

The Hasse norm principle for abelian extensions

Article

Accepted Version

Frei, C., Loughran, D. and Newton, R. ORCID:
<https://orcid.org/0000-0003-4925-635X> (2018) The Hasse norm principle for abelian extensions. *American Journal of Mathematics*, 140 (6). pp. 1639-1685. ISSN 1080-6377 doi:
<https://doi.org/10.1353/ajm.2018.0048> Available at
<https://centaur.reading.ac.uk/60488/>

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

To link to this article DOI: <http://dx.doi.org/10.1353/ajm.2018.0048>

Publisher: John Hopkins University Press

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

www.reading.ac.uk/centaur

CentAUR

Central Archive at the University of Reading

Reading's research outputs online



THE HASSE NORM PRINCIPLE FOR ABELIAN EXTENSIONS

CHRISTOPHER FREI, DANIEL LOUGHRAN, AND RACHEL NEWTON

ABSTRACT. We study the distribution of abelian extensions of bounded discriminant of a number field k which fail the Hasse norm principle. For example, we classify those finite abelian groups G for which a positive proportion of G -extensions of k fail the Hasse norm principle. We obtain a similar classification for the failure of weak approximation for the associated norm one tori. These results involve counting abelian extensions of bounded discriminant with infinitely many local conditions imposed, which we achieve using tools from harmonic analysis, building on work of Wright.

CONTENTS

1. Introduction	1
2. From discriminant series to conductor series	9
3. Harmonic analysis	11
4. Proof of Theorem 1.7	19
5. Some applications of Theorem 1.7	31
6. The Hasse principle and weak approximation	34
References	39

1. INTRODUCTION

1.1. The Hasse norm principle. Let K/k be an extension of number fields and denote by $N_{K/k} : \mathbf{A}_K^* \rightarrow \mathbf{A}_k^*$ the norm map from the ideles of K to the ideles of k . We say that K/k satisfies the *Hasse norm principle* if $N_{K/k}K^* = N_{K/k}\mathbf{A}_K^* \cap k^*$. This property takes its name from a theorem of Hasse, which states that cyclic extensions always satisfy the Hasse norm principle. In this paper, we fix a finite abelian group G and ask how many Galois extensions of k with Galois group G satisfy the Hasse norm principle. This idea of studying Hasse principles in families has attracted a lot of attention recently in other settings; see for example [4], [8], [7], [11].

Let us begin by considering the case of biquadratic extensions, which is the simplest case where the Hasse norm principle can fail. A biquadratic extension fails the Hasse norm principle if and only if all its decomposition groups are cyclic. This condition may be viewed in an entirely elementary way over \mathbb{Q} , as we now explain. Let $a, b \in \mathbb{Z}$ and assume for simplicity that a, b are coprime, square-free, that $a, b \neq 1$ and that $a, b \equiv 1 \pmod{4}$. Then the biquadratic extension

2010 *Mathematics Subject Classification*. 11R37 (primary), 11R45, 43A70, 14G05, 20G30. (secondary).

$\mathbb{Q}(\sqrt{a}, \sqrt{b})/\mathbb{Q}$ fails the Hasse norm principle if and only if

$$\left(\frac{a}{p}\right) = 1 \text{ for all } p \mid b \quad \text{and} \quad \left(\frac{b}{p}\right) = 1 \text{ for all } p \mid a, \quad (1.1)$$

where (\cdot) denotes the Legendre symbol. A simple sieving argument shows that, for fixed a as above, 0% of all such b satisfy (1.1). In particular, it leads one to guess that 0% of all biquadratic extensions, when ordered by discriminant, fail the Hasse norm principle. Our first result shows that this is indeed the case, and moreover applies to a slightly larger class of abelian extensions.

In order to state this result, we shall need some definitions. Let G be a finite group and let k be a number field with a fixed choice of algebraic closure \bar{k} . By a G -extension of k , we mean a surjective continuous homomorphism $\varphi : \text{Gal}(\bar{k}/k) \rightarrow G$. Clearly, a G -extension is the same as a pair $(K/k, \psi)$, where K/k is a Galois extension contained in \bar{k} and $\psi : \text{Gal}(K/k) \rightarrow G$ is an isomorphism. We write K_φ/k for the extension corresponding to φ and $\Delta(\varphi)$ for the absolute norm of the relative discriminant ideal of K_φ over k . We say that φ satisfies the Hasse norm principle if K_φ does. We denote by $G\text{-ext}(k)$ the set of all G -extensions of k . Our first theorem is then the following.

Theorem 1.1. *Let $n, r \in \mathbb{Z}$ with $n > 1$ and $r \geq 0$. Let Q be the smallest prime dividing n and let $G = \mathbb{Z}/n\mathbb{Z} \oplus (\mathbb{Z}/Q\mathbb{Z})^r$. Then 0% of G -extensions of k fail the Hasse norm principle.*

Here, given a finite abelian group G , a number field k and a property P , we say that 0% of G -extensions of k satisfy P if

$$\limsup_{B \rightarrow \infty} \frac{\#\{\varphi \in G\text{-ext}(k) : \Delta(\varphi) \leq B, \varphi \text{ satisfies } P\}}{N(k, G, B)} = 0,$$

where

$$N(k, G, B) := \#\{\varphi \in G\text{-ext}(k) : \Delta(\varphi) \leq B\}$$

is the function which counts G -extensions of k of discriminant at most B .

Our next result shows that Theorem 1.1 is non-trivial, namely that the set of G -extensions which fail the Hasse norm principle is non-empty.

Theorem 1.2. *Let G be a finite abelian group. Then there exists a G -extension of k which fails the Hasse norm principle if and only if G is non-cyclic.*

This result was previously known only in some very special cases. For example, when $k = \mathbb{Q}$ and G an elementary abelian p -group of even rank, Horie has shown the existence of infinitely many G -extensions of \mathbb{Q} that fail the Hasse principle [20, Thm. 3].

We prove Theorem 1.2 using Shafarevich's resolution of the inverse Galois problem for solvable groups, together with some cohomological calculations. In particular, this also allows us to obtain the following extension to solvable groups.

Theorem 1.3. *Let G be a finite solvable group. Then there exists a G -extension of k which fails the Hasse norm principle if and only if*

$$H^3(G, \mathbb{Z}) \neq 0.$$

For a finite abelian group G , we have $H^3(G, \mathbb{Z}) = 0$ if and only if G is cyclic (see, for example, Lemmas 6.4 and 6.5). In contrast, there are many finite non-abelian groups G with $H^3(G, \mathbb{Z}) = 0$; for example, groups for which every Sylow subgroup is either cyclic or a generalised quaternion group (see [10, Ch. VI.9], in particular Theorem 9.5 and Exercise 4). This observation allows us to obtain counter-examples to the statement of [18, Cor. 3.2], showing that the forward implication given there is false in general. For example, the quaternion group Q has $H^3(Q, \mathbb{Z}) = 0$, yet is non-cyclic.

Returning to quantitative results, it turns out that there is an extreme dichotomy: for all finite abelian non-cyclic groups G other than those occurring in Theorem 1.1, the Hasse norm principle fails for a positive proportion of G -extensions.

Theorem 1.4. *Let G be a non-trivial finite abelian group and let Q be the smallest prime dividing $|G|$. Assume that G is not isomorphic to a group of the form $\mathbb{Z}/n\mathbb{Z} \oplus (\mathbb{Z}/Q\mathbb{Z})^r$ for any n divisible by Q and $r \geq 0$. Then a positive proportion of G -extensions of k fail the Hasse norm principle.*

Here, given a finite abelian group G , a number field k and a property P , we say that a positive proportion of G -extensions of k satisfy P if

$$\liminf_{B \rightarrow \infty} \frac{\#\{\varphi \in G\text{-ext}(k) : \Delta(\varphi) \leq B, \varphi \text{ satisfies } P\}}{N(k, G, B)} > 0.$$

Note the distinction between our work and the work of Browning and Newton in [11]. There the authors fix an extension K/\mathbb{Q} and count those rational numbers of bounded height that are norms everywhere locally but not globally, whereas in our work it is the extensions themselves that are being counted.

1.2. Norm one tori. Our results on the Hasse norm principle may be interpreted via the arithmetic of norm one tori. Given a finite field extension K/k , denote by

$$R_{K/k}^1 \mathbb{G}_m := \ker(R_{K/k} \mathbb{G}_m \rightarrow \mathbb{G}_m)$$

the associated norm one torus. The failure of the Hasse norm principle for K/k is completely controlled by the Tate-Shafarevich group $\text{III}(R_{K/k}^1 \mathbb{G}_m)$, in the sense that K/k fails the Hasse norm principle if and only if $\text{III}(R_{K/k}^1 \mathbb{G}_m) \neq 0$ (see Section 6.1). In particular, for G as in Theorem 1.4, a positive proportion of the tori $R_{K/k}^1 \mathbb{G}_m$ have non-trivial Tate-Shafarevich group. Note that non-isomorphic Galois extensions give rise to non-isomorphic norm one tori (see Proposition 6.3), hence it makes sense to count such tori by the discriminant of the associated extension.

From the viewpoint of norm one tori, another interesting problem is to study the failure of weak approximation for the tori $R_{K_\varphi/k}^1 \mathbb{G}_m$ as φ varies over all G -extensions of k . Recall that a variety X over a number field k is said to satisfy weak approximation if $X(k)$ is dense in $\prod_v X(k_v)$ for the product topology. Here we have the following simple group theoretic criterion, which gives a complete answer to this problem.

Theorem 1.5. *Let G be a non-trivial finite abelian group and let Q be the smallest prime dividing $|G|$. Then as φ varies over all G -extensions of k , the following hold.*

- (1) *If the Q -Sylow subgroup of G is cyclic, then a positive proportion of the tori $R_{K_\varphi/k}^1 \mathbb{G}_m$ satisfy weak approximation.*
- (2) *If the Q -Sylow subgroup of G is not cyclic, then 0% of the tori $R_{K_\varphi/k}^1 \mathbb{G}_m$ satisfy weak approximation.*

In particular, Theorem 1.5 gives examples of G for which 100% of the tori $R_{K/k}^1 \mathbb{G}_m$ fail weak approximation. Results of this type were recently obtained in [9], where the authors gave examples of families of varieties for which 100% of the members which are everywhere locally soluble fail weak approximation. Our set-up is slightly different to [9], however, as there the authors dealt with families of varieties ordered by height, where the family could contain many isomorphic fibres, whereas here we only count each isomorphism class over k once. (To be more precise, we count each isomorphism class exactly $|\text{Aut}(G)|$ times, but this is clearly equivalent.)

In [9] it was left open whether there exist families of varieties for which both a positive proportion of the everywhere locally soluble members satisfy weak approximation and a positive proportion also fail weak approximation. We are able to give examples which satisfy this condition, at least in our setting. These are obtained by combining Theorem 1.5 with the following result.

Theorem 1.6. *Let G be a finite abelian non-cyclic group. Then as φ varies over all G -extensions of k , the following hold.*

- (1) *A positive proportion of the K_φ/k satisfy the Hasse norm principle.*
- (2) *A positive proportion of the tori $R_{K_\varphi/k}^1 \mathbb{G}_m$ fail weak approximation.*

Note that Theorem 1.6 implies the existence of some Galois extension K/k with Galois group isomorphic to G for which $R_{K/k}^1 \mathbb{G}_m$ fails weak approximation; something which is by no means obvious.

For any group as in Theorem 1.4, by Theorem 1.6 we also obtain examples of families of fields for which a positive proportion of the members satisfy the Hasse norm principle and also a positive proportion fail the Hasse norm principle. This result should be compared with work of Bhargava [4], which shows that a positive proportion of cubic curves fail the Hasse principle, and a positive proportion also satisfy the Hasse principle.

1.3. Counting with local conditions. To prove our quantitative results, we require a theorem concerning counting abelian extensions with infinitely many local conditions imposed. This is Theorem 1.7 below, which is in some respects our main result. It states general conditions under which one may obtain the existence of a positive proportion of abelian extensions which satisfy infinitely many local conditions.

In order to state the result, we will need some more notation. 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 $\text{Gal}(\bar{F}/F) \rightarrow G$. 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 $\text{Gal}(L/F) \rightarrow G$.

For every place v of the number field k , we fix an algebraic closure \bar{k}_v and an embedding of \bar{k} into \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 $\Lambda := (\Lambda_v)_v$ we study the function

$$N(k, G, \Lambda, B) := \#\{\varphi \in G\text{-ext}(k) : \Delta(\varphi) \leq B, \varphi_v \in \Lambda_v \forall v\}, \quad (1.2)$$

which counts those G -extensions of k of bounded discriminant which satisfy the local conditions imposed by Λ .

Let Q be the smallest prime dividing $|G|$ and let $\phi_Q(G)$ be the number of elements of order Q in G . Denote by μ_Q the group of Q th roots of unity in \bar{k} and set

$$\alpha(G) := |G|(1 - Q^{-1}), \quad \nu(k, G) := \phi_Q(G)/[k(\mu_Q) : k]. \quad (1.3)$$

Note that $\alpha(G), \nu(k, G) \in \mathbb{N}$. Our main result is the following.

Theorem 1.7. *Let G be a non-trivial finite abelian group and let Q be the smallest prime dividing $|G|$. For each place v of k , let Λ_v be a set of sub- G -extensions of k_v and let $\Lambda := (\Lambda_v)_v$. Assume that for almost all places v ,*

$$\begin{aligned} & \text{the set } \Lambda_v \text{ contains all sub-}G\text{-extensions } (K_v/k_v, \psi_v) \text{ for which} \\ & \text{the inertia group of } K_v/k_v \text{ has order dividing } Q. \end{aligned} \quad (1.4)$$

Furthermore, suppose that there exists some G -extension φ of k such that $\varphi_v \in \Lambda_v$ for all v . Then there is $\gamma > 0$ and a real polynomial P of degree $\nu(k, G) - 1$ with positive leading coefficient, such that we have an asymptotic formula

$$N(k, G, \Lambda, B) = B^{1/\alpha(G)} P(\log B) + O(B^{1/\alpha(G)-\gamma}), \quad B \rightarrow \infty.$$

Note that Theorem 1.7 implies the existence of a positive proportion of G -extensions of k satisfying the infinitely many local conditions imposed by Λ .

At first sight, the appearance of Condition (1.4) in Theorem 1.7 may seem surprising. Yet there is a simple heuristic explanation for its presence. Namely, since we are ordering field extensions by their discriminants, the asymptotic behaviour is controlled by the ‘‘mildly’’ ramified G -extensions. Condition (1.4) says that provided one counts extensions with small inertia groups, one obtains enough G -extensions of small discriminant to guarantee a positive proportion of all G -extensions. Theorem 5.1 also illustrates that the conclusion of Theorem 1.7 can fail if the local conditions Λ_v do not satisfy (1.4).

One of the main difficulties in the proof of Theorem 1.7 is that, in general, the leading constant occurring in the asymptotic formula for $N(k, G, \Lambda, B)$ is an *infinite* alternating sum of Euler products (see (4.13)). We have to work quite hard to show that this infinite sum converges absolutely and that it is non-zero. In order to prove this non-vanishing, it is crucial in Theorem 1.7 that we assume the existence of *some* G -extension which realises all the local conditions imposed by Λ ; there even exist *finite* sets of local conditions which are not realised by any G -extension of k , as first noticed by Wang [35] in his counter-example to Grunwald’s ‘‘theorem’’.

1.4. Proof strategy. We now explain some of the methods used in this paper.

Counting with local conditions. Our approach to counting abelian extensions of bounded discriminant is based upon the work of Wright [37], who provided the definitive result on counting abelian extensions of bounded discriminant, building upon numerous special cases handled by other authors [14], [33], [22], [1], [2], [31] [32], [38], [23]. Like Wright, we proceed by studying the discriminant zeta function

$$\sum_{\varphi} \frac{1}{\Delta(\varphi)^s}, \quad \operatorname{Re} s \gg 1, \quad (1.5)$$

where the sum is over suitable G -extensions of k . We relate the analytic properties of such zeta functions to the original counting problem via standard Tauberian theorems (e.g. [12, Thm. A.1]). Wright’s method uses class field theory to translate the problem of counting G -extensions of k into a problem concerning the ideles of k . Note that Wright considered the slightly different problem of counting Galois extensions K/k inside \bar{k} with Galois group isomorphic to G , without specifying the isomorphism. We include the choice of isomorphism as part of the data as it required for our applications, leads to a more natural framework, and also simplifies some parts of the proof.

There are a few differences between our approach and Wright’s. First, we replace some of the ad hoc steps in his paper by more conceptual methods, namely harmonic analysis on the idele class group. This new approach leads to a more powerful and versatile framework. This is for more than just aesthetic purposes; it is exactly the tools from harmonic analysis which allow us to count number fields with infinitely many local conditions, via a version of the Poisson summation formula. This approach is inspired, at least on a philosophical level, by the harmonic analysis approach to Manin’s conjecture for toric varieties, as pioneered by Batyrev and Tschinkel [3]. Next, at numerous points Wright uses the “fact” that the map

$$k^*/k^{*n} \rightarrow \mathbf{A}_k^*/\mathbf{A}_k^{*n},$$

is injective for all $n \in \mathbb{N}$; see for instance the claim just before [37, Lem. 3.1] and the discussion following [37, Prop. 4.1]. This is not true in general, as first noticed by Wang [35] (see [27, Ch. IX.1] for a modern account). Our harmonic analysis approach highlights where these mistakes occur and moreover shows why they do not affect Wright’s main result (see e.g. the proof of Proposition 3.8).

Hasse norm principle and weak approximation. In order to apply our counting results to the study of the Hasse norm principle, we use a theorem of Tate which explicitly calculates the Tate-Shafarevich group of the associated norm one torus (see Theorem 6.1). Whilst this gives a complete criterion to check whether a given Galois extension satisfies the Hasse norm principle, part of the difficulty with combining this with our counting results is that, in general, this criterion is not a simple collection of independent local conditions, i.e., different places may interfere with each other. However, in Section 6 we use Tate’s theorem to obtain both necessary and sufficient collections of independent local conditions for the Hasse norm principle to hold, and it is these conditions that turn out to be susceptible to our counting methods. Note that these difficulties do not arise for the question of weak approximation: it turns out that the problem of whether

$R_{K/k} \mathbb{G}_m^1$ satisfies weak approximation *is* completely controlled by independent local conditions when K/k is abelian (see Lemma 6.7).

