University of Reading

Explicit methods for the Hasse norm principle and applications to A_n and S_n extensions

Article

Published Version

Creative Commons: Attribution 4.0 (CC-BY)

Open Access

Macedo, A. and Newton, R. ORCID: https://orcid.org/0000-0003-4925-635X (2022) Explicit methods for the Hasse norm principle and applications to A_n and S_n extensions. Mathematical Proceedings of the Cambridge Philosophical Society, 172 (3). pp. 489-529. ISSN 1469-8064 doi: 10.1017/S0305004121000268 Available at https://centaur.reading.ac.uk/85677/

It is advisable to refer to the publisher's version if you intend to cite from the work. See Guidance on citing.

To link to this article DOI: http://dx.doi.org/10.1017/S0305004121000268

Publisher: Cambridge University Press

All outputs in CentAUR are protected by Intellectual Property Rights law, including copyright law. Copyright and IPR is retained by the creators or other copyright holders. Terms and conditions for use of this material are defined in the End User Agreement.

www.reading.ac.uk/centaur

University of Reading

CentAUR

Central Archive at the University of Reading

Reading's research outputs online

Math. Proc. Camb. Phil. Soc.: page 1 of 41
doi:10.1017/S0305004121000268

Explicit methods for the Hasse norm principle and applications to A_n and S_n extensions

BY ANDRÉ MACEDO AND RACHEL NEWTON

University of Reading, Department of Mathematics and Statistics, Pepper Lane, Whiteknights, Reading RG6 6AX, UK
e-mails: c.a.v.macedo@pgr.reading.ac.uk, r.d.newton@reading.ac.uk

(*Received* 22 *July* 2019; *revised* 6 *January* 2021; *accepted* 16 *December* 2020)

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 $R^1_{K/k}\mathbb{G}_m$. 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.

2020 Mathematics Subject Classification: 14G05 (primary); 11E72, 11R37, 20G30 (secondary).

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*

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

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 $\mathrm{Gal}(K/k)$ is cyclic [30];
(II) $[K:k]$ is prime [2];
(III) $[K:k] = n$ and $\mathrm{Gal}(N/k) \cong D_n$ is dihedral of order $2n$ [3];
(IV) $[K:k] = n$ and $\mathrm{Gal}(N/k) \cong S_n$ [54] (see also [53]);
(V) $[K:k] = n \geq 5$ and $\mathrm{Gal}(N/k) \cong A_n$ [41].

© The Author(s), 2021. Published by Cambridge University Press on behalf of Cambridge Philosophical Society. This is an Open Access article, distributed under the terms of the Creative Commons Attribution licence (https://creativecommons.org/licenses/by/4.0/), which permits unrestricted re-use, distribution, and reproduction in any medium, provided the original work is properly cited.
Downloaded from https://www.cambridge.org/core. The University of Reading, on 03 Mar 2022 at 12:42:21, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/S0305004121000268

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 [30].

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

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

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 $R^1_{K/k}\mathbb{G}_m$.

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 [52], ties together weak approximation for a torus T and the Hasse principle for principal homogeneous spaces for T:

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

Here X denotes a smooth compactification of T and we write $\mathrm{H}^1(k, \mathrm{Pic}\,\overline{X})^\sim$ for the dual group $\mathrm{Hom}\,(\mathrm{H}^1(k, \mathrm{Pic}\,\overline{X}), \mathbb{Q}/\mathbb{Z})$. Note that the Hochschild–Serre spectral sequence gives an isomorphism $\mathrm{Br}\,X/\mathrm{Br}_0\,X \cong \mathrm{H}^1(k, \mathrm{Pic}\,\overline{X})$, where $\mathrm{Br}_0\,X = \mathrm{Im}(\mathrm{Br}\,k \to \mathrm{Br}\,X)$. While results of Colliot–Thélène and Sansuc (see e.g. Theorem 2·2) enable computation of the invariant $\mathrm{H}^1(k, \mathrm{Pic}\,\overline{X})$, and a result of Tate (see Theorem 2·3) does the same for the Tate–Shafarevich group, actually computing these groups in practice can be challenging. In this paper we give new methods for computing these invariants in the case of norm one tori associated to extensions of number fields.

Set-up. Except where stated otherwise, our assumptions throughout the rest of the paper will be as follows. Let $T = R^1_{K/k}\mathbb{G}_m$ and let X denote a smooth compactification of T. Let L/k be a Galois extension containing K/k and set $G = \mathrm{Gal}(L/k)$ and $H = \mathrm{Gal}(L/K)$.

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 [17] as

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

i.e. as the cokernel of the natural map $\mathfrak{K}(L/k) \to \mathfrak{K}(K/k)$. As shown in [17], 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, see Theorem 4·5.

Let X_0 be a smooth compactification of the torus $R^1_{L/k}\mathbb{G}_m$. The map $N_{L/K} : R^1_{L/k}\mathbb{G}_m \to R^1_{K/k}\mathbb{G}_m$ induces a canonical map $f_{L/K} : \mathrm{H}^1(k, \mathrm{Pic}\,\overline{X_0})^\sim \to \mathrm{H}^1(k, \mathrm{Pic}\,\overline{X})^\sim$, see [9, section 1·2·2]. In order to study the birational invariant $\mathrm{H}^1(k, \mathrm{Pic}\,\overline{X})$, we introduce an object called the '*unramified cover of the first obstruction to the HNP for K/k corresponding to the tower $L/K/k$*' defined as

$$\mathfrak{F}_{nr}(L/K/k) = \mathrm{Coker}(f_{L/K}).$$

In similar fashion to the first obstruction to the HNP, its unramified cover $\mathfrak{F}_{nr}(L/K/k)$ also admits an explicit group-theoretic description:

Downloaded from https://www.cambridge.org/core. The University of Reading, on 03 Mar 2022 at 12:42:21, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/S0305004121000268

THEOREM 1·1. *There is a canonical isomorphism*

$$\mathfrak{F}_{nr}(L/K/k) = (H \cap [G, G])/\Phi^G(H),$$

where $\Phi^G(H)$ *denotes the focal subgroup of* H *in* G, *see Definition* 4·7.

As a corollary, one can compute the p-primary parts of the knot group, the invariant $\mathrm{H}^1(k, \mathrm{Pic}\,\overline{X})$, and the defect of weak approximation for all but finitely many primes p. In what follows, let $\mathfrak{F}(G, H) = (H \cap [G, G])/\Phi^G(H)$ and write $M_{(p)}$ for the p-primary part of an abelian group M.

COROLLARY 1·2. *If* p *is a prime such that* $\mathrm{H}^3(G, \mathbb{Z})_{(p)} = 0$, *then:*

(i) $\mathfrak{K}(K/k)_{(p)} = \mathfrak{F}(L/K/k)_{(p)}$;
(ii) $\mathrm{H}^1(k, \mathrm{Pic}\,\overline{X})^{\sim}_{(p)} = \mathfrak{F}(G, H)_{(p)}$;
(iii) $A(T)_{(p)} = \ker\left(\mathfrak{F}(G, H)_{(p)} \to \mathfrak{F}(L/K/k)_{(p)}\right)$, *where the map* $\mathfrak{F}(G, H) \to \mathfrak{F}(L/K/k)$ *is a natural surjection, see Section* 4.

We now restrict our focus to extensions with normal closure having Galois group isomorphic to A_n or S_n. Our first main theorem enables a purely computational analysis of the HNP and weak approximation for extensions in this family.

THEOREM 1·3. *Suppose that* G *is isomorphic to* A_n *or* S_n *for some* $n \geq 4$ *and* $G \ncong A_6, A_7$. *Then:*

$$\mathfrak{K}(K/k) = \begin{cases} \mathfrak{F}(L/K/k), \text{ if } |H| \text{ is even,} \\ \mathfrak{F}(L/K/k) \times \mathfrak{K}(L/k), \text{ if } |H| \text{ is odd.} \end{cases}$$

and

$$\mathrm{H}^1(k, \mathrm{Pic}\,\overline{X})^{\sim} = \begin{cases} \mathfrak{F}_{nr}(L/K/k), \text{ if } |H| \text{ is even,} \\ \mathfrak{F}_{nr}(L/K/k) \times \mathbb{Z}/2, \text{ if } |H| \text{ is odd.} \end{cases}$$

Theorem 2·3, due to Tate, shows that the knot group of the Galois extension L/k is dual to $\mathrm{Ker}(\mathrm{H}^3(G, \mathbb{Z}) \to \prod_v \mathrm{H}^3(D_v, \mathbb{Z}))$, 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 $\mathrm{H}^3(D_v, \mathbb{Z}) = 0$. In the setting of Theorem 1·3 we obtain 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 $\mathfrak{K}(K/k)$, the invariant $\mathrm{H}^1(k, \mathrm{Pic}\,\overline{X})$, and the defect of weak approximation $A(T)$ for $T = R^1_{K/k}\mathbb{G}_m$.

Using Theorem 1·3 we also characterise the possible isomorphism classes of the group $\mathrm{H}^1(k, \mathrm{Pic}\,\overline{X})$:

THEOREM 1·4.

(i) *For* $G \cong S_n$ *the invariant* $\mathrm{H}^1(k, \mathrm{Pic}\,\overline{X})$ *is an elementary abelian* 2*-group. Moreover, every possibility for* $\mathrm{H}^1(k, \mathrm{Pic}\,\overline{X})$ *is realised: given an elementary abelian* 2*-group* A, *there exists* $n \in \mathbb{N}$ *and an extension of number fields* K/k *whose normal closure has*

Downloaded from https://www.cambridge.org/core. The University of Reading, on 03 Mar 2022 at 12:42:21, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/S0305004121000268

Galois group S_n such that $\mathrm{H}^1(k, \mathrm{Pic}\,\overline{X}) \cong A$, where X is a smooth compactification of $R^1_{K/k}\mathbb{G}_m$.

(ii) *For $G \cong A_n$ the invariant $\mathrm{H}^1(k, \mathrm{Pic}\,\overline{X})$ is either isomorphic to C_3, C_6 or an elementary abelian 2-group. Again, every possibility for $\mathrm{H}^1(k, \mathrm{Pic}\,\overline{X})$ is realised.*

Remark 1·5. The statement of Theorem 1·4 also holds if one replaces $\mathrm{H}^1(k, \mathrm{Pic}\,\overline{X})$ by $\mathfrak{K}(K/k)$ or $A(T)$, see Proposition 7·3.

Theorems 1·3 and 1·4 can be combined to obtain more precise information, as demonstrated in Corollary 1·6 and Example 1·7 below.

COROLLARY 1·6. *Retain the assumptions of Theorem 1·3 and, for p prime, let H_p denote a Sylow p-subgroup of H. Then $\mathrm{H}^1(k, \mathrm{Pic}\,\overline{X})_{(p)} = 0$ for all primes $p > 3$, $\mathrm{H}^1(k, \mathrm{Pic}\,\overline{X})_{(3)} = 0$ if $G \cong S_n$,*

$$\mathrm{H}^1(k, \mathrm{Pic}\,\overline{X})^{\sim}_{(2)} = \begin{cases} \mathfrak{F}(G, H)[2] \cong \mathfrak{F}(G, H_2) & \text{if } |H| \text{ is even,} \\ \mathbb{Z}/2 & \text{if } |H| \text{ is odd,} \end{cases}$$

and if $G \cong A_n$ then

$$\mathrm{H}^1(k, \mathrm{Pic}\,\overline{X})^{\sim}_{(3)} = \mathfrak{F}(G, H)[3] \cong \mathfrak{F}(G, H_3).$$

In particular, if $3 \nmid |H|$ then $\mathrm{H}^1(k, \mathrm{Pic}\,\overline{X})$ is 2-torsion.

Example 1·7. Suppose that $G \cong S_n$ and $|H|$ is odd. Then $\mathrm{H}^1(k, \mathrm{Pic}\,\overline{X}) = \mathbb{Z}/2$ and $\mathfrak{K}(K/k) = \mathfrak{K}(L/k)$. The same conclusion holds for $G \cong A_n$ under the stronger assumption that $|H|$ is coprime to 6.

As a further application of Theorem 1·3, one can obtain conditions on the decomposition groups determining whether the HNP and weak approximation hold in A_n and S_n extensions. In Propositions 1·8 and 1·9, we exhibit such a characterisation for $n = 4$ or 5, when these local conditions are particularly simple.

PROPOSITION 1·8. *Suppose that G is isomorphic to A_4, A_5, S_4 or S_5. Then $\mathfrak{K}(K/k) \hookrightarrow C_2$ and:*

(i) *if $|H|$ is odd, then $\mathfrak{K}(K/k) = 1 \iff \exists\, v$ such that $V_4 \hookrightarrow D_v$;*

(ii) *if $\exists\, C \leq H$ generated by a double transposition with $[H : C]$ odd, then $\mathfrak{K}(K/k) = 1 \iff \exists\, v$ such that D_v contains a copy of V_4 generated by two double transpositions;*

(iii) *in all other cases, $\mathfrak{K}(K/k) = 1$.*

PROPOSITION 1·9. *Retain the assumptions of Proposition 1·8. Then*

$$\mathrm{H}^1(k, \mathrm{Pic}\,\overline{X}) = \begin{cases} \mathbb{Z}/2 & \text{in cases (i) and (ii) of Proposition 1·8;} \\ 0 & \text{otherwise.} \end{cases}$$

Therefore, in cases (i) and (ii) of Proposition 1·8, 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 $R^1_{K/k}\mathbb{G}_m$.

Downloaded from https://www.cambridge.org/core. The University of Reading, on 03 Mar 2022 at 12:42:21, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/S0305004121000268

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 1·3), see Propositions 6·15 and 6·21. The proof uses the first obstruction to the HNP, along with various tricks involving moving between subextensions as detailed in Section 3.

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 [**21**] (ordering by discriminant) and [**22**] (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 [**46**].

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 Proposition 1·8 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 1·10. *Let K/k be a quartic extension of number fields with normal closure L/k such that $G = \mathrm{Gal}(L/k)$ is isomorphic to A_4. Let F be the fixed field of the copy of V_4 in G. Then*

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

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 $R^1_{K/k}\mathbb{G}_m$ if and only if it holds for $R^1_{L/F}\mathbb{G}_m$.

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 [**42**], 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 capitalise on recent advances in counting within families of number fields, see e.g. [**1**, **4**, **5**, **6**, **8**, **18**, **23**, **32**, **44**, **55**], and contribute to the ongoing rapid progress in the area of rational points and failures of local-global principles in families of varieties. See [**12**] 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 [**43**]) predicts that the number $N(k, G, X)$ of degree n extensions K of a number field k with Galois group G and $|N_{k/\mathbb{Q}}(\mathrm{Disc}_{K/k})| \leq X$ satisfies

$$X^{\frac{1}{a(G)}} \ll N(k, G, X) \ll X^{\frac{1}{a(G)}+\epsilon}, \tag{1·2}$$

where $a(G) = \min_{g \in G\setminus\{1\}}\{\mathrm{ind}(g)\}$ and $\mathrm{ind}(g)$ equals n minus the number of orbits of g on $\{1, \ldots, n\}$. Using a computational method developed by Hoshi and Yamasaki to determine $\mathrm{H}^1(k, \mathrm{Pic}\,\overline{X})$ (see Section 6·2), we obtain the following consequence of this conjecture:

Downloaded from https://www.cambridge.org/core. The University of Reading, on 03 Mar 2022 at 12:42:21, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/S0305004121000268

THEOREM 1·11. *Fix a number field k and an integer $n \leq 15$ with $n \neq 8, 12$. Suppose that Conjecture (1·2) 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.*

In fact, the assertions of Theorem 1·11 remain true if one only assumes Conjecture (1·2) for a few transitive subgroups of S_n, see Remark 6·13(iii). An analysis of the invariant $\mathrm{H}^1(k, \mathrm{Pic}\,\overline{X})$ for extensions K/k of degree $n \leq 15$ has also recently been carried out independently by Hoshi, Kanai and Yamasaki in [**35**] and [**36**]. In these works, the computation of $\mathrm{H}^1(k, \mathrm{Pic}\,\overline{X})$ for such extensions (which in the present paper happened behind the scenes of the proof of Theorem 1·11) is made explicit and, additionally, necessary and sufficient conditions for the vanishing of $\mathfrak{K}(K/k)$ are given.

