_{v \in S} D_v/[D_v, D_v] \\
\end{array}
\] (10)

Therefore, by duality $\alpha_2^{-1}(\text{Im} \psi_1)/\text{Im} \varphi_1$ is isomorphic to $\ker \psi_1 / \varphi_1(\ker \psi_2)$. Assertion (i) now follows from Theorem 2.16. For (ii) note that when $S$ consists of only the unramified places of $L/k$, we have $\varphi_1(\ker \psi_2) = \varphi_1(\ker \psi_2^{nr})$ and, by Theorem 2.19 $\varphi_1(\ker \psi_2^{nr}) = \Phi^G(H)/[H, H]$. □

We are now ready to prove Theorem 1.3.

**Proof of Theorem 1.3.** (i) Let $T = R_{K/k}^1 G_m$ and recall that $\mathfrak{g}(K/k) = \text{III}(T)$. In the notation of diagram (9), Theorem 2.11 gives $\text{III}(T) \cong \ker \alpha_3$ and hence it is enough to show that $(\ker \alpha_3)_{(p)} \cong \mathfrak{g}(L/K/k)_{(p)}$. We omit this last step since it is analogous to what will be done in the proof of (ii).

(ii) By Theorem 2.8 $H^1(k, \text{Pic} X) = \text{III}^2_w(G, J_{G/H})$. Consider the version of diagram (9) where $S$ is the set of unramified places of $L/k$. In this case, the Chebotarev density theorem yields

\[ \ker \alpha_3 = \ker \left( H^2(G, J_{G/H}) \xrightarrow{\text{Res}} \prod_{g \in G} H^2(g, J_{G/H}) \right) = \text{III}^2_w(G, J_{G/H}). \]

Therefore, it suffices to prove that $(\ker \alpha_3)_{(p)} \cong \mathfrak{g}(G, H)_{(p)}$. Since $H^3(G, \mathbb{Z})_{(p)} = 0$, a diagram chase shows that $(\ker \alpha_3)_{(p)} \cong (\alpha_2^{-1}(\text{Im} \psi_1)/\text{Im} \varphi_1)_{(p)}$ via $\varphi_2$. Now apply Lemma 3.4(ii). □
4. USING SUBEXTENSIONS AND SUPEREXTENSIONS

As usual, throughout this section $k$ denotes a number field.

4.1. Hasse norm principle. In order to study the HNP in non-Galois extensions, it is often useful to be able deduce information about the knot group of an extension $K/k$ from information about its subextensions or superextensions, by which we mean extensions of $k$ containing $K$. In this section we collect some results that serve this purpose.

**Lemma 4.1.** Let $L/K/k$ be a tower of number fields. Then the knot group $\mathfrak{A}(K/k)$ is killed by $\exp(\mathfrak{A}(L/k)) \cdot [L : K]$.

**Proof.** Let $x \in k^* \cap N_{K/k} \mathbb{A}_K^*$. Let $d = [L : K]$ and $e = \exp(\mathfrak{A}(L/k))$. Then $x^d \in k^* \cap N_{L/k} \mathbb{A}_L^*$ and hence $x^{de} \in N_{L/k}L^* \subset N_{K/k}K^*$.

**Corollary 4.2.** Let $K/k$ be a finite extension and suppose that there are finite extensions $L_1, L_2, \ldots, L_r$ of $K$ such that

(i) the HNP holds for $L_i/k$ for $i = 1, 2, \ldots, r$;

(ii) $\gcd_{1 \leq i \leq r} ([L_i : K]) = 1$.

Then the HNP holds for $K/k$.

**Remark 4.3.** Lemma 4.1 and Corollary 4.2 also follow from Proposition 4.5 below.

**Corollary 4.4.** Let $L/K/k$ be a tower of number fields. If $\exp(\mathfrak{A}(L/k)) \cdot [L : K]$ is coprime to $[K : k]$, then the HNP holds for $K/k$.

**Proof.** This follows from Lemma 4.1 and the fact that $\mathfrak{A}(K/k)$ is killed by $[K : k]$.

The following result is a slight generalization of [28, Proposition 1] and will be very useful for us.

**Proposition 4.5.** Let $L/K/k$ be a tower of finite extensions and let $d = [L : K]$. Then the map $x \mapsto x^d$ induces a group homomorphism

$$\varphi : \mathfrak{A}(K/k) \to \mathfrak{A}(L/k)$$

with $\ker \varphi \subset \mathfrak{A}(K/k)[d]$ and $\{x^d \mid x \in \mathfrak{A}(L/k)\} \subset \operatorname{Im} \varphi$. In particular, if $|\mathfrak{A}(K/k)|$ is coprime to $d$, then $\varphi$ induces an isomorphism $\mathfrak{A}(K/k) \cong \{x^d \mid x \in \mathfrak{A}(L/k)\}$.

**Proof.** The statements follow from the inclusions $N_{L/k} \mathbb{A}_L^* \subset N_{K/k} \mathbb{A}_K^*$, $N_{L/k}L^* \subset N_{K/k}K^*$ and $(N_{K/k} \mathbb{A}_K^*)^d \subset N_{K/k} \mathbb{A}_L^*$. If $|\mathfrak{A}(K/k)|$ is coprime to $d$, then we have $\operatorname{Im} \varphi \subset \{x^d \mid x \in \mathfrak{A}(L/k)\}$.

**Corollary 4.6.** Let $L/K/k$ be a tower of number fields. If $p$ is a prime with $p \nmid [L : K]$ then

$$\mathfrak{A}(K/k)_{(p)} \cong \mathfrak{A}(L/k)_{(p)}$$

**Proof.** Proposition 4.5 shows that $x \mapsto x^d$ induces the desired isomorphism.
We finish this section by establishing a generalization of Gurak’s criterion (see [28 Proposition 2]) for the validity of the HNP in a compositum of two subextensions with coprime degrees.

**Proposition 4.7.** Let $L/k$ be a finite extension with subextensions $K/k$ and $M/k$ such that $L = KM$. Let $m = [L : M]$, $n = [L : K]$, $a = \exp(\mathfrak{R}(K/k))$, $b = \exp(\mathfrak{R}(M/k))$, and let $h = \gcd(m, n)$. Then

$$\varphi : \mathfrak{R}(K/k) \times \mathfrak{R}(M/k) \to \mathfrak{R}(L/k)$$

$$\varphi(x, y) = x^n y^m$$

satisfies $\text{Ker}\varphi \subset \mathfrak{R}(K/k)[bm] \times \mathfrak{R}(M/k)[am]$ and \{ $z^h | z \in \mathfrak{R}(L/k)$ \} $\subset \text{Im}\varphi$. Additionally, if $[K : k]$ and $[M : k]$ are coprime, then $\varphi$ is an isomorphism.

**Proof.** First, we prove the statement regarding $\text{Ker}\varphi$. Let $x \in k^* \cap N_{K/k}^* K$ and $y \in k^* \cap N_{M/k}^* M$ be such that $x^n y^m \in N_{L/k}^* L$. Since $y^b \in N_{M/k}^* M$, we have $y^{bm} \in N_{L/k}^* L$. Now, since $(x^n y^m)^b \in N_{L/k}^* L$, we have $x^{bm} \in N_{L/k}^* L \subset N_{K/k}^* K$. Likewise, $y^{bm} \in N_{L/k}^* L \subset N_{M/k}^* M$.

Next, we prove the statement regarding $\text{Im}\varphi$. Let $\alpha \in k^* \cap N_{L/k}^* L$. Then $\alpha \in k^* \cap N_{K/k}^* K$ and $\alpha^h \in \text{Im}\varphi$. Additionally, $\alpha^m \in \text{Im}\varphi$ and consequently $\alpha^h \in \text{Im}\varphi$.

Finally, suppose that $[K : k]$ and $[M : k]$ are coprime. Since $L = KM$, we have $[L : k] = mn$ and hence $m = [K : k]$ and $n = [M : k]$. In particular, $m$ and $n$ are coprime, so that $h = 1$ and $\varphi$ is surjective. Additionally, since the knot groups $\mathfrak{R}(K/k)$ and $\mathfrak{R}(M/k)$ are killed by $[K : k] = m$ and $[M : k] = n$, respectively, we have $a \mid m$ and $b \mid n$. Therefore, $\mathfrak{R}(K/k)[bm] \subset \mathfrak{R}(K/k)[n^2] = 1$. Likewise, $\mathfrak{R}(M/k)[am] \subset \mathfrak{R}(M/k)[m^2] = 1$. \hfill $\square$

4.2. **Weak approximation.** In this section we present several results regarding the validity of weak approximation for the norm one torus associated to an extension of number fields. These results are of a similar shape to the ones given in Section 4.1 and can be seen as weak approximation analogues of results for the HNP by Gurak and others. We start with an explicit description of the defect of weak approximation when the extension is Galois.

**Proposition 4.8.** Let $L/k$ be Galois with finite Galois group $G$ and let $T = R^1_{L/k} \mathbb{G}_m$. Then

$$A(T)^\sim = \text{Im} \left( H^3(G, \mathbb{Z}) \xrightarrow{\text{Res}} \prod_{v \in \Omega_k} H^3(D_v, \mathbb{Z}) \right)$$

where $D_v = \text{Gal}(L_v/k_v)$ is the decomposition group at $v$.

**Proof.** Follows from [41 Ex. 5.6] and the first isomorphism theorem. \hfill $\square$

The following proposition, which is the weak approximation analogue of Lemma 4.1, gives a useful result when studying weak approximation for norm one tori.

**Proposition 4.9.** Let $L/K/k$ be a tower of number fields, let $T_1 = R^1_{K/k} \mathbb{G}_m$ and $T_2 = R^1_{L/k} \mathbb{G}_m$. Then $A(T_1)$ is killed by $\exp(A(T_2)) \cdot [L : K]$. 
Proof. Let $d = [L : K]$ and let $e = \exp(A(T_2))$. The natural inclusion $i : T_1 \to T_2$ and the norm map $N_{L/K} : T_2 \to T_1$ induce homomorphisms

$$A(T_1) \xrightarrow{i} A(T_2) \xrightarrow{N_{L/K}} A(T_1)$$

whose composition is $x \mapsto x^d$. Let $x \in A(T_1)$. Then $x^{de} = N_{L/K}(i(x)^e) = 1$, since $e$ kills $A(T_2)$. \hfill \Box

As a consequence of this result, we obtain the following weak approximation analogues of Corollary 4.2 and \cite[Proposition 2]{28}, respectively.

\begin{corollary}
Let $K/k$ be a finite extension and suppose that there are finite extensions $L_1, L_2, \ldots, L_r$ of $K$ such that

\begin{enumerate}[(i)]
  \item weak approximation holds for $T_i = R^1_{L_i/k}G_m$ for $i = 1, 2, \ldots, r$;
  \item $\gcd([L_i : K]) = 1$.
\end{enumerate}

Then weak approximation holds for $T = R^1_{K/k}G_m$.

\end{corollary}

\textbf{Proof.} Follows immediately from Proposition 4.9. \hfill \Box

\begin{corollary}
Let $L/K/k$ be a tower of number fields such that $\gcd([L : K], [K : k]) = 1$. If weak approximation holds for $R^1_{L/k}G_m$, then weak approximation holds for $R^1_{K/k}G_m$.

