COMPOSITIO MATHEMATICA

Weak approximation on the norm one torus

P. Koymans and N. Rome

Weak approximation on the norm one torus

P. Koymans [ID] and N. Rome [ID]

Dedicated to Adèle Koymans-Funcken

ABSTRACT

For any abelian group A, we prove an asymptotic formula for the number of A-extensions $K/\mathbb{Q}$ of bounded discriminant such that the associated norm one torus $R^1_{K/\mathbb{Q}}\mathbb{G}_m$ satisfies weak approximation. We are also able to produce new results on the Hasse norm principle and to provide new explicit values for the leading constant in some instances of Malle's conjecture.

1. Introduction

Fix a finite abelian group A of order d. Let $K/\mathbb{Q}$ be a Galois extension with $\mathrm{Gal}(K/\mathbb{Q}) \cong A$. We can view K as d-dimensional $\mathbb{Q}$ vector space. Suppose that $\omega_1, \ldots, \omega_d$ is a basis; then consider the affine variety T over $\mathbb{Q}$ defined by the equation $N_{K/\mathbb{Q}}(x_1\omega_1 + \cdots + x_n\omega_n) = 1$. (Alternatively, T is the kernel $R^1_{K/\mathbb{Q}}\mathbb{G}_m$ of the norm map from the Weil restriction of scalars $R_{K/\mathbb{Q}}\mathbb{G}_m \to \mathbb{G}_m$.) The arithmetic of this torus is particularly interesting as both a question in the study of rational points on Fano varieties and in the context of arithmetic statistics. The close parallels between counting number fields of bounded discriminant and studying rational points on varieties has been the subject of much recent interest (see [ESZ23] and [DY22]). The torus will always have rational points, so we can ask how the rational points are distributed (qualitatively) on T.

DEFINITION 1.1. Let X/k be a smooth variety. We say that *weak approximation* holds for X if the rational points $X(k)$ are dense in the product of local points $\prod_\nu X(k_\nu)$, under the product topology.

If A is cyclic, then weak approximation is guaranteed on T by the Hasse norm theorem in class field theory (or by (1.2)). However, it was recently shown by Frei, Loughran and Newton [FLN18, Theorem 1.5] that for any non-cyclic abelian group A, there exist extensions $K/\mathbb{Q}$ with Galois group A such that the associated norm one torus fails to satisfy weak approximation. Our main result is to establish an asymptotic formula for precisely how many A-extensions, when ordered by absolute discriminant, are such that weak approximation holds on the norm one torus.

THEOREM 1.2. *Let A be a non-trivial finite abelian group and ℓ the smallest prime divisor of $|A|$. There exist constants $C(A)$, $\delta(A)$ and $\alpha(A)$, all positive, such that for all $X \geq 100$,*

we have

$$\#\{K/\mathbb{Q} : \mathrm{Disc}(K/\mathbb{Q}) \leq X, \mathrm{Gal}(K/\mathbb{Q}) \cong A \text{ and } R^1_{K/\mathbb{Q}}\mathbb{G}_m \text{ satisfies weak approximation}\}$$
$$= C(A)X^{\ell/(|A|\cdot(\ell-1))}(\log X)^{\alpha(A)-1} + O(X^{\ell/(|A|\cdot(\ell-1))}(\log X)^{\alpha(A)-1-\delta(A)}).$$

The constant $\alpha(A)$ has the explicit expression

$$\alpha(A) = \sum_{a \in A[\ell]-\{0\}} \frac{|\{b \in A : \mathrm{Hom}(\wedge^2(A), \mathbb{Q}/\mathbb{Z}) \to \mathrm{Hom}(\wedge^2(\langle a,b\rangle), \mathbb{Q}/\mathbb{Z}) \text{ is the zero map}\}|}{(\ell-1) \cdot |A|},$$
(1.1)

where $\wedge^2$ is the second exterior algebra and $\mathrm{Hom}(\wedge^2(A), \mathbb{Q}/\mathbb{Z}) \to \mathrm{Hom}(\wedge^2(\langle a,b\rangle), \mathbb{Q}/\mathbb{Z})$ is simply the natural restriction map.

Frei *et al.* [FLN18, Theorem 1.5] established that 0% of A-extensions (of any given number field) satisfy the weak approximation property when ordered by discriminant if the ℓ-Sylow subgroup of A is not cyclic (and otherwise a positive proportion do). This result is recovered for abelian extensions of $\mathbb{Q}$ by combining our result with Wright's theorem on the number of A-extensions of bounded discriminant [Wri89, Theorem 1.2]. Their results gave density statements but no information about the order of magnitude of the size of the set in Theorem 1.2. The only case where an asymptotic formula had previously been known is when $A \cong (\mathbb{Z}/2\mathbb{Z})^2$, by work of the second named author [Rom18].

1.1 The Hasse norm principle

The problem of weak approximation on $R^1_{K/\mathbb{Q}}\mathbb{G}_m$ is closely related to determining whether the *Hasse norm principle* holds for $K/\mathbb{Q}$. This problem asks: if an element of K is a norm for every local extension $K_{\mathfrak{p}}/\mathbb{Q}_p$, is it also a norm for the global extension $K/\mathbb{Q}$? In geometric language, do all the principal homogeneous spaces for the torus $R^1_{K/\mathbb{Q}}\mathbb{G}_m$ satisfy the Hasse principle? The connection between the two problems is made explicit by the following short exact sequence due to Voskresenskii [Vos70, Theorem 6]:

$$0 \to A(T) \to H^3(A, \mathbb{Z})^{\vee} \to \text{Ш}(T) \to 0,$$
(1.2)

where $\text{Ш}(T)$ is the Tate–Shafarevich group of the torus and $A(T) = (\prod_{\nu} T(\mathbb{Q}_{\nu}))/\overline{T(\mathbb{Q})}$ is the defect of weak approximation. This sequence can also be viewed as an artifact of the fact that the Brauer–Manin obstruction is the only obstruction to weak approximation for the torus and to the Hasse principle for any principal homogeneous space under the torus (see [San81]).

If $K/\mathbb{Q}$ is cyclic then Tate's theorem shows that $H^3(A, \mathbb{Z})^{\vee}$ is trivial, guaranteeing both the Hasse norm principle and weak approximation on the norm one torus. If the group $H^3(A, \mathbb{Z})^{\vee}$ is cyclic of prime order then either $\text{Ш}(T) = 0$ or $A(T) = 0$ but not both. In other words, the Hasse norm principle fails if and only if $R^1_{K/\mathbb{Q}}\mathbb{G}_m$ satisfies weak approximation. Therefore, in certain cases, one can deduce information about Hasse norm principle failure from our main theorem.

COROLLARY 1.3. *Suppose that $A \cong \prod_{i=1}^r (C_{p_i})^{n_i}$ for primes $p_1 < \cdots < p_r$ and natural numbers n_i such that $\prod_{i=1}^r n_i = 2$. Then there exist constants $C(A)$, $\delta(A)$ and $\alpha(A)$, all positive, such that for all $X \geq 100$, we have*

$$\#\{K/\mathbb{Q} : \mathrm{Disc}(K/\mathbb{Q}) \leq X, \mathrm{Gal}(K/\mathbb{Q}) \cong A \text{ and } K/\mathbb{Q} \text{ fails the Hasse norm principle}\}$$
$$= C(A)X^{\ell/(|A|\cdot(\ell-1))}(\log X)^{\alpha(A)-1} + O(X^{\ell/(|A|\cdot(\ell-1))}(\log X)^{\alpha(A)-1-\delta(A)}).$$

Moreover, if $n_1 \neq 2$, then a positive proportion of A-extensions fail the Hasse norm principle.

1305

When combined with Wright's theorem [Wri89], this corollary recovers density results due to Frei, Loughran and Newton [FLN18, Theorem 1.1] and the authors [KR23, Theorem 1.2] for such A. In §9, we give an explicit expression for the proportion of $(C_2 \times C_3 \times C_3)$-extensions failing the Hasse norm principle.

1.2 Proof structure

The arithmetic of the norm one torus is intimately connected with the arithmetic of the field K. Write D_p for the decomposition group of a prime p.

LEMMA 1.4. *The norm one torus $R^1_{K/\mathbb{Q}}$ satisfies weak approximation if and only if the restriction map $\mathrm{Hom}(\wedge^2(A), \mathbb{Q}/\mathbb{Z}) \to \mathrm{Hom}(\wedge^2(D_p), \mathbb{Q}/\mathbb{Z})$ is identically zero for all primes p.*

This lemma provides the key criterion by which we may distinguish fields with the weak approximation property. Therefore, our main result can be reinterpreted as a problem concerning counting the number of A-extensions, ordered by discriminant, with a set of allowed splitting conditions at every finite place. In general, such problems are extremely difficult and of great interest to the arithmetic statistics community. We are able to achieve success in this particular case by a combination of a clever parametrisation of the fields and detecting our splitting conditions using character sums.

More specifically, in §2, A-extensions will be parametrised by tuples of squarefree integers $(v_a)_{a \in A - \{0\}}$. In the formula for the discriminant, the higher the order of the group element a, the larger the exponent of the component v_a. Therefore, the components v_a with $a \in A[\ell] - \{0\}$ will carry the most weight in the formula and we assume that the remaining variables are quite small. In other words, we may fix an extension $L/\mathbb{Q}$ with $\mathrm{Gal}(L/\mathbb{Q}) \cong A/A[\ell]$ of small discriminant and allow K to vary across $A[\ell]$-extensions of L. This reduces the problem to understanding the number of multicyclic extensions of bounded discriminant with certain splitting conditions at each prime. This also explains the form of the logarithmic exponent given in (1.1), since inertia subgroups will typically live in $A[\ell]$.

The nature of the splitting conditions imposed on the multicyclic extension is encapsulated in the notion of f-*correctness* in §5. Theorem 5.2 establishes the necessary count for multicyclic extensions and this is used to establish the general statement in Theorem 5.3. Sections 6–8 are devoted to proving Theorem 5.2. Finally, in §9, we compute some explicit examples, elucidating the proof strategy and providing completely explicit leading constants in certain cases.

Remark. The fact that we can essentially reduce the problem to the multicyclic case is a consequence of the discriminant being an unfair counting function (in the language of Wood [Woo10]). It is very plausible that a similar approach will be fruitful when ordering fields in another way, but the task is made simpler under this parametrisation when ordering by discriminant.

Remark. Frei–Loughran–Newton [FLN22] also considered such problems when ordering fields by conductor instead of discriminant. In this setting, 0% of fields have weak approximation on the norm one torus, for any non-cyclic abelian group A. If A is a multicyclic group, then the discriminant is a fixed power of the conductor. As such our main results (in particular, the calculations in §9.1) recover (and improve) this density result for extensions over $\mathbb{Q}$.

It is also interesting to consider the problem of the statistics of the Hasse norm principle and weak approximation on the norm one torus for non-abelian extensions. Macedo showed in his thesis [Mac21] that 100% of D_4 octics over $\mathbb{Q}$ satisfy the Hasse norm principle and that 0% satisfy the weak approximation property, when ordering by either conductor or discriminant. The

conductor ordering part of his work is unconditional (thanks to work of Altuğ, Shankar, Varma and Wilson [ASVW21]) but the discriminant ordering part is conditional on work in progress of Shankar and Varma on Malle's conjecture for D_4 octics. Macedo–Newton [MN22] have given criteria for the failure of weak approximation and the Hasse norm principle in fields with normal closure S_n and A_n. Combining this with the counting techniques of Bhargava [Bha05, Bha10], Newton and Varma (in forthcoming work) study the frequency of Hasse norm principle failures in non-quartic S_4 fields and non-quintic S_5 fields. (Note that the Hasse norm principle is guaranteed in S_n extensions of degree n (see Voskresenskiĭ [Vos89]), and in D_n extensions of degree n by Bartels [Bar81].) There has also been recent work by Monnet [Mon22] on the related problem of counting how often certain prescribed elements of a number field k are norms as one varies over S_4 quartic extensions of k.

1.3 Equidistribution of Frobenius

As mentioned above, the key step in our proof is a reduction to the case of multicyclic extensions. It will be important that we can count multicyclic extensions which have the necessary local properties to ensure that weak approximation is satisfied for the full extension. This is the crux of Theorem 5.2, the main technical input into the proof, which should be viewed as a *quantitative Frobenius equidistribution* result. Essentially it states that one can uniformly count multicyclic extensions of a number field F while imposing that the Frobenius element of primes ramifying in the multicyclic extension or the number field F lands in (essentially) any given subset of the Galois group. This equidistribution is reflected nicely in the leading constants for these problems.