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 [**21**, theorem 1·7], for example. Our next result addresses this issue. Let G be a finite group and H a subgroup of G. We define a (G, H)-extension of a number field k to be an extension K/k for which there exists a Galois extension L/k containing K/k such that $\mathrm{Gal}(L/k) \cong G$ and $\mathrm{Gal}(L/K) \cong H$. We write $F_{G/H}$ for a flasque module in a flasque resolution of the Chevalley module $J_{G/H}$, see Section 2.

THEOREM 1·12. *Let G be a finite group and H a subgroup of G. Then:*

(i) *there exist a number field k and a (G, H)-extension of k satisfying the HNP and, furthermore, if $\mathrm{H}^1(G, F_{G/H}) \neq 0$ then weak approximation fails for the norm one torus associated to this extension*;
(ii) *there exist a number field k and a (G, H)-extension of k whose norm one torus satisfies weak approximation and, furthermore, if $\mathrm{H}^1(G, F_{G/H}) \neq 0$ then this extension fails the HNP.*

The condition $\mathrm{H}^1(G, F_{G/H}) \neq 0$ in Theorem 1·12 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 $\mathrm{H}^1(k, \mathrm{Pic}\,\overline{X}) = \mathrm{H}^1(G, F_{G/H})$. This is due to Colliot-Thélène and Sansuc (see Theorem 2·2).

It is interesting to compare Theorem 1·12 with [**21**, 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 1·12, may be of quite large degree over $\mathbb{Q}$. In Section 7, we give explicit examples of extensions of number fields illustrating all cases of Proposition 1·8. 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 some relevant background material concerning the arithmetic of algebraic tori. In Section 3 we gather results that allow one to transfer information regarding

Downloaded from https://www.cambridge.org/core. The University of Reading, on 03 Mar 2022 at 12:42:21, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/S0305004121000268

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 4 we prove Theorem 1·1 and Corollary 1·2. In Section 5 we introduce generalised representation groups and outline work of Drakokhrust which uses these groups to describe the invariant $\mathrm{H}^1(k, \operatorname{Pic}\overline{X})$ occurring in Voskresenskiĭ's exact sequence (1·1). In Section 6 we apply our results to extensions whose normal closure has Galois group A_n or S_n, proving Theorems 1·3 and 1·4, Corollary 1·6, Propositions 1·8 and 1·9, Corollary 1·10 and Theorem 1·11. In Section 7 we prove Theorem 1·12 and give examples of successes and failures of the HNP in all cases covered by Proposition 1·8.

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;
O_k	the ring of integers of k;
Ω_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 $\operatorname{Spec}(K[t, t^{-1}])$ of K (when 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;
$\operatorname{Pic} X$	the Picard group of X;
$\widehat{T}$	the character group $\operatorname{Hom}(\overline{T}, \mathbb{G}_{m,\overline{K}})$ of T;
$R_{K/k}T$	the Weil restriction of T to a subfield k of K;
$R^1_{K/k}\mathbb{G}_m$	the kernel of the norm map $N_{K/k} : R_{K/k}\mathbb{G}_m \to \mathbb{G}_{m,k}$.

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

$$Ш(T) := \operatorname{Ker}\left(\mathrm{H}^1(k, T) \to \prod_{v\in\Omega_k} \mathrm{H}^1(k_v, T)\right) \text{ and } A(T) := \left(\prod_{v\in\Omega_k} T(k_v)\right)/\overline{T(k)},$$

respectively.

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

$\lvert G\rvert$	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 $\operatorname{Hom}(G, \mathbb{Q}/\mathbb{Z})$ of G;
G_p	a Sylow p-subgroup of G;

Downloaded from https://www.cambridge.org/core. The University of Reading, on 03 Mar 2022 at 12:42:21, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/S0305004121000268

$\hat{\mathrm{H}}^q(G, A)$ the Tate cohomology group;
$Ш^q_\omega(G, A)$ the kernel of the restriction map $\hat{\mathrm{H}}^q(G, A) \xrightarrow{\mathrm{Res}} \prod_{g\in G} \hat{\mathrm{H}}^q(\langle g\rangle, A)$.

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 use the following notation:

$G[d]$ the d-torsion of G;
$G_{(d)}$ the d-primary part of G.

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

2. *Preliminaries on the arithmetic of algebraic tori*

Let T be a torus over a number field k. As mentioned above, Voskresenskiĭ's exact sequence ties together the Tate–Shafarevich group $Ш(T)$ and the defect of weak approximation $A(T)$:

THEOREM 2·1 (Voskresenskiĭ). *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*

$$0 \to A(T) \to \mathrm{H}^1(k, \mathrm{Pic}\,\overline{X})^\sim \to Ш(T) \to 0. \tag{2·1}$$

Proof. See [**52**, theorem 6].

Voskresenskiĭ proved Theorem 2·1 by considering the following exact sequence of Galois modules:

$$0 \to \widehat{T} \to \mathrm{Div}_{\overline{X}-\overline{T}}\,\overline{X} \to \mathrm{Pic}\,\overline{X} \to 0, \tag{2·2}$$

where $\widehat{T}$ denotes the group of characters of T. The key point is that (2·2) is a *flasque resolution* of the Galois module $\widehat{T}$. We explain this concept below (see [**13**] and [**14**] 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 $\hat{\mathrm{H}}^{-1}(G', A) = 0$ 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 $[A]$.

Recall that if T is split by a Galois subextension L/k of $\overline{k}/k$, then $\mathrm{Gal}(\overline{k}/L)$ acts trivially on the character group $\widehat{T} = \mathrm{Hom}(\overline{T}, \mathbb{G}_{m,\overline{k}})$ and thus $\widehat{T}$ is a $\mathrm{Gal}(L/k)$-module. Implicit in much of our work is the fact that the norm one torus $R^1_{K/k}\mathbb{G}_m$ is split by any Galois extension of k containing K. The followng result shows that the group $\mathrm{H}^1(k, \mathrm{Pic}\,\overline{X})$ has a simple cohomological description and can be computed using *any* flasque resolution of $\widehat{T}$.

Downloaded from https://www.cambridge.org/core. The University of Reading, on 03 Mar 2022 at 12:42:21, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/S0305004121000268

THEOREM 2·2 (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 $G = \mathrm{Gal}(L/k)$. Let*

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

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

$$\mathrm{H}^1(k, \mathrm{Pic}\,\overline{X}) = \mathrm{H}^1(G, \mathrm{Pic}\,X_L) = \mathrm{H}^1(G, F). \tag{2·3}$$

Additionally,

$$\mathrm{H}^1(G, F) = Ш^2_\omega(G, \widehat{T}) := \mathrm{Ker}\left(\mathrm{H}^2(G, \widehat{T}) \xrightarrow{\mathrm{Res}} \prod_{g \in G} \mathrm{H}^2(\langle g \rangle, \widehat{T})\right). \tag{2·4}$$

In the special case where $T = R^1_{L/k}\mathbb{G}_m$, we have

$$Ш^2_\omega(G, \widehat{T}) = \mathrm{H}^2(G, \widehat{T}) = \mathrm{H}^3(G, \mathbb{Z}). \tag{2·5}$$

Proof. See [**13**, lemme 5 and proposition 6] for the proof of (2·3). The isomorphism $\mathrm{H}^1(G, F) = Ш^2_\omega(G, \widehat{T})$ is proved in [**14**, proposition 9·5(ii)]. The final assertion for $R^1_{L/k}\mathbb{G}_m$ follows from its defining sequence.

The Tate–Shafarevich group $Ш(T)$ also has a description in terms of the cohomology of $\widehat{T}$:

THEOREM 2·3 (Tate). *Let T be a torus defined over a number field k and split by a finite Galois extension L/k with $G = \mathrm{Gal}(L/k)$. Then Poitou–Tate duality gives a canonical isomorphism*

$$Ш(T)^\sim = Ш^2(G, \widehat{T}), \tag{2·6}$$

where $Ш^2(G, \widehat{T}) = \mathrm{Ker}(\mathrm{H}^2(G, \widehat{T}) \xrightarrow{\mathrm{Res}} \prod_{v \in \Omega_k} \mathrm{H}^2(D_v, \widehat{T}))$. In the special case where $T = R^1_{L/k}\mathbb{G}_m$,

$$Ш(T)^\sim = \mathrm{Ker}\left(\mathrm{H}^3(G, \mathbb{Z}) \xrightarrow{\mathrm{Res}} \prod_{v \in \Omega_k} \mathrm{H}^3(D_v, \mathbb{Z})\right), \tag{2·7}$$

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

Proof. This is the case $i = 1$ of [**45**, theorem 6·10]. For the case $T = R^1_{L/k}\mathbb{G}_m$, see [**50**, p· 198].

PROPOSITION 2·4. *Let T be a torus defined over a number field k and split by a finite Galois extension L/k with $G = \mathrm{Gal}(L/k)$. Then taking duals in Voskresenskiĭ's exact sequence (2·1) yields the exact sequence*

$$0 \to Ш^2(G, \widehat{T}) \to Ш^2_\omega(G, \widehat{T}) \to A(T)^\sim \to 0, \tag{2·8}$$

where the map $Ш^2(G, \widehat{T}) \to Ш^2_\omega(G, \widehat{T})$ is the natural inclusion arising from the Chebotarev density theorem.

Downloaded from https://www.cambridge.org/core. The University of Reading, on 03 Mar 2022 at 12:42:21, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/S0305004121000268

Proof. This follows from the proof of [**52**, theorem 6] and isomorphisms (2·4) and (2·6).

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. Taking character modules in the defining sequence for T shows that $\widehat{T}$ is isomorphic to the G-module $J_{G/H}$, defined as follows:

Definition 2·5 (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 $J_{G/H} = \operatorname{coker} \eta$ is called the *Chevalley module of* G/H.

Furthermore, for $T = R^1_{K/k}\mathbb{G}_m$ we have

$$Ш(T) = \text{Ř}(K/k)$$

(see [**45**, p· 307]). Hence, Theorem 2·1 gives a necessary and sufficient condition for the simultaneous validity of the HNP for K/k and weak approximation for T, namely the vanishing of $\mathrm{H}^1(k, \operatorname{Pic} \overline{X})$.

LEMMA 2·6. *Let K/k be a finite extension and let X be a smooth compactification of $T = R^1_{K/k}\mathbb{G}_m$. Then $T \times_k K$ is stably rational. Consequently,* $\mathrm{H}^1(K, \operatorname{Pic} \overline{X}) = 0$ *and* $\mathrm{H}^1(k, \operatorname{Pic} \overline{X})$ *is killed by* $[K : k]$.

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

$$1 \to T_K \to (R_{K/k}\mathbb{G}_m) \times_k K \xrightarrow{N_{K/k}} \mathbb{G}_{m,K} \to 1. \tag{2·9}$$

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

$$0 \to \mathbb{Z} \xrightarrow{N_{G/H}} \mathbb{Z}[G/H] \to \widehat{T_K} \to 0 \tag{2·10}$$

where $N_{G/H} : 1 \mapsto \sum_{gH \in G/H} gH$. The map $\sum_{gH \in G/H} a_{gH} \cdot gH \mapsto a_H$ defines a left splitting of (2·10). Therefore, (2·9) splits and consequently

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

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

The corollary below is an immediate consequence of Theorem 2·1 and Lemma 2·6.

COROLLARY 2·7. *Let $T = R^1_{K/k}\mathbb{G}_m$. Then $A(T)$ and* Ř(K/k) *are killed by* $[K : k]$.

Downloaded from https://www.cambridge.org/core. The University of Reading, on 03 Mar 2022 at 12:42:21, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/S0305004121000268

3. *Using subextensions and superextensions*

Let k be a number field. In order to study the HNP and weak approximation in non-Galois extensions of k, it is often useful to be able to deduce information about the knot group of an extension K/k from information about its subextensions or superextensions, the latter meaning extensions of k containing K. In this section we collect some results that serve this purpose.

LEMMA 3·1. *Let $\phi : T_1 \to T_2$ be a morphism of algebraic tori over k, and let X_1 and X_2 be smooth compactifications of T_1 and T_2, respectively. Then we obtain a commutative diagram with exact rows as follows, where the vertical arrows are induced by ϕ:*

$$\begin{array}{ccccccccc} 0 & \longrightarrow & A(T_1) & \longrightarrow & \mathrm{H}^1(k, \mathrm{Pic}\,\overline{X_1})^{\sim} & \longrightarrow & Ш(T_1) & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & A(T_2) & \longrightarrow & \mathrm{H}^1(k, \mathrm{Pic}\,\overline{X_2})^{\sim} & \longrightarrow & Ш(T_2) & \longrightarrow & 0. \end{array}$$

Proof. This follows from Voskresenskiĭ's proof of [**52**, theorem 6].

COROLLARY 3·2. *Let $\phi : T_1 \to T_2$ be an isogeny of algebraic tori over k with kernel μ. Let X_1 and X_2 be smooth compactifications of T_1 and T_2, respectively. Then for any prime p such that $p \nmid |\mu(\bar{k})|$, we obtain a commutative diagram with exact rows as follows, where the vertical isomorphisms are induced by ϕ:*

$$\begin{array}{ccccccccc} 0 & \longrightarrow & A(T_1)_{(p)} & \longrightarrow & \mathrm{H}^1(k, \mathrm{Pic}\,\overline{X_1})^{\sim}_{(p)} & \longrightarrow & Ш(T_1)_{(p)} & \longrightarrow & 0 \\ & & \cong\downarrow & & \cong\downarrow & & \cong\downarrow & & \\ 0 & \longrightarrow & A(T_2)_{(p)} & \longrightarrow & \mathrm{H}^1(k, \mathrm{Pic}\,\overline{X_2})^{\sim}_{(p)} & \longrightarrow & Ш(T_2)_{(p)} & \longrightarrow & 0. \end{array}$$

Proof. Let $\psi : T_2 \to T_1$ be the dual isogeny. Then $\psi \circ \phi$ is multiplication by $|\mu(\bar{k})|$ on T_1. Now apply Lemma 3·1.

The following theorem is an application of Corollary 3·2 to norm one tori which will be very useful later in this section as well as in Section 6.

THEOREM 3·3. *Let $L/K/k$ be a tower of finite extensions. Let $T_0 = R^1_{L/k}\mathbb{G}_m$, let $T = R^1_{K/k}\mathbb{G}_m$ and let X_0 and X be smooth compactifications of T_0 and T, respectively. Then for a prime p with $p \nmid [L : K]$ we obtain a commutative diagram with exact rows as follows, where the vertical isomorphisms are induced by the natural inclusion $j : T \hookrightarrow T_0$:*

$$\begin{array}{ccccccccc} 0 & \longrightarrow & A(T)_{(p)} & \longrightarrow & \mathrm{H}^1(k, \mathrm{Pic}\,\overline{X})^{\sim}_{(p)} & \longrightarrow & Ш(T)_{(p)} & \longrightarrow & 0 \\ & & \cong\downarrow & & \cong\downarrow & & \cong\downarrow & & \\ 0 & \longrightarrow & A(T_0)_{(p)} & \longrightarrow & \mathrm{H}^1(k, \mathrm{Pic}\,\overline{X_0})^{\sim}_{(p)} & \longrightarrow & Ш(T_0)_{(p)} & \longrightarrow & 0. \end{array}$$

Alternatively, the norm map $N_{L/K} : T_0 \twoheadrightarrow T$ can be used to obtain a similar commutative diagram with the direction of the vertical isomorphisms reversed.