\end{corollary}

\textbf{Proof.} Follows from Theorem 2.5, Lemma 2.6 and Proposition 4.9. \hfill \Box

We now establish a weak approximation analogue of Proposition 4.7.

\begin{proposition}
Let $L/k$ be a finite extension with subextensions $K/k$ and $M/k$ such that $L = KM$. Let $T = R^1_{L/k}G_m$, $T_1 = R^1_{K/k}G_m$ and $T_2 = R^1_{M/k}G_m$. If $[K : k]$ and $[M : k]$ are coprime, then

$$A(T) \cong A(T_1) \times A(T_2)$$

and, in particular, weak approximation holds for $T$ if and only if it holds for $T_1$ and $T_2$.

\end{proposition}

\textbf{Proof.} Let $p$ be a prime. Note that $p$ divides at most one of $[K : k]$ and $[M : k]$. First suppose that $p \nmid [M : k]$. Let $d = [M : k] = [L : K]$. As in the proof of Theorem 4.7, we obtain an isogeny $\phi : S \times T_1 \to T$ whose kernel $\mu$ is killed by $d$, and where the torus $S$ has a smooth compactification $\overline{Z}$ with $H^1(k, \Pic \overline{Z})_{(p)} = 0$. Now Theorem 2.5 implies that $A(S)_{(p)} = 0$. Therefore, Lemma 3.1 shows that $A(T)_{(p)} \cong A(T_1)_{(p)}$ for all primes $p$ such that $p \nmid [M : k]$. If $p \mid [M : k]$ then $p \mid [K : k]$ and a similar argument shows that $A(T)_{(p)} \cong A(T_2)_{(p)}$. So

$$A(T) \cong \prod_{p \mid d} A(T_1)_{(p)} \times \prod_{p \mid d} A(T_2)_{(p)}.$$ 

Now Theorem 2.5 and Lemma 2.6 show that $\prod_{p \mid d} A(T_2)_{(p)} = A(T_2)$ and $\prod_{p \mid d} A(T_1)_{(p)} = A(T_1)$. \hfill \Box

We end this section by proving a version of \cite[Theorem 1]{28} for weak approximation in nilpotent Galois extensions. We require the following weak approximation version of \cite[Lemma 2.3]{27}:
**Lemma 4.13.** Let $K/k$ and $M/k$ be finite subextensions of $L/k$ such that $[K : k]$ and $[M : k]$ are coprime. Then weak approximation holds for $R_{K/k}^1 \mathbb{G}_m$ if and only if it holds for $R_{K/k}^1 \mathbb{G}_m$.

**Proof.** Let $T = R_{K/k}^1 \mathbb{G}_m$, $T_M = T \times_k M$ and $T_K = T \times_k K$. If weak approximation holds for $T$ then it holds for $R_{K/k}^1 \mathbb{G}_m = T_M$. Now suppose that weak approximation holds for $T_M$. By Lemma 2.3, weak approximation holds for $T_K$. To complete the proof, observe that weak approximation for $T$ and $T_M$ implies weak approximation for $R_{K/k}^1 \mathbb{G}_m$.

**Proposition 4.14.** Let $L/k$ be a Galois extension such that $G = \text{Gal}(L/k)$ is nilpotent. For every prime $p$, let $G_p$ be a Sylow $p$-subgroup of $G$. Let $k_p$ and $L_p$ be the fixed fields of the subgroups $G_p$ and $\prod_{q \neq p} G_q$, respectively. The following are equivalent:

(i) Weak approximation holds for $R_{L/k}^1 \mathbb{G}_m$.

(ii) Weak approximation holds for each $R_{L_p/k}^1 \mathbb{G}_m$.

(iii) Weak approximation holds for each $R_{L/k_p}^1 \mathbb{G}_m$.

**Proof.** (i) $\implies$ (iii) Follows from Corollary 4.11

(iii) $\implies$ (i) We prove $A(R_{L/k}^1 \mathbb{G}_m) = 0$ for every prime $p$. Consider the commutative diagram

$$
\begin{array}{ccc}
H^3(G, \mathbb{Z})_p & \longrightarrow & \prod_{v \in \Omega_k} H^3(D_v, \mathbb{Z})_p \\
\downarrow \text{Res}_4 & & \downarrow \text{Res}_2 \\
H^3(G_p, \mathbb{Z}) & \longrightarrow & \prod_{v \in \Omega_k} H^3(D_v^p, \mathbb{Z})
\end{array}
$$

where $D^p_v = G_p \cap D_v$ is a decomposition group of $L/k_p$ at $v$. Since weak approximation holds for $R_{L/k_p}^1 \mathbb{G}_m$, Proposition 4.8 yields $\text{Im Res}_3 = 0$. Furthermore, Proposition 2.1 shows that $\text{Res}_2$ is injective. It follows that $\text{Im Res}_1 = 0$, which implies that $A(R_{L/k}^1 \mathbb{G}_m) = 0$ by Proposition 4.8. □

**Remark 4.15.** We note that the implication (iii) $\implies$ (i) in Proposition 4.14 does not require the hypothesis that $G$ is nilpotent. This is analogous to the corresponding result for the HNP (see Gurak's remarks preceding [28, Theorem 2]).

**Remark 4.16.** Let $L/k$ be a finite abelian extension. A consequence of [20, Lemma 6.7] is that weak approximation for $R_{L/k}^1 \mathbb{G}_m$ implies weak approximation for $R_{K/k}^1 \mathbb{G}_m$, where $K/k$ is any subextension of $L/k$. Conversely, Proposition 4.14 shows that if weak approximation holds for $R_{K/k}^1 \mathbb{G}_m$ for every
subextension $K/k$ of $L/k$ of maximal prime power degree, then weak approximation holds for $R^1_{L/k} \mathbb{G}_m$. This result can be seen as the weak approximation version of $[12, \text{Theorem 2}].$

5. Applications to $A_n$ and $S_n$ extensions

In this section we apply the results of Sections 3 and 4 to study the HNP and weak approximation for norm one tori of $A_n$ and $S_n$ extensions. Throughout the section, we fix the following notation: $L/K/k$ is a tower of number fields such that $L/k$ is Galois and $G = \text{Gal}(L/k)$ is isomorphic to $A_n$ or $S_n$ with $n \geq 4$. We set $H = \text{Gal}(L/K)$. For any subgroup $G'$ of $G$, we denote by $F_{G/G'}$ a flasque module in a flasque resolution of the Chevalley module $J_{G/G'}$. We use Theorem 2.8 to identify $H^1(k, \text{Pic } \overline{X})$ with $H^1(G, F_{G/H}).$

5.1. Results for general $n$. First, we complete the proof of Theorem 1.7. For $G \cong A_n$ or $S_n$, we have $H^3(G, \mathbb{Z}) \cong \mathbb{Z}/2$, unless $G \cong A_6$ or $A_7$ in which case $H^3(G, \mathbb{Z}) \cong \mathbb{Z}/6$. Therefore, in our proof of Theorem 1.7 we can apply Theorem 1.3 to deal with the odd order torsion. It remains to analyze the $2$-primary parts of $\mathfrak{A}(K/k)$ and $H^1(G, F_{G/H})$. We start with the simpler case where $|H|$ is odd.

**Proposition 5.1.** If $|H|$ is odd, we have

(i) $\mathfrak{A}(K/k)(2) \cong \mathfrak{A}(L/k)(2) \hookrightarrow C_2$;

(ii) $H^1(G, F_{G/H})(2) \cong \mathbb{Z}/2$.

**Proof.** (i) This is a consequence of Corollary 4.6 and Theorem 2.11.

(ii) This follows from Theorem 1.2. $\square$

**Proof of Theorem 1.7 for $|H|$ odd.** We analyze the $p$-primary parts of the groups in Theorem 1.7 for each prime $p$. For $p$ odd, apply Theorem 1.3 and use the fact that $\mathfrak{A}(L/k) \hookrightarrow H^2(G, \mathbb{Z}) = \mathbb{Z}/2$ (Theorem 2.11). For $p = 2$, use Proposition 5.1. As $\mathfrak{A}(G, H)$ is a subquotient of $H \cap [G, G]$, and $|H|$ is odd, $\mathfrak{A}(G, H)(2) = 0$. Since $\mathfrak{A}(G, H)$ surjects onto $\mathfrak{A}(L/K/k)$, we also have $\mathfrak{A}(L/K/k)(2) = 0$. $\square$

We now solve the case where $|H|$ is even. For this, we will use the generalized representation group $\overline{G}$ of $G$, the projection map $\lambda$ and the base normal subgroup $K = \langle z \rangle$ presented in Proposition 2.4, so our next two results do not apply when $G \cong A_6$ or $A_7$.

**Lemma 5.2.** Suppose that $G$ is not isomorphic to $A_6$ or $A_7$ and that $|H|$ is even. Let $h \in H$ be any element of order 2. Then there exists a copy $A$ of $V_4$ inside $G$ such that

- $h \in A$;
- $z \in [\lambda^{-1}(A), \lambda^{-1}(A)]$.

**Proof.** Case 1) $h$ comprises a single transposition. Relabeling if necessary, we can assume that $h = (1 \ 2)$. Take $A = \langle (1 \ 2), (3 \ 4) \rangle$ and note that $[\lambda^{-1}((1 \ 2)), \lambda^{-1}((3 \ 4))] = [t_1, t_3]$ in the notation of Proposition 2.4. Using the relations satisfied by the elements $t_i \in \overline{G}$ given in Proposition 2.4 it is clear that this commutator is equal to $z$, as desired.

Case 2) $h$ comprises more than one transposition. Relabeling if necessary, we can assume that $h = (1 \ 2)(3 \ 4) \cdots (n - 1 \ n)$ for some even $n \geq 4$. Take $A = \langle h, x \rangle$, where $x = (1 \ 3)(2 \ 4)$ and...
let us prove by induction that \( z = [\lambda^{-1}(h), \lambda^{-1}(x)] \). Note that, in the notation of Proposition 2.4 we have \( h = t_1 t_3 \cdots t_{n-1} \) and \( x = t_2 t_1 t_2 t_3 t_2 t_3 \).

**Base case** \( n = 4 \): A straightforward (but long) computation using the relations satisfied by the elements \( t_i \) given in Proposition 2.4 shows that \( [\lambda^{-1}(h), \lambda^{-1}(x)] = [t_1 t_3, t_2 t_1 t_2 t_3 t_2 t_3] = z \).

**Inductive step:** Suppose that \( h = (1 \ 2)(3 \ 4) \cdots (n - 1 \ n)(n + 1 \ n + 2) \). Denoting the permutation \((1 \ 2)(3 \ 4) \cdots (n - 1 \ n)\) by \( \tilde{h} \), write \( h = \tilde{h} t_{n+1} \). Now

\[
[\lambda^{-1}(h), \lambda^{-1}(x)] = [\lambda^{-1}(\tilde{h}) t_{n+1}, \lambda^{-1}(x)] = [\lambda^{-1}(\tilde{h}), \lambda^{-1}(x)] t_{n+1} t_{n+1}, \lambda^{-1}(x)].
\]

By the inductive hypothesis and the relations of Proposition 2.4 \( [\lambda^{-1}(\tilde{h}), \lambda^{-1}(x)] t_{n+1} t_{n+1} = z t_{n+1} = z \) and \( t_{n+1}, \lambda^{-1}(x)] = [t_{n+1}, t_2 t_1 t_2 t_3 t_2 t_3] = 1 \), as desired.