The total number of ℓ-multicyclic fields (for $\ell \neq 2$) of bounded discriminant has the following leading constant in its asymptotic formula:

$$\frac{(1 + (\ell^n - 1)/\ell^2)(\ell^n - \ell^{n-1})^{-((\ell^n - 1)/(\ell - 1)) + 1}}{\Gamma((\ell^n - 1)/(\ell - 1)) \prod_{i=0}^{n-1} (\ell^n - \ell^i)} \prod_{p \equiv 1 \bmod \ell} \left(1 + \frac{\ell^n - 1}{p}\right) \prod_p \left(1 - \frac{1}{p}\right)^{(\ell^n - 1)/(\ell - 1)}.$$

This fact is proven in Theorem 9.1. When counting such extensions for which weak approximation holds on the norm one torus the leading constant (cf. § 9.1) is

$$\frac{(1 + (\ell^n - 1)/\ell^2)(\ell^n - \ell^{n-1})^{-((\ell^n - 1)/(\ell^{n-1}(\ell - 1))) + 1}}{\Gamma((\ell^n - 1)/(\ell^{n-1}(\ell - 1))) \prod_{i=0}^{n-1} (\ell^n - \ell^i)}$$

$$\times \prod_{p \equiv 1 \bmod \ell} \left(1 + \frac{\ell^n - 1}{\ell^{n-1}p}\right) \prod_p \left(1 - \frac{1}{p}\right)^{(\ell^n - 1)/(\ell^{n-1}(\ell - 1))}.$$

One notes that the constants are remarkably similar and that one major change is to the terms within the Euler product. The factors in the Euler product corresponding to the weak approximation count feature an extra $1/\ell^{n-1}$ which reflects the fact that at each prime p, if Frobenius elements were distributed uniformly at random among all elements of the Galois group (quotiented by inertia), the probability that the Frobenius element is trivial is $1/\ell^{n-1}$. More generally, Theorem 5.2 features a product of factors corresponding to the probability that Frobenius lands in the specified subgroups at each prime. This quantitative equidistribution is key for our purposes but also likely to be highly useful in many further problems in arithmetic statistics.

1.4 Notations and conventions

– The symbol v denotes a place of $\mathbb{Q}$, and p denotes a finite place of $\mathbb{Q}$. Given a finite place p, we write v_p for the corresponding valuation.

- We say that an integer d is squarefree if $p \mid d$ implies $p^2 \nmid d$. In particular, squarefree integers may be negative.
- We say that two squarefree integers d, e are coprime if we have $\gcd(d, e) = 1$ and, furthermore, d and e are not both negative.
- We write ∞ for the infinite place of $\mathbb{Q}$. We say that ∞ divides d, written $\infty \mid d$, if $d < 0$. Then we have that two squarefree integers d, e are coprime if and only if there does not exist a place v of $\mathbb{Q}$ such that $v \mid d$ and $v \mid e$.
- A Galois extension $K/\mathbb{Q}$ is called multicyclic if $\mathrm{Gal}(K/\mathbb{Q}) \cong (\mathbb{Z}/\ell\mathbb{Z})^n$ for some prime ℓ.
- Elements ϕ of $\mathrm{Epi}(G_{\mathbb{Q}}, A)$ will often be referred to as A-extensions. This is the same data as a Galois extension $K/\mathbb{Q}$ together with an isomorphism between $\mathrm{Gal}(K/\mathbb{Q})$ and A. If a property depends only on the field K, then we shall frequently abuse notation by also referring to $K/\mathbb{Q}$ as an A-extension by forgetting the choice of isomorphism.

2. Parametrisation of abelian extensions

The following parametrisation is based on the methods of Koymans and Pagano [KP23]. Fix an algebraic closure $\overline{\mathbb{Q}}$ of $\mathbb{Q}$ and fix a finite abelian group A, which we view as a topological group by using the discrete topology. Our goal is to describe the set

$$\{K : \mathrm{Gal}(K/\mathbb{Q}) \cong A, D_K \leq X\},$$

where all our number fields K are implicitly taken inside $\overline{\mathbb{Q}}$. There is a natural surjective map ψ

$$\mathrm{Epi}(G_{\mathbb{Q}}, A) \to \{K : \mathrm{Gal}(K/\mathbb{Q}) \cong A\}$$

from the set of continuous epimorphisms $G_{\mathbb{Q}} \to A$ to $\{K : \mathrm{Gal}(K/\mathbb{Q}) \cong A\}$. The map ψ sends a continuous epimorphism ϕ to the fixed field of $\ker(\phi)$. If we define the discriminant of $\phi : G_{\mathbb{Q}} \to A$ to be the discriminant of the fixed field, then this map trivially preserves the discriminant. Furthermore, a field K with $\mathrm{Gal}(K/\mathbb{Q}) \cong A$ has precisely $|\mathrm{Aut}(A)|$ preimages under ψ. Hence, we will now shift our attention to $\mathrm{Epi}(G_{\mathbb{Q}}, A)$.

It turns out to be slightly easier to work with $\mathrm{Hom}(G_{\mathbb{Q}}, A)$, and we will later deduce results for $\mathrm{Epi}(G_{\mathbb{Q}}, A)$ from this. We will now create a bijection between $\mathrm{Hom}(G_{\mathbb{Q}}, A)$ and certain tuples of integers. Let us first define the space $\mathcal{A}$.

DEFINITION 2.1. Let A be a finite abelian group. Let $\mathcal{A}$ be the set of tuples $(v_a)_{a \in A - \{0\}}$ satisfying the following conditions:

- v_a is a squarefree integer for every $a \in A - \{0\}$;
- v_a and v_b are coprime for all $a, b \in A - \{0\}$ with $a \neq b$;
- we have

$$p \equiv 1 \bmod \frac{\mathrm{ord}(a)}{p^{v_p(\mathrm{ord}(a))}}$$

for all prime divisors p of v_a;
- if $\mathrm{ord}(a) > 2$, then $v_a > 0$.

To create the bijection, we make some arbitrary choices. Let

$$K_p := \begin{cases} \mathbb{Q}(\zeta_{p^\infty}), & \text{if } p > 2, \\ \mathbb{Q}(\zeta_{2^\infty})^+, & \text{if } p = 2, \end{cases}$$

where $\mathbb{Q}(\zeta_{2^\infty})^+$ denotes the maximal real subfield of $\mathbb{Q}(\zeta_{2^\infty})$. We have an isomorphism

$$\mathrm{Gal}(K_p/\mathbb{Q}) \cong \mathbb{Z}_p \oplus \mathbb{Z}/(p-1)\mathbb{Z}.$$

1308

Since $\mathrm{Gal}(K_p/\mathbb{Q})$ is procyclic, we may choose a topological generator τ_p of $\mathrm{Gal}(K_p/\mathbb{Q})$. Let τ_∞ be a generator of $\mathrm{Gal}(\mathbb{Q}(\sqrt{-1})/\mathbb{Q})$. Then the maximal abelian extension $\mathbb{Q}^{\mathrm{ab}}$ of $\mathbb{Q}$ is the compositum of K_p and $\mathbb{Q}(\sqrt{-1})$ over all primes p. Furthermore, these fields are linearly disjoint, which gives an isomorphism

$$\mathrm{Gal}(\mathbb{Q}^{\mathrm{ab}}/\mathbb{Q}) \cong \mathrm{Gal}(\mathbb{Q}(\sqrt{-1})/\mathbb{Q}) \times \prod_p \mathrm{Gal}(K_p/\mathbb{Q}).$$

Define σ_p and σ_∞ to be the unique elements in $\mathrm{Gal}(\mathbb{Q}^{\mathrm{ab}}/\mathbb{Q})$ that project to respectively τ_p, τ_∞ and zero everywhere else. Then the σ_p and σ_∞ together form a minimal set of topological generators of $\mathrm{Gal}(\mathbb{Q}^{\mathrm{ab}}/\mathbb{Q})$.

Let p be a prime, let $n \geq 0$ and let ℓ be a prime congruent to $1 \bmod p^n$. Let

$$\psi_{\ell,p,n} \in \mathrm{Hom}(G_\mathbb{Q}, \mathbb{Z}/p^n\mathbb{Z})$$

be the unique homomorphism that is unramified away from ℓ and satisfies $\psi_{\ell,p,n}(\sigma_\ell) = 1$. Note that it makes sense to evaluate $\psi_{\ell,p,n}$ in σ_ℓ, since any homomorphism $\psi_{\ell,p,n} : G_\mathbb{Q} \to \mathbb{Z}/p^n\mathbb{Z}$ must factor through $\mathrm{Gal}(\mathbb{Q}^{\mathrm{ab}}/\mathbb{Q})$. Similarly, let

$$\psi_{p,p,n} \in \mathrm{Hom}(G_\mathbb{Q}, \mathbb{Z}/p^n\mathbb{Z})$$

be the unique homomorphism that is unramified away from p and sends σ_p to 1. Finally, let

$$\psi_{\infty,2,1} \in \mathrm{Hom}(G_\mathbb{Q}, \mathbb{Z}/2\mathbb{Z})$$

be the unique surjective homomorphism that factors through $\mathrm{Gal}(\mathbb{Q}(\sqrt{-1})/\mathbb{Q})$.

If x is a squarefree integer such that all its prime divisors are $1, p \bmod p^n$ and such that $x > 0$ if $(p, n) \neq (2, 1)$, we define

$$\psi_{x,p,n} = \sum_{\ell \mid x} \psi_{\ell,p,n} \in \mathrm{Hom}(G_\mathbb{Q}, \mathbb{Z}/p^n\mathbb{Z}).$$

If $\ell \neq p$ is not congruent to $1 \bmod p^n$, we let $m \geq 0$ be the largest integer such that ℓ is congruent to $1 \bmod p^m$. Then we define $\psi_{\ell,p,n}$ to be any lift of $\psi_{\ell,p,m}$, which means that $q_{n,m} \circ \psi_{\ell,p,n} = \psi_{\ell,p,m}$, where $q_{n,m}$ is the unique map $\mathbb{Z}/p^n\mathbb{Z} \to \mathbb{Z}/p^m\mathbb{Z}$ sending 1 to 1. We let $\psi_{\infty,2,n}$ be any lift of $\psi_{\infty,2,1}$, while $\psi_{\infty,p,n}$ is defined to be any lift of the zero map for $p \neq 2$. We may then still define $\psi_{x,p,n}$ as above.

Using these choices, we will construct a map $\mathrm{Par} : \mathcal{A} \to \mathrm{Hom}(G_\mathbb{Q}, A)$. Take $(v_a)_{a \in A - \{0\}} \in \mathcal{A}$. Choose a cyclic quotient $\mathbb{Z}/p^n\mathbb{Z}$ of A. Write $\pi : A \to \mathbb{Z}/p^n\mathbb{Z}$ for the quotient map and π^* for the induced map $\mathrm{Hom}(G_\mathbb{Q}, A) \to \mathrm{Hom}(G_\mathbb{Q}, \mathbb{Z}/p^n\mathbb{Z})$. Then we demand that

$$\pi^*(\mathrm{Par}((v_a)_{a \in A - \{0\}})) = \sum_{a \in A - \{0\}} \pi(a) \cdot \psi_{v_a,p,n} \tag{2.1}$$

for all π. We emphasise that each $\pi(a) \cdot \psi_{v_a,p,n}$ is a homomorphism despite the fact that $\psi_{v_a,p,n}$ need not be.

We claim that (2.1) uniquely specifies the homomorphism $\mathrm{Par}((v_a)_{a \in A - \{0\}})$. By the fundamental theorem of abelian groups, we may decompose A as

$$A = \bigoplus_{i=1}^{k} \mathbb{Z}/p_i^{e_i}\mathbb{Z}.$$

Writing π_i for the natural projection map $A \to \mathbb{Z}/p_i^{e_i}\mathbb{Z}$, we see that each homomorphism $\pi_i \circ \mathrm{Par}((v_a)_{a \in A - \{0\}})$ is determined by (2.1). Therefore, (2.1) specifies at most one homomorphism $\mathrm{Par}((v_a)_{a \in A - \{0\}})$.

To prove existence, we observe that there certainly exists a homomorphism $\mathrm{Par}((v_a)_{a \in A-\{0\}})$ satisfying (2.1) for $\pi \in \{\pi_1, \ldots, \pi_k\}$. Viewing each π_i as taking values in $\mathbb{Q}/\mathbb{Z}$ by fixing an inclusion $\mathbb{Z}/p_i^{e_i}\mathbb{Z} \to \mathbb{Q}/\mathbb{Z}$, we see that each map $\pi : A \to \mathbb{Z}/p^n\mathbb{Z} \to \mathbb{Q}/\mathbb{Z}$ is a $\mathbb{Z}$-linear combination of the π_i, since the maps π_i generate the dual space $\mathrm{Hom}(A, \mathbb{Q}/\mathbb{Z})$. Therefore, (2.1) holds for all π by linearity.

We conclude that Par is well-defined. Furthermore, we have the key property

$$\left(\sum_{a \in A-\{0\}} \pi(a) \cdot \psi_{v_a, p, n} \right)(\sigma_\ell) = \begin{cases} \pi(a), & \text{if } a \in A - \{0\} \text{ satisfies } \ell \mid v_a, \\ 0, & \text{otherwise.} \end{cases} \tag{2.2}$$

THEOREM 2.2. *The map* Par *is a bijection.*

Proof. We will construct an explicit inverse Ev of Par. Take some $\phi \in \mathrm{Hom}(G_\mathbb{Q}, A)$. Then $\mathrm{Ev}(\phi)$ is the unique tuple $(v_a)_{a \in A-\{0\}}$ of squarefree integers satisfying the property

$$p \mid v_a \Longleftrightarrow \phi(\sigma_p) = a$$

for all $a \in A - \{0\}$ and for all places p of $\mathbb{Q}$ (including the infinite place ∞). Using (2.2), one directly checks that

$$\mathrm{Par}(\mathrm{Ev}(\phi))(\sigma) = \phi(\sigma)$$

for σ equal to σ_p or σ_∞. This implies that

$$\mathrm{Par}(\mathrm{Ev}(\phi)) = \phi,$$

since the σ_p and σ_∞ together form a set of topological generators of $\mathrm{Gal}(\mathbb{Q}^{\mathrm{ab}}/\mathbb{Q})$. A routine verification shows that $\mathrm{Ev} \circ \mathrm{Par} = \mathrm{id}$, which completes the proof of the theorem. $\square$

The map Par has two convenient properties. First of all, the space $\mathcal{A}$ is analytically easy to describe. Second, we have good control of the discriminant, which we make precise in our next theorem.