1.5. Concluding remarks. We hope that the tools and results developed in this paper for counting abelian extensions with infinitely many local conditions imposed may be of independent interest. Indeed, for many applications it is often necessary to count extensions with imposed local conditions, e.g. counting only those extensions for which certain primes have some given splitting behaviour. Analogous results have recently been obtained for extensions of degrees $d \in \{2, 3, 4, 5\}$ with Galois group S_d and fairly general local conditions by Bhargava [5]. Wright also has a result [37, Thm. 1.4] on counting abelian extensions with a *single* local condition and there is, moreover, work of Wood [36] on counting abelian extensions of *bounded conductor* with finitely many local conditions imposed. However, the authors know of no previously existing work where general abelian extensions have been successfully counted with *infinitely* many non-trivial local conditions.

We finish by discussing possible further directions. First, as in Wright's paper, our methods should extend to global fields, providing that one avoids suitable characteristics as Wright does. Secondly, in this paper we have focused on counting abelian extensions by *discriminant*, in order to put the problem into a more general framework. Another natural problem would be to instead count abelian extensions of bounded *conductor*, by combining our harmonic analysis methods with the approach of Wood [36]. Thirdly, one could try to improve Theorem 1.1 from a zero density result to a precise asymptotic formula; even the biquadratic case appears to be non-trivial. Finally, there is a wealth of literature on counting number fields of bounded discriminant. It would be interesting to see if these tools could be adapted to count failures of the Hasse norm principle for some non-abelian extensions.

1.6. Outline of the paper. Sections 2 and 3 are devoted to setting up our general framework for counting abelian extensions. In particular, we use class field theory to translate the problem to the study of certain conductor series, which we explain how to attack using tools from harmonic analysis in Section 3.

Section 4 is the technical heart of the paper. Here we use the general tools developed in the previous two sections to prove Theorem 1.7, which is in some respects our main theorem. Section 5 contains some applications of Theorem 1.7 which will be used in our later proofs.

In Section 6, we finish by proving the remaining theorems stated in the introduction. These are obtained by combining various algebraic and cohomological calculations with suitable applications of Theorem 1.7 and the results from Section 5.

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

\mathbf{A}^*	the ideles of k
\mathcal{O}_k	the ring of integers of k
Ω_k	the set of all places of k
Ω_∞	the set of all archimedean places of k

Ω_L or $\Omega(L)$	the set of all places of a finite extension L of k
S	a finite set of places of k
\mathcal{O}_S	the S -integers of k
\mathbf{A}_S^* or $\mathbf{A}^*(S)$	the S -ideles of k , $\mathbf{A}_S^* := \prod_{v \in S} k_v^* \prod_{v \notin S} \mathcal{O}_v^*$
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 $\mathcal{O}_v := k_v$
π_v	a uniformiser at a finite place v
q_v	the cardinality of the residue field at a finite place v
K	a Galois extension of k
K_v	the completion of K at some choice of place above v
D_v	the Galois group of K_v/k_v
I_v	the inertia group of K_v/k_v

For a Dedekind domain R , we use the following notation.

$I(R)$	the group of non-zero fractional ideals of R
$P(R)$	the subgroup of principal ideals in $I(R)$
$\text{Pic}(R)$	the ideal class group of R , $\text{Pic}(R) := I(R)/P(R)$

All locally compact abelian groups in this paper are assumed to be Hausdorff. For locally compact abelian groups A and B , we use the following notation.

$\text{Hom}(A, B)$	the group of <i>continuous</i> homomorphisms from A to B , equipped with the compact-open topology
S^1	the unit circle
μ_n	the group of n th roots of unity
A^\wedge	the Pontryagin dual of A , $A^\wedge := \text{Hom}(A, S^1)$
A^\sim	the \mathbb{Q}/\mathbb{Z} -dual of A , $A^\sim := \text{Hom}(A, \mathbb{Q}/\mathbb{Z})$
$\langle \cdot, \cdot \rangle$	the natural pairing $A \times A^\wedge \rightarrow S^1$

If B is finite or $B = S^1$, then $\text{Hom}(A, B)$ is itself a locally compact abelian group (this is a special case of [25, Cor., p. 377]).

If B is a closed subgroup of A , then we identify $(A/B)^\wedge$ with the subgroup B^\perp of characters of A^\wedge that are trivial on B . We view k^* and k_v^* as closed subgroups of the locally compact abelian group \mathbf{A}^* . The induced topology on k^* is discrete. For a finite abelian group G and $x \in k^* \otimes G$, we write x_v for its image under the natural map $k^* \otimes G \rightarrow k_v^* \otimes G$ induced by the natural inclusion $k^* \rightarrow k_v^*$; note that this former map is not injective in general.

For a finite abelian group G endowed with the discrete topology, we use the following notation.

$ G $	the order of G
$\exp(G)$	the exponent of G
Q	the smallest prime dividing $ G $
$\phi_Q(G)$	the number of elements of order Q in G
$\beta_G := \log_Q(\phi_Q(G) + 1)$	
$\alpha(G) := G (1 - Q^{-1})$	

$$\nu(k, G) := \phi_Q(G)/[k(\mu_Q) : k]$$

Every finite abelian group G may be written uniquely, up to reordering, as

$$G = \mathbb{Z}/n_1\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/n_l\mathbb{Z}, \quad (1.6)$$

with $n_j > 1$ and $n_{j+1} \mid n_j$ for $1 \leq j < l$. We reserve the variables n_1, \dots, n_l for the above notation throughout the paper.

For a commutative group scheme X over a number field k , we denote by

$$\text{III}(k, X) := \ker \left(\text{H}^1(k, X) \rightarrow \prod_v \text{H}^1(k_v, X) \right) \quad (1.7)$$

the Tate-Shafarevich group of X . We shall often omit k if it is clear. The non-zero elements of $\text{III}(k, X)$ classify those X -torsors which fail the Hasse principle.

Given a set X , we denote by $\mathbb{1}_X : X \rightarrow \{1\}$ the constant function with value 1 (we shall often omit the subscript if it is clear from the context).

Given $a, b \in \mathbb{Z}$, we write (a, b) for their greatest common divisor.

1.8. Acknowledgements. Part of this work was completed whilst attending the *Rational points 2015* workshop – we thank Michael Stoll for providing such a stimulating working environment. We thank Jeremy Rickard and Norbert Hoffmann for useful discussions, and are grateful to Manjul Bhargava and Melanie Matchett Wood for their interest in our paper. We also thank Jean-Louis Colliot-Thélène for useful comments and references, and the referees for helpful remarks.

2. FROM DISCRIMINANT SERIES TO CONDUCTOR SERIES

Let k be a number field and let G be a non-trivial finite abelian group. We begin by describing our set-up for counting G -extensions of k and the transition to the study of conductor series. This closely follows [37, §2], though unlike Wright we do not choose a presentation of G .

2.1. Discriminant series. Let f be any complex-valued function on the set of sub- G -extensions of k . Consider the (formal, for now) Dirichlet series

$$D_{G,f}(s) := \sum_{\varphi \in G\text{-ext}(k)} \frac{f(\varphi)}{\Delta(\varphi)^s}. \quad (2.1)$$

Since G is abelian, global class field theory allows us to identify G -extensions of k with surjective continuous homomorphisms $\mathbf{A}^*/k^* \rightarrow G$, where G is endowed with the discrete topology. The conductor-discriminant formula gives

$$D_{G,f}(s) = \sum_{\varphi \in G\text{-ext}(k)} f(\varphi) \prod_{\psi \in (\mathbf{A}^*/\ker \varphi)^\wedge} \Phi(\psi)^{-s}, \quad (2.2)$$

where $\Phi(\psi)$ is the reciprocal of the idelic norm of the conductor of ψ . To deal with the rather unpleasant surjectivity condition, we introduce certain conductor series.

2.2. Conductor series. Let X be one of the following locally compact abelian groups: the group \mathbf{A}^* of ideles, the idele class group \mathbf{A}^*/k^* , the local multiplicative group k_v^* at the place v of k , or the local unit group \mathcal{O}_v^* at v . In each case, the conductor of a character $\psi \in X^\wedge$ of finite order is defined as the conductor of its kernel. Let us denote by $\Phi(\psi)$ the reciprocal of the (idelic or v -adic) norm of this conductor.

Let H be a finite abelian group endowed with the discrete topology, and let $\chi \in \text{Hom}(X, H)$. The kernel of χ is a finite-index open subgroup of X . By Pontryagin duality, we obtain from χ a canonical surjective homomorphism

$$\widehat{\chi} : H^\wedge \rightarrow (X/\ker \chi)^\wedge.$$

We define

$$\Phi_H(\chi) := \prod_{h \in H^\wedge} \Phi(\widehat{\chi}(h)) = \prod_{\psi \in (X/\ker \chi)^\wedge} \Phi(\psi)^{|H|/|X/\ker \chi|}. \quad (2.3)$$

Note that there is a natural inclusion $\text{Hom}(\mathbf{A}^*/k^*, H) \subseteq \text{Hom}(\mathbf{A}^*, H)$, and for any $\chi \in \text{Hom}(\mathbf{A}^*/k^*, H)$, the two corresponding definitions (2.3) of $\Phi_H(\chi)$ coincide. In the case where $X = \mathbf{A}^*$, we have a restricted direct product

$$\text{Hom}(\mathbf{A}^*, H) = \lim_{S \rightarrow \Omega_k} \text{Hom}(\mathbf{A}^*, H)(S) \quad (2.4)$$

(see e.g. [24, Thm. 1.7]), where

$$\text{Hom}(\mathbf{A}^*, H)(S) := \prod_{v \in S} \text{Hom}(k_v^*, H) \times \prod_{v \notin S} \text{Hom}(k_v^*/\mathcal{O}_v^*, H).$$

Note that $\text{Hom}(k_v^*, H)$ is finite and discrete, and coincides with the group of abstract group homomorphisms $k_v^* \rightarrow H$. Moreover, $\text{Hom}(k_v^*/\mathcal{O}_v^*, H)$ may be identified with those homomorphisms $k_v^* \rightarrow H$ which are trivial on \mathcal{O}_v^* . Here for archimedean v , by convention we set $\mathcal{O}_v^* = k_v^*$. For non-archimedean v , a choice of uniformiser in k_v yields an isomorphism

$$\text{Hom}(k_v^*, H) \cong \text{Hom}(k_v^*/\mathcal{O}_v^*, H) \oplus \text{Hom}(\mathcal{O}_v^*, H). \quad (2.5)$$

For $\chi_1 \in \text{Hom}(k_v^*/\mathcal{O}_v^*, H)$ and $\chi_2 \in \text{Hom}(k_v^*, H)$, we have $\Phi_H(\chi_1 \chi_2) = \Phi_H(\chi_2)$. Let $\chi = (\chi_v)_v \in \text{Hom}(\mathbf{A}^*, H)$, where $\chi_v \in \text{Hom}(k_v^*, H)$. Then $\Phi_H(\chi_v) = 1$ for all but finitely many v , and

$$\Phi_H(\chi) = \prod_v \Phi_H(\chi_v).$$

We are now ready to define the conductor series

$$F_{H,f}(s) := \sum_{\chi \in \text{Hom}(\mathbf{A}^*/k^*, H)} \frac{f(\chi)}{\Phi_H(\chi)^s}. \quad (2.6)$$

Lemma 2.1. *For any subgroup H of G , we have*

$$F_{H,f}(s) = \sum_{J \subseteq H} D_{J,f}(s|H|/|J|),$$

where the sum runs over all subgroups J of H . The series $D_{J,f}(s)$ is defined as in (2.1), but with G replaced by J .

Proof. If the image of $\chi \in \text{Hom}(\mathbf{A}^*/k^*, H)$ is a subgroup J of H , then

$$\Phi_H(\chi) = \prod_{\psi \in (\mathbf{A}^*/\ker \chi)^\wedge} \Phi(\psi)^{|H|/|J|}.$$

Now sort the homomorphisms $\chi \in \text{Hom}(\mathbf{A}^*/k^*, H)$ by their images. \square

2.3. Möbius inversion. 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 $n \in \mathbb{N}$.

Lemma 2.2. *We have*

$$D_{G,f}(s) = \sum_{H \subseteq G} \mu(G/H) F_{H,f}(s|G|/|H|),$$

where the sum runs over all subgroups H of G .

Proof. This is Delsarte's inversion formula [17], applied as in [37, Section 2]. \square

3. HARMONIC ANALYSIS

In the previous section, we reduced the study of our problem to the study of various conductor series. We shall tackle these using tools from harmonic analysis. The main result of this section is Proposition 3.8, which is a version of Poisson summation. Throughout this section we work over a number field k and with a finite abelian group G endowed with the discrete topology; note that in later sections we shall also apply the following results to subgroups H of a given discrete finite abelian group G .

We will assume that the reader is familiar with the basic definitions and tools from abstract harmonic analysis on locally compact abelian groups. A detailed treatment can be found in [6, Ch. 2]. For a general overview, see [24, §1.1].

3.1. Topological considerations. We begin our analysis with some topological considerations. In this paper, we will need to consider certain tensor products of topological groups. This theory can be quite complicated in general; see for example [19] and [25]. However, we will only require this theory in some special cases where everything is well-behaved, which we now explain.

Our first result may be viewed as a generalisation of [25, Cor., p. 386].

Lemma 3.1. *Let X be a locally compact abelian group. Let $n \in \mathbb{N}$ and assume that nX is a closed subgroup of X . Then there is a canonical isomorphism*

$$\text{Hom}(X, \mu_n)^\wedge \cong X/nX$$

of locally compact abelian groups, where X/nX is equipped with the quotient topology.

Proof. As $nX \subset X$ is closed, we have

$$(nX)^\perp \cong (X/nX)^\wedge.$$

However, by definition we have

$$\text{Hom}(X, \mu_n) = \{\chi \in X^\wedge : \chi^n = 1\} = (nX)^\perp.$$

Applying Pontrygin duality, we obtain the result. \square

For many locally compact abelian groups X , the subgroup $nX \subset X$ is closed for all $n \in \mathbb{N}$. For example, this is the case if X is compact or discrete. This property is closed under arbitrary direct products and direct sums (but not under restricted direct products, in general). Moreover, an elementary argument shows that nX is a closed subgroup for all $n \in \mathbb{N}$ when $X = \mathbf{A}^*$ or $X = \mathbf{A}^*/k^*$. These cases will be sufficient for all the applications required in this paper.

Lemma 3.2. *Let X be a locally compact abelian group and let G be a finite abelian group. Assume that nX is a closed subgroup of X for all $n \mid |G|$. Then there is a canonical isomorphism*

$$\mathrm{Hom}(X, G)^\wedge \cong X \otimes G^\wedge$$

of abelian groups.

Here $X \otimes G^\wedge$ denotes the usual tensor product of X with G^\wedge , considered as abelian groups (i.e. forgetting the topology on X).

Proof. Consider the natural homomorphism

$$X \otimes G^\wedge \rightarrow \mathrm{Hom}(X, G)^\wedge, \quad x \otimes \chi \mapsto ((\phi : X \rightarrow G) \mapsto \chi(\phi(x)))$$

(a simple calculation shows that the induced homomorphism $\mathrm{Hom}(X, G) \rightarrow S^1$ is indeed continuous). To show that this is an isomorphism, it suffices to treat the case where $G = \mu_n$. Here we obtain the following commutative diagram

$$\begin{array}{ccc} X \otimes \mathbb{Z}/n\mathbb{Z} & \longrightarrow & \mathrm{Hom}(X, \mu_n)^\wedge \\ & \searrow & \uparrow \\ & & X/nX. \end{array}$$

The diagonal arrow is the usual isomorphism of abelian groups, and the vertical arrow is the isomorphism of Lemma 3.1. This proves the result. \square

Let X be as in Lemma 3.2. Then Lemma 3.2 canonically identifies the Pontryagin dual of $\mathrm{Hom}(X, G)$ with $X \otimes G^\wedge$, as an abelian group. Since $\mathrm{Hom}(X, G)^\wedge$ carries a topology, we may use this isomorphism to equip $X \otimes G^\wedge$ with the structure of a locally compact abelian group. Lemma 3.1 gives a very simple way to visualise the topology on $X \otimes G^\wedge$, on choosing a presentation of G . For example, if X is discrete then we see that $X \otimes G^\wedge$ is also discrete.

Henceforth, for X as in Lemma 3.2, we identify $X \otimes G^\wedge$ with the Pontryagin dual of $\mathrm{Hom}(X, G)$, viewed as locally compact abelian groups. We denote by

$$\langle \cdot, \cdot \rangle : \mathrm{Hom}(X, G) \times (X \otimes G^\wedge) \rightarrow S^1$$

the pairing induced by Pontryagin duality.

3.2. Haar Measures. We now return to the study of $\mathrm{Hom}(\mathbf{A}^*, G)$, beginning with a choice of normalisation for its Haar measure. For each place v , we equip $\mathrm{Hom}(k_v^*, G)$ with the unique Haar measure $d\chi_v$ such that

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

For archimedean v this is simply the counting measure (as $\mathcal{O}_v^* = k_v^*$ by convention), whilst for non-archimedean v the measure $d\chi_v$ is a factor of

$$\frac{1}{\#\mathrm{Hom}(k_v^*/\mathcal{O}_v^*, G)} = \frac{1}{|G|}$$

times the counting measure. Recalling the restricted product description (2.4) of $\mathrm{Hom}(\mathbf{A}^*, G)$, one easily sees that the product of these Haar measures converges to give a Haar measure $d\chi$ on $\mathrm{Hom}(\mathbf{A}^*, G)$.