The next proposition completes the proof of Theorem 1.7.

**Proposition 5.3.** Suppose that \( G \) is not isomorphic to \( A_6 \) or \( A_7 \) and that \( |H| \) is even. Then

(i) \( \mathfrak{H}(K/k) \cong \mathfrak{H}(L/K/k) \);

(ii) \( H^1(G, F_{G/H}) \cong \mathfrak{H}(G, H) \).

**Proof.** (i) Let \( A \) be the copy of \( V_4 \) constructed in Lemma 5.2. By Theorem 2.13 in order to prove that \( \mathfrak{H}(K/k) \cong \mathfrak{H}(L/K/k) \) it is enough to show the following two assertions:

(a) The HNP holds for \( L^{A \cap H}/L^A \);

(b) \( \text{Cor}^G_A : \hat{H}^{-3}(A, \mathbb{Z}) \to \hat{H}^{-3}(G, \mathbb{Z}) \) is surjective.

Statement [a] is clear because \( L^{A \cap H}/L^A \) is at most quadratic. Now we prove [b]. Applying Lemma 2.3 and using the generalized representation group of Proposition 2.4 yields

\[
\text{Im} (\text{Cor}^G_A) \cong K \cap [\lambda^{-1}(A), \lambda^{-1}(A)] = \langle z \rangle \cap [\lambda^{-1}(A), \lambda^{-1}(A)] = \langle z \rangle.
\]

(ii) By Theorems 2.8 and 2.22 it is enough to show that \( \mathfrak{H}(G, H) \cong \mathfrak{H}(G, H) \). By Proposition 2.4 it suffices to show that \( \text{Ker} \lambda \subset \Phi^{-2}(H) \), i.e. that \( z \in \Phi^{-2}(H) \). Let \( A = \langle h, x \rangle \) be the copy of \( V_4 \) constructed in the proof of Lemma 5.2. Then \( h \in H \cap x H x^{-1} \) and therefore \( z = [\lambda^{-1}(h), \lambda^{-1}(x)] \in \Phi^{-2}(H) \), as desired.

Now that we have proved Theorem 1.7 we have reduced the study of the HNP and weak approximation for norm one tori of \( A_n \) and \( S_n \) extensions to a purely computational problem (except in the cases of \( A_6 \) and \( A_7 \)). The groups \( \mathfrak{H}(L/K/k) \) and \( \mathfrak{H}(L/k) \) can be computed using the GAP algorithms described in Remark 2.20 and at the end of Section 5.2 below. The calculations of the knot group and of \( H^1(k, \text{Pic} X) \) in the remaining cases where \( G \cong A_6, A_7 \) are done in Section 5.3.

**Remark 5.4.** The method employed in this section to provide explicit and computable formulae for the knot group and fundamental invariant \( H^1(k, \text{Pic} X) \) in \( A_n \) and \( S_n \) extensions works for other families of extensions. For example, let \( G' \) be any finite group such that \( H^3(G', \mathbb{Z}) = \mathbb{Z}/2 \). Embed \( G' \) into \( S_n \) for some \( n \) and suppose that \( G' \) contains a copy of \( V_4 \) conjugate to \( \langle (1, 2)(3, 4), (1, 3)(2, 4) \rangle \).
For such a group $G'$, analogues of Lemma 5.2 and Propositions 5.1 and 5.3 yield a systematic approach to the study of the HNP and weak approximation for $G'$-extensions.

We proceed by investigating the possible isomorphism classes of the finite abelian group $\Phi(G, H)$ (and thus, by Theorems 1.7 and 2.8 of the invariant $H^1(G, F_{G/H})$ as well).

**Theorem 5.5.** The group $\Phi(S_n, H)$ is either trivial or an elementary abelian 2-group. Moreover, every elementary abelian 2-group occurs as $\Phi(S_n, H)$ for some $n$ and some $H \leq S_n$.

**Proof.** It suffices to prove that for every element $h \in H \cap [S_n, S_n]$, we have $h^2 \in \Phi^{S_n}(H)$. This is clear from the definition of $\Phi^{S_n}(H)$ because $h$ is conjugate to its inverse in $S_n$. The statement on the occurrence of every elementary abelian 2-group is shown in Proposition 5.7 below.

**Theorem 5.6.** The group $\Phi(A_n, H)$ is either trivial, isomorphic to $C_3$, or an elementary abelian 2-group. Moreover, every such possibility is realised for some choice of $n$ and $H$.

**Proof.** First, we claim that any element of even order in $\Phi(A_n, H)$ is 2-torsion. Let $h \in H$ have even order. By [26], $h$ is $A_n$-conjugate to $h^{-1}$. Therefore $h^2 \in \Phi^{A_n}(H)$, which proves the claim.

Next, we claim that any element of odd order in $\Phi(A_n, H)$ is 3-torsion. Let $h \in H$ be such that its image in $\Phi(A_n, H)$ has odd order. Replacing $h$ by a suitable power, we may assume that $h$ itself has odd order, whereby $h$ is $S_n$-conjugate to $h^2$. By the pigeonhole principle, at least two of the three $S_n$-conjugate elements $h, h^{-1}, h^2$ are $A_n$-conjugate. Therefore, at least one of $h^{-2}, h, h^3$ is in $\Phi^{A_n}(H_p)$. Since $h$ has odd order, we conclude that in all cases $h^3 \in \Phi^{A_n}(H_p)$, whence the claim.

Next, we show that $\Phi(A_n, H)_{(3)}$ is cyclic. Theorems 1.1 and 1.7 yield $\Phi(A_n, H)_{(3)} = \Phi(A_n, H_3)$, where $H_3$ denotes a Sylow 3-subgroup of $H$. Suppose for contradiction that the images in $\Phi(A_n, H_3)$ of $h_1, h_2 \in H_3$ generate a copy of $C_3 \times C_3$. Since $h_1, h_2 \in H_3$, the lengths of the cycles making up $h_1$ and $h_2$ are powers of 3, say $3^{i_1} \leq 3^{i_2} \leq \cdots \leq 3^{i_k}$ for $h_1$ and $3^{s_1} \leq 3^{s_2} \leq \cdots \leq 3^{s_l}$ for $h_2$, where $k, l \geq 1$ and $r_i, s_j \in \mathbb{Z}_{\geq 0}$. Note that $h_1$ and $h_1^{-1}$ cannot be $A_n$-conjugate, or else we would have $h_1^2 \in \Phi^{A_n}(H_3)$, and similarly for $h_2$. The criterion [26] for an element of $A_n$ to be conjugate to its inverse yields $3^{r_i} \neq 3^{r_j}$ and $3^{s_i} \neq 3^{s_j}$ for $i \neq j$.

The trivial case $\Phi(A_n, H)_{(3)} = 0$ is realised by taking $H = 1$. One can compute (using GAP, for example) that $\Phi(A_{12}, H) \cong C_3$ for $H = \langle (1, 2, 3)(4, 5, 6, 7, 8, 9, 10, 11, 12) \rangle$. The statement on the occurrence of every elementary abelian 2-group is shown in Proposition 5.7 below.

**Proposition 5.7.** For every $k \geq 0$, there exists $n$ and a subgroup $H$ of $A_n$ such that $\Phi(A_n, H)_{(2)} \cong \Phi(S_n, H)_{(2)} \cong C_2^k$. 
Proof. The case \( k = 0 \) is realised by letting \( H = 1 \). From now on, assume that \( k \geq 1 \). Let \( H \) be generated by \( k \) commuting and even permutations of order 2 such that, for any \( x, y \in H \) with \( x \neq y \), the permutations \( x \) and \( y \) have distinct cycle structures. We define such a group recursively as \( H = H_k \), starting from \( H_1 = \langle (1, 2)(3, 4) \rangle \), \( H_2 = \langle (1, 2)(3, 4), (5, 6)(7, 8)(9, 10)(11, 12) \rangle \) and adding, at step \( i \), a new generator \( h_i \) such that:

- \( h_i \) is an even permutation of order 2;
- \( h_i \) is disjoint to the previous generators \( h_1, \ldots, h_{i-1} \);
- \( h_i \) moves enough points so that its product with any element of \( H_{i-1} \) has cycle structure different from that of any element of \( H_{i-1} \).

Let \( n \) be large enough so that \( H \subset A_n \). It is straightforward to check that one then has \( \Phi^{A_n}(H) = \Phi^{S_n}(H) = 1 \). Therefore, \( \mathfrak{F}(A_n, H) = H \cap [A_n, A_n] = H \cong C_2^k \) and similarly for \( \mathfrak{F}(S_n, H) \).

As a consequence of the work done so far, we can now establish Theorem 1.4.

Proof of Theorem 1.4. For \( G \neq A_6 \) or \( A_7 \) the results follow from Theorems 1.7, 5.3, and 5.6. For the \( A_6 \) and \( A_7 \) cases, we describe how to compute \( H^1(k, \text{Pic} \mathcal{X}) \) in Section 5.2 – the results of these computations are in Tables 5 and 6 of the Appendix and the \( C_3 \) and \( C_6 \) cases occur therein.

The next lemma will aid our characterization of the existence of elements of order 3 in \( \mathfrak{F}(A_n, H) \).

Lemma 5.8. Let \( n = 3^l \) for some \( l \geq 0 \) and let \( \rho = (a_1 \cdots a_{3^l}) \) be a \( 3^l \)-cycle in \( S_n \). Let \( j \in \mathbb{Z} \) with \( j \equiv -1 \pmod 3 \). Then \( \rho^j \) is \( A_n \)-conjugate to \( \rho \) if and only if \( l \) is even.

Proof. Observe that \( \rho^j(a_i) = a_{i+j} \), where the subscripts are considered modulo \( 3^l \). Therefore, the permutation \( x \in S_n \) defined by \( x(a_i) = a_{i+(i-1)j} \) satisfies \( x^j \rho x^{-1} = \rho^j \). Let \( C \) be the \( A_n \)-conjugacy class of \( \rho \). Since the \( S_n \)-conjugacy class of \( \rho \) splits as a disjoint union \( C \sqcup gCg^{-1} \) for any \( g \in S_n \setminus A_n \), it is enough to show that \( x \in A_n \) if and only if \( l \) is even. We study the cycle structure of \( x \) by analyzing the fixed points of its powers. Observe that \( x^t(a_i) = a_{i+(i-1)j}^t \) for every \( t \geq 0 \) and so

\[
x^t(a_i) = a_i \iff 1 + (i-1)j^t \equiv i \pmod {3^l} \iff (i-1)(j^t-1) \equiv 0 \pmod {3^l}.
\]

Therefore, the number of fixed points of \( x^t \) is \( \gcd(3^l, j^t-1) \). Using this fact, we note two useful properties of the cycles occurring in a disjoint cycle decomposition of \( x \):

(i) The only cycle of \( x \) with odd length corresponds to the fixed point \( a_1 \): It suffices to show that, for odd \( t \geq 1 \), the only fixed point of \( x^t \) is \( a_1 \). As \( j \equiv -1 \pmod 3 \), it is easy to see that \( j^t \equiv 1 \pmod 3 \) for odd \( t \) and thus \( \gcd(3^l, j^t-1) = 1 \).