THEOREM 2.3. *Let* $\mathbf{v} = (v_a)_{a \in A-\{0\}} \in \mathcal{A}$ *be such that* $\mathrm{Par}(\mathbf{v}) \in \mathrm{Epi}(G_\mathbb{Q}, A)$. *Then we have*

$$v_p(\mathrm{Disc}(\mathrm{Par}(\mathbf{v}))) = v_p \left(\prod_{a \in A-\{0\}} v_a^{|A| \cdot (1 - 1/\mathrm{ord}(a))} \right) \tag{2.3}$$

for all primes p *coprime to* $2 \cdot |A|$.

Proof. Let $\mathbf{v} = (v_a)_{a \in A-\{0\}} \in \mathcal{A}$ and let p be a prime coprime to $2 \cdot |A|$. Write $\phi = \mathrm{Par}(\mathbf{v})$ and write L for the extension corresponding to ϕ. Recall that the inertia subgroup I_p of $\mathrm{Gal}(\mathbb{Q}^{\mathrm{ab}}/\mathbb{Q})$ is topologically generated by σ_p (here we use that $p \neq 2$). Also recall that I_p surjects on the inertia subgroup I_p' of $\mathrm{Gal}(L/\mathbb{Q})$.

Suppose that $\phi(\sigma_p) = a$. We compute that

$$v_p \left(\prod_{a \in A-\{0\}} v_a^{|A| \cdot (1 - 1/\mathrm{ord}(a))} \right) = |A| \cdot \left(1 - \frac{1}{\mathrm{ord}(a)} \right),$$

since $v_p(v_a) = 1$ and the entries of $\mathbf{v}$ are coprime. In order to compute the discriminant, write K for the field corresponding to $\pi \circ \phi$, where $\pi : A \to A/\langle a \rangle$ is the natural quotient map. Then p is unramified in the extension $K/\mathbb{Q}$, and all places of K above p are totally, tamely ramified in the

1310

cyclic extension L/K of degree $\operatorname{ord}(a)$. Therefore, we have

$$v_p(\operatorname{Disc}(\operatorname{Par}(\mathbf{v}))) = |A| \cdot \left(1 - \frac{1}{\operatorname{ord}(a)}\right)$$

as desired. $\qquad\square$

It is most convenient to have a version of the above theorem that also deals with the wild places.

THEOREM 2.4. *Let* $\mathbf{v} = (v_a)_{a \in A - \{0\}} \in \mathcal{A}$ *be such that* $\operatorname{Par}(\mathbf{v}) \in \operatorname{Epi}(G_{\mathbb{Q}}, A)$. *Then, for* $p > 2$, $v_p(\operatorname{Disc}(\operatorname{Par}(\mathbf{v})))$ *depends only on the order of* $\operatorname{Par}(\mathbf{v})(\sigma_p)$.

Proof. This is completely a local question. Let B be a finite abelian group and, furthermore, let $\phi \in \operatorname{Epi}(\operatorname{Gal}(\mathbb{Q}_p^{\mathrm{ab}}/\mathbb{Q}_p), B)$. Then we have to show that the discriminant depends only on the order of $\phi(\sigma_p)$.

Write $K/\mathbb{Q}_p$ for the abelian extension corresponding to $\ker(\phi)$ by Galois theory. Denote by $I_{K/\mathbb{Q}_p}$ the inertia subgroup of $K/\mathbb{Q}_p$, which is equal to $\phi(I_p)$. We have an exact sequence

$$0 \to I_{K/\mathbb{Q}_p} \to \operatorname{Gal}(K/\mathbb{Q}_p) \to \frac{\operatorname{Gal}(K/\mathbb{Q}_p)}{I_{K/\mathbb{Q}_p}} \to 0.$$

After replacing K by the compositum KL' for $L'/\mathbb{Q}_p$ an unramified extension of degree equal to $|\operatorname{Gal}(K/\mathbb{Q}_p)|$, we observe that the above exact sequence is split. We may now filter KL' as $KL'/M/\mathbb{Q}_p$, where M is the unique subfield of $\mathbb{Q}_p(\zeta_{p^\infty})$ of degree $|I_{K/\mathbb{Q}_p}|$ followed by an unramified extension. One may therefore directly compute the discriminant of $M/\mathbb{Q}_p$. Then the theorem follows by several applications of the tower formula for the discriminant. $\qquad\square$

3. Criterion for weak approximation

We recall the following results from [FLN18]. Let A be a finite abelian group, and write $A^\vee := \operatorname{Hom}(A, \mathbb{Q}/\mathbb{Z})$ for the dual group. Recall that an A-extension is a surjective, continuous homomorphism from $G_{\mathbb{Q}}$ to A. We fix embeddings $G_{\mathbb{Q}_v} \to G_{\mathbb{Q}}$ for each place v of $\mathbb{Q}$.

THEOREM 3.1 [FLN18, Theorem 6.2]. *Let* $K/\mathbb{Q}$ *be an* A-extension. *Then weak approximation holds if and only if the natural surjective map*

$$H^3(A, \mathbb{Z})^\vee \to \operatorname{III}(R_{K/\mathbb{Q}}^1, \mathbb{G}_m)$$

is an isomorphism.

THEOREM 3.2 [FLN18, Theorem 6.1]. *We have*

$$\operatorname{III}(R_{K/\mathbb{Q}}^1, \mathbb{G}_m)^\vee = \ker\left(H^3(A, \mathbb{Z}) \to \prod_v H^3(\operatorname{im}(G_{\mathbb{Q}_v}), \mathbb{Z})\right).$$

Combining these two theorems, we see that weak approximation holds if and only if

$$H^3(A, \mathbb{Z}) = \ker\left(H^3(A, \mathbb{Z}) \to \prod_v H^3(\operatorname{im}(G_{\mathbb{Q}_v}), \mathbb{Z})\right).$$

Following [FLN18, Lemma 6.4], we see that the universal coefficient theorem gives canonical isomorphisms

$$H^3(B, \mathbb{Z}) \cong \operatorname{Ext}(H_2(B, \mathbb{Z}), \mathbb{Z}) \cong \operatorname{Hom}(\wedge^2(B), \mathbb{Q}/\mathbb{Z})$$

1311

for B any finite abelian group. Then we get the following diagram.

$$
\begin{array}{ccc}
H^3(A, \mathbb{Z}) & \xrightarrow{\ \text{res}\ } & H^3(\text{im}(G_{\mathbb{Q}_v}), \mathbb{Z}) \\
\downarrow & & \downarrow \\
\text{Hom}(\wedge^2(A), \mathbb{Q}/\mathbb{Z}) & \xrightarrow{\ \varphi\ } & \text{Hom}(\wedge^2(\text{im}(G_{\mathbb{Q}_v})), \mathbb{Q}/\mathbb{Z})
\end{array}
$$

The bottom map φ in the above diagram is simply as follows. Consider the map $\text{im}(G_{\mathbb{Q}_v}) \to A$. By functoriality of $\wedge^2$, we get a map $\wedge^2(\text{im}(G_{\mathbb{Q}_v})) \to \wedge^2(A)$, which gives φ after dualising. We summarise our discussion as follows.

THEOREM 3.3. *Weak approximation holds if and only if the natural restriction map*

$$
\text{Hom}(\wedge^2(A), \mathbb{Q}/\mathbb{Z}) \to \text{Hom}(\wedge^2(\text{im}(G_{\mathbb{Q}_v}), \mathbb{Q}/\mathbb{Z})
$$

is the zero map for each place v.

We decompose A as

$$
A = \bigoplus_{i=1}^{r} \bigoplus_{j=1}^{n_i} \mathbb{Z}/p_i^{e_j}\mathbb{Z},
$$

where $p_1 < \cdots < p_r$ are prime numbers, and $e_1, \ldots, e_{n_i}$ are non-negative exponents with $e_1 \leq \cdots \leq e_{n_i}$.

THEOREM 3.4. *There exists a subspace $\mathcal{S}$ of $A[p_1]$ with the following property. Suppose that $a \in A[p_1] - \{0\}$. Then for $b \in A$, we have that*

$$
\text{Hom}(\wedge^2(A), \mathbb{Q}/\mathbb{Z}) \to \text{Hom}(\wedge^2(\langle a, b \rangle), \mathbb{Q}/\mathbb{Z})
$$

is the zero map if and only if the following assertions hold.

– *If $a \in \mathcal{S}$, then b must be in a certain subset of $A/A[p_1]$ depending only on a.*
– *If $a \notin \mathcal{S}$, then $b \in p_1 A + \langle a \rangle$.*

Proof. We take $\mathcal{S} = A[p_1] \cap p_1 A$. Let us first suppose that $a \in \mathcal{S}$. Also recall that we have a canonical isomorphism

$$
\text{Hom}(\wedge^2(A), \mathbb{Q}/\mathbb{Z}) \cong \{\text{alternating } \mathbb{Z}\text{-multilinear maps } A \times A \to \mathbb{Q}/\mathbb{Z}\}
$$

by the universal property of $\wedge^2$. Let $\varphi : A \times A \to \mathbb{Q}/\mathbb{Z}$ be alternating and let $t \in A[p_1]$. We claim that

$$
\varphi(a, t) = 0.
$$

Once the claim is proven, we immediately see that $\text{Hom}(\wedge^2(A), \mathbb{Q}/\mathbb{Z}) \to \text{Hom}(\wedge^2(\langle a, b \rangle), \mathbb{Q}/\mathbb{Z})$ is the zero map if and only if $\text{Hom}(\wedge^2(A), \mathbb{Q}/\mathbb{Z}) \to \text{Hom}(\wedge^2(\langle a, b + t \rangle), \mathbb{Q}/\mathbb{Z})$ is the zero map. Therefore, the first part of the theorem follows from the claim.

Let us now prove the claim. Since $a \in p_1 A$, we may take $b \in A$ such that $p_1 b = a$. We then have the equalities

$$
\varphi(a, t) = p_1 \varphi(b, t) = \varphi(b, p_1 t) = \varphi(b, 0) = 0
$$

as claimed.

It remains to prove the second part of the theorem. To this end, let $a \notin \mathcal{S}$. One readily verifies that the map $\text{Hom}(\wedge^2(A), \mathbb{Q}/\mathbb{Z}) \to \text{Hom}(\wedge^2(\langle a, b \rangle), \mathbb{Q}/\mathbb{Z})$ is identically zero for

$b \in p_1 A + \langle a \rangle$. Now suppose that $b \notin p_1 A + \langle a \rangle$. We must show that the map $\mathrm{Hom}(\wedge^2(A), \mathbb{Q}/\mathbb{Z}) \to \mathrm{Hom}(\wedge^2(\langle a, b \rangle), \mathbb{Q}/\mathbb{Z})$ is not identically zero. Write $\Gamma := \langle a, b \rangle$. We claim that the injection

$$0 \to \Gamma[p_1^\infty] \to A[p_1^\infty]$$

is split. This is equivalent to the claim that

$$p_1^k A[p_1^\infty] \cap \Gamma[p_1^\infty] = p_1^k \Gamma[p_1^\infty]$$

for all $k > 0$. Observe that the inclusion $\supseteq$ is always true.

Let $c \in p_1^k A[p_1^\infty] \cap \Gamma[p_1^\infty]$ and take d such that $p_1^k d = c$. Then we have

$$p_1^k d = n \cdot a + m \cdot b$$

for some integers $n, m \in \mathbb{Z}$. In particular, we deduce that $m \cdot b \in p_1 A + \langle a \rangle$. Since $A/(p_1 A + \langle a \rangle)$ has exponent p_1 and since $b \notin p_1 A + \langle a \rangle$ by assumption, it follows that m must be divisible by p_1. Therefore, we conclude that $n \cdot a$ is a multiple of p_1 in A. Because $a \notin \mathcal{S}$, this forces that p_1 divides n and thus $n \cdot a = 0$. We conclude that $c = p_1^k d = m \cdot b$. Because $b \notin p_1 A$, we deduce that $p_1^k \mid m$ and then $c \in p_1^k \Gamma[p_1^\infty]$ as desired.

We next claim that $\Gamma \otimes_{\mathbb{Z}} \mathbb{F}_{p_1}$ has dimension two. Once the claim is proven, we deduce that $\wedge^2(\Gamma[p_1^\infty]) \cong \mathbb{F}_{p_1}$. Using that the injection $0 \to \Gamma[p_1^\infty] \to A[p_1^\infty]$ is split, one readily verifies that the map

$$\mathrm{Hom}(\wedge^2(A), \mathbb{Q}/\mathbb{Z}) \to \mathrm{Hom}(\wedge^2(\Gamma), \mathbb{Q}/\mathbb{Z})$$

is not identically zero. Therefore, it is enough to establish the claim.