3.3. Fourier transforms. Throughout this section, for each place v we let $f_v : \mathrm{Hom}(k_v^*, G) \rightarrow \mathbb{C}$ be functions which take only the value 1 on $\mathrm{Hom}(k_v^*/\mathcal{O}_v^*, G)$ for all but finitely many v . The product $f = \prod_v f_v : \mathrm{Hom}(\mathbf{A}^*, G) \rightarrow \mathbb{C}$ is then a well-defined continuous function. For $s \in \mathbb{C}$, $x_v \in k_v^* \otimes G^\wedge$ and $x = (x_v)_v \in \mathbf{A}^* \otimes G^\wedge$, we denote by

$$\widehat{f}_v(x_v; s) = \int_{\chi_v \in \mathrm{Hom}(k_v^*, G)} \frac{f_v(\chi_v) \langle \chi_v, x_v \rangle}{\Phi_G(\chi_v)^s} d\chi_v, \quad \widehat{f}(x; s) = \int_{\chi \in \mathrm{Hom}(\mathbf{A}^*, G)} \frac{f(\chi) \langle \chi, x \rangle}{\Phi_G(\chi)^s} d\chi$$

the local and global Fourier transforms of the function $f\Phi_G^{-s}$, respectively, if they exist. Here, as explained in Section 3.1, we are identifying $\mathbf{A}^* \otimes G^\wedge$ and $k_v^* \otimes G^\wedge$ with the Pontryagin duals of $\mathrm{Hom}(\mathbf{A}^*, G)$ and $\mathrm{Hom}(k_v^*, G)$, respectively, and denote by $\langle \cdot, \cdot \rangle$ the pairing induced by Pontryagin duality. We first calculate the local Fourier transforms at almost all places. Let v be non-archimedean. Note that, by our choice of measures, we have

$$\widehat{f}_v(x_v; s) = \frac{1}{|G|} \sum_{\chi_v \in \mathrm{Hom}(k_v^*, G)} \frac{f_v(\chi_v) \langle \chi_v, x_v \rangle}{\Phi_G(\chi_v)^s}.$$

Recalling (2.5), for $x_v \in k_v^* \otimes G^\wedge$ and $\chi_v \in \mathrm{Hom}(\mathcal{O}_v^*, G)$ we define the ‘‘average’’

$$\tau_{f_v}(\chi_v, x_v) := \frac{1}{|G|} \sum_{\psi_v \in \mathrm{Hom}(k_v^*/\mathcal{O}_v^*, G)} f_v(\chi_v \psi_v) \langle \psi_v, x_v \rangle.$$

Lemma 3.3. *Let v be a non-archimedean place of k such that $(\exp(G), q_v) = 1$. Then for $x_v \in k_v^* \otimes G^\wedge$ we have*

$$\widehat{f}_v(x_v; s) = \sum_{m | (\exp(G), q_v - 1)} \left(\sum_{\substack{\chi_v \in \mathrm{Hom}(\mathcal{O}_v^*, G) \\ \ker \chi_v = \mathcal{O}_v^{*m}}} \langle \chi_v, x_v \rangle \tau_{f_v}(\chi_v, x_v) \right) q_v^{-|G|(1-1/m)s}.$$

Proof. This is inspired by the proof of [37, Prop. 4.1]. From (2.5), we obtain

$$\widehat{f}_v(x_v; s) = \sum_{\chi_v \in \mathrm{Hom}(\mathcal{O}_v^*, G)} \frac{\langle \chi_v, x_v \rangle}{\Phi_G(\chi_v)^s} \tau_{f_v}(\chi_v, x_v).$$

Let $\chi_v \in \mathrm{Hom}(\mathcal{O}_v^*, G)$. Since q_v is coprime to $\exp(G)$, we get $1 + \pi_v \mathcal{O}_v \subseteq \ker \chi_v$. Hence, χ_v factors through the units of the residue field, so $\ker \chi_v = \mathcal{O}_v^{*m}$ for some divisor m of $(\exp(G), q_v - 1)$. Hence, sorting the χ_v by their kernels,

$$\widehat{f}_v(x_v; s) = \sum_{m | (\exp(G), q_v - 1)} \sum_{\substack{\chi_v \in \mathrm{Hom}(\mathcal{O}_v^*, G) \\ \ker \chi_v = \mathcal{O}_v^{*m}}} \frac{\langle \chi_v, x_v \rangle}{\Phi_G(\chi_v)^s} \tau_{f_v}(\chi_v, x_v).$$

For $\chi_v \in \text{Hom}(\mathcal{O}_v^*, G)$ with $\ker \chi_v = \mathcal{O}_v^{*m}$, we have

$$\Phi_G(\chi_v) = \prod_{\chi \in (\mathcal{O}_v^*/\mathcal{O}_v^{*m})^\wedge} \Phi(\chi)^{|G|/m} = q_v^{|G| \frac{m-1}{m}}.$$

Indeed, the trivial character $\mathbb{1}$ has $\Phi(\mathbb{1}) = 1$, and the other $m - 1$ characters χ have conductor π_v , so $\Phi(\chi) = q_v$. \square

We now establish rapid decay for the local Fourier transforms, which will be used to guarantee the convergence of the Poisson summation formula. Furthermore, we show that if f is suitably nice, then the local Fourier transforms are often zero. In the next lemma, we let $\alpha(G)$ be as in (1.3).

Lemma 3.4. *Let v be a non-archimedean place of k such that $(\exp(G), q_v) = 1$ and such that $f_v(\text{Hom}(k_v^*/\mathcal{O}_v^*, G)) = 1$. Let $\gamma = \max\{|f_v(\chi_v)|\}$ be the maximum taken over all $\chi_v \in \text{Hom}(k_v^*, G)$. Then*

$$\widehat{f}_v(x_v; s) = \begin{cases} 1 + O_\gamma(q_v^{-\alpha(G)s}), & x_v \in \mathcal{O}_v^* \otimes G^\wedge, \\ O_\gamma(q_v^{-\alpha(G)s}), & x_v \notin \mathcal{O}_v^* \otimes G^\wedge. \end{cases}$$

Moreover, if f_v is $\text{Hom}(k_v^*/\mathcal{O}_v^*, G)$ -invariant and $x_v \notin \mathcal{O}_v^* \otimes G^\wedge$, then

$$\widehat{f}_v(x_v; s) = 0.$$

Proof. For $x_v \in \mathcal{O}_v^* \otimes G^\wedge$, the result follows easily from the calculation of the lower order terms in Lemma 3.3. Henceforth, let $x_v \notin \mathcal{O}_v^* \otimes G^\wedge$. Then by character orthogonality we have

$$\tau_{f_v}(\mathbb{1}_v, x_v) = 0,$$

where $\mathbb{1}_v : \mathcal{O}_v^* \rightarrow G$ denotes the trivial homomorphism. The first part of the lemma now follows easily from Lemma 3.3. Under the additional assumption that f_v is $\text{Hom}(k_v^*/\mathcal{O}_v^*, G)$ -invariant, we similarly obtain

$$\tau_{f_v}(\chi_v, x_v) = 0$$

for all $\chi_v \in \text{Hom}(\mathcal{O}_v^*, G)$. The result then follows from Lemma 3.3. \square

We now show the existence of the global Fourier transform and an Euler product formula under suitable assumptions.

Lemma 3.5. *Assume that there exists some $\gamma > 0$ such that $|f_v(\chi_v)| \leq \gamma$ for all places v and all $\chi_v \in \text{Hom}(k_v^*, G)$. Then, in the half plane $\text{Re } s > 1/\alpha(G)$, the global Fourier transform $\widehat{f}(\cdot; s)$ of $f\Phi_G^{-s}$ defines a holomorphic function and*

$$\widehat{f}((x_v)_v; s) = \prod_v \widehat{f}_v(x_v; s), \quad \text{Re } s > 1/\alpha(G).$$

Proof. It follows easily from Lemma 3.4 that the above infinite product is absolutely convergent for $\text{Re } s > 1/\alpha(G)$. The result then follows from a standard argument (see e.g. [24, Lem. 1.4]). \square

3.4. Poisson summation. The main result of this section is a version of Poisson summation applied to the conductor series. We begin with an algebraic lemma. For x in $k^* \otimes G^\wedge$, we denote its image in $k_v^* \otimes G^\wedge$ by x_v .

Lemma 3.6. *Let S be a finite set of places of k and let*

$$\mathcal{U}_S(G) = \{x \in k^* \otimes G^\wedge : x_v \in \mathcal{O}_v^* \otimes G^\wedge \ \forall v \notin S\}. \quad (3.1)$$

Then there is an exact sequence of abelian groups

$$1 \rightarrow \mathcal{O}_S^* \otimes G^\wedge \rightarrow \mathcal{U}_S(G) \rightarrow \mathrm{Tor}(\mathrm{Pic} \mathcal{O}_S, G^\wedge) \rightarrow 1.$$

In particular, $\mathcal{U}_S(G)$ is finite.

Proof. Denote by $I(\mathcal{O}_S)$ the group of non-zero fractional ideals of \mathcal{O}_S , and denote by $P(\mathcal{O}_S)$ the subgroup generated by the principal ideals. Note that $\mathrm{Tor}(I(\mathcal{O}_S), G) = \mathrm{Tor}(P(\mathcal{O}_S), G) = 0$. Therefore, we have the following commutative diagram of abelian groups

$$\begin{array}{ccccccc} 0 & \longrightarrow & \mathbf{A}_S^* \otimes G^\wedge & \longrightarrow & \mathbf{A}^* \otimes G^\wedge & \longrightarrow & I(\mathcal{O}_S) \otimes G^\wedge \longrightarrow 0 \\ & & \uparrow & & \uparrow & & \uparrow \\ 0 & \longrightarrow & \mathcal{O}_S^* \otimes G^\wedge & \longrightarrow & k^* \otimes G^\wedge & \longrightarrow & P(\mathcal{O}_S) \otimes G^\wedge \longrightarrow 0 \\ & & & & & & \uparrow \\ & & & & & & \mathrm{Tor}(\mathrm{Pic} \mathcal{O}_S, G^\wedge) \\ & & & & & & \uparrow \\ & & & & & & 0 \end{array}$$

with exact rows and columns. The result then follows from a simple diagram chase. \square

The following lemma will be used to show convergence of the Poisson sum.

Lemma 3.7. *Let $g_v : k_v^* \otimes G^\wedge \rightarrow \mathbb{C}$ for each place v of k . Assume that there exists some $\sigma > 1$ such that*

$$g_v(x_v) = \begin{cases} 1 + O(q_v^{-\sigma}), & x_v \in \mathcal{O}_v^* \otimes G^\wedge, \\ O(q_v^{-\sigma}), & x_v \notin \mathcal{O}_v^* \otimes G^\wedge. \end{cases}$$

Then $g = \prod_v g_v : \mathbf{A}^ \otimes G^\wedge \rightarrow \mathbb{C}$ is well defined and the sum*

$$\sum_{x \in k^* \otimes G^\wedge} g(x)$$

is absolutely convergent.

Proof. That g is well defined is clear. Choose some finite set of places S such that $\mathrm{Pic} \mathcal{O}_S = 0$. Let $I(\mathcal{O}_S)$ denote the group of non-zero fractional ideals of \mathcal{O}_S . Then, since $\mathrm{Tor}(I(\mathcal{O}_S), G^\wedge) = 0$, we have the following short exact sequence

$$1 \rightarrow \mathcal{O}_S^* \otimes G^\wedge \rightarrow k^* \otimes G^\wedge \rightarrow I(\mathcal{O}_S) \otimes G^\wedge \rightarrow 1.$$

Let \mathcal{R} be a system of representatives for the cosets of $\mathcal{O}_S^* \otimes G^\wedge$ in $k^* \otimes G^\wedge$. This allows us to write

$$\sum_{x \in k^* \otimes G^\wedge} |g(x)| = \sum_{u \in \mathcal{O}_S^* \otimes G^\wedge} \sum_{r \in \mathcal{R}} |g(ur)|.$$

It now follows from Dirichlet's S -unit theorem and our assumptions on g that there exists some constant $\gamma > 0$ and some $0 < \varepsilon < \sigma - 1$ such that

$$\sum_{x \in k^* \otimes G^\wedge} |g(x)| \ll \sum_{r \in \mathcal{R}} \prod_{\substack{v \notin S \\ r_v \in \mathcal{O}_v^* \otimes G^\wedge}} \left(1 + \frac{\gamma}{q_v^\sigma}\right) \prod_{\substack{v \notin S \\ r_v \notin \mathcal{O}_v^* \otimes G^\wedge}} \frac{\gamma}{q_v^\sigma} \ll \sum_{r \in \mathcal{R}} \prod_{\substack{v \notin S \\ r_v \notin \mathcal{O}_v^* \otimes G^\wedge}} \frac{1}{q_v^{\sigma-\varepsilon}}. \quad (3.2)$$

To proceed, choose a presentation

$$G^\wedge \cong \mathbb{Z}/n_1\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/n_l\mathbb{Z}.$$

This induces an isomorphism

$$I(\mathcal{O}_S) \otimes G^\wedge \cong \bigoplus_{j=1}^l I(\mathcal{O}_S)/I(\mathcal{O}_S)^{n_j}.$$

For an ideal \mathfrak{a} of \mathcal{O}_S , let $\text{rad}(\mathfrak{a})$ denote the product of all prime ideals of \mathcal{O}_S which divide \mathfrak{a} . Then we may represent each element of $I(\mathcal{O}_S) \otimes G^\wedge$ by an l -tuple $(\mathfrak{a}_1, \dots, \mathfrak{a}_l)$ of integral ideals of \mathcal{O}_S , such that $\mathfrak{a}_j \mid \text{rad}(\mathfrak{a}_j)^{n_j-1}$ for all $1 \leq j \leq l$. If $r \in \mathcal{R}$ represents the class of $(\mathfrak{a}_1, \dots, \mathfrak{a}_l)$ in $I(\mathcal{O}_S) \otimes G^\wedge$, then from (3.2) we find that

$$\sum_{x \in k^* \otimes G^\wedge} |g(x)| \ll \sum_{\substack{(\mathfrak{a}_1, \dots, \mathfrak{a}_l) \\ \mathfrak{a}_j \mid \text{rad}(\mathfrak{a}_j)^{M-1}}} \frac{1}{N(\text{rad}(\mathfrak{a}_1 \cdots \mathfrak{a}_l))^{\sigma-\varepsilon}} = \sum_{\mathfrak{a} \leq \mathcal{O}_S} \frac{\rho(\mathfrak{a})}{N(\mathfrak{a})^{\sigma-\varepsilon}}, \quad (3.3)$$

where $M = \max\{n_j\}$, $N(\mathfrak{a})$ denotes the absolute norm of the ideal \mathfrak{a} , and

$$\rho(\mathfrak{a}) = |\mu(\mathfrak{a})|^2 \#\{(\mathfrak{a}_1, \dots, \mathfrak{a}_l) : \mathfrak{a}_j \leq \mathcal{O}_S, \mathfrak{a}_j \mid \text{rad}(\mathfrak{a}_j^{M-1}) \forall j, \text{rad}(\mathfrak{a}_1 \cdots \mathfrak{a}_l) = \mathfrak{a}\}.$$

By $\mathfrak{a} \leq \mathcal{O}_S$, we mean that \mathfrak{a} is an integral ideal of \mathcal{O}_S . It is easily seen that ρ is multiplicative and that for any prime ideal \mathfrak{p} we have

$$\rho(\mathfrak{p}) = M^l - 1.$$

Whence the sum in (3.3) converges, as required. \square

We now come to the application of Poisson summation.

Proposition 3.8. *Let $f = \prod_v f_v : \text{Hom}(\mathbf{A}^*, G) \rightarrow \mathbb{C}$ be a product of functions $f_v : \text{Hom}(k_v^*, G) \rightarrow \mathbb{C}$ such that for all but finitely many places v of k , the function f_v takes only the value 1 on $\text{Hom}(k_v^*/\mathcal{O}_v^*, G)$. Assume that there exists some $\gamma > 0$ such that $|f_v(\chi_v)| \leq \gamma$ for all places v and all $\chi_v \in \text{Hom}(k_v^*, G)$.*

Then for $\text{Re } s > 1/\alpha(G)$ the Fourier transform $\widehat{f}(\cdot; s)$ of $f\Phi_G^{-s}$ exists and we have the Poisson formula

$$\sum_{\chi \in \text{Hom}(\mathbf{A}^*/k^*, G)} \frac{f(\chi)}{\Phi_G(\chi)^s} = \frac{1}{|\mathcal{O}_k^* \otimes G^\wedge|} \sum_{x \in k^* \otimes G^\wedge} \widehat{f}(x; s), \quad \text{Re } s > 1/\alpha(G). \quad (3.4)$$

Moreover, the right-hand side defines a holomorphic function on $\text{Re } s > 1/\alpha(G)$.

Suppose furthermore that there exists a finite set of places S such that f_v is $\text{Hom}(k_v^*/\mathcal{O}_v^*, G)$ -invariant for all $v \notin S$. Then $\widehat{f}(x; s)$ is zero if $x \notin \mathcal{U}_S(G)$ (see (3.1)). In particular, the above sum over x is finite.

Proof. Step 1: Topological considerations. We let $A = \text{Hom}(\mathbf{A}^*, G)$, we let $B = \text{Hom}(\mathbf{A}^*/k^*, G)$, and set $C = A/B$. The topology on B induced from A coincides with the compact-open topology and is discrete. In particular, B is a closed subgroup of A . We equip B with the counting measure db . Next, we have the following exact sequence of locally compact abelian groups, where each morphism is open onto its image

$$1 \rightarrow \text{III}(k, \widehat{G}) \rightarrow k^* \otimes G^\wedge \rightarrow \mathbf{A}^* \otimes G^\wedge \rightarrow \mathbf{A}^*/k^* \otimes G^\wedge \rightarrow 1. \quad (3.5)$$

Here $\widehat{G} = \text{Hom}(G^\wedge, \mathbb{G}_m)$ denotes the Cartier dual of G^\wedge . To check our claims, we may assume that $G = \mu_n$. In this case, the result follows from the canonical topological isomorphism $X \otimes \mathbb{Z}/n\mathbb{Z} \cong X/nX$, which holds for every locally compact abelian group X for which nX is a closed subgroup (see Section 3.1), together with Kummer theory, which identifies the kernel of $k^*/k^{*n} \rightarrow \mathbf{A}^*/\mathbf{A}^{*n}$ with $\text{III}(k, \mu_n)$. Next, it follows from [27, Thm. 9.1.3] that $\text{III}(k, \widehat{G})$ is a finite elementary abelian 2-group. In particular,

$$C^\wedge \cong (k^* \otimes G^\wedge) / \text{III}(k, \widehat{G}) \quad (3.6)$$

is discrete. We equip C^\wedge with the dual of the quotient measure on C induced by $d\chi$ and db ; this is some constant ω times the counting measure on C^\wedge .