(ii) \( x \) does not contain a cycle with length divisible by 4: It is enough to prove that, for any \( m \geq 1 \), the number of fixed points of \( x^{4m} \) and \( x^{2m} \) coincide, i.e. that \( \gcd(3^l, j^{4m} - 1) = \gcd(3^l, j^{2m} - 1) \). This is clear since \( j^{4m} - 1 = (j^{2m} - 1)(j^{2m} + 1) \) and \( j^{2m} + 1 \equiv 0 \pmod 3 \).

Let \( c_1 \cdots c_k \) be a disjoint cycle decomposition of \( x \) where the cycle \( c_i \) has length \( |c_i| \). By (i) and (ii) we may assume that \( |c_1| = 1 \) and \( |c_i| \equiv 2 \pmod 4 \) for all \( i \geq 2 \). Note that \( x \in A_n \) if and only if \( k \) is odd. Now \( 3^l = \sum_i |c_i| \equiv 1 + \sum_{i \geq 2} 2 \pmod 4 \). Thus, \( x \in A_n \) if and only if \( 3^l \equiv 1 \pmod 4 \). \( \square \)
**Proposition 5.9.** There exists $H \leq A_n$ such that $\mathfrak{F}(A_n, H)(3) \cong C_3$ if and only if $n \geq 5$ and $n = \sum_{i=1}^{k} 3^{r_i}$ with $0 \leq r_1 < \cdots < r_k$ and $|\{i \mid r_i \text{ is odd}\}|$ is odd.

**Proof.** Suppose that $\mathfrak{F}(A_n, H)(3) \cong C_3$. It is easy to check that $\mathfrak{F}(A_4, H)(3) = 0$ for all $H \leq A_4$ so $n \geq 5$. By Theorems 1.1 and 1.7, $\mathfrak{F}(A_n, H)(3) \cong C_3$ is equivalent to $\mathfrak{F}(A_n, H_3) \cong C_3$ for any 3-Sylow subgroup $H_3$ of $H$. Let $h \in H_3 \setminus \Phi^{A_n}(H_3)$. Suppose that the lengths of the cycles making up $h$ are $3^{r_1} \leq \cdots \leq 3^{r_k}$ with $r_i \in \mathbb{Z}_{\geq 0}$. If $h$ were $A_n$-conjugate to $h^{-1}$ then we would obtain $h \in \Phi^{A_n}(H_3)$, a contradiction. Therefore, by criterion 20 we have $3^{r_i} \neq 3^{r_j}$ for $i \neq j$ and $\sum_{i=1}^{k} \frac{2^{r_i} - 1}{2}$ is odd, i.e. the number of odd $r_i$ is odd.

Conversely, assume that $n \geq 5$ is equal to $\sum_{i=1}^{k} 3^{r_i}$ with $r_1 < r_2 < \cdots < r_k$ and $|\{i \mid r_i \text{ is odd}\}|$ odd and let $H$ be the cyclic group of order $3^k$ generated by $h$, where

$$h = (1 \cdots 3^{r_1})(3^{r_1} + 1 \cdots 3^{r_1} + 3^{r_2}) \cdots (\sum_{i=1}^{k-1} 3^{r_i} + 1 \cdots n).$$

We will prove that $\mathfrak{F}(A_n, H)(3) \cong C_3$. By Theorem 5.6 it is enough to show that $h \notin \Phi^{A_n}(H)$. Observe that $\Phi^{A_n}(H)$ is generated by elements of the form $h^{s-t}$ where $h^s$ is $A_n$-conjugate to $h^t$.

We complete the proof by showing that $\Phi^{A_n}(H) \subset \langle h^3 \rangle$. Suppose that $h^s$ is $A_n$-conjugate to $h^t$. We claim that $s \equiv t \pmod{3}$. Since conjugate elements have the same order, $3 \mid s$ if and only if $3 \mid t$. Now assume that $3 \nmid s$. Then $h^s$ generates $H$ and has the same cycle type as $h$ so, relabelling if necessary, we may assume that $s = 1$. Suppose for contradiction that $t \equiv -1 \pmod{3}$. For every $1 \leq i \leq k$, let $x_i \in S_n$ be such that $x_i$ only moves points appearing in $c_i$ and $x_i c_i x_i^{-1} = c_i'$. Then $x = x_1 \cdots x_k$ satisfies $xhx^{-1} = h^t$. Lemma 5.8 shows that $x_i \in A_n$ if and only if $r_i$ is even. Since $|\{i \mid r_i \text{ is odd}\}|$ is odd, $x \in S_n \setminus A_n$. This gives the desired contradiction as the $S_n$-conjugacy class of $h$ splits as a disjoint union $C \sqcup x C x^{-1}$ where $C$ denotes the $A_n$-conjugacy class of $h$. $\square$

**Remark 5.10.** For fixed $n$, it would be interesting to determine the list of isomorphism classes of $\mathfrak{F}(A_n, H)(2)$ or $\mathfrak{F}(S_n, H)(2)$ as $H$ ranges through the subgroups of $A_n$ or $S_n$, respectively. We give some observations regarding this problem without proof:

- One can restrict the focus to $A_n$ since $\mathfrak{F}(A_n, H)(2) \cong \mathfrak{F}(S_n, H)(2)$.
- One can assume that $H$ is a 2-group by Theorems 1.1 and 1.7.
- If $\mathfrak{F}(A_n, H)(2) \cong C_2^k$ for some $k \in \mathbb{Z}_{\geq 0}$, then $k \leq d(H)$, where $d(H)$ denotes the minimal number of generators of $H$; in particular, it follows that $k \leq \frac{n}{2}$.
- If $\tilde{H}$ is a subgroup of $H$ of index 2, then $|\mathfrak{F}(A_n, \tilde{H})(2)| \leq 2|\mathfrak{F}(A_n, H)(2)| \leq 4|\mathfrak{F}(A_n, H)(2)|$.
- If $\mathfrak{F}(A_{n_0}, H)(2) \cong C_2^k$ for some $n_0 \geq 1$ and $k \in \mathbb{Z}_{\geq 0}$, then $\mathfrak{F}(A_n, H)(2) \cong C_2^k$ for all $n \geq n_0$.
- One has $\mathfrak{F}(A_n, H)(2) \in \{1, C_2\}$ for all $n \leq 11$ and $H \leq A_n$ and $\mathfrak{F}(A_n, H)(2) \in \{1, C_2, C_2^2\}$ for $n = 12, 13, 14$ and all $H \leq A_n$.

### 5.2. Computational methods and results for small $n$. In this section we prove Theorems 1.9, 1.10 and 1.12. In order to prove Theorems 1.10 and 1.12 we must compute the groups $H^1(k, \text{Pic} X)$
where $X$ is a smooth compactification of the norm one torus $R^1_{K/k} \mathbb{G}_m$ and $K/k$ is contained in a Galois extension $L/k$ with $\text{Gal}(L/k) = G \cong S_4, S_5, A_4, A_5, A_6$ or $A_7$. One method to achieve this is via the isomorphism $H^1(k, \text{Pic} X) = H^1(G, F_{G/H})$ provided by Theorem 2.8 where $H = \text{Gal}(L/K)$.

In [33 §5], Hoshi and Yamasaki developed several algorithms in the computer algebra system GAP to construct flasque resolutions. Using this work, one can compute the invariant $H^1(G, F_{G/H})$ for low-degree field extensions, see e.g. [37 §4] for some examples. This computational method can also be used to prove Theorem 1.14.

Proof of Theorem 1.14. Note that an extension $K/k$ of degree $n$ is a $(G, H)$-extension (as defined on p. 3), where $G$ is a transitive subgroup of $S_n$ and $H$ is an index $n$ subgroup of $G$. Since there are a finite number of possibilities for $G$ and $H$, one can compute all possibilities for $H^1(G, F_{G/H})$ using the aforementioned algorithms. If $H^1(G, F_{G/H}) = 0$, then both the HNP for $K/k$ and weak approximation for $R^1_{K/k} \mathbb{G}_m$ hold by Theorems 2.5 and 2.8. If $H^1(G, F_{G/H}) \neq 0$, one can compute the integer $\alpha(G)$ of Malle’s conjecture and for every such case one obtains $\alpha(G) > 1$. Thus, if the conjecture holds, then the number of degree $n$ extensions with discriminant bounded by $X$ and for which the HNP or weak approximation fails is $o(X)$. The result then follows by observing that Malle’s conjecture also implies that the number of degree $n$ extensions of $k$ with discriminant bounded by $X$ is asymptotically at least $c(k, n)X$ for some positive constant $c(k, n)$. 

Remark 5.11. We list a few observations about Theorem 1.14 and its proof.

(i) The reason for excluding degrees $n = 8$ and 12 is that in these cases there are pairs $(G, H)$, where $G \leq S_n$ is a transitive subgroup and $H$ is an index $n$ subgroup of $G$, such that $H^1(G, F_{G/H})$ is non-trivial and $\alpha(G) = 1$. A more detailed analysis of the proportion of these $(G, H)$-extensions for which the local-global principles fail is needed in these cases.

(ii) Computing the values of $\alpha(G)$ for all transitive subgroups $G$ of $S_n$ with $H^1(G, F_{G/H}) \neq 0$ and $[G : H] = n$ yields an upper bound (conditional on Malle’s conjecture) on the number of degree $n$ extensions for which the HNP (or weak approximation for the norm one torus) fails. For example, the number of degree 14 extensions of $k$ for which the HNP (or weak approximation for the norm one torus) fails is $\ll_{k, \epsilon} x^{\frac{9}{8} + \epsilon}$, when ordered by discriminant.

(iii) In the statement of Theorem 1.14 it suffices to assume Malle’s conjecture only for the few transitive subgroups $G \leq S_n$ containing an index $n$ subgroup $H$ such that $H^1(G, F_{G/H})$ is not trivial. Indeed, the assumption for all $G \leq S_n$ was used solely to show that the number of degree $n$ extensions of $k$ with discriminant bounded by $X$ is $\gg_{k, n} X$. For $n \leq 15$ composite, one can use an argument similar to that of [18 pp. 723–724] for $n$ even and the results of Datskovsky and Wright [14] for cubics and of Bhargava, Shankar and Wang [7] for quintics to prove the aforementioned result. Finally, for $n$ prime we do not need any assumptions as the HNP for $K/k$ and weak approximation for $R^1_{K/k} \mathbb{G}_m$ always hold for extensions of prime degree (see [13 Proposition 9.1 and Remark 9.3]).

(iv) To simplify the statement we only presented results for degree $n \leq 15$ but one can obtain results for higher degrees in a similar way. However, Hoshi and Yamasaki’s algorithms require
one to embed the Galois group \( G \) as a transitive subgroup of \( S_n \), whereupon one quickly reaches the limit of the databases of such groups stored in computational algebra systems such as GAP. To overcome this problem, one can employ a modification of Hoshi and Yamasaki’s algorithms written by the first author and made available at [36].

