Citation for published version:
Frei, C, Loughran, D & Newton, R 2022, 'Number fields with prescribed norms', *Commentarii Mathematici Helvetici*, vol. 97, no. 1, pp. 133-181. https://doi.org/10.4171/CMH/528

DOI:
10.4171/CMH/528

Publication date:
2022

Document Version
Peer reviewed version

Link to publication

Copyright © 2022 EMS Publishing House. The final publication is available at Commentarii Mathematici Helvetici via https://doi.org/10.4171/CMH/528

University of Bath

Alternative formats
If you require this document in an alternative format, please contact:
openaccess@bath.ac.uk

General rights
Copyright and moral rights for the publications made accessible in the public portal are retained by the authors and/or other copyright owners and it is a condition of accessing publications that users recognise and abide by the legal requirements associated with these rights.

Take down policy
If you believe that this document breaches copyright please contact us providing details, and we will remove access to the work immediately and investigate your claim.

Download date: 08. Jun. 2022

NUMBER FIELDS WITH PRESCRIBED NORMS

CHRISTOPHER FREI, DANIEL LOUGHRAN, AND RACHEL NEWTON
WITH AN APPENDIX BY YONATAN HARPAZ AND OLIVIER WITTENBERG

Abstract. We study the distribution of extensions of a number field k with fixed abelian Galois group G, from which a given finite set of elements of k are norms. In particular, we show the existence of such extensions. Along the way, we show that the Hasse norm principle holds for 100% of G-extensions of k, when ordered by conductor. The appendix contains an alternative purely geometric proof of our existence result.

Contents

1. Introduction 1
2. Frobenian functions 8
3. Counting with local conditions 10
4. Proof of results 25
Appendix A. An algebro-geometric point of view on Theorem 1.1 30
References 38

1. Introduction

Let k be a number field. In this paper we are interested in the images of the norm maps $N_{K/k} : K^* \to k^*$ for finite field extensions K/k. Specifically, given an element $\alpha \in k^*$ and a finite group G, does there exist an extension K/k with Galois group G such that α is a norm from K? We are able to answer this question positively if one restricts to abelian extensions of k. Furthermore, in the abelian setting, we prove the existence of such an extension from which a given finite set of elements of k^* are norms.

Theorem 1.1. *Let k be a number field, G a finite abelian group and $\mathcal{A} \subset k^*$ a finitely generated subgroup. Then there exists an abelian extension K/k with Galois group G such that every element of $\mathcal{A}$ is a norm from K.*

As an application, we obtain the following corollary.

Corollary 1.2. *Let k be a number field, G a finite abelian group and S a finite set of places of k. Then there exists an abelian extension K/k with Galois group G such that every S-unit of k is a norm from K.*

We prove Theorem 1.1 by *counting* the collection of abelian extensions under consideration; we obtain an asymptotic formula for the number of such extensions

2010 *Mathematics Subject Classification.* 11R37 (primary), 11R45, 43A70, 14G05. (secondary).

of bounded conductor, and show explicitly that the leading constant in this formula is non-zero. In particular, we prove the existence of infinitely many extensions with the desired properties. The strategy of proving existence via counting is widely used in analytic number theory, for example in the context of the Hardy–Littlewood circle method. Our proof of Theorem 1.1 seems to be the first case where it is implemented for number fields. Our methods even allow us to prove existence of such an extension K/k which satisfies any finite collection of admissible local conditions (Corollary 4.12).

Before we can explain these more general results, we must introduce some notation. Fix a choice of algebraic closure $\overline{k}$ of k and let G be a finite abelian group. By a *G-extension* of k, we mean a surjective continuous homomorphism $\varphi : \mathrm{Gal}(\overline{k}/k) \to G$. This corresponds to choosing an extension $k \subset K \subset \overline{k}$ together with an isomorphism $\mathrm{Gal}(K/k) \cong G$. Keeping track of the isomorphism with G simplifies the set-up and the counting. It has no qualitative effect on the results; forgetting the choice of isomorphism merely scales all the counting results by $|\operatorname{Aut}(G)|$. We write G-$\mathrm{ext}(k)$ for the set of all G-extensions of k. Given $\varphi \in G$-$\mathrm{ext}(k)$, we write K_φ for the corresponding number field, and $\Phi(\varphi)$ for the norm of the conductor of K_φ (viewed as an ideal of k). Moreover, we write $\mathbf{A}^*_{K_\varphi}$ for the ideles of the number field K_φ. We are interested in the counting functions

$$\begin{aligned} N(k,G,B) &= \#\{\varphi \in G\text{-}\mathrm{ext}(k) : \Phi(\varphi) \le B\}, \\ N_{\mathrm{loc}}(k,G,\mathcal{A},B) &= \#\{\varphi \in G\text{-}\mathrm{ext}(k) : \Phi(\varphi) \le B, \mathcal{A} \subset \mathrm{N}_{K_\varphi/k}\, \mathbf{A}^*_{K_\varphi}\}, \\ N_{\mathrm{glob}}(k,G,\mathcal{A},B) &= \#\{\varphi \in G\text{-}\mathrm{ext}(k) : \Phi(\varphi) \le B, \mathcal{A} \subset \mathrm{N}_{K_\varphi/k}\, K^*_\varphi\}. \end{aligned} \tag{1.1}$$

The first counts all G-extensions φ of k of bounded conductor, the second counts only those for which every element of $\mathcal{A}$ is everywhere locally a norm, the third only those for which every element of $\mathcal{A}$ is a global norm.

An asymptotic formula for $N(k,G,B)$ was first obtained by Wood in [51], building on numerous special cases. In this paper we obtain asymptotic formulae for the other counting functions. Our formulae are stated in terms of the invariant $\varpi(k,G,\mathcal{A})$ which we now define.

Definition 1.3. Let k be a number field, G a finite abelian group, and $\mathcal{A} \subset k^*$ a finitely generated subgroup. For $d \in \mathbb{Z}_{\ge 1}$, let $k_d = k(\mu_d, \sqrt[d]{\mathcal{A}})$. We define

$$\varpi(k,G,\mathcal{A}) = \sum_{g \in G \smallsetminus \{\mathrm{id}_G\}} \frac{1}{[k_{|g|} : k]},$$

where $|g|$ denotes the order of g in G and $\mathrm{id}_G \in G$ is the identity element.

Theorem 1.4. *Let k be a number field, G a non-trivial finite abelian group, and $\mathcal{A} \subset k^*$ a finitely generated subgroup. Then*

$$N_{\mathrm{glob}}(k,G,\mathcal{A},B) \sim c_{k,G,\mathcal{A}} B (\log B)^{\varpi(k,G,\mathcal{A})-1}$$

as $B \to \infty$, for some $c_{k,G,\mathcal{A}} > 0$.

This theorem gives an asymptotic formula for the number of G-extensions from which every element of $\mathcal{A}$ is a global norm. It is natural to ask how the number of such extensions compares with the total number $N(k,G,B)$ of G-extensions of k of conductor bounded by B. We observe that $N(k,G,B) = N_{\mathrm{glob}}(k,G,\{1\},B)$ and note that in this case the formula of Theorem 1.4 agrees with [51, Thm. 3.1].

Example 1.5. In the special case where $G = \mathbb{Z}/2\mathbb{Z}$ and $\alpha \in k^* \smallsetminus k^{*2}$, we compute $\varpi(k, \mathbb{Z}/2\mathbb{Z}, \langle\alpha\rangle) = 1/2$ and thus $N_{\mathrm{glob}}(k, \mathbb{Z}/2\mathbb{Z}, \langle\alpha\rangle, B) \sim c_{k,\mathbb{Z}/2\mathbb{Z},\langle\alpha\rangle} B(\log B)^{-1/2}$. When compared to the asymptotic $N(k, \mathbb{Z}/2\mathbb{Z}, B) \sim c_{k,\mathbb{Z}/2\mathbb{Z}} B$, this shows that for 100% of quadratic extensions of k the number α is not a norm.

The next theorem generalises this observation. It says that, unless we are in a very special case, for 100% of G-extensions of k not all elements of $\mathcal{A}$ are norms.

Theorem 1.6. *Let k be a number field, G a non-trivial finite abelian group of exponent e, and $\mathcal{A} \subset k^*$ a finitely generated subgroup. Then the following are equivalent:*

(1) $\lim_{B\to\infty} \frac{N_{\mathrm{glob}}(k,G,\mathcal{A},B)}{N(k,G,B)} > 0$*;*
(2) $\mathcal{A} \subset k(\mu_d)^{*d}$ *for all* $d \mid e$*;*
(3) $\mathcal{A} \subset k_v^{*e}$ *for all but finitely many places* v *of* k*.*

There is a nice cohomological way to interpret the condition (3) in Theorem 1.6 via certain Tate–Shafarevich groups (see §4.6). Together with some class field theory, this will allow us to deduce the following result.

Corollary 1.7. *Let $\mathcal{A} \subset k^*$ be a finitely generated subgroup and let e be the exponent of G. Then the limit*

$$\lim_{B\to\infty} \frac{N_{\mathrm{glob}}(k, G, \mathcal{A}, B)}{N(k, G, B)} \tag{1.2}$$

(i) only depends on the image $\mathcal{A}k^{*e}$ of $\mathcal{A}$ in k^*/k^{*e};
(ii) equals one if $\mathcal{A} \subset k^{*e}$;
(iii) is zero for all but finitely many finite subgroups $\mathcal{A}k^{*e} \subset k^*/k^{*e}$;
(iv) is zero for all finitely generated subgroups $\mathcal{A} \not\subset k^{*e}$ if and only if the extension $k(\mu_{2^r})/k$ is cyclic, where 2^r is the largest power of 2 dividing e.

Condition (iv) holds for example if $8 \nmid e$ or $\mu_e \subset k^*$. Our next result shows that if G is cyclic then in order to have

$$0 < \lim_{B\to\infty} \frac{N_{\mathrm{glob}}(k, G, \mathcal{A}, B)}{N(k, G, B)} < 1,$$

for some choice of $\mathcal{A}$, the field k must have more than one prime lying above 2.

Theorem 1.8. *Let k be a number field, let $\mathcal{A} \subset k^*$ be a finitely generated subgroup, and let G be a finite cyclic group. Suppose that k has only one prime lying above 2. Then the following are equivalent:*

(1) $\lim_{B\to\infty} \frac{N_{\mathrm{glob}}(k,G,\mathcal{A},B)}{N(k,G,B)} > 0$*;*
(2) every element of $\mathcal{A}$ is a global norm from every G-extension of k.

A necessary condition for an element of k to be a global norm is that it is a norm everywhere locally. However, this is not a sufficient condition in general due to possible failures of the *Hasse norm principle* (HNP). Nevertheless, to prove Theorem 1.4, we reduce to the case of everywhere local norms via the following theorem, which shows that, when ordered by conductor, "most" abelian extensions satisfy the Hasse norm principle.

Theorem 1.9. *Let k be a number field, G a finite abelian group, and $\mathcal{A} \subset k^*$ a finitely generated subgroup. Then*

$$\lim_{B\to\infty} \frac{\#\{\varphi \in G\text{-}ext(k) : \Phi(\varphi) \leq B, \mathcal{A} \subset \mathrm{N}_{K_\varphi/k}\, \mathbf{A}^*_{K_\varphi}, K_\varphi \text{ fails the HNP}\}}{N_{\mathrm{loc}}(k, G, \mathcal{A}, B)} = 0.$$

In particular Theorem 1.9 implies that

$$\lim_{B\to\infty} \frac{N_{\mathrm{glob}}(k, G, \mathcal{A}, B)}{N_{\mathrm{loc}}(k, G, \mathcal{A}, B)} = 1.$$

Theorem 1.4 can thus be proved via an asymptotic formula for $N_{\mathrm{loc}}(k, G, \mathcal{A}, B)$, which we obtain in Theorem 4.1. We prove Theorem 1.9 using a purely local criterion for failure of the Hasse norm principle (Proposition 4.2). Taking $\mathcal{A} = \{1\}$ in Theorem 1.9, we obtain the following result.

Corollary 1.10. *Let k be a number field and G a finite abelian group. Then* 100% *of G-extensions of k, ordered by conductor, satisfy the Hasse norm principle.*

Corollary 1.10 stands in stark contrast to the results of [21], where a dichotomy occurs when counting by discriminant: in *op. cit.* we showed that for certain finite abelian groups G a positive proportion of G-extensions can fail the Hasse norm principle, when ordered by discriminant. This contrasting behaviour illustrates the fact, already observed by Wood in [51], that counting by conductor often leads to more natural statements than counting by discriminant. In fact, after seeing the results we obtained in [21] when counting extensions ordered by discriminant, Wood remarked that the dichotomy we had observed should disappear when ordering by conductor, and conjectured the statement of Corollary 1.10.

There are two reasons why it seems quite difficult to prove Theorem 1.1 when counting by discriminant, rather than conductor. Firstly, the condition that every element of $\mathcal{A}$ is a norm everywhere locally may be only rarely satisfied and, in the setting of [21, Thm. 1.4] where a positive proportion of G-extensions fail the Hasse norm principle, it becomes challenging to show the existence of a G-extension for which every element of $\mathcal{A}$ is a norm everywhere locally and the Hasse norm principle holds. Secondly, the leading constant obtained when counting by discriminant is very complicated, with potential for further cancellation, so it is difficult to prove its positivity, whereas when counting by conductor we have a simple criterion for positivity of the leading constant (see Theorem 3.1).

The counting techniques employed in this paper are fairly robust and enable us to prove a strengthening of Theorem 1.1 in which we impose local conditions at finitely many places. See Theorem 3.1 and Corollary 4.11 for precise statements.

Our work on the statistical behaviour of the Hasse norm principle brings together two major areas of modern number theory: namely, counting within families of number fields, and the quantitative study of the failure of local-global principles. Notable recent papers on the statistics of number fields include [1], [2], [4], [5], [19], [22], [28], [35] and [52]. Some significant contributions to the study of local-global principles in families include [3], [6], [7], [8], [20], [30] and [31]. For a summary of recent progress on counting failures of the Hasse principle, see [9]. More specifically, the statistical behaviour of the Hasse norm principle is examined in [10], [32] and [37]. In particular, in [37] Rome obtains an asymptotic

formula for the number of biquadratic extensions of $\mathbb{Q}$ (ordered by discriminant) which fail the Hasse norm principle. Obtaining asymptotic formulae for the number of such failures for other classes of field extensions would seem to be an interesting problem.

Below, we give some examples illustrating our results in a variety of settings to demonstrate the wide range of phenomena manifested by norms in extensions of number fields.

Examples 1.11.

(1) Take $G = \mathbb{Z}/n\mathbb{Z}$ with $8 \nmid n$ and $\alpha \in k^*$ not an nth power. Then Corollary 1.7 implies that for 100% of all $\mathbb{Z}/n\mathbb{Z}$-extensions of k ordered by conductor, α is not a norm. In the special case $n = 2$ of quadratic extensions, this result can be proved using standard techniques in analytic number theory; all other cases are new.

(2) Take $k = \mathbb{Q}, \alpha = 16$ and $G = \mathbb{Z}/8\mathbb{Z}$. As is well known, 16 is an 8th power in $\mathbb{Q}_p^*$ for all odd primes p and in $\mathbb{R}^*$. It therefore follows from Theorems 1.6 and 1.8 that 16 is a norm from every $\mathbb{Z}/8\mathbb{Z}$-extension $K/\mathbb{Q}$, despite not being an 8th power in $\mathbb{Q}$.

(3) Take $k = \mathbb{Q}(\sqrt{17})$, $\alpha = 16$ and $G = \mathbb{Z}/8\mathbb{Z}$. Then, as above, we see that 16 is locally an 8th power at all places v such that $v \nmid 2$. Hence 16 is a local norm from all $\mathbb{Z}/8\mathbb{Z}$-extensions of k at all places $v \nmid 2$. However, let $\mathfrak{p}, \mathfrak{q}$ be the two primes of k above 2. By [34, Thm. 9.2.8] there exists a $\mathbb{Z}/8\mathbb{Z}$-extension F/k such that $F_\mathfrak{p}/k_\mathfrak{p}$ is unramified of degree 8. Therefore, 16 is not a local norm from $F_\mathfrak{p}/k_\mathfrak{p}$, and consequently not a global norm from F/k. Given the existence of one such an extension, an application of [51, Cor. 1.7] (or Theorem 3.1) yields the existence of a positive proportion of $\mathbb{Z}/8\mathbb{Z}$-extensions K/k which are unramified of degree 8 over $\mathfrak{p}$, thus the limit (1.2) is positive but not equal to 1 in this case.

Let us explain in more detail why [34, Thm. 9.2.8] applies here but not in the previous example. Recall that a place v of a number field L is said to *split* (or *decompose*) in an extension M/L if there exist at least two distinct places of M above v. All places of $\mathbb{Q}$ apart from 2 split in the non-cyclic extension $\mathbb{Q}(\mu_8)/\mathbb{Q}$, so that $(\mathbb{Q}, 8, \Omega_\mathbb{Q} \setminus \{2\})$ is a so-called special case and [34, Thm. 9.2.8] does not apply in example (2). However, in example (3), $\mathfrak{q}$ is non-split in $k(\mu_8)/k$: both $\mathfrak{p}$ and $\mathfrak{q}$ are totally ramified in $k(\mu_8)/k$, since 2 is split in $k/\mathbb{Q}$ and totally ramified in $\mathbb{Q}(\mu_8)/\mathbb{Q}$. Therefore, $(k, 8, \Omega_k \setminus \{\mathfrak{p}\})$ is not a special case and [34, Thm. 9.2.8] can be applied in example (3).

(4) Take $k = \mathbb{Q}, \alpha = 5^2$ and $G = (\mathbb{Z}/2\mathbb{Z})^2$. A simple argument (cf. Lemma 4.4) shows that 5^2 is a norm everywhere locally from *every* biquadratic extension of $\mathbb{Q}$. By Theorem 1.9, it is thus a global norm from 100% of biquadratic extensions of $\mathbb{Q}$ ordered by conductor. However, 5^2 is not a global norm from $K = \mathbb{Q}(\sqrt{13}, \sqrt{17})$ (failure of the Hasse norm principle [11, p. 360, Exercise 5.3]). Therefore, it is not true that 5^2 is a global norm from *every* biquadratic extension of $\mathbb{Q}$.

Remark 1.12. A simple application of local class field theory (Lemma 4.4) shows that every element of k^{*e} is everywhere locally a norm from every G-extension of k, where e denotes the exponent of G. Using this, one can show that in our results, the assumption that $\mathcal{A}$ is a finitely generated subgroup of k^* can be replaced by the weaker assumption that the image of $\mathcal{A}$ in k^*/k^{*e} is finite. We have chosen to make the stronger assumption as it simplifies the exposition and some technical aspects of the proofs.

We finish with a simple example which solves the problem analogous to Theorem 1.1 for field extensions of degree n with maximal Galois group.

Example 1.13. Let $\alpha \in \mathbb{Q}^*$ and $n \geq 3$. Then the polynomial

$$x^n + cx^{n-1} + tx + (-1)^n \alpha$$

has Galois group S_n over $\mathbb{Q}(t)$ for all but finitely many $c \in \mathbb{Q}$ (see [27, Satz 1]). Therefore, Hilbert's irreducibility theorem implies that for infinitely many specialisations $t \in \mathbb{Q}$, the Galois group is S_n, and α is clearly a norm from such an extension, being the product of the roots of the defining polynomial.

1.1. **Methodology and structure of the paper.** In §2 we recall some of the theory of *frobenian functions* from Serre's book [43, §3.3], in order to help analyse the Dirichlet series which arise in this paper.

In §3 we prove our main technical result, Theorem 3.1. This is a general theorem for counting abelian extensions with local conditions imposed. To prove this we study the analytic properties of the Dirichlet series corresponding to our counting functions. We achieve this with the help of the harmonic analysis techniques developed in our earlier paper [21]. In our case, however, the analysis is more difficult as the singularities of our Dirichlet series will be *branch point* singularities, rather than poles, in general; this is reflected in the fact that $\varpi(k, G, \mathcal{A})$ in Theorem 1.4 can be a *non-integral rational number*. This section is the technical heart of the paper and is dedicated to the proof of Theorem 3.1.

Let us emphasise once more that we prove Theorem 1.1 by first counting the extensions of interest and then showing that the leading constant obtained is positive. Our situation presents an interesting difficulty, however: the leading constant we obtain is not an Euler product but a *sum* of Euler products and, in general, cancellation within these sums may occur for some choices of local conditions. For example, a famous theorem of Wang [49] says that there is no $\mathbb{Z}/8\mathbb{Z}$-extension of $\mathbb{Q}$ which realises the unramified extension of $\mathbb{Q}_2$ of degree 8; in this case Wright observed in [53, p. 48] that the Euler products appearing in the leading constant cancel out. We have to carefully analyse these sums of Euler products and explicitly show that no cancellation occurs in our case.

In §4, we prove the major results stated in the introduction via suitable applications of Theorem 3.1 combined with Galois-cohomological techniques. At the end of §4 we also give a generalisation of Theorem 1.1 which allows one to impose local conditions on the abelian extension K/k at finitely many places.

The appendix (by Yonatan Harpaz and Olivier Wittenberg) contains a purely geometric proof of Theorem 1.1. It uses descent and a version of the fibration method developed in [25] to show that the Brauer–Manin obstruction controls the failure of weak approximation on a certain auxiliary variety. The existence of the

required abelian extension is then shown using a version of Hilbert's irreducibility theorem due to Ekedahl [18] (see also [44, §§3.5–3.6]).