To prove the claim, we remark that the order of b is divisible by p_1. Indeed, if not, we would have $b \in p_1 A$ contrary to our assumptions. We have an exact sequence

$$0 \to \langle a \rangle \cap \langle b \rangle \xrightarrow{\Delta} \langle a \rangle \oplus \langle b \rangle \xrightarrow{\Sigma} \langle a, b \rangle \to 0,$$

where Δ is the map $x \to (x, -x)$ and Σ is the sum map $(x, y) \mapsto x + y$. Therefore, it suffices to show that $\langle a \rangle \cap \langle b \rangle = \{0\}$. If not, then there must be some $k \in \mathbb{Z}$ such that $k \cdot b = a$. Since $a \notin \mathcal{S}$, it follows that k is not divisible by p_1. But then we deduce that $b \in p_1 A + \langle a \rangle$, contrary to our assumptions. This gives the claim upon tensoring the above sequence by $\mathbb{F}_{p_1}$. $\qquad\square$

4. Analytic tools

4.1 Sums of multiplicative functions

After the various reduction steps in the later sections, the count in which we are interested will be expressed as a character sum. For $\ell > 2$, the main term will occur when the combinations of characters are principal. In such cases, we will repeatedly call upon the following general theorem of Koukoulopoulos [Kou19, Theorem 13.2] based on the earlier work of Granville and Koukoulopoulos [GK19].

THEOREM 4.1 [GK19, Theorem 1]. *Let $Q \geq 2$ be a parameter and let f be a multiplicative function such that there exists $\alpha \in \mathbb{C}$ with*

$$\sum_{p \leq x} f(p) \log p = \alpha x + O_A\left(\frac{x}{(\log x)^A}\right) \quad (x \geq Q) \tag{4.1}$$

for all $A > 0$. Moreover, suppose, for all n, that $|f(n)| \leq \tau_k(n)$ for some positive real number k. Fix $\epsilon > 0$ and $J \in \mathbb{Z}_{\geq 1}$. Then we have

$$\sum_{n \leq x} f(n) = x \sum_{j=0}^{J-1} c_j \frac{(\log x)^{\alpha-j-1}}{\Gamma(\alpha-j)} + O\left(\frac{x(\log Q)^{2k+J-1}}{(\log x)^{J+1-\mathrm{Re}(\alpha)}}\right)$$

for $x \geq e^{(\log Q)^{1+\epsilon}}$ and some explicit constants c_j. The implied constant depends at most on k, J, ϵ and the implied constant in (4.1) for A large enough in terms of k, J and ϵ only. Furthermore, we have

$$c_0 = \prod_p \left(1 + \frac{f(p)}{p} + \frac{f(p^2)}{p^2} + \cdots\right)\left(1 - \frac{1}{p}\right)^\alpha$$

and $c_j \ll_{j,k} (\log Q)^{j+2k}$.

4.2 An abstract large sieve

To handle some of the combinations of characters with large modulus which are non-principal, we will use a number field large sieve. Let K be a number field and let ℓ be a prime number. If $\mathfrak{f}$ is an ideal, we write $S_\mathfrak{f}$ for the subset of $\alpha \in O_K$ coprime with $\mathfrak{f}$. We also write $N(w)$ for the absolute norm of an element. Let $M \geq 1$ be an integer. Suppose that we are given a map

$$\gamma : S_{MO_K} \times S_{MO_K} \to \{0\} \cup \{\zeta_\ell^i : i = 0, \ldots, \ell-1\}$$

and a subset A_{bad} of $\mathbb{Z}_{\geq 0}$ satisfying the following properties.

(P1) *Multiplicativity:* we have

$$\gamma(w, z_1 z_2) = \gamma(w, z_1)\gamma(w, z_2) \quad \text{for all } w, z_1 \text{ and } z_2$$

and

$$\gamma(w_1 w_2, z) = \gamma(w_1, z)\gamma(w_2, z) \quad \text{for all } w_1, w_2 \text{ and } z.$$

(P2) *Periodicity:* if $z_1, z_2, w \in S_{MO_K}$ satisfy $z_1 \equiv z_2 \bmod N(w)$ and $z_1 \equiv z_2 \bmod M$, then we have $\gamma(w, z_1) = \gamma(w, z_2)$. Furthermore, if $N(w) \notin A_{\mathrm{bad}}$, then we have

$$\sum_{\substack{\xi \bmod MN(w) \\ \gcd(\xi, M)=(1)}} \gamma(w, \xi) = 0.$$

(P3) *Bad count:* we have

$$\sum_{\substack{n \in A_{\mathrm{bad}} \\ n \leq X}} 1 \leq C_1 X^{1-C_2}$$

for some absolute constants $C_1 > 0$ and $0 < C_2 < 1$.

Decompose

$$O_K^* = T \oplus V,$$

where T is torsion and V is free. Such a decomposition is not unique, but we will fix one such decomposition. Fix a fundamental domain $\mathcal{D} \subseteq O_K$ as in [KM19, §3.3] for the action of V on O_K. We will recite the properties of the fundamental domain that we need.

LEMMA 4.2. *The fundamental domain $\mathcal{D} \subseteq O_K$ has the following properties.*

– *For all $\alpha \in O_K$, there exists a unique $v \in V$ such that $v\alpha \in \mathcal{D}$. Furthermore, we have*

$$\{u \in O_K^* : u\alpha \in \mathcal{D}\} = \{\mu v : \mu \in T\}.$$

1314

– Fix an integral basis $\eta = \{\eta_1, \ldots, \eta_n\}$ of O_K. Then there exists a constant $C_\eta > 0$ such that $\alpha = a_1 \eta_1 + \cdots + a_n \eta_n \in \mathcal{D}$ $(a_i \in \mathbb{Z})$ implies that $|a_i| \leq C_\eta \cdot N(\alpha)^{1/n}$.

Proof. This is [KM19, Lemma 3.5]. □

We will consider bilinear sums of the type

$$B(X, Y, \delta, \epsilon, t_1, t_2) = \sum_{\substack{w \in t_1 \mathcal{D}(X) \\ w \equiv \delta \bmod M}} \sum_{\substack{z \in t_2 \mathcal{D}(Y) \\ z \equiv \epsilon \bmod M}} \alpha_w \beta_z \gamma(w, z),$$

where $(\alpha_w)_w$ and $(\beta_z)_z$ are sequences of complex numbers bounded in absolute value by 1, δ and ϵ are invertible congruence classes modulo M, t_1 and t_2 are fixed elements of T (so $t_i \mathcal{D}$ is a translate of the fundamental domain) and $X, Y \geq 2$ are real numbers. Here we use the notation $(t_i \mathcal{D})(X)$ for the subset of $\alpha \in t_i \mathcal{D}$ with $N(\alpha) \leq X$.

PROPOSITION 4.3. *Assume that $X \leq Y$. Then we have*

$$|B(X, Y, \delta, \epsilon, t_1, t_2)| \ll \left(X^{(-C_2)/3n} + Y^{(-1)/6n} \right) XY (\log XY)^{C_K},$$

where $n = [K : \mathbb{Q}]$ and C_K is a constant depending only on K. The implied constant depends only on K, M and the constants C_1, C_2.

Since $0 < C_2 < 1$, we achieve a power saving in both X and Y. Careful scrutiny of the proof shows that the constant C_K may be taken to depend at most on n. However, the same cannot be said of the implicit constant, which will likely depend on the regulator of K with the current argument. This will not be a cause for concern; however, as in our application this field will be a fixed cyclotomic field of the form $\mathbb{Q}(\zeta_\ell)$.

Remark. This result should be compared with Heath-Brown's sieve for quadratic characters, see [Hea95, Corollary 4] or its number field analogues (e.g., [GL13, Theorem 1.1] and [BGL14, Theorem 1.3]). There one considers bilinear sums of the Legendre symbol (z/w) (or an analogous Hecke family), which naturally satisfies properties (P1)–(P3). Heath-Brown is able to produce a greater power saving, but in his result the $(\log XY)^{C_{K,k}}$ term is replaced by $(XY)^\epsilon$. It will be crucial in our application that this term is at worst a fixed power of the logarithm.

Proof of Proposition 4.3. The argument is a minor generalisation of [KM19, Proposition 3.6]. Pick an integer $k \geq 1$ that we will optimise later. We start the proof by applying Hölder's inequality to

$$1 = \frac{k-1}{k} + \frac{1}{k},$$

which gives

$$|B(X, Y, \delta, \epsilon, t_1, t_2)|^k \leq \left(\sum_{\substack{w \in t_1 \mathcal{D}(X) \\ w \equiv \delta \bmod M}} |\alpha_w| \cdot \left| \sum_{\substack{z \in t_2 \mathcal{D}(Y) \\ z \equiv \epsilon \bmod M}} \beta_z \gamma(w, z) \right| \right)^k$$

$$\leq \left(\sum_{\substack{w \in t_1 \mathcal{D}(X) \\ w \equiv \delta \bmod M}} |\alpha_w|^{k/(k-1)} \right)^{k-1} \cdot \left(\sum_{\substack{w \in t_1 \mathcal{D}(X) \\ w \equiv \delta \bmod M}} \left| \sum_{\substack{z \in t_2 \mathcal{D}(Y) \\ z \equiv \epsilon \bmod M}} \beta_z \gamma(w, z) \right|^k \right)$$

$$\ll X^{k-1} \cdot \sum_{\substack{w \in t_1 \mathcal{D}(X) \\ w \equiv \delta \bmod M}} \left| \sum_{N(z) \leq Y^k} \beta_z' \gamma(w, z) \right|,$$

1315

where

$$\beta_z' := \sum_{\substack{z_1 \cdot \ldots \cdot z_k = z \\ z_i \in t_2 \mathcal{D}(Y) \\ z_i \equiv \epsilon \bmod M}} \beta_{z_1} \cdot \ldots \cdot \beta_{z_k}.$$

Here we used property (P1) to expand the k-fold product.

Fix an integral basis $\eta_1, \ldots, \eta_n$ of O_K, where $n = [K : \mathbb{Q}]$. We call an element z (C, Y)-well-balanced if

$$z = a_1 \eta_1 + \ldots + a_n \eta_n, \quad a_i \in \mathbb{Z}, \tag{4.2}$$

implies that $|a_i| \leq CY^{1/n}$. From the construction of the fundamental domain $\mathcal{D}(Y)$ (see the second property of Lemma 4.2), it follows that there exists a constant $C > 0$ depending only on k, K and the choice of integral basis such that $\beta_z' = 0$ if z is not (C, Y^k)-well-balanced. Fix such a choice of absolute constant C. Then we may assume from now on that we are summing over all z such that $N(z) \leq Y^k$ and z is (C, Y^k)-well-balanced. Write $\mathcal{B}(Y, C)$ for the set of $z \in O_K$ such that $|a_i| \leq CY^{1/n}$ upon expanding z as in (4.2) and such that z is coprime with M. For the remainder of this proof, all our implied constants may depend on K, M, k, C_1, C_2, our choice of C and our choice of integral basis. We rewrite

$$\sum_{\substack{w \in t_1 \mathcal{D}(X) \\ w \equiv \delta \bmod M}} \left| \sum_{\substack{N(z) \leq Y^k \\ z \in \mathcal{B}(Y^k, C)}} \beta_z' \gamma(w, z) \right| = \sum_{\substack{w \in t_1 \mathcal{D}(X) \\ w \equiv \delta \bmod M}} \epsilon(w) \sum_{\substack{N(z) \leq Y^k \\ z \in \mathcal{B}(Y^k, C)}} \beta_z' \gamma(w, z)$$

$$= \sum_{\substack{N(z) \leq Y^k \\ z \in \mathcal{B}(Y^k, C)}} \beta_z' \sum_{\substack{w \in t_1 \mathcal{D}(X) \\ w \equiv \delta \bmod M}} \epsilon(w) \gamma(w, z),$$

where $\epsilon(w)$ are complex numbers of absolute value 1. We now drop the condition $N(z) \leq Y^k$. This does not change the sum, since $\beta_z' = 0$ if $N(z) > Y^k$. Then the Cauchy–Schwarz inequality yields

$$|B(X, Y, \delta, \epsilon, t_1, t_2)|^{2k} \ll X^{2k-2} \cdot \left(\sum_{z \in \mathcal{B}(Y^k, C)} |\beta_z'|^2 \right)$$

$$\cdot \left(\sum_{z \in \mathcal{B}(Y^k, C)} \sum_{\substack{w_1 \in t_1 \mathcal{D}(X) \\ w_1 \equiv \delta \bmod M}} \sum_{\substack{w_2 \in t_1 \mathcal{D}(X) \\ w_2 \equiv \delta \bmod M}} \epsilon(w_1) \epsilon(w_2) \gamma(w_1 w_2, z) \right)$$

thanks to property (P1). We bound the former sum by

$$\sum_{z \in \mathcal{B}(Y^k, C)} |\beta_z'|^2 \ll Y^k (\log Y)^{C_{K,k}},$$

where $C_{K,k}$ is an effectively computable constant depending only on K and k. For the latter sum we invert the order of summation to get

$$\sum_{\substack{w_1 \in t_1 \mathcal{D}(X) \\ w_1 \equiv \delta \bmod M}} \sum_{\substack{w_2 \in t_1 \mathcal{D}(X) \\ w_2 \equiv \delta \bmod M}} \epsilon(w_1) \epsilon(w_2) \sum_{z \in \mathcal{B}(Y^k, C)} \gamma(w_1 w_2, z).$$

1316

We have the estimates

$$\sum_{z \in \mathcal{B}(Y^k, C)} \gamma(w_1 w_2, z) \ll \begin{cases} Y^k, & \text{if } N(w_1 w_2) \in A_{\text{bad}}, \\ \sum_{i=1}^n X^{2i} Y^{k(1-i/n)}, & \text{if } N(w_1 w_2) \notin A_{\text{bad}}. \end{cases}$$

Indeed, the first inequality is just the trivial bound. For the second inequality, we use property (P2) and split $\mathcal{B}(Y^k, C)$ into boxes of side length $MN(w_1 w_2) \leq MX^2$.