For most of our computational results, we did not employ the algorithms of Hoshi and Yamasaki and instead used the formula of Theorem 2.22 which expresses \( H^1(k, \text{Pic } X) \) in terms of generalized representation groups of \( G \) and \( H \). We implemented this formula, along with the simplification afforded by Theorem 1.1 as an algorithm in GAP (see [36]). For the groups \( G \) of Theorem 1.9, our calculations were further simplified thanks to Theorem 1.7. The outcome of our computations appears in Tables 1 – 6 of the Appendix. Theorems 1.10 and 1.12 follow immediately.

It is noteworthy to compare the two computational methods described above. The approach based on Theorem 2.22 involves the computation of the focal subgroup \( \Phi^G(H) \), which is generally fast for small subgroups \( H \) but impractical for large ones. On the contrary, Hoshi and Yamasaki’s method using flasque resolutions deals only with the \( G \)-module \( J_{G/H} \), whose \( \mathbb{Z} \)-rank \( \frac{|G|}{|H|} - 1 \) decreases as \( |H| \) grows. Therefore this technique (or the modified version available at [36]) is usually preferable when \( H \) is large. In general, a combination of the two algorithms is the most convenient way to compute \( H^1(k, \text{Pic } X) \) for all subgroups of a fixed group \( G \).

We now move on to the proof of Theorem 1.9. We use Theorem 1.7 to reduce our task to the calculation of the first obstruction \( \mathfrak{F}(L/K/k) \) and the knot group \( \mathfrak{K}(L/k) \) for the Galois extension \( L/k \). The former is achieved using the algorithm described in Remark 2.20. The computation of \( \mathfrak{K}(L/k) \) follows from a simple application of Theorem 2.11 together with Proposition 2.1 and Lemma 5.12 below. Note that if \( G = A_4, S_4, A_5 \) or \( S_5 \) then \( H^3(G, \mathbb{Z}) \cong \mathbb{Z}/2 \).

**Lemma 5.12.** Let \( G = A_4, S_4, A_5, S_5, A_6 \) or \( A_7 \) and let \( A \) be a copy of \( V_4 \) inside \( G \). Then

\[
\text{Res}^G_A : H^3(G, \mathbb{Z}) \to H^3(A, \mathbb{Z})
\]

is an isomorphism.

**Proof.** Follows from the injectivity of \( \text{Res}^{D_4}_{V_4} : H^3(D_4, \mathbb{Z}) \to H^3(V_4, \mathbb{Z}) \) and Proposition 2.1. \( \square \)

More generally, the knot group of a Galois extension \( L/k \) can be computed by combining Theorem 2.11 and Lemma 2.3. We used these two results to implement an algorithm (available at [36]) in GAP that, given the group \( \text{Gal}(L/k) \) and the list \( l \) of decomposition groups \( D_v \) at the ramified places, returns the knot group \( \mathfrak{K}(L/k) \). We end this subsection by proving Corollary 1.13.

**Proof of Corollary 1.13.** The isomorphisms \( \mathfrak{K}(K/k) \cong \mathfrak{K}(L/k) \) and \( \mathfrak{K}(L/k) \cong \mathfrak{K}(L/F) \) follow from Theorems 1.9 and 2.11. The statement about weak approximation follows from Lemma 4.13. \( \square \)

**5.3. The \( A_6 \) and \( A_7 \) Cases.** In this section we prove Theorem 1.11 and also give a complete characterization of weak approximation for the norm one tori associated to \( A_6 \) and \( A_7 \) extensions. Various subgroups of \( A_6 \) and \( A_7 \) are given by semidirect products of smaller subgroups. For brevity,
Proposition 5.13. If $L/k$ is Galois with Galois group $A_6$ or $A_7$, then $\mathfrak{S}(L/k) \hookrightarrow C_6$ and

- $\mathfrak{S}(L/k)_{(2)} = 1$ if and only if there exists a place $v$ of $k$ such that $V_4 \hookrightarrow D_v$;
- $\mathfrak{S}(L/k)_{(3)} = 1$ if and only if there exists a place $v$ of $k$ such that $C_3 \times C_3 \hookrightarrow D_v$.

Proof. This is an immediate consequence of Theorem 2.11, Proposition 2.1 and Lemma 5.12. □

We now solve the non-Galois case. As detailed in Section 5.2, we can compute the invariant $H^1(k, \text{Pic } X) = H^1(G, F_{G/H})$ of Theorems 2.5 and 2.8 for every possibility of $H = \text{Gal}(L/K)$. The result of this computation is given in Tables 5 and 6 of the Appendix and proves Theorem 5.12. Building upon the outcome of this computation, we establish multiple results on the knot group $\mathfrak{S}(K/k)$. Looking at Tables 5 and 6 we immediately see that the invariant $H^1(G, F_{G/H})$ is trivial if $H$ is isomorphic to $A_4$, $C_2 \times C_6$, $6$, $(C_6 \times C_2) \times C_2$, $S_4$, $A_4 \times C_3$, $A_5$, $(A_4 \times C_3) \times C_2$, $S_5$, $\text{PSL}(3, 2)$ or $A_6$. Thus, by Theorems 2.5 and 2.8 both groups $A(T)$ and $\mathfrak{S}(K/k)$ are trivial in all these cases.

Next, we investigate the cases where the first obstruction to the HNP for the tower $L/K/k$ coincides with the total obstruction (the knot group).

Proposition 5.14. If $6$ divides $|H|$, then $\mathfrak{S}(K/k) = \mathfrak{F}(L/K/k)$.

Proof. Let $G_1$ be a copy of $V_4$ inside $G$ such that $H \cap G_1 \neq 1$ and $G_2$ a copy of $C_3 \times C_3$ inside $G$ such that $H \cap G_2 \neq 1$. Set $H_i = H \cap G_i$ for $i = 1, 2$ and notice that the HNP holds for the extensions $L^{H_i}/L^{G_i}$ as they are of degree at most 3. Using Proposition 2.1, Lemma 5.12 and the duality between restriction and corestriction, we conclude that the maps $\text{Cor}^G_{G_1} : \hat{H}^{-3}(G_1, \mathbb{Z}) \to \hat{H}^{-3}(G, \mathbb{Z})_{(2)}$ and $\text{Cor}^G_{G_2} : \hat{H}^{-3}(G_2, \mathbb{Z}) \to \hat{H}^{-3}(G, \mathbb{Z})_{(3)}$ are surjective. Hence

$$\text{Cor}^G_{G_1} \oplus \text{Cor}^G_{G_2} : \hat{H}^{-3}(G_1, \mathbb{Z}) \oplus \hat{H}^{-3}(G_2, \mathbb{Z}) \to \hat{H}^{-3}(G, \mathbb{Z})$$

is surjective (recall that $\hat{H}^{-3}(G, \mathbb{Z}) \cong \mathbb{Z}/6$) and therefore $\mathfrak{F}(L/K/k) = \mathfrak{S}(K/k)$ by Theorem 2.13. □

As a consequence of this result, one can use the GAP function 1obs described in Remark 2.20 to computationally solve the cases where $6 \mid |H|$ and $H^1(G, F_{G/H}) \neq 0$. The remaining possibilities for $H$ are dealt with in the two following results.

Proposition 5.15. (i) If $H \cong V_4$ or $D_4$, then $\mathfrak{S}(K/k) \cong \mathfrak{S}(L/k)_{(3)}$;
(ii) If $H \cong C_5$ or $C_7$, then $\mathfrak{S}(K/k) \cong \mathfrak{S}(L/k)$;
(iii) If $H \cong C_3 \times C_3$ or $C_4 \times C_3$, then $\mathfrak{S}(K/k) \cong \mathfrak{S}(L/k)_{(2)}$.

Proof. We prove only (i) (ii) and (iii) follow analogously). In this case we have $H^1(G, F_{G/H}) = \mathbb{Z}/3$ (see Tables 5 and 6 of the Appendix) and thus $\mathbb{Z}/3 \to \mathfrak{S}(K/k)$ by Theorems 2.5 and 2.8. The result now follows by Corollary 4.6, noticing that $d = [L: K] = 4$ or 8 is coprime to $|\mathfrak{S}(K/k)|$. □

Proposition 5.16. (i) If $H \cong C_2$ or $D_5$, then $\mathfrak{S}(K/k) \cong \mathfrak{S}(L/k)$;
Theorem 5.17. Let $\text{torus } R$ and 6 of the Appendix, one can also compute the defect of weak approximation for the norm one $K/k$. Proof. First, note that in all cases $\mathfrak{R}(K/k) \cong \mathfrak{R}(L/k) \times \mathfrak{R}(M/k) \cong \mathfrak{R}(L/M/k)$, where $M$ is the fixed field of a copy of $(C_3 \times C_3) \times C_4$ inside $G$ containing $H_2 \cong C_4$.

We have thus completely proved the characterization of the HNP for an $A_6$ or $A_7$ extension given in Theorem 6.1. Moreover, combining this result with Theorems 2.5, 2.8 and the contents of Tables 5 and 6 of the Appendix, one can also compute the defect of weak approximation for the norm one torus $R_{K/k}^1 \mathbb{G}_m$. The conclusions regarding the validity of weak approximation are the following:

**Theorem 5.17.** Let $K/k$ be an extension of number fields contained in a Galois extension $L/k$ such that $G = \text{Gal}(L/k) \cong A_6$ or $A_7$. Let $H = \text{Gal}(L/K)$ and $T = R_{K/k}^1 \mathbb{G}_m$.

- If $V_4 \leftrightarrow H$ and $C_3 \leftrightarrow H$, then weak approximation holds for $T$.
- If $H \cong 1, C_2, C_5, C_7$ or $D_5$, then weak approximation holds for $T$ if and only if $V_4 \nleftrightarrow D_v$ and $C_3 \times C_3 \nleftrightarrow D_v$ for every place $v$ of $K/k$.
- If $H \cong C_4$ or $C_5 \times C_4$, then weak approximation holds for $T$ if and only if $D_4 \nleftrightarrow D_v$ and $C_3 \times C_3 \nleftrightarrow D_v$ for every place $v$ of $K/k$.
- In all other cases, weak approximation holds for $T$ if and only if the HNP fails for $K/k$.

6. **Examples**

This section concerns the existence of number fields with prescribed Galois group for which the HNP holds, and the existence of those for which it fails. The main result is Theorem 1.14. To prove it, we will use the notion of $k$-adequate extensions, as introduced by Schacher in [15].

**Definition 6.1.** An extension $K/k$ of number fields is said to be $k$-adequate if $K$ is a maximal subfield of a finite dimensional $k$-central division algebra.

A conjecture of Bartels (see [2] p. 198) predicted that the HNP would hold for any $k$-adequate extension. This was proved by Gurak (see [27] Theorem 3.1) for Galois extensions, but disproved in general by Drakokhrust and Platonov (see [16], §9, §11). Given a Galois extension $L/k$, a result of Schacher (see [45], Proposition 2.6) shows that $L$ is $k$-adequate if and only if for every prime $p \mid [L : k]$ there are at least two places $v_1$ and $v_2$ of $k$ such that $\text{Gal}(L_{v_1}/k_{v_1})$ contains a Sylow $p$-subgroup of $\text{Gal}(L/k)$. This led Schacher to establish the following result:
Theorem 6.2. [43] Theorem 9.1] For any finite group $G$ there exists a number field $k$ and a $k$-adequate Galois extension $L/k$ with $\text{Gal}(L/k) \cong G$.