1.2. **Notation and conventions.** We fix a number field k throughout the paper and use the following notation:

$\mathbf{A}^*$	the ideles of k
$\mathbf{A}_L^*$	the ideles of a finite extension L of k
$\mathcal{O}_k$	the ring of integers of k
Ω_k	the set of all places of k
$\mathcal{O}_S$	the S-integers of k
v	a place of k
k_v	the completion of k at v
$\mathcal{O}_v$	the ring of integers of k_v. For $v \mid \infty$, by convention $\mathcal{O}_v := k_v$
$\mathbb{F}_v$	the residue field at a finite place v
q_v	the cardinality of the residue field at a finite place v
$\zeta_k(s)$	the Dedekind zeta function of k.

For locally compact abelian groups A and B, we use the following notation:

$\mathrm{Hom}(A, B)$	the group of *continuous* homomorphisms from A to B, equipped with the compact-open topology
$A^\wedge$	the Pontryagin dual of A, $A^\wedge := \mathrm{Hom}(A, S^1)$
$\langle \cdot, \cdot \rangle$	the natural pairing $A \times A^\wedge \to S^1$.

All finite groups are viewed as topological groups with the discrete topology.

For a place v of k, a finite abelian group G, and $\chi \in \mathrm{Hom}(k_v^*, G)$, we denote by $\Phi_v(\chi_v)$ the reciprocal of the v-adic norm of the conductor of $\operatorname{Ker} \chi_v$. For every $\chi \in \mathrm{Hom}(\mathbf{A}^*/k^*, G)$, we let $\Phi(\chi)$ be the reciprocal of the idelic norm of the conductor of the kernel of χ; this equals the norm $\Phi(\varphi)$ of the conductor of the sub-G-extension φ corresponding to χ via the global Artin map.

Let K/k be an extension of number fields and $\alpha \in k^*$. We say that α is a *(global) norm from* K if $\alpha \in \mathrm{N}_{K/k} K^*$. We say that α is a *local norm at* v *from* K if $\alpha \in \prod_{w|v} \mathrm{N}_{K_w/k_v} K_w^* \subset k_v^*$; if K/k is Galois this is equivalent to the existence of *some* place $w \mid v$ of K such that $\alpha \in \mathrm{N}_{K_w/k_v} K_w^*$.

If F is a field which contains d distinct dth roots of unity and $\mathcal{A} \subset F^*$ is a finitely generated subgroup, then we denote by $F(\sqrt[d]{\mathcal{A}})$ the splitting field of the polynomials $x^d - \alpha$, where α runs over a set of generators of $\mathcal{A}$.

For a subgroup $\mathcal{A} \subset k^*$ and a place v of k, we denote by $\mathcal{A}_v$ the image of $\mathcal{A}$ in k_v^*.

Acknowledgements. Our work on this project began at Michael Stoll's workshop *Rational Points 2017* held at Franken-Akademie Schloss Schney. Substantial progress was made when the third author visited the other two at the University of Manchester, and also at the workshop *Rational and Integral Points via Analytic and Geometric Methods* organised by Tim Browning, Ulrich Derenthal and Cecília Salgado at Hotel Hacienda Los Laureles, Oaxaca. We are very grateful to the organisers of both workshops, to the funding bodies, and to the staff at all three places for providing us with excellent working conditions. We thank the anonymous referee for a meticulous reading of an earlier draft of this

paper and for several suggestions that helped improve it. The second-named author is supported by EPSRC grant EP/R021422/1 and UKRI Future Leaders Fellowship MR/V021362/1. The third-named author is supported by EPSRC grant EP/S004696/1 and UKRI Future Leaders Fellowship MR/T041609/1.

2. Frobenian functions

For the proofs of our main results, we will require some of the theory of frobenian functions, as can be found in Serre's book [43, §3.3]. Recall that a *class function* on a group is a function which is constant on conjugacy classes.

Definition 2.1. Let k be a number field and $\rho : \Omega_k \to \mathbb{C}$ a function on the set of places of k. Let S be a finite set of places of k. We say that ρ is *S-frobenian* if there exist

(a) a finite Galois extension K/k, with Galois group Γ, such that S contains all places which ramify in K/k, and
(b) a class function $\varphi : \Gamma \to \mathbb{C}$,

such that for all $v \notin S$ we have

$$\rho(v) = \varphi(\mathrm{Frob}_v),$$

where $\mathrm{Frob}_v \in \Gamma$ denotes a Frobenius element of v. We say that ρ is *frobenian* if it is S-frobenian for some S. A subset of Ω_k is called (S-)*frobenian* if its indicator function is (S-)frobenian.

In Definition 2.1, we adopt a common abuse of notation (see [43, §3.2.1]), and denote by $\mathrm{Frob}_v \in \Gamma$ the choice of some element of the Frobenius conjugacy class at v; note that $\varphi(\mathrm{Frob}_v)$ is well defined as φ is a class function.

We define the *mean* of ρ to be

$$m(\rho) = \frac{1}{|\Gamma|} \sum_{\gamma \in \Gamma} \varphi(\gamma) \in \mathbb{C}.$$

Example 2.2. Let $f \in k[x]$ be a (not necessarily irreducible) polynomial. Then the set

$$\{v \in \Omega_k : f(x) \text{ has a root in } k_v\}$$

is frobenian. Indeed, take K to be the splitting field of f. Then for a place v which is unramified in K, the polynomial f has a root in k_v if and only if Frob_v acts with a fixed point on the roots of f over $\bar{k}$; the set of such elements is a conjugacy invariant subset of the Galois group Γ.

We require the following result on the zeta function of a frobenian function. Throughout the paper, we write q_v for the size of the residue field at a finite place v. Moreover, for any place v, let $\zeta_{k,v}(s)$ be the Euler factor of $\zeta_k(s)$ at v if v is non-archimedean, and $\zeta_{k,v}(s) = 1$ otherwise.

Proposition 2.3. *Let S be a finite set of places of k containing all archimedean places and let ρ be an S-frobenian function. Assume that $|\rho(v)| < q_v$ holds for all $v \notin S$. Then the Euler product*

$$F(s) = \prod_{v \notin S} \left(1 + \frac{\rho(v)}{q_v^s}\right) \tag{2.1}$$

has the form

$$F(s) = \zeta_k^{m(\rho)}(s)G(s), \quad \operatorname{Re} s > 1, \tag{2.2}$$

for a function $G(s)$ that is holomorphic in a region

$$\operatorname{Re} s > 1 - \frac{c}{\log(|\operatorname{Im} s| + 3)}, \tag{2.3}$$

for some $c = c_\rho > 0$, and satisfies in this region the bound

$$|G(s)| \ll_\rho (1 + |\operatorname{Im} s|)^{1/2}. \tag{2.4}$$

Moreover,

$$\lim_{s\to 1}(s-1)^{m(\rho)}F(s) = (\operatorname{Res}_{s=1}\zeta_k(s))^{m(\rho)} \prod_{v\notin S} \frac{1+\rho(v)q_v^{-1}}{\zeta_{k,v}(1)^{m(\rho)}} \prod_{v\in S} \frac{1}{\zeta_{k,v}(1)^{m(\rho)}}, \tag{2.5}$$

and the limit in (2.5) *is non-zero.*

Proof. First, note that the Euler factors $1 + \rho(v)q_v^{-s}$ are holomorphic on $\mathbb{C}$ and non-zero for $\operatorname{Re} s \geq 1$, as $|\rho(v)| < q_v$ by assumption. Next, recall that the irreducible characters of a finite group Γ form a basis for the space of complex class functions of Γ [23, Prop. 2.30]. In particular, if $\varphi : \Gamma \to \mathbb{C}$ is the class function associated to ρ, then we may write

$$\varphi = \sum_\chi \lambda_\chi \chi$$

where $\lambda_\chi \in \mathbb{C}$ and the sum runs over the irreducible characters of Γ. For $\operatorname{Re} s > 1$, we find that

$$F(s) = \prod_{v\notin S}\left(1 + \frac{\sum_\chi \lambda_\chi \chi(\operatorname{Frob}_v)}{q_v^s}\right) = G_1(s)\prod_\chi L(\chi, s)^{\lambda_\chi},$$

where $L(\chi, s)$ denotes the Artin L-function of χ and $G_1(s)$ is a holomorphic function with absolutely convergent Euler product on $\operatorname{Re} s > 1/2$, which is non-zero on $\operatorname{Re} s \geq 1$.

For the trivial character $\chi = \mathbb{1}$, we have $L(\mathbb{1}, s) = \zeta_k(s)$. Since $\lambda_{\mathbb{1}} = m(\rho)$, we get the equality (2.2) with

$$G(s) = G_1(s)\prod_{\chi\neq\mathbb{1}} L(\chi, s)^{\lambda_\chi}.$$

By the Brauer induction theorem [11, Thm. VIII.7, p. 225], we may decompose each remaining $L(\chi, s)$ as a product of $\mathbb{Z}$-powers of Hecke L-functions of non-trivial Hecke characters of subfields of K. Hence, we assume from now on that each $L(\chi, s)$ is an entire Hecke L-function (for some possibly different number field). By [29, Thm. 5.35], $L(\chi, s)$ respects a zero-free region of the form (2.3), for some $c < 1/4$ that may depend on χ. Since there are only finitely many characters to consider, we can find a constant c that works for all of them. Decreasing c further, we obtain a bound

$$\log|L(\chi, s)| \ll \log\log(|\operatorname{Im} s| + 3),$$

valid in the region (2.3) (cf. [40, p.230]). Using this bound and the fact that $|G_1(s)| \ll_\rho 1$ in $\operatorname{Re} s \geq 3/4$ due to the absolute convergence of its Euler product, it is simple to verify that $G(s)$ satisfies (2.4).

To verify (2.5), we start with the following fact, which is well known at least in the classical case of Dirichlet L-functions: for non-trivial χ, the Euler product of $L(\chi, s)$ converges for $s = 1$ and takes the value $L(\chi, 1)$. To see this, observe that $\log L(\chi, s)$ can be defined for $\operatorname{Re} s > 1$ as a Dirichlet series, use the prime number theorem for $L(\chi, s)$ (see [29, Thm. 5.13]) and partial summation to verify that this Dirichlet series converges for $s = 1$, and apply Abel's theorem.

Since $G_1(s)$ has an absolutely convergent Euler product for $\operatorname{Re} s > 1/2$, this shows that the Euler product of $\zeta_k(s)^{-m(\rho)}F(s) = G(s)$ does indeed converge at $s = 1$ and takes the value

$$G(1) = \lim_{s\to 1} \zeta_k(s)^{-m(\rho)}F(s) = (\operatorname{Res}_{s=1}\zeta_k(s))^{-m(\rho)} \lim_{s\to 1}(s-1)^{m(\rho)}F(s).$$

Recalling our assumption that $|\rho(v)| < q_v$, it is clear that the right-hand side of (2.5) is non-zero. □

Remark 2.4.

(1) Note that frobenian functions are bounded; thus the condition $|\rho(v)| < q_v$ in Proposition 2.3 is always satisfied for all but finitely many v.

(2) The conclusion (2.5) may fail if one includes the places $v \in S$ in the Euler product in Proposition 2.3. To see this, take $k = \mathbb{Q}, \rho(2) = -2$ and $\rho(p) = 0$ for $p \neq 2$; this is frobenian with $K = \mathbb{Q}$ and $S = \{2\}$. Then the Euler factor

$$1 - \frac{2}{2^s}$$

has a zero at $s = 1$, despite the fact that $m(\rho) = 0$.

(3) The conclusion (2.5) can fail to hold for some innocuous looking Dirichlet series. Consider for example $F(s) = \zeta(2s-1)/\zeta(s)$. Then $\lim_{s\to 1} F(s) = 1/2$, but $\prod_p \lim_{s\to 1}(1-p^{-s})/(1-p^{-2s+1}) = 1$.

3. Counting with local conditions

All of the main counting results in this paper are obtained from a more general counting result, which we present in this section. To state this result we require some notation.

3.1. **Statement of the result.** Let G be a finite abelian group, let F be a field and $\bar{F}$ a separable closure of F. We define a *sub-G-extension* of F to be a continuous homomorphism $\operatorname{Gal}(\bar{F}/F) \to G$. A sub-$G$-extension corresponds to a pair $(L/F, \psi)$, where L/F is a Galois extension inside $\bar{F}$ and ψ is an injective homomorphism $\operatorname{Gal}(L/F) \to G$.

For each place v of the number field k, we fix an algebraic closure $\bar{k}_v$ and compatible embeddings $k \hookrightarrow \bar{k} \hookrightarrow \bar{k}_v$ and $k \hookrightarrow k_v \hookrightarrow \bar{k}_v$.

Hence, a sub-G-extension φ of k induces a sub-G-extension φ_v of k_v at every place v. For each place v of k, let Λ_v be a set of sub-G-extensions of k_v. For $\Lambda := (\Lambda_v)_{v\in\Omega_k}$ we are interested in the function

$$N(k, G, \Lambda, B) := \#\left\{\varphi \in G\text{-ext}(k) : \Phi(\varphi) \leq B,\ \varphi_v \in \Lambda_v \forall v\right\}, \tag{3.1}$$

which counts those G-extensions of k of bounded conductor which satisfy the local conditions imposed by Λ at all places v. (Here Φ is as in §1.2.)

In general, it is difficult to say anything about the counting function given in (3.1), especially when there are infinitely many local conditions imposed. Even in the case when one imposes finitely many conditions, the set being counted may be empty, as explained in §1.1. Our main technical result imposes arbitrary conditions at finitely many places, but at the remaining places we only impose those conditions which force every element of $\mathcal{A}$ to be a local norm.

Theorem 3.1. *Let k be a number field, G a non-trivial finite abelian group, and $\mathcal{A} \subset k^*$ a finitely generated subgroup. Let S be a finite set of places of k and for $v \in S$ let Λ_v be a non-empty set of sub-G-extensions of k_v. For $v \notin S$ we let Λ_v be the set of sub-G-extensions of k_v determined by those extensions of local fields L/k_v for which every element of $\mathcal{A}$ is a local norm from L/k_v. Let $\Lambda := (\Lambda_v)_{v \in \Omega_k}$. Then there exist $c_{k,G,\Lambda} \geq 0$ and $\delta = \delta(k, G, \mathcal{A}) > 0$ such that*

$$N(k, G, \Lambda, B) = c_{k,G,\Lambda} B(\log B)^{\varpi(k,G,\mathcal{A})-1} + O(B(\log B)^{\varpi(k,G,\mathcal{A})-1-\delta}), \quad B \to \infty,$$

where $\varpi(k, G, \mathcal{A})$ is as in Definition 1.3. Moreover we have $c_{k,G,\Lambda} > 0$ if there exists a sub-G-extension of k which realises the given local conditions for all places v.

The leading constant $c_{k,G,\Lambda}$ in this theorem is given by a finite sum of Euler products (see Theorem 3.22 for an explicit expression). Our condition for positivity is only the existence of some *sub*-G-extension of k which realises the given local conditions; we do not require the existence of a genuine G-extension of k, so we do not need to assume that the set of G-extensions being counted is non-empty to deduce the positivity of the constant. This means that one need only look for an extension with possibly smaller Galois group to prove positivity of the constant; we use this trick to great effect when proving Theorem 1.1.

We illustrate how one applies Theorem 3.1 in some simple cases. Firstly, one counts the total number of G-extensions of k by applying Theorem 3.1 with $\mathcal{A} = \{1\}$ and no local conditions, i.e. taking Λ_v to be the set of all sub-G-extensions of k_v for all places v. These local conditions are realised by the sub-G-extension given by the trivial extension k/k. For a more interesting example, consider the case $\mathcal{A} = \{1\}$ and the trivial local conditions $\Lambda_v = \{\mathbb{1}\}$ for $v \in S$, which are again realised by the trivial extension k/k. This gives the following corollary. (Note that we do not need to avoid the places above 2.)

Corollary 3.2. *Let S be a finite set of places. Then a positive proportion of G-extensions of k, ordered by conductor, are completely split at all places in S.*

The rest of this section is dedicated to the proof of Theorem 3.1. All implied constants in the O and $\ll$ notation are allowed to depend on $k, G, \mathcal{A}$ and Λ.

3.2. **The set of places S.** To prove Theorem 3.1, we are free to increase the size of S if we wish. Henceforth, we will assume that S contains all archimedean places of k and all places of k lying above the primes $p \leq |G|$, that $\mathcal{A} \subset \mathcal{O}_S^*$, and that $\mathcal{O}_S$ has trivial class group.

The reader should note that many of the formulae which follow are only valid for finite sets of places S which satisfy these conditions. For example, in the case where $k = \mathbb{Q}$, $G = \mathbb{Z}/8\mathbb{Z}$, $\mathcal{A} = \{1\}$, $S = \emptyset$, the expression for the leading

constant in Theorem 3.22 does not hold. To compute $c_{k,G,\Lambda}$ in this instance, we may take $S = \{\infty, 2, 3, 5\}$ instead.

3.3. **Dirichlet series.** To prove Theorem 3.1 we study the associated Dirichlet series

$$F_\Lambda(s) = \sum_{\varphi \in G\text{-ext}(k)} \frac{f_\Lambda(\varphi)}{\Phi(\varphi)^s}, \tag{3.2}$$

with f_Λ the indicator function of those sub-G-extensions $\varphi \in \mathrm{Hom}(\mathrm{Gal}(\bar{k}/k), G)$ for which $\varphi_v \in \Lambda_v$ for all $v \in \Omega_k$. Hence, f_Λ is the product of the local indicator functions f_{Λ_v} of Λ_v. As $|f_\Lambda(\varphi)| \leq 1$, this Dirichlet series defines a holomorphic function on $\mathrm{Re}\, s > 1$. (This follows from [51, Lem. 2.10], but also from the analysis later in this paper.)

3.3.1. *Möbius inversion.* Recall that a G-extension of k is a surjective continuous homomorphism $\varphi : \mathrm{Gal}(\bar{k}/k) \to G$. The condition that φ be surjective is difficult to deal with, hence we perform a Möbius inversion to remove it. Let μ be the Möbius function on isomorphism classes of finite abelian groups. That is, $\mu(G) = 0$ if G has a cyclic subgroup of order p^n with p a prime and $n \geq 2$, $\mu(G_1 \times G_2) = \mu(G_1)\mu(G_2)$ if G_1 and G_2 have coprime order, and $\mu((\mathbb{Z}/p\mathbb{Z})^n) = (-1)^n p^{n(n-1)/2}$ for a prime p and $n \in \mathbb{Z}_{\geq 0}$. Let f be a function on the subgroups of G. For subgroups $H \subset G$, we consider the function

$$g(H) = \sum_{J \subset H} f(J),$$

where the sum runs over all subgroups $J \subset H$. The Möbius inversion formula for finite abelian groups [17] states that

$$f(G) = \sum_{H \subset G} \mu(G/H) g(H). \tag{3.3}$$

Lemma 3.3. *We have*

$$F_\Lambda(s) = \sum_{H \subset G} \mu(G/H) \sum_{\varphi \in \mathrm{Hom}(\mathrm{Gal}(\bar{k}/k), H)} \frac{f_\Lambda(\varphi)}{\Phi(\varphi)^s}.$$

Proof. Sorting the sub-H-extensions $\varphi : \mathrm{Gal}(\bar{k}/k) \to H$ by their images, we get

$$\sum_{J \subset H} \sum_{\varphi \in J\text{-ext}(k)} \frac{f_\Lambda(\varphi)}{\Phi(\varphi)^s} = \sum_{\varphi \in \mathrm{Hom}(\mathrm{Gal}(\bar{k}/k), H)} \frac{f_\Lambda(\varphi)}{\Phi(\varphi)^s}.$$

Call the right-hand side $g(H)$ and apply Möbius inversion (3.3). □

We now consider the contribution to $F_\Lambda(s)$ of each subgroup H in turn. The contribution from $H = \{1\}$ is either 0 or 1. From now on we focus on the contributions of the non-trivial subgroups H.

3.3.2. *Class field theory.* Via global class field theory, we make the identification

$$\mathrm{Hom}(\mathrm{Gal}(\bar{k}/k), H) = \mathrm{Hom}(\mathbf{A}^*/k^*, H). \tag{3.4}$$

The canonical isomorphism (3.4) is induced by the global Artin map $\mathbf{A}^*/k^* \to \mathrm{Gal}(k^{\mathrm{ab}}/k)$. Using this isomorphism, we consider f_Λ now as a function on $\mathrm{Hom}(\mathbf{A}^*/k^*, H)$. For every $\chi \in \mathrm{Hom}(\mathbf{A}^*/k^*, H)$, let $\Phi(\chi)$ be the reciprocal of the idelic norm of the conductor of the kernel of χ, which is precisely the norm of the conductor of the sub-H-extension corresponding to χ. Together with Lemma 3.3, this discussion shows the following:

Lemma 3.4. *We have*

$$F_\Lambda(s) = \sum_{H \subset G} \mu(G/H) \sum_{\chi \in \mathrm{Hom}(\mathbf{A}^*/k^*, H)} \frac{f_\Lambda(\chi)}{\Phi(\chi)^s}.$$

Hence, in our analysis of $F_\Lambda(s)$ we can now focus on the inner sums

$$\sum_{\chi \in \mathrm{Hom}(\mathbf{A}^*/k^*, H)} \frac{f_\Lambda(\chi)}{\Phi(\chi)^s}.$$

Our counting problem fits very well within the class-field-theoretic framework. For each place $v \in \Omega_k$, we use local class field theory (specifically, the local Artin map $k_v^* \to \mathrm{Gal}(k_v^{\mathrm{ab}}/k_v)$) to make the identification

$$\mathrm{Hom}(\mathrm{Gal}(\bar{k}_v/k_v), H) = \mathrm{Hom}(k_v^*, H).$$

Thus, we consider Λ_v as a subset of $\mathrm{Hom}(k_v^*, H)$. By the compatibility of local and global class field theory, we still have $f_\Lambda = \prod_v f_{\Lambda_v}$, with f_{Λ_v} the indicator function of Λ_v.