Downloaded from https://www.cambridge.org/core. The University of Reading, on 03 Mar 2022 at 12:42:21, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/S0305004121000268

Proof. Let S be the kernel of $N_{L/K} : R_{L/k}\mathbb{G}_m \to R_{K/k}\mathbb{G}_m$ and let $i : S \to R_{L/k}\mathbb{G}_m$ be the inclusion. Then the following diagram with exact rows commutes:

$$\begin{array}{ccccccccc} 1 & \longrightarrow & S & \xrightarrow{i} & R^1_{L/k}\mathbb{G}_m & \xrightarrow{N_{L/K}} & R^1_{K/k}\mathbb{G}_m & \longrightarrow & 1 \\ & & \| & & \downarrow & & \downarrow & & \\ 1 & \longrightarrow & S & \xrightarrow{i} & R_{L/k}\mathbb{G}_m & \xrightarrow{N_{L/K}} & R_{K/k}\mathbb{G}_m & \longrightarrow & 1. \end{array}$$

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

$$S \times R_{K/k}\mathbb{G}_m \to R_{L/k}\mathbb{G}_m$$

whose kernel μ is finite for dimension reasons. Moreover, since $N_{L/K} \circ j = [d]$, μ is killed by d. Let Z, W and W_0 be smooth compactifications of S, $R_{K/k}\mathbb{G}_m$ and $R_{L/k}\mathbb{G}_m$, respectively. By [**52**, lemma 3], $\mathrm{Pic}(\overline{Z \times W}) = \mathrm{Pic}\,\overline{Z} \oplus \mathrm{Pic}\,\overline{W}$. Thus, Corollary 3·2 yields

$$\mathrm{H}^1(k, \mathrm{Pic}\,\overline{Z})_{(p)} \oplus \mathrm{H}^1(k, \mathrm{Pic}\,\overline{W})_{(p)} \cong \mathrm{H}^1(k, \mathrm{Pic}\,\overline{W_0})_{(p)}.$$

Furthermore, $R_{K/k}\mathbb{G}_m$ and $R_{L/k}\mathbb{G}_m$ are k-rational so $\mathrm{H}^1(k, \mathrm{Pic}\,\overline{W}) = \mathrm{H}^1(k, \mathrm{Pic}\,\overline{W_0}) = 0$ and hence $\mathrm{H}^1(k, \mathrm{Pic}\,\overline{Z})_{(p)} = 0$. Therefore, $Ш(S)_{(p)} = A(S)_{(p)} = 0$ by Theorem 2·1. Now the result follows from applying Corollary 3·2 to the surjective morphism

$$S \times R^1_{K/k}\mathbb{G}_m \to R^1_{L/k}\mathbb{G}_m$$

whose finite kernel is killed by d.

The following special case of Theorem 3·3 reduces the calculation of $A(T)$, $\mathrm{H}^1(k, \mathrm{Pic}\,\overline{X})$ and $Ш(T)$ to the case where K/k is the fixed field of a p-group.

COROLLARY 3·4. *Let $L/K/k$ be a tower of finite extensions with L/k Galois. Let $G = \mathrm{Gal}(L/k)$ and $H = \mathrm{Gal}(L/K)$. For p prime, let H_p denote a Sylow p-subgroup of H and let K_p denote its fixed field. Let X and X_p be smooth compactifications of $T = R^1_{K/k}\mathbb{G}_m$ and $T_p = R^1_{K_p/k}\mathbb{G}_m$, respectively. Then we obtain a commutative diagram with exact rows as follows, where the vertical isomorphisms are induced by the natural inclusion $T \hookrightarrow T_p$:*

$$\begin{array}{ccccccccc} 0 & \longrightarrow & A(T)_{(p)} & \longrightarrow & \mathrm{H}^1(k, \mathrm{Pic}\,\overline{X})^{\sim}_{(p)} & \longrightarrow & Ш(T)_{(p)} & \longrightarrow & 0 \\ & & \cong\downarrow & & \cong\downarrow & & \cong\downarrow & & \\ 0 & \longrightarrow & A(T_p)_{(p)} & \longrightarrow & \mathrm{H}^1(k, \mathrm{Pic}\,\overline{X_p})^{\sim}_{(p)} & \longrightarrow & Ш(T_p)_{(p)} & \longrightarrow & 0. \end{array}$$

Alternatively, the norm map $N_{K_p/K} : T_p \twoheadrightarrow T$ can be used to obtain a similar commutative diagram with the direction of the vertical isomorphisms reversed.

As a consequence of Corollary 3·4, we obtain the following result which deals with the two extremes in terms of the power of p dividing $|H|$.

COROLLARY 3·5. *Retain the notation of Corollary 3·4.*

(i) *If $p \nmid |H|$, then $\mathrm{H}^1(k, \mathrm{Pic}\,\overline{X})_{(p)} \cong \mathrm{H}^3(G, \mathbb{Z})_{(p)}$.*

Downloaded from https://www.cambridge.org/core. The University of Reading, on 03 Mar 2022 at 12:42:21, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/S0305004121000268

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

Proof.

(i) Follows from Theorem 2·2 and Corollary 3·4.
(ii) Follows from Lemma 2·6.

We additionally obtain the following result when H is a *Hall subgroup* of G, i.e. a subgroup such that $\gcd(|H|, [G : H]) = 1$.

COROLLARY 3·6. *Retain the notation of Corollary 3·4. If H is a Hall subgroup of G, then*

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

where $T = R^1_{K/k}\mathbb{G}_m$ and $T_0 = R^1_{L/k}\mathbb{G}_m$.

Proof. Follows from Corollaries 3·4 and 3·5, Lemma 2·6 and Corollary 2·7.

We now drop the assumption that L/k is Galois and return to the more general setting of Theorem 3·3.

COROLLARY 3·7. *Retain the notation of Theorem 3·3. Then*:

(i) *$A(T)$ is killed by $[L : K] \cdot \exp(A(T_0))$;*
(ii) *$\mathrm{H}^1(k, \mathrm{Pic}\,\overline{X})$ is killed by $[L : K] \cdot \exp(\mathrm{H}^1(k, \mathrm{Pic}\,\overline{X_0}))$;*
(iii) *$Ш(T)$ is killed by $[L : K] \cdot \exp(Ш(T_0))$.*

Proof. We give the proof for $A(T)$ – the other proofs are analogous. Let $d = [L : K]$, $e = \exp(A(T_0))$ and let $x \in A(T)$. Since $N_{L/K} \circ j = [d]$, we have $x^{de} = N_{L/K}(j(x)^e) = 1$, as $j(x) \in A(T_0)$.

COROLLARY 3·8. *Retain the notation of Theorem 3·3.*

(i) *If $\exp(A(T_0)) \cdot [L : K]$ is coprime to $[K : k]$, then weak approximation holds for T.*
(ii) *If $\exp(Ш(T_0)) \cdot [L : K]$ is coprime to $[K : k]$, then the HNP holds for K/k.*

Proof. This follows immediately from Corollaries 3·7 and 2·7.

The following result is a slight generalisation of [**29**, proposition 1].

Downloaded from https://www.cambridge.org/core. The University of Reading, on 03 Mar 2022 at 12:42:21, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/S0305004121000268

PROPOSITION 3·9. *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*

$$\varphi : Ш(K/k) \to Ш(L/k)$$

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

Proof. This follows from the fact that under the identification of $\mathrm{H}^1(k, R^1_{K/k}\mathbb{G}_m)$ and $\mathrm{H}^1(k, R^1_{L/k}\mathbb{G}_m)$ with $k^*/N_{K/k}K^*$ and $k^*/N_{L/k}L^*$, the maps j and $N_{L/K}$ from Theorem 3·3 induce multiplication by d and projection respectively. Alternatively, observe that the proposition follows from the inclusions $N_{L/k}\mathbb{A}_L^* \subset N_{K/k}\mathbb{A}_K^*$, $N_{L/k}L^* \subset N_{K/k}K^*$, $(N_{K/k}\mathbb{A}_K^*)^d \subset N_{L/k}\mathbb{A}_L^*$ and $(N_{K/k}K^*)^d \subset N_{L/k}L^*$. If $|Ш(K/k)|$ is coprime to d, then $\mathrm{Im}\,\varphi \subset \{x^d \mid x \in Ш(L/k)\}$.

Next, we establish a generalisation of Gurak's criterion (see [**29**, proposition 2]) for the validity of the HNP in a compositum of two subextensions with coprime degrees.

PROPOSITION 3·10. *Let L/k be a finite extension with subextensions K/k and M/k such that $L = KM$. Let $T = R^1_{L/k}\mathbb{G}_m$, $T_1 = R^1_{K/k}\mathbb{G}_m$ and $T_2 = R^1_{M/k}\mathbb{G}_m$ and let X, X_1 and X_2 be their respective smooth compactifications. Then we obtain a commutative diagram with exact rows as follows, where the vertical homomorphisms are induced by the natural inclusions $T_1 \hookrightarrow T$ and $T_2 \hookrightarrow T$:*

$$\begin{array}{ccccccccc}
0 & \longrightarrow & A(T_1) \oplus A(T_2) & \longrightarrow & \mathrm{H}^1(k, \mathrm{Pic}\,\overline{X_1})^{\sim} \oplus \mathrm{H}^1(k, \mathrm{Pic}\,\overline{X_2})^{\sim} & \longrightarrow & Ш(T_1) \oplus Ш(T_2) & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & A(T) & \longrightarrow & \mathrm{H}^1(k, \mathrm{Pic}\,\overline{X})^{\sim} & \longrightarrow & Ш(T) & \longrightarrow & 0.
\end{array}$$

If $[K : k]$ and $[M : k]$ are coprime, then the vertical maps in the diagram are isomorphisms.

Proof. The commutative diagram comes from Lemma 3·1. If $[K : k]$ and $[M : k]$ are coprime, then any prime number divides at most one of $[L : K]$ and $[L : M]$, whence Lemma 2·6 and Theorem 3·3 show that the vertical maps in the diagram are isomorphisms.

PROPOSITION 3·11. *In the notation of Proposition 3·10, the map* $Ш(T_1) \oplus Ш(T_2) \to Ш(T)$ *induces the following homomorphism on the relevant knot groups*

$$\begin{aligned} \varphi : Ш(K/k) \times Ш(M/k) &\to Ш(L/k) \\ (x, y) &\mapsto x^n y^m, \end{aligned}$$

where $m = [L : M]$ *and* $n = [L : K]$. *Moreover, if* $a = \exp(Ш(K/k))$, $b = \exp(Ш(M/k))$, *and* $h = \gcd(m, n)$, *then* φ *satisfies* $\mathrm{Ker}\varphi \subset Ш(K/k)[bn] \times Ш(M/k)[am]$ *and* $\{z^h \mid z \in Ш(L/k)\} \subset \mathrm{Im}\,\varphi$.

Proof. This follow from the argument in the proof of Proposition 3·9.

Downloaded from https://www.cambridge.org/core. The University of Reading, on 03 Mar 2022 at 12:42:21, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/S0305004121000268

We end this section by proving a version of [**29**, theorem 1] for weak approximation in nilpotent Galois extensions. We require the following description of the defect of weak approximation:

PROPOSITION 3·12. *Let T be a torus defined over a number field k and split by a finite Galois extension L/k with $G = \mathrm{Gal}(L/k)$. Then*

$$A(T)^{\sim} = \mathrm{Im}\left(Ш^2_{\omega}(G, \widehat{T}) \xrightarrow{\mathrm{Res}} \prod_{v \in \Omega_k} \mathrm{H}^2(D_v, \widehat{T}) \right), \tag{3·1}$$

where $D_v = \mathrm{Gal}(L_v/k_v)$ is the decomposition group at v. If $T = R^1_{L/k}\mathbb{G}_m$ then

$$A(T)^{\sim} = \mathrm{Im}\left(\mathrm{H}^3(G, \mathbb{Z}) \xrightarrow{\mathrm{Res}} \prod_{v \in \Omega_k} \mathrm{H}^3(D_v, \mathbb{Z}) \right). \tag{3·2}$$

Proof. The equality in (3·1) follows from Proposition 2·4. Then (3·2) follows from the isomorphism (2·5) of Theorem 2·2 and the analogous result that $\mathrm{H}^2(D_v, \widehat{T}) = \mathrm{H}^3(D_v, \mathbb{Z})$ in this setting.

We make use of the following weak approximation version of [**28**, lemma 2·3]:

LEMMA 3·13. *Let K/k and M/k be finite subextensions of L/k such that $[K : k]$ and $[M : k]$ are coprime. If weak approximation holds for $R^1_{KM/M}\mathbb{G}_m$, then it holds for $R^1_{K/k}\mathbb{G}_m$. Under the additional assumption that K/k is Galois, weak approximation for $R^1_{K/k}\mathbb{G}_m$ implies weak approximation for $R^1_{KM/M}\mathbb{G}_m$.*

Proof. Let $T = R^1_{K/k}\mathbb{G}_m$, $T_M = T \times_k M$ and $T_K = T \times_k K$. Suppose first that weak approximation holds for $R^1_{KM/M}\mathbb{G}_m = T_M$. By Lemma 2·6 and Theorem 2·1, weak approximation holds for T_K. To complete the proof, observe that weak approximation for T_K and T_M implies weak approximation for $R_{K/k}T_K$ and $R_{M/k}T_M$. Since $[K : k]$ and $[M : k]$ are coprime, the surjective morphism of algebraic groups

$$\begin{aligned} R_{K/k}T_K \times R_{M/k}T_M &\to T \\ (x, y) &\to N_{K/k}(x)N_{M/k}(y) \end{aligned}$$

has a section. Therefore, weak approximation for T follows from weak approximation for $R_{K/k}T_K$ and $R_{M/k}T_M$.

Now suppose that K/k is Galois and that weak approximation holds for $R^1_{K/k}\mathbb{G}_m$. Then KM/M is Galois with Galois group isomorphic to $\mathrm{Gal}(K/k)$. Let w be a place of M and let v be the place of k lying below w. The various restriction maps give a commutative diagram

$$\begin{array}{ccc} \mathrm{H}^3(\mathrm{Gal}(K/k), \mathbb{Z}) & \xrightarrow{\cong} & \mathrm{H}^3(\mathrm{Gal}(KM/M), \mathbb{Z}) \\ \downarrow{\scriptstyle \mathrm{Res}_v} & & \downarrow{\scriptstyle \mathrm{Res}_w} \\ \mathrm{H}^3(D_v, \mathbb{Z}) & \longrightarrow & \mathrm{H}^3(D_w, \mathbb{Z}). \end{array}$$

Downloaded from https://www.cambridge.org/core. The University of Reading, on 03 Mar 2022 at 12:42:21, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/S0305004121000268

Since weak approximation holds for $R^1_{K/k}\mathbb{G}_m$, isomorphism (3·2) of Proposition 3·12 shows that Res_v is trivial, and hence Res_w is also trivial. As w was arbitrary, weak approximation for $R^1_{KM/M}\mathbb{G}_m$ follows from (3·2).

Remark 3·14. The hypothesis that K/k is Galois in the second implication of Lemma 3·13 is necessary. To see this, consider a Galois extension L/k with Galois group $G = C_3 \times S_3$ and with a decomposition group D_v containing the Sylow 3-subgroup of G for some place v of k (such an extension always exists, see Section 7). Let K/k and M/k be subextensions of L/k of degree 9 and 2, respectively. One can verify that the invariant $\mathrm{H}^1(k, \mathrm{Pic}\,\overline{X})$ vanishes for K/k and thus weak approximation holds for $R^1_{K/k}\mathbb{G}_m$ by Theorem 2·1. On the other hand, $KM/M = L/M$ is Galois with Galois group $C_3 \times C_3$ and decomposition group $C_3 \times C_3$ for a prime of M above v. It follows that weak approximation fails for $R^1_{KM/M}\mathbb{G}_m$ by isomorphism (3·2) of Proposition 3·12. See [**38**] for some other examples of varieties over number fields that satisfy weak approximation over the base field but not over a quadratic extension.