We can now prove Theorem 1.15 which generalizes [27] Corollary 3.3 to non-normal extensions.

Proof of Theorem 1.15. (i) Let $L/k$ be a $k$-adequate Galois extension with Galois group $G$ as given in Theorem 6.2. Let $K = L^H$ and $T = R^1_{K/k}G_m$. Recall that, by Theorem 2.11

$$\text{III}(T)^\sim = \text{Ker} \left( H^2(G, J_{G/H}) \xrightarrow{\text{Res}} \prod_{v \in \Omega_k} H^2(D_v, J_{G/H}) \right).$$

Since for every $p$ dividing $|G|$ there exists a place $v$ such that $D_v = \text{Gal}(L_v/k_v)$ contains a Sylow $p$-subgroup, Proposition 2.1 and the transitivity of restriction show that the map

$$H^2(G, J_{G/H})(p) \xrightarrow{\text{Res}} \prod_{v \in \Omega_k} H^2(D_v, J_{G/H})(p)$$

is injective. It follows that $\text{III}(T) = 0$ and so $\mathfrak{h}(K/k)$ is trivial, as desired.

(ii) By [16, Lemma 6], there is a Galois extension $L/k$ of number fields with $\text{Gal}(L/k) \cong G$ such that every decomposition group is cyclic. Let $K = L^H$, $T = R^1_{K/k}G_m$ and let $X$ be a smooth compactification of $T$. By [50], §3, Theorem 6 and Corollary 2, we have $A(T) = 0$ and $\text{III}(T) \cong H^1(k, \text{Pic} \overline{X})^\sim$. The result now follows from Theorem 2.8 and the fact that $\mathfrak{h}(K/k) = \text{III}(T)$.

To conclude this section, we provide examples of number fields over $\mathbb{Q}$ illustrating that in every case addressed by Theorems 1.9 and 1.11 there exists an extension of the desired type satisfying the HNP. Furthermore, in the cases where failure of the HNP is theoretically possible, we construct examples showing that failures actually occur (over at most a quadratic extension of $\mathbb{Q}$). When looking for such examples, [47] Lemmas 18 and 20 give useful practical conditions to test the local properties of Theorem 1.9. Some of these extensions were found using the LMFDB database [35] and all assertions below concerning Galois groups and ramification properties were verified using the computer algebra system MAGMA [9].

6.1. Successes.

• First consider $G = A_4$ or $S_4$. Let $L/\mathbb{Q}$ be the splitting field of the polynomial $f(x)$ defined as

$$f(x) = \begin{cases} x^4 - 2x^3 + 2x^2 + 2 & \text{if } G = A_4, \\ x^4 - 2x^3 - 4x^2 - 6x - 2 & \text{if } G = S_4. \end{cases}$$

In both cases $L/\mathbb{Q}$ is a Galois extension with Galois group $G$ such that the decomposition group at the prime 2 is the full Galois group. Applying Theorem 1.9 we thus conclude that the HNP holds for $L/\mathbb{Q}$ as well as for any subextension $K/\mathbb{Q}$ contained in $L/\mathbb{Q}$.

• For $G = A_5$, let $K = \mathbb{Q}(\alpha)$, where $\alpha$ is a root of the polynomial $x^5 - x^4 + 2x^2 - 2x + 2$, and let $L/\mathbb{Q}$ be the normal closure of $K/\mathbb{Q}$. We have $\text{Gal}(L/\mathbb{Q}) \cong A_5$ and there exists a prime $p$ of $K$ above 2 with ramification index 4, so it follows that $4 \mid |D_2|$. Since any subgroup of $A_5$ with
order divisible by 4 contains a copy of $V_4$ generated by two double transpositions, Theorem 1.9 shows that the HNP holds for any subextension of $L\mathbb{Q}$.

- For $G = S_5$, take $K = \mathbb{Q}(\alpha)$, where $\alpha$ is a root of the polynomial $x^{10} - 4x^9 - 24x^8 + 80x^7 + 174x^6 - 416x^5 - 372x^4 + 400x^3 + 370x^2 + 32x - 16$, and let $L\mathbb{Q}$ be the normal closure of $K\mathbb{Q}$. One can verify that $\text{Gal}(L\mathbb{Q}) \cong S_5$ and that there is a prime $p$ of $K$ above 2 with ramification index 8. By the same reasoning as in the $A_5$ case, $D_2$ contains a copy of $V_4$ generated by two double transpositions, and thus the HNP holds for any subextension of $L\mathbb{Q}$ by Theorem 1.9.

- For $G = A_6$, let $K = \mathbb{Q}(\alpha)$, where $\alpha$ is a root of the polynomial $x^{15} - 3x^{13} - 2x^{12} + 12x^{10} + 50x^9 - 54x^7 + 68x^6 - 162x^5 + 30x^4 - 67x^3 + 15x + 4$, and let $L\mathbb{Q}$ be the normal closure of $K\mathbb{Q}$. We have $\text{Gal}(L\mathbb{Q}) \cong A_6$ and there are primes $p$ and $q$ of $K$ above 2 and 3, respectively, such that $[K_p : \mathbb{Q}_2] = 8$ and $[K_q : \mathbb{Q}_3] = 9$. Since every subgroup of $A_6$ with order divisible by 8 contains a copy of $D_4$, it follows that $D_4 \hookrightarrow D_2$. Analogously, we have $C_3 \times C_3 \hookrightarrow D_3$. Theorem 1.11 then shows that the HNP holds for any subextension of $L\mathbb{Q}$.

- For $G = A_7$, let $L\mathbb{Q}$ be the splitting field of the polynomial $x^7 - 3x^6 - 3x^5 - x^4 + 12x^3 + 24x^2 + 16x + 24$. We have $\text{Gal}(L\mathbb{Q}) \cong A_7$ and the primes 2 and 3 ramify in $L\mathbb{Q}$. Let $M$ be the fixed field of the subgroup $\langle (2,3)(5,7), (1,2)(4,5,6,7), (2,3)(5,6) \rangle \cong (A_4 \times C_3) \rtimes C_2$ of $A_7$, a degree 35 extension of $\mathbb{Q}$. Given a prime $p$, let $e = e(p)$ denote its ramification index and $f = f(p)$ its inertial degree in $\mathbb{Q}$. Note that if the decomposition $O_M/pO_M \cong \bigoplus_i \mathbb{F}_{p^{e_i}}[t]/(t^{e_i})$ holds for some $e_i, f_i \in \mathbb{Z}_{\geq 0}$, then $\text{lcm}(e_i) | e$, $\text{lcm}(f_i) | f$ and hence $\text{lcm}(e_i) \cdot \text{lcm}(f_i) | ef = |D_p|$. Factoring the prime $p = 2$ in $M$ gives $\text{lcm}(e_i) = 12$ and $\text{lcm}(f_i) = 2$, so $24 | |D_2|$. Since any subgroup of $A_7$ with order divisible by 24 contains a copy of $D_4$, we conclude that $D_4 \hookrightarrow D_2$. Using the same reasoning with the prime $p = 3$, we find $18 | |D_3|$ and consequently $D_3$ contains a copy of $C_3 \times C_3$.

By Theorem 1.11 it follows that the HNP holds for any subextension of $L\mathbb{Q}$.

**Remark 6.3.** An alternative approach to find examples of number fields satisfying the HNP and with Galois groups as in Theorems 1.9 and 1.11 is to use $\mathbb{Q}$-adequate extensions. Indeed, examining the local conditions of Theorems 1.9 and 1.11 it is clear that the HNP holds for any subextension of a $\mathbb{Q}$-adequate Galois extension with Galois group $G = A_4, S_4, A_5, S_5, A_6, A_7$. The existence of $\mathbb{Q}$-adequate extensions with prescribed Galois group $G$ has been studied by Schacher and others. For $G = A_4, S_4, A_5, S_5, A_6, A_7$, there exist $\mathbb{Q}$-adequate Galois extensions $L\mathbb{Q}$ with $\text{Gal}(L\mathbb{Q}) \cong G$. We give some references for the interested reader. For $G = A_4, A_5$ see [24], [25], respectively. In fact, for these two groups stronger results hold. For $G = A_4$ there exist $k$-adequate Galois extensions with Galois group $A_4$ for any global field $k$ of characteristic not equal to 2 or 3 (see [24 Corollary 2.2]). For $G = A_5$, [25 Theorem 1] constructs $k$-adequate Galois extensions with Galois group $A_5$ for any number field $k$ such that $\sqrt{-1} \not\in k$. For $G = S_4, S_5$ see [15, Theorem 7.1]. Finally, the cases $G = A_6, A_7$ are treated in [19]. We chose not to pursue this approach because the polynomials defining the relevant field extensions were rather cumbersome, particularly for $A_6$ and $A_7$.

6.2. Failures.
• We start with the cases where $G$ is $A_4$ or $S_4$. Let $L/Q$ be the splitting field of $f(x)$, where

$$f(x) = \begin{cases} 
    x^4 + 3x^2 - 7x + 4 & \text{if } G = A_4, \\
    x^4 - x^3 - 4x^2 + x + 2 & \text{if } G = S_4.
\end{cases}$$

In both cases $L/Q$ is a Galois extension with Galois group $G$ such that every decomposition group is cyclic. Therefore, Theorem 1.9 shows that the HNP fails for any subextension of $L/k$ falling under case (i) or (ii) of Theorem 1.9, i.e. an extension where the HNP can theoretically fail.

• We now find examples for the $A_5$ and $S_5$ cases using work of Uchida [49]. Examples for the $A_6$ and $A_7$ cases can be obtained in a manner analogous to the construction for $A_5$. Let $F/Q$ be the splitting field of $f(x) = x^5 - x + 1$ and set $D = \text{Disc}(f) = 19 \cdot 151$. By [49, Corollary and Theorem 2], $F/Q(\sqrt{D})$ is an unramified Galois extension with Galois group $A_5$, while $F(\sqrt{2})/Q(\sqrt{2D})$ is an unramified Galois extension with Galois group $S_5$. Set $L = F, k = Q(\sqrt{D})$ if $G = A_5$ and $L = F(\sqrt{2}), k = Q(\sqrt{2D})$ if $G = S_5$. Let $K/k$ be a subextension of $L/k$ falling under case (i) or (ii) of Theorem 1.9. Since $L/k$ is unramified, all its decomposition groups are cyclic, whereby the HNP fails for $K/k$ by the criterion of Theorem 1.9.

By Theorem 1.11 this last construction provides examples of $A_6$ and $A_7$-extensions that fail the HNP with knot group equal to $C_6$. It is also possible to construct failures with knot group $C_2$ or $C_3$. Indeed, if $G = A_6$ or $A_7$, one can set $S = C_3 \times C_3$ in [16, Lemma 6] in order to get a Galois extension of number fields with decomposition group $D_v = C_3 \times C_3$ for every ramified place $v$. Since the remaining places have cyclic decomposition groups, it follows from Theorem 1.11 that the knot group of this extension is $C_2$. An analogous construction choosing $S = D_4$ gives a Galois extension of number fields with knot group equal to $C_3$.

**Appendix**

We present the results of the computer calculations outlined in Section 5.2. In the following tables, we distinguish non-conjugate but isomorphic groups with a letter in front of the isomorphism class.