Lemma 3.5. *Let $v \notin S$ and let $\chi_v \in \mathrm{Hom}(k_v^*, G)$. Then*

$$f_{\Lambda_v}(\chi_v) = 1 \quad \Leftrightarrow \quad \mathcal{A}_v \subset \mathrm{Ker}\, \chi_v.$$

Proof. Let φ_v be the sub-G-extension of k_v associated to χ_v. By local class field theory we have

$$\mathrm{Ker}\, \chi_v = \mathrm{N}_{K_{\varphi_v}/k_v} K_{\varphi_v}^*,$$

where K_{φ_v} is the extension field of k_v associated to φ_v. However, as $v \notin S$, by assumption in Theorem 3.1 we have $f_{\Lambda_v}(\chi_v) = 1$ if and only if every element of $\mathcal{A}$ is a local norm from K_{φ_v}; the result follows. □

3.4. **Harmonic analysis.** To deal with the sums

$$\sum_{\chi \in \mathrm{Hom}(\mathbf{A}^*/k^*, H)} \frac{f_\Lambda(\chi)}{\Phi(\chi)^s}$$

we shall use a version of the Poisson summation formula from harmonic analysis. The theory relevant to us was worked out in detail in [21, §3] when counting by *discriminant*. The same theory transfers almost verbatim to show the validity of the Poisson summation formula for counting by conductor.

However, for the purposes of Theorem 3.1, our case is special enough that we merely require a simplified version of the Poisson summation formula that can be proved using only character orthogonality for finite abelian groups. We may therefore forego some of the general theory from [21, §3] and proceed in a more explicit manner. We first recall the set-up for the harmonic analysis.

3.4.1. *Fourier transforms.* The group $\mathrm{Hom}(\mathbf{A}^*/k^*, H)$ is locally compact. Its Pontryagin dual is naturally identified with $\mathbf{A}^*/k^* \otimes H^\wedge$ (see [21, §3.1]). We denote the associated pairing by $\langle \cdot, \cdot \rangle : \mathrm{Hom}(\mathbf{A}^*/k^*, H) \times (\mathbf{A}^*/k^* \otimes H^\wedge) \to S^1$. Similarly, the Pontryagin dual of $\mathrm{Hom}(k_v^*, H)$ is naturally identified with $k_v^* \otimes H^\wedge$, and we also denote the relevant Pontryagin pairing by $\langle \cdot, \cdot \rangle$. For each place v, we equip the finite group $\mathrm{Hom}(k_v^*, H)$ with the unique Haar measure $\mathrm{d}\chi_v$ such that

$$\mathrm{vol}(\mathrm{Hom}(k_v^*/\mathcal{O}_v^*, H)) = 1.$$

If v is non-archimedean, this is $|H|^{-1}$ times the counting measure; for archimedean v, recalling our convention that $\mathcal{O}_v = k_v$, we obtain the counting measure. The product of these measures yields a well-defined measure $\mathrm{d}\chi$ on $\mathrm{Hom}(\mathbf{A}^*, H)$. We say that an element of $\mathrm{Hom}(k_v^*, H)$ is *unramified* if it lies in the subgroup $\mathrm{Hom}(k_v^*/\mathcal{O}_v^*, H)$, i.e. if it is trivial on $\mathcal{O}_v^*$, and that it is *tamely ramified* if it is ramified and trivial on $1 + \pi_v \mathcal{O}_v$.

The function f_Λ/Φ^s is a product of local functions f_{Λ_v}/Φ_v^s on $\mathrm{Hom}(k_v^*, H)$, where $\Phi_v(\chi_v)$ is the reciprocal of the v-adic norm of the conductor of $\mathrm{Ker}\,\chi_v$. For $v \notin S$, these local functions take only the value 1 on the unramified elements by our choice of S and Lemma 3.5, and thus f_Λ/Φ^s extends to a well-defined and continuous function on $\mathrm{Hom}(\mathbf{A}^*, H)$. We define its Fourier transform to be

$$\widehat{f}_{\Lambda,H}(x; s) = \int_{\chi \in \mathrm{Hom}(\mathbf{A}^*, H)} \frac{f_\Lambda(\chi)\langle \chi, x \rangle}{\Phi(\chi)^s} \mathrm{d}\chi,$$

where $x = (x_v)_v \in \mathbf{A}^* \otimes H^\wedge$. Similarly, for $x_v \in k_v^* \otimes H^\wedge$ we have the local Fourier transform

$$\widehat{f}_{\Lambda_v,H}(x_v; s) = \int_{\chi_v \in \mathrm{Hom}(k_v^*, H)} \frac{f_{\Lambda_v}(\chi_v)\langle \chi_v, x_v \rangle}{\Phi_v(\chi_v)^s} \mathrm{d}\chi_v.$$

For $\mathrm{Re}\, s \gg 1$, the global Fourier transform exists and defines a holomorphic function in this domain, and there is an Euler product decomposition

$$\widehat{f}_{\Lambda,H}(x; s) = \prod_v \widehat{f}_{\Lambda_v,H}(x_v; s). \tag{3.5}$$

3.4.2. *The local Fourier transforms.* Let $v \in \Omega_k$ and $x_v \in k_v^* \otimes H^\wedge$.

Lemma 3.6. *The local Fourier transform $\widehat{f}_{\Lambda_v,H}(x_v; s)$ is holomorphic on $\mathbb{C}$ and satisfies $\widehat{f}_{\Lambda_v,H}(x_v; s) \ll_{k,H} 1$ on $\mathrm{Re}\, s \geq 0$. Moreover $\widehat{f}_{\Lambda_v,H}(1; s) > 0$ for $s \in \mathbb{R}$.*

Proof. We prove the result when v is non-archimedean, the case of archimedean v being analogous. By our choice of measures, we have

$$\widehat{f}_{\Lambda_v,H}(x_v; s) = \frac{1}{|H|} \sum_{\chi_v \in \mathrm{Hom}(k_v^*, H)} \frac{f_{\Lambda_v}(\chi_v)\langle \chi_v, x_v \rangle}{\Phi_v(\chi_v)^s}. \tag{3.6}$$

This finite sum clearly defines a holomorphic function on $\mathbb{C}$. If $\mathrm{Re}\, s \geq 0$ then the sum is $\ll_{k,H} 1$, since every summand is bounded absolutely and the number of summands is $\ll_{k,H} 1$. For the last part, we have

$$\widehat{f}_{\Lambda_v,H}(1; s) = \frac{1}{|H|} \sum_{\chi_v \in \Lambda_v} \frac{1}{\Phi_v(\chi_v)^s}.$$

For $v \in S$ the set Λ_v is non-empty by assumption. For $v \notin S$ the set Λ_v is again non-empty, as it always contains the trivial homomorphism $k_v^* \to H$ by Lemma 3.5. For $s \in \mathbb{R}$, we therefore obtain a finite non-empty sum of positive real numbers, which is positive. $\square$

Now let v be non-archimedean. Choosing a uniformiser of k_v identifies $k_v^*/\mathcal{O}_v^*$ with $\mathbb{Z}$ and gives a splitting of the exact sequence

$$1 \to \mathcal{O}_v^* \to k_v^* \to k_v^*/\mathcal{O}_v^* \to 1. \tag{3.7}$$

This implies that the sequence

$$1 \to \operatorname{Hom}(k_v^*/\mathcal{O}_v^*, H) \to \operatorname{Hom}(k_v^*, H) \to \operatorname{Hom}(\mathcal{O}_v^*, H) \to 1$$

is split exact. Thus

$$\widehat{f}_{\Lambda_v,H}(x_v; s) = \frac{1}{|H|} \sum_{\psi_v \in \operatorname{Hom}(k_v^*/\mathcal{O}_v^*, H)} \sum_{\chi_v \in \operatorname{Hom}(\mathcal{O}_v^*, H)} \frac{f_{\Lambda_v}(\psi_v\chi_v)\langle \psi_v\chi_v, x_v\rangle}{\Phi_v(\chi_v)^s}, \tag{3.8}$$

since ψ_v is unramified and hence $\Phi(\psi_v\chi_v) = \Phi_v(\chi_v)$.

Lemma 3.7. *Let $v \notin S$. Then f_{Λ_v} is $\operatorname{Hom}(k_v^*/\mathcal{O}_v^*, H)$-invariant and, in particular, $f_{\Lambda_v}(\psi_v) = 1$ for all $\psi_v \in \operatorname{Hom}(k_v^*/\mathcal{O}_v^*, H)$.*

Proof. Let $\chi_v \in \operatorname{Hom}(k_v^*, H)$ and let $\psi_v \in \operatorname{Hom}(k_v^*/\mathcal{O}_v^*, H)$. We use the criterion from Lemma 3.5. We have $\mathcal{A}_v \subset \mathcal{O}_v^* \subset \operatorname{Ker}\psi_v$. Therefore $\mathcal{A}_v \subset \operatorname{Ker}\psi_v\chi_v$ if and only if $\mathcal{A}_v \subset \operatorname{Ker}\chi_v$, whence $f_{\Lambda_v}(\psi_v\chi_v) = f_{\Lambda_v}(\chi_v)$, as required. With $\chi_v = \mathbb{1}$, this also shows the second assertion. $\square$

In the statement of the following lemma, note that the natural map $\mathcal{O}_v^* \otimes H^\wedge \to k_v^* \otimes H^\wedge$ is injective, as the sequence (3.7) is split exact. Therefore, we may naturally view $\mathcal{O}_v^* \otimes H^\wedge$ as a subgroup of $k_v^* \otimes H^\wedge$.

Lemma 3.8. *Let $v \notin S$. Then*

$$\widehat{f}_{\Lambda_v,H}(x_v; s) = \begin{cases} \displaystyle\sum_{\chi_v \in \operatorname{Hom}(\mathcal{O}_v^*, H)} \frac{f_{\Lambda_v}(\chi_v)\langle \chi_v, x_v\rangle}{\Phi_v(\chi_v)^s}, & \text{if } x_v \in \mathcal{O}_v^* \otimes H^\wedge, \\ 0, & \text{otherwise.} \end{cases}$$

Proof. From (3.8) and Lemma 3.7 we have

$$\widehat{f}_{\Lambda_v,H}(x_v; s) = \frac{1}{|H|} \sum_{\chi_v \in \operatorname{Hom}(\mathcal{O}_v^*, H)} \frac{f_{\Lambda_v}(\chi_v)\langle \chi_v, x_v\rangle}{\Phi_v(\chi_v)^s} \sum_{\psi_v \in \operatorname{Hom}(k_v^*/\mathcal{O}_v^*, H)} \langle \psi_v, x_v\rangle.$$

Now character orthogonality gives

$$\sum_{\psi_v \in \operatorname{Hom}(k_v^*/\mathcal{O}_v^*, H)} \langle \psi_v, x_v\rangle = \begin{cases} |\operatorname{Hom}(k_v^*/\mathcal{O}_v^*, H)|, & \text{if } x_v \in \mathcal{O}_v^* \otimes H^\wedge, \\ 0, & \text{otherwise.} \end{cases}$$

Indeed, the subgroup $\mathcal{O}_v^* \otimes H^\wedge \subset k_v^* \otimes H^\wedge$ is naturally identified with the Pontryagin dual of $\operatorname{Hom}(k_v^*/\mathcal{O}_v^*, H)$. The result now follows on noting that $k_v^*/\mathcal{O}_v^* \cong \mathbb{Z}$ and hence $|\operatorname{Hom}(k_v^*/\mathcal{O}_v^*, H)| = |H|$. $\square$

3.4.3. *Poisson summation.* We now prove the version of Poisson summation that we will require. In the statement, we view $\mathcal{O}_S^* \otimes H^\wedge$ as a subgroup of $k^* \otimes H^\wedge$ as follows: we have the exact sequence

$$0 \to \mathcal{O}_S^* \to k^* \to P(\mathcal{O}_S) \to 0 \tag{3.9}$$

where $P(\mathcal{O}_S)$ denotes the group of non-zero principal fractional ideals of $\mathcal{O}_S$. Since $P(\mathcal{O}_S)$ is a free abelian group, we have $\mathrm{Tor}(P(\mathcal{O}_S), H^\wedge) = 0$. Therefore applying $(\cdot) \otimes H^\wedge$ to (3.9) we find that the map $\mathcal{O}_S^* \otimes H^\wedge \to k^* \otimes H^\wedge$ is injective, as required.

Proposition 3.9. *For* $\mathrm{Re}\, s > 1$ *the Fourier transform* $\widehat{f}_{\Lambda,H}(\cdot; s)$ *exists and defines a holomorphic function on this domain. Moreover, we have the Poisson formula*

$$\sum_{\chi \in \mathrm{Hom}(\mathbf{A}^*/k^*, H)} \frac{f_\Lambda(\chi)}{\Phi(\chi)^s} = \frac{1}{|\mathcal{O}_k^* \otimes H^\wedge|} \sum_{x \in \mathcal{O}_S^* \otimes H^\wedge} \widehat{f}_{\Lambda,H}(x; s), \quad \mathrm{Re}\, s > 1. \tag{3.10}$$

Note that the group $\mathcal{O}_S^* \otimes H^\wedge$ is finite by Dirichlet's S-unit theorem; in particular the right-hand sum is finite.

Proof. Let $x \in \mathcal{O}_S^* \otimes H^\wedge$. Let x_v denote its image in $k_v^* \otimes H^\wedge$. Recall that we have normalised our Haar measures on $\mathrm{Hom}(k_v^*, H)$ to be $|H|^{-1}$ times the counting measure for non-archimedean v, and equal to the counting measure for archimedean v. We let S_f be the set of non-archimedean places in S. Now Lemma 3.8 and (3.5) give

$$\begin{aligned}\widehat{f}_{\Lambda,H}(x; s) &= \frac{1}{|H|^{|S_\mathrm{f}|}} \prod_{v \in S} \sum_{\chi_v \in \mathrm{Hom}(k_v^*, H)} \frac{f_{\Lambda_v}(\chi_v)\langle \chi_v, x_v\rangle}{\Phi_v(\chi_v)^s} \prod_{v \notin S} \sum_{\chi_v \in \mathrm{Hom}(\mathcal{O}_v^*, H)} \frac{f_{\Lambda_v}(\chi_v)\langle \chi_v, x_v\rangle}{\Phi_v(\chi_v)^s} \\ &= \frac{1}{|H|^{|S_\mathrm{f}|}} \sum_{\chi \in \mathrm{Hom}(\mathbf{A}_S^*, H)} \frac{f_\Lambda(\chi)\langle \chi, x\rangle}{\Phi(\chi)^s}\end{aligned}$$

where $\mathbf{A}_S^* = \prod_{v \in S} k_v^* \times \prod_{v \notin S} \mathcal{O}_v^*$. We now change the order of summation in the right-hand sum of (3.10) to obtain

$$\sum_{x \in \mathcal{O}_S^* \otimes H^\wedge} \widehat{f}_{\Lambda,H}(x; s) = \frac{1}{|H|^{|S_\mathrm{f}|}} \sum_{\chi \in \mathrm{Hom}(\mathbf{A}_S^*, H)} \frac{f_\Lambda(\chi)}{\Phi(\chi)^s} \sum_{x \in \mathcal{O}_S^* \otimes H^\wedge} \langle \chi, x\rangle.$$

As $\mathbf{A}_S^*$ and $\mathbf{A}_S^*/\mathcal{O}_S^*$ are locally compact groups and their subgroups of nth powers are closed, an application of [21, Lem. 3.2] gives canonical isomorphisms of abelian groups $\mathrm{Hom}(\mathbf{A}_S^*, H) \cong (\mathbf{A}_S^* \otimes H^\wedge)^\wedge$ and $\mathrm{Hom}(\mathbf{A}_S^*/\mathcal{O}_S^*, H) \cong (\mathbf{A}_S^*/\mathcal{O}_S^* \otimes H^\wedge)^\wedge$. Therefore, we can view an element $\chi \in \mathrm{Hom}(\mathbf{A}_S^*, H)$ as a character of $\mathbf{A}_S^* \otimes H^\wedge$. It is easily seen that χ induces the trivial character on $\mathcal{O}_S^* \otimes H^\wedge$ if and only if $\chi \in \mathrm{Hom}(\mathbf{A}_S^*/\mathcal{O}_S^*, H)$. Thus, we may apply character orthogonality to find that

$$\sum_{x \in \mathcal{O}_S^* \otimes H^\wedge} \langle \chi, x\rangle = \begin{cases} |\mathcal{O}_S^* \otimes H^\wedge|, & \text{if } \chi \in \mathrm{Hom}(\mathbf{A}_S^*/\mathcal{O}_S^*, H), \\ 0, & \text{otherwise.}\end{cases}$$

We therefore obtain

$$\sum_{x \in \mathcal{O}_S^* \otimes H^\wedge} \widehat{f}_{\Lambda,H}(x; s) = \frac{|\mathcal{O}_S^* \otimes H^\wedge|}{|H|^{|S_\mathrm{f}|}} \sum_{\chi \in \mathrm{Hom}(\mathbf{A}_S^*/\mathcal{O}_S^*, H)} \frac{f_\Lambda(\chi)}{\Phi(\chi)^s}.$$

Dirichlet's S-unit theorem gives a (non-canonical) isomorphism $\mathcal{O}_S^* \cong \mathcal{O}_k^* \times \mathbb{Z}^{S_{\mathrm{f}}}$, whereby

$$\frac{|\mathcal{O}_S^* \otimes H^\wedge|}{|H|^{|S_{\mathrm{f}}|}} = |\mathcal{O}_k^* \otimes H|.$$

Moreover, as $\mathcal{O}_S$ has trivial class group, the natural map $\mathbf{A}_S^*/\mathcal{O}_S^* \to \mathbf{A}^*/k^*$ is an isomorphism [51, Lem. 2.8]. The result now easily follows. □

3.5. **Analytic continuation of the Fourier transforms.** We now use the Poisson formula to study the analytic behaviour of the Dirichlet series under consideration. To do so, we shall calculate explicitly the local Fourier transforms for $v \notin S$. Fix some subgroup H of G. By a slight abuse of notation, for $x_v \in k_v^* \otimes H^\wedge$ we write $x_v \in \mathcal{A}_v \otimes H^\wedge$ to express that x_v is in the image of the (not necessarily injective) map $\mathcal{A}_v \otimes H^\wedge \to k_v^* \otimes H^\wedge$.

Lemma 3.10. *Let $v \notin S$ and let $x_v \in \mathcal{O}_v^* \otimes H^\wedge$. Then*

$$\widehat{f}_{\Lambda_v,H}(x_v;s) = \begin{cases} 1 + (|\operatorname{Hom}(\mathbb{F}_v^*/(\mathcal{A} \bmod v), H)| - 1)q_v^{-s}, & \text{if } x_v \in \mathcal{A}_v \otimes H^\wedge, \\ 1 - q_v^{-s}, & \text{if } x_v \notin \mathcal{A}_v \otimes H^\wedge. \end{cases}$$

Proof. An element $\chi_v \in \operatorname{Hom}(\mathcal{O}_v^*, H)$ is unramified if and only if it is trivial. Furthermore, since $v \notin S$ and our assumptions on S in §3.2, the ramification is tame and hence for non-trivial characters $\chi_v \in \operatorname{Hom}(\mathcal{O}_v^*, H)$, we have $\Phi_v(\chi_v) = q_v$. Therefore, by Lemmas 3.5 and 3.8 we have

$$\begin{aligned} \widehat{f}_{\Lambda_v,H}(x_v;s) &= \sum_{\chi_v \in \operatorname{Hom}(\mathcal{O}_v^*,H)} \frac{f_{\Lambda_v}(\chi_v)\langle \chi_v, x_v\rangle}{\Phi_v(\chi_v)^s} \\ &= 1 + \sum_{\substack{\chi_v \in \operatorname{Hom}(\mathcal{O}_v^*,H) \\ \chi_v \neq \mathbb{1}}} \frac{f_{\Lambda_v}(\chi_v)\langle \chi_v, x_v\rangle}{q_v^s} \\ &= 1 + q_v^{-s} \sum_{\substack{\chi_v \in \operatorname{Hom}(\mathcal{O}_v^*,H) \\ \chi_v \neq \mathbb{1} \\ \mathcal{A}_v \subset \operatorname{Ker}\chi_v}} \langle \chi_v, x_v\rangle \\ &= 1 - q_v^{-s} + q_v^{-s} \sum_{\substack{\chi_v \in \operatorname{Hom}(\mathcal{O}_v^*,H) \\ \mathcal{A}_v \subset \operatorname{Ker}\chi_v}} \langle \chi_v, x_v\rangle. \end{aligned} \tag{3.11}$$

We claim that the natural map

$$\operatorname{Hom}(\mathbb{F}_v^*/(\mathcal{A} \bmod v), H) \to \{\chi_v \in \operatorname{Hom}(\mathcal{O}_v^*, H) : \mathcal{A}_v \subset \operatorname{Ker}\chi_v\} \tag{3.12}$$

is an isomorphism. To see this, recall that Hensel's lemma yields a split short exact sequence

$$1 \to 1 + \mathfrak{p}_v \to \mathcal{O}_v^* \to \mathbb{F}_v^* \to 1,$$

where $\mathfrak{p}_v$ denotes the maximal ideal of $\mathcal{O}_v$. Applying $\operatorname{Hom}(\cdot, H)$, we obtain

$$1 \to \operatorname{Hom}(\mathbb{F}_v^*, H) \to \operatorname{Hom}(\mathcal{O}_v^*, H) \to \operatorname{Hom}(1 + \mathfrak{p}_v, H) \to 1.$$

The kernel of a continuous homomorphism $1 + \mathfrak{p}_v \to H$ contains $1 + \mathfrak{p}_v^n$ for some $n \in \mathbb{N}$, and the successive quotients in the filtration $1 + \mathfrak{p}_v \supset 1 + \mathfrak{p}_v^2 \supset \cdots \supset 1 + \mathfrak{p}_v^n$ each have order $|\mathcal{O}_v/\mathfrak{p}_v| = q_v$ (see [41, Prop. IV.2.6]). Consequently, the quotient $(1 + \mathfrak{p}_v)/(1 + \mathfrak{p}_v^n)$ has order a power of q_v. Now recall that we assumed in §3.2

that $\gcd(q_v, H) = 1$. Therefore, any continuous homomorphism $1 + \mathfrak{p}_v \to H$ is trivial. It follows that $\mathrm{Hom}(\mathbb{F}_v^*, H) = \mathrm{Hom}(\mathcal{O}_v^*, H)$.