We also require the following well-known fact:

PROPOSITION 3·15. *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*

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

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

Proof. See, for example, [**11**, theorem III·10·3].

PROPOSITION 3·16. *Let L/k be a Galois extension such that $G = \mathrm{Gal}(L/k)$ 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 $R^1_{L/k}\mathbb{G}_m$;*
(ii) *weak approximation holds for each $R^1_{L_p/k}\mathbb{G}_m$;*
(iii) *weak approximation holds for each $R^1_{L/k_p}\mathbb{G}_m$.*

Proof.
(i) $\Longrightarrow$ (ii): follows from Corollary 3·8.
(ii) $\Longrightarrow$ (iii): follows from Lemma 3·13.
(iii) $\Longrightarrow$ (i): we prove $A(R^1_{L/k}\mathbb{G}_m)_{(p)} = 0$ for every prime p. Let v be a place of k and let w be a place of k_p above v. The various restriction maps give a commutative diagram

$$\begin{array}{ccc} \mathrm{H}^3(G, \mathbb{Z})_{(p)} & \xrightarrow{\mathrm{Res}_1} & \mathrm{H}^3(D_v, \mathbb{Z})_{(p)} \\ \downarrow{\scriptstyle \mathrm{Res}_4} & & \downarrow{\scriptstyle \mathrm{Res}_2} \\ \mathrm{H}^3(G_p, \mathbb{Z}) & \xrightarrow{\mathrm{Res}_3} & \mathrm{H}^3(D_w, \mathbb{Z}). \end{array}$$

Downloaded from https://www.cambridge.org/core. The University of Reading, on 03 Mar 2022 at 12:42:21, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/S0305004121000268

As weak approximation holds for $R^1_{L/k_p}\mathbb{G}_m$, isomorphism (3·2) of Proposition 3·12 yields $\operatorname{Im}\operatorname{Res}_3 = 0$. Furthermore, Proposition 3·15 shows that Res_2 is injective. It follows that $\operatorname{Im}\operatorname{Res}_1 = 0$ and, since v was arbitrary, we conclude that $A(R^1_{L/k}\mathbb{G}_m)_{(p)} = 0$ by (3·2).

Remark 3·17. We note that the implication (iii) $\Longrightarrow$ (i) in Proposition 3·16 does not require the hypothesis that G is nilpotent. This is analogous to the corresponding result for the HNP – see Gurak's remarks preceding [**29**, theorem 2].

4. *The first obstruction to the Hasse norm principle*

In this section, we give some background concerning the first obstruction to the Hasse norm principle and then go on to prove Theorem 1·1 and Corollary 1·2. Throughout the section, we fix a tower of number fields $L/K/k$ such that L/k is Galois. Let X and X_0 be smooth compactifications of the tori $R^1_{K/k}\mathbb{G}_m$ and $R^1_{L/k}\mathbb{G}_m$, respectively. Applying Lemma 3·1 to the norm map $N_{L/K} : R^1_{L/k}\mathbb{G}_m \to R^1_{K/k}\mathbb{G}_m$ gives a commutative diagram with exact rows as follows, where the vertical arrows are induced by $N_{L/K}$:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & A(R^1_{L/k}\mathbb{G}_m) & \longrightarrow & \mathrm{H}^1(k, \operatorname{Pic}\overline{X_0})^{\sim} & \longrightarrow & Ш(R^1_{L/k}\mathbb{G}_m) & \longrightarrow & 0 \\ & & \downarrow & & \downarrow{\scriptstyle f_{L/K}} & & \downarrow{\scriptstyle g_{L/K}} & & \\ 0 & \longrightarrow & A(R^1_{K/k}\mathbb{G}_m) & \longrightarrow & \mathrm{H}^1(k, \operatorname{Pic}\overline{X})^{\sim} & \longrightarrow & Ш(R^1_{K/k}\mathbb{G}_m) & \longrightarrow & 0. \end{array} \tag{4·1}$$

Definition 4·1. In the notation of diagram (4·1), we define

(i) $\mathfrak{F}(L/K/k) := \operatorname{Coker}(g_{L/K}) = (k^* \cap N_{K/k}\mathbb{A}_K^*)/(k^* \cap N_{L/k}\mathbb{A}_L^*)N_{K/k}K^*$, called the *first obstruction to the HNP for K/k corresponding to the tower $L/K/k$*, see [**17**, Definition 1];

(ii) $\mathfrak{F}_{nr}(L/K/k) := \operatorname{Coker}(f_{L/K})$, called the *unramified cover of* $\mathfrak{F}(L/K/k)$.

Clearly the knot group $\mathfrak{K}(K/k)$ (which is sometimes called the total obstruction to the HNP) surjects 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 [**17**], Drakokhrust and Platonov give another very useful sufficient criterion for this equality to hold, as follows:

THEOREM 4·2. [**17**, theorem 3] *Set $G = \operatorname{Gal}(L/k)$, $H = \operatorname{Gal}(L/K)$. 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*

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

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

In order to compute $\mathfrak{F}(L/K/k)$, 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

Downloaded from https://www.cambridge.org/core. The University of Reading, on 03 Mar 2022 at 12:42:21, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/S0305004121000268

let S be a set of subgroups of G. Consider the following commutative diagram:

$$\begin{array}{ccc} H/[H,H] & \xrightarrow{\psi_1} & G/[G,G] \\ \uparrow{\scriptstyle \varphi_1} & & \uparrow{\scriptstyle \varphi_2} \\ \displaystyle\bigoplus_{D\in S}\left(\bigoplus_{Hx_iD\in H\backslash G/D} H_i/[H_i,H_i]\right) & \xrightarrow{\psi_2} & \displaystyle\bigoplus_{D\in S} D/[D,D], \end{array} \tag{4·2}$$

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 ψ_1, φ_1 and φ_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

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

Given a subgroup $D \in S$, we denote by ψ_2^D the restriction of the map ψ_2 in diagram (4·2) to the subgroup $\bigoplus_{Hx_iD\in H\backslash G/D} H_i/[H_i,H_i]$.

LEMMA 4·3. *In diagram (4·2), $\varphi_1(\mathrm{Ker}\psi_2^D) \subset \varphi_1(\mathrm{Ker}\psi_2^{D'})$ whenever $D \subset D'$.*

Proof. The proof follows in the same manner as the proof of [**17**, lemma 2].

LEMMA 4·4. [**17**, lemma 1] *Set $G = \mathrm{Gal}(L/k)$ and $H = \mathrm{Gal}(L/K)$. 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 $G = \bigcup_{i=1}^{r_v} Hx_iD_v$. If w corresponds to Hx_iD_v, then the decomposition group H_w of the extension L/K at w equals $H \cap x_iD_vx_i^{-1}$.*

Set $G = \mathrm{Gal}(L/k)$, $H = \mathrm{Gal}(L/K)$ and $S = \{D_v \mid v \in \Omega_k\}$. Lemma 4·4 shows that, with these choices, diagram (4·2) takes the form

$$\begin{array}{ccc} H/[H,H] & \xrightarrow{\psi_1} & G/[G,G] \\ \uparrow{\scriptstyle \varphi_1} & & \uparrow{\scriptstyle \varphi_2} \\ \displaystyle\bigoplus_{v\in\Omega_k}\left(\bigoplus_{w|v} H_w/[H_w,H_w]\right) & \xrightarrow{\psi_2} & \displaystyle\bigoplus_{v\in\Omega_k} D_v/[D_v,D_v], \end{array} \tag{4·3}$$

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 4·5. [**17**, theorem 1] *With the notation of diagram (4·3), there is a canonical isomorphism*

$$\mathfrak{F}(L/K/k) = \mathrm{Ker}\psi_1/\varphi_1(\mathrm{Ker}\psi_2).$$

We write ψ_2^{nr} for the restriction of the map ψ_2 to the subgroup

$$\bigoplus_{v \text{ unramified in } L/k}\left(\bigoplus_{w|v} H_w/[H_w,H_w]\right)$$

Downloaded from https://www.cambridge.org/core. The University of Reading, on 03 Mar 2022 at 12:42:21, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/S0305004121000268

and define ψ_2^r similarly using the ramified places.

LEMMA 4·6. *Set $G = \mathrm{Gal}(L/k)$ and $H = \mathrm{Gal}(L/K)$. Let C be the set of all cyclic subgroups of G and let φ_1^C and ψ_2^C denote the relevant maps in diagram (4·2) with $S = C$. Then*

$$\varphi_1(\mathrm{Ker}\psi_2^{nr}) = \varphi_1^C(\mathrm{Ker}\psi_2^C),$$

where the maps in the expression on the left are the ones in diagram (4·3).

Proof. This follows from the Chebotarev density theorem and Lemma 4·3.

Definition 4·7. Let H be a subgroup of a finite group G. The *focal subgroup of H in G* is

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

THEOREM 4·8. [**17**, theorem 2] *In the notation of diagram (4·3), we have*

$$\varphi_1(\mathrm{Ker}\psi_2^{nr}) = \Phi^G(H)/[H, H].$$

Theorem 4·8 is very useful – quite often one can show that $\Phi^G(H) = H \cap [G, G]$ and hence the first obstruction $\mathfrak{F}(L/K/k)$ 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 $\mathfrak{F}(L/K/k) = 1$. This criterion generalises [**29**, theorem 3].

Remark 4·9. The group $\mathrm{Ker}\psi_1/\varphi_1(\mathrm{Ker}\psi_2)$ featured in Theorem 4·5 can be computed in finite time. Indeed, $\mathrm{Ker}\psi_1$ is given in terms of the relevant Galois groups, and by [**17**, p· 307] we have

$$\varphi_1(\mathrm{Ker}\psi_2) = \varphi_1(\mathrm{Ker}\psi_2^{nr})\varphi_1(\mathrm{Ker}\psi_2^r). \tag{4·4}$$

Hence, Theorem 4·8 and the fact that only finitely many places of k ramify in L/k show that $\varphi_1(\mathrm{Ker}\psi_2)$ can be obtained by a finite computation. We combined these facts to assemble a function `1obs(G,H,l)` in GAP [**24**] that, given the groups $G = \mathrm{Gal}(L/k)$, $H = \mathrm{Gal}(L/K)$ and the list l of decomposition groups D_v at the ramified places v, returns the group $\mathrm{Ker}\psi_1/\varphi_1(\mathrm{Ker}\psi_2)$ isomorphic to the first obstruction $\mathfrak{F}(L/K/k)$. The code for this function is available at [**40**].

Our next task is to prove Theorem 1·1, which gives a purely group-theoretic description of $\mathfrak{F}_{nr}(L/K/k)$. First, recall the definition of the group $\mathfrak{F}(G, H)$:

Definition 4·10. Let G be a finite group and let $H \leq G$. We define the group $\mathfrak{F}(G, H)$ as

$$\mathfrak{F}(G, H) = (H \cap [G, G])/\Phi^G(H).$$

Returning to the situation of a tower of number fields $L/K/k$ with L/k Galois, $G = \mathrm{Gal}(L/k)$ and $H = \mathrm{Gal}(L/K)$ and letting ψ_1, φ_1^C and ψ_2^C denote the relevant maps in diagram (4·2) with $S = C$, the set of all cyclic subgroups of G, we have

$$\mathfrak{F}(G, H) = \mathrm{Ker}\psi_1/\varphi_1^C(\mathrm{Ker}\psi_2^C). \tag{4·5}$$

Downloaded from https://www.cambridge.org/core. The University of Reading, on 03 Mar 2022 at 12:42:21, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/S0305004121000268

We now prove the following strengthening of Theorem 1·1:

THEOREM 4·11. *There is a canonical isomorphism* $\mathfrak{F}_{nr}(L/K/k) = \mathfrak{F}(G, H)$ *under which the natural surjection* $\mathfrak{F}_{nr}(L/K/k) \twoheadrightarrow \mathfrak{F}(L/K/k)$ *coincides with the natural surjection* $\mathfrak{F}(G, H) \twoheadrightarrow \mathfrak{F}(L/K/k)$ *induced by Theorem* 4·5.

Proof. The norm map $N_{L/K}$ induces a commutative diagram of k-tori with exact lines:

$$\begin{array}{ccccccccc} 1 & \longrightarrow & R^1_{L/k}\mathbb{G}_m & \longrightarrow & R_{L/k}\mathbb{G}_m & \longrightarrow & \mathbb{G}_m & \longrightarrow & 1 \\ & & \downarrow{\scriptstyle N_{L/K}} & & \downarrow{\scriptstyle N_{L/K}} & & \downarrow{\scriptstyle =} & & \\ 1 & \longrightarrow & R^1_{K/k}\mathbb{G}_m & \longrightarrow & R_{K/k}\mathbb{G}_m & \longrightarrow & \mathbb{G}_m & \longrightarrow & 1. \end{array} \tag{4·6}$$

Taking character groups in (4·6) and then taking G-cohomology gives the following commutative diagram of abelian groups with exact lines:

$$\begin{array}{ccccccc} \mathrm{H}^2(G, \mathbb{Z}) & \xrightarrow{\theta_1} & \mathrm{H}^2(G, \mathbb{Z}[G/H]) & \xrightarrow{\theta_2} & \mathrm{H}^2(G, \widehat{T}) & \xrightarrow{\theta_3} & \mathrm{H}^3(G, \mathbb{Z}) \\ \downarrow{\scriptstyle =} & & \downarrow & & \downarrow{\scriptstyle f^*_{L/K}} & & \downarrow{\scriptstyle =} \\ \mathrm{H}^2(G, \mathbb{Z}) & \longrightarrow & \mathrm{H}^2(G, \mathbb{Z}[G]) = 0 & \longrightarrow & \mathrm{H}^2(G, \widehat{T}_0) & \longrightarrow & \mathrm{H}^3(G, \mathbb{Z}). \end{array} \tag{4·7}$$

By Theorem 2·2, the group $\mathfrak{F}_{nr}(L/K/k) = \mathrm{Coker}\left(f_{L/K} : \mathrm{H}^1(k, \mathrm{Pic}\,\overline{X_0})^\sim \to \mathrm{H}^1(k, \mathrm{Pic}\,\overline{X})^\sim\right)$ is dual to $\mathrm{Ker}\left(f^*_{L/K}|_{Ш^2_\omega(G,\widehat{T})} : Ш^2_\omega(G, \widehat{T}) \to Ш^2_\omega(G, \widehat{T}_0)\right)$. As the first line of diagram (4·7) is exact, we have

$$\mathrm{Ker}\left(f^*_{L/K}|_{Ш^2_\omega(G,\widehat{T})}\right) = \mathrm{Im}\,\theta_2 \cap Ш^2_\omega(G, \widehat{T}).$$

Furthermore, taking character groups in the second line of (4·6) and then taking both G-cohomology and $\langle g\rangle$-cohomology, we obtain the following commutative diagram with exact lines

$$\begin{array}{ccccc} \mathrm{H}^2(G, \mathbb{Z}) & \xrightarrow{\theta_1} & \mathrm{H}^2(G, \mathbb{Z}[G/H]) & \xrightarrow{\theta_2} & \mathrm{H}^2(G, \widehat{T}) \\ \downarrow & & \downarrow{\scriptstyle \theta_4} & & \downarrow \\ \prod_{g\in G} \mathrm{H}^2(\langle g\rangle, \mathbb{Z}) & \xrightarrow{\theta_5} & \prod_{g\in G} \mathrm{H}^2(\langle g\rangle, \mathbb{Z}[G/H]) & \longrightarrow & \prod_{g\in G} \mathrm{H}^2(\langle g\rangle, \widehat{T}) \end{array} \tag{4·8}$$

and a straightforward diagram chase shows that θ_2 induces an isomorphism

$$\theta_4^{-1}(\mathrm{Im}\,\theta_5)/\,\mathrm{Im}\,\theta_1 \cong \mathrm{Im}\,\theta_2 \cap Ш^2_\omega(G, \widehat{T}).$$

In [**45**, theorem 6·12] and pages leading to it, the authors show that the first square in diagram (4·8) is dual to diagram (4·2) with $S = C =$ {cyclic subgroups of G}, reproduced below:

Downloaded from https://www.cambridge.org/core. The University of Reading, on 03 Mar 2022 at 12:42:21, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/S0305004121000268

$$\begin{array}{ccc} H/[H,H] & \xrightarrow{\psi_1} & G/[G,G] \\ \uparrow{\scriptstyle \varphi_1^C} & & \uparrow \\ \bigoplus_{g\in G}\left(\bigoplus_{Hx_i\langle g\rangle\in H\backslash G/\langle g\rangle}\langle x_i g x_i^{-1}\rangle\cap H\right) & \xrightarrow{\psi_2^C} & \bigoplus_{g\in G}\langle g\rangle. \end{array} \tag{4·9}$$

In particular, $\theta_4^{-1}(\operatorname{Im}\theta_5)/\operatorname{Im}\theta_1$ is dual to $\operatorname{Ker}\psi_1/\varphi_1^C(\operatorname{Ker}\psi_2^C)$ and the existence of a canonical isomorphism $\mathfrak{F}_{nr}(L/K/k)=\mathfrak{F}(G,H)$ follows from (4·5). Theorem 4·5 can be proved in an analogous way by considering a version of diagram (4·8) with all decomposition groups in place of all cyclic subgroups of G and recalling from Theorem 2·3 that $Ш(T)$ is dual to $Ш^2(G,\widehat{T})$. Proposition 2·4 now yields the desired compatibility.