**Table 1**

| $G = A_4$ | $[K : k]$ | $H$ | $H^1(G, F_{G/H})$ |
|---------|-----------|-----|-------------------|
|         | 12        | 1   | $\mathbb{Z}/2$    |
|         | 6         | $C_2 = \langle (1, 2)(3, 4) \rangle$ | $\mathbb{Z}/2$ |
|         | 4         | $C_3 = \langle (1, 2, 3) \rangle$ | $\mathbb{Z}/2$ |
|         | 3         | $V_4 = \langle (1, 2)(3, 4), (1, 3)(2, 4) \rangle$ | 0 |
### Table 2

| $[K : k]$ | $H$ | $\text{H}^1(G, F_{G/H})$ |
|-----------|-----|--------------------------|
| 24        | 1   | $\mathbb{Z}/2$           |
| 12        | $C_2a = \langle (1, 2) \rangle$ | 0                        |
| 12        | $C_2b = \langle (1, 2)(3, 4) \rangle$ | $\mathbb{Z}/2$         |
| 8         | $C_3 = \langle (1, 2, 3) \rangle$ | $\mathbb{Z}/2$         |
| 6         | $C_4 = \langle (1, 2, 3, 4) \rangle$ | 0                        |
| 6         | $V_4 = \langle (1, 2), (3, 4) \rangle$ | 0                        |
| 6         | $V_4 = \langle (1, 2)(3, 4), (1, 3)(2, 4) \rangle$ | 0                        |
| 4         | $S_3 = \langle (1, 2, 3), (1, 2) \rangle$ | 0                        |
| 3         | $D_4 = \langle (1, 2, 3, 4), (1, 3) \rangle$ | 0                        |
| 2         | $A_4 = \langle (1, 2)(3, 4), (1, 2, 3) \rangle$ | 0                        |

### Table 3

| $[K : k]$ | $H$ | $\text{H}^1(G, F_{G/H})$ |
|-----------|-----|--------------------------|
| 60        | 1   | $\mathbb{Z}/2$           |
| 30        | $C_2 = \langle (1, 2)(3, 4) \rangle$ | $\mathbb{Z}/2$         |
| 20        | $C_3 = \langle (1, 2, 3) \rangle$ | $\mathbb{Z}/2$         |
| 15        | $V_4 = \langle (1, 2)(3, 4), (1, 3)(2, 4) \rangle$ | 0                        |
| 12        | $C_5 = \langle (1, 2, 3, 4, 5) \rangle$ | $\mathbb{Z}/2$         |
| 10        | $S_3 = \langle (1, 2, 3), (1, 2)(4, 5) \rangle$ | $\mathbb{Z}/2$         |
| 6         | $D_5 = \langle (1, 2, 3, 4, 5), (2, 5)(3, 4) \rangle$ | $\mathbb{Z}/2$         |
| 5         | $A_4 = \langle (1, 2)(3, 4), (1, 2, 3) \rangle$ | 0                        |
## Table 4

$G = S_5$

| $[K : k]$ | $H$ | $\text{H}^1(G, F_{G/H})$ |
|-----------|-----|---------------------|
| 120       | 1   | $\mathbb{Z}/2$      |
| 60        | $C_2a = \langle (1, 2) \rangle$ | 0   |
| 60        | $C_2b = \langle (1, 2)(3, 4) \rangle$ | $\mathbb{Z}/2$ |
| 40        | $C_3 = \langle (1, 2, 3) \rangle$ | $\mathbb{Z}/2$ |
| 30        | $C_4 = \langle (1, 2, 3, 4) \rangle$ | 0   |
| 30        | $V_4a = \langle (1, 2), (3, 4) \rangle$ | 0   |
| 30        | $V_4b = \langle (1, 2)(3, 4), (1, 3)(2, 4) \rangle$ | 0   |
| 24        | $C_5 = \langle (1, 2, 3, 4, 5) \rangle$ | $\mathbb{Z}/2$ |
| 20        | $C_6 = \langle (1, 2, 3, (4, 5)) \rangle$ | 0   |
| 20        | $S_3a = \langle (1, 2, 3), (1, 2) \rangle$ | 0   |
| 20        | $S_3b = \langle (1, 2, 3), (1, 2)(4, 5) \rangle$ | $\mathbb{Z}/2$ |
| 15        | $D_4 = \langle (1, 2, 3, 4), (1, 3) \rangle$ | 0   |
| 12        | $D_5 = \langle (1, 2, 3, 4, 5), (2, 5)(3, 4) \rangle$ | $\mathbb{Z}/2$ |
| 10        | $A_4 = \langle (1, 2)(3, 4), (1, 2, 3) \rangle$ | 0   |
| 10        | $S_3 \times C_2 = \langle (1, 2, 3), (1, 2), (4, 5) \rangle$ | 0   |
| 6         | $C_5 \times C_4 = \langle (1, 2, 3, 4, 5), (2, 3, 5, 4) \rangle$ | 0   |
| 5         | $S_4 = \langle (1, 2, 3, 4), (1, 2) \rangle$ | 0   |
| 2         | $A_5 = \langle (1, 2, 3, 4, 5), (1, 2, 3) \rangle$ | 0   |
| $[K : k]$ | $H$ | $\text{H}^1(G, F_{G/H})$ |
|-----------|------|----------------|
| 360       | $C_2 = \langle (1, 2)(3, 4) \rangle$ | $\mathbb{Z}/6$ |
| 180       | $C_3 = \langle (1, 2, 3) \rangle$ | $\mathbb{Z}/6$ |
| 120       | $C_3 = \langle (1, 2, 3)(4, 5, 6) \rangle$ | $\mathbb{Z}/2$ |
| 90        | $C_4 = \langle (1, 2, 3, 4)(5, 6) \rangle$ | $\mathbb{Z}/6$ |
| 90        | $V_4a = \langle (1, 2)(3, 4), (1, 3)(2, 4) \rangle$ | $\mathbb{Z}/3$ |
| 90        | $V_4b = \langle (1, 2)(5, 6), (1, 2)(3, 4) \rangle$ | $\mathbb{Z}/3$ |
| 72        | $C_5 = \langle (1, 2, 3, 4, 5) \rangle$ | $\mathbb{Z}/6$ |
| 60        | $S_3a = \langle (1, 2, 3)(4, 5, 6), (1, 2)(4, 5) \rangle$ | $\mathbb{Z}/2$ |
| 60        | $S_3b = \langle (1, 2, 3), (1, 2)(4, 5) \rangle$ | $\mathbb{Z}/2$ |
| 45        | $D_4 = \langle (1, 2, 3, 4)(5, 6), (1, 3)(5, 6) \rangle$ | $\mathbb{Z}/3$ |
| 40        | $C_3 \times C_3 = \langle (1, 2, 3), (4, 5, 6) \rangle$ | $\mathbb{Z}/2$ |
| 36        | $D_5 = \langle (1, 2, 3, 4, 5), (2, 5)(3, 4) \rangle$ | $\mathbb{Z}/6$ |
| 30        | $A_4a = \langle (1, 2)(3, 4), (1, 2, 3) \rangle$ | $0$ |
| 30        | $A_4b = \langle (1, 2, 3)(4, 5, 6), (1, 4)(2, 5) \rangle$ | $0$ |
| 20        | $(C_3 \times C_3) \times C_2 = \langle (1, 2, 3), (4, 5, 6), (1, 2)(4, 5) \rangle$ | $\mathbb{Z}/2$ |
| 15        | $S_4a = \langle (1, 2, 3, 4)(5, 6), (1, 2)(5, 6) \rangle$ | $0$ |
| 15        | $S_4b = \langle (1, 3, 5)(2, 4, 6), (1, 6)(2, 5) \rangle$ | $0$ |
| 10        | $(C_3 \times C_3) \times C_4 = \langle (1, 2, 3), (4, 5, 6), (1, 4)(2, 5, 3, 6) \rangle$ | $\mathbb{Z}/2$ |
| 6         | $A_5a = \langle (1, 2, 3, 4, 5), (1, 2, 3) \rangle$ | $0$ |
| 6         | $A_5b = \langle (1, 2, 3, 4, 5), (1, 4)(5, 6) \rangle$ | $0$ |
Table 6