Moreover, $\mathcal{A} \bmod v$ lies in the kernel of a homomorphism $\mathbb{F}_v^* \to H$ if and only if $\mathcal{A}_v$ lies in the kernel of the induced homomorphism $\mathcal{O}_v^* \to H$; whence (3.12) is an isomorphism as claimed.

Orthogonality of characters now gives

$$\sum_{\substack{\chi_v \in \mathrm{Hom}(\mathcal{O}_v^*, H) \\ \mathcal{A} \subset \mathrm{Ker}\, \chi_v}} \langle \chi_v, x_v \rangle = \begin{cases} |\,\mathrm{Hom}(\mathbb{F}_v^*/(\mathcal{A} \bmod v), H)|, & \text{if } x_v \in \mathcal{A}_v \otimes H^\wedge, \\ 0, & \text{otherwise.} \end{cases}$$

Inputting this into (3.11), the result follows. □

To study the analytic behaviour of the global Fourier transforms $\widehat{f}_{\Lambda,H}(x; s)$, we use the theory of frobenian functions from §2.

Lemma 3.11. *Let e be the exponent of H. Consider a function $d_{\mathcal{A},H} : \Omega_k \to \mathbb{C}$ which for all $v \notin S$ satisfies*

$$d_{\mathcal{A},H}(v) = \max\{d \in \mathbb{Z} : d \text{ divides } \gcd(e, q_v - 1) \text{ and } \mathcal{A} \bmod v \subset \mathbb{F}_v^{*d}\}.$$

Then

(1) $d_{\mathcal{A},H}$ is S-frobenian, and
(2) for $v \notin S$, we have $|\,\mathrm{Hom}(\mathbb{F}_v^*/(\mathcal{A} \bmod v), H)| = |H[d_{\mathcal{A},H}(v)]|$.

Proof. (1) For every $d \mid e$, consider the number field $k_d = k(\zeta_d, \sqrt[d]{\mathcal{A}})$. The subset

$$\Sigma_d = \mathrm{Gal}(k_e/k_d) \smallsetminus \bigcup_{\substack{d' \mid \frac{e}{d} \\ d' \neq 1}} \mathrm{Gal}(k_e/k_{dd'}) \subset \mathrm{Gal}(k_e/k)$$

is a union of conjugacy classes, since each $\mathrm{Gal}(k_e/k_d)$ is normal in $\mathrm{Gal}(k_e/k)$. The sets Σ_d for $d \mid e$ form a partition of $\mathrm{Gal}(k_e/k)$. Let $\varphi : \mathrm{Gal}(k_e/k) \to \mathbb{C}$ be the class function that takes the constant value d on Σ_d, for all $d \mid e$. We claim that $d_{\mathcal{A},H}(v) = \varphi(\mathrm{Frob}_v)$ for all $v \notin S$, so in particular it is S-frobenian.

Note that $\mathrm{Frob}_v \in \Sigma_d$ if and only if d is the largest divisor of e such that v splits completely in k_d/k. Equivalently, d is the largest divisor of e such that $d \mid q_v - 1$ and $x^d - \alpha$ has a root in k_v for all $\alpha \in \mathcal{A}$. By Hensel's lemma, this is equivalent to $d = d_{\mathcal{A},H}(v)$, and thus $\varphi(\mathrm{Frob}_v) = d_{\mathcal{A},H}(v)$, as desired.

(2) Let m be the largest divisor of $q_v - 1$ such that $\mathcal{A} \bmod v \subset \mathbb{F}_v^{*m}$. Then $\mathcal{A} \bmod v = \mathbb{F}_v^{*m}$, and thus $\mathbb{F}_v^*/(\mathcal{A} \bmod v) \cong \mathbb{Z}/m\mathbb{Z}$. Hence

$$\begin{aligned} |\,\mathrm{Hom}(\mathbb{F}_v^*/(\mathcal{A} \bmod v), H)| &= |\,\mathrm{Hom}(\mathbb{Z}/m\mathbb{Z}, H)| = |\,\mathrm{Hom}(\mathbb{Z}, H[m])| \\ &= |H[m]| = |H[\gcd(m, e)]| = |H[d_{\mathcal{A},H}(v)]|. \end{aligned}$$ □

Lemma 3.12. *Let $x \in \mathcal{O}_S^* \otimes H^\wedge$. Then the set*

$$\{v \in \Omega_k : x_v \in \mathcal{A}_v \otimes H^\wedge\}$$

is S-frobenian. In the special case $H^\wedge = \mathbb{Z}/e\mathbb{Z}$, on identifying $k^* \otimes H^\wedge$ with k^*/k^{*e}, this set equals

$$\left\{ v \in \Omega_k : \text{the polynomial } \prod_{\alpha \in \mathcal{A}/\mathcal{A}^e} (t^e - x\alpha) \text{ has a root in } k_v \right\}. \tag{3.13}$$

Note that the group $\mathcal{A}/\mathcal{A}^e$ is finite. Moreover, our slight abuse of notation is harmless, as whether or not the polynomial appearing in (3.13) has a root is independent of the choice of representative of each element of $\mathcal{A}/\mathcal{A}^e$.

Proof. To prove this we choose a presentation of $H^\wedge$. We then work coordinatewise on $H^\wedge$, using the fact that the intersection of finitely many frobenian sets is frobenian. Thus, we reduce to the case $H^\wedge = \mathbb{Z}/e\mathbb{Z}$. Here we have $\mathcal{O}_S^* \otimes H^\wedge = \mathcal{O}_S^*/\mathcal{O}_S^{*e}$. For $x \in \mathcal{O}_S^*$, we have to show that the set

$$\{v \in \Omega_k : x_v \in \mathcal{A}_v k_v^{*e}\}$$

is S-frobenian. However, we have $x_v \in \mathcal{A}_v k_v^{*e}$ if and only if $x_v \alpha_v \in k_v^{*e}$ for some $\alpha_v \in \mathcal{A}_v$ (depending on v). We find that the set in question is the set of places v such that the equation

$$\prod_{\alpha \in \mathcal{A}/\mathcal{A}^e} (t^e - x\alpha) = 0$$

has a solution in k_v; this set is frobenian (see Example 2.2). As x is an S-unit, it is easily seen that this is S-frobenian for our choice of S in §3.2. □

Corollary 3.13. *Let $x \in \mathcal{O}_S^* \otimes H^\wedge$. Then the function*

$$v \mapsto \begin{cases} |\operatorname{Hom}(\mathbb{F}_v^*/(\mathcal{A} \bmod v), H)| - 1, & \text{if } x_v \in \mathcal{A}_v \otimes H^\wedge, \\ -1, & \text{if } x_v \notin \mathcal{A}_v \otimes H^\wedge, \end{cases}$$

is S-frobenian.

Proof. The product or sum of two S-frobenian functions is clearly S-frobenian (in Definition 2.1 one takes the compositum of the relevant field extensions). Moreover, the complement of a S-frobenian set is S-frobenian. The result therefore follows from Lemmas 3.11 and 3.12. □

Definition 3.14. We denote by $\varpi(k, H, \mathcal{A}, x)$ the mean of the S-frobenian function described in Corollary 3.13.

We now compare $\varpi(k, H, \mathcal{A}, x)$ with $\varpi(k, H, \mathcal{A})$, as defined in Definition 1.3.

Lemma 3.15. *We have $\varpi(k, H, \mathcal{A}, x) \leq \varpi(k, H, \mathcal{A})$ for all $x \in \mathcal{O}_S^* \otimes H^\wedge$. Moreover, $\varpi(k, H, \mathcal{A}, 1) = \varpi(k, H, \mathcal{A})$.*

Proof. As clearly $\varpi(k, H, \mathcal{A}, x) \leq \varpi(k, H, \mathcal{A}, 1)$, the first assertion follows immediately from the second. So let us prove the second assertion. By Corollary 3.13 and Lemma 3.11, we see that $\varpi(k, H, \mathcal{A}, 1)$ is the mean of an S-frobenian function ρ with $\rho(v) = |\operatorname{Hom}(\mathbb{F}_v^*/(\mathcal{A} \bmod v), H)| - 1 = |H[d_{\mathcal{A},H}(v)]| - 1$ for all $v \notin S$. With the notation of the proof of Lemma 3.11, the corresponding class function on $\operatorname{Gal}(k_e/k)$ is given by $\sigma \mapsto |H[\varphi(\sigma)]| - 1$. Hence,

$$\varpi(k, H, \mathcal{A}, 1) = \frac{1}{[k_e : k]} \sum_{\sigma \in \operatorname{Gal}(k_e/k)} (|H[\varphi(\sigma)]| - 1) = \frac{1}{[k_e : k]} \sum_{d|e} (|H[d]| - 1)|\Sigma_d|.$$

By inclusion-exclusion, we get $|\Sigma_d| = \sum_{c|\frac{e}{d}} \mu(c)\,|\operatorname{Gal}(k_e/k_{cd})|$, and thus

$$\begin{aligned}\varpi(k,H,\mathcal{A},1) &= \sum_{d|e}(|H[d]|-1)\sum_{c|\frac{e}{d}}\frac{\mu(c)}{[k_{cd}:k]} = \sum_{f|e}\frac{1}{[k_f:k]}\sum_{d|f}(|H[d]|-1)\mu(f/d)\\ &= -1+\sum_{f|e}\frac{1}{[k_f:k]}\sum_{d|f}|H[d]|\mu(f/d)\\ &= -1+\sum_{f|e}\frac{\#\{g\in H:|g|=f\}}{[k_f:k]} = \varpi(k,H,\mathcal{A}).\end{aligned}$$

□

Recall that $\zeta_{k,v}(s)$ is the Euler factor of $\zeta_k(s)$ at a non-archimedean place v. If v is archimedean, then we let $\zeta_{k,v}(s)=1$.

Proposition 3.16. *Let $x\in\mathcal{O}_S^*\otimes H^\wedge$. Then the Fourier transform satisfies*

$$\widehat{f}_{\Lambda,H}(x;s) = \zeta_k(s)^{\varpi(k,H,\mathcal{A},x)}G(x;s),\quad \operatorname{Re}s>1,$$

where $G(x;s)$ is holomorphic in the region (2.3)*, for some $c>0$, and satisfies* (2.4)*. Moreover, we have*

$$\lim_{s\to1}(s-1)^{\varpi(k,H,\mathcal{A},x)}\widehat{f}_{\Lambda,H}(x;s) = (\operatorname{Res}_{s=1}\zeta_k(s))^{\varpi(k,H,\mathcal{A},x)}\prod_{v\in\Omega_k}\frac{\widehat{f}_{\Lambda_v,H}(x_v;1)}{\zeta_{k,v}(1)^{\varpi(k,H,\mathcal{A},x)}}.$$

In the case $x=1$, this limit is non-zero.

Proof. We consider the Euler product expansion of $\widehat{f}_{\Lambda,H}(x;s)$ from (3.5), where the Euler factors at $v\notin S$ were determined in Lemma 3.10. By Corollary 3.13 and our assumptions on S, we may apply Proposition 2.3 to obtain

$$F(s) := \prod_{v\notin S}\widehat{f}_{\Lambda_v,H}(x_v;s) = \zeta_k(s)^{\varpi(k,H,\mathcal{A},x)}\mathcal{H}(x;s),$$

with a function $\mathcal{H}(x;s)$ that is holomorphic in a region (2.3) and satisfies the bound (2.4). By Lemma 3.6, we may multiply $\mathcal{H}(x;s)$ by the Euler factors $\widehat{f}_{\Lambda_v,H}(x_v;s)$ for $v\in S$ while still preserving these properties (possibly for a smaller $c>0$ in (2.3)). Finally, the explicit form of the limit follows from (2.5) which, together with Lemma 3.6, also shows that the limit is non-zero if $x=1$. □

3.6. **The asymptotic formula in Theorem 3.1.** We now bring all our tools together to prove the first part of Theorem 3.1. Recall from Lemma 3.4 that we performed a Möbius inversion to obtain a sum over the subgroups H of G. Moreover, in Proposition 3.9 we used Poisson summation to understand the inner sums from Lemma 3.4. In summary,

$$F_\Lambda(s) = \sum_{H\subset G}\frac{\mu(G/H)}{|\mathcal{O}_k^*\otimes H^\wedge|}\sum_{x\in\mathcal{O}_S^*\otimes H^\wedge}\widehat{f}_{\Lambda,H}(x;s),\quad \operatorname{Re}s>1, \tag{3.14}$$

where F_Λ is the Dirichlet series from (3.2). Furthermore, we described the analytic properties of the Fourier transforms $\widehat{f}_{\Lambda,H}(x;s)$ in Proposition 3.16.

By Lemma 3.10, we can expand each of the Euler products $\widehat{f}_{\Lambda,H}(x;s)$ as a Dirichlet series

$$\widehat{f}_{\Lambda,H}(x;s) = \sum_{n\in\mathbb{Z}_{\geq1}}\frac{a_n(H,x)}{n^s}, \tag{3.15}$$

with coefficients $a_n(H,x) \in \mathbb{C}$.

Lemma 3.17. *Let $H \subset G$ be a subgroup, let $x \in \mathcal{O}_S^* \otimes H^\wedge$, and let $a_n(H,x)$ be the Dirichlet coefficient from* (3.15)*. Then*

$$\sum_{n \le B} a_n(H,x) = c_{H,x} B (\log B)^{\varpi(k,H,\mathcal{A},x)-1} + O(B(\log B)^{\varpi(k,H,\mathcal{A},x)-2}),$$

where

$$c_{H,x} = \frac{1}{\Gamma(\varpi(k,H,\mathcal{A},x))} \lim_{s\to 1} (s-1)^{\varpi(k,H,\mathcal{A},x)} \widehat{f}_{\Lambda,H}(x;s).$$

Proof. Let start by recalling that for every $\delta > 0$ there is a value of $c = c(\delta) > 0$ such that $|\zeta_k(s)/\zeta(s)| \ll_\delta (|\operatorname{Im} s| + 3)^\delta$ for all s in the region (2.3). Indeed, in the case $\operatorname{Re}(s) \ge 2$ a stronger bound follows directly from the fact that the Euler product of $\zeta_k(s)/\zeta(s)$ converges absolutely. In the compact region defined by $|\operatorname{Im}(s)| \le 2$ and $1 - c/\log(|\operatorname{Im} s| + 3) \le \operatorname{Re} s \le 2$ for some small enough c, the function $\zeta_k(s)/\zeta(s)$ is holomorphic and thus bounded. It remains to consider the case $|\operatorname{Im} s| \ge 2$, where we stay away from the poles at $s = 1$. It is well known that $\zeta(s) \ne 0$ and $|1/\zeta(s)| \ll \log|\operatorname{Im} s|$ for small enough c (e.g. [48, (3.11.8)]). Sufficient upper bounds for $|\zeta_k(s)|$ follow from standard convexity bounds (e.g. [29, Theorem 5.30]).

Write $\varpi = \varpi(k,H,\mathcal{A},x)$. Let $G(x;s)$ be as in Proposition 3.16, and let the constant c be small enough to ensure that $\zeta(s) \ne 0$, $\zeta_k(s) \ne 0$, and $|\zeta_k(s)/\zeta(s)|^\varpi \ll (|\operatorname{Im} s|+3)^{1/4}$ for all s in the region (2.3). Then the function $h(s) := \zeta_k(s)^\varpi/\zeta(s)^\varpi$, defined on $\operatorname{Re} s > 1$ via the binomial series applied to the Euler factors, has an analytic continuation to the region (2.3). Hence, the function $H(x;s) = h(s)G(x;s)$ is holomorphic and satisfies $H(x;s) \ll (|\operatorname{Im} s| + 3)^{3/4}$ in the region (2.3). Since $\widehat{f}_{\Lambda,H}(x;s) = \zeta(s)^\varpi H(x;s)$, we may apply the Selberg–Delange method in the form of [47, Thm. II.5.2] (with $N = 0$) to obtain the required asymptotic. (For the sequence $(b_n)_n$ required in [47, Thm. II.5.2], we take the coefficients $a_n(H,1)$. One can observe directly from the definition of the Euler factors $\widehat{f}_{\Lambda_v,H}(x_v;s)$ that these coefficients satisfy $a_n(H,1) \ge |a_n(H,x)|$.) □

Let us note that the leading term will come from $H = G$.

Lemma 3.18. *Let $H \subset G$ be a proper subgroup. Then $\varpi(k,H,\mathcal{A}) < \varpi(k,G,\mathcal{A})$.*

Proof. Follows immediately from Definition 1.3. □

We are now finally in the position to prove the required asymptotic formula.

Proposition 3.19. *Write $\varpi = \varpi(k,G,\mathcal{A})$. There exists $\delta = \delta(k,G,\mathcal{A}) > 0$ such that*

$$N(k,G,\Lambda,B) = c_{k,G,\Lambda} B (\log B)^{\varpi-1} + O(B(\log B)^{\varpi-1-\delta}),$$

where

$$c_{k,G,\Lambda} = \frac{1}{\Gamma(\varpi)|\mathcal{O}_k^* \otimes G|} \sum_{\substack{x \in \mathcal{O}_S^* \otimes G^\wedge \\ \varpi(k,G,\mathcal{A},x) = \varpi}} \lim_{s\to 1} (s-1)^\varpi \widehat{f}_{\Lambda,G}(x;s).$$

Proof. By (3.14) and (3.15), the Dirichlet coefficients f_n of $F_\Lambda(s)$ satisfy

$$f_n = \sum_{H \subset G} \frac{\mu(G/H)}{|\mathcal{O}_k^* \otimes H^\wedge|} \sum_{x \in \mathcal{O}_S^* \otimes H^\wedge} a_n(H, x).$$

Since $N(k, G, \Lambda, B) = \sum_{n \leq B} f_n$, the proposition now follows from Lemmas 3.15, 3.17, and 3.18. □

This proves the asymptotic formula in Theorem 3.1. Next, we study the leading constant.

3.7. **Formula for the leading constant.** To calculate the leading constant, we first need to understand exactly which elements of $\mathcal{O}_S^* \otimes H^\wedge$ give rise to the leading singularity in the Poisson sum (Proposition 3.9).

Lemma 3.20. *Let*

$$\mathcal{X}(k, G, \mathcal{A}) = \{x \in k^* \otimes G^\wedge : x_v \in \mathcal{A}_v \otimes G^\wedge \text{ for all but finitely many } v\}.$$

Then $\mathcal{X}(k, G, \mathcal{A})$ *is finite and*

$$\mathcal{X}(k, G, \mathcal{A}) = \{x \in \mathcal{O}_S^* \otimes G^\wedge : x_v \in \mathcal{A}_v \otimes G^\wedge \text{ for all } v \notin S\}.$$

Proof. It is enough to prove the result for $G^\wedge$ a cyclic group of prime power order. Henceforth, let $G^\wedge = \mathbb{Z}/q\mathbb{Z}$, where $q = p^r$ is a prime power. We view $\mathcal{X}(k, G, \mathcal{A})$ as a subgroup of k^*/k^{*q}.

First, we claim that the image of $\mathcal{X}(k, G, \mathcal{A})$ in $k(\mu_q)^*/k(\mu_q)^{*q}$ is equal to the image of $\mathcal{A}$. One containment is clear, as $\mathcal{A} \otimes G^\wedge \subset \mathcal{X}(k, G, \mathcal{A})$. For the other, let $K = k(\mu_q, \sqrt[q]{\mathcal{A}})$, so $K = k_q$ in the notation of Definition 1.3. Let K_v be the completion of k at a choice of place of K above v. The image of $\mathcal{X}(k, G, \mathcal{A})$ in $k(\mu_q)^*/k(\mu_q)^{*q}$ is contained in the following set:

$$\{x \in k(\mu_q)^*/k(\mu_q)^{*q} : x_v \in K_v^{*q} \text{ for all but finitely many } v\}.$$

As $\mu_q \subset K$, an application of the Chebotarev density theorem shows that this set equals $(k(\mu_q)^* \cap K^{*q})/k(\mu_q)^{*q}$ (this also follows from Lemma 4.9). On the other hand, Kummer theory shows that $(k(\mu_q)^* \cap K^{*q})/k(\mu_q)^{*q}$ is equal to the image of $\mathcal{A}$ in $k(\mu_q)^*/k(\mu_q)^{*q}$, and the claim is proved. In particular, the image $\mathcal{X}(k, G, \mathcal{A})$ in $k(\mu_q)^*/k(\mu_q)^{*q}$ is finite, as $\mathcal{A}$ is finitely generated.