From now on we shall take $k \geq 2n$. Hence, we have $Y^{k/n} \geq X^2$, since we assumed that $Y \geq X$. Therefore, the last bound can be simplified to $X^2 Y^{k(1-1/n)}$. Thanks to property (P3), we get the bound

$$\sum_{\substack{w_1 \in t_1 \mathcal{D}(X) \\ w_1 \equiv \delta \bmod M}} \sum_{\substack{w_2 \in t_1 \mathcal{D}(X) \\ w_2 \equiv \delta \bmod M}} \mathbf{1}_{N(w_1 w_2) \in A_{\text{bad}}} \ll_{K,k,C_1} X^{2-2C_2} (\log X)^{C_{K,k}}$$

for a potentially different effectively computable constant $C_{K,k}$ depending only on K and k. This shows that

$$\sum_{\substack{w_1 \in t_1 \mathcal{D}(X) \\ w_1 \equiv \delta \bmod M}} \sum_{\substack{w_2 \in t_1 \mathcal{D}(X) \\ w_2 \equiv \delta \bmod M}} \epsilon(w_1) \epsilon(w_2) \sum_{z \in \mathcal{B}(Y^k, C)} \gamma(w_1 w_2, z)$$

$$\ll \left(X^{2-2C_2} Y^k + X^4 Y^{k(1-1/n)} \right) (\log XY)^{C_{K,k}}.$$

We conclude that

$$|B(X, Y, \delta, \epsilon, t_1, t_2)|^{2k} \ll \left(X^{2k-2C_2} Y^{2k} + X^{2k+2} Y^{2k-k/n} \right) (\log XY)^{C_{K,k}}.$$

We take $k = 3n$, which depends only on K, to finish the proof of the proposition. $\square$

5. Reduction to multicyclic extensions

The aim of this section is to reduce our main theorem to the case of multicyclic extensions. This is not quite possible, but instead we may reduce to multicyclic extensions where the decomposition group condition is replaced by a splitting condition depending on $p \bmod M$, where we think of M as being (almost) fixed. We formalise these types of conditions in our next definition. Write $\mathcal{P}(X)$ for the power set of a set X.

DEFINITION 5.1. Let $A = \mathbb{F}_\ell^n$ for some prime ℓ and integer $n > 0$. Write $\mathcal{S}$ for the set of subspaces of A of dimension at most one. Also write $\mathbb{P}$ for the set of prime numbers. Let $M \in \mathbb{Z}_{\geq 1}$ and let $B \subseteq A$ be a subspace. Let $f : \mathbb{P} \times \mathcal{S} \to \sqcup_{S \in \mathcal{S}} \mathcal{P}(A/S)$ be a function satisfying the following properties.

- We have $f(p, S) \subseteq A/S$ for all (p, S). Furthermore, if $S \cap B = \{0\}$, then $f(p, S)$ is a coset of B viewed as subgroup of A/S. If $S \cap B \neq \{0\}$, then $f(p, S) = A/S$.
- For every fixed $S \in \mathcal{S}$, the function $p \mapsto f(p, S)$ depends only on $p \bmod M$.

Let $g : \{p \in \mathbb{P} : p \mid M\} \to \{\emptyset \subset F \subseteq \mathbb{F}_\ell^n\}$. We say that the pair (f, g) is a *congruence function for M*. Moreover, let K be an A-extension of $\mathbb{Q}$ given by $\phi \in \text{Epi}(G_\mathbb{Q}, A)$. If p is a prime, we write K_p for the extension of $\mathbb{Q}$ corresponding to $G_\mathbb{Q} \xrightarrow{\phi} A \to A/\phi(I_p)$. We say that K has the correct Frobenius elements for (f, g) (abbreviated as (f, g)-correct or simply f-correct) if the following assertions hold.

1317

– We have

$$\mathrm{Frob}_{K_p/\mathbb{Q}}(p) \in f(p, \phi(I_p))$$

for all p dividing the discriminant of K such that p is coprime to $2M$.
– We have that all $p \mid M$ are unramified in K and that

$$\mathrm{Frob}_{K/\mathbb{Q}}(p) \in g(p)$$

for all p dividing M, assuming that $p \neq 2$ or $\ell \neq 2$.

Observe that $\phi(I_p)$ can have dimension greater than one only if $p = \ell = 2$.

In the coming sections we will show the following result. We set $d(\ell)$ equal to 16 if $\ell = 2$ and 1 if $\ell > 2$. Let $\Delta = \Delta_\ell$ be the unique strongly multiplicative function satisfying $\Delta(p) = p$ for $p \neq \ell$ and $\Delta(\ell) = \ell^2$.

THEOREM 5.2. *Let $C > 0$. Let $A = \mathbb{F}_\ell^n$ for some prime ℓ and integer $n > 0$ and let B be a subgroup of A. Then there exists $\delta > 0$ such that the following statement holds. Let (f, g) be a congruence function for $M \in \mathbb{Z}_{\geq 1}$. Let $(c_a)_{a \in A - \{0\}}$ be a vector of integers. Let G be a subgroup of $(\mathbb{Z}/M\mathbb{Z})^*$. Let H_a be a union of cosets of G such that $|H_a| = |H_{a'}|$ for all $a, a' \in A - B$. Assume that $M \leq (\log X)^C$ and that $[(\mathbb{Z}/M\mathbb{Z})^* : G] \leq C$. Let S be a subset of $A - \{0\}$. Further, assume that*

$$f(p, \langle a \rangle) = f(p', \langle a \rangle) \tag{5.1}$$

if $p \bmod M$ and $p' \bmod M$ are in the same coset of G. Then there is $C_{\mathrm{lead}} \geq 0$ such that for all real numbers $X \geq 100$,

$$\sum_{\substack{\mathbf{v} = (v_a)_{a \in A - \{0\}} \in \mathcal{A} \\ \prod_{a \in A - \{0\}} \Delta(|v_a|) \leq X \\ v_a \neq 1 \ \forall a \in S \\ v_a \equiv c_a \bmod d(\ell) \\ \gcd(v_a, M) = 1 \\ p | v_a \Rightarrow p \bmod M \in H_a}} \mathbf{1}_{\mathrm{Par}(\mathbf{v}) f\text{-correct}} = C_{\mathrm{lead}} X (\log X)^{\alpha - 1} + O\big(X (\log X)^{\alpha - 1 - \delta}\big),$$

where

$$\alpha = \sum_{a \in B - \{0\}} \frac{|\mathrm{Lift}(H_a)|}{\varphi(\mathrm{lcm}(M, \ell))} + \sum_{a \in A - B} \frac{|B|}{\ell^{n-1}} \cdot \frac{|\mathrm{Lift}(H_a)|}{\varphi(\mathrm{lcm}(M, \ell))}.$$

Here $\mathrm{Lift}(G)$ denotes the subset of $(\mathbb{Z}/\mathrm{lcm}(M, \ell)\mathbb{Z})^*$ consisting of elements that map to 1 in $(\mathbb{Z}/\ell\mathbb{Z})^*$ and to an element of G in $(\mathbb{Z}/M\mathbb{Z})^*$. The implied constant depends only on C and A.

Furthermore, the leading constant C_{lead} does not depend on S, and there exists a constant $C_{\max}$, depending only on ℓ and n, such that $C_{\mathrm{lead}} \leq C_{\max}$. We have $C_{\mathrm{lead}} > 0$ if $\ell > 2$ or

– $f(p, S) = B$ *for all p coprime to M and all S such that $S \cap B = \{0\}$;*
– $0 \in g(p)$ *for all $p \mid M$;*
– $c_a = 1$ *for all $a \in A - \{0\}$.*

In our application, the A in the theorem will be the ℓ-torsion subgroup of a fixed abelian group A. In light of the work of §3, we will take B to be $A[\ell] \cap \ell A$. Then, in order to study A-extensions failing to have the weak approximation condition, we must ensure that Frobenius lands in one of the acceptable classes, as specified in Theorem 3.4. This is the purpose of the notion of congruence functions and f-correctness. The conditions on primes dividing v_a allow us to control the splitting behaviour of primes which do not ramify in the extension from $\mathbb{Q}$ to a fixed field of $A/A[\ell]$ but do ramify in the remaining $A[\ell]$-extension.

Remark. This theorem is in many ways best possible. Further uniformity in M is plausible but likely out of reach given the current state of knowledge regarding zeros of L-functions. Perhaps the most interesting condition in the theorem is that the H_a all have the same cardinality for $a \in A - B$. Indeed, the theorem is no longer true if the H_a are allowed to be of arbitrary cardinality. More precisely, the true log exponent may be bigger than $\alpha - 1$.

Consider, for example, the situation that $B = \{0\}$ and $f(p, S)$ is always the zero element of A/S. Fix some $a \in A - \{0\}$. If one takes $|H_b|$ very small for $b \neq a$ and $|H_a|$ very large, then one can obtain a larger log exponent by taking $v_b = 1$ for $b \neq a$ and letting v_a vary freely. Note that this example critically depends both on the form of the congruence function and the sizes of $|H_a|$.

We will now show how to derive our main theorem from Theorem 5.2. It is important to remark that the exponents appearing in the discriminant, (2.3), are not equal. In fact, the exponent is minimised by taking a to be in $A[\ell]$, where ℓ is the smallest prime divisor of A. In the language of [Woo10], the discriminant is not a fair counting function. It is precisely for this reason that we may reduce to multicyclic extensions, which is certainly not possible for fair counting functions.

Write $\mathcal{B}$ for those tuples in $\mathcal{A}$ that give rise to an element in $\mathrm{Epi}(G_{\mathbb{Q}}, A)$ and we say that WA holds for $\mathbf{v}$ if weak approximation holds on $R^1 K/\mathbb{Q}$ for $K/\mathbb{Q}$ the extension associated to $\mathbf{v}$.

THEOREM 5.3. *Let A be a non-trivial, finite, abelian group. Write ℓ for the smallest prime divisor of A. Then there exist $C_{\mathrm{weak}} > 0$ and $\delta > 0$ such that for all $X \geq 100$,*

$$\sum_{\substack{\mathbf{v}=(v_a)_{a \in A - \{0\}} \in \mathcal{B} \\ \mathrm{Disc}(\mathrm{Par}(\mathbf{v})) \leq X}} \mathbf{1}_{\mathrm{WA \ holds}} = C_{\mathrm{weak}} X^{\ell/(|A| \cdot (\ell-1))} (\log X)^{\alpha(A)-1} + O\big(X^{\ell/(|A| \cdot (\ell-1))} \cdot (\log X)^{\alpha(A)-1-\delta}\big),$$

where

$$\alpha(A) = \sum_{a \in A[\ell] - \{0\}} \frac{|\{b \in A : \mathrm{Hom}(\wedge^2(A), \mathbb{Q}/\mathbb{Z}) \to \mathrm{Hom}(\wedge^2(\langle a, b \rangle), \mathbb{Q}/\mathbb{Z}) \text{ is zero}\}|}{(\ell-1) \cdot |A|}.$$

The implied constant depends only on A.