Proof of Corollary 1·2. This is a direct consequence of diagram (4·1) and Theorems 2·2 and 4·11.

COROLLARY 4·12. *If H is a Hall subgroup of G, then $\mathfrak{F}_{nr}(L/K/k)=\mathfrak{F}(L/K/k)=1$.*

Proof. The focal subgroup theorem [**31**] shows that for a Hall subgroup H of G, we have $\mathfrak{F}(G,H)=1$. The result therefore follows from Theorem 1·1 and the surjection $\mathfrak{F}_{nr}(L/K/k)\twoheadrightarrow\mathfrak{F}(L/K/k)$.

5. *Generalised representation groups*

Theorem 5·3 below gives an explicit description of the birational invariant $\mathrm{H}^1(k,\operatorname{Pic}\overline{X})$ in terms of generalised representation groups, which we now define:

Definition 5·1. Let G be a finite group. A finite group $\overline{G}$ is called a *generalised representation group* of G if there exists a central extension

$$1\to K\to\overline{G}\xrightarrow{\lambda}G\to 1, \tag{5·1}$$

such that the transgression map $\operatorname{Tr}_G:\hat{\mathrm{H}}^1(K,\mathbb{Q}/\mathbb{Z})\to\hat{\mathrm{H}}^2(G,\mathbb{Q}/\mathbb{Z})$ in the inflation-restriction exact sequence is surjective. We call K the base normal subgroup of $\overline{G}$.

Remark 5·2. Surjectivity of the transgression map Tr_G in Definition 5·1 is equivalent to injectivity of the dual map Tr_G^* in the exact sequence $\hat{\mathrm{H}}^{-3}(G,\mathbb{Z})\xrightarrow{\operatorname{Tr}_G^*}\hat{\mathrm{H}}^{-2}(K,\mathbb{Z})\to\hat{\mathrm{H}}^{-2}(\overline{G},\mathbb{Z})$, where the second map is induced by the inclusion $K\subset\overline{G}$. Hence, a central extension as in (5·1) gives a generalised representation group if and only if Tr_G^* gives an isomorphism $\hat{\mathrm{H}}^{-3}(G,\mathbb{Z})\cong K\cap[\overline{G},\overline{G}]$.

Let L/k be a Galois extension of number fields with Galois group G and let $\overline{G}$ be a generalised representation group of G with base normal subgroup K. Then the middle group in Voskresenskiĭ's exact sequence (2·1) for $R^1_{L/k}\mathbb{G}_m$ is $\hat{\mathrm{H}}^{-3}(G,\mathbb{Z})\cong K\cap[\overline{G},\overline{G}]=\mathfrak{F}(\overline{G},K)$. Theorem 5·3 below shows that this is a special case of a more general phenomenon.

Downloaded from https://www.cambridge.org/core. The University of Reading, on 03 Mar 2022 at 12:42:21, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/S0305004121000268

THEOREM 5·3 (Drakokhrust). *Let $L/K/k$ be a tower of number fields with L/k Galois. Let X/k be a smooth compactification of the norm one torus $R^1_{K/k}\mathbb{G}_m$. Let $G = \mathrm{Gal}(L/k)$ and $H = \mathrm{Gal}(L/K)$. Let $\overline{G}$ be a generalised representation group of G with projection map λ and for any subgroup $B \leq G$ let $\overline{B} = \lambda^{-1}(B)$. Then there is a canonical isomorphism*

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

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 (4·2) with respect to the groups $\overline{G}$, $\overline{H}$ and $S = \{S_v \mid v \in \Omega_k\}$. In this setting, Drakokhrust shows in [**16**, theorem 2] that

$$\mathrm{H}^1(k, \mathrm{Pic}\,\overline{X})^{\sim} = \mathrm{Ker}\psi_1/\varphi_1(\mathrm{Ker}\psi_2^{nr}),$$

where ψ_2^{nr} denotes the restriction of ψ_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

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

Indeed, we clearly have $\mathrm{Ker}\psi_1 = (\overline{H} \cap [\overline{G}, \overline{G}])/[\overline{H}, \overline{H}]$ and the equality $\varphi_1(\mathrm{Ker}\psi_2^{nr}) = \Phi^{\overline{G}}(\overline{H})/[\overline{H}, \overline{H}]$ follows from Lemma 4·6 and an argument similar to the proof of [**17**, theorem 2].

The following lemma will be used alongside Theorem 5·3 in the proof of Theorem 1·3, see Proposition 6·3 below.

LEMMA 5·4. *We have $\mathfrak{F}(\overline{G}, \overline{H}) \cong \mathfrak{F}(G, H)$ if and only if $\mathrm{Ker}\lambda \cap [\overline{G}, \overline{G}] \subset \Phi^{\overline{G}}(\overline{H})$, where the notation is as in Theorem 5·3.*

Proof. Easy exercise.

The next lemma enables us to employ generalised representation groups to calculate knot groups using the isomorphism (2·7) of Theorem 2·3 (via duality) or Theorem 4·2.

LEMMA 5·5. [**17**, lemma 4] *Let G be a finite group, H a subgroup of G and $\overline{G}$ a generalised representation group of G with projection map λ and base normal subgroup K. Then*

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

Downloaded from https://www.cambridge.org/core. The University of Reading, on 03 Mar 2022 at 12:42:21, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/S0305004121000268

It is well known that every finite group has a generalised representation group (see [37, theorem 2·1·4]). The following result of Schur, which gives presentations of generalised representation groups of A_n and S_n, will be used in Section 6 when investigating the Hasse norm principle for A_n and S_n extensions.

PROPOSITION 5·6. *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 generalised 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

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

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

Proof. See Schur's original paper [48] or [33, chapter 2] for a more modern exposition regarding generalised representation groups of S_n. The A_n case is dealt with in [41, section 3].

6. *Applications to A_n and S_n extensions*

In this section we apply the results of the preceding sections 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 $G = \mathrm{Gal}(L/k)$ is isomorphic to A_n or S_n with $n \geq 4$. We set $H = \mathrm{Gal}(L/K)$. For any subgroup G' of G, we denote by $F_{G/G'}$ a flasque module in a flasque resolution of the Chevalley module $J_{G/G'}$. Let X/k be a smooth compactification of the torus $T = R^1_{K/k}\mathbb{G}_m$. We use the isomorphism (2·3) in Theorem 2·2 to identify $\mathrm{H}^1(k, \mathrm{Pic}\,\overline{X})$ with $\mathrm{H}^1(G, F_{G/H})$.

6·1. *Results for general n*

First, we complete the proof of Theorem 1·3. For $G \cong A_n$ or S_n, we have $\mathrm{H}^3(G, \mathbb{Z}) \cong \mathbb{Z}/2$, unless $G \cong A_6$ or A_7 in which case $\mathrm{H}^3(G, \mathbb{Z}) \cong \mathbb{Z}/6$. Therefore, in our proof of Theorem 1·3, we can apply Corollary 1·2 to deal with the odd order torsion. It remains to analyse the 2-primary parts of $\text{Ш}(K/k)$ and $\mathrm{H}^1(G, F_{G/H})$. We start with the simpler case where $|H|$ is odd.

PROPOSITION 6·1. *If $|H|$ is odd, then*

(i) $\mathrm{H}^1(G, F_{G/H})_{(2)} = \mathbb{Z}/2$, *and*
(ii) $\text{Ш}(K/k)_{(2)} = \text{Ш}(L/k)_{(2)}$ *and* $\text{Ш}(K/k)_{(2)}$ *has size at most 2.*

Downloaded from https://www.cambridge.org/core. The University of Reading, on 03 Mar 2022 at 12:42:21, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/S0305004121000268

Proof.

(i) This follows from Corollary 3·5(i).

(ii) This is a consequence of Theorem 3·3 and isomorphism (2·7) of Theorem 2·3.

Proof of Theorem 1·3 for $|H|$ odd. We analyse the p-primary parts of the groups in Theorem 1·3 for each prime p. For p odd, apply Corollary 1·2 and use the fact that $\mathfrak{K}(L/k)^{\sim} \hookrightarrow \mathrm{H}^3(G, \mathbb{Z}) = \mathbb{Z}/2$ (Theorem 2·3). For $p = 2$, use Proposition 6·1. By Theorem 1·1, $\mathfrak{F}_{nr}(L/K/k) = \mathfrak{F}(G, H)$ is a subquotient of $H \cap [G, G]$, whereby $\mathfrak{F}_{nr}(L/K/k)_{(2)} = 1$, since $|H|$ is odd. As $\mathfrak{F}_{nr}(L/K/k)$ surjects onto $\mathfrak{F}(L/K/k)$, we also have $\mathfrak{F}(L/K/k)_{(2)} = 1$.

We now solve the case where $|H|$ is even. For this, we will use the generalised representation group $\overline{G}$ of G, the projection map λ and the base normal subgroup $K = \langle z \rangle$ presented in Proposition 5·6, so our next two results do not apply when $G \cong A_6$ or A_7.

LEMMA 6·2. *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:*

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

Proof. ***Case (1)*** *h* ***comprises a single transposition.*** Relabelling if necessary, we can assume that $h = (1\ \ 2)$. Take $A = \langle (1\ \ 2), (3\ \ 4) \rangle$ and note that $[\lambda^{-1}((1\ \ 2)), \lambda^{-1}((3\ \ 4))] = [\overline{t_1}, \overline{t_3}]$ in the notation of Proposition 5·6. Using the relations satisfied by the elements $\overline{t_i} \in \overline{G}$ given in Proposition 5·6, it is clear that this commutator is equal to z, as desired.

Case (2) *h* ***comprises more than one transposition.*** Relabelling 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 5·6, 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 $\overline{t_i}$ given in Proposition 5·6 shows that $[\lambda^{-1}(h), \lambda^{-1}(x)] = [\overline{t_1}.\overline{t_3}, \overline{t_2}.\overline{t_1}.\overline{t_2}.\overline{t_3}.\overline{t_2}.\overline{t_3}] = z$.

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

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

By the inductive hypothesis and the relations of Proposition 5·6, $[\lambda^{-1}(\tilde{h}), \lambda^{-1}(x)]^{\overline{t_{n+1}}} = z^{\overline{t_{n+1}}} = z$ and $[\overline{t_{n+1}}, \lambda^{-1}(x)] = [\overline{t_{n+1}}, \overline{t_2}.\overline{t_1}.\overline{t_2}.\overline{t_3}.\overline{t_2}.\overline{t_3}] = 1$, as desired.

The next proposition completes the proof of Theorem 1·3.

PROPOSITION 6·3. *Suppose that G is not isomorphic to A_6 or A_7 and that $|H|$ is even. Then:*

(i) $\mathrm{H}^1(G, F_{G/H})^{\sim} = \mathfrak{F}_{nr}(L/K/k)$;
(ii) $\mathfrak{K}(K/k) = \mathfrak{F}(L/K/k)$.

Downloaded from https://www.cambridge.org/core. The University of Reading, on 03 Mar 2022 at 12:42:21, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/S0305004121000268

Proof.

(i) By Theorems 1·1, 5·3 and isomorphism (2·3) of Theorem 2·2, if we can show that $\mathfrak{F}(\overline{G}, \overline{H}) \cong \mathfrak{F}(G, H)$ then it will follow that the natural surjection $\mathrm{H}^1(G, F_{G/H})^\sim \twoheadrightarrow \mathfrak{F}_{nr}(L/K/k)$ is an isomorphism. By Lemma 5·4, it suffices to check that $\mathrm{Ker}\lambda \subset \Phi^{\overline{G}}(\overline{H})$, i.e. that $z \in \Phi^{\overline{G}}(\overline{H})$. Let $A = \langle h, x\rangle$ be the copy of V_4 constructed in the proof of Lemma 6·2. Then $h \in H \cap xHx^{-1}$ and therefore $z = [\lambda^{-1}(h), \lambda^{-1}(x)] \in \Phi^{\overline{G}}(\overline{H})$, as desired.

(ii) By the isomorphism (2·3) of Theorem 2·2, the statement in (i) implies that the map $f_{L/K}$ in diagram (4·1) is trivial. As this diagram is commutative, it follows that $g_{L/K}$ is also trivial and thus $\text{Ш}(K/k) = \text{Ш}(T) = \mathrm{Coker}(g_{L/K}) = \mathfrak{F}(L/K/k)$.

Now that we have proved Theorem 1·3, 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 $\mathfrak{F}(L/K/k)$ and $\text{Ш}(L/k)$ can be computed using the GAP algorithms described in Remark 4·9 and at the end of Section 6·2 below. The calculations of the knot group and of $\mathrm{H}^1(k, \mathrm{Pic}\,\overline{X})$ in the remaining cases where $G \cong A_6, A_7$ are done in Section 6·3.

Remark 6·4. The method employed in this section to provide explicit and computable formulae for the knot group and the invariant $\mathrm{H}^1(k, \mathrm{Pic}\,\overline{X})$ in A_n and S_n extensions works for other families of extensions. For example, let G' be any finite group such that $\mathrm{H}^3(G', \mathbb{Z}) = \mathbb{Z}/2$. 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 6·2 and Propositions 6·1 and 6·3 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 $\mathfrak{F}(G, H)$ (and thus, by Theorems 1·1, 1·3 and isomorphism (2·3), of the invariant $\mathrm{H}^1(G, F_{G/H})$ as well).

PROPOSITION 6·5. *The group $\mathfrak{F}(S_n, H)$ is an elementary abelian 2-group. Moreover, every elementary abelian 2-group occurs as $\mathfrak{F}(S_n, H)$ 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 6·7 below.

PROPOSITION 6·6. *The group $\mathfrak{F}(A_n, H)$ is either 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 $\mathfrak{F}(A_n, H)$ is 2-torsion. Let $h \in H$ have even order. By [**27**], 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 $\mathfrak{F}(A_n, H)$ is 3-torsion. Let $h \in H$ be such that its image in $\mathfrak{F}(A_n, H)$ 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,

Downloaded from https://www.cambridge.org/core. The University of Reading, on 03 Mar 2022 at 12:42:21, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/S0305004121000268

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 $\Phi^{A_n}(H)$. Since h has odd order, we conclude that in all cases $h^3 \in \Phi^{A_n}(H)$, whence the claim.