Next, the map $k^*/k^{*q} \to k(\mu_q)^*/k(\mu_q)^{*q}$ is none other than the restriction map $\mathrm{H}^1(k, \mu_q) \to \mathrm{H}^1(k(\mu_q), \mu_q)$, which has kernel $\mathrm{H}^1(\mathrm{Gal}(k(\mu_q)/k), \mu_q)$. By [34, Prop. 9.1.6], we have $\mathrm{H}^1(\mathrm{Gal}(k(\mu_q)/k), \mu_q) = 0$ unless we are in the special case where $p = 2$, $r \geq 2$ and $\mathbb{Q}(\mu_{2^r}) \cap k$ is real. In this special case, $\mathrm{H}^1(\mathrm{Gal}(k(\mu_{2^r})/k), \mu_{2^r}) \cong \mathbb{Z}/2\mathbb{Z}$. In particular, the kernel of the natural map $k^*/k^{*q} \to k(\mu_q)^*/k(\mu_q)^{*q}$ is finite, and hence the finiteness of $\mathcal{X}(k, G, \mathcal{A})$ follows from the finiteness of its image in $k(\mu_q)^*/k(\mu_q)^{*q}$.

We now show that $\mathcal{X}(k, G, \mathcal{A}) \subset \mathcal{O}_S^* \otimes G^\wedge$; the rest follows from the fact that our condition is S-frobenian (see Lemma 3.12). Let $x \in k^*$ be such that its image in k^*/k^{*q} is in $\mathcal{X}(k, G, \mathcal{A})$. By the argument above, the image of x in $k(\mu_q)^*/k(\mu_q)^{*q}$ is in $(k(\mu_q)^* \cap K^{*q})/k(\mu_q)^{*q}$. In particular, $x = y^q$ for some $y \in K^*$. By our assumptions in §3.2 that $\mathcal{A} \subset \mathcal{O}_S^*$ and that S includes all primes dividing $|G|$, the extension K/k is unramified at all $v \notin S$. Therefore, for all $v \notin S$, the valuation $\mathrm{ord}_v(x) = \mathrm{ord}_v(y^q)$ is divisible by q. Consequently, the

fractional ideal $x\mathcal{O}_S$ is the qth power of some fractional ideal I of $\mathcal{O}_S$. By our assumption in §3.2 that $\mathcal{O}_S$ has trivial class group, $I = z\mathcal{O}_S$ for some $z \in k^*$. Therefore, $x = uz^q$ for some $u \in \mathcal{O}_S^*$. This completes the proof. □

Lemma 3.21. *Let $x \in \mathcal{O}_S^* \otimes G^\wedge$. Then $\varpi(k, G, \mathcal{A}, x) = \varpi(k, G, \mathcal{A})$ if and only if $x \in \mathcal{X}(k, G, \mathcal{A})$.*

Moreover $\widehat{f}_{\Lambda_v,G}(x_v; 1) = \widehat{f}_{\Lambda_v,G}(1; 1)$ for $x \in \mathcal{X}(k, G, \mathcal{A})$ and $v \notin S$.

Proof. Let $x \in \mathcal{X}(k, G, \mathcal{A})$. The first part follows from the definition, S-frobeniality, Corollary 3.13, and Lemma 3.15 that $\varpi(k, G, \mathcal{A}, x) = \varpi(k, G, \mathcal{A})$. The equality of Fourier transforms follows from Lemma 3.10 and Lemma 3.20.

So assume that $x \notin \mathcal{X}(k, G, \mathcal{A})$. Let $v \notin S$ be such that $x_v \notin \mathcal{A}_v \otimes G^\wedge$. Then

$$-1 < |\operatorname{Hom}(\mathbb{F}_v^*/(\mathcal{A} \bmod v), G)| - 1$$

as this group always contains the trivial homomorphism. The result now follows from the fact that the function in Corollary 3.13 is S-frobenian. □

These lemmas show that the leading singularity comes from finitely many terms which are *independent* of S and our choice of local conditions for $v \in S$. This makes applications much easier when one is varying S (we require such applications for the proof of Theorem 1.9).

Theorem 3.22. *Retain the assumptions of Theorem 3.1 and the additional assumptions on the finite set of places S from §3.2. Let $\mathcal{X}(k, G, \mathcal{A})$ be as in Lemma 3.20 and let S_{f} be the set of non-archimedean places in S. Write $\varpi = \varpi(k, G, \mathcal{A})$. Then*

$$c_{k,G,\Lambda} = \frac{(\operatorname{Res}_{s=1}\zeta_k(s))^{\varpi}}{\Gamma(\varpi)|\mathcal{O}_k^* \otimes G||G|^{|S_{\mathrm{f}}|}} \prod_{v \notin S} \left(\sum_{\substack{\chi_v \in \operatorname{Hom}(\mathcal{O}_v^*, G) \\ \mathcal{A}_v \subset \operatorname{Ker}\chi_v}} \frac{1}{\Phi_v(\chi_v)} \right) \zeta_{k,v}(1)^{-\varpi}$$
$$\times \left(\sum_{\substack{\chi \in \operatorname{Hom}\left(\prod_{v \in S} k_v^*, G\right) \\ \chi_v \in \Lambda_v \forall v \in S}} \frac{1}{\prod_{v \in S} \Phi_v(\chi_v)\zeta_{k,v}(1)^{\varpi}} \sum_{x \in \mathcal{X}(k,G,\mathcal{A})} \prod_{v \in S} \langle \chi_v, x_v \rangle \right),$$

where the product over $v \notin S$ is non-zero.

Proof. From Proposition 3.16, Proposition 3.19, and Lemma 3.21, we get the leading constant

$$c_{k,G,\Lambda} = \frac{(\operatorname{Res}_{s=1}\zeta_k(s))^{\varpi}}{\Gamma(\varpi)|\mathcal{O}_k^* \otimes G|} \sum_{x \in \mathcal{X}(k,G,\mathcal{A})} \prod_v \frac{\widehat{f}_{\Lambda_v,G}(x_v; 1)}{\zeta_{k,v}(1)^{\varpi}}.$$

We have $\widehat{f}_{\Lambda_v,G}(x_v; 1) = \widehat{f}_{\Lambda_v,G}(1; 1)$ for $x \in \mathcal{X}(k, G, \mathcal{A})$ and $v \notin S$ by Lemma 3.21, and these factors are non-zero by Lemma 3.6. The explicit expressions for $v \notin S$ follow from Lemma 3.8. For $v \in S$, we simply apply directly the definition of the local Fourier transforms from §3.4.1 (see (3.6) for a formula in the non-archimedean case) and change the order of summation. □

Note that the expression for $c_{k,G,\Lambda}$ is independent of S, for any S which satisfies the assumptions of §3.2.

Remark 3.23. In the special case $\mathcal{A} = \{1\}$, our constant agrees with the constant which Wood obtains in [51, Thm. 3.1], up to the factor $(\mathrm{Res}_{s=1}\zeta_k(s))^{\varpi(k,G,\mathcal{A})}$. This factor is missing from Wood's paper: in the proof of [51, Thm. 3.1], she mistakenly uses the equality $\lim_{s\to 1}(s-1)\zeta_K(s) = 1$, which holds for $K = \mathbb{Q}$ but does not hold in general (the residue is given by the analytic class number formula). Thus the right-hand side of [51, Thm. 3.1] should contain an additional factor of $(\mathrm{Res}_{s=1}\zeta_K(s))^{w_{K,C}}$.

Remark 3.24. Let $\widehat{G} = \mathrm{Hom}(G^\wedge, \mathbb{G}_m)$ denote the Cartier dual of $G^\wedge$. Then $Ш(k, \widehat{G}) = \mathrm{Ker}(k^* \otimes G^\wedge \to \mathbf{A}^* \otimes G^\wedge)$. An examination of the proof of Lemma 3.20 gives the bounds

$$|Ш(k, \widehat{G}) \cdot (\mathcal{A} \otimes G^\wedge)| \leq |\mathcal{X}(k, G, \mathcal{A})| \leq |2G^\wedge/4G^\wedge||\mathcal{A} \otimes G^\wedge|.$$

The following examples show that either bound can be sharp.

For the lower bound, take $k = \mathbb{Q}$, $\mathcal{A} = \{1\}$ and $G^\wedge = \mathbb{Z}/4\mathbb{Z}$. Then $\mathcal{A} \otimes G^\wedge = 1$, $\mathcal{X}(k, G, \{1\}) = Ш(k, \widehat{G}) = 0$, and $|2G^\wedge/4G^\wedge| = 2$.

For the upper bound, take $k = \mathbb{Q}$, $\mathcal{A} = \{\pm 1\}$ and $G^\wedge = \mathbb{Z}/4\mathbb{Z}$. Then one checks that $\mathcal{X}(\mathbb{Q}, \mathbb{Z}/4\mathbb{Z}, \{\pm 1\}) = \langle \pm 1, \pm 4\rangle$, despite the fact that $Ш(\mathbb{Q}, \mu_4) = 0$.

An example where both bounds coincide is given by taking $\mathcal{A} = \{1\}$ and $G^\wedge = \mathbb{Z}/2\mathbb{Z}$. One easily sees that in this case $\mathcal{X}(k, G, \{1\})$ is trivial.

3.8. **Positivity of the leading constant.** To finish the proof of Theorem 3.1, we need to show that $c_{k,G,\Lambda} > 0$ if there exists some sub-G-extension which realises all the given local conditions. It suffices to consider the contributions from $v \in S$ to the explicit expression given in Theorem 3.22, as the factors at $v \notin S$ are clearly non-zero. By character orthogonality we have

$$\sum_{x \in \mathcal{X}(k,G,\mathcal{A})} \prod_{v \in S} \langle \chi_v, x_v \rangle = \begin{cases} |\mathcal{X}(k, G, \mathcal{A})| & \text{if } \prod_{v\in S} \chi_v \text{ is trivial on } \mathcal{X}(k, G, \mathcal{A}), \\ 0 & \text{otherwise.} \end{cases}$$

In particular, this sum is non-negative for all $\chi \in \mathrm{Hom}(\prod_{v\in S} k_v^*, G)$. Hence, it suffices to show the existence of some χ such that this sum is non-zero. However, we have assumed the existence of a sub-G-extension φ which realises all the local conditions. Let $\psi : \mathbf{A}^*/k^* \to G$ be the associated homomorphism coming from class field theory. Note that $\prod_v \langle \psi_v, x_v \rangle = 1$ for all $x \in k^* \otimes G^\wedge$, hence

$$\prod_{v \in S} \langle \psi_v, x_v \rangle = \prod_{v \notin S} \frac{1}{\langle \psi_v, x_v \rangle}.$$

It therefore suffices to show that

$$\langle \psi_v, x_v \rangle = 1 \quad \text{for all } v \notin S \text{ and all } x \in \mathcal{X}(k, G, \mathcal{A}). \tag{3.16}$$

However, for $x \in \mathcal{X}(k, G, \mathcal{A})$ we have $x_v \in \mathcal{A}_v \otimes G^\wedge$ for all $v \notin S$, by Lemma 3.20. Moreover, by assumption every element of $\mathcal{A}$ is a local norm from K_φ for all $v \notin S$, thus $\mathcal{A}_v \subset \mathrm{Ker}\,\psi_v$ for all $v \notin S$ by Lemma 3.5. The claim (3.16) follows, which completes the proof of Theorem 3.1. □

4. Proof of results

We now apply Theorem 3.1 in various ways to prove the results from the introduction.

4.1. **Asymptotic formula for everywhere local norms.** We first derive an asymptotic formula for $N_{\mathrm{loc}}(k, G, \mathcal{A}, B)$ (see (1.1)) using Theorem 3.1.

Theorem 4.1. *We have*

$$N_{\mathrm{loc}}(k, G, \mathcal{A}, B) = c_{k,G,\mathcal{A},\mathrm{loc}} B(\log B)^{\varpi(k,G,\mathcal{A})-1} + O(B(\log B)^{\varpi(k,G,\mathcal{A})-1-\delta})$$

as $B \to \infty$, for some $c_{k,G,\mathcal{A},\mathrm{loc}} > 0$ and some $\delta = \delta(k, G, \mathcal{A}) > 0$.

Proof. For all $v \in \Omega_k$, let Λ_v be the set of sub-G-extensions of k_v corresponding to those extensions L/k_v for which every element of $\mathcal{A}$ is a local norm from L/k_v. Thus, in this setting $\Lambda = (\Lambda_v)_{v\in\Omega_k}$ is determined by $\mathcal{A}$. We clearly have $N_{\mathrm{loc}}(k, G, \mathcal{A}, B) = N(k, G, \Lambda, B)$. It therefore suffices to show that the leading constant in Theorem 3.1 is positive. To do so, we need to exhibit some *sub-G-extension* of k for which every element of $\mathcal{A}$ is everywhere locally a norm. However, the trivial extension k/k is such an extension. □

4.2. **Proof of Theorem 1.9.** As cyclic extensions always satisfy the Hasse norm principle, we may assume that G is non-cyclic. We use the following criterion for failure of the Hasse norm principle in the abelian setting, which was originally pointed out to us by Melanie Matchett Wood. (We use the notation from §3.1.)

Proposition 4.2. *Let φ be a G-extension of k. Then φ fails the Hasse norm principle if and only if there exists a proper subgroup $\Upsilon \subset \wedge^2(G)$ that contains the image of the natural map*

$$\prod_v \wedge^2(\operatorname{Im}\varphi_v) \to \wedge^2(G).$$

Proof. Let K be the number field determined by φ. Recall that the failure of the Hasse norm principle is measured by the Tate–Shafarevich group

$$Ш(k, \mathrm{R}^1_{K/k}\mathbb{G}_{\mathrm{m}}) := \operatorname{Ker}\Big(\mathrm{H}^1(k, \mathrm{R}^1_{K/k}\mathbb{G}_{\mathrm{m}}) \to \prod_v \mathrm{H}^1(k_v, \mathrm{R}^1_{K/k}\mathbb{G}_{\mathrm{m}})\Big),$$

where $\mathrm{R}^1_{K/k}\mathbb{G}_{\mathrm{m}}$ denotes the associated norm 1 torus, see [36, §6.3]. This group is finite by [36, Prop. 6.9]. As K/k is Galois, a theorem of Tate [36, Thm. 6.11] (see also [38, Ex. 5.6]) implies that there is an exact sequence

$$0 \to \operatorname{Hom}(Ш(k, \mathrm{R}^1_{K/k}\mathbb{G}_{\mathrm{m}}), \mathbb{Q}/\mathbb{Z}) \to \mathrm{H}^3(G, \mathbb{Z}) \to \prod_v \mathrm{H}^3(\operatorname{Im}\varphi_v, \mathbb{Z}).$$

However, as G is abelian, we have a well-known canonical isomorphism

$$\mathrm{H}^3(G, \mathbb{Z}) \cong \operatorname{Hom}(\wedge^2(G), \mathbb{Q}/\mathbb{Z})$$

(see e.g. [21, Lem. 6.4]). Using this and applying $\operatorname{Hom}(\cdot, \mathbb{Q}/\mathbb{Z})$, we therefore obtain the exact sequence

$$\prod_v \wedge^2(\operatorname{Im}\varphi_v) \to \wedge^2(G) \to Ш(k, \mathrm{R}^1_{k_\varphi/k}\mathbb{G}_{\mathrm{m}}) \to 0. \tag{4.1}$$

Thus, failure of the Hasse norm principle is equivalent to the first map in (4.1) failing to be surjective. □

Therefore, to prove Theorem 1.9, it suffices to show the following.

Theorem 4.3. *Let $\Upsilon \subset \wedge^2(G)$ be a proper subgroup. Then*

$$\lim_{B\to\infty} \frac{\#\left\{\varphi \in G\text{-}ext(k) \,:\, \Phi(\varphi) \le B, \mathcal{A} \subset \mathrm{N}_{K_\varphi/k}\, \mathbf{A}^*_{K_\varphi}, \wedge^2(\operatorname{Im}\varphi_v) \subset \Upsilon\, \forall v\right\}}{N_{\mathrm{loc}}(k, G, \mathcal{A}, B)} = 0.$$

Note that in Theorem 4.3, and henceforth, we abuse notation by writing $\wedge^2(\operatorname{Im}\varphi_v) \subset \Upsilon$ to mean that the image of the natural map $\wedge^2(\operatorname{Im}\varphi_v) \to \wedge^2(G)$ is contained in Υ, despite the fact that this map is not injective in general.

We prove Theorem 4.3 via an application of Theorem 3.1. Note, however, that one cannot apply Theorem 3.1 directly, as the local conditions imposed at the infinitely many places will not be compatible with the assumptions of Theorem 3.1. We therefore apply Theorem 3.1 to a suitable finite set of places, which we then allow to increase.

4.2.1. *Proof of Theorem 4.3.* Let S_0 be a finite set of places of k satisfying the conditions of §3.2, which we consider as being fixed. Let T be a finite set of places of k which is disjoint from S_0. Eventually, we will consider what happens as T increases. Let $S = S_0 \cup T$.

We consider the local conditions Λ_v given by

$$\{\varphi_v \in \operatorname{Hom}(\operatorname{Gal}(\bar{k}_v/k_v), G) : \mathcal{A}_v \subset \mathrm{N}_{K_{\varphi_v}/k_v}(K^*_{\varphi_v})\},\ v \notin T;$$
$$\{\varphi_v \in \operatorname{Hom}(\operatorname{Gal}(\bar{k}_v/k_v), G) : \mathcal{A}_v \subset \mathrm{N}_{K_{\varphi_v}/k_v}(K^*_{\varphi_v}), \wedge^2(\operatorname{Im}\varphi_v) \subset \Upsilon\},\ v \in T.$$

We denote the collection of such conditions by Λ_T. Note that we clearly have

$$\frac{\#\left\{\varphi \in G\text{-ext}(k) \,:\, \begin{array}{c}\Phi(\varphi) \le B, \mathcal{A} \subset \mathrm{N}_{K_\varphi/k}\, \mathbf{A}^*_{K_\varphi},\\ \wedge^2(\operatorname{Im}\varphi_v) \subset \Upsilon\, \forall v\end{array}\right\}}{N_{\mathrm{loc}}(k, G, \mathcal{A}, B)} \le \frac{N(k, G, \Lambda_T, B)}{N_{\mathrm{loc}}(k, G, \mathcal{A}, B)}$$

for all B. Applying Theorem 3.1 gives

$$\lim_{B\to\infty} \frac{N(k, G, \Lambda_T, B)}{N_{\mathrm{loc}}(k, G, \mathcal{A}, B)} = \frac{c_{k,G,\Lambda_T}}{c_{k,G,\mathcal{A},\mathrm{loc}}}$$

where $c_{k,G,\mathcal{A},\mathrm{loc}} > 0$ by Theorem 4.1. To prove Theorem 4.3 it therefore suffices to show that

$$\lim_{S_0\cup T\to\Omega_k} \frac{c_{k,G,\Lambda_T}}{c_{k,G,\mathcal{A},\mathrm{loc}}} = 0 \tag{4.2}$$

where as explained we consider S_0 as fixed and T as increasing and disjoint from S_0. We do this using the explicit expression for the leading constant given in Theorem 3.22. We let e be the exponent of G. We require the following elementary observation.

Lemma 4.4. *Let $\alpha \in k^*$. If v is such that $\alpha \in k_v^{*e}$, then α is a local norm at v from every sub-G-extension of k.*

Proof. Let K be an extension of k with Galois group isomorphic to a subgroup of G and v a place of k such that $\alpha \in k_v^{*e}$. Let K_v be the completion of k at a choice of place of K above v. Then local class field theory yields

$$k_v^*/\,\mathrm{N}_{K_v/k_v}\, K_v^* \cong \operatorname{Gal}(K_v/k_v) \hookrightarrow G.$$

Now G has exponent e, whereby the group $k_v^*/\operatorname{N}_{K_v/k_v} K_v^*$ has exponent dividing e. It follows that an eth power in k_v^* is a local norm. $\square$

We now obtain the following bounds.