Proof. Fix a large number C_3. We split the sum as

$$\sum_{\substack{\mathbf{v}=(v_a)_{a \in A - \{0\}} \in \mathcal{B} \\ \mathrm{Disc}(\mathrm{Par}(\mathbf{v})) \leq X}} \mathbf{1}_{\mathrm{WA \ holds}} = \sum_{\substack{\mathbf{v}=(v_a)_{a \in A - \{0\}} \in \mathcal{B} \\ \mathrm{Disc}(\mathrm{Par}(\mathbf{v})) \leq X \\ \prod_{a \notin A[\ell]} v_a > (\log X)^{C_3}}} \mathbf{1}_{\mathrm{WA \ holds}}$$

$$+ \sum_{\substack{\mathbf{v}=(v_a)_{a \in A - \{0\}} \in \mathcal{B} \\ \mathrm{Disc}(\mathrm{Par}(\mathbf{v})) \leq X \\ \prod_{a \notin A[\ell]} v_a \leq (\log X)^{C_3}}} \mathbf{1}_{\mathrm{WA \ holds}}. \tag{5.2}$$

The main term will come from the latter sum in (5.2). We will start by bounding the former sum. It will be convenient to set

$$e_a := |A| \cdot \left(1 - \frac{1}{\mathrm{ord}(a)}\right).$$

Note that e_a is minimal for $a \in A[\ell] - \{0\}$. We bound the former sum in (5.2) by

$$\sum_{\substack{\mathbf{v}=(v_a)_{a \in A - \{0\}} \in \mathcal{B} \\ \mathrm{Disc}(\mathrm{Par}(\mathbf{v})) \leq X \\ \prod_{a \notin A[\ell]} v_a > (\log X)^{C_3}}} 1 \leq \sum_{\substack{(w_a)_{a \in A - A[\ell]} \\ w_a \in \mathbb{Z}_{\geq 1} \\ \prod_{a \notin A[\ell]} w_a > (\log X)^{C_3}}} \sum_{\substack{(v_a)_{a \in A[\ell] - \{0\}} \\ v_a \text{ squarefree coprime} \\ p|v_a \Rightarrow p \equiv 0,1 \bmod \ell \\ \prod_{a \in A[\ell] - \{0\}} v_a^{|A| \cdot (1-1/\ell)} \leq X/(\prod_{a \in A - A[\ell]} w_a^{e_a})}} 1. \tag{5.3}$$

Writing $|A[\ell]| = \ell^n$, classical analytic number theory shows that

$$\sum_{\substack{(v_a)_{a \in A[\ell]-\{0\}} \\ v_a \text{ squarefree coprime} \\ p|v_a \Rightarrow p \equiv 0,1 \bmod \ell \\ \prod_{a \in A[\ell]-\{0\}} v_a^{|A| \cdot (1-1/\ell)} \leq X/(\prod_{a \in A-A[\ell]} w_a^{e_a})}} 1 \ll_\ell \left(\frac{X}{\prod_{a \in A-A[\ell]} w_a^{e_a}} \right)^{\ell/(|A| \cdot (\ell-1))} (\log X)^{(\ell^n-1)/(\ell-1)-1}.$$

Plugging this in (5.3) yields the bound

$$X^{\ell/(|A| \cdot (\ell-1))} \cdot (\log X)^{(\ell^n-1)/(\ell-1)-1} \sum_{\substack{(w_a)_{a \in A-A[\ell]} \\ w_a \in \mathbb{Z}_{\geq 1} \\ \prod_{a \notin A[\ell]} w_a > (\log X)^{C_3}}} \frac{1}{\prod_{a \in A-A[\ell]} w_a^{(\ell \cdot e_a)/(|A| \cdot (\ell-1))}}.$$

Since e_a is minimal when $a \in A[\ell]$, we see that the sum

$$\sum_{\substack{(w_a)_{a \in A-A[\ell]} \\ w_a \in \mathbb{Z}_{\geq 1}}} \frac{1}{\prod_{a \in A-A[\ell]} w_a^{(\ell \cdot e_a)/(|A| \cdot (\ell-1))}}$$

converges, because the exponent of w_a is bigger than 1. Therefore, the tail can be bounded by

$$X^{\ell/(|A| \cdot (\ell-1))} \cdot (\log X)^{(\ell^n-1)/(\ell-1)-1} \sum_{\substack{(w_a)_{a \in A-A[\ell]} \\ w_a \in \mathbb{Z}_{\geq 1} \\ \prod_{a \notin A[\ell]} w_a > (\log X)^{C_3}}} \frac{1}{\prod_{a \in A-A[\ell]} w_a^{(\ell \cdot e_a)/(|A| \cdot (\ell-1))}}$$

$$\ll X^{\ell/(|A| \cdot (\ell-1))} \cdot (\log X)^{(\ell^n-1)/(\ell-1)-1-\delta C_3}$$

for some $\delta > 0$ depending only on A. This is negligible, provided that we pick C_3 sufficiently large in terms of A. It remains to deal with the latter sum in (5.2). $\qquad \square$

5.1 The main term: the reduction step

To prepare for our application of Theorem 5.2, we start by fixing all the variables v_a with $a \in A - A[\ell]$. The induced homomorphism $\varphi : G_\mathbb{Q} \to A \to A/A[\ell]$ depends only on the v_a with $a \in A - A[\ell]$. Define for $a \in A$ the set

$$\mathrm{Adm}(a) := \{b \in A : \mathrm{Hom}(\wedge^2(A), \mathbb{Q}/\mathbb{Z}) \to \mathrm{Hom}(\wedge^2(\langle a, b \rangle), \mathbb{Q}/\mathbb{Z}) \text{ is zero}\}.$$

Write $\widetilde{\pi} : A \to A/A[\ell]$ for the natural quotient map. We make the following assumptions.

(P1) The homomorphism φ is surjective. Write K for the fixed field of φ, which is an $A/A[\ell]$-extension of $\mathbb{Q}$.

(P2) For all $p \mid v_a$, we have $\varphi(\mathrm{Frob}_p) \in \widetilde{\pi}(\mathrm{Adm}(a))$. Here and henceforth we make a fixed choice of a prime ideal $\mathfrak{p}$ of $\overline{\mathbb{Z}}$ above p and we also make a fixed choice of an element $\mathrm{Frob}_p \in \{\sigma : \sigma(\mathfrak{p}) = \mathfrak{p}\} \subseteq \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ lifting the Frobenius automorphism of $\overline{\mathbb{Z}}/\mathfrak{p} \cong \overline{\mathbb{F}_p}$.

(P3) There exists an A-extension of $\mathbb{Q}$ containing K that satisfies weak approximation. We remark that this condition in fact implies (P1) and (P2).

If these conditions are not met, we may freely ignore the variables v_a, since they do not contribute to the counting function. There exists at least one tuple v_a satisfying (P1), (P2) and (P3) by an application of [FLN18, Proposition 5.5] with $k = \mathbb{Q}$ and $G = A$. Indeed, weak approximation certainly holds if all decomposition groups are cyclic. We will use this later on to guarantee that our leading constant C_{weak} is strictly greater than zero.

We will now work towards applying Theorem 5.2. We take $M = \mathfrak{f}(K)^2$, where $\mathfrak{f}(K)$ is the conductor of K. There exists a subgroup G of $(\mathbb{Z}/M\mathbb{Z})^*$ such that p splits completely in K if and only if $p \bmod M \in G$. Then for $a \in A[\ell] - \{0\}$ we take

$$H_a := \bigcup_{b \in \widetilde{\pi}(\mathrm{Adm}(a))} \mathrm{FrobInv}(b) \cdot G,$$

where $\mathrm{FrobInv}(b)$ is any prime p, not dividing M, with Artin symbol in K equal to b. By choosing C sufficiently large in terms of the abelian group A, we see that the condition $[(\mathbb{Z}/M\mathbb{Z})^* : G] \le C$ in Theorem 5.2 holds.

We take $B = A[\ell] \cap \ell A$. We have to check that $|H_a| = |H_{a'}|$ for all $a, a' \in A[\ell] - B$. This is equivalent to showing that

$$|\widetilde{\pi}(\mathrm{Adm}(a))| = |\widetilde{\pi}(\mathrm{Adm}(a'))| \tag{5.4}$$

for all $a, a' \in A[\ell] - B$. If $\langle a \rangle = \langle a' \rangle$, then the result is correct. So now suppose that $\langle a \rangle \ne \langle a' \rangle$. We claim that there exists an automorphism ψ of A such that $\psi(a) = a'$.

Let us first show that the claim implies (5.4). To this end, take an automorphism ψ that sends a to a'. Consider the induced map $\psi^* : \mathrm{Adm}(a) \to \mathrm{Adm}(a')$, which sends b to $\psi(b)$. To check that this is well-defined, we further claim that

$$\mathrm{Hom}(\wedge^2(A), \mathbb{Q}/\mathbb{Z}) \to \mathrm{Hom}(\wedge^2(\langle a, b \rangle), \mathbb{Q}/\mathbb{Z}) \text{ is zero}$$

if and only if

$$\mathrm{Hom}(\wedge^2(A), \mathbb{Q}/\mathbb{Z}) \to \mathrm{Hom}(\wedge^2(\langle \psi(a), \psi(b) \rangle), \mathbb{Q}/\mathbb{Z}) \text{ is zero}.$$

The former statement is equivalent to all alternating maps $\lambda : A \times A \to \mathbb{Q}/\mathbb{Z}$ satisfying $\lambda(a, b) = 0$, while the latter statement is equivalent to all alternating maps $\lambda : A \times A \to \mathbb{Q}/\mathbb{Z}$ satisfying $\lambda(\psi(a), \psi(b)) = 0$. As λ runs through all alternating maps, so does $\lambda(\psi(-), \psi(-))$ and therefore the above statements are all equivalent. This shows that ψ^* is well-defined. It is now readily verified that ψ^* is a bijection. We next observe that $\mathrm{Adm}(a)$ is a subgroup of A. Therefore, to establish (5.4), it suffices to show that $|\mathrm{Adm}(a) \cap A[\ell]| = |\mathrm{Adm}(a') \cap A[\ell]|$. But this is true because ψ is an automorphism that restricts to an isomorphism between $\mathrm{Adm}(a)$ and $\mathrm{Adm}(a')$. We conclude that the claim indeed implies (5.4).

Let us now prove the claim. If the injection

$$0 \to \langle a, a' \rangle \to A$$

is split, then it is straightforward to construct the desired bijection ψ. So now suppose that the above injection is not split. Because $a, a' \notin B$, this means that there exist $n, m \in \mathbb{Z}$ both not divisible by ℓ such that $na + ma' \in \ell A$. Using that $a \notin B$, we may decompose A as an internal direct sum $\langle a \rangle \oplus C$ for some subgroup C of A. Now consider the homomorphism ψ that is the identity on C and sends a to a'.

It remains to prove that ψ is surjective. By construction we have that $C \subseteq \mathrm{im}(\psi)$ and that $a' \in \mathrm{im}(\psi)$. Therefore, it suffices to show that $a \in \mathrm{im}(\psi)$. By the relation $na + ma' \in \ell A$ and the inclusion $\ell A \subseteq C$, we deduce that $na \in \mathrm{im}(\psi)$. Because n is coprime to ℓ, we conclude that $a \in \mathrm{im}(\psi)$. We have proven the claim and thus (5.4).

We will now construct a congruence function (f, g) for M. Suppose that $p \ne 2$ is unramified in K. Then, if p ramifies in $\mathrm{Par}(\mathbf{v})$, we have $p \mid v_a$ for some $a \in A[\ell] - \{0\}$. Take $S = \langle a \rangle \in \mathcal{S}$, which has dimension one. For weak approximation to hold, we certainly must have that $\mathrm{Frob}_{K/\mathbb{Q}}(p) \in \widetilde{\pi}(\mathrm{Adm}(a))$ (or equivalently $p \bmod M \in H_a$), which we will assume from now on. We will now distinguish two cases.

1321

Case I: $a \in B$. In this case, Theorem 3.4 yields that Frob_p automatically lands in $\mathrm{Adm}(a)$. Correspondingly, we take $f(p, S) = A/S$.

Case II: $a \notin B$. In this case Theorem 3.4 tells us that $\mathrm{Adm}(a) = \ell A + \langle a \rangle$. Define $\mathbf{x}_Q$ to be the unique tuple that equals v_a for $a \in A - A[\ell]$ and equals 1 for $a \in A[\ell] - \{0\}$. We claim that there exists an element $h(p, S) \in A[\ell]$ such that

$$\mathrm{Par}(\mathbf{x}_Q)(\mathrm{Frob}_p) + h(p, S) \in \mathrm{Adm}(a). \tag{5.5}$$

By construction of $\mathbf{x}_Q$ we have that $\widetilde{\pi} \circ \mathrm{Par}(\mathbf{x}_Q) = \varphi$. Therefore, it follows from $\mathrm{Frob}_{K/\mathbb{Q}}(p) \in \widetilde{\pi}(\mathrm{Adm}(a))$ that (5.5) is true after applying $\widetilde{\pi}$, establishing the claim. Then we take $f(p, S)$ to be the coset $h(p, S) + B$. One may now directly verify that condition (5.1) is satisfied.

5.2 The bad primes

Next consider a prime $p \neq 2$ that divides the conductor of K, which implies that $p \mid v_a$ for some $a \notin A[\ell]$. Let $g(p)$ be the subset of $a \in A[\ell]$ satisfying

$$\mathrm{Par}(\mathbf{x}_Q)(\mathrm{Frob}_p) + a \in \mathrm{Adm}(a).$$

We deduce from property (P2) of K that $g(p)$ is non-empty.