\begin{table}
\begin{tabular}{|c|c|c|}
\hline
\textbf{\([K : k]\)} & \textbf{\(H\)} & \textbf{\(H^1(G, F_{G/H})\)} \\
\hline
2520 & 1 & \(\mathbb{Z}/6\) \\
1260 & \(C_2 = \langle (1, 2)(3, 4) \rangle\) & \(\mathbb{Z}/6\) \\
840 & \(C_3 a = \langle (1, 2, 3) \rangle\) & \(\mathbb{Z}/2\) \\
840 & \(C_3 b = \langle (1, 2, 3)(4, 5, 6) \rangle\) & \(\mathbb{Z}/2\) \\
630 & \(C_4 = \langle (1, 2, 3, 4)(5, 6) \rangle\) & \(\mathbb{Z}/6\) \\
630 & \(V_4 a = \langle (1, 2)(3, 4), (1, 3)(2, 4) \rangle\) & \(\mathbb{Z}/3\) \\
630 & \(V_4 b = \langle (1, 2)(5, 6), (1, 2)(3, 4) \rangle\) & \(\mathbb{Z}/3\) \\
504 & \(C_5 = \langle (1, 2, 3, 4, 5) \rangle\) & \(\mathbb{Z}/6\) \\
420 & \(C_6 = \langle (1, 2)(3, 4)(5, 6, 7) \rangle\) & \(\mathbb{Z}/2\) \\
420 & \(S_3 a = \langle (1, 2, 3)(4, 5, 6), (1, 2)(4, 5) \rangle\) & \(\mathbb{Z}/2\) \\
420 & \(S_3 b = \langle (1, 2, 3), (1, 2)(4, 5) \rangle\) & \(\mathbb{Z}/2\) \\
360 & \(C_7 = \langle (1, 2, 3, 4, 5, 6, 7) \rangle\) & \(\mathbb{Z}/6\) \\
315 & \(D_4 = \langle (1, 2, 3, 4)(5, 6), (1, 3)(5, 6) \rangle\) & \(\mathbb{Z}/3\) \\
280 & \(C_3 \times C_3 = \langle (1, 2, 3), (4, 5, 6) \rangle\) & \(\mathbb{Z}/2\) \\
252 & \(D_5 = \langle (1, 2, 3, 4, 5), (2, 5)(3, 4) \rangle\) & \(\mathbb{Z}/6\) \\
210 & \(A_4 a = \langle (1, 2)(3, 4), (1, 2, 3) \rangle\) & 0 \\
210 & \(A_4 b = \langle (1, 2, 3)(4, 5, 6), (1, 4)(2, 5) \rangle\) & 0 \\
210 & \(A_4 c = \langle (1, 5, 3)(4, 7, 6), (2, 6)(4, 7) \rangle\) & 0 \\
210 & \(A_4 d = \langle (1, 2, 5)(4, 6, 7), (3, 4)(6, 7) \rangle\) & 0 \\
210 & \(C_2 \times C_6 = \langle (1, 2)(3, 5)(4, 6, 7), (1, 3)(2, 5) \rangle\) & 0 \\
210 & \(D_6 = \langle (1, 2)(3, 5)(4, 6, 7), (1, 2)(6, 7) \rangle\) & 0 \\
210 & \(C_3 \times C_4 = \langle (2, 3, 6), (1, 4, 7, 5)(3, 6) \rangle\) & \(\mathbb{Z}/2\) \\
140 & \((C_3 \times C_3) \times C_2 = \langle (1, 2, 3), (4, 5, 6), (1, 2)(4, 5) \rangle\) & \(\mathbb{Z}/2\) \\
126 & \(C_5 \times C_4 = \langle (1, 2)(4, 5, 7, 6), (3, 6, 7, 4, 5) \rangle\) & \(\mathbb{Z}/6\) \\
120 & \(C_7 \times C_3 = \langle (1, 7, 4, 2, 6, 5, 3), (2, 3, 5)(4, 6, 7) \rangle\) & \(\mathbb{Z}/2\) \\
105 & \((C_6 \times C_2) \times C_2 = \langle (1, 2)(3, 5)(4, 6, 7), (1, 3)(2, 5), (1, 2)(6, 7) \rangle\) & 0 \\
105 & \(S_4 a = \langle (1, 2, 3, 4)(5, 6), (1, 2)(5, 6) \rangle\) & 0 \\
105 & \(S_4 b = \langle (1, 3, 5)(2, 4, 6), (1, 6)(2, 5) \rangle\) & 0 \\
105 & \(S_4 c = \langle (1, 2, 3)(5, 6, 7), (2, 3)(4, 5, 6, 7) \rangle\) & 0 \\
105 & \(S_4 d = \langle (1, 3, 2)(5, 6, 7), (2, 3)(4, 5, 6, 7) \rangle\) & 0 \\
70 & \(A_4 \times C_3 = \langle (1, 3, 5)(4, 6, 7), (1, 2, 3) \rangle\) & 0 \\
70 & \((C_3 \times C_3) \times C_4 = \langle (1, 2, 3), (4, 5, 6), (1, 4)(2, 5, 3, 6) \rangle\) & \(\mathbb{Z}/2\) \\
42 & \(A_5 a = \langle (1, 2, 3, 4, 5), (1, 2, 3) \rangle\) & 0 \\
42 & \(A_5 b = \langle (1, 2, 3, 4, 5), (1, 4)(5, 6) \rangle\) & 0 \\
35 & \((A_4 \times C_3) \times C_2 = \langle (2, 3)(5, 7), (1, 2)(4, 5, 6, 7), (2, 3)(5, 6) \rangle\) & 0 \\
21 & \(S_5 = \langle (1, 2)(3, 7), (2, 6, 5, 4)(3, 7) \rangle\) & 0 \\
15 & \(\text{PSL}(3, 2) a = \langle (1, 4)(2, 3), (2, 4, 6)(3, 5, 7) \rangle\) & 0 \\
15 & \(\text{PSL}(3, 2) b = \langle (1, 3)(2, 7), (1, 5, 7)(3, 4, 6) \rangle\) & 0 \\
7 & \(A_6 = \langle (1, 2, 3, 4, 5)(4, 5, 6) \rangle\) & 0 \\
\hline
\end{tabular}
\end{table}
References

[1] S. A. Altug, A. Shankar, I. Varma, K. H. Wilson, The number of quartic $D_4$-fields ordered by conductor. Preprint. arXiv:1704.01729
[2] H.-J. Bartels, Zur Arithmetik von Konjugationsklassen in algebraischen Gruppen. J. Algebra 70 (1981), 179–199.
[3] H.-J. Bartels, Zur Arithmetik von Diedergruppenweiterungen. Math. Ann. 256 (1981), 465–473.
[4] M. Bhargava, The density of discriminants of quartic rings and fields. Ann. of Math. 162(2) (2005), 1031–1063.
[5] M. Bhargava, The density of discriminants of quintic rings and fields. Ann. of Math. 172(3) (2010) 1559–1591.
[6] M. Bhargava, A. Shankar, J. Tsimerman, On the Davenport-Heilbronn theorems and second order terms. Invent. Math. 193(2) (2013), 439–499.
[7] M. Bhargava, A. Shankar, X. Wang, Geometry-of-numbers methods over global fields I: Prehomogeneous vector spaces. Preprint. arXiv:1704.01729
[8] M. Bhargava, I. Varma, On the mean number of 2-torsion elements in the class groups, narrow class groups, and ideal groups of cubic orders and fields. Duke Math. J. 164(10) (2015), 1911-1933.
[9] W. Bosma, J. Cannon, C. Playoust, The Magma algebra system. I. The user language. J. Symbolic Comput., 24 (1997), 235–265.
[10] K. S. Brown, Cohomology of groups. Graduate Texts in Mathematics 87, Springer-Verlag, 1982.
[11] T.D. Browning, How often does the Hasse principle hold? Algebraic Geometry: Salt Lake City 2015, Proc. Symposia Pure Math. 97.2 (2018), AMS, 89–102.
[12] J.-L. Colliot-Thélène, J.-J. Sansuc, La R-équivalence sur les tores. Ann. Sc. E.N.S. 10 (1977), 175–229.
[13] J.-L. Colliot-Thélène, J.-J. Sansuc, Principal homogeneous spaces under flasque tori: Applications. J. Algebra 106 (1987), 148–205.
[14] B. Datskovsky, D. J. Wright, Density of discriminants of cubic extensions. J. reine angew. Math. 386 (1988), 116–138.
[15] Y. A. Drakokhrust, On the complete obstruction to the Hasse principle. Amer. Math. Soc. Transl.(2) 143 (1989), 29-34.
[16] Y. A. Drakokhrust, V. P. Platonov, The Hasse norm principle for algebraic number fields. Math. USSR-Izv. 29 (1987), 299-322.
[17] J. S. Ellenberg, L. B. Pierce, M. M. Wood, On $\ell$-torsion in class groups of number fields. Algebra and Number Theory 11-8 (2017), 1739–1778.
[18] J. S. Ellenberg, A. Venkatesh, The number of extensions of a number field with fixed degree and bounded discriminant. Ann. of Math. 163(2) (2006), 723-741.
[19] B. Fein, M. Schacher, $\mathbb{Q}$-Admissibility Questions for Alternating Groups. Journal of Algebra 142 (1991), 360-382.
[20] C. Frei, D. Loughran, R. Newton, The Hasse norm principle for abelian extensions. Amer. J. Math 140(6) (2018), 1639-1685.
[21] C. Frei, D. Loughran, R. Newton, with an appendix by Y. Harpaz, O. Wittenberg, Number fields with prescribed norms. Preprint. arXiv:1810.06024
[22] C. Frei, M. Widmer, Average bounds for the $\ell$-torsion in class groups of cyclic extensions. Res. Number Theory 4(34) (2018).
[23] GAP Group, GAP – Groups, Algorithms, and Programming, Version 4.8.10 (2018). Available at https://www.gap-system.org
[24] B. Gordon, M. Schacher, Quartic coverings of a cubic. In Number Theory and Algebra, 97-101, Academic Press, New York, 1977.
[25] B. Gordon, M. Schacher, The admissibility of $A_5$. Journal of Number Theory 11 (1979), 489-504.
[26] Groupprops, The Group Properties Wiki, Criterion for element of alternating group to be real. Available at https://groupprops.subwiki.org/wiki/Criterion_for_element_of_alternating_group_to_be_real
[27] S. Gurak, On the Hasse norm principle. *J. reine angew. Math.* 299/300 (1978), 16–27.
[28] S. Gurak, The Hasse norm principle in non-abelian extensions. *J. reine angew. Math.* 0303/0304 (1978), 314–318.
[29] H. Hasse, Beweis eines Satzes und Wiederlegung einer Vermutung über das allgemeine Normenrestsymbol. *Nachr. Ges. Wiss. Göttingen Math.-Phys. Kl.* (1931), 64–69.
[30] D. Higman, Focal series in finite groups. *Canad. J. Math.* 5 (1953), 477—497.
[31] W. Ho, A. Shankar, I. Varma, Odd degree number fields with odd class number. *Duke Math. J.* 167 (2018), No. 5, 995–1047.
[32] P. N. Hoffman, J. F. Humphreys, *Projective representations of the symmetric groups*. Oxford Mathematical Monographs, Clarendon Press, Oxford, 1992.
[33] A. Hoshi, A. Yamasaki, *Rationality problem for algebraic tori*. Memoirs of the American Mathematical Society 248 (2017), No. 1176.
[34] G. Karpilovsky, *The Schur Multiplier*. Clarendon Press, Oxford, 1987.
[35] The LMFDB Collaboration, *The L-functions and Modular Forms Database*. [online; accessed 16 September 2013].
[36] A. Macedo, GAP code (2019). Available at [https://sites.google.com/view/andre-macedo/code](https://sites.google.com/view/andre-macedo/code).
[37] A. Macedo, The Hasse norm principle for $A_n$-extensions. Preprint. [arXiv:1806.11563](https://arxiv.org/abs/1806.11563).
[38] A. Macedo, The Hasse norm principle for $D_4$-octics. In preparation.
[39] G. Malle, On the distribution of Galois groups. *Journal of Number Theory* 92(2) (2002), 315–329.
[40] L. B. Pierce, C. L. Turnage-Butterbaugh, M. M. Wood, An effective Chebotarev density theorem for families of number fields, with an application to $\ell$-torsion in class groups. Preprint. [arXiv:1709.09637](https://arxiv.org/abs/1709.09637).
[41] V. Platonov, A. Rapinchuk, *Algebraic groups and number theory*. Pure and Applied Mathematics 139, Academic Press, Inc., Boston, MA, 1994.
[42] M. J. Razar, Central and genus class fields and the Hasse norm theorem. *Compositio Math.* 35 (1977), 281–298.
[43] N. Rome, The Hasse norm principle for biquadratic extensions. *J. Théor. Nombres Bordeaux* 30 No. 3 (2018), 947-964.
[44] 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.
[45] M. Schacher, Subfields of division rings I. *J. Algebra* 9 (1968) 451-477.
[46] J. Schur, Über die Darstellung der symmetrischen und der alternierenden Gruppe durch gebrochene lineare Substitutionen. *J. reine angew. Math.* 139 (1911), 155–250.
[47] L. Stern, Equality of norm groups of subextensions of $S_n$ ($n \leq 5$) extensions of algebraic number fields. *Journal of Number Theory* 102(2) (2003), 257-277.
[48] J. T. Tate, Global class field theory. pp. 162–203 in: J.W.S. Cassels, A. Fröhlich (eds), *Algebraic number theory*, Second Edition, London Mathematical Society, 2010.
[49] K. Uchida, Unramified extensions of quadratic number fields I. *Tôhoku Math. Journal* 22 (1970), 220-224.
[50] V. E. Voskresenskiî, 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.
[51] V. E. Voskresenskiî, B. È. Kunyavskiî, Maximal tori in semisimple algebraic groups. Manuscript deposited at VINITI 15.03.84, No. 1269-84, 28pp. (in Russian)
[52] M. M. Wood, Nonabelian Cohen-Lenstra Moments (including an appendix with P. M. Wood). *Duke Math. J.* 168 No. 3 (2019), 377-427.