Step 2: Poisson summation. We shall use the version of Poisson summation given in the Corollary of [6, §II.8, p. 127]. Note that the existence of the Fourier transform $\widehat{f}(\cdot; s)$ for $\text{Re } s > 1/\alpha(G)$ follows from Lemma 3.5. In order to apply Poisson summation, it suffices to show that

- (1) The sum

$$\sum_{x \in k^* \otimes G^\wedge} |\widehat{f}(x; s)|$$

exists for $\text{Re } s > 1/\alpha(G)$.

- (2) For $\text{Re } s > 1/\alpha(G)$, the sum

$$\sum_{\chi \in \text{Hom}(\mathbf{A}^*/k^*, G)} \frac{|f(\chi a)|}{|\Phi_G(\chi a)^s|}$$

exists for all $a \in \text{Hom}(\mathbf{A}^*, G)$ and defines a continuous function on $\text{Hom}(\mathbf{A}^*, G)$.

In light of Lemma 3.4, the validity of Condition (1) follows from Lemma 3.7, which also shows that the right-hand side in (3.4) defines a holomorphic function on $\text{Re } s > 1/\alpha(G)$. As for Condition (2), let S be a finite set of places of k containing those places v with $f_v(\text{Hom}(k_v^*/\mathcal{O}_v^*, G)) \neq \{1\}$ and large enough such that $\text{Pic } \mathcal{O}_S = 0$. Then $\mathbf{A}^*/k^* \cong \mathbf{A}_S^*/\mathcal{O}_S^*$. We define local functions $\rho_v : \text{Hom}(k_v^*, G) \rightarrow \mathbb{C}$ by

$$\rho_v(\chi_v) = \begin{cases} 1, & \chi_v \in \text{Hom}(k_v^*/\mathcal{O}_v^*, G), \\ \gamma, & \chi_v \notin \text{Hom}(k_v^*/\mathcal{O}_v^*, G), \end{cases}$$

for $v \notin S$ and $\rho_v(\chi_v) = \gamma$ for $v \in S$. Recall that, by continuity,

$$\mathrm{Hom}(\mathbf{A}_S^*, G) = \bigoplus_{v \in S} \mathrm{Hom}(k_v^*, G) \oplus \bigoplus_{v \notin S} \mathrm{Hom}(\mathcal{O}_v^*, G).$$

Since ρ_v is $\mathrm{Hom}(k_v^*/\mathcal{O}_v^*, G)$ -invariant for all v , this allows us to define the function $\rho := \prod_v \rho_v : \mathrm{Hom}(\mathbf{A}_S^*, G) \rightarrow \mathbb{C}$. We also use ρ to denote the pullback of ρ to $\mathrm{Hom}(\mathbf{A}^*, G)$, which dominates f . Since $\mathrm{Hom}(\mathbf{A}^*, G)$ is second-countable, it is enough to show continuity in terms of sequences. Let $(a_n)_n$ be a sequence in $\mathrm{Hom}(\mathbf{A}^*, G)$ with limit a , and assume without loss of generality that

$$a_n \in a \cdot \prod_{v \in S} \{\mathbb{1}_{k_v^*}\} \prod_{v \notin S} \mathrm{Hom}(k_v^*/\mathcal{O}_v^*, G)$$

holds for all $n \in \mathbb{N}$. Then

$$\left| \frac{f(\chi a_n)}{\Phi_G(\chi a_n)^s} \right| \leq \frac{\rho(\chi a_n)}{\Phi_G(\chi a_n)^{\mathrm{Re} s}} = \frac{\rho(\chi a)}{\Phi_G(\chi a)^{\mathrm{Re} s}}$$

holds for all $\chi \in \mathrm{Hom}(\mathbf{A}^*/k^*, G)$. Moreover,

$$\begin{aligned} & \sum_{\chi \in \mathrm{Hom}(\mathbf{A}^*/k^*, G)} \frac{\rho(\chi a)}{\Phi_G(\chi a)^{\mathrm{Re} s}} = \sum_{\chi \in \mathrm{Hom}(\mathbf{A}_S^*/\mathcal{O}_S^*, G)} \frac{\rho(\chi a)}{\Phi_G(\chi a)^{\mathrm{Re} s}} \\ & \ll \sum_{\chi \in \mathrm{Hom}(\mathbf{A}_S^*, G)} \frac{\rho(\chi a)}{\Phi_G(\chi a)^{\mathrm{Re} s}} = \sum_{\chi \in \mathrm{Hom}(\mathbf{A}_S^*, G)} \frac{\rho(\chi)}{\Phi_G(\chi)^{\mathrm{Re} s}} \\ & = \prod_{v \in S} \sum_{\chi_v \in \mathrm{Hom}(k_v^*, G)} \frac{\rho_v(\chi_v)}{\Phi_G(\chi_v)^{\mathrm{Re} s}} \prod_{v \notin S} \sum_{\chi_v \in \mathrm{Hom}(\mathcal{O}_v^*, G)} \frac{\rho_v(\chi_v)}{\Phi_G(\chi_v)^{\mathrm{Re} s}} \\ & = \prod_{v \in S} \sum_{\chi_v \in \mathrm{Hom}(k_v^*, G)} \frac{\rho_v(\chi_v)}{\Phi_G(\chi_v)^{\mathrm{Re} s}} \prod_{v \notin S} \widehat{\rho}_v(\mathbb{1}_v; \mathrm{Re} s). \end{aligned}$$

The absolute convergence of this for $\mathrm{Re} s > 1/\alpha(G)$ follows from the bounds given in Lemma 3.4. Continuity then follows from Lebesgue's dominated convergence theorem, and hence Condition (2) holds. Using (3.6), Poisson summation yields

$$\sum_{\chi \in \mathrm{Hom}(\mathbf{A}^*/k^*, G)} \frac{f(\chi)}{\Phi_G(\chi)^s} = \omega \sum_{x \in \mathcal{C}^\wedge} \widehat{f}(x; s) = \frac{\omega}{|\mathbb{III}(k, \widehat{G})|} \sum_{x \in k^* \otimes G^\wedge} \widehat{f}(x; s). \quad (3.7)$$

Step 3: Calculation of ω . To complete the proof of (3.4), it suffices to show

$$\omega = \frac{|\mathbb{III}(k, \widehat{G})|}{|\mathcal{O}_k^* \otimes G^\wedge|}. \quad (3.8)$$

We shall do this by applying the Poisson formula to a special choice of f . For each place v of k , let f_v be the indicator function of $\mathrm{Hom}(k_v^*/\mathcal{O}_v^*, G)$. Then

$$\begin{aligned} \sum_{\chi \in \mathrm{Hom}(\mathbf{A}^*/k^*, G)} \frac{f(\chi)}{\Phi_G(\chi)^s} &= \#\{\chi \in \mathrm{Hom}(\mathbf{A}^*/k^*, G) : \chi_v \in \mathrm{Hom}(k_v^*/\mathcal{O}_v^*, G) \forall v\} \\ &= \#\ker \left(\mathrm{Hom}(\mathbf{A}^*/k^*, G) \rightarrow \bigoplus_v \mathrm{Hom}(\mathcal{O}_v^*, G) \right). \end{aligned}$$

Consider the exact sequence of locally compact abelian groups

$$\prod_v \mathcal{O}_v^* \rightarrow \mathbf{A}^*/k^* \rightarrow \text{Pic } \mathcal{O}_k \rightarrow 1.$$

From this we obtain the exact sequence

$$1 \rightarrow \text{Hom}(\text{Pic } \mathcal{O}_k, G) \rightarrow \text{Hom}(\mathbf{A}^*/k^*, G) \rightarrow \bigoplus_v \text{Hom}(\mathcal{O}_v^*, G),$$

thus

$$\sum_{\chi \in \text{Hom}(\mathbf{A}^*/k^*, G)} \frac{f(\chi)}{\Phi_G(\chi)^s} = |\text{Hom}(\text{Pic } \mathcal{O}_k, G)|. \quad (3.9)$$

Next, we have

$$\begin{aligned} \sum_{x \in k^* \otimes G^\wedge} \widehat{f}(x; s) &= \#\{x \in k^* \otimes G^\wedge : x_v \in \mathcal{O}_v^* \otimes G^\wedge \forall v\} \\ &= |\mathcal{O}_k^* \otimes G^\wedge| \cdot |\text{Tor}(\text{Pic } \mathcal{O}_k, G^\wedge)|, \end{aligned}$$

where the second equality follows from Lemma 3.6. Combine this with (3.7) and (3.9) to obtain (3.8). The rest of the proposition follows from Lemma 3.4 and Lemma 3.6. \square

Remark 3.9. In Wright's setting (which corresponds to $f = \mathbb{1}$), he was in the second case of Proposition 3.8. He used character orthogonality to obtain a finite sum in [37, §3] (see in particular [37, (3.2)]). For more general applications, however, it may happen that the right hand sum in Proposition 3.8 is infinite (this occurs for example in the proof of Theorem 1.7). Notice also the consideration of the factor $\text{III}(k, \widehat{G})$ in the proof of Proposition 3.8, which was overlooked in Wright's work [37, Lem. 3.1]. Lemma 3.6 may be viewed as a corrected version of [37, Lem. 3.1].

4. PROOF OF THEOREM 1.7

4.1. **Set-up.** For any place v of k and any sub- G -extension φ_v of k_v , let

$$f_v(\varphi_v) := \begin{cases} 1 & \text{if } \varphi_v \in \Lambda_v \\ 0 & \text{otherwise,} \end{cases}$$

where the set Λ_v is as in Theorem 1.7. For any sub- G -extension φ of k , let $(\varphi_v)_v$ be the induced local sub- G -extensions, and define

$$f(\varphi) := \prod_v f_v(\varphi_v),$$

the product running over all places v of k .

Throughout this section, we use the characterization of a sub- G -extension φ as a continuous homomorphism $\mathbf{A}^*/k^* \rightarrow G$, where G is endowed with the discrete topology. The interplay between local and global class field theory shows that for each place v , the sub- G -extension induced by the natural embedding $k_v^* \rightarrow \mathbf{A}^*$ is φ_v .

Theorem 1.7 will follow from a standard Tauberian theorem once we prove that the Dirichlet series $D_{G,f}(s)$ defined in (2.1) gives a meromorphic function for $\text{Re } s > 1/\alpha(G) - \gamma$, for some $\gamma > 0$, and has its rightmost pole at $s = 1/\alpha(G)$

of order $\nu(k, G)$. The current section is devoted to the proof of this result, starting with applications of the general techniques from Sections 2 and 3. From Lemma 2.2, we see that, formally,

$$D_{G,f}(s) = \sum_{H \subseteq G} \mu(G/H) F_{H,f}(s|G|/|H|), \quad (4.1)$$

with the conductor series $F_{H,f}(s)$ defined as in (2.6).

We will soon see that $F_{H,f}(s|G|/|H|)$ converges absolutely for $\operatorname{Re} s > 1/\alpha(G)$ (which also follows directly from Wright's result). Since the sum over all subgroups H of G in (4.1) is finite, a meromorphic continuation of the conductor series $F_{H,f}(s)$ will yield the required analytic properties of $D_{G,f}(s)$, except for the possible cancellation of poles. In Subsection 4.7, we will show that, under the assumptions of Theorem 1.7, no such cancellation occurs.

4.2. Poisson-summation. Fix a subgroup H of G . We now apply the results of Section 3 to the conductor series $F_{H,f}(s)$. The assumption (1.4) implies that for all but finitely many v , the Λ_v contain all unramified sub- G -extensions of k_v . Hence the product $f(\chi) := \prod_v f_v(\chi_v)$ gives a well-defined continuous function $\operatorname{Hom}(\mathbf{A}^*, H) \rightarrow \mathbb{C}$. Since f clearly satisfies the hypotheses of Proposition 3.8 (with G replaced by H), we obtain

$$F_{H,f}(s) = \frac{1}{|\mathcal{O}_k^* \otimes H^\wedge|} \sum_{x \in k^* \otimes H^\wedge} \widehat{f}_H(x; s), \quad \text{for } \operatorname{Re} s > 1/\alpha(H), \quad (4.2)$$

where $\widehat{f}_H(x; s)$ denotes the Fourier transform of $f\Phi_H^{-s}$. In particular, the complex function $F_{H,f}(x; s|G|/|H|)$ is holomorphic on $\operatorname{Re} s > |H|/(\alpha(H)|G|)$.

Let Q be the smallest prime dividing $|G|$. If $Q \nmid |H|$, then $\alpha(H)|G|/|H| \geq \alpha(G) + 1$, so $F_{H,f}(x; s|G|/|H|)$ is holomorphic on $\operatorname{Re} s > 1/(\alpha(G) + 1)$. If $Q \mid |H|$, then we will show that $F_{H,f}(x; s|G|/|H|)$ has a meromorphic continuation to the left of $\operatorname{Re} s = 1/\alpha(G)$.

The main difference between our situation and [37, §4, §5], is that in our case the sum over x in (4.2) may be infinite, whereas the analogue in Wright's situation is a finite sum (cf. Remark 3.9). Hence, in our analysis of $\widehat{f}_H(x; s)$ it is vitally important to control the dependence on x . In particular, in what follows all implied constants in Landau's O -notation and Vinogradov's \ll -notation will not depend on x or s . Aside from this, our strategy follows the same classical steps of relating the resulting Euler products to Dedekind zeta functions.

4.3. Euler factors. In this subsection, we will assume that $Q \mid |H|$. By Lemma 3.5, we obtain the Euler product $\widehat{f}_H(x; s) = \prod_v \widehat{f}_{H,v}(x_v; s)$, with

$$\widehat{f}_{H,v}(x_v; s) := \frac{1}{|H|} \sum_{\chi_v \in \operatorname{Hom}(k_v^*, H)} \frac{f_v(\chi_v) \langle \chi_v, x_v \rangle}{\Phi_H(\chi_v)^s} \quad (4.3)$$

for non-archimedean v .

We now evaluate the leading terms of the Euler factors $\widehat{f}_{H,v}(x_v; s)$ at almost all places of k . We allow ourselves to exclude the places in a finite set S which contains all archimedean places, all places dividing the order of G , all places v where Λ_v does not satisfy (1.4), and enough places to ensure that the ring of

S -integers \mathcal{O}_S is a principal ideal domain. At later points, we will enlarge S as necessary, but it will never depend on anything but k , G and our collection Λ of local conditions.

Let $\beta_H \geq 1$ be the largest integer such that $(\mathbb{Z}/Q\mathbb{Z})^{\beta_H}$ is isomorphic to a subgroup of H . We set $\beta := \beta_G$. Let $x_v \in \mathcal{O}_v^* \otimes H^\wedge$. We write $x_v \in \mathcal{O}_v^{*Q} \otimes H^\wedge$ to say that x_v is in the image of $\mathcal{O}_v^{*Q} \otimes H^\wedge$ in $\mathcal{O}_v^* \otimes H^\wedge$ under the natural map (which is not injective in general).

The following is inspired by [37, Prop. 4.3].

Lemma 4.1. *Let $v \notin S$ and assume that $Q \mid |H|$. Let $\operatorname{Re} s \geq 0$.*

If $x_v \in \mathcal{O}_v^ \otimes H^\wedge$, then $\widehat{f}_{H,v}(x_v; s|G|/|H|)$ equals*

$$\begin{aligned} & 1 + (Q^{\beta_H} - 1)q_v^{-\alpha(G)s} + O(q_v^{-\alpha(G)+1)s}), \text{ if } q_v \equiv 1 \pmod{Q} \text{ and } x_v \in \mathcal{O}_v^{*Q} \otimes H^\wedge, \\ & 1 - q_v^{-\alpha(G)s} + O(q_v^{-\alpha(G)+1)s}), \text{ if } q_v \equiv 1 \pmod{Q} \text{ and } x_v \notin \mathcal{O}_v^{*Q} \otimes H^\wedge, \\ & 1 + O(q_v^{-\alpha(G)+1)s}), \text{ if } q_v \not\equiv 1 \pmod{Q}. \end{aligned}$$

If $x_v \notin \mathcal{O}_v^ \otimes H^\wedge$, then $\widehat{f}_{H,v}(x_v; s|G|/|H|) = O(q_v^{-\alpha(G)+1)s}$.*

Proof. From Lemma 3.3, with G replaced by H , we get

$$\widehat{f}_{H,v}(x_v; s) = \sum_{\substack{m|d_{H,v} \\ m \in \{1, Q\}}} \sum_{\substack{\chi_v \in \operatorname{Hom}(\mathcal{O}_v^*, H) \\ \ker \chi_v = \mathcal{O}_v^{*m}}} \langle \chi_v, x_v \rangle \tau_{f_v}(\chi_v, x_v) q_v^{-|H|(1-1/m)s} + O(q_v^{-\alpha(H)+1)s}),$$

where $d_{H,v}$ is the greatest common divisor of $q_v - 1$ and the exponent of H . By our conditions (1.4) on Λ_v , we have $f_v(\psi_v) = 1$ for $\psi_v \in \operatorname{Hom}(k_v^*/\mathcal{O}_v^*, H)$. As in the proof of Lemma 3.4, we see that $\tau_{f_v}(\mathbb{1}_v, x_v) = 1$ if $x_v \in \mathcal{O}_v^* \otimes H^\wedge$ and $\tau_{f_v}(\mathbb{1}_v, x_v) = 0$ otherwise.