5.3 Completing the reduction step

We now rewrite

$$\sum_{\substack{\mathbf{v} = (v_a)_{a \in A - \{0\}} \in \mathcal{B} \\ \mathrm{Disc}(\mathrm{Par}(\mathbf{v})) \leq X \\ \prod_{a \notin A[\ell]} v_a \leq (\log X)^{C_3}}} \mathbf{1}_{\mathrm{WA\ holds}}$$

as

$$\sum_{\substack{(v_a)_{a \in A - A[\ell]} \\ \prod_{a \notin A[\ell]} v_a \leq (\log X)^{C_3}}} \sum_{\substack{(c_a)_{a \in A[\ell] - \{0\}} \in (\mathbb{Z}/d(\ell)\mathbb{Z})^{A[\ell] - \{0\}}}} \mathbf{1}_{(c_a)\ \mathrm{nice}} \sum_{\substack{\mathbf{w} = (w_a)_{a \in A[\ell] - \{0\}} \\ \mathbf{v} \in \mathcal{B} \\ \mathrm{Disc}(\mathrm{Par}(\mathbf{v})) \leq X \\ w_a \equiv c_a \bmod d(\ell) \\ p \mid v_a \Rightarrow p \bmod M \in H_a}} \mathbf{1}_{\mathrm{WA\ holds}},$$

where $\mathbf{v}$ is the tuple obtained by concatenating (v_a) and (w_a) and where we will soon define when (c_a) is nice.

Fix the tuple $\mathbf{v}_Q = (v_a)_{a \in A - A[\ell]}$ satisfying assumptions (P1), (P2) and (P3) and fix a tuple $(c_a)_{a \in A[\ell] - \{0\}}$. We first claim that the condition $\mathbf{1}_{\mathrm{WA\ holds}}$ may be replaced by $\mathbf{1}_{\mathrm{Par}(\mathbf{w})f\text{-correct}}$. First of all, we remark that D_p is certainly cyclic if p is unramified in $\mathrm{Par}(\mathbf{v})$. At the odd ramified places this is true by construction of f. Finally, whether the natural restriction map $\mathrm{Hom}(\wedge^2(A), \mathbb{Q}/\mathbb{Z}) \to \mathrm{Hom}(\wedge^2(\mathrm{im}(G_{\mathbb{Q}_2}), \mathbb{Q}/\mathbb{Z})$ is zero is entirely determined by $\mathbf{v}_Q = (v_a)_{a \in A - A[\ell]}$ and $(c_a)_{a \in A[\ell] - \{0\}}$. Indeed, if $\ell > 2$, then this map is always zero as 2 is necessarily unramified in A. If $\ell = 2$, then this follows from the fact that the restrictions of $\psi_{v_a, 2, 1}$ and $\psi_{v_b, 2, 1}$ to $G_{\mathbb{Q}_2}$ are equal if $v_a \equiv v_b \bmod 16$ (recall that $d(2) = 16$) combined with (2.1). Now we simply define (c_a) to be nice if the above map is zero.

Let us now explicate the condition $\mathbf{v} = (v_a)_{a \in A - \{0\}} \in \mathcal{B}$ in terms of the variables in $A[\ell] - \{0\}$. One directly checks that

$$\mathbf{v} \in \mathcal{B} \iff \langle a \in A - \{0\} : v_a \neq 1 \rangle = A$$

for all $\mathbf{v} \in \mathcal{A}$. Therefore, since φ is already assumed to be surjective by (P1), we have that there exists a subspace T, containing B and depending on $\mathbf{v}_Q = (v_a)_{a \in A - A[\ell]}$, such that

$$\mathbf{v} \in \mathcal{B} \iff T + \langle a \in A[\ell] - \{0\} : v_a \neq 1 \rangle = A[\ell]. \tag{5.6}$$

Next we compare $\text{Disc}(\text{Par}(\mathbf{v}))$ with $\text{Disc}(\text{Par}(\mathbf{w}))$. To do so, we compute the p-adic valuation of the discriminant using Theorem 2.3 for primes $p \nmid 2|A|$. Locally at 2, we have just proven that the restriction of $\text{Par}(\mathbf{v})$ is unramified if $\ell > 2$ and completely determined by c_a and $\mathbf{v}_Q = (v_a)_{a \in A - A[\ell]}$ if $\ell = 2$. For the odd places $p \mid |A|$, we compute the p-adic valuation of the discriminant using Theorem 2.4. More precisely, if $\text{Par}(\sigma_p)$ is the identity, then $v_p(\text{Disc}(\text{Par}(\mathbf{v}))) = 0$. If instead $\text{Par}(\sigma_p) \in A - A[\ell]$, then $v_p(\text{Disc}(\text{Par}(\mathbf{v})))$ is determined by $\mathbf{v}_Q$ as a consequence of Theorem 2.4. Finally, if $\text{Par}(\sigma_p) \in A[\ell] - \{0\}$, then the proof of Theorem 2.4 shows that $v_p(\text{Disc}(\text{Par}(\mathbf{v})))$ equals $|A|/\ell$ multiplied by the p-adic valuation of the discriminant of the unique degree ℓ subfield of $\mathbb{Q}_p(\zeta_{p^\infty})$. Therefore, the conductor–discriminant formula demonstrates the validity of

$$v_p(\text{Disc}(\text{Par}(\mathbf{v}))) = \begin{cases} |A| \cdot \left(1 - \dfrac{1}{\ell}\right), & \text{if } \ell \neq p, \\ 2|A| \cdot \left(1 - \dfrac{1}{\ell}\right), & \text{if } \ell = p. \end{cases}$$

Therefore, there exists $C_4 > 0$, depending only on c_a and $\mathbf{v}_Q = (v_a)_{a \in A - A[\ell]}$, such that

$$\text{Disc}(\text{Par}(\mathbf{v})) = C_4 \cdot \left(\prod_{a \in A[\ell] - \{0\}} \Delta(|w_a|) \right)^{(|A| \cdot (\ell - 1))/\ell}.$$

We are now ready to apply Theorem 5.2 to the innermost sum. We shall do so with every choice of $S \subseteq A[\ell] - \{0\}$ satisfying $T + S = A[\ell]$, which allows us to detect the condition (5.6) using inclusion–exclusion. Here we make essential use of the fact that the leading constant C_{lead} from Theorem 5.2 is independent of S.

5.4 The exponent of the logarithm in the main term

Let us compute $\alpha(A)$, the exponent of the logarithm appearing in Theorem 1.2. When we apply Theorem 5.2, the exponent of the logarithm, denoted by α in the theorem statement, is equal to

$$\sum_{a \in B - \{0\}} \frac{|\text{Lift}(H_a)|}{\varphi(\text{lcm}(M, \ell))} + \sum_{a \in A - B} \frac{|B|}{\ell^{n-1}} \cdot \frac{|\text{Lift}(H_a)|}{\varphi(\text{lcm}(M, \ell))}$$

with n the dimension of $A[\ell]$ as an $\mathbb{F}_\ell$-vector space. Since ℓ is the smallest prime divisor of A, it follows that $\mathbb{Q}(\zeta_\ell)$ and K are disjoint extensions of $\mathbb{Q}$. Therefore, we have

$$\frac{|\text{Lift}(H_a)|}{\varphi(\text{lcm}(M, \ell))} = \frac{|H_a|}{(\ell - 1)\varphi(M)}.$$

By construction, we have that

$$\frac{|H_a|}{\varphi(M)} = \frac{|\widetilde{\pi}(\text{Adm}(a))| \cdot |G|}{\varphi(M)} = \frac{|\widetilde{\pi}(\text{Adm}(a))|}{[K : \mathbb{Q}]} = \frac{|\widetilde{\pi}(\text{Adm}(a))|}{|A/A[\ell]|}.$$

Finally, it follows from Theorem 3.4 that

$$\frac{|\widetilde{\pi}(\text{Adm}(a))|}{|A/A[\ell]|} = \begin{cases} \dfrac{|\text{Adm}(a)|}{|A|}, & \text{if } a \in B - \{0\}, \\ \dfrac{|\text{Adm}(a)|}{|A|} \cdot \dfrac{\ell^{n-1}}{|B|}, & \text{if } a \in A - B. \end{cases}$$

This shows that $\alpha(A)$ is the correct exponent.

1323

5.5 The leading constant

To finish the proof, we now apply Theorem 5.2 for each tuple $\mathbf{v}_Q = (v_a)_{a \in A - A[\ell]}$ such that the associated map $\varphi : G_{\mathbb{Q}} \to A/A[\ell]$ satisfies (P1), (P2) and (P3). Every such tuple $\mathbf{v}_Q$ together with a choice of $\mathbf{c} = (c_a)_{a \in A[\ell] - \{0\}}$ gives a leading constant that we denote by $C_{\mathrm{lead}}(\mathbf{v}_Q, \mathbf{c})$ and also a constant $C_4(\mathbf{v}_Q, \mathbf{c}) > 0$ satisfying

$$\mathrm{Disc}(\mathrm{Par}(\mathbf{v})) = C_4(\mathbf{v}_Q, \mathbf{c}) \cdot \left(\prod_{a \in A[\ell] - \{0\}} \Delta(|w_a|) \right)^{(|A| \cdot (\ell-1))/\ell}.$$

Then we take

$$C_{\mathrm{weak}} = \sum_{\mathbf{v}_Q} \sum_{\mathbf{c}} \frac{C_{\mathrm{lead}}(\mathbf{v}_Q, \mathbf{c})}{C_4(\mathbf{v}_Q, \mathbf{c})}.$$

Because the exponent in the discriminant for all variables outside $A[\ell]$ is bigger than the exponent for the variables in $A[\ell]$, one sees that the sum

$$\sum_{\mathbf{v}_Q} \sum_{\mathbf{c}} \frac{1}{C_4(\mathbf{v}_Q, \mathbf{c})}$$

converges and also may be truncated (to those $\mathbf{v}_Q$ satisfying that $M \leq (\log X)^{C_5}$) with an acceptable error term. Since the leading constant $C_{\mathrm{lead}}(\mathbf{v}_Q, \mathbf{c})$ is uniformly bounded, we conclude that the sum defining C_{weak} may also be truncated. Hence, the contribution from the error term in Theorem 5.2 is negligible.

In order to show that $C_{\mathrm{weak}} > 0$, it suffices to show that $C_{\mathrm{lead}}(\mathbf{v}_Q, \mathbf{c}) > 0$ for some choice of $\mathbf{v}_Q$ and $\mathbf{c}$. We choose a splitting of $A[\ell]$ as $A[\ell] = B \oplus B_{\mathrm{comp}}$ and a splitting $A = \widetilde{B} \oplus B_{\mathrm{comp}}$ with $B \subseteq \widetilde{B}$. By [FLN18, Proposition 5.5], we may find a surjective homomorphism $\varphi' : G_{\mathbb{Q}} \to \widetilde{B}$ such that all decomposition groups are cyclic. In particular, φ' satisfies weak approximation. We extend φ' to a homomorphism $\varphi'' : G_{\mathbb{Q}} \to A$ by sending g to $(\varphi'(g), 0)$, where we have implicitly used our splitting $A = \widetilde{B} \oplus B_{\mathrm{comp}}$.

Now we apply Theorem 5.2 with M equal to the absolute discriminant of φ'', $B = A[\ell] \cap \ell A$ as above, $f(p, S) = B$ for S intersecting B trivially, $g(p) = \{0\}$ and $c_a = 1$. Now twisting φ'' with such multicyclic extensions gives a new A-extension satisfying weak approximation. This forces $C_{\mathrm{lead}}(\mathbf{v}_Q, \mathbf{c}) > 0$ and therefore $C_{\mathrm{weak}} > 0$.

6. The character sum

This section and the following two are devoted to the proof of Theorem 5.2. Let $A = \mathbb{F}_\ell^n$ and let $\mathbf{v} = (v_a)_{a \in \mathbb{F}_\ell^n - \{0\}} \in \mathcal{A}$. Write π_i for the projection map $\pi_i : \mathbb{F}_\ell^n \to \mathbb{F}_\ell$ on the ith coordinate. We begin by expressing the indicator function for a tuple $\mathbf{v}$ being f-correct as an explicit character sum. Define

$$\psi_i = \sum_{\substack{a \in \mathbb{F}_\ell^n \\ \pi_i(a) \neq 0}} \pi_i(a) \cdot \psi_{v_a, \ell, 1}$$

for $i \in [n] := \{1, \ldots, n\}$. We write $\psi : G_{\mathbb{Q}} \to A$ for the homomorphism given by

$$\psi(\sigma) = (\psi_1(\sigma), \ldots, \psi_n(\sigma)),$$

1324

so $\psi = \mathrm{Par}(\mathbf{v})$ by construction. Our aim is to express the sum

$$\sum_{\substack{\mathbf{v}=(v_a)_{a\in A-\{0\}}\in\mathcal{A} \\ \prod_{a\in\mathbb{F}_\ell^n-\{0\}}\Delta(|v_a|)\leq X \\ v_a\neq 1\ \forall a\in S \\ v_a\equiv c_a\bmod d(\ell) \\ \gcd(v_a,M)=1 \\ p|v_a\Rightarrow p\bmod M\in H_a}} \mathbf{1}_{\mathrm{Par}(\mathbf{v})}\ f\text{-correct} \tag{6.1}$$

as a sum of Dirichlet characters. First we will see how to rewrite the indicator function. We have a perfect bilinear pairing

$$A \times A^\vee \to \mathbb{C}^*, \quad (a,\chi) \mapsto \chi(a).$$

Now take some $a \in A$. Then we get an induced perfect bilinear pairing

$$\frac{A}{\langle a \rangle} \times \{\chi \in A^\vee : \chi(a) = 1\} \to \mathbb{C}^*.$$

By definition of f-correct, we need to check the following conditions.