Next, we show that $\mathfrak{F}(A_n, H)_{(3)}$ is cyclic. Suppose for contradiction that the images in $\mathfrak{F}(A_n, H)$ of $h_1, h_2 \in H$ generate a copy of $C_3 \times C_3$. Replacing h_1 and h_2 by suitable powers if necessary, we may assume that the lengths of the cycles making up h_1 and h_2 are powers of 3, say $3^{r_1} \leq 3^{r_2} \leq \cdots \leq 3^{r_k}$ 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 $h_1^2 \in \Phi^{A_n}(H)$, and similarly for h_2. The criterion [27] 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 $i \neq j$. Since $n = \sum_{i=1}^{k} 3^{r_i} = \sum_{i=1}^{l} 3^{s_i}$, the uniqueness of the representation of n in base 3 implies that $k = l$ and $r_i = s_i$ for every i. Thus the cycle structures of h_1 and h_2 are identical and hence h_1, h_2 and h_2^2 are conjugate in S_n. Therefore, at least two of these elements are A_n-conjugate, whereby at least one of $h_1^{-1}h_2, h_1^{-1}h_2^2, h_2$ is in $\Phi^{A_n}(H)$. This contradicts the assumption that the images of h_1 and h_2 generate a non-cyclic subgroup of $\mathfrak{F}(A_n, H)$. One can compute that $\mathfrak{F}(A_{12}, H) \cong C_3$ for $H = \langle (1, 2, 3)(4, 5, 6, 7, 8, 9, 10, 11, 12) \rangle$ using GAP, for example. The statement on the occurrence of every elementary abelian 2-group is shown in Proposition 6·7 below.

PROPOSITION 6·7. *For every $k \geq 0$, there exists n and a subgroup H of A_n such that*

$$\mathfrak{F}(A_n, H)_{(2)} \cong \mathfrak{F}(S_n, H)_{(2)} \cong C_2^k.$$

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:

(i) h_i is an even permutation of order 2;
(ii) h_i is disjoint to the previous generators $h_1, \ldots, h_{i-1}$;
(iv) 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 $\mathfrak{F}(S_n, H)$. This completes the proof.

As a consequence of the work done so far, we can now establish Theorem 1·4 and Corollary 1·6.

Proof of Theorem 1·4. For $G \ncong A_6$ or A_7 the results follow from Theorems 1·1 and 1·3 and Propositions 6·5 and 6·6. For the A_6 and A_7 cases, we describe how to compute $\mathrm{H}^1(k, \mathrm{Pic}\, \overline{X})$ in Section 6·3 – the results of these computations are in Tables V and VI of the Appendix and the C_3 and C_6 cases occur therein.

Proof of Corollary 1·6. Theorem 1·4 shows that $\mathrm{H}^1(k, \mathrm{Pic}\, \overline{X})_{(p)} = 0$ for a prime $p > 3$ and that $\mathrm{H}^1(k, \mathrm{Pic}\, \overline{X})_{(3)} = 0$ if $G \cong S_n$. Theorem 1·1 gives $\mathfrak{F}_{nr}(L/K/k) = \mathfrak{F}(G, H)$. By Theorem 1·4, $\mathrm{H}^1(k, \mathrm{Pic}\, \overline{X})^{\sim}_{(3)}$ is 3-torsion, so Theorem 1·3 gives $\mathrm{H}^1(k, \mathrm{Pic}\, \overline{X})^{\sim}_{(3)} =$

Downloaded from https://www.cambridge.org/core. The University of Reading, on 03 Mar 2022 at 12:42:21, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/S0305004121000268

$\mathfrak{F}(G, H)[3]$. Let $K_3 = L^{H_3}$ and let X_3 be a smooth compactification of $R^1_{K_3/k}\mathbb{G}_m$. Now Corollary 3·4 and Theorem 1·3 give $\mathrm{H}^1(k, \mathrm{Pic}\,\overline{X})^{\sim}_{(3)} \cong \mathrm{H}^1(k, \mathrm{Pic}\,\overline{X_3})^{\sim}_{(3)} = \mathfrak{F}(G, H_3)$. If $|H|$ is odd then $\mathfrak{F}(G, H)_{(2)}$ is trivial and hence $\mathrm{H}^1(k, \mathrm{Pic}\,\overline{X})^{\sim}_{(2)} = \mathbb{Z}/2$ by Theorem 1·3. The result for $\mathrm{H}^1(k, \mathrm{Pic}\,\overline{X})^{\sim}_{(2)}$ when $|H|$ is even is obtained in a similar way to the result for the 3-primary part.

The following corollary of Theorem 1·4 and Corollary 3·4 gives a useful shortcut when analysing the HNP and weak approximation for S_n extensions, enabling one to reduce to the case where H is a 2-group.

COROLLARY 6·8. *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 X_2 be a smooth compactification of $T_2 = R^1_{K_2/k}\mathbb{G}_m$. Then we obtain a commutative diagram with exact rows as follows, where the vertical isomorphisms are induced by the natural inclusion $T \hookrightarrow T_2$:*

$$\begin{array}{ccccccccc} 0 & \longrightarrow & A(T) & \longrightarrow & \mathrm{H}^1(k, \mathrm{Pic}\,\overline{X})^{\sim} & \longrightarrow & Ш(T) & \longrightarrow & 0 \\ & & \cong\downarrow & & \cong\downarrow & & \cong\downarrow & & \\ 0 & \longrightarrow & A(T_2) & \longrightarrow & \mathrm{H}^1(k, \mathrm{Pic}\,\overline{X_2})^{\sim} & \longrightarrow & Ш(T_2) & \longrightarrow & 0. \end{array}$$

Alternatively, the norm map $N_{K_2/K} : T_2 \twoheadrightarrow T$ can be used to obtain a similar commutative diagram with the direction of the vertical isomorphisms reversed.

Remark 6·9. Corollary 6·8 also holds in the case $G \cong A_n$ provided $n \neq 6, 7$ and $\mathfrak{F}(G, H)_{(3)} = 1$. In Proposition 6·11 we show that for most n we have $\mathfrak{F}(A_n, H)_{(3)} = 1$ for all subgroups H.

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

LEMMA 6·10. *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 ρ^j is A_n-conjugate to ρ 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 $x(a_i) = a_{1+(i-1)j}$ satisfies $x\rho x^{-1} = \rho^j$. Let C be the A_n-conjugacy class of ρ. Since the S_n-conjugacy class of ρ 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 analysing the fixed points of its powers. Observe that $x^t(a_i) = a_{1+(i-1)j^t}$ 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 $j^t - 1 \not\equiv 0 \pmod 3$ for odd t and thus $\gcd(3^l, j^t - 1) = 1$.

Downloaded from https://www.cambridge.org/core. The University of Reading, on 03 Mar 2022 at 12:42:21, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/S0305004121000268

(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 $j^{2m} + 1 \not\equiv 0 \pmod 3$.

Let $c_1 \cdot \ldots \cdot c_k$ 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 $3^l \equiv 1 \pmod 4$.

PROPOSITION 6·11. *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 $\mathfrak{F}(A_4, H)_{(3)} = 1$ for all $H \leq A_4$ so $n \geq 5$. Let h be an element of H such that its image in $\mathfrak{F}(A_n, H)$ generates $\mathfrak{F}(A_n, H)_{(3)}$. Replacing h by a suitable power if necessary, we may assume that the lengths of the cycles making up h are powers of 3, say $3^{r_1} \leq 3^{r_2} \leq \cdots \leq 3^{r_k}$ with $r_i \in \mathbb{Z}_{\geq 0}$. If h were A_n-conjugate to h^{-1} then we would obtain $h \in \Phi^{A_n}(H)$, a contradiction. Therefore, by criterion [27] we have $3^{r_i} \neq 3^{r_j}$ for $i \neq j$ and $\sum_{i=1}^{k} (3^{r_i} - 1)/2$ is odd, i.e. the number of odd r_i is odd.

Conversely, assume that $n \geq 5$ satisfies $n = \sum_{i=1}^{k} 3^{r_i}$ with $0 \leq r_1 < r_2 < \cdots < r_k$ and $|\{i \mid r_i \text{ is odd}\}|$ odd and let H be the cyclic group of order 3^{r_k} generated by h, where

$$h = \underbrace{(1 \ \cdots \ 3^{r_1})}_{c_1} \underbrace{(3^{r_1} + 1 \ \cdots \ 3^{r_1} + 3^{r_2})}_{c_2} \ldots \underbrace{\left(\sum_{i=1}^{k-1} 3^{r_i} + 1 \ \cdots \ n\right)}_{c_k}.$$

We will prove that $\mathfrak{F}(A_n, H)_{(3)} \cong C_3$. By Proposition 6·6, 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 $x_i c_i x_i^{-1} = c_i^t$. Then $x = x_1 \cdot \ldots \cdot x_k$ satisfies $xhx^{-1} = h^t$. Lemma 6·10 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 $C \sqcup xCx^{-1}$, where C denotes the A_n-conjugacy class of h.

Remark 6·12. 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:

(i) one can restrict the focus to A_n since $\mathfrak{F}(A_n, H)_{(2)} \cong \mathfrak{F}(S_n, H)_{(2)}$;
(ii) one can assume that H is a 2-group as $\mathfrak{F}(A_n, H)_{(2)} \cong \mathfrak{F}(A_n, H_2)$;
(iii) 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 $k \leq n/2$;

Downloaded from https://www.cambridge.org/core. The University of Reading, on 03 Mar 2022 at 12:42:21, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/S0305004121000268

(iv) if $\tilde{H}$ is a subgroup of H of index 2, then $\frac{1}{2}|\mathfrak{F}(A_n, \tilde{H})_{(2)}| \leq |\mathfrak{F}(A_n, H)_{(2)}| \leq 2|\mathfrak{F}(A_n, \tilde{H})_{(2)}|$;

(v) 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 $n \geq n_0$;

(vi) 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 $H \leq A_n$.

6·2. *Computational methods and results for small n*

In this section we prove Propositions 1·8, 1·9, Corollary 1·10 and Theorem 1·11. In order to prove Proposition 1·9, we must compute the groups $\mathrm{H}^1(k, \mathrm{Pic}\,\overline{X})$ 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 $\mathrm{Gal}(L/k) = G \cong S_4, S_5, A_4, A_5$. One method to achieve this is via the identification $\mathrm{H}^1(k, \mathrm{Pic}\,\overline{X}) = \mathrm{H}^1(G, F_{G/H})$ in (2·3), where $H = \mathrm{Gal}(L/K)$. In [**34**, section 5], Hoshi and Yamasaki developed several algorithms in the computer algebra system GAP [**24**] to construct flasque resolutions. Using this work, one can compute the invariant $\mathrm{H}^1(G, F_{G/H})$ for low-degree field extensions, see e.g. [**41**, section 4] for some examples. This computational method can also be used to prove Theorem 1·11:

Proof of Theorem 1·11. Note that an extension K/k of degree n is a (G, H)-extension (as defined on p. 6), 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 $\mathrm{H}^1(G, F_{G/H})$ using the aforementioned algorithms. If $\mathrm{H}^1(G, F_{G/H}) = 0$, then both the HNP for K/k and weak approximation for $R^1_{K/k}\mathbb{G}_m$ hold by Theorem 2·1 and the isomorphism (2·3). If $\mathrm{H}^1(G, F_{G/H}) \neq 0$, 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 6·13. We list a few observations about Theorem 1·11 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 $\mathrm{H}^1(G, F_{G/H})$ 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 $\alpha(G)$ for all transitive subgroups G of S_n with $\mathrm{H}^1(G, F_{G/H}) \neq 0$ 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 $\ll_{k,\epsilon} x^{\frac{1}{6}+\epsilon}$, when ordered by discriminant.

(iii) In the statement of Theorem 1·11 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 $\mathrm{H}^1(G, F_{G/H})$ is not trivial. Indeed, the assumption for all $G \leq S_n$ was used solely

Downloaded from https://www.cambridge.org/core. The University of Reading, on 03 Mar 2022 at 12:42:21, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/S0305004121000268

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 [19, pp· 723–724] for n even and the results of Datskovsky and Wright [15] 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 [14, 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 [40].

For most of our computational results, we did not employ the algorithms of Hoshi and Yamasaki and instead used the formula of Theorem 5·3 which expresses $\mathrm{H}^1(k, \mathrm{Pic}\,\overline{X})$ in terms of generalised representation groups of G and H. We implemented this formula, along with the simplification afforded by Corollary 3·4, as an algorithm in GAP (see [40]). For the groups G of Proposition 1·8, our calculations were further simplified thanks to Theorem 1·3. The outcome of our computations appears in Tables I – VI of the Appendix. Proposition 1·9 follows immediately.

It is noteworthy to compare the two computational methods described above. The approach based on Theorem 5·3 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 [40]) is usually preferable when H is large. In general, a combination of the two algorithms is the most convenient way to compute $\mathrm{H}^1(k, \mathrm{Pic}\,\overline{X})$ for all subgroups of a fixed group G.

We now move on to the proof of Proposition 1·8. We use Theorem 1·3 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 4·9. The computation of $\mathfrak{K}(L/k)$ follows from a simple application of isomorphism (2·7) of Theorem 2·3 together with Proposition 3·15 and Lemma 6·14 below. Note that if $G = A_4$, S_4, A_5 or S_5 then $\mathrm{H}^3(G, \mathbb{Z}) \cong \mathbb{Z}/2$.

LEMMA 6·14. *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*

$$\mathrm{Res}^G_A : \mathrm{H}^3(G, \mathbb{Z})_{(2)} \to \mathrm{H}^3(A, \mathbb{Z})$$

is an isomorphism.

Proof. Follows from the injectivity of $\mathrm{Res}^{D_4}_{V_4} : \mathrm{H}^3(D_4, \mathbb{Z}) \to \mathrm{H}^3(V_4, \mathbb{Z})$ and Proposition 3·15.

More generally, the knot group of any Galois extension L/k can be computed by combining the isomorphism (2·7) of Theorem 2·3 and Lemma 5·5. We used these two results to implement an algorithm (available at [40]) in GAP that, given the group $\mathrm{Gal}(L/k)$ and the

Downloaded from https://www.cambridge.org/core. The University of Reading, on 03 Mar 2022 at 12:42:21, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/S0305004121000268

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 1·10.

Proof of Corollary 1·10. The isomorphisms $\mathfrak{K}(K/k) \cong \mathfrak{K}(L/k)$ and $\mathfrak{K}(L/k) \cong \mathfrak{K}(L/F)$ follow from Proposition 1·8 and isomorphism (2·7) of Theorem 2·3. The statement about weak approximation follows from the isomorphism $\mathfrak{K}(K/k) \cong \mathfrak{K}(L/F)$, Voskresenskiĭ's exact sequence (2·1) and the fact that the middle group in this sequence is $\mathbb{Z}/2$ for both $R^1_{K/k}\mathbb{G}_m$ and $R^1_{L/F}\mathbb{G}_m$.

6·3. *The A_6 and A_7 cases*

In this section we give a complete characterisation of the Hasse norm principle and 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, we omit the precise construction of these semidirect products from the main text and refer the reader to Tables V and VI of the Appendix containing the generators of these subgroups. Our main result is the following:

PROPOSITION 6·15. *Suppose that G is isomorphic to A_6 or A_7. Then $\mathfrak{K}(K/k) \hookrightarrow C_6$ and*

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

$$\text{(ii)}\ \ \mathfrak{K}(K/k)_{(3)} = 1 \iff \begin{cases} C_3 \hookrightarrow H; \text{ or} \\ \exists\, v \text{ such that } C_3 \times C_3 \hookrightarrow D_v. \end{cases}$$

We start by settling the Galois case of this proposition.