Lemma 4.5. *Let $k_e = k(\mu_e, \sqrt[e]{\mathcal{A}})$. Then*

$$\frac{c_{k,G,\Lambda_T}}{c_{k,G,\mathcal{A},\mathrm{loc}}} \leq \prod_{\substack{v\in T \\ v \text{ completely split in } k_e/k}} \frac{\sum_{\substack{\chi_v\in\mathrm{Hom}(k_v^*,G) \\ \wedge^2(\mathrm{Im}\,\chi_v)\subset\Upsilon}} \frac{1}{\Phi_v(\chi_v)}}{\sum_{\chi_v\in\mathrm{Hom}(k_v^*,G)} \frac{1}{\Phi_v(\chi_v)}}.$$

Proof. The factors in Theorem 3.22 cancel out in the quotient $c_{k,G,\Lambda_T}/c_{k,G,\mathcal{A},\mathrm{loc}}$, except those at places $v \in S$. By Lemma 3.20, we have

$$\mathcal{X}(k,G,\mathcal{A}) = \{x \in \mathcal{O}_{S_0}^* \otimes G^\wedge : x_v \in \mathcal{A}_v \otimes G^\wedge \text{ for all } v \notin S_0\}$$

(this statement holds for any set of places satisfying the assumptions of §3.2). Moreover, for $v \in T$ any element of $\mathcal{A}_v$ is a local norm at v by our choice of Λ_v; it follows that $\langle \chi_v, x_v\rangle = 1$ for $\chi_v \in \Lambda_v$ as in Theorem 3.22, hence

$$\sum_{x\in\mathcal{X}(k,G,\mathcal{A})} \prod_{v\in S} \langle \chi_v, x_v\rangle = \sum_{x\in\mathcal{X}(k,G,\mathcal{A})} \prod_{v\in S_0} \langle \chi_v, x_v\rangle.$$

Therefore, we can split off Euler factors for all $v \in T$ from the term involving S, while the remaining sum over $\mathrm{Hom}(\prod_{v\in S_0} k_v^*, G)$ is the same in c_{k,G,Λ_T} and $c_{k,G,\mathcal{A},\mathrm{loc}}$. We have obtained the equality

$$\frac{c_{k,G,\Lambda_T}}{c_{k,G,\mathcal{A},\mathrm{loc}}} = \prod_{v\in T} \frac{\sum_{\chi_v\in\Lambda_v} \frac{1}{\Phi_v(\chi_v)}}{\sum_{\substack{\chi_v\in\mathrm{Hom}(k_v^*,G) \\ \mathcal{A}_v\subset\mathrm{Ker}\,\chi_v}} \frac{1}{\Phi_v(\chi_v)}}.$$

The quotient of each local factor is at most 1, so to obtain an upper bound we may just consider those places $v \in T$ which are completely split in k_e/k. For such places every element of $\mathcal{A}$ is an eth power in k_v^*, hence the condition that they are local norms is automatic by Lemma 4.4. The result follows. $\square$

We will make use of the following fact from [21, Lem. 6.9]. Here, we use the term *bicyclic* for a non-cyclic group that is a direct sum of two cyclic groups.

Lemma 4.6. *Let G be a finite abelian non-cyclic group. Then there exists a finite collection of bicyclic subgroups $G_i \subset G$ for $i \in I$ such that the natural map*

$$\bigoplus_{i\in I} \wedge^2(G_i) \to \wedge^2(G)$$

is an isomorphism.

As $\Upsilon \subset \wedge^2(G)$ is a proper subgroup, there exists some i such that $\wedge^2(G_i) \not\subset \Upsilon$. Fix this i and write $G_i \cong \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$ where $n, m \mid e$. Let $v \in T$ be a place of k which is completely split in the extension $k(\mu_e, \sqrt[e]{\mathcal{A}})$. There exists a G_i-extension of k_v: simply adjoin an nth root of a uniformiser to the unique unramified extension of k_v of degree m. Thus, by local class field theory, there

exists $\chi_v \in \mathrm{Hom}(k_v^*, G)$ such that $\mathrm{Im}\,\chi_v = G_i$. In particular we have $\wedge^2(\mathrm{Im}\,\chi_v) \not\subset \Upsilon$. For such places v we find that

$$\begin{aligned}&\#\{\chi_v \in \mathrm{Hom}(k_v^*, G) : \wedge^2(\mathrm{Im}\,\chi_v) \subset \Upsilon, \chi_v \text{ ramified}\}\\ &< \#\{\chi_v \in \mathrm{Hom}(k_v^*, G) : \chi_v \text{ ramified}\}.\end{aligned}$$

Let $a_v = \#\{\chi_v \in \mathrm{Hom}(k_v^*, G) : \chi_v \text{ ramified}\}$. Recall that tamely ramified χ_v have conductor q_v and there are $|G|$ unramified G-characters. Using Lemma 4.5, it follows that

$$\begin{aligned}\frac{c_{k,G,\Lambda_T}}{c_{k,G,\mathcal{A},\mathrm{loc}}} &\leq \prod_{\substack{v\in T\\ v \text{ completely split in } k_e}} \frac{|G| + \frac{a_v-1}{q_v} + O\left(\frac{1}{q_v^2}\right)}{|G| + \frac{a_v}{q_v} + O\left(\frac{1}{q_v^2}\right)}\\ &= \prod_{\substack{v\in T\\ v \text{ completely split in } k_e}} \left(1 - \frac{1}{|G|q_v} + O\left(\frac{1}{q_v^2}\right)\right)\end{aligned}$$

However this diverges to 0 as $S_0 \cup T \to \Omega_k$ since

$$-\sum_{v \text{ completely split in } k_e} \frac{1}{q_v}$$

diverges by the Chebotarev density theorem. This proves (4.2) and completes the proof of Theorem 4.3, hence the proof of Theorem 1.9. □

Remark 4.7. Lemma 4.6 is the first part of the statement of [21, Lem. 6.9]. Unfortunately the second part of the statement [21, Lem. 6.9] is false (this claims that if the exponent of $\wedge^2(G)$ divides a prime p, then all the G_i may chosen isomorphic to $(\mathbb{Z}/p\mathbb{Z})^2$). A counterexample is given by the group $G = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$ and the subgroup $G_1 = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$; here the induced map

$$\mathbb{Z}/2\mathbb{Z} = \wedge^2(G_1) \to \wedge^2(G) = \mathbb{Z}/2\mathbb{Z}$$

is trivial. This mistake in [21, Lem. 6.9] has various consequences for [21] which will be addressed in a forthcoming corrigendum.

4.3. **Proof of Theorem 1.4.** Follows from Theorems 4.1 and 1.9. □

4.4. **Proof of Theorem 1.1.** Follows immediately from Theorem 1.4. □

4.5. **Proof of Theorem 1.6.** The implication (3)⇒(1) in Theorem 1.6 follows from Lemma 4.4, Theorem 3.1 and Theorem 1.9, as clearly $\varpi(k, G, \mathcal{A}) = \varpi(k, G, \{1\})$ in this case (we are only imposing finitely many local conditions). The implication (1)⇒(2) is clear from Definition 1.3 and Theorem 1.4. For the remaining implication (2)⇒(3), we note that (2) clearly implies that

$$\mathcal{A}_v \subset k_v^{*d} \text{ for all } d \mid e \text{ and all } v \nmid \infty \text{ with } q_v \equiv 1 \bmod d. \tag{4.3}$$

Moreover, we have the following elementary observation.

Lemma 4.8. *Let $e \in \mathbb{Z}_{\geq 1}$, let $\alpha \in k^*$, and let v be place of k such that $e, \alpha \in \mathcal{O}_v^*$. Let $d = \gcd(e, q_v - 1)$. If $\alpha \in k_v^{*d}$ then $\alpha \in k_v^{*e}$.*

Proof. As $\alpha \in k_v^{*d}$ and α is a unit, its image in the residue field lies in $\mathbb{F}_v^{*d}$. However, as $d = \gcd(e, q_v - 1)$, we have $\mathbb{F}_v^{*d} = \mathbb{F}_v^{*e}$. The result therefore follows from Hensel's lemma. □

Hence, the remaining implication (2)⇒(3) in Theorem 1.6 follows immediately from (4.3) and Lemma 4.8. □

4.6. **Proof of Corollary 1.7.** Let $\alpha \in \mathcal{A}$ and consider $\alpha\beta^e$ for some $\beta \in k^*$. By Lemma 4.4, we see that β^e is a norm everywhere locally from all G-extensions of k. It follows that $\alpha\beta^e$ is a norm everywhere locally from a given G-extension if and only if α is a norm everywhere locally. Part (i) now follows from Theorem 1.9 and Theorem 4.1. Part (ii) also follows from Lemma 4.4 and Theorem 1.9.

For (iii) and (iv), we use the ω-version of Tate–Shafarevich groups. Namely, for a finite abelian group scheme M over k we let

$$Ш_\omega(k, M) = \{c \in \mathrm{H}^1(k, M) : c_v = 0 \in \mathrm{H}^1(k_v, M) \text{ for all but finitely many } v\}.$$

By Kummer theory we have $\mathrm{H}^1(L, \mu_e) = L^*/L^{*e}$ for any field L of characteristic 0. Therefore Part (iii) of Theorem 1.6 is equivalent to

$$\mathcal{A}k^{*e} \subset Ш_\omega(k, \mu_e).$$

The key observation is now the following.

Lemma 4.9. *Let k be a number field, let $e \in \mathbb{Z}_{\geq 1}$ and let 2^r be the largest power of 2 dividing e. Then $Ш_\omega(k, \mu_e) = 0$, unless the extension $k(\mu_{2^r})/k$ is non-cyclic, where we have $Ш_\omega(k, \mu_e) \cong \mathbb{Z}/2\mathbb{Z}$.*

Proof. Follows immediately from [34, Thm. 9.1.11]. □

The remaining parts of Corollary 1.7 now follow from Lemma 4.9. □

Remark 4.10. Even though we have $N_{\mathrm{loc}}(k, G, \mathcal{A}, B) = N_{\mathrm{loc}}(k, G, \mathcal{A}\langle\beta^e\rangle, B)$ and $N_{\mathrm{glob}}(k, G, \mathcal{A}, B) \sim N_{\mathrm{glob}}(k, G, \mathcal{A}\langle\beta^e\rangle, B)$, we can still have $N_{\mathrm{glob}}(k, G, \mathcal{A}, B) \neq N_{\mathrm{glob}}(k, G, \mathcal{A}\langle\beta^e\rangle, B)$. For example, take $k = \mathbb{Q}, G = (\mathbb{Z}/2\mathbb{Z})^2, \mathcal{A} = \{1\}$, and $\beta = 5$ (see Example 1.11(4)).

4.7. **Proof of Theorem 1.8.** The implication (2) ⇒ (1) is self-evident. So suppose that $\lim_{B\to\infty} \frac{N_{\mathrm{glob}}(k,G,\mathcal{A},B)}{N(k,G,B)} > 0$. Then by Theorem 1.6 there exists a cofinite set of places $T \subset \Omega_k$ such that $\mathcal{A} \subset k_v^{*e}$ for all $v \in T$. By [34, Thm. 9.1.11],

$$\mathrm{Ker}\Big(k^*/k^{*e} \to \prod_{v\in T} k_v^*/k_v^{*e}\Big) = \mathrm{Ker}\Big(k^*/k^{*e} \to \prod_{v\in T\cup\{v\nmid 2\}} k_v^*/k_v^{*e}\Big)$$

so we may assume that T contains all $v \nmid 2$. Let $\mathfrak{p}$ be the unique prime of k lying above 2. Let $\chi : \mathrm{Gal}(\bar{k}/k) \to G$ be a G-extension and let $\alpha \in \mathcal{A}$. Then at all places $v \neq \mathfrak{p}$, the cyclic algebra (χ, α) over k has local invariant zero, because α is a local norm at v by Lemma 4.4. Now the Albert–Brauer–Hasse–Noether Theorem [34, Thm. 8.1.17] shows that (χ, α) has local invariant zero at $\mathfrak{p}$, meaning that α is also a local norm at $\mathfrak{p}$. Therefore, all elements of $\mathcal{A}$ are everywhere local norms from all G-extensions of k. But G is cyclic, hence every G-extension satisfies the Hasse norm principle; (2) now follows. □

4.8. **Variants of Theorems 1.1 and 1.4.** We finish with some variants of our results, which allow one to impose local conditions at finitely many places. Our first result is a variant of Theorem 1.4, and follows immediately from Theorem 3.1 and Theorem 1.9.

Corollary 4.11. *Retain the assumptions of Theorem 3.1. Assume further that every element of $\mathcal{A}$ is a local norm from every extension in Λ_v for all v, and that there exists a sub-G-extension of k which realises the given local conditions for all places v. Then*

$$\begin{aligned}&\#\{\varphi \in G\text{-}ext(k) : \Phi(\varphi) \leq B,\, \varphi_v \in \Lambda_v\, \forall v,\, \mathcal{A} \subset \mathrm{N}_{K_\varphi/k} K_\varphi^*\}\\ &= c_{k,G,\Lambda} B (\log B)^{\varpi(k,G,\mathcal{A})-1}(1+o(1)),\end{aligned}$$

for some leading constant $c_{k,G,\Lambda} > 0$.

From this we immediately obtain the following strengthening of Theorem 1.1.

Corollary 4.12. *Let k be a number field, S a finite set of places of k, G a finite abelian group, and $\mathcal{A} \subset k^*$ a finitely generated subgroup. Let ψ be a sub-G-extension of k such that every element of $\mathcal{A}$ is everywhere locally a norm from K_ψ. There exists a G-extension φ of k such that every element of $\mathcal{A}$ is a global norm from K_φ and such that $\varphi_v = \psi_v$ for all $v \in S$.*

Remark 4.13. Taking ψ to correspond to the trivial extension k/k, we find the existence of an extension K/k with Galois group G such that every element of $\mathcal{A}$ is a norm from K and such that K is completely split at all places of S.

Appendix A. An algebro-geometric point of view on Theorem 1.1

by Yonatan Harpaz and Olivier Wittenberg

We give, in this appendix, an algebro-geometric proof of Theorem 1.1, based on a combination of the descent and fibration methods in the formulation they are given in [25]. The main argument is described in §§A.1–A.3. In §A.4 we show that the refinement of Theorem 1.1 formulated in Corollary 4.12 can also be deduced in this manner by proving a certain verticality result on the Brauer groups of the varieties in question. This verticality uses in an essential way the fact that G is abelian. In §A.5 we show that when G is not abelian, the statement of Corollary 4.12 is *false*, by constructing a counterexample in the form of an explicit 2-group. Nonetheless, as we show in the upcoming work [26], Theorem 1.1 does hold for 2-groups (and more generally for nilpotent groups, even for supersolvable groups).

Let us fix, for the whole of §§A.1–A.4, a finite abelian group G, a field k of characteristic 0, a finite collection $\alpha_1, \ldots, \alpha_m \in k^*$ and an algebraic closure $\bar{k}$ of k. In §§A.1–A.3, we assume that k is a number field.

A.1. **Statements.** Let us choose an embedding $G \hookrightarrow \mathrm{SL}_n(k)$ for some $n \geq 1$. Let SL_n and $\mathbb{G}_\mathrm{m}$ implicitly denote the corresponding algebraic groups over k. For any $\alpha \in k^*$, let $T^\alpha \subset \prod_{g\in G} \mathbb{G}_\mathrm{m}$ denote the subvariety whose $\bar{k}$-points are the maps $t : G \to \bar{k}^*$ such that $\prod_{g\in G} t(g) = \alpha$. Thus T^α is a (trivial) torsor under the (trivial) torus T^1.

Let $Y = \mathrm{SL}_n \times T^{\alpha_1} \times \cdots \times T^{\alpha_m}$. Let G act on SL_n by right multiplication, on T^α (for any α) by the right action $(t \cdot \gamma)(\gamma') = t(\gamma\gamma')$, and on Y by the resulting diagonal right action. As G acts freely on SL_n, it acts freely on Y; hence, letting $X = Y/G$, the quotient map $\pi : Y \to X$ is a G-torsor.

The fibre of π above any rational point of X is a G-torsor over $\mathrm{Spec}(k)$, say $\mathrm{Spec}(K)$, where K is an étale k-algebra endowed with elements $\beta_1, \ldots, \beta_m \in K^*$ such that $N_{K/k}(\beta_i) = \alpha_i$ for all i. Namely β_i is the restriction to the fibre in question of the invertible function $(s, t_1, \ldots, t_m) \mapsto t_i(1)$ on Y, where 1 denotes the identity element of G. If the algebra K is a field, then K/k is Galois with group G, since it is a G-torsor. Thus, all we need to do, to show Theorem 1.1, is to prove that there exists $x \in X(k)$ such that $\pi^{-1}(x)$ is irreducible. Letting X' denote a smooth compactification of X (i.e. any smooth and proper variety containing X as a dense open subset), we shall in fact prove the following theorem.

Theorem A.1. *The set $X'(k)$ is dense in the Brauer–Manin set $X'(\mathbb{A}_k)^{\mathrm{Br}(X')}$.*

We note that $X'(\mathbb{A}_k)^{\mathrm{Br}(X')}$ is non-empty since so is $X(k)$; indeed, even $Y(k)$ is non-empty. The desired result now follows from Theorem A.1:

Corollary A.2. *The set of $x \in X(k)$ such that $\pi^{-1}(x)$ is irreducible is dense in the (non-empty) Brauer–Manin set $X'(\mathbb{A}_k)^{\mathrm{Br}(X')}$.*

Proof. This is essentially an application of a theorem of Ekedahl [18, Thm. 1.3] (also discussed and proved in [44, §§3.5–3.6]). What Ekedahl really shows in [18] is that for any finite étale morphism $\pi : Y \to X$ between geometrically irreducible varieties over k and for any finite set S of places of k, there exist a finite set S' of places of k, disjoint from S, and a collection $(x'_v)_{v \in S'} \in \prod_{v \in S'} X(k_v)$ such that for any $x \in X(k)$ close enough to $(x'_v)_{v \in S'}$ for the product topology on $\prod_{v \in S'} X(k_v)$, the scheme $\pi^{-1}(x)$ is irreducible. Theorem A.1 implies Corollary A.2 in view of this statement and of the remark that the Brauer–Manin set is open in $X'(\mathbb{A}_k)$ as X is geometrically unirational (see [50, Remarks 2.4 (i)–(ii)]). □

As we have seen, Corollary A.2 implies Theorem 1.1. In a less immediate way, it also implies Corollary 4.12. Indeed, noting that any sub-G-extension of k, in the terminology of §3.1, arises as the fibre of the quotient map $\mathrm{SL}_n \to \mathrm{SL}_n/G$ above a rational point of SL_n/G (see [42, Ch. I, §5.4, Cor. 1] and recall that $\mathrm{H}^1(k, \mathrm{SL}_n)$ is a singleton by Hilbert's Theorem 90), we see that Corollary 4.12 follows from combining Corollary A.2 with Proposition A.3 below.

Proposition A.3. *Let $B = \mathrm{SL}_n/G$ and $b \in B(k)$. Let $f : X \to B$ be the map induced by the first projection $Y \to \mathrm{SL}_n$. Let Ω denote the set of places of k. Let $(x_v)_{v \in \Omega} \in \prod_{v \in \Omega} X(k_v)$. If $f(x_v) = b$ for all $v \in \Omega$, then $(x_v)_{v \in \Omega} \in X'(\mathbb{A}_k)^{\mathrm{Br}(X')}$.*

We shall prove Theorem A.1 in §§A.2–A.3 and Proposition A.3 in §A.4.

A.2. **Descent.** To prove Theorem A.1, we first perform a descent, in the sense of Colliot-Thélène and Sansuc [14], to reduce ourselves to studying the arithmetic of hopefully simpler auxiliary varieties. If V is a variety over k, we denote by $\bar{k}[V]^*$ the group of global invertible functions on $V \otimes_k \bar{k}$.

Proposition A.4. *We have $\bar{k}[X]^* = \bar{k}^*$.*

Proof. We first remark that there is a canonical exact sequence of abelian groups

$$0 \to \bar{k}^* \to \bar{k}[Y]^* \to (\mathbb{Z}[G]/\mathbb{Z})^m \to 0 \tag{A.1}$$

whose arrows are equivariant with respect to the actions of $\mathrm{Gal}(\bar{k}/k)$ and of G; indeed, Rosenlicht's lemma (see [13, Lem. 10]) shows that

$$\bar{k}[Y]^*/\bar{k}^* = \bar{k}[\mathrm{SL}_n]^*/\bar{k}^* \oplus \bar{k}[T^{\alpha_1}]^*/\bar{k}^* \oplus \cdots \oplus \bar{k}[T^{\alpha_m}]^*/\bar{k}^*, \tag{A.2}$$

while it is well known that $\bar{k}[\mathrm{SL}_n]^* = \bar{k}^*$ and that $\bar{k}[T^\alpha]^*/\bar{k}^*$, for any $\alpha \in k^*$, is the character group of the torus under which T^α is a torsor. On the other hand, by the exact sequence

$$0 \to \mathbb{Z} \to \mathbb{Z}[G] \to \mathbb{Z}[G]/\mathbb{Z} \to 0 \tag{A.3}$$

and by the vanishing of $\mathrm{H}^1(G, \mathbb{Z})$, we have $\mathrm{H}^0(G, \mathbb{Z}[G]/\mathbb{Z}) = 0$. We can now deduce from (A.1) that $\bar{k}[X]^* = (\bar{k}[Y]^*)^G = \bar{k}^*$. □

Set $\widehat{G} = \mathrm{Hom}(G, \bar{k}^*)$. We recall that the *type* of the G-torsor $\pi : Y \to X$ is, by definition, the isomorphism class of $\pi \otimes_k \bar{k} : Y \otimes_k \bar{k} \to X \otimes_k \bar{k}$ as a G-torsor over $X \otimes_k \bar{k}$ and that it can be identified, thanks to Proposition A.4, with a homomorphism $\lambda : \widehat{G} \to \mathrm{Pic}(X \otimes_k \bar{k})$. (See [25, (3.3)], for this (standard) identification.) The homomorphism λ is injective as G is finite and Y is geometrically connected (see [46, p. 40, Exercise 2]).