If $q_v \not\equiv 1 \pmod{Q}$, then $Q \nmid d_{H,v}$, and hence we obtain

$$\widehat{f}_{H,v}(x_v; s) = \begin{cases} 1 + O(q_v^{-\alpha(H)+1)s}), & \text{if } x_v \in \mathcal{O}_v^* \otimes H^\wedge, \\ O(q_v^{-\alpha(H)+1)s}), & \text{if } x_v \notin \mathcal{O}_v^* \otimes H^\wedge. \end{cases}$$

Now assume that $q_v \equiv 1 \pmod{Q}$, so that $Q \mid d_{H,v}$. Let $\chi_v \in \operatorname{Hom}(\mathcal{O}_v^*, H)$ with $\ker \chi_v = \mathcal{O}_v^{*Q}$. The conditions (1.4) on Λ_v ensure that $f_v(\chi_v \psi_v) = 1$ for all $\psi_v \in \operatorname{Hom}(k_v^*/\mathcal{O}_v^*, H)$. Hence,

$$\tau_{f_v}(\chi_v, x_v) := \frac{1}{|H|} \sum_{\psi_v \in \operatorname{Hom}(k_v^*/\mathcal{O}_v^*, H)} \langle \psi_v, x_v \rangle = \begin{cases} 1 & \text{if } x_v \in \mathcal{O}_v^* \otimes H^\wedge, \\ 0 & \text{otherwise.} \end{cases}$$

Thus, we have shown that

$$\widehat{f}_{H,v}(x_v; s) = \begin{cases} 1 + \sigma_v(x_v) q_v^{-\alpha(H)s} + O(q_v^{-\alpha(H)+1)s}) & \text{if } x_v \in \mathcal{O}_v^* \otimes H^\wedge, \\ O(q_v^{-\alpha(H)+1)s}) & \text{if } x_v \notin \mathcal{O}_v^* \otimes H^\wedge, \end{cases}$$

where

$$\sigma_v(x_v) := \sum_{\substack{\chi_v \in \operatorname{Hom}(\mathcal{O}_v^*, H) \\ \ker \chi_v = \mathcal{O}_v^{*Q}}} \langle \chi_v, x_v \rangle.$$

It is a simple task to evaluate $\sigma_v(x_v)$. Indeed, using character orthogonality, $\sigma_v(x_v) + 1$ equals

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

Moreover, $|\text{Hom}(\mathcal{O}_v^*/\mathcal{O}_v^{*Q}, H)| = Q^{\beta_H}$, the number of elements of order dividing Q in H . We finish our proof with the observation that $\alpha(H)|G|/|H| = \alpha(G)$, so that $(\alpha(H) + 1)|G|/|H| \geq \alpha(G) + 1$. \square

4.4. Splitting conditions. Assume that $Q \mid |H|$. Our goal is to relate the Fourier transform $\widehat{f}_H(x; s)$ to a product of Dedekind zeta functions. Hence, we want to express the conditions deciding the shape of the Euler factors in Lemma 4.1 in terms of splitting properties of v . Recall that x_v denotes the image of $x \in k^* \otimes H^\wedge$ under the natural map $k^* \otimes H^\wedge \rightarrow k_v^* \otimes H^\wedge$. Let

$$T := T(x) := S \cup \{v \text{ place of } k : x_v \notin \mathcal{O}_v^* \otimes H^\wedge\}. \quad (4.4)$$

Let $k_0 := k(\mu_Q)$ be the field obtained by adjoining to k all Q -th roots of unity.

Each $\psi \in \text{Hom}(\mu_Q, H)$ induces a map $\Psi \in \text{Hom}(k^* \otimes H^\wedge, k_0^*/k_0^{*Q})$ as follows:

$$k^* \otimes H^\wedge \rightarrow k_0^*/k_0^{*Q} \otimes H^\wedge \xrightarrow{1 \otimes \psi^\wedge} k_0^*/k_0^{*Q} \otimes \mu_Q^\wedge = k_0^*/k_0^{*Q}. \quad (4.5)$$

Thus, by Kummer theory, each $x \in k^* \otimes H^\wedge$ determines an elementary abelian Q -extension k_x/k_0 , corresponding to the subgroup of k_0^*/k_0^{*Q} generated by the images of x under all such Ψ . Let us collect some properties of the extensions k_0 and k_x (cf. the end of [37, §4]).

Lemma 4.2. *Let $x \in k^* \otimes H^\wedge$.*

- (1) *The extension k_0/k is cyclic of degree dividing $Q - 1$, and the extension k_x/k_0 is abelian with Galois group isomorphic to a subgroup of $(\mathbb{Z}/Q\mathbb{Z})^{\beta_H}$.*
- (2) *The conductor of k_x/k_0 has absolute norm $\ll \prod_{v \in T(x)} q_v^{[k_0:k]}$.*
- (3) *For any place v of k with $v \notin T(x)$, we have the equivalences*

$$v \text{ splits completely in } k_0 \iff q_v \equiv 1 \pmod{Q},$$

$$v \text{ splits completely in } k_x \iff q_v \equiv 1 \pmod{Q} \text{ and } x_v \in \mathcal{O}_v^{*Q} \otimes H^\wedge.$$

Proof. The \mathbb{F}_Q -vector subspace of k_0^*/k_0^{*Q} corresponding to k_x/k_0 is spanned by the images of x in k_0^*/k_0^{*Q} under the β_H maps coming from an \mathbb{F}_Q -basis of $\text{Hom}(\mu_Q, H)$. The statement on the \mathbb{F}_Q -rank of $\text{Gal}(k_x/k_0)$ then follows from Kummer theory. All other statements in (1) are obvious.

Now let v be a non-archimedean place of k and let w be a place of k_0 above v . If $v \notin T(x)$, then $x_v \in \mathcal{O}_v^* \otimes H^\wedge$ and it follows that the induced extension of $k_{0,w}$ is unramified. On the other hand, if $v \in T(x)$ then ramification may occur, but when $w \nmid Q$ any such ramification must be tame. This shows (2).

We now prove (3). It is well known that v splits completely in k_0 if and only if $q_v \equiv 1 \pmod{Q}$. Let $v \notin T(x)$ be completely split in k_0 , so that $k_v = k_{0,w}$. A variant of the construction (4.5) associates to each $\psi \in \text{Hom}(\mu_Q, H)$ a map $\Psi_v \in \text{Hom}(k_v^* \otimes H^\wedge, k_v^*/k_v^{*Q})$, and v is completely split in k_x/k if and only if

$x_v \in \ker \Psi_v$ for all ψ . Therefore, as $x_v \in \mathcal{O}_v^* \otimes H^\wedge$, to prove the result it suffices to show that

$$\bigcap_{\psi \in \text{Hom}(\mu_Q, H)} \ker \Psi_v = \ker (k_v^* \otimes H^\wedge \rightarrow k_v^*/k_v^{*Q} \otimes H^\wedge), \quad (4.6)$$

since $\ker(k_v^* \otimes H^\wedge \rightarrow k_v^*/k_v^{*Q} \otimes H^\wedge) = \text{Im}(k_v^{*Q} \otimes H^\wedge \rightarrow k_v^* \otimes H^\wedge)$. The equality (4.6) follows from the fact that the map

$$k_v^*/k_v^{*Q} \otimes H^\wedge \longrightarrow \prod_{\psi \in \text{Hom}(\mu_Q, H)} k_v^*/k_v^{*Q},$$

induced by the product of the $\psi \in \text{Hom}(\mu_Q, H)$, is injective. \square

4.5. L -functions. We continue to assume that $Q \mid |H|$. We now find a meromorphic continuation of the partial Euler product

$$L_{f,H}(x; s \mid G \mid |H|) := \prod_{v \notin T(x)} \widehat{f}_{H,v}(x_v; s \mid G \mid |H|)$$

to the left of $\text{Re } s = 1/\alpha(G)$, making the dependence on x explicit. We will take care of the contribution of places $v \in T(x)$ in the next subsection.

To continue, we introduce some notation. Let $a, b > 0$ and let $f(x; s), g(x; s)$ be families of holomorphic functions on some half-plane $\text{Re } s > b \geq a$, parameterised by x . We write $f(x; s) \approx_a g(x; s)$ if there is a family of holomorphic functions $\phi(x; s)$ on the half-plane $\text{Re } s > a$, satisfying $1 \ll_\epsilon \phi(x; s) \ll_\epsilon 1$ on $\text{Re } s > a + \epsilon$, independently of x , such that $f(x; s) = \phi(x; s)g(x; s)$ for $\text{Re } s > b$.

For any finite Galois extension K/k , the partial Euler product

$$\zeta_{K,T}(s) := \prod_{\substack{w \in \Omega_K \\ w|_k \notin T}} \frac{1}{1 - q_w^{-s}},$$

of the Dedekind zeta function defines a meromorphic function with a simple pole at $s = 1$. We use Lemma 4.1 and Lemma 4.2 to relate $L_{f,H}(x; s \mid G \mid |H|)$ to a product formed from $\zeta_{k_0,T}(s)$ and $\zeta_{k_x,T}(s)$.

Lemma 4.3. *Let $d := [k_0 : k]$ and $Q^m := [k_x : k_0]$, with $m = m(x) \leq \beta_H$, and $T = T(x)$ as in (4.4). Then*

$$L_{f,H}(x; s \mid G \mid |H|)^d \approx_{1/(\alpha(G)+1)} \zeta_{k_x,T}(\alpha(G)s)^{(Q^{\beta_H-m})-1} \left(\frac{\zeta_{k_x,T}(\alpha(G)s)}{\zeta_{k_0,T}(\alpha(G)s)} \right). \quad (4.7)$$

Proof. The argument is fairly standard and can be found in more detail in [37, §5]. In each step we might need to enlarge our set S by some small places, to ensure that all occurring Euler factors are bounded away from 0. We can choose these places independently of x (and T), since all explicit and implicit constants appearing in the Euler factors are bounded independently of x . By Lemma 4.2

and the usual argument about split primes, we obtain

$$\zeta_{k_0, T}(s) \approx_{1/2} \prod_{\substack{v \notin T \\ q_v \equiv 1 \pmod{Q}}} (1 + dq_v^{-s}), \text{ and}$$

$$\zeta_{k_x, T}(s) \approx_{1/2} \prod_{\substack{v \notin T \\ q_v \equiv 1 \pmod{Q} \\ x_v \in \mathcal{O}_v^* \otimes H^\wedge}} (1 + dQ^m q_v^{-s}).$$

Hence, the expression on the right-hand side of (4.7) is

$$\approx_{1/(2\alpha(G))} \prod_{\substack{v \notin T \\ q_v \equiv 1 \pmod{Q} \\ x_v \in \mathcal{O}_v^* \otimes H^\wedge}} (1 + d(Q^{\beta_H} - 1)q_v^{-\alpha(G)s}) \prod_{\substack{v \notin T \\ q_v \equiv 1 \pmod{Q} \\ x_v \notin \mathcal{O}_v^* \otimes H^\wedge}} (1 - dq_v^{-\alpha(G)s}).$$

Together with Lemma 4.1, this yields the desired result. \square

We want to isolate the pole at $s = 1/\alpha(G)$ on the right-hand side of (4.7) independently of x . This is achieved in the next lemma. For any number field K , we let $\zeta_K(s)$ be its Dedekind zeta function.

Lemma 4.4. *The complex functions $\zeta_{k_x, T}(s)/\zeta_{k_0, T}(s)$ and $\zeta_{k_x, T}(s)/\zeta_{k_0}(s)$ are entire. For any $\delta > 0$ there is a positive constant $\gamma(\delta)$ that depends only on δ , k , and G , such that*

$$\frac{\zeta_{k_x, T}(s)}{\zeta_{k_0, T}(s)} \ll_\delta (1 + |\operatorname{Im} s|)^\delta \prod_{v \in T} q_v^\delta \quad \text{and} \quad \frac{\zeta_{k_x, T}(s)}{\zeta_{k_0}(s)} \ll_\delta (1 + |\operatorname{Im} s|)^\delta \prod_{v \in T} q_v^\delta \quad (4.8)$$

hold for $\operatorname{Re} s > 1 - \gamma(\delta)$, where the implied constant depends only on k , G and δ .

Proof. Let $\mathbf{A}_{k_0}^*$ be the idele group of k_0 , and let U be the open subgroup corresponding to the abelian extension k_x/k_0 . Then

$$\zeta_{k_x}(s) = \prod_{\chi \in (\mathbf{A}_{k_0}^*/U)^\wedge} L(s, \chi),$$

where $L(s, \chi)$ is the L -function associated to χ . Then $L(s, \mathbb{1}) = \zeta_{k_0}(s)$, and $L(s, \chi)$ is entire for $\chi \neq \mathbb{1}$. This shows that $\zeta_{k_x}(s)/\zeta_{k_0}(s)$ is entire.

The conductor of every character $\chi \in (\mathbf{A}_{k_0}^*/U)^\wedge$ divides the conductor of k_x/k_0 , so by Lemma 4.2 its absolute norm is $\ll \prod_{v \in T(x)} q_v^d$, where $d = [k_0 : k]$. The standard convexity bound (see [21, (5.20)]) yields, for $\chi \neq \mathbb{1}$ and $\operatorname{Re} s \in [0, 1]$,

$$L(s, \chi) \ll_\epsilon \left((3 + |s|)^d \prod_{v \in T} q_v^d \right)^{(1 - \operatorname{Re} s)/2 + \epsilon} \ll_\epsilon (1 + |\operatorname{Im}(s)|)^{2\epsilon} \prod_{v \in T} q_v^{2\epsilon},$$

for $1 - \gamma'(\epsilon) < \operatorname{Re} s \leq 1$, with a suitable $\gamma'(\epsilon) > 0$. This estimate extends to the half-plane $\operatorname{Re} s > 1 - \gamma'(\epsilon)$, by the Phragmen-Lindelöf principle and the bound $L(s, \chi) \ll_\epsilon 1$ for $\operatorname{Re} s > 1 + \epsilon$. Since $|(\mathbf{A}_{k_0}^*/U)^\wedge| \leq Q^{\beta_H} \ll 1$, this shows that for any $\delta > 0$ there is a positive constant $\gamma(\delta)$, such that

$$\frac{\zeta_{k_x}(s)}{\zeta_{k_0}(s)} \ll_\delta (1 + |\operatorname{Im} s|)^\delta \prod_{v \in T} q_v^\delta,$$

whenever $\operatorname{Re} s > 1 - \gamma(\delta)$. Let

$$P(T; s) := \prod_{v \in T \setminus \Omega_\infty} \prod_{\substack{w \in \Omega(k_0) \\ w|v}} (1 - q_w^{-s})^{-1} \prod_{\substack{w' \in \Omega(k_x) \\ w'|w}} (1 - q_{w'}^{-s}).$$

Then

$$\frac{\zeta_{k_x, T}(s)}{\zeta_{k_0, T}(s)} = P(T; s) \cdot \frac{\zeta_{k_x}(s)}{\zeta_{k_0}(s)}. \quad (4.9)$$

Since $(1 - X)$ divides $(1 - X^f)$ for any positive integer f , the function $P(T; s)$ is entire, and $|P(T; s)| \leq 2^{dQ^{\beta|T|}}$ for $\operatorname{Re} s > 0$. This proves the first part of (4.8). For the second part, use

$$\tilde{P}(T; s) := \prod_{\substack{w' \in \Omega(k_x) \\ w'|_k \in T \setminus \Omega_\infty}} (1 - q_{w'}^{-s}). \quad \square$$

It is proved in [37, §5] that the d -th root of $\zeta_{k_x, T}(s)/\zeta_{k_0, T}(s)$ can be defined as a single-valued holomorphic function (this is because each zero and pole occurs with multiplicity divisible by d). Hence, we have proved the following lemma, which is the main result of this subsection.

Lemma 4.5. *For any $x \in k^* \otimes H^\wedge$, let T, m, d be as in Lemma 4.3. Then there is a function $\phi(x; s)$, holomorphic on $\operatorname{Re} s > 1/(\alpha(G) + 1)$, such that*

$$L_{f, H}(x; s|G|/|H|) = \phi(x; s) \cdot \zeta_{k_0}(\alpha(G)s)^{(Q^{\beta_H - m} - 1)/d}.$$

Moreover, for any $\delta > 0$ there is a positive constant $\gamma(\delta)$, independent of x , such that for $\operatorname{Re}(s) > 1/\alpha(G) - \gamma(\delta)$, we have

$$\phi(x; s) \ll_\delta (1 + |\operatorname{Im} s|)^\delta \prod_{v \in T} q_v^\delta. \quad (4.10)$$

The highest order of the potential pole at $s = 1/\alpha(G)$ is achieved when $m = 0$, that is, when $k_x = k_0$.

4.6. Global analysis. We now apply our results from the previous subsections to analyse the sum on the right-hand side of (4.2), still under the assumption that $Q \mid |H|$. Recall that for $x \in k^* \otimes H^\wedge$, we defined $m(x) \in \{0, \dots, \beta_H\}$ by $[k_x : k_0] = Q^{m(x)}$. We sort all x by their respective values of $m(x)$ and apply Lemma 4.5 to obtain

$$F_{H, f}(s|G|/|H|) = \frac{1}{|\mathcal{O}_k^* \otimes H^\wedge|} \sum_{m=0}^{\beta_H} \zeta_{k_0}(\alpha(G)s)^{(Q^{\beta_H - m} - 1)/d} S(m; s), \quad (4.11)$$

where

$$S(m; s) := \sum_{\substack{x \in k^* \otimes H^\wedge \\ m(x)=m}} \phi(x; s) \prod_{v \in T(x)} \hat{f}_{H, v}(x_v; s|G|/|H|).$$

Since the sum over m is finite, it suffices to consider each $S(m; s)$ separately.

Lemma 4.6. *Let $m \in \{0, \dots, \beta_H\}$. There are constants $\delta, \gamma > 0$, depending only on k, G , such that the series $S(m; s)$ converges absolutely for $\operatorname{Re} s > 1/\alpha(G) - \gamma$ and satisfies $S(m; s) \ll (1 + |\operatorname{Im} s|)^\delta$ in this half-plane. Moreover, the convergence is uniform for s in compact discs, so $S(m; s)$ defines a holomorphic function for $\operatorname{Re} s > 1/\alpha(G) - \gamma$.*

Proof. Since we only consider absolute convergence, we may ignore the condition $m(x) = m$. Fix $\delta > 0$ and let $\gamma(\delta)$ be as in Lemma 4.5. Then

$$\phi(x; s) \ll_\delta (1 + |\operatorname{Im} s|)^\delta \prod_{v \in T(x)} q_v^\delta, \quad \operatorname{Re} s > 1/\alpha(G) - \gamma(\delta).$$

An inspection of (4.3) shows that $\widehat{f}_{H,v}(x_v; s|G|/|H|)$ is bounded independently of x_v . For $v \in T(x) \setminus S$, we have the bound

$$|\widehat{f}_{H,v}(x_v; s|G|/|H|)| \leq Cq_v^{-(\alpha(G)+1)\operatorname{Re} s}, \quad \operatorname{Re} s \geq 0,$$

from Lemma 4.1, with $C > 0$ depending only on k and G . Fix $\gamma \in (0, \gamma(\delta))$. On $\operatorname{Re} s > 1/\alpha(G) - \gamma$, we obtain the majorant

$$\phi(x; s) \prod_{v \in T(x)} \widehat{f}_{H,v}(x_v; s|G|/|H|) \ll_\delta (1 + |\operatorname{Im} s|)^\delta \prod_v g_v(x_v),$$

where $g_v(x_v) := 1$ if $x_v \in \mathcal{O}_v^* \otimes H^\wedge$ and

$$g_v(x_v) := Cq_v^{-(\alpha(G)+1)(1/\alpha(G)-\gamma)+\delta}$$

otherwise. Choosing δ and γ small enough gives $(\alpha(G) + 1)(1/\alpha(G) - \gamma) - \delta > 1$. The result then follows from Lemma 3.7. \square

We now come to the main result of this subsection.