PROPOSITION 6·16. *If L/k is Galois with Galois group A_6 or A_7, then $\mathfrak{K}(L/k) \hookrightarrow C_6$ and:*

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

Proof. This follows from isomorphism (2·7) of Theorem 2·3, Proposition 3·15 and Lemma 6·14.

We now solve the non-Galois case. As detailed in Section 6·2, we can compute the invariant $\mathrm{H}^1(k, \mathrm{Pic}\,\overline{X}) = \mathrm{H}^1(G, F_{G/H})$ for every possibility of $H = \mathrm{Gal}(L/K)$. The result of this computation is given in Tables V and VI of the Appendix and it proves the following:

PROPOSITION 6·17. *Suppose that G is isomorphic to A_6 or A_7. Then $\mathrm{H}^1(k, \mathrm{Pic}\,\overline{X}) \hookrightarrow \mathbb{Z}/6$ and:*

(i) $\mathrm{H}^1(k, \mathrm{Pic}\,\overline{X})_{(2)} = 0$ *if and only if $V_4 \hookrightarrow H$;*
(ii) $\mathrm{H}^1(k, \mathrm{Pic}\,\overline{X})_{(3)} = 0$ *if and only if $C_3 \hookrightarrow H$.*

Building upon this proposition, we establish several results concerning the knot group $\mathfrak{K}(K/k)$. In particular, we immediately see that the invariant $\mathrm{H}^1(G, F_{G/H})$ is trivial if H

Downloaded from https://www.cambridge.org/core. The University of Reading, on 03 Mar 2022 at 12:42:21, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/S0305004121000268

is isomorphic to A_4, $C_2 \times C_6$, D_6, $(C_6 \times C_2) \rtimes C_2$, S_4, $A_4 \times C_3$, A_5, $(A_4 \times C_3) \rtimes C_2$, S_5, PSL(3, 2) or A_6. Thus, by Theorem 2·1 and isomorphism (2·3), both groups $A(T)$ and $\mathfrak{K}(K/k)$ 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, i.e. the knot group.

PROPOSITION 6·18. *If* 6 *divides* $|H|$, *then* $\mathfrak{K}(K/k) = \mathfrak{F}(L/K/k)$.

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 3·15, Lemma 6·14 and duality, we find that the maps $\mathrm{Cor}^G_{G_1} : \hat{\mathrm{H}}^{-3}(G_1, \mathbb{Z}) \to \hat{\mathrm{H}}^{-3}(G, \mathbb{Z})_{(2)}$ and $\mathrm{Cor}^G_{G_2} : \hat{\mathrm{H}}^{-3}(G_2, \mathbb{Z}) \to \hat{\mathrm{H}}^{-3}(G, \mathbb{Z})_{(3)}$ are surjective. Hence

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

is surjective (recall that $\hat{\mathrm{H}}^{-3}(G, \mathbb{Z}) \cong \mathbb{Z}/6$) and therefore $\mathfrak{F}(L/K/k) = \mathfrak{K}(K/k)$ by Theorem 4·2.

As a consequence of this result, one can use the GAP function `lobs` described in Remark 4·9 to computationally solve the cases where $6 \mid |H|$ and $\mathrm{H}^1(G, F_{G/H}) \neq 0$. The remaining possibilities for H are dealt with in the two following results.

PROPOSITION 6·19.

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

Proof. We prove only (i) ((ii) and (iii) follow analogously). In this case $\mathrm{H}^1(G, F_{G/H}) = \mathbb{Z}/3$ (see Tables V and VI of the Appendix) and thus $\mathbb{Z}/3 \twoheadrightarrow \mathfrak{K}(K/k)$ by Theorem 2·1 and isomorphism (2·3). The result now follows by Theorem 3·3, noting that $d = [L : K] = 4$ or 8 is coprime to 3.

PROPOSITION 6·20.

(i) *If* $H \cong C_2$ *or* D_5, *then* $\mathfrak{K}(K/k) \cong \mathfrak{K}(L/k)$;
(ii) *If* $H \cong C_4$ *or* $C_5 \rtimes C_4$, *then*

$$\mathfrak{K}(K/k) \cong \mathfrak{K}(L/k)_{(3)} \times \mathfrak{K}(M/k) \cong \mathfrak{K}(L/k)_{(3)} \times \mathfrak{F}(L/M/k),$$

where M *is the fixed field of a copy of* $(C_3 \times C_3) \rtimes C_4$ *inside* G *containing* $H_2 \cong C_4$.

Proof. First, note that in all cases $\mathfrak{K}(K/k)_{(3)} \cong \mathfrak{K}(L/k)_{(3)}$, by Theorem 3·3. By Proposition 6·17 and Theorem 2·1, it only remains to compute $\mathfrak{K}(K/k)_{(2)}$. For case (i), let A be a copy of S_3 inside G such that $A \cap H = H_2 \cong C_2$ and let $F = L^A$ and $K_2 = L^{H_2}$. Now Theorem 3·3 shows that $\mathfrak{K}(K/k)_{(2)} \cong \mathfrak{K}(K_2/k)_{(2)} \cong \mathfrak{K}(F/k)_{(2)}$. Computing

Downloaded from https://www.cambridge.org/core. The University of Reading, on 03 Mar 2022 at 12:42:21, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/S0305004121000268

$\mathfrak{K}(F/k)_{(2)}$ using Proposition 6·18 and the GAP function `1obs` described in Remark 4·9 gives $\mathfrak{K}(F/k)_{(2)} \cong \mathfrak{K}(L/k)_{(2)}$, as required. For case (ii), again let $K_2 = L^{H_2}$. Then $\mathfrak{K}(K/k)_{(2)} \cong \mathfrak{K}(K_2/k)_{(2)} \cong \mathfrak{K}(M/k)_{(2)}$, by Theorem 3·3. Now Proposition 6·18 gives $\mathfrak{K}(M/k) \cong \mathfrak{F}(L/M/k)$. Furthermore, Theorem 2·1 and isomorphism (2·3) combined with the results for $(C_3 \times C_3) \rtimes C_4$ in Tables V and VI of the Appendix show that $\mathfrak{K}(M/k)$ is 2-torsion.

We have thus established the characterisation of the HNP for an A_6 or A_7 extension given in Proposition 6·15. Using Proposition 6·17, we can also give a full description of weak approximation. The local conditions controlling the validity of this principle are given in detail in the next theorem; they are a direct consequence of Propositions 6·15 and 6·17 and Voskresenskiĭ's exact sequence (2·1).

PROPOSITION 6·21. *Suppose that G is isomorphic to A_6 or A_7.*

(i) *If $V_4 \hookrightarrow H$ and $C_3 \hookrightarrow H$, then weak approximation holds for T.*
(ii) *If $H \cong 1, C_2, C_5, C_7$ or D_5, then weak approximation holds for T if and only if $V_4 \not\hookrightarrow D_v$ and $C_3 \times C_3 \not\hookrightarrow D_v$ for every place v of k.*
(iii) *If $H \cong C_4$ or $C_5 \rtimes C_4$, then weak approximation holds for T if and only if $D_4 \not\hookrightarrow D_v$ and $C_3 \times C_3 \not\hookrightarrow D_v$ for every place v of k.*
(iv) *In all other cases, weak approximation holds for T if and only if the HNP fails for K/k.*

7. *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 1·12. To prove it, we will use the notion of k-adequate extensions, as introduced by Schacher in [**47**].

Definition 7·1. 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 [**28**, theorem 3·1]) for Galois extensions, but disproved in general by Drakokhrust and Platonov (see [**17**, section 9, section 11]). Given a Galois extension L/k, a result of Schacher (see [**47**, 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 $D_{v_i} = \mathrm{Gal}(L_{v_i}/k_{v_i})$ contains a Sylow p-subgroup of $\mathrm{Gal}(L/k)$. This led Schacher to establish the following result:

THEOREM 7·2. [**47**, theorem 9·1] *For any finite group G there exists a number field k and a k-adequate Galois extension L/k with* $\mathrm{Gal}(L/k) \cong G$.

We can now prove Theorem 1·12, which generalises [**28**, corollary 3·3] to non-normal extensions.

Downloaded from https://www.cambridge.org/core. The University of Reading, on 03 Mar 2022 at 12:42:21, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/S0305004121000268

Proof of Theorem 1·12.

(i) Let L/k be a k-adequate Galois extension with Galois group G as given in Theorem 7·2. Let $K = L^H$ and $T = R^1_{K/k}\mathbb{G}_m$. Recall that, by Theorem 2·3,

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

Let p be a prime dividing $|G|$ and let D_v be a decomposition group containing a Sylow p-subgroup of G. Then Proposition 3·15 and the transitivity of restriction show that the map

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

is injective. It follows that $Ш(T) = 0$ and so $\text{Ř}(K/k)$ is trivial. The statement regarding weak approximation follows from Theorem 2·1 and isomorphism (2·3) of Theorem 2·2.

(ii) By [**17**, lemma 6], there is a Galois extension L/k of number fields with $\mathrm{Gal}(L/k) \cong G$ such that every decomposition group is cyclic. Let $K = L^H$, $T = R^1_{K/k}\mathbb{G}_m$ and let X be a smooth compactification of T. By [**52**, section 3, theorem 6 and corollary 2], we have $A(T) = 0$ and $Ш(T) \cong \mathrm{H}^1(k, \mathrm{Pic}\,\overline{X})^\sim$. The result now follows from isomorphism (2·3) of Theorem 2·2 and the fact that $\text{Ř}(K/k) = Ш(T)$.

As a consequence of the work done in the proof of Theorem 1·12, we can also obtain a version of Theorem 1·4 for the knot group and the defect of weak approximation. In what follows, let $L/K/k$ be a tower of number fields where L/k is Galois with Galois group $G \cong A_n$ or S_n and let $T = R^1_{K/k}\mathbb{G}_m$.

PROPOSITION 7·3.

(i) *For $G \cong S_n$ the groups $\text{Ř}(K/k)$ and $A(T)$ are elementary abelian 2-groups. Moreover, every possibility for $\text{Ř}(K/k)$ is realised: given an elementary abelian 2-group A, there exists $n \in \mathbb{N}$ and an extension of number fields K/k whose normal closure has Galois group S_n such that $\text{Ř}(K/k) \cong A$. Likewise, every possibility for $A(T)$ is realised.*

(ii) *For $G \cong A_n$ the groups $\text{Ř}(K/k)$ and $A(T)$ are elementary abelian 2-groups or isomorphic to C_3 or C_6. Again, every possibility for $\text{Ř}(K/k)$ is realised, and likewise for $A(T)$.*

Proof. This follows from Theorems 1·4, 1·12 and 2·1.

To conclude this section, we provide examples of number fields over $\mathbb{Q}$ illustrating that in every case addressed by Propositions 1·8 and 6·15, 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, [**49**, Lemmas 18 and 20] give useful practical conditions to test the local properties of Proposition 1·8. Some of these

Downloaded from https://www.cambridge.org/core. The University of Reading, on 03 Mar 2022 at 12:42:21, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/S0305004121000268

extensions were found using the LMFBD database [**39**] and all assertions below concerning Galois groups and ramification properties were verified using the computer algebra system MAGMA [**10**].

7·1. *Successes*

(i) 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 Proposition 1·8 we thus conclude that the HNP holds for $L/\mathbb{Q}$ as well as for any subextension $K/\mathbb{Q}$ contained in $L/\mathbb{Q}$.

(ii) For $G = A_5$, let $K = \mathbb{Q}(\alpha)$, where α 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 $\mathrm{Gal}(L/\mathbb{Q}) \cong A_5$ and there exists a prime $\mathfrak{p}$ 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, Proposition 1·8 shows that the HNP holds for any subextension of $L/\mathbb{Q}$.

(iii) For $G = S_5$, take $K = \mathbb{Q}(\alpha)$, where α 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 $\mathrm{Gal}(L/\mathbb{Q}) \cong S_5$ and that there is a prime $\mathfrak{p}$ 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 Proposition 1·8.

(iv) For $G = A_6$, let $K = \mathbb{Q}(\alpha)$, where α 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 $\mathrm{Gal}(L/\mathbb{Q}) \cong A_6$ and there are primes $\mathfrak{p}$ and $\mathfrak{q}$ of K above 2 and 3, respectively, such that $[K_\mathfrak{p} : \mathbb{Q}_2] = 8$ and $[K_\mathfrak{q} : \mathbb{Q}_3] = 9$. 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 $C_3 \times C_3 \hookrightarrow D_3$. Proposition 6·15 then shows that the HNP holds for any subextension of $L/\mathbb{Q}$.

(v) For $G = A_7$, let $L/\mathbb{Q}$ be the splitting field of the polynomial $x^7 - 3x^6 - 3x^5 - x^4 + 12x^3 + 24x^2 + 16x + 24$. Then $\mathrm{Gal}(L/\mathbb{Q}) \cong A_7$ 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 L. Note that if the decomposition $O_M/pO_M \cong \bigoplus_i \mathbb{F}_{p^{f_i}}[t_i]/(t_i^{e_i})$ holds for some $e_i, f_i \in \mathbb{Z}_{\geq 0}$, then $\mathrm{lcm}(e_i) \mid e$, $\mathrm{lcm}(f_i) \mid f$ and hence $\mathrm{lcm}(e_i) \cdot \mathrm{lcm}(f_i) \mid ef = |D_p|$. Factoring the prime $p = 2$ in O_M gives $\mathrm{lcm}(e_i) = 12$ and $\mathrm{lcm}(f_i) = 2$, so $24 \mid |D_2|$. 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 $18 \mid |D_3|$ and consequently D_3 contains a copy of $C_3 \times C_3$. By Proposition 6·15, it follows that the HNP holds for any subextension of $L/\mathbb{Q}$.

Downloaded from https://www.cambridge.org/core. The University of Reading, on 03 Mar 2022 at 12:42:21, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/S0305004121000268

Remark 7·4. An alternative approach to find examples of number fields satisfying the HNP and with Galois groups as in Propositions 1·8 and 6·15 is to use $\mathbb{Q}$-adequate extensions. Indeed, examining the local conditions of Propositions 1·8 and 6·15, 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 $\mathrm{Gal}(L/\mathbb{Q}) \cong G$. We give some references for the interested reader. For $G = A_4, A_5$ see [**25**], [**26**], 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 [**25**, corollary 2·2]). For $G = A_5$, [**26**, theorem 1] constructs k-adequate Galois extensions with Galois group A_5 for any number field k such that $\sqrt{-1} \notin k$. For $G = S_4, S_5$ see [**47**, theorem 7·1]. The cases $G = A_6, A_7$ are treated in [**20**]. We chose not to pursue this approach because the polynomials defining the field extensions were rather cumbersome, particularly for A_6 and A_7.

7·2. *Failures*

(i) We start with the cases where G is A_4 or S_4. Let $L/\mathbb{Q}$ 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 $L/\mathbb{Q}$ is a Galois extension with Galois group G such that every decomposition group is cyclic. Therefore, Proposition 1·8 shows that the HNP fails for any subextension of L/k falling under case (i) or (ii) of Proposition 1·8, i.e. an extension where the HNP can theoretically fail.

(ii) We now find examples for the A_5 and S_5 cases using work of Uchida [**51**]. Examples for the A_6 and A_7 cases can be obtained in a manner analogous to the construction for A_5. Let $F/\mathbb{Q}$ be the splitting field of $f(x) = x^5 - x + 1$ and set $D = \mathrm{Disc}(f) = 19 \cdot 151$. By [**51**, proofs of corollary 1 and theorem 2], $F/\mathbb{Q}(\sqrt{D})$ is an unramified Galois extension with Galois group A_5, while $F(\sqrt{2})/\mathbb{Q}(\sqrt{2D})$ is an unramified Galois extension with Galois group S_5. If $G = A_5$ then set $L = F$, $k = \mathbb{Q}(\sqrt{D})$. If $G = S_5$ then set $L = F(\sqrt{2})$, $k = \mathbb{Q}(\sqrt{2D})$. Let K/k be a subextension of L/k falling under case (i) or (ii) of Proposition 1·8. Since L/k is unramified, all its decomposition groups are cyclic, whereby the HNP fails for K/k by the criterion of Proposition 1·8.