Let us denote by $\nu : \widehat{T} \hookrightarrow \mathrm{Pic}(X' \otimes_k \bar{k})$ the inverse image of $\lambda : \widehat{G} \hookrightarrow \mathrm{Pic}(X \otimes_k \bar{k})$ by the restriction map $\mathrm{Pic}(X' \otimes_k \bar{k}) \to \mathrm{Pic}(X \otimes_k \bar{k})$. As in [25, (3.1)], we have a short exact sequence of $\mathrm{Gal}(\bar{k}/k)$-modules

$$0 \longrightarrow \widehat{Q} \longrightarrow \widehat{T} \longrightarrow \widehat{G} \longrightarrow 0, \tag{A.4}$$

where $\widehat{Q}$ is a permutation $\mathrm{Gal}(\bar{k}/k)$-module, and, dually, a short exact sequence

$$1 \longrightarrow G \longrightarrow T \longrightarrow Q \longrightarrow 1 \tag{A.5}$$

of commutative algebraic groups over k, where Q is a quasi-trivial torus and G is viewed as a constant k-group. We note that T is a torus since $\mathrm{Pic}(X' \otimes_k \bar{k})_{\mathrm{tors}} = 0$ (see [39, Prop. 1]).

As $X'(k) \neq \varnothing$, there exists a torsor over X', under T, of type ν (see [46, Cor. 2.3.9]). Applying [25, Cor. 2.2][1] to such a torsor, we now see that in order to prove Theorem A.1, it suffices to prove that rational points are dense in the Brauer–Manin set for a smooth compactification of any torsor over X', under T, of type ν.

A.3. **Fibration.** By [25, Prop. 3.1], which we can apply since $\bar{k}[X]^* = \bar{k}^*$ (see Proposition A.4), any torsor over X', under T, of type ν contains an open subset W admitting a smooth map $p : W \to Q$ whose fibres over the rational points of Q are torsors over X, under G, of type λ. In order to prove that rational points are dense in the Brauer–Manin set for a smooth compactification of W, we shall first prove that the base Q and the fibres of p over the rational points of Q satisfy this property, then solve the "fibration problem" to deduce it for W.

The variety Q is rational over k since it is a quasi-trivial torus, so the assertion on the base is trivial. The fibre of p above any rational point of Q is in fact a

[1] All of the Brauer groups that appear in Corollaire 2.2 of [25] are unramified Brauer groups, hence this corollary is really a statement about Brauer–Manin sets of smooth compactifications of torsors, even though smooth compactifications do not figure explicitly in it.

twist Y^σ of Y by a 1-cocycle $\sigma \in Z^1(k, G)$, since two torsors of a given type can only differ by such a twist. As G acts diagonally on $Y = \mathrm{SL}_n \times T^{\alpha_1} \times \cdots \times T^{\alpha_m}$, we have $Y^\sigma = (\mathrm{SL}_n)^\sigma \times (T^{\alpha_1})^\sigma \times \cdots \times (T^{\alpha_m})^\sigma$. On the one hand, we have $(\mathrm{SL}_n)^\sigma \simeq \mathrm{SL}_n$ since $\mathrm{H}^1(k, \mathrm{SL}_n)$ is a singleton (Hilbert's Theorem 90); hence $(\mathrm{SL}_n)^\sigma$ is rational over k. On the other hand, for any $\alpha \in k^*$, the variety $(T^\alpha)^\sigma$ is a torsor under the torus $(T^1)^\sigma$. All in all Y^σ is birationally equivalent to a torsor under a torus over k. We conclude that for any smooth compactification Z of a fibre of p above a rational point of Q, the set $Z(k)$ is indeed dense in $Z(\mathbb{A}_k)^{\mathrm{Br}(Z)}$ (see [46, Thm. 6.3.1], [12, Prop. 6.1 (iii)]).

A positive solution to the fibration problem for fibrations into rationally connected varieties over a quasi-trivial torus is obtained in [25, Th. 4.2 (ii)] under the assumption that a rational section exists over $\bar{k}$. (The existence of such a rational section ensures that the hypothesis of *loc. cit.* is satisfied, as shown in [45, Lem. 1.1(b)].) Fortunately, this last condition holds in our situation.

Proposition A.5. *The generic fibre of $p \otimes_k \bar{k} : W \otimes_k \bar{k} \to Q \otimes_k \bar{k}$ possesses a rational point.*

Proof. This generic fibre is a twist of $Y \otimes_k \bar{k}(Q)$ by a 1-cocycle $\sigma \in Z^1(\bar{k}(Q), G)$. Arguing as above, we see that it has a rational point if and only if $(T^{\alpha_i} \otimes_k \bar{k}(Q))^\sigma$ has a rational point for each i. Writing α_i as a $|G|$-th power in $\bar{k}^*$ determines a G-invariant $\bar{k}$-point of T^{α_i}, hence a G-equivariant isomorphism $T^{\alpha_i} \otimes_k \bar{k} = T^1 \otimes_k \bar{k}$. Thus $(T^{\alpha_i} \otimes_k \bar{k}(Q))^\sigma$ is isomorphic to $(T^1 \otimes_k \bar{k}(Q))^\sigma$, a variety which certainly has a rational point since it is a torus. □

Applying [25, Th. 4.2 (ii)] to a suitable compactification of p therefore completes the proof of Theorem A.1.

A.4. **Verticality of the Brauer group.** It remains to prove Proposition A.3. As $X'(\mathbb{A}_k)^{\mathrm{Br}(X')}$ is closed in $X'(\mathbb{A}_k)$, we are free to replace x_v, for v outside of an arbitrarily large finite set of places of k, with another k_v-point of the same fibre of f. In particular, we may assume that $(x_v)_{v \in \Omega}$ is an adelic point of this fibre. We may then view it as an adelic point of X. As such, it is orthogonal, for the Brauer–Manin pairing $X(\mathbb{A}_k) \times \mathrm{Br}(X) \to \mathbb{Q}/\mathbb{Z}$, to $f^*\mathrm{Br}(B)$. Proposition A.3 therefore results from the following purely algebraic statement, in which k is allowed to be an arbitrary field of characteristic 0.

Proposition A.6. *Viewing* $\mathrm{Br}(X')$ *and* $f^*\mathrm{Br}(B)$ *as subgroups of* $\mathrm{Br}(X)$*, one has an inclusion* $\mathrm{Br}(X') \subseteq f^*\mathrm{Br}(B)$.

Proof. Let V be a smooth compactification of the generic fibre V^0 of f. As V^0 is a torsor under a torus over $k(B)$ split by the extension $k(\mathrm{SL}_n)/k(B)$, as $V^0 \otimes_k \bar{k}$ is a torsor under a torus over $\bar{k}(B)$ split by the extension $\bar{k}(\mathrm{SL}_n)/\bar{k}(B)$ and as the natural map $\mathrm{Gal}(\bar{k}(\mathrm{SL}_n)/\bar{k}(B)) \to \mathrm{Gal}(k(\mathrm{SL}_n)/k(B))$ is an isomorphism, the following well-known lemma implies that the pull-back map

$$\mathrm{Br}(V)/f^*\mathrm{Br}(k(B)) \to \mathrm{Br}(V \otimes_k \bar{k})/f^*\mathrm{Br}(\bar{k}(B))$$

is injective.

Lemma A.7. *Let T be a torus over a field K, with character group $\widehat{T}$, split by a finite Galois extension L/K. For any smooth and proper variety V over K containing a torsor under T as a dense open subset, there is a canonical embedding* $\mathrm{Coker}(\mathrm{Br}(K) \to \mathrm{Br}(V)) \hookrightarrow \mathrm{H}^2(\mathrm{Gal}(L/K), \widehat{T})$.

Proof. Let $\bar{L}$ denote a separable closure of L and V^0 the open subset in question. As $\mathrm{Br}(V \otimes_K \bar{L}) = 0$ and $\mathrm{Br}(L) \twoheadrightarrow \mathrm{Br}(V \otimes_K L)$, the Hochschild–Serre spectral sequence provides an embedding of $\mathrm{Coker}(\mathrm{Br}(K) \to \mathrm{Br}(V))$ into the kernel of the restriction map $\mathrm{H}^1(K, \mathrm{Pic}(V \otimes_K \bar{L})) \to \mathrm{H}^1(L, \mathrm{Pic}(V \otimes_K \bar{L}))$, that is, into $\mathrm{H}^1(\mathrm{Gal}(L/K), \mathrm{Pic}(V \otimes_K L))$. On the other hand, the exact sequence

$$0 \to \widehat{T} \to \mathrm{Div}_{(V \setminus V^0) \otimes_K L}(V \otimes_K L) \to \mathrm{Pic}(V \otimes_K L) \to 0$$

(see [46, p. 130]) embeds this group into $\mathrm{H}^2(\mathrm{Gal}(L/K), \widehat{T})$. □

As f is smooth and surjective, we have $f^*\mathrm{Br}(k(B)) \cap \mathrm{Br}(X') \subseteq f^*\mathrm{Br}(B)$ as subgroups of $\mathrm{Br}(k(X))$. It follows that the pull-back map

$$\mathrm{Br}(X')/\Big(\mathrm{Br}(X') \cap f^*\mathrm{Br}(B)\Big) \to \mathrm{Br}(X' \otimes_k \bar{k})/\Big(\mathrm{Br}(X' \otimes_k \bar{k}) \cap f^*\mathrm{Br}(B \otimes_k \bar{k})\Big)$$

is injective as well. Thanks to this injectivity, we now see that in order to prove Proposition A.6, we may assume that k is algebraically closed.

The generic fibre of the natural map $X \to (T^{\alpha_1} \times \cdots \times T^{\alpha_m})/G$ is a left torsor under SL_n, hence is isomorphic to SL_n (Hilbert's Theorem 90). It follows that X is stably birationally equivalent to $(T^{\alpha_1} \times \cdots \times T^{\alpha_m})/G$. This variety is isomorphic to $(T^1 \times \cdots \times T^1)/G$ when k is algebraically closed, as we have seen in the proof of Proposition A.5. In addition, the unramified Brauer group of $(T^1 \times \cdots \times T^1)/G$ vanishes when k is algebraically closed, by Saltman's formula [15, Thm. 8.7] and by the next lemma. Hence $\mathrm{Br}(X') = 0$ in this case.

Lemma A.8. *Let $\mathcal{B}_G$ denote the set of subgroups of G generated by two elements. For any finite abelian group G and for $M = \mathbb{Z}[G]/\mathbb{Z}$ or $M = \mathbb{Q}/\mathbb{Z}$, the product of restriction maps $\mathrm{H}^2(G, M) \to \prod_{H \in \mathcal{B}_G} \mathrm{H}^2(H, M)$ is injective.*

Proof. As $\mathrm{H}^2(G, \mathbb{Q})$ and $\mathrm{H}^2(G, \mathbb{Z}[G])$ vanish, this follows from the injectivity of the product of restriction maps

$$\mathrm{H}^3(G, \mathbb{Z}) \to \prod_{H \in \mathcal{B}_G} \mathrm{H}^3(H, \mathbb{Z}). \tag{A.6}$$

It is a general fact, valid for an arbitrary finite group G, that the kernel of (A.6) remains unchanged if one replaces $\mathcal{B}_G$ with the set of abelian subgroups of G (see [15, Thm. 7.1]), which implies the desired injectivity when G is abelian. Alternatively, this injectivity results from Lemma 4.6 and [21, Lem. 6.4]. □

This completes the proof of Proposition A.6. □

A.5. **Nonabelian Galois groups.** The descent-fibration argument described in §A.2 and §A.3 is modelled after a similar argument appearing in [25], profiting in addition from the favourable circumstance of G being abelian. In general, the inductive argument of [25] is constructed to handle also nonabelian groups, as long as they admit a suitable filtration into normal subgroups whose successive quotients are cyclic; such groups are also known as *supersolvable*. Though the

variety X considered here is more complicated than the one considered in [25], the argument of *loc. cit.* can be adapted to yield the statement of Theorem 1.1 for any supersolvable G, see [26]. Interestingly enough, though, it turns out that the stronger claim appearing in Corollary 4.12 *does not* hold for a general nonabelian group G, even when G is supersolvable (indeed, even when G is a 2-group). This is due to the fact that the variety X may contain unramified Brauer classes which are not vertical with respect to the projection $f : X \to B$, and which can obstruct the weak approximation of local points on X, even when those local points lie over a rational point of B. (Such Brauer classes do not exist in the abelian case; see Proposition A.6.) Let us now illustrate how one can construct a nonabelian example where exactly this happens.

We shall say that a group H is *weakly bicyclic* if it is an extension of a cyclic group by a cyclic group. We note that if K/k is a Galois extension with Galois group G then the decomposition subgroups $H_v \subseteq G$ are weakly bicyclic at every finite place v which does not divide the order of G. Given a group G, we shall denote by $\mathcal{B}_G$ the set of weakly bicyclic subgroups of G (a notation compatible with Lemma A.8 when G is abelian).

Proposition A.9. *Let G be a finite 2-group satisfying the following properties:*

(i) G has exponent ≤ 16.

(ii) The abelianization G^{ab} has exponent 2 and is generated by images of elements of G of order 2.

(iii) There exists an element $\varphi \in \mathrm{H}^2(G, \mathbb{Z}/2\mathbb{Z})$ whose restriction to every cyclic subgroup of G of order 16 vanishes, whose restriction to at least one cyclic subgroup of G of order 8 does not vanish, and whose image by the natural map $\delta : \mathrm{H}^2(G, \mathbb{Z}/2\mathbb{Z}) \to \mathrm{H}^2(G, \mathbb{Q}/\mathbb{Z})$ belongs to, and spans, the kernel of the product of restriction maps $\mathrm{H}^2(G, \mathbb{Q}/\mathbb{Z}) \to \prod_{H \in \mathcal{B}_G} \mathrm{H}^2(H, \mathbb{Q}/\mathbb{Z})$.

Let $H \subseteq G$ be a cyclic subgroup of order 8 on which φ does not vanish. Then:

(1) There exist G-extensions $K/\mathbb{Q}$ which are unramified at 2 and whose decomposition groups at 2 are conjugate to H.

(2) For every G-extension $K/\mathbb{Q}$ as in (1), the element $256 \in \mathbb{Q}^*$ is a local norm from K at every place of $\mathbb{Q}$, but not a global norm from K.

In particular, the statement of Corollary 4.12 does not hold for G with $k = \mathbb{Q}$, $S = \{2\}$ and $\mathcal{A} \subset k^*$ the subgroup generated by 256.

The proof of Proposition A.9 requires a bit of preparation. In the next lemma, we denote by $\mathrm{Br}_{\mathrm{nr}}(B)$, $\mathrm{Br}_1(B)$, $\mathrm{Br}_{1,\mathrm{nr}}(B)$, $\mathrm{Br}_0(B)$ the subgroups of $\mathrm{Br}(B)$ consisting, respectively, of unramified, algebraic, algebraic unramified, constant classes.

Lemma A.10. *Let $G \subseteq \mathrm{SL}_n(\mathbb{Q})$ be a finite subgroup. Let $B = \mathrm{SL}_n/G$.*

(1) If G satisfies Condition (ii) of Proposition A.9, then $\mathrm{Br}_{1,\mathrm{nr}}(B) = \mathrm{Br}_0(B)$.

(2) If G satisfies Condition (iii) of Proposition A.9, then $\mathrm{Br}_{\mathrm{nr}}(B) = \mathrm{Br}_{1,\mathrm{nr}}(B)$.

In particular, for G as in Proposition A.9, we have $\mathrm{Br}_{\mathrm{nr}}(B) = \mathrm{Br}_0(B)$.

Proof. Condition (ii) implies that for any field K, the group $\mathrm{H}^1(K, G^{\mathrm{ab}})$ is generated by elements in the image of the pointed set $\mathrm{H}^1(K, G)$ (and even by elements coming from $\mathrm{H}^1(K, \mathbb{Z}/2\mathbb{Z})$ via homomorphisms $\mathbb{Z}/2\mathbb{Z} \to G$). The first claim then follows, by local and global duality, from [24, Prop. 4]. Let us now explain why

Condition (iii) implies that $\mathrm{Br}_{\mathrm{nr}}(B) = \mathrm{Br}_{1,\mathrm{nr}}(B)$. For every subgroup $H \subseteq G$, the Hochschild–Serre spectral sequences for the H-coverings $\pi_H : \mathrm{SL}_n \to \mathrm{SL}_n/H$ and $\mathrm{SL}_{n,\bar{\mathbb{Q}}} \to \mathrm{SL}_{n,\bar{\mathbb{Q}}}/H$, together with the inclusion of roots of unity $\mu_\infty \subseteq \bar{\mathbb{Q}}^*$, give rise to a commutative diagram

$$\begin{tikzcd}
\mathrm{Ker}\Big(\mathrm{Br}(\mathrm{SL}_n/H) \to \mathrm{Br}(\mathrm{SL}_n)\Big) \arrow[d] & \mathrm{H}^2(H, \mathbb{Q}^*) \arrow[l, "\sim"'] \arrow[d] & \mathrm{H}^2(H, \mu_2) \arrow[l] \arrow[d, two heads] \\
\mathrm{Ker}\Big(\mathrm{Br}(\mathrm{SL}_{n,\bar{\mathbb{Q}}}/H) \to \mathrm{Br}(\mathrm{SL}_{n,\bar{\mathbb{Q}}})\Big)^{\Gamma_{\mathbb{Q}}} & \mathrm{H}^2(H, \bar{\mathbb{Q}}^*)^{\Gamma_{\mathbb{Q}}} \arrow[l, "\sim"'] & \mathrm{H}^2(H, \mu_\infty)^{\Gamma_{\mathbb{Q}}} \arrow[l, "\sim"']
\end{tikzcd} \tag{A.7}$$

where $\Gamma_{\mathbb{Q}} = \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ is the absolute Galois group of $\mathbb{Q}$. The horizontal arrows between the first two columns are isomorphisms since $\mathrm{Pic}(\mathrm{SL}_n) = \mathrm{Pic}(\mathrm{SL}_{n,\bar{\mathbb{Q}}}) = 0$, and the bottom right horizontal map is an isomorphism since $\bar{\mathbb{Q}}^*/\mu_\infty$ is uniquely divisible. In addition, the rightmost vertical map is surjective: indeed, this map fits in the middle of the commutative diagram with exact rows

$$\begin{tikzcd}
0 \arrow[r] & \mathrm{Ext}^1(\mathrm{H}_1(H), \mu_2) \arrow[r] \arrow[d] & \mathrm{H}^2(H, \mu_2) \arrow[r, two heads] \arrow[d, two heads] & \mathrm{Hom}(\mathrm{H}_2(H), \mu_2) \arrow[d, "\wr"] \\
0 \arrow[r, "\sim"] & \mathrm{Ext}^1(\mathrm{H}_1(H), \mu_\infty)^{\Gamma_{\mathbb{Q}}} \arrow[r] & \mathrm{H}^2(H, \mu_\infty)^{\Gamma_{\mathbb{Q}}} \arrow[r, "\sim"] & \mathrm{Hom}(\mathrm{H}_2(H), \mu_\infty)^{\Gamma_{\mathbb{Q}}}
\end{tikzcd}$$

determined by the universal coefficient theorem, where $\mathrm{Ext}^1(\mathrm{H}_1(H), \mu_\infty) = 0$ since μ_∞ is a divisible group.

We now fix a $\beta \in \mathrm{Br}_{\mathrm{nr}}(B)$ and aim to show that β is algebraic. By adding to β a constant class, we may assume that $\beta(\pi_G(1)) = 0$. As SL_n is rational over $\mathbb{Q}$, we have $\mathrm{Br}_{\mathrm{nr}}(\mathrm{SL}_n) = \mathrm{Br}_0(\mathrm{SL}_n)$, and so $\pi_G^*\beta = 0$. Considering the diagram (A.7) for $G = H$ and using the surjectivity of its right vertical map, we find $\beta_G \in \mathrm{H}^2(G, \mu_2)$ whose eventual image in $\mathrm{Br}(B_{\bar{\mathbb{Q}}})$ is the same as the image of β. Now by Bogomolov's formula (see, e.g., [15, Thm. 7.1]), the group $\mathrm{Br}_{\mathrm{nr}}(\mathrm{SL}_{n,\bar{\mathbb{Q}}}/H)$ vanishes whenever H is weakly bicyclic, and so by the naturality of (A.7), the image of β_G in $\mathrm{H}^2(H, \mu_\infty)$ vanishes for every $H \in \mathcal{B}_G$. Since $\mu_\infty \cong \mathbb{Q}/\mathbb{Z}$ as abelian groups via a choice of a compatible system of roots of unity, Condition (iii) implies that the image of β_G in $\mathrm{H}^2(G, \mu_\infty)$ is either 0 or the image of $\varphi \in \mathrm{H}^2(G, \mathbb{Z}/2) = \mathrm{H}^2(G, \mu_2)$ under the natural map $\mathrm{H}^2(G, \mu_2) \to \mathrm{H}^2(G, \mu_\infty)$. By possibly amending the choice of β_G, we may assume that $\beta_G \in \{0, \varphi\}$. We then write $\beta_1 \in \mathrm{Br}(B)$ for the image of β_G, and set $\beta_2 := \beta - \beta_1$. By construction, β_1 (and hence also β_2) vanishes when pulled back to SL_n, and β_2 also vanishes when pulled back to $B_{\bar{\mathbb{Q}}}$. In particular, $\beta_2 \in \mathrm{Ker}(\mathrm{Br}_1(B) \to \mathrm{Br}_1(\mathrm{SL}_n))$.

Let now $H \subseteq G$ be a cyclic subgroup of order 8 on which φ does not vanish. As β is unramified, there exists a prime p_0 such that β evaluates trivially on $B(\mathbb{Q}_p)$ for all $p > p_0$. Choose $p > p_0$ such that there exists a cyclic extension $L/\mathbb{Q}_p$ of degree 4 that does not extend to a cyclic extension of degree 8 (any p such that -1 is a square but not a 4th power modulo p will do). Embed $\mathrm{Gal}(L/\mathbb{Q}_p)$ into H. The image of the class of $L/\mathbb{Q}_p$ by the resulting map $\mathrm{H}^1(\mathbb{Q}_p, \mathrm{Gal}(L/\mathbb{Q}_p)) \to \mathrm{H}^1(\mathbb{Q}_p, G)$ is the class of the torsor $\pi_G^{-1}(b)$ for some point $b \in B(\mathbb{Q}_p)$ (see [24, §1.2]), which we fix.