Lemma 4.7. *If $Q \mid |H|$, then the function $F_{H,f}(s|G|/|H|)$ has a meromorphic continuation to $\operatorname{Re} s > 1/\alpha(G) - \gamma$. It is holomorphic in this half-plane, with the possible exception of a pole at $s = 1/\alpha(G)$ of order at most $\nu(k, H) = (Q^{\beta_H} - 1)/d$. Moreover, there is $\delta > 0$ such that*

$$F_{H,f}(s|G|/|H|)(1 - 1/(\alpha(G)s))^{\nu(k,H)} \ll (1 + |\operatorname{Im} s|)^\delta, \quad \operatorname{Re} s > 1/\alpha(G) - \gamma. \quad (4.12)$$

Proof. Lemma 4.6 and (4.11) show that $F_{H,f}(s|G|/|H|)$ is a finite sum of meromorphic functions on $\operatorname{Re} s > 1/\alpha(G) - \gamma$ whose poles come from finitely many powers of $\zeta_{k_0}(\alpha(G)s)$. The estimate (4.12) follows from the estimate for $S(m; s)$ in Lemma 4.6 and standard convexity bounds for Dedekind zeta functions. \square

If $Q \nmid |H|$ then we already know that $F_{H,f}(s|G|/|H|)$ is holomorphic for $\operatorname{Re} s > 1/(\alpha(G) + 1)$. Together with the expansion (4.1), this immediately implies that $D_{G,f}(s)$ has a meromorphic continuation to $\operatorname{Re} s > 1/\alpha(G) - \gamma$, with the rightmost possible pole at $s = 1/\alpha(G)$ of order at most $\nu(k, G)$.

As we will show in the next subsection, the order of the pole is indeed $\nu(k, G)$. Then Theorem 1.7 follows immediately from standard power-saving Tauberian theorems, such as [12, Théorème A.1.].

4.7. Positivity of the constant. In this subsection, we let $\alpha := \alpha(G)$ and $\nu := \nu(k, G)$. We now show that $D_{G,f}(s)$ does indeed have a pole of order ν at $s = 1/\alpha$. To do this, it suffices to prove that the limit

$$c_f(k, G) := \lim_{s \rightarrow 1/\alpha} \zeta_{k_0}(\alpha s)^{-\nu} D_{G,f}(s)$$

is positive. Our argument is loosely based on [37, §6]. From (4.1), (4.2) and Lemma 4.6, we obtain

$$c_f(k, G) = \sum_{H \subseteq G} \frac{\mu(G/H)}{|\mathcal{O}_k^* \otimes H^\wedge|} \sum_{x \in k^* \otimes H^\wedge} \prod_v \frac{\widehat{f}_{H,v}(x_v; |G|/(|H|\alpha))}{\zeta_{k_0,v}(1)^\nu}, \quad (4.13)$$

where $\zeta_{k_0,v}(s)$ is the product of the Euler factors of $\zeta_{k_0}(s)$ at all places of k_0 lying above v if v is non-archimedean, and $\zeta_{k_0,v}(s) = 1$ otherwise. We would like to express $c_f(k, G)$ as a sum of non-negative terms, by applying Poisson summation and Möbius inversion backwards. In order to apply Poisson summation, however, we need to approximate the innermost summand by simpler functions. Let

$$\widehat{E}_{H,v}(x_v) := \frac{\widehat{f}_{H,v}(x_v; |G|/(|H|\alpha))}{\zeta_{k_0,v}(1)^\nu},$$

and, for a finite set $T \supseteq S$ of places of k ,

$$\widehat{E}_{H,T,v}(x_v) := \begin{cases} \widehat{E}_{H,v}(x_v) & \text{if } v \in T, \\ 1 & \text{if } v \notin T \text{ and } x_v \in \mathcal{O}_v^* \otimes H^\wedge, \\ 0 & \text{if } v \notin T \text{ and } x_v \notin \mathcal{O}_v^* \otimes H^\wedge. \end{cases}$$

Moreover, for $x \in k^* \otimes H^\wedge$, let

$$\widehat{E}_H(x) := \prod_v \widehat{E}_{H,v}(x_v) \quad \text{and} \quad \widehat{E}_{H,T}(x) := \prod_v \widehat{E}_{H,T,v}(x_v).$$

We observe that $\widehat{E}_{H,T}(x) = 0$ if $x \notin \mathcal{O}_T^* \otimes H^\wedge$, so

$$\sum_{x \in k^* \otimes H^\wedge} \widehat{E}_{H,T}(x) \quad (4.14)$$

exists for any finite set T , as the sum may be taken over $\mathcal{O}_T^* \otimes H^\wedge$, which is a finite set. Moreover, by definition, $\widehat{E}_{H,T}(x)$ converges pointwise to $\widehat{E}_H(x)$, as $T \rightarrow \Omega_K$. We now show something stronger.

Lemma 4.8. *We have*

$$\lim_{T \rightarrow \Omega_K} \sum_{x \in k^* \otimes H^\wedge} \widehat{E}_{H,T}(x) = \sum_{x \in k^* \otimes H^\wedge} \widehat{E}_H(x).$$

Proof. Let $v \notin S$ and recall the bounds from Lemma 4.1 if $Q \mid |H|$ and from Lemma 3.4 (with H instead of G) if $Q \nmid |H|$. If $x_v \notin \mathcal{O}_v^* \otimes H^\wedge$, they show that $\widehat{E}_{H,v}(x_v) \ll q_v^{-1-1/\alpha}$, and consequently also

$$|\widehat{E}_{H,T,v}(x_v)| \leq C q_v^{-1-1/\alpha},$$

with $C > 0$ depending only on k and G . If $x_v \in \mathcal{O}_v^* \otimes H^\wedge$, we compare them with the bounds

$$\zeta_{k_0,v}(1)^{-\nu} = \begin{cases} 1 - (Q^\beta - 1)q_v^{-1} + O(q_v^{-2}) & \text{if } q_v \equiv 1 \pmod{Q}, \\ 1 + O(q_v^{-2}) & \text{if } q_v \not\equiv 1 \pmod{Q}, \end{cases} \quad (4.15)$$

and conclude that

$$\widehat{E}_{H,T,v}(x_v) = 1 - c(x_v)q_v^{-1} + O(q_v^{-1-1/\alpha}),$$

for some $c(x_v) \in \{0, \dots, Q^\beta\}$. All explicit and implied constants are bounded independently of x , hence we may assume that the set S of excluded places was chosen large enough to ensure that $\widehat{E}_{H,T,v}(x_v) \geq 0$ for all $v \notin S$ and all $x_v \in \mathcal{O}_v^* \otimes H^\wedge$. Putting everything together, we see that $\widehat{E}_{H,T}(x)$ is

$$\ll \prod_{\substack{v \notin S \\ x_v \notin \mathcal{O}_v^* \otimes H^\wedge}} Cq_v^{-1-1/\alpha} \prod_{\substack{v \notin S \\ x_v \in \mathcal{O}_v^* \otimes H^\wedge}} (1 + O(q_v^{-1-1/\alpha})) \ll \prod_{x_v \notin \mathcal{O}_v^* \otimes H^\wedge} Cq_v^{-1-1/\alpha}.$$

The sum of this last bound over $x \in k^* \otimes H^\wedge$ converges by Lemma 3.7, so the desired result follows from Lebesgue's dominated convergence theorem. \square

By the last lemma, we get

$$c_f(k, G) = \lim_{T \rightarrow \Omega_k} c_{f,T}(k, G),$$

where

$$c_{f,T}(k, G) := \sum_{H \subseteq G} \frac{\mu(G/H)}{|\mathcal{O}_k^* \otimes H^\wedge|} \sum_{x \in k^* \otimes H^\wedge} \widehat{E}_{H,T}(x). \quad (4.16)$$

Observe that $\widehat{E}_{H,T}(x)$ defines a function on $\mathbf{A}^* \otimes H^\wedge$ which is zero outside

$$\mathbf{A}_T^* \otimes H^\wedge = \prod_{v \in T} (k_v^* \otimes H^\wedge) \prod_{v \notin T} (\mathcal{O}_v^* \otimes H^\wedge).$$

We now describe the inverse Fourier transform of $\widehat{E}_{H,T}(x)$. For $\chi = (\chi_v)_v \in \text{Hom}(\mathbf{A}^*, H)$, let

$$E_T(\chi) := \prod_v E_{T,v}(\chi_v),$$

where

$$E_{T,v}(\chi_v) := \begin{cases} \zeta_{k_0,v}(1)^{-\nu} f_v(\chi_v) & v \in T, \\ 1 & v \notin T \text{ and } \chi_v \in \text{Hom}(k_v^*/\mathcal{O}_v^*, H) \\ 0 & v \notin T \text{ and } \chi_v \notin \text{Hom}(k_v^*/\mathcal{O}_v^*, H). \end{cases}$$

By a simple local calculation, $\widehat{E}_{H,T}(x) = \widehat{E}_T(x; 1/(|H|(1-Q^{-1})))$, where $\widehat{E}_T(x; s)$ is defined as at the start of Subsection 3.3, with E_T for f and H for G . As in Proposition 3.8, we obtain

$$\frac{1}{|\mathcal{O}_k^* \otimes H^\wedge|} \sum_{x \in k^* \otimes H^\wedge} \widehat{E}_{H,T}(x) = \sum_{\chi \in \text{Hom}(\mathbf{A}^*/k^*, H)} \frac{E_T(\chi)}{\Phi_H(\chi)^{1/(|H|(1-Q^{-1}))}}. \quad (4.17)$$

Indeed, if $Q \nmid |H|$ then we can apply Proposition 3.8 directly. If $Q \mid |H|$ then we already know that the Fourier transform $\widehat{E}_T(x; s)$ exists for $s = 1/\alpha(H)$. Moreover, the sums on both sides are finite, as the summands $\widehat{E}_{H,T}(x)$ and

$E_T(\chi)$ are supported on compact sets, and both $k^* \otimes H^\wedge$ and $\text{Hom}(\mathbf{A}^*/k^*, H)$ are discrete. Hence, conditions (1) and (2) in the proof of Proposition 3.8 hold trivially.

Using Lemma 2.1 to express the right-hand side of (4.17) in terms of discriminant series, and substituting this into (4.16), we see that $c_{f,T}(k, G)$ equals

$$\sum_{H \subseteq G} \mu(G/H) \sum_{J \subseteq H} \sum_{\chi \in \text{J-ext}(k)} \frac{E_T(\chi)}{\Delta(\chi)^{1/(|J|(1-Q^{-1}))}} = \sum_{\chi \in G\text{-ext}(k)} \frac{E_T(\chi)}{\Phi_G(\chi)^{1/\alpha}}, \quad (4.18)$$

where the last equality holds by Delsarte's inversion formula [17]. Note that the right-hand side is a sum with non-negative terms.

Recall our assumption in the statement of Theorem 1.7 that there exists a G -extension φ of k such that $f(\varphi) = 1$. Let T_0 be a finite set of places of k , containing S and all places at which φ is ramified, that is, all places where $\mathcal{O}_v^* \not\subseteq \ker \varphi_v$. Furthermore, we choose T_0 big enough to ensure that

$$\mathbf{A}^*(T_0)/(\ker \varphi \cap \mathbf{A}^*(T_0)) \cong \left(\prod_{v \in T_0} k_v^* \right) / (\ker \varphi \cap \prod_{v \in T_0} k_v^*) \cong G.$$

For any $T \supseteq T_0$, the G -extension φ appears in the sum on the right-hand side of (4.18), and $E_T(\varphi) > 0$.

We now use φ to construct many more G -extensions χ of k that contribute to the sum on the right-hand side of (4.18). Let $\chi \in \text{Hom}(\mathbf{A}^*/k^*, G)$ be any sub- G -extension with the property that $\chi_v = \psi_v$ for all $v \in T_0$. Then we have $\ker \chi \cap \prod_{v \in T_0} k_v^* = \ker \varphi \cap \prod_{v \in T_0} k_v^*$, so $\mathbf{A}^*/\ker \chi \cong G$, and thus $\chi \in G\text{-ext}(k)$. Therefore,

$$c_{f,T}(k, G) \geq \sum_{\substack{\chi \in \text{Hom}(\mathbf{A}^*/k^*, G) \\ \chi_v = \varphi_v \text{ for } v \in T_0}} \frac{E_T(\chi)}{\Phi_G(\chi)^{1/\alpha}}.$$

We construct $\chi \in \text{Hom}(\mathbf{A}^*/k^*, G)$ with $\chi_v = \varphi_v$ for $v \in T_0$ and $E_T(\chi) > 0$ as follows. For $\psi = (\psi_v)_v \in \text{Hom}(\mathbf{A}^*, G)$, let

$$h_v(\psi_v) := \begin{cases} 1 & \text{if } [\mathcal{O}_v^* : (\ker \psi_v \cap \mathcal{O}_v^*)] \in \{1, Q\}, \\ 0 & \text{if } [\mathcal{O}_v^* : (\ker \psi_v \cap \mathcal{O}_v^*)] \notin \{1, Q\}, \end{cases}$$

and

$$h_{T,v}(\psi_v) := \begin{cases} 1 & \text{if } \psi_v = \mathbb{1} \text{ and } v \in T_0, \\ 0 & \text{if } \psi_v \neq \mathbb{1} \text{ and } v \in T_0, \\ \zeta_{k_0,v}(1)^{-\nu} h_v(\psi_v) & \text{if } v \in T \setminus T_0, \\ 1 & \text{if } \mathcal{O}_v^* \subseteq \ker \psi_v \text{ and } v \notin T, \\ 0 & \text{if } \mathcal{O}_v^* \not\subseteq \ker \psi_v \text{ and } v \notin T. \end{cases}$$

Let $h_T := \prod_v h_{T,v}$. For any ψ with $h_T(\psi) \neq 0$, let $\chi := \psi\varphi$. Then $\chi_v = \varphi_v$ for $v \in T_0$. Our condition (1.4) on Λ_v and the fact that φ is unramified outside T_0 show that $h_{T,v}(\psi_v) \neq 0$ implies $f_v(\chi_v) = 1$ for $v \in T$. Also, $\Phi_G(\chi_v) = \Phi_G(\varphi_v)$ if $v \in T_0$, and $\Phi_G(\chi_v) = \Phi_G(\psi_v)$ if $v \notin T_0$. We have shown that

$$c_{f,T}(k, G) \geq \prod_{v \in T_0} (\zeta_{k_0,v}(1)^{-\nu} \Phi_G(\varphi_v)^{-1/\alpha}) \sum_{\psi \in \text{Hom}(\mathbf{A}^*/k^*, G)} \frac{h_T(\psi)}{\Phi_G(\psi)^{1/\alpha}}.$$

The factor in front of the sum is positive and does not depend on T . Hence, it is enough to show that

$$R := \lim_{T \rightarrow \Omega_k} \sum_{\psi \in \text{Hom}(\mathbf{A}^*/k^*, G)} \frac{h_T(\psi)}{\Phi_G(\psi)^{1/\alpha}} > 0.$$

We observe that h_T is supported on $\text{Hom}(\mathbf{A}^*, G)(T)$, and that $h_{T,v}(\psi_v) = 1$ whenever $v \notin T$ and $\psi_v \in \text{Hom}(k_v^*/\mathcal{O}_v^*, G)$. In particular, the above sum is finite for every T . As in Subsection 3.3, but with $s = 1/\alpha$ and $h_{T,v}$ instead of f_v , we define the local and global Fourier transforms $\widehat{h}_{T,v}(x_v; 1/\alpha)$ and $\widehat{h}_T(x; 1/\alpha)$ of $h_T \Phi_G^{-1/\alpha}$. Then $\widehat{h}_T(x; 1/\alpha) = \prod_v \widehat{h}_{T,v}(x_v; 1/\alpha)$ and

$$\widehat{h}_{T,v}(x_v; 1/\alpha) = \begin{cases} |G|^{-1} & \text{if } v \in T_0, \\ \zeta_{k_0,v}(1)^{-\nu} \widehat{h}_v(x_v; 1/\alpha) & \text{if } v \in T \setminus T_0, \\ 1 & \text{if } x_v \in \mathcal{O}_v^* \otimes G^\wedge \text{ and } v \notin T, \\ 0 & \text{if } x_v \notin \mathcal{O}_v^* \otimes G^\wedge \text{ and } v \notin T, \end{cases}$$

where

$$\widehat{h}_v(x_v; 1/\alpha) := \frac{1}{|G|} \sum_{\psi_v \in \text{Hom}(k_v^*, G)} \frac{h_v(\psi_v) \langle \psi_v, x_v \rangle}{\Phi_G(\psi_v)^{1/\alpha}}.$$

By the Poisson summation formula, as in Proposition 3.8, we obtain

$$R = \lim_{T \rightarrow \Omega_k} \frac{1}{|\mathcal{O}_k^* \otimes G^\wedge|} \sum_{x \in k^* \otimes G^\wedge} \widehat{h}_T(x; 1/\alpha). \quad (4.19)$$

The sum over x is finite, since all summands for $x \notin \mathcal{O}_T^* \otimes G^\wedge$ vanish. In fact, even more holds. Let us compute the local factors $\widehat{h}_v(x_v; 1/\alpha)$.

Lemma 4.9. *Let $v \notin T_0$. If $x_v \in \mathcal{O}_v^* \otimes G^\wedge$, then*

$$\widehat{h}_v(x_v; 1/\alpha) = \begin{cases} 1 + (Q^\beta - 1)q_v^{-1} & \text{if } q_v \equiv 1 \pmod{Q} \text{ and } x_v \in \mathcal{O}_v^{*Q} \otimes G^\wedge, \\ 1 - q_v^{-1} & \text{if } q_v \equiv 1 \pmod{Q} \text{ and } x_v \notin \mathcal{O}_v^{*Q} \otimes G^\wedge, \\ 1 & \text{if } q_v \not\equiv 1 \pmod{Q}. \end{cases}$$

If $x_v \notin \mathcal{O}_v^* \otimes G^\wedge$, then $\widehat{h}_v(x_v; 1/\alpha) = 0$.