A similar construction allows us to provide examples of unramified Galois A_6 and A_7 extensions. By Proposition 6·15, these extensions have knot groups isomorphic to C_6 and therefore the HNP fails for them. 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 [**17**, 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 Proposition 6·15 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.

Downloaded from https://www.cambridge.org/core. The University of Reading, on 03 Mar 2022 at 12:42:21, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/S0305004121000268

Appendix

We present the results of the computer calculations outlined in Section 6·2. In the following tables, we distinguish non-conjugate but isomorphic groups with a letter in front of the isomorphism class.

Table I.

$G = A_4$		
$[K : k]$	H	$\mathrm{H}^1(G, F_{G/H})$
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 II.

$G = S_4$		
$[K : k]$	H	$\mathrm{H}^1(G, F_{G/H})$
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 III.

$G = A_5$		
$[K : k]$	H	$\mathrm{H}^1(G, F_{G/H})$
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

Downloaded from https://www.cambridge.org/core. The University of Reading, on 03 Mar 2022 at 12:42:21, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/S0305004121000268

Table IV.

$G = S_5$		
$[K:k]$	H	$\mathrm{H}^1(G, F_{G/H})$
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	$C_5 \rtimes C_4 = \langle (1,2,3,4,5), (2,3,5,4) \rangle$	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

Table V.

$G = A_6$		
$[K:k]$	H	$\mathrm{H}^1(G, F_{G/H})$
360	1	$\mathbb{Z}/6$
180	$C_2 = \langle (1,2)(3,4) \rangle$	$\mathbb{Z}/6$
120	$C_3 = \langle (1,2,3) \rangle$	$\mathbb{Z}/2$
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	$(C_3 \times C_3) \rtimes C_2 = \langle (1,2,3), (4,5,6), (1,2)(4,5) \rangle$	$\mathbb{Z}/2$
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	$(C_3 \times C_3) \rtimes C_4 = \langle (1,2,3), (4,5,6), (1,4)(2,5,3,6) \rangle$	$\mathbb{Z}/2$
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

Downloaded from https://www.cambridge.org/core. The University of Reading, on 03 Mar 2022 at 12:42:21, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/S0305004121000268

Table VI.

$G = A_7$		
$[K : k]$	H	$\mathrm{H}^1(G, F_{G/H})$
2520	1	$\mathbb{Z}/6$
1260	$C_2 = \langle (1, 2)(3, 4) \rangle$	$\mathbb{Z}/6$
840	$C_3a = \langle (1, 2, 3) \rangle$	$\mathbb{Z}/2$
840	$C_3b = \langle (1, 2, 3)(4, 5, 6) \rangle$	$\mathbb{Z}/2$
630	$C_4 = \langle (1, 2, 3, 4)(5, 6) \rangle$	$\mathbb{Z}/6$
630	$V_4a = \langle (1, 2)(3, 4), (1, 3)(2, 4) \rangle$	$\mathbb{Z}/3$
630	$V_4b = \langle (1, 2)(5, 6), (1, 2)(3, 4) \rangle$	$\mathbb{Z}/3$
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	$S_3a = \langle (1, 2, 3)(4, 5, 6), (1, 2)(4, 5) \rangle$	$\mathbb{Z}/2$
420	$S_3b = \langle (1, 2, 3), (1, 2)(4, 5) \rangle$	$\mathbb{Z}/2$
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	$A_4a = \langle (1, 2)(3, 4), (1, 2, 3) \rangle$	0
210	$A_4b = \langle (1, 2, 3)(4, 5, 6), (1, 4)(2, 5) \rangle$	0
210	$A_4c = \langle (1, 5, 3)(4, 7, 6), (2, 6)(4, 7) \rangle$	0
210	$A_4d = \langle (1, 2, 5)(4, 6, 7), (3, 4)(6, 7) \rangle$	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	$C_3 \rtimes C_4 = \langle (2, 3, 6), (1, 4, 7, 5)(3, 6) \rangle$	$\mathbb{Z}/2$
140	$(C_3 \times C_3) \rtimes C_2 = \langle (1, 2, 3), (4, 5, 6), (1, 2)(4, 5) \rangle$	$\mathbb{Z}/2$
126	$C_5 \rtimes C_4 = \langle (1, 2)(4, 5, 7, 6), (3, 6, 7, 4, 5) \rangle$	$\mathbb{Z}/6$
120	$C_7 \rtimes C_3 = \langle (1, 7, 4, 2, 6, 5, 3), (2, 3, 5)(4, 6, 7) \rangle$	$\mathbb{Z}/2$
105	$(C_6 \times C_2) \rtimes C_2 = \langle (1, 2)(3, 5)(4, 6, 7), (1, 3)(2, 5), (1, 2)(6, 7) \rangle$	0
105	$S_4a = \langle (1, 2, 3, 4)(5, 6), (1, 2)(5, 6) \rangle$	0
105	$S_4b = \langle (1, 3, 5)(2, 4, 6), (1, 6)(2, 5) \rangle$	0
105	$S_4c = \langle (1, 2, 3)(5, 6, 7), (2, 3)(4, 5, 6, 7) \rangle$	0
105	$S_4d = \langle (1, 3, 2)(5, 6, 7), (2, 3)(4, 5, 6, 7) \rangle$	0
70	$A_4 \times C_3 = \langle (1, 3, 5)(4, 6, 7), (1, 2, 3) \rangle$	0
70	$(C_3 \times C_3) \rtimes C_4 = \langle (1, 2, 3), (4, 5, 6), (1, 4)(2, 5, 3, 6) \rangle$	$\mathbb{Z}/2$
42	$A_5a = \langle (1, 2, 3, 4, 5), (1, 2, 3) \rangle$	0
42	$A_5b = \langle (1, 2, 3, 4, 5), (1, 4)(5, 6) \rangle$	0
35	$(A_4 \times C_3) \rtimes C_2 = \langle (2, 3)(5, 7), (1, 2)(4, 5, 6, 7), (2, 3)(5, 6) \rangle$	0
21	$S_5 = \langle (1, 2)(3, 7), (2, 6, 5, 4)(3, 7) \rangle$	0
15	$\mathrm{PSL}(3, 2)a = \langle (1, 4)(2, 3), (2, 4, 6)(3, 5, 7) \rangle$	0
15	$\mathrm{PSL}(3, 2)b = \langle (1, 3)(2, 7), (1, 5, 7)(3, 4, 6) \rangle$	0
7	$A_6 = \langle (1, 2, 3, 4, 5), (4, 5, 6) \rangle$	0

Downloaded from https://www.cambridge.org/core. The University of Reading, on 03 Mar 2022 at 12:42:21, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/S0305004121000268

Acknowledgements. We are grateful to Manjul Bhargava for conversations that motivated our work on this topic, to Jean-Louis Colliot–Thélène for useful discussions which led to a cleaner proof of Corollary 3·4 and to the anonymous referees for valuable suggestions and for pointing out the geometric interpretation of the first obstruction to the HNP (Theorem 1·1) which improved several results and proofs in the paper. 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 and UKRI Future Leaders Fellowship MR/T041609/1.

REFERENCES

[1] S. A. ALTUG, A. SHANKAR, I. VARMA and 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 Diedergruppenerweiterungen. *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 and J. TSIMERMAN. On the Davenport–Heilbronn theorems and second order terms. *Invent. Math.* **193**(2) (2013), 439–499.
[7] M. BHARGAVA, A. SHANKAR and X. WANG. Geometry-of-numbers methods over global fields I: Prehomogeneous vector spaces. Preprint. arXiv:1704.01729.
[8] M. BHARGAVA and 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] M. BOROVOI and B. È. KUNYAVSKIĬ. Formulas for the Unramified Brauer Group of a Principal Homogeneous Space of a Linear Algebraic Group. *J. Algebra* **225** (2000), 804âĂŞ821.
[10] W. BOSMA, J. CANNON and C. PLAYOUST. The Magma algebra system. I. The user language. *J. Symbolic Comput.* **24** (1997), 235–265.
[11] K. S. BROWN. *Cohomology of groups.* Graduate Texts in Mathematics **87** (Springer–Verlag), 1982.
[12] T.D. BROWNING. How often does the Hasse principle hold? *Algebraic Geometry: Salt Lake City* 2015, *Proc. Symposia Pure Math.* A.M.S. 97.2 (2018), 89–102.
[13] J.-L. COLLIOT–THÉLÈNE and J.–J. SANSUC. La R-équivalence sur les tores. *Ann. Sci. Ecole. Norm. Sup.* **10** (1977), 175–229.
[14] J.-L. COLLIOT–THÉLÈNE and J.–J. SANSUC. Principal homogeneous spaces under flasque tori: Applications. *J. Algebra* **106** (1987), 148–205.
[15] B. DATSKOVSKY and D. J. WRIGHT. Density of discriminants of cubic extensions. *J. reine angew. Math.* **386** (1988), 116–138.
[16] Y. A. DRAKOKHRUST. On the complete obstruction to the Hasse principle. *Amer. Math. Soc. Transl.*(2) **143** (1989), 29–34.
[17] Y. A.DRAKOKHRUST and V. P. PLATONOV. The Hasse norm principle for algebraic number fields. *Math. USSR-Izv.* **29** (1987), 299–322.
[18] J. S. ELLENBERG, L. B. PIERCE and M. M. WOOD. On ℓ-torsion in class groups of number fields. *Algebra and Number Theory* 11-8 (2017), 1739–1778.
[19] J. S. ELLENBERG and A. VENKATESH. The number of extensions of a number field with fixed degree and bounded discriminant. *Ann. of Math.* **163**(2) (2006), 723–741.
[20] B. FEIN and M. SCHACHER. $\mathbb{Q}$-Admissibility Questions for Alternating Groups. *J. Algebra* **142** (1991), 360–382.
[21] C. FREI, D. LOUGHRAN and R. NEWTON. The Hasse norm principle for abelian extensions. *Amer. J. Math* **140**(6) (2018), 1639–1685.
[22] C. FREI, D. LOUGHRAN and R. NEWTON. with an appendix by Y. Harpaz, O. Wittenberg, Number fields with prescribed norms. Preprint. arXiv:1810.06024.
[23] C. FREI and M. WIDMER. Average bounds for the ℓ-torsion in class groups of cyclic extensions. *Res. Number Theory* **4**(34) (2018).

Downloaded from https://www.cambridge.org/core. The University of Reading, on 03 Mar 2022 at 12:42:21, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/S0305004121000268

[24] GAP Group. GAP – Groups, Algorithms, and Programming, Version 4.8.10 (2018). Available at https://www.gap-system.org.
[25] B. GORDON and M. SCHACHER. Quartic coverings of a cubic. In *Number Theory and Algebra*, 97–101 (Academic Press, New York, 1977).
[26] B. GORDON and M. SCHACHER. The admissibility of A_5. *J. Number Theory* **11** (1979), 489–504.
[27] 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.
[28] S. GURAK. On the Hasse norm principle. *J. Reine Angew. Math.* **299/300** (1978), 16–27.
[29] S. GURAK. The Hasse norm principle in non-abelian extensions. *J. Reine Angew. Math.* **0303/0304** (1978), 314–318.
[30] H. HASSE. Beweis eines Satzes und Wiederlegung einer Vermutung über das allgemeine Normenrestsymbol. *Nachr. Ges. Wiss. Göttingen Math.-Phys. Kl.* (1931), 64–69.
[31] D. HIGMAN. Focal series in finite groups. *Canad. J. Math.* **5** (1953), 477–497.
[32] W. HO, A. SHANKAR and I. VARMA. Odd degree number fields with odd class number. *Duke Math. J.* **167** (2018), No. 5, 995–1047.
[33] P. N. HOFFMAN and J. F. HUMPHREYS. *Projective representations of the symmetric groups*. Oxford Math. Monogr. (Clarendon Press, Oxford, 1992).
[34] A. HOSHI and A. YAMASAKI. Rationality problem for algebraic tori. *Mem. Amer. Math. Soc.* **248** (2017), No. 1176.
[35] A. HOSHI, K. KANAI and A. YAMASAKI. Norm one tori and Hasse norm principle. Preprint. arXiv:1910.01469.
[36] A. HOSHI, K. KANAI and A. YAMASAKI. Norm one tori and Hasse norm principle II: degree 12 case. Preprint. arXiv:2003.08253.
[37] G. KARPILOVSKY. *The Schur Multiplier* (Clarendon Press, Oxford, 1987).
[38] Y. LIANG. Non-invariance of weak approximation properties under extension of the ground field. Preprint. arXiv:1805.08851
[39] The LMFDB Collaboration. *The L-functions and Modular Forms Database*. http://www.lmfdb.org, 2013, [Online; accessed July 2019].
[40] A. MACEDO. GAP code (2019). Available at https://sites.google.com/view/andre-macedo/code.
[41] A. MACEDO. The Hasse norm principle for A_n-extensions. *J. Number Theory* **211** (2020), 500–512.
[42] A. MACEDO. A note on the density of D_4-fields failing the Hasse norm principle. In preparation.
[43] G. MALLE. On the distribution of Galois groups. *J. Number Theory* **92**(2) (2002), 315–329.
[44] L. B. PIERCE, C. L. TURNAGE-BUTTERBAUGH and M. M. WOOD. An effective Chebotarev density theorem for families of number fields, with an application to ℓ-torsion in class groups. *Invent. Math.* **219** (2020), 701–778.
[45] V. PLATONOV and A. RAPINCHUK. *Algebraic groups and number theory*. Pure and Applied Mathematics 139 (Academic Press, Inc., Boston, MA, 1994).
[46] N. ROME. The Hasse norm principle for biquadratic extensions. *J. Théor. Nombres Bordeaux* **30** No. 3 (2018), 947–964.
[47] M. SCHACHER. Subfields of division rings I. *J. Algebra* **9** (1968) 451–477.
[48] J. SCHUR. Über die Darstellung der symmetrischen und der alternierenden Gruppe durch gebrochene lineare Substitutionen. *J. Reine Angew. Math.* **139** (1911), 155–250.
[49] L. STERN. Equality of norm groups of subextensions of S_n ($n \leq 5$) extensions of algebraic number fields. *J. Number Theory* **102**(2) (2003), 257–277.
[50] J. T. TATE. Global class field theory. pp. 162–203 in: J.W.S. Cassels, A. Fröhlich (eds), *Algebraic number theory*, Second Edition, London Math. Soc. (2010).
[51] K. UCHIDA. Unramified extensions of quadratic number fields I. *Tohoku Math. J.* **22** (1970), 220–224.
[52] V. E. VOSKRESENSKIĬ. Birational properties of linear algebraic groups. *Izv. Akad. Nauk SSSR Ser. Mat.* **34** (1970) 3âĂŞ19. English translation: *Math. USSR-Izv.* Vol. **4** (1970), 1–17.
[53] V. E. VOSKRESENSKIĬ. Maximal tori without affect in semisimple algebraic groups, *Mat. Zametki* **44** (1988) 309–318; English transl. in *Math. Notes* **44** (1989) 651–655.
[54] V. E. VOSKRESENSKIĬ. B. È. Kunyavskiĭ. Maximal tori in semisimple algebraic groups. Manuscript deposited at VINITI 15.03.84, No. 1269-84, 28pp. (in Russian).
[55] M. M. WOOD. Nonabelian Cohen–Lenstra moments (including an appendix with P. M. Wood). *Duke Math. J.* **168** no. 3 (2019), 377–427.

Downloaded from https://www.cambridge.org/core. The University of Reading, on 03 Mar 2022 at 12:42:21, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/S0305004121000268