By the choice of p, we have $\beta(b) = 0$. We claim that $\beta_2(b) = 0$ as well. Indeed, as β_2 is algebraic and $\beta_2(\pi_G(1)) = 0$, it follows that β_2 vanishes when pulled back

to the universal torsor $\mathrm{SL}_n/G' \to B$, where $G' := \mathrm{Ker}(G \to G^{\mathrm{ab}})$ is the derived subgroup of G. On the other hand, since G^{ab} has exponent 2 and the subgroup $\mathrm{Gal}(L/\mathbb{Q}_p) \subseteq H$ consists of elements divisible by 2, we have $\mathrm{Gal}(L/\mathbb{Q}_p) \subseteq G'$. This means that b lifts to SL_n/G' and so $\beta_2(b) = 0$. Therefore $\beta_1(b) = 0$.

Let us prove that $\beta_G = 0$. By contradiction, assume that $\beta_G = \varphi$. Then the restriction of β_G to H is the non-trivial element of $\mathrm{H}^2(H, \mathbb{Z}/2\mathbb{Z}) = \mathbb{Z}/2\mathbb{Z}$, which is the one classifying the central extension $\tilde{H} \to H$ with $\tilde{H}$ cyclic of order 16. This element restricts to the non-trivial element of $\mathrm{H}^2(\mathrm{Gal}(L/\mathbb{Q}_p), \mathbb{Z}/2\mathbb{Z})$ for the cyclic order 4 subgroup $\mathrm{Gal}(L/\mathbb{Q}_p) \subseteq H$, and further to a non-trivial element of $\mathrm{H}^2(\mathbb{Q}_p, \mathbb{Z}/2\mathbb{Z})$ by the assumption that L does not extend to a cyclic degree 8 extension. As $\beta_1(b) = 0$, this is absurd. We conclude that $\beta_G = 0$ and $\beta = \beta_2$, which completes the proof that $\mathrm{Br}_{\mathrm{nr}}(B) = \mathrm{Br}_{1,\mathrm{nr}}(B)$. □

Proof of Proposition A.9. Fix an embedding $G \hookrightarrow \mathrm{SL}_n(\mathbb{Q})$ and let $B = \mathrm{SL}_n/G$. By Lemma A.10, we have $\mathrm{Br}_{\mathrm{nr}}(B) = \mathrm{Br}_0(G)$, and so the existence of a G-extension $K/\mathbb{Q}$ as in (1) follows from [25, Th. B], since G is nilpotent and in particular supersolvable. Let us choose such an extension $K/\mathbb{Q}$. As 256 is positive, it is a norm from K_∞. In addition, 16 is an 8th power (and hence 256 is a 16th power) in $\mathbb{Q}_p$ for every odd p; indeed, one of $2, -2$ or -1 is a square, and in the latter case $2i = (1+i)^2$ is a square. Since G has exponent at most 16 and 256 is a unit outside 2, it follows that in $K/\mathbb{Q}$, the element 256 is a local norm at every odd finite place. Finally, at 2 the extension $K/\mathbb{Q}$ is unramified with Frobenius element of order 8, and hence $256 = 2^8$ is a norm from K_2 as well.

It is left to show that 256 is not a global norm from K. Let us first recall some notation used above. For $\alpha \in k^*$, we consider the variety $X^\alpha := (\mathrm{SL}_n \times T^\alpha)/G$, equipped with the projection $X^\alpha \to B$. Given a rational point $b \in B(k)$, the fibre of $X^1 \to B$ over b is naturally isomorphic to the norm 1 torus of K/k, which we denote by T^1_b. The fibre X^α_b of $X^\alpha \to B$ over b is then naturally isomorphic to the norm α torsor of T^1_b. We also recall that $\widehat{T}^1$ denotes the character lattice of T^1, which carries a natural action of G.

Let $b \in B(\mathbb{Q})$ be such that $[b] \in \mathrm{H}^1(\mathbb{Q}, G)$ classifies the extension $K/\mathbb{Q}$ (see [24, §1.2]). In order to prove that $X^{256}_b(\mathbb{Q}) = \varnothing$, i.e. that 256 is not a norm from K, we shall now exhibit a Brauer–Manin obstruction on X^{256}_b.

As $G = \pi_1(B, \pi_G(1))$, we may identify G-modules with locally constant étale sheaves of abelian groups on B. In this way, we view $\widehat{T}^1/2\widehat{T}^1$ as an étale sheaf on B and φ as an element of $\mathrm{H}^1(B, \widehat{T}^1/2\widehat{T}^1)$ via the natural isomorphism $\mathrm{H}^1(B, \widehat{T}^1/2\widehat{T}^1) = \mathrm{H}^2(G, \mathbb{Z}/2\mathbb{Z})$. The map $p : X^{16} \to X^{256}$ induced by the squaring map $T^{16} \to T^{256}$ is a torsor under the 2-torsion subgroup scheme of $X^1 \to B$, which we identify with the G-module $T^1[2] = \{x \in T^1(\bar{\mathbb{Q}}) : x^2 = 1\}$; this torsor is classified by an element $\psi \in \mathrm{H}^1(X^{256}, T^1[2])$. We set $\mathfrak{P} := \psi \cup \varphi \in \mathrm{H}^2(X^{256}, \mu_2)$. We will abusively identify $\mathfrak{P}$ with its image in $\mathrm{Br}(X^{256})$ and consider it as a *Brauer element* of order 2.

We have already seen that $X^{256}_b(\mathbb{Q}_v) \neq \varnothing$ for any place v of $\mathbb{Q}$. Let us show that the evaluation

$$\sum_v \mathrm{inv}_v(x_v^* \mathfrak{P}) \in \mathbb{Q}/\mathbb{Z}$$

is well defined and non-zero for any collection $(x_v)_v$ of local points in X^{256}_b.

Our assumptions on φ imply that we can choose, for every weakly bicyclic subgroup $H \subseteq G$, a class $\widetilde{\varphi}_H \in \mathrm{H}^1(H, \mathbb{Q}/\mathbb{Z})$ whose image, under the boundary map $\mathrm{H}^1(H, \mathbb{Q}/\mathbb{Z}) \to \mathrm{H}^2(H, \mathbb{Z}/2\mathbb{Z})$, is the restriction $\varphi_H \in \mathrm{H}^2(H, \mathbb{Z}/2\mathbb{Z})$ of φ.

For any place v of $\mathbb{Q}$, let K_v denote the completion of K at a place of K dividing v. The corresponding decomposition group $D_v \subseteq G$ is weakly bicyclic since G is a 2-group and $K_2/\mathbb{Q}_2$ is unramified. Letting $\mathbb{Q}_v \subseteq K_{\widetilde{\varphi}_{D_v}} \subseteq K_v$ denote the intermediate cyclic extension determined by $\widetilde{\varphi}_{D_v} \in \mathrm{H}^1(D_v, \mathbb{Q}/\mathbb{Z})$, a direct computation now reveals that $x_v^*\mathfrak{P} = (16, K_{\widetilde{\varphi}_{D_v}}/\mathbb{Q}_v) \in \mathrm{Br}(\mathbb{Q}_v)$.

Since φ is assumed to vanish on every cyclic subgroup of order 16, the class $\widetilde{\varphi}_{D_v}$ becomes divisible by 2 when restricted to every such subgroup. Since the exponent of G divides 16, it follows that $8\widetilde{\varphi}_{D_v} \in \mathrm{H}^1(D_v, \mathbb{Q}/\mathbb{Z}) = \mathrm{Hom}(D_v, \mathbb{Q}/\mathbb{Z})$ vanishes when restricted to any cyclic subgroup of D_v, and hence vanishes; in other words, the degree of the extension $K_{\widetilde{\varphi}_{D_v}}/\mathbb{Q}_v$ divides 8. On the other hand, as D_2 is cyclic of order 8 and φ does not vanish when restricted to D_2 we have that $\widetilde{\varphi}_{D_2} \in \mathrm{H}^1(D_2, \mathbb{Q}/\mathbb{Z}) \cong \mathbb{Z}/8\mathbb{Z}$ is not divisible by 2 and so $K_{\widetilde{\varphi}_{D_2}} = K_2$. We conclude that $\mathrm{inv}_v(x_v^*\mathfrak{P}) = 0$ for all $v \neq 2$ (recall that 16 is an 8th power at such v) while $\mathrm{inv}_2(x_2^*\mathfrak{P}) = 1/2 \in \mathbb{Q}/\mathbb{Z}$. $\square$

We shall now construct a 2-group G satisfying the conditions of Proposition A.9. Let N be the group generated by 4 generators x, y, z_+, z_- under the following relations:

(1) $x^{16} = y^{16} = z_+^8 = z_-^8 = 1$;
(2) each of z_+, z_- commutes with each of x, y, z_+, z_-;
(3) $[x, y] = z_+z_-$.

In particular, N is a central extension of the bicyclic group $\mathbb{Z}/16\mathbb{Z}\langle x, y\rangle$ by the bicyclic group $\mathbb{Z}/8\mathbb{Z}\langle z_+, z_-\rangle$. Let $\sigma : N \to N$ be the involution given by $\sigma(x) = x^{-1}, \sigma(y) = y^{-1}, \sigma(z_+) = z_-$ and $\sigma(z_-) = z_+$. We define $G := N \rtimes \mathbb{Z}/2\mathbb{Z}\langle\sigma\rangle$ to be the associated semi-direct product and view σ as an element of G.

It is straightforward that G satisfies Conditions (i) and (ii) of Proposition A.9. Let us now construct an element $\varphi \in \mathrm{H}^2(G, \mathbb{Z}/2\mathbb{Z})$ satisfying Condition (iii). The homomorphism $\rho : N \to \mathbb{Z}/8\mathbb{Z}$ which sends x, y to 0, z_+ to 1 and z_- to -1 intertwines the action of σ with the action of $-1 : \mathbb{Z}/8\mathbb{Z} \to \mathbb{Z}/8\mathbb{Z}$. Consequently, it induces a homomorphism $\rho' : G = N \rtimes \mathbb{Z}/2\mathbb{Z} \to \mathbb{Z}/8\mathbb{Z} \rtimes \mathbb{Z}/2\mathbb{Z} =: D_8$ to the dihedral group of order 16. Consider the short exact sequence

$$1 \to \mathbb{Z}/2\mathbb{Z} \to D_{16} \xrightarrow{q} D_8 \to 1 \tag{A.8}$$

where $D_{16} := \mathbb{Z}/16\mathbb{Z} \rtimes \mathbb{Z}/2\mathbb{Z}$ is the dihedral group of order 32 and the map q is induced by the surjective map $\mathbb{Z}/16\mathbb{Z} \to \mathbb{Z}/8\mathbb{Z}$. Let $\varphi_{D_8} \in \mathrm{H}^2(D_8, \mathbb{Z}/2\mathbb{Z})$ be the element classifying the central extension (A.8) and let $\varphi := (\rho')^*\varphi_{D_8} \in \mathrm{H}^2(G, \mathbb{Z}/2\mathbb{Z})$. We leave it to the reader to verify that φ has the desired properties.

References

[1] S.A. Altuğ, A. Shankar, I. Varma, K.H. Wilson, The number of D_4-quartic fields ordered by conductor. *J. Eur. Math. Soc.* **23** (2021), 2733–2785.

[2] A. Bartel, H.W. Lenstra Jr., On class groups of random number fields. *Proc. Lond. Math. Soc.* **121** no. 3 (2020), 927–953.

[3] M. Bhargava, A positive proportion of plane cubics fail the Hasse principle, preprint. arXiv:1402.1131.
[4] M. Bhargava, A. Shankar, J. Tsimerman, On the Davenport-Heilbronn theorems and second order terms. *Invent. math.* (2013), 193–439.
[5] M. Bhargava, I. Varma, On the mean number of 2-torsion elements in the class groups, narrow class groups, and ideal groups of cubic orders and fields. *Duke Math. J.* **164** (2015), No. 10, 1911–1933.
[6] R. de la Bretèche, T.D. Browning, Contre-exemples au principe de Hasse pour certains tores coflasques. *J. Théor. Nombres Bordeaux* **26** (2014), 25–44.
[7] R. de la Bretèche, T.D. Browning, Density of Châtelet surfaces failing the Hasse principle. *Proc. London Math. Soc.* **108** (2014), 1030–1078.
[8] M. Bright, T.D. Browning, D. Loughran, Failures of weak approximation in families, Compositio Math., **152** (71) (2016), 1435–1475.
[9] T.D. Browning. How often does the Hasse principle hold? *Algebraic Geometry: Salt Lake City 2015, Proc. Symposia Pure Math.* **97.2** (2018), AMS, 89–102.
[10] T.D. Browning, R. Newton, The proportion of failures of the Hasse norm principle. *Mathematika* **62** (2016), 337–347.
[11] J.W.S. Cassels, A. Fröhlich. *Algebraic Number Theory.* Second Edition. London Mathematical Society. 2010.
[12] J.-L. Colliot-Thélène, A. Pál, A. N. Skorobogatov, Pathologies of the Brauer-Manin obstruction, *Math. Z.* **282** (2016), no. 3–4, 799–817.
[13] J.-L. Colliot-Thélène, J.-J. Sansuc, La R-équivalence sur les tores, *Ann. Sci. École Norm. Sup. (4)* **10** (1977), no. 2, 175–229.
[14] J.-L. Colliot-Thélène, J.-J. Sansuc, La descente sur les variétés rationnelles. II, *Duke Math. J.* **54** (1987), no. 2, 375–492.
[15] J.-L. Colliot-Thélène, J.-J. Sansuc, The rationality problem for fields of invariants under linear algebraic groups (with special regards to the Brauer group), *Algebraic groups and homogeneous spaces*, 113–186, Tata Inst. Fund. Res. Stud. Math., 19, Tata Inst. Fund. Res., Mumbai, 2007.
[16] C. Demarche, Groupe de Brauer non ramifié d'espaces homogènes à stabilisateurs finis, *Math. Ann.* **346** (2010), no. 4, 949–968.
[17] S. Delsarte, Fonctions de Möbius sur les groupes abeliens finis. *Ann. of Math.* **49** (1948), 600–609.
[18] T. Ekedahl, *An effective version of Hilbert's irreducibility theorem*, Séminaire de Théorie des Nombres, Paris 1988–1989, 241–249, Progress in Mathematics, vol. 91, Birkhäuser Boston, Boston, MA, 1990.
[19] J. Ellenberg, L.B. Pierce, M.M. Wood, On ℓ-torsion in class groups of number fields. *Algebra Number Theory* **11** (2017), No. 8, 1739–1778.
[20] A.-S. Elsenhans, J. Jahnel, Cubic surfaces violating the Hasse principle are Zariski dense in the moduli scheme. *Advances Math.* **280** (2015), 360–378.
[21] C. Frei, D. Loughran, R. Newton, The Hasse norm principle for abelian extensions. *Amer. J. Math.* **140**(6) (2018), 1639–1685.
[22] C. Frei, M. Widmer, Average bounds for the ℓ-torsion in class groups of cyclic extensions. *Res. Number Theory* **4**, 34 (2018).
[23] W. Fulton, J. Harris, *Representation theory. A first course.* Graduate Texts in Mathematics, **129**. Springer-Verlag, New York, 1991.
[24] D. Harari, Quelques propriétés d'approximation reliées à la cohomologie galoisienne d'un groupe algébrique fini, Bull. Soc. Math. France **135** (2007), no. 4, 549–564.
[25] Y. Harpaz, O. Wittenberg, Zéro-cycles sur les espaces homogènes et problème de Galois inverse. *J. Am. Math. Soc.* **33** (3), 2020, 775–805.
[26] Y. Harpaz, O. Wittenberg, Supersolvable descent for rational points, in preparation.
[27] H. Hering, *Seltenheit der Gleichungen mit Affekt bei linearem Parameter*, Math. Ann. **186** (1970), 263–270.

[28] W. Ho, A. Shankar, I. Varma, Odd degree number fields with odd class number, *Duke Math. J.* **167** (2018), No. 5, 995–1047.
[29] H. Iwaniec, E. Kowalski, *Analytic number theory.* Amer. Math. Soc., Providence, RI, 2004.
[30] D. Loughran and A. Smeets, Fibrations with few rational points. *Geometric and Functional Analysis (GAFA)*, **26** (5) (2016), 1449–1482.
[31] A. Macedo, The Hasse norm principle for A_n-extensions. *J. Number Theory*, **211** (2020), 500–512.
[32] A. Macedo, *Local-global principles for norms.* PhD thesis, University of Reading, 2021. `https://www.reading.ac.uk/web/files/maths/MacedoTheses.pdf`.
[33] H. Montgomery, R. Vaughan, *Multiplicative Number Theory: I. Classical Theory.* Cambridge University Press, 2006.
[34] J. Neukirch, A. Schmidt, K. Wingberg, *Cohomology of Number Fields.* Second edition. Grundlehren der Mathematischen Wissenschaften **323**, Springer-Verlag, 2008.
[35] L.B. Pierce, C.L. Turnage-Butterbaugh, 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), no. 2, 701–778.
[36] V. Platonov, A. Rapinchuk, *Algebraic groups and number theory.* Pure and Applied Mathematics, 139. Academic Press, Inc., Boston, MA, 1994.
[37] N. Rome, The Hasse norm principle for biquadratic extensions. *J. Théor. Nombres Bordeaux*, **30** (2018), no. 3, 947–964.
[38] J.-J. Sansuc, Groupe de Brauer et arithmétique des groupes algébriques linéaires sur un corps de nombres. *J. reine angew. Math.* **327** (1981), 12–80.
[39] J.-P. Serre, On the fundamental group of a unirational variety, *J. London Math. Soc.* **34** (1959), 481–484.
[40] J.-P. Serre, Divisibilité de certaines fonctions arithmétiques. *Enseign. Math. (2)*, **22** (1976), 227–260.
[41] J.-P. Serre, *Local fields.* Graduate Texts in Mathematics, **67**. Springer-Verlag, New York-Berlin, 1979.
[42] J.-P. Serre, *Cohomologie galoisienne*, fifth edition, Lecture Notes in Mathematics, **5**. Springer-Verlag, Berlin, 1994.
[43] J.-P. Serre, *Lectures on $N_X(p)$.* Chapman & Hall/CRC Research Notes in Mathematics, 11. CRC Press, Boca Raton, FL, 2012.
[44] J.-P. Serre, *Topics in Galois theory*, second edition, Research Notes in Mathematics, vol. 1, A K Peters, Ltd., Wellesley, MA, 2008, xvi+120 pp.
[45] A.N. Skorobogatov, Descent on fibrations over the projective line, *Amer. J. Math.* **118** (1996), no. 5, 905–923.
[46] A.N. Skorobogatov, *Torsors and rational points*, Cambridge Tracts in Mathematics, vol. 144, CUP, Cambridge, 2001.
[47] G. Tenenbaum, *Introduction to analytic and probabilistic number theory.* Third edition. Graduate Studies in Mathematics, 163. American Mathematical Society, Providence, RI, 2015.
[48] E.C. Titchmarsh, *The theory of the Riemann zeta-function.* Second edition. The Clarendon Press, Oxford University Press, New York, 1986.
[49] S. Wang, On Grunwald's theorem. *Ann. of Math.* **51** (1950), 471–484.
[50] O. Wittenberg, *Rational points and zero-cycles on rationally connected varieties over number fields*, in Algebraic Geometry: Salt Lake City 2015, Part 2, pp. 597–635, Proceedings of Symposia in Pure Mathematics 97, American Mathematical Society, Providence, RI, 2018.
[51] M. Wood, On the probabilities of local behaviors in abelian field extensions. *Compositio Math.* **146** (2010), no. 1, 102–128.
[52] M.M. Wood, Nonabelian Cohen-Lenstra Moments (appendix by P.M. Wood). *Duke Math. J.* **168** (2019), no. 3, 377–427.
[53] D. Wright, Distribution of discriminants of abelian extensions. *Proc. London Math. Soc.* **58** (1989), no. 1, 17–50.

Christopher Frei, TU Graz, Institute of Analysis and Number Theory, Steyrergasse 30/II, 8010 Graz, Austria.
Email address: frei@math.tugraz.at
URL: https://www.math.tugraz.at/~frei/

Daniel Loughran, Department of Mathematical Sciences, University of Bath, Claverton Down, Bath, BA2 7AY, UK
URL: https://sites.google.com/site/danielloughran/

Rachel Newton, Department of Mathematics, King's College London, Strand, London, WC2R 2LS, UK.
Email address: rachel.newton@kcl.ac.uk
URL: https://racheldominica.wordpress.com/

Yonatan Harpaz, Institut Galilée, Université Sorbonne Paris Nord, 99 avenue Jean-Baptiste Clément, 93430 Villetaneuse, France
Email address: harpaz@math.univ-paris13.fr
URL: https://www.math.univ-paris13.fr/~harpaz/

Olivier Wittenberg, Institut Galilée, Université Sorbonne Paris Nord, 99 avenue Jean-Baptiste Clément, 93430 Villetaneuse, France
Email address: olivier.wittenberg@math.u-psud.fr
URL: http://www.math.u-psud.fr/~wittenberg/