Proof. This follows from Lemma 3.3, similarly to the proof of Lemma 4.1. \square

Hence, $\widehat{h}_T(x; 1/\alpha) = 0$ unless $x \in \mathcal{O}_{T_0}^* \otimes G^\wedge$. Since this is independent of T , we may exchange limit and sum in (4.19) to obtain

$$R = \frac{1}{|\mathcal{O}_k^* \otimes G^\wedge| |G|^{|T_0|}} \sum_{x \in \mathcal{O}_{T_0}^* \otimes G^\wedge} \prod_{v \notin T_0} \zeta_{k_0,v}(1)^{-\nu} \widehat{h}_v(x_v; 1/\alpha). \quad (4.20)$$

Compare Lemma 4.9 to the bounds (4.15) for $\zeta_{k_0,v}(1)^{-\nu}$. For $x \neq \mathbb{1}$, the Euler product in (4.20) may diverge to 0 or converge. However, it is clear that the Euler product converges for $x = \mathbb{1}$. Possibly enlarging T_0 by some small places, we may assume that all occurring Euler factors are positive. Thus, the product for $x = \mathbb{1}$ is positive and hence $R > 0$. This completes the proof of Theorem 1.7. \square

5. SOME APPLICATIONS OF THEOREM 1.7

We now present two applications of Theorem 1.7, upon which the proofs of Theorem 1.1 and Theorem 1.5 will be based. Given a finite abelian extension K/k and a place v of k , we denote by D_v the decomposition group at v .

Even though Theorem 1.7 gives a positive proportion result, it can also be used to prove 0% results.

Theorem 5.1. *Let G be a finite abelian group and let Q be the smallest prime dividing $|G|$. Assume that G contains a subgroup A which is isomorphic to $(\mathbb{Z}/Q\mathbb{Z})^2$. Let S be a finite set of places of k . Then 0% of G -extensions $(K/k, \psi)$ have the property that $\psi(D_v) \neq A$ for all $v \notin S$.*

Note that Theorem 5.1 does not contradict Theorem 1.7; one may check using Lemma 6.6 below that the crucial assumption (1.4) does not hold in this case. The following will be used to prove Theorem 1.5.

Theorem 5.2. *Let G be a finite abelian group and let Q be the smallest prime dividing $|G|$. Let S be a finite set of places of k . Then as φ varies over all G -extensions of k , the following hold.*

- (1) *If the Q -Sylow subgroup of G is cyclic, then a positive proportion of the extensions K_φ/k have the property that all of their decomposition groups are cyclic.*
- (2) *If the Q -Sylow subgroup of G is not cyclic, then 0% of the extensions K_φ/k have the property that D_v is cyclic for all $v \notin S$*

5.1. Proof of Theorem 5.1. We are free to increase the size of S so that it contains all archimedean places, all places dividing the order of G , and so that various Euler factors appearing in the following proofs are positive. Let $\alpha := \alpha(G)$ and let $\nu := \nu(k, G)$. We keep the notation β_H and β , for a subgroup $H \subseteq G$, from Subsection 4.3.

Now let R be a finite set of places of k which contains S . Let

$$\Lambda_v := \{\text{sub-}G\text{-extensions } \varphi_v \text{ of } k_v : \varphi_v(\text{Gal}(\bar{k}_v/k_v)) \neq A\}, \quad v \in R \setminus S,$$

and let Λ_v be the set of all sub- G -extensions of k_v for $v \notin R \setminus S$. Let $\Lambda_R = (\Lambda_v)_v$. We now apply Theorem 1.7 to obtain

$$\lim_{B \rightarrow \infty} \frac{N(k, G, \Lambda_R, B)}{N(k, G, B)} =: c_R$$

for some constant $c_R \geq 0$. To prove Theorem 5.1, it suffices to show that

$$\lim_{R \rightarrow \Omega_k} c_R = 0. \tag{5.1}$$

For each place v , let $f_{R,v}$ be the indicator function associated to Λ_v , as defined in Section 4.1. Then from (4.13) we obtain

$$c_R \ll \sum_{H \subseteq G} \sum_{x \in k^* \otimes H^\wedge} \prod_v \frac{|\widehat{f}_{R,H,v}(x_v; |G|/(|H|^\alpha))|}{\zeta_{k_0,v}(1)^\nu}. \tag{5.2}$$

We begin by calculating the local Fourier transforms at places in R .

Lemma 5.3. *Let $H \subseteq G$ be a subgroup for which $\beta_H = \beta$. Let $v \in R \setminus S$, let $\operatorname{Re} s \geq 0$ and let $\delta_H := (Q^2 - 1)(Q^2 - Q)/|H|$.*

If $x_v \in \mathcal{O}_v^ \otimes H^\wedge$, then there exists some $c_v(x_v) \in \mathbb{C}$ with $|c_v(x_v)| \leq (Q^\beta - 1 - \delta_H)$, such that*

$$\widehat{f}_{R,H,v}(x_v; s|G|/|H|) = \begin{cases} 1 + c_v(x_v)q_v^{-\alpha(G)s} + O(q_v^{-(\alpha(G)+1)s}), & \text{if } q_v \equiv 1 \pmod{Q}, \\ 1 + O(q_v^{-(\alpha(G)+1)s}), & \text{if } q_v \not\equiv 1 \pmod{Q}. \end{cases}$$

If $x_v \notin \mathcal{O}_v^ \otimes H^\wedge$, then $\widehat{f}_{R,H,v}(x_v; s|G|/|H|) = O(q_v^{-(\alpha(G)+1)s})$.*

Proof. The proof is very similar to the proof of Lemma 4.1, so we shall be brief. If $x_v \notin \mathcal{O}_v^* \otimes H^\wedge$, then since we are not removing any unramified sub- G -extensions, a similar proof to Lemma 4.1 gives the upper bound. So assume that $x_v \in \mathcal{O}_v^* \otimes H^\wedge$. The case $q_v \not\equiv 1 \pmod{Q}$ is handled as in Lemma 4.1. From now on, we assume that $q_v \equiv 1 \pmod{Q}$. We apply Lemma 3.3 to obtain

$$\widehat{f}_{R,H,v}(x_v; s|G|/|H|) = 1 + \frac{1}{|H|} \sum_{\substack{\chi_v \in \operatorname{Hom}(k_v^*, H) \\ \ker \chi_v \cap \mathcal{O}_v^* = \mathcal{O}_v^{*Q}}} f_v(\chi_v) \langle \chi_v, x_v \rangle q_v^{-\alpha(G)s} + O(q_v^{-(\alpha(G)+1)s}).$$

Using $|\langle \chi_v, x_v \rangle| \leq 1$ and the definition of f_v , we have

$$\left| \sum_{\substack{\chi_v \in \operatorname{Hom}(k_v^*, H) \\ \ker \chi_v \cap \mathcal{O}_v^* = \mathcal{O}_v^{*Q}}} f_v(\chi_v) \langle \chi_v, x_v \rangle \right| \leq \# \left\{ \chi_v \in \operatorname{Hom}(k_v^*, H) : \begin{array}{l} \ker \chi_v \cap \mathcal{O}_v^* = \mathcal{O}_v^{*Q}, \\ \chi_v(k_v^*) \neq A. \end{array} \right\}$$

However, as in the proof of Lemma 4.1, we have

$$\#\{\chi_v \in \operatorname{Hom}(k_v^*, H) : \ker \chi_v \cap \mathcal{O}_v^* = \mathcal{O}_v^{*Q}\} = (Q^\beta - 1)|H|.$$

Moreover, as the ramification is tame, the condition $\chi_v(k_v^*) = A$ implies that $\ker \chi_v \cap \mathcal{O}_v^* = \mathcal{O}_v^{*Q}$. Hence it suffices to observe that

$$\#\{\chi_v \in \operatorname{Hom}(k_v^*, H) : \chi_v(k_v^*) = A\} = (Q^2 - 1)(Q^2 - Q),$$

as this equals the number of surjective homomorphisms $k_v^* \rightarrow A$. This proves the lemma. \square

We use this to show the following.

Lemma 5.4. *Let H be a subgroup of G , let $x \in k^* \otimes H^\wedge$ and let*

$$F(R, x) := \prod_v \frac{|\widehat{f}_{R,H,v}(x_v; |G|/(|H|\alpha))|}{\zeta_{k_0,v}(1)^\nu}.$$

Let

$$T(x) = S \cup \{v \text{ place of } k : x_v \notin \mathcal{O}_v^* \otimes H^\wedge\}.$$

Then the following statements hold.

- (1) *Pointwise in x , we have $\lim_{R \rightarrow \Omega_k} F(R, x) = 0$.*
- (2) *There is $C > 0$ such that $F(R, x) \ll \prod_{v \in T(x)} Cq_v^{-1-1/\alpha}$, uniformly in R and x .*

Proof. If $\beta_H \neq \beta$, then Lemma 4.5 shows that $F(R, x) = 0$ for all R, x . So let us assume that $\beta_H = \beta$. We fix R, x and define, for $v \in \Omega_k$,

$$F_v := \frac{|\widehat{f}_{R,H,v}(x_v; |G|/(|H|\alpha))|}{\zeta_{k_0,v}(1)^\nu}.$$

Then

$$F(R, x) = \prod_{v \in T(x)} F_v \prod_{\substack{v \in \Omega_k \setminus T(x) \\ q_v \not\equiv 1 \pmod{Q}}} F_v \prod_{\substack{v \in R \setminus T(x) \\ q_v \equiv 1 \pmod{Q}}} F_v \prod_{\substack{v \in \Omega_k \setminus (R \cup T(x)) \\ q_v \equiv 1 \pmod{Q}}} F_v.$$

We now bound these four products explicitly in R, x , by comparing the bounds for $\widehat{f}_{R,H,v}$ from Lemma 4.1 and Lemma 5.3 with the bounds for $\zeta_{k_0,v}(1)^{-\nu}$ from (4.15). We obtain

$$\prod_{v \in T(x)} F_v \ll \prod_{v \in T(x)} Cq_v^{-1-1/\alpha}, \quad (5.3)$$

$$\prod_{\substack{v \in R \setminus T(x) \\ q_v \equiv 1 \pmod{Q}}} F_v \ll \prod_{\substack{v \in R \setminus T(x) \\ q_v \equiv 1 \pmod{Q}}} (1 - \delta_H q_v^{-1} + O(q_v^{-1-1/\alpha})), \quad (5.4)$$

$$\prod_{\substack{v \in \Omega_k \setminus T(x) \\ q_v \not\equiv 1 \pmod{Q}}} F_v \ll 1, \quad \prod_{\substack{v \in \Omega_k \setminus (R \cup T(x)) \\ q_v \equiv 1 \pmod{Q}}} F_v \ll 1,$$

where δ_H is as in Lemma 5.3. Assertion (1) in the lemma follows from (5.4) and Chebotarev's density theorem. Assertion (2) follows from (5.3) and the fact that all other products are $\ll 1$. \square

Now (5.1), and thus Theorem 5.1, follows immediately from Lemma 3.7, Lemma 5.4 and Lebesgue's dominated convergence theorem. \square

5.2. Proof of Theorem 5.2. We require the following proposition.

Proposition 5.5. *Let k be a number field and G a finite solvable group. Then there exists a G -extension $(K/k, \psi)$ all of whose decomposition groups are cyclic.*

Proof. As explained in the proof of [30, Thm. 2], Shafarevich constructed such an extension in his resolution of the inverse Galois problem for solvable groups [27]. \square

To prove Theorem 5.2, first suppose that the Q -Sylow subgroup of G is cyclic. For each place v , let Λ_v be the set of all cyclic sub- G -extensions of k_v . We claim that Λ_v satisfies the condition (1.4) of Theorem 1.7 for all v . Indeed, let K_v/k_v be a sub- G -extension whose inertia group I_v injects into $\mathbb{Z}/Q\mathbb{Z}$. If $I_v = 0$ then G_v is clearly cyclic. Otherwise G_v is an extension of a cyclic group by $\mathbb{Z}/Q\mathbb{Z}$. Our assumptions on G now imply that G_v is also cyclic in this case, which proves the claim. Applying Theorem 1.7 and using Proposition 5.5, we obtain the result.

Now suppose that the Q -Sylow subgroup of G is not cyclic, so that G contains a subgroup A which is isomorphic to $(\mathbb{Z}/Q\mathbb{Z})^2$. Let $(K/k, \psi)$ be a G -extension such that D_v is cyclic for all $v \notin S$. Clearly $\psi(D_v) \neq A$ for all $v \notin S$. However, such extensions have density 0 in all G -extensions by Theorem 5.1, which proves the result in this case. \square

6. THE HASSE PRINCIPLE AND WEAK APPROXIMATION

We now use our analytic results to prove the remaining results on the Hasse norm principle and weak approximation, as stated in the introduction.

6.1. Norm one tori. We begin by recalling some results on norm one tori. Let K/k be a finite separable extension of fields. Consider the associated norm one torus $R_{K/k}^1 \mathbb{G}_m$, given as the kernel of the norm map

$$R_{K/k}^1 \mathbb{G}_m := \ker(R_{K/k} \mathbb{G}_m \rightarrow \mathbb{G}_m),$$

where $R_{K/k} \mathbb{G}_m$ denotes the Weil restriction of \mathbb{G}_m from K to k . If k is a number field, we denote by $\text{III}(R_{K/k}^1 \mathbb{G}_m)$ the Tate-Shafarevich group of $R_{K/k}^1 \mathbb{G}_m$ over k (see (1.7)). Our interest in this stems from the following well-known relation to the Hasse norm principle

$$\text{III}(R_{K/k}^1 \mathbb{G}_m) \cong (k^* \cap N_{K/k}(\mathbf{A}_K^*)) / N_{K/k}(K^*)$$

(see e.g. [28, p. 307]). We now recall how to calculate this group.

Theorem 6.1 (Tate). *Let G be a finite group and let $(K/k, \psi)$ be a G -extension of number fields. Then there is a canonical isomorphism*

$$\text{III}(R_{K/k}^1 \mathbb{G}_m)^\sim \cong \ker \left(\mathrm{H}^3(G, \mathbb{Z}) \rightarrow \prod_v \mathrm{H}^3(\psi(D_v), \mathbb{Z}) \right).$$

Proof. See e.g. [29, Ex. 5.6]. □

Here D_v denotes the decomposition group of K/k at v . Note that if H is a finite cyclic group, then $\mathrm{H}^3(H, \mathbb{Z}) = \mathrm{H}^1(H, \mathbb{Z}) = 0$. In particular, it is only the ramified primes which are relevant in Theorem 6.1.

Given a torus T over a number field k , we write

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

where $\overline{T(k)}$ denotes the closure of $T(k)$ in $\prod_v T(k_v)$ with respect to the product topology. This group measures the failure of weak approximation for T . The next result encapsulates the fact that the Brauer-Manin obstruction is the only obstruction to the Hasse principle and weak approximation for the norm one tori $R_{K/k}^1 \mathbb{G}_m$, which is a special case of a general result of Voskresenskiĭ [34, Thm. 6].

Theorem 6.2 (Voskresenskiĭ). *Let G be a finite group and let $(K/k, \psi)$ be a G -extension of number fields. Then there is an exact sequence*

$$0 \rightarrow A(R_{K/k}^1 \mathbb{G}_m) \rightarrow \mathrm{H}^3(G, \mathbb{Z})^\sim \rightarrow \text{III}(R_{K/k}^1 \mathbb{G}_m) \rightarrow 0.$$

In particular, if $\mathrm{H}^3(G, \mathbb{Z}) \neq 0$ and $\text{III}(R_{K/k}^1 \mathbb{G}_m) = 0$, then $R_{K/k}^1 \mathbb{G}_m$ fails weak approximation.

Proof. This follows from [34, Thm. 6] and [15, Prop. 7] (see also [29, Ex. 5.6]). □

In our density results, we order norm one tori by the discriminant of the associated extension and count extensions of bounded discriminant. The following observation makes clear that we are only counting each such torus once this way.

Proposition 6.3. *Let k be a number field and let K_1/k and K_2/k be Galois extensions. Then $R_{K_1/k}^1 \mathbb{G}_m \cong R_{K_2/k}^1 \mathbb{G}_m$ if and only if K_1/k and K_2/k are isomorphic extensions.*

Proof. A Galois extension K/k is determined up to k -isomorphism by the set of primes of k which split completely in K [26, Cor. 13.19]. The proposition then follows from the fact that a prime \mathfrak{p} of k splits completely in K if and only if the base-change of $R_{K/k}^1 \mathbb{G}_m$ to $k_{\mathfrak{p}}$ is a split torus. \square

6.2. Proof of Theorem 1.3. Let G be a finite solvable group. If $H^3(G, \mathbb{Z}) = 0$, then G -extensions satisfy the Hasse norm principle by Theorem 6.1. On the other hand, if $H^3(G, \mathbb{Z}) \neq 0$ then let K/k be as in Proposition 5.5. Then $H^3(D_v, \mathbb{Z}) = 0$ for all v , hence the Hasse norm principle fails by Theorem 6.1. \square

6.3. Computations in group cohomology. We now proceed with some cohomological computations. Lemma 6.4 and Lemma 6.5 are certainly well-known; we include proofs for completeness.

Lemma 6.4. *Let G be a finite abelian group. Then there exists a canonical isomorphism*

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

Proof. The universal coefficient theorem yields an isomorphism

$$H^3(G, \mathbb{Z}) \cong \text{Ext}(H_2(G, \mathbb{Z}), \mathbb{Z}).$$

Next, one has a canonical identification $H_2(G, \mathbb{Z}) \cong \wedge^2 G$ (see [10, Thm. V.6.4]), for example). Applying $\text{Hom}(\wedge^2 G, \cdot)$ to the exact sequence

$$0 \rightarrow \mathbb{Z} \rightarrow \mathbb{Q} \rightarrow \mathbb{Q}/\mathbb{Z} \rightarrow 0,$$

one obtains the exact sequence

$$\text{Hom}(\wedge^2 G, \mathbb{Q}) \rightarrow \text{Hom}(\wedge^2 G, \mathbb{Q}/\mathbb{Z}) \rightarrow \text{Ext}(\wedge^2 G, \mathbb{Z}) \rightarrow \text{Ext}(\wedge^2 G, \mathbb{Q}).$$

However, the first group is trivial as $\wedge^2 G$ is finite, and the last group is trivial as \mathbb{Q} is divisible. This proves the result. \square

The above result is very important for our work, as, together with Theorem 6.1, it allows one to translate problems involving the Hasse norm principle for abelian extensions into simple problems in linear algebra. We will use this duality between $H^3(G, \mathbb{Z})$ and $\wedge^2 G$ implicitly throughout the rest of this paper.

Lemma 6.5. *Let $n_{j+1} \mid n_j$ and*

$$G = \mathbb{Z}/n_1\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/n_l\mathbb{Z}.$$

Then

$$\wedge^2 G \cong (\mathbb{Z}/n_2\mathbb{Z}) \oplus \cdots \oplus (\mathbb{Z}/n_j\mathbb{Z})^{j-1} \oplus \cdots \oplus (\mathbb{Z}/n_l\mathbb{Z})^{l-1}.$$

In particular $\wedge^2 G = 0$ if and only if G is cyclic.

Proof. We use the following facts:

- (1) $\wedge^2(G_1 \oplus G_2) = \wedge^2 G_1 \oplus (G_1 \otimes G_2) \oplus \wedge^2 G_2$.
- (2) $\wedge^2(\mathbb{Z}/n\mathbb{Z}) = 0$.
- (3) $\mathbb{Z}/n\mathbb{Z} \otimes \mathbb{Z}/m\mathbb{Z} \cong \mathbb{Z}/\text{gcd}(n, m)\mathbb{Z}$.

By induction, we therefore obtain

$$\wedge^2 G \cong \bigoplus_{i < j} (\mathbb{Z}/n_i \mathbb{Z} \otimes \mathbb{Z}/n_j \mathbb{Z}) \cong \bigoplus_{i < j} \mathbb{Z}/n_j \mathbb{Z},$$

which yields the result. \square

The next lemma is the reason for the dichotomy which occurs between Theorem 1.1 and Theorem 1.4.

Lemma 6.6. *Let G be a finite abelian group and let p be a prime dividing $|G|$. Then the exponent of $\wedge^2 G$ divides p if and only if $G \cong \mathbb{Z}/n\mathbb{Z} \oplus (\mathbb{Z}/p\mathbb{Z})^r$ for some n with $p \mid n$ and some $r \geq 0$.*

Proof. This follows easily from Lemma 6.5. \square

Whilst the question of whether an abelian extension satisfies the Hasse norm principle is quite complicated in general, it turns out that for weak approximation there is a simple local criterion.

Lemma 6.7. *Let K/k be an abelian extension of number fields. Then $R_{K/k}^1 \mathbb{G}_m$ satisfies weak approximation if and only if the decomposition group of K/k at each place of k is cyclic.*

Proof. Let $G = \text{Gal}(K/k)$. By Theorem 6.1 and Theorem 6.2, it suffices to show that the equality

$$H^3(G, \mathbb{Z}) = \ker \left(H^3(G, \mathbb{Z}) \rightarrow \prod_v H^3(D_v, \mathbb{Z}) \right)$$

holds if and only if all D_v are cyclic. For each place v , the homomorphism $H^3(G, \mathbb{Z}) \rightarrow H^3(D_v, \mathbb{Z})$ is surjective, as the dual homomorphism $\wedge^2 D_v \rightarrow \wedge^2 G$ is injective. The result then follows from the final assertion of Lemma 6.5, namely that $H^3(D_v, \mathbb{Z}) = 0$ if and only if D_v is cyclic. \square

6.4. Proof of Theorem 1.2. This follows from Theorem 1.3 and Lemma 6.5, which show that $H^3(G, \mathbb{Z}) = 0$ if and only if G is cyclic. \square

6.5. Proof of Theorem 1.5. This follows immediately from Theorem 5.2 and Lemma 6.7. \square

6.6. Proof of Theorem 1.6. To prove Theorem 1.6 it suffices to show the following.

Proposition 6.8. *Let k be a number field and let G be a finite abelian group. Then there exists a G -extension $(K/k, \psi)$ such that $\text{III}(R_{K/k}^1 \mathbb{G}_m) = 0$.*

Indeed, assume that G is non-cyclic and let $(K/k, \psi)$ be as in Proposition 6.8. Then our assumptions, together with Theorem 6.2 and Lemma 6.5, imply that

$$A(R_{K/k}^1 \mathbb{G}_m) \neq 0, \quad \text{III}(R_{K/k}^1 \mathbb{G}_m) = 0. \quad (6.1)$$

Hence K/k satisfies the Hasse norm principle and $R_{K/k}^1 \mathbb{G}_m$ fails weak approximation. Moreover, let S be the set of places where K/k is ramified. Then applying Theorem 1.7 with $\Lambda_v = \{(K_v/k_v, \psi_v)\}$ for $v \in S$ and Λ_v taken to be the set of all sub- G -extensions of k_v for $v \notin S$, by Theorem 6.1 we obtain the existence of a

positive proportion of G -extensions of k which also satisfy (6.1). This is clearly sufficient for Theorem 1.6.

We prove Proposition 6.8 by finding sufficient local conditions for the Hasse norm principle to hold. We begin with the following lemma (cf. a result of Bogomolov [16, Thm. 7.1]). We call an abelian group bicyclic if it is a product of two cyclic groups and is not cyclic.

Lemma 6.9. *Let G be a finite abelian non-cyclic group. Then there exists a finite collection of bicyclic subgroups $G_i \subseteq G$ for $i \in I$, such that the natural map*

$$\bigoplus_{i \in I} \wedge^2 G_i \rightarrow \wedge^2 G$$

is an isomorphism. Furthermore, if the exponent of $\wedge^2 G$ divides a prime p , then all G_i may be chosen isomorphic to $(\mathbb{Z}/p\mathbb{Z})^2$.

Proof. Write

$$G = \mathbb{Z}/n_1\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/n_l\mathbb{Z}, \quad n_{j+1} \mid n_j$$

and let

$$G_{i,j} = \mathbb{Z}/n_i\mathbb{Z} \oplus \mathbb{Z}/n_j\mathbb{Z}, \quad 1 \leq i < j \leq l.$$

Then the natural map

$$\varphi : \bigoplus_{1 \leq i < j \leq l} \wedge^2 G_{i,j} \rightarrow \wedge^2 G$$

is surjective. Moreover, Lemma 6.5 shows that the domain and codomain have the same cardinality, thus φ is an isomorphism. This proves the first part of the lemma. If the exponent of $\wedge^2 G$ divides a prime p , then a similar argument, combined with Lemma 6.6, gives the result. \square

We now show that one can realise any bicyclic extension over *some* local field.

Lemma 6.10. *Let k be a number field and let $n, m \in \mathbb{N}$. Let v be a place of k which is completely split in $k(\mu_n)$. Then there exists an abelian extension K_v/k_v whose Galois group is isomorphic to*

$$\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}.$$

Proof. Adjoin an n th root of a uniformiser to the unique unramified extension of k_v of degree m . \square

We now need to construct an abelian extension which realises certain given local extensions. As explained in the introduction, this need not always be possible. However, the only problems which arise concern the prime 2. We shall content ourselves with the following well-known result, which may be deduced, for example, from the methods and results of [27, §IX.2].

Proposition 6.11. *Let S be a finite set of non-archimedean places of a number field k and let G be a finite abelian group. For each $v \in S$, let $(K_v/k_v, \psi_v)$ be a sub- G -extension. Assume that S does not contain any primes which lie above 2. Then there exists a G -extension $(K/k, \psi)$ which has the given completions $(K_v/k_v, \psi_v)$ for $v \in S$.*

Using this, we may now prove Proposition 6.8.

Proof of Proposition 6.8. Let G_i be as in Lemma 6.9. By Lemma 6.10, there exist distinct places $v_i \nmid 2$ of k and G_i -extensions $(K_{v_i}/k_{v_i}, \psi_{v_i})$. By Proposition 6.11, there exists a G -extension $(K/k, \psi)$ which realises these local extensions. Then by Lemma 6.4 and Lemma 6.9 the map

$$H^3(G, \mathbb{Z}) \rightarrow \prod_v H^3(\psi_v(D_v), \mathbb{Z}),$$

is injective. Hence $\text{III}(\mathbb{R}_{K/k}^1 \mathbb{G}_m) = 0$ by Theorem 6.1, as required. \square

As explained at the beginning of the section, this completes the proof of Theorem 1.6. \square

6.7. Proof of Theorem 1.1. We begin with the following lemma, which gives necessary local conditions for the Hasse norm principle to fail.

Lemma 6.12. *Let k be a number field, let $n > 1$ and $r \geq 0$. Let Q be the smallest prime dividing n and let $G = \mathbb{Z}/n\mathbb{Z} \oplus (\mathbb{Z}/Q\mathbb{Z})^r$. Then there exists a collection of subgroups $G_i \subseteq G$ for $i \in I$ that are each isomorphic to $(\mathbb{Z}/Q\mathbb{Z})^2$, with the following property. If a G -extension $(K/k, \psi)$ fails the Hasse norm principle, then there exists some $i \in I$ such that $\psi(D_v) \neq G_i$ for all places v of k .*

Proof. By Lemma 6.6, the exponent of $\wedge^2 G$ divides Q . We then choose the G_i as in the second part of Lemma 6.9. Let $(K/k, \psi)$ be a G -extension which fails the Hasse norm principle. If for each $i \in I$ there exists some v such that $\psi(D_v) = G_i$, then by Theorem 6.1 we see that $\text{III}(\mathbb{R}_{K/k}^1 \mathbb{G}_m) = 0$; a contradiction. \square

Using Lemma 6.12, we therefore obtain

$$\begin{aligned} & \#\{(K/k, \psi) \in G\text{-ext}(k) : \Delta(K/k) \leq B, \text{III}(\mathbb{R}_{K/k}^1 \mathbb{G}_m) \neq 0\} \\ & \leq \#\{(K/k, \psi) \in G\text{-ext}(k) : \Delta(K/k) \leq B, \exists i \in I \text{ s.t. } \psi(D_v) \neq G_i \forall v\} \\ & \leq \sum_{i \in I} \#\{(K/k, \psi) \in G\text{-ext}(k) : \Delta(K/k) \leq B, \psi(D_v) \neq G_i \forall v\}. \end{aligned}$$

As $G_i \cong (\mathbb{Z}/Q\mathbb{Z})^2$, we may now apply Theorem 5.1 to obtain Theorem 1.1. \square

6.8. Proof of Theorem 1.4. The following lemma gives sufficient local conditions for the Hasse norm principle to fail.

Lemma 6.13. *Let G be as in Theorem 1.4 and let $(K/k, \psi)$ be a G -extension. Suppose that for all places v , either the inertia group at v has order dividing Q or the decomposition group D_v is cyclic. Then K/k fails the Hasse norm principle.*

Proof. By Lemma 6.6, we see that $\wedge^2 G$ has a non-zero element whose order is not Q . Let v be a place of k . If D_v is cyclic, then $\wedge^2 D_v = 0$. Otherwise, by our assumptions, we have $D_v \cong \mathbb{Z}/Q\mathbb{Z} \oplus H$ for some cyclic group H with $Q \mid |H|$. Thus by Lemma 6.5, we obtain $\wedge^2 D_v \cong \mathbb{Z}/Q\mathbb{Z}$. Hence the map

$$\prod_v \wedge^2(\psi(D_v)) \rightarrow \wedge^2 G$$

is not surjective. Therefore its dual is not injective, and so the Hasse norm principle fails by Theorem 6.1. \square

Theorem 1.4 is now an immediate consequence of Theorem 1.7, Proposition 5.5, and Lemma 6.13. \square

REFERENCES

- [1] A. Baily, On the density of discriminants of quartic fields. *J. reine angew. Math.* **315** (1980) 190–210.
- [2] A. Baily, On octic fields of exponent 2. *J. reine angew. Math.* **328** (1981) 33–38
- [3] V. Batyrev, Y. Tschinkel, Manin’s conjecture for toric varieties. *J. Algebraic Geom.*, **7**(1) (1998), 15–53.
- [4] M. Bhargava, A positive proportion of plane cubics fail the Hasse principle, preprint. arXiv:1402.1131.
- [5] M. Bhargava, The geometric sieve and the density of squarefree values of invariant polynomials, preprint. arXiv:1402.0031.
- [6] N. Bourbaki, *Éléments de mathématique. Fasc. XXXII. Théories spectrales. Ch. I: Algèbres normées. Ch. II: Groupes localement compacts commutatifs*, Actualités Scientifiques et Industrielles, No. 1332 Hermann, Paris 1967
- [7] R. de la Bretèche, T. Browning, Contre-exemples au principe de Hasse pour certains tores coflasques. *J. Théor. Nombres Bordeaux* **26** (2014), 25–44.
- [8] R. de la Bretèche, T. Browning, Density of Châtelet surfaces failing the Hasse principle. *Proc. London Math. Soc.* **108** (2014), 1030–1078.
- [9] M. Bright, T. Browning, D. Loughran, Failures of weak approximation in families. *Compositio Math.* **152**(71) (2016), 1435–1475.
- [10] K. Brown, *Cohomology of groups*. Graduate Texts in Mathematics, **87**. Springer-Verlag, New York-Berlin, 1982.
- [11] T. Browning, R. Newton, The proportion of failures of the Hasse norm principle. *Mathematika* **62** (2016), 337–347.
- [12] A. Chambert-Loir, Y. Tschinkel, Fonctions Zêta des hauteurs des espaces fibrés. *Rational points on algebraic varieties*, 71–115, Progress in Math. 199, Birkhäuser, 2001
- [13] H. Cohen, F. Diaz y Diaz, M. Olivier, Enumerating quartic dihedral extensions of \mathbb{Q} . *Compositio Math.* **133**(1) (2002), 65–93.
- [14] H. Cohn, The density of abelian cubic fields. *Proc. Amer. Math. Soc.* **5** (1954), 476–477.
- [15] J.-L. Colliot-Thélène, J.-J. Sansuc, La R-équivalence sur les tores. *Ann. Sc. E.N.S.* **10** (1977), 175–229.
- [16] 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., Mumbai, 2007.
- [17] S. Delsarte, Fonctions de Möbius sur les groupes abéliens finis. *Ann. of Math.* **49** (1948), 600–609.
- [18] S. Gurak, On the Hasse norm principle. *J. reine angew. Math.* **299/300** (1978), 16–27.
- [19] N. Hoffmann, M. Spitzweck, Homological algebra with locally compact abelian groups. *Adv. Math.*, **212** (2007), 504–524.
- [20] M. Horie, The Hasse norm principle for elementary abelian extensions. *Proc. Amer. Math. Soc.* **118**(1) (1993) 47–56.
- [21] H. Iwaniec, E. Kowalski, *Analytic number theory*. Amer. Math. Soc., 2004.
- [22] M. Khushvaktov, Distribution of the discriminants of regular abelian extensions of degree n of the field of rational numbers, *Tashkent. Gos. Univ. Nauchn. Trody* **548** Voprosy Mat. (1977) 109–114, 146.
- [23] S. Mäki, On the density of abelian number fields. *Ann. Acad. Sci. Fenn. Ser. A I. Math. Diss.* **54** (1985).
- [24] C. Moreno, *Advanced analytic number theory: L-functions*. Mathematical Surveys and Monographs, 115. American Mathematical Society, Providence, RI, 2005.
- [25] M. Moskowitz, Homological algebra in locally compact abelian groups. *Trans. Amer. Math. Soc.*, **127** (1967), 361–404.

- [26] J. Neukirch, *Algebraic number theory*. Grundlehren der Mathematischen Wissenschaften, **322**. Springer-Verlag, Berlin, 1999.
- [27] J. Neukirch, A. Schmidt, K. Wingberg, *Cohomology of Number Fields*. Springer-Verlag, 2000.
- [28] V. Platonov, A. Rapinchuk, *Algebraic groups and number theory*. Pure and Applied Mathematics, 139. Academic Press, Inc., Boston, MA, 1994.
- [29] 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.
- [30] J. Sonn, Polynomials with roots in \mathbb{Q}_p for all p . *Proc. Amer. Math. Soc.* **136** (2008), no. 6, 1955–1960.
- [31] H. Steckel, Dichte von Frobeniuskörpern bei fixiertem Kernkörper. *J. reine angew. Math.* **343** (1983) 36–63.
- [32] M. Taylor, On the equidistribution of Frobenius in cyclic extensions of a number field, *J. London Math. Soc.* (2) **29** (1984) 211–223.
- [33] B. Urazbaev, The distribution of cyclic fields. *Izv. Akad. Nauk. Kazakh. SSR Ser. Fiz.-Mat.* (1977) No. 5, 66–70, 93.
- [34] V. Voskresenskii, Birational properties of linear algebraic groups. *Izv. Akad. Nauk SSSR Ser. Mat.* **34** (1970), 3–19.
- [35] S. Wang, On Grunwald’s theorem. *Ann. of Math.* **51** (1950), 471–484.
- [36] M. Wood, On the probabilities of local behaviors in abelian field extensions. *Compositio Math.* **146** (2010), no. 1, 102–128.
- [37] D. Wright, Distribution of discriminants of abelian extensions. *Proc. London Math. Soc.* **58** (1989), no. 1, 17–50.
- [38] X. Zhang, On number fields of type (l, l, \dots, l) . *Sci. Sinica Ser. A* **27** (1984) 1018–1026.

CHRISTOPHER FREI, TECHNISCHE UNIVERSITÄT GRAZ, INSTITUT FÜR ANALYSIS UND ZAHLENTHEORIE, STEYRERGASSE 30/II, A-8010 GRAZ, AUSTRIA.

E-mail address: frei@math.tugraz.at

URL: <http://www.math.tugraz.at/~frei/>

DANIEL LOUGHRAN, SCHOOL OF MATHEMATICS, UNIVERSITY OF MANCHESTER, OXFORD ROAD, MANCHESTER, M13 9PL, UK.

E-mail address: daniel.loughran@manchester.ac.uk

URL: <https://sites.google.com/site/danielloughran>

RACHEL NEWTON, DEPARTMENT OF MATHEMATICS AND STATISTICS, UNIVERSITY OF READING, WHITEKNIGHTS, PO BOX 220, READING RG6 6AX, UK.

E-mail address: r.d.newton@reading.ac.uk

URL: <https://racheldominica.wordpress.com/>