(Q1) For all $a \notin B$ and all $p \mid v_a$ coprime to $2M$,

$$\psi(\mathrm{Frob}_p) - \epsilon_{a,p\bmod M,f} \in B + \langle a \rangle, \tag{6.2}$$

where $\epsilon_{a,p\bmod M,f}$ is an element of A depending only on a, $p \bmod M$ and f.

(Q2) Let $p \mid M$. Suppose that $p \neq 2$ or $\ell \neq 2$. Then we have that p is unramified and, furthermore,

$$\psi(\mathrm{Frob}_p) \in g(p). \tag{6.3}$$

Write e_i for the ith standard basis vector. Also denote by $\chi_i : \mathbb{F}_\ell^n \to \langle \zeta_\ell \rangle$ the element in $A^\vee$ satisfying

$$\chi_i(e_j) = \zeta_\ell^{\delta(i,j)}.$$

Write $B_a = B + \langle a \rangle$. Then we have

$$\{\chi \in A^\vee : \chi(B_a) = 1\} = \left\{ \prod_{j\in[n]} \chi_j^{\pi_j(\mathbf{x})} : \mathbf{x} \in \mathbb{F}_\ell^n, \langle \gamma, \mathbf{x} \rangle = 0 \text{ for all } \gamma \in B_a \right\}.$$

Using orthogonality of characters on the abelian group $\mathbb{F}_\ell^n$, we are now in a position to detect condition (Q1) (i.e., (6.2)) by

$$\frac{1}{\ell^m} \sum_{\substack{\mathbf{x}\in\mathbb{F}_\ell^n \\ \langle\gamma,\mathbf{x}\rangle=0\ \forall\gamma\in B_a}} \prod_{j\in[n]} \chi_j(\psi(\mathrm{Frob}_p))^{\pi_j(\mathbf{x})} \prod_{j\in[n]} \overline{\chi_j(\epsilon_{a,p\bmod M,f})}^{\pi_j(\mathbf{x})},$$

where m equals $n - 1 - \dim_{\mathbb{F}_\ell} B$. We observe that $\chi_j \circ \psi$ is simply ψ_j after identifying $\mathbb{F}_\ell$ with $\langle \zeta_\ell \rangle$ by sending 1 to ζ_ℓ. Therefore, we can rewrite the above as

$$\frac{1}{\ell^m} \sum_{\substack{\mathbf{x}\in\mathbb{F}_\ell^n \\ \langle\gamma,\mathbf{x}\rangle=0\ \forall\gamma\in B_a}} \prod_{j\in[n]} \psi_j(\mathrm{Frob}_p)^{\pi_j(\mathbf{x})} \delta_{a,p\bmod M,j,f}^{\pi_j(\mathbf{x})},$$

where we have renamed $\overline{\chi_j(\epsilon_{a,p\bmod M,f})}$ as $\delta_{a,p\bmod M,j,f}$. We may similarly detect condition (Q2) (i.e., equation (6.3)) by the simultaneous conditions $v_a \not\equiv 0 \bmod p$ for all a and

$$\frac{1}{\ell^n} \sum_{\alpha\in g(p)} \sum_{\mathbf{x}\in\mathbb{F}_\ell^n} \prod_{j\in[n]} \psi_j(\mathrm{Frob}_p)^{\pi_j(\mathbf{x})} \overline{\chi_j(\alpha)}^{\pi_j(\mathbf{x})}. \tag{6.4}$$

We will now return the character sum for condition (Q1) only. It will be straightforward to then insert condition (Q2) later. With this in hand, we are now able to rewrite the indicator function for condition (Q1) as

$$\mathbf{1}_{f \text{ satisfies (Q1)}} = \ell^{-m \sum_{a \in \mathbb{F}_\ell^n - B} \tilde{\omega}(v_a)} \prod_{a \in \mathbb{F}_\ell^n - B} \prod_{\substack{p|v_a \\ p \equiv 1 \bmod 2}} \sum_{\substack{\mathbf{x} \in \mathbb{F}_\ell^n \\ \langle \gamma, \mathbf{x} \rangle = 0 \ \forall \gamma \in B_a}} \prod_{j \in [n]} \psi_j^{\pi_j(\mathbf{x})}(\mathrm{Frob}_p) \delta_{a,p \bmod M, j, f}^{\pi_j(\mathbf{x})},$$

where $\tilde{\omega}$ denotes the number of odd prime divisors. The product equals

$$\prod_{a \in \mathbb{F}_\ell^n - B} \sum_{\substack{(\mathbf{x}_p)_{p|v_a \text{ odd}} \\ \mathbf{x}_p \in \mathbb{F}_\ell^n \\ \langle \gamma, \mathbf{x}_p \rangle = 0 \ \forall \gamma \in B_a}} \prod_{\substack{p|v_a \\ p \equiv 1 \bmod 2}} \prod_{j \in [n]} \psi_j^{\pi_j(\mathbf{x}_p)}(\mathrm{Frob}_p) \delta_{a,p \bmod M, j, f}^{\pi_j(\mathbf{x}_p)},$$

which is in turn

$$\sum_{\substack{(\mathbf{x}_{p,a})_{p|v_a \text{ odd}, a \in \mathbb{F}_\ell^n - B} \\ \mathbf{x}_{p,a} \in \mathbb{F}_\ell^n \\ \langle \gamma, \mathbf{x}_{p,a} \rangle = 0 \ \forall \gamma \in B_a}} \prod_{a \in \mathbb{F}_\ell^n - B} \prod_{\substack{p|v_a \\ p \equiv 1 \bmod 2}} \prod_{j \in [n]} \psi_j^{\pi_j(\mathbf{x}_{p,a})}(\mathrm{Frob}_p) \delta_{a,p \bmod M, j, f}^{\pi_j(\mathbf{x}_{p,a})}.$$

For every $a \in \mathbb{F}_\ell^n - B$ and every $b \in \mathbb{F}_\ell^n$ with $\langle \gamma, b \rangle = 0$ for all $\gamma \in B_a$, we introduce a new variable

$$w_{a,b} = \prod_{\substack{p|v_a \\ p \equiv 1 \bmod 2 \\ \mathbf{x}_{p,a} = b}} p, \quad w_{a,\bullet} = \mathrm{sgn}(v_a) \cdot 2^{v_2(v_a)}.$$

We can recover v_a and the vectors $\mathbf{x}_{p,a}$ from the $w_{a,b}$. Indeed, we have

$$v_a = w_{a,\bullet} \prod_{\substack{b \in \mathbb{F}_\ell^n \\ \langle \gamma, b \rangle = 0 \ \forall \gamma \in B_a}} w_{a,b}.$$

Now to find $\mathbf{x}_{p,a}$, note that $p \mid v_a$ by the definition of $\mathbf{x}_{p,a}$. Therefore, we may take the unique p such that $p \mid w_{a,b}$. Then we reconstruct $\mathbf{x}_{p,a}$ by taking this b. This transforms the sum into

$$\sum_{(v_a)_{a \in B - \{0\}}} \sideset{}{'}\sum_{\substack{(w_{a,b})_{a,b} \\ \prod_a \Delta(|v_a|) \prod_{a,b} \Delta(|w_{a,b}|) \leq X}} \ell^{-m \sum_{a,b} \tilde{\omega}(w_{a,b})} \prod_{a \in \mathbb{F}_\ell^n - B} \prod_{\substack{p|v_a \\ p \equiv 1 \bmod 2}} \prod_{j \in [n]} \psi_j^{\pi_j(b)}(\mathrm{Frob}_p) \delta_{a,p \bmod M, j, f}^{\pi_j(b)},$$

where $\sum'$ also includes the additional summation conditions

$$v_a \equiv c_a \bmod d(\ell), \quad \gcd(v_a, M) = 1, \quad p \mid w_{a,b} \Rightarrow p \bmod M \in H_a$$

and

$$v_a \neq 1 \ \forall a \in S, \quad p \mid v_a \Rightarrow p \bmod M \in H_a, \quad \mathbf{v} \in \mathcal{A}.$$

We now expand ψ_j to deduce that the above sum equals

$$\sum_{(v_a)_{a \in B - \{0\}}} \sideset{}{'}\sum_{\substack{(w_{a,b})_{a,b} \\ \prod_a \Delta(|v_a|) \prod_{a,b} \Delta(|w_{a,b}|) \leq X}} \ell^{-m \sum_{a,b} \tilde{\omega}(w_{a,b})} \prod_{a_1, b_1} \epsilon' \prod_{p|w_{a_1,b_1}} \prod_{j \in [n]} \prod_{\substack{a_2 \in \mathbb{F}_\ell^n \\ \pi_j(a_2) \neq 0}} \psi_{v_{a_2}, \ell, 1}^{\pi_j(b_1) \pi_j(a_2)}(\mathrm{Frob}_p),$$

where

$$\epsilon' = \prod_{j \in [n]} \prod_{p|w_{a_1,b_1}} \delta_{a_1, p \bmod M, j, f}^{\pi_j(b_1)}.$$

By construction we have $\langle b_1, a_2 \rangle = 0$ for $a_2 \in B$. Therefore, we may further expand ψ_j to rewrite the above sum as

$$\sum_{\substack{(v_a)_{a \in B - \{0\}} \\ \prod_a \Delta(|v_a|) \prod_{a,b} \Delta(|w_{a,b}|) \leq X}} \sideset{}{'}\sum_{(w_{a,b})_{a,b}} \ell^{-m \sum_{a,b} \tilde{\omega}(w_{a,b})} \prod_{a_1, b_1} \epsilon' \prod_{p | w_{a_1, b_1}} \prod_{j \in [n]} \prod_{\substack{a_2 \in \mathbb{F}_\ell^n \\ \pi_j(a_2) \neq 0}} \prod_{b_2} \psi_{w_{a_2, b_2}, \ell, 1}^{\pi_j(b_1)\pi_j(a_2)}(\mathrm{Frob}_p),$$

where the product over b_2 includes $\bullet$, while the product over b_1 does not. Using the definition of $\langle \cdot, \cdot \rangle$, we may finally rewrite this as

$$\sum_{\substack{(v_a)_{a \in B - \{0\}} \\ \prod_a \Delta(|v_a|) \prod_{a,b} \Delta(|w_{a,b}|) \leq X}} \sideset{}{'}\sum_{(w_{a,b})_{a,b}} \ell^{-m \sum_{a,b} \tilde{\omega}(w_{a,b})} \prod_{a_1, b_1} \epsilon' \prod_{a_2, b_2} \psi_{w_{a_2, b_2}, \ell, 1}^{\langle b_1, a_2 \rangle}(\mathrm{Frob}_{w_{a_1, b_1}}).$$

Inserting the conditions from (Q2) (see (6.4)) and writing out the implicit summation conditions in $\sum'$, we conclude that

$$\sum_{\substack{\mathbf{v} = (v_a)_{a \in A - \{0\}} \in \mathcal{A} \\ \prod_{a \in \mathbb{F}_\ell^n - \{0\}} \Delta(|v_a|) \leq X \\ v_a \neq 1 \ \forall a \in S \\ v_a \equiv c_a \bmod d(\ell) \\ \gcd(v_a, M) = 1 \\ p | v_a \Rightarrow p \bmod M \in H_a}} \mathbf{1}_{\mathrm{Par}(\mathbf{v})} \ f\text{-correct}$$

equals

$$N(X) = \sum_{\substack{(v_a)_{a \in B - \{0\}} \\ p | v_a \Rightarrow p \bmod M \in H_a}} \sum_{\substack{(w_{a,b})_{a,b} \\ \prod_a \Delta(|v_a|) \prod_{a,b} \Delta(|w_{a,b}|) \leq X \\ v_a \equiv c_a \bmod d(\ell) \\ \gcd(v_a, M) = 1 \\ p | w_{a,b} \Rightarrow p \bmod M \in H_a}} \mathbf{1}_{v_a \neq 1 \ \forall a \in S} \times \mathbf{1}_{\mathbf{v} \in \mathcal{A}}$$

$$\times \prod_{p | M'} \left(\frac{1}{\ell^n} \sum_{\alpha \in g(p)} \sum_{\mathbf{x} \in \mathbb{F}_\ell^n} \prod_{j \in [n]} \psi_j(\mathrm{Frob}_p)^{\pi_j(\mathbf{x})} \overline{\chi_j(\alpha)}^{\pi_j(\mathbf{x})} \right)$$

$$\times \ell^{-m \sum_{a,b} \tilde{\omega}(w_{a,b})} \prod_{a_1, b_1} \epsilon' \prod_{a_2, b_2} \psi_{w_{a_2, b_2}, \ell, 1}^{\langle b_1, a_2 \rangle}(\mathrm{Frob}_{w_{a_1, b_1}}), \tag{6.5}$$

where

$$M' = \begin{cases} \dfrac{M}{2^{v_2(M)}}, & \text{if } \ell = 2, \\ M, & \text{if } \ell > 2. \end{cases}$$

We will now see how to find the main term of the above sum.

7. Combinatorial considerations and the main term

When the characters appearing in the sum described above are non-trivial then they will oscillate, giving rise to cancellation in the sum. However, should the combination of characters cancel then the contribution to the sum will be much larger. The purpose of this section is to develop combinatorial conditions on the indices a, b such that the resulting combination of characters yields a principal character and hence a dominant contribution to the sum. The reader should compare this process to that carried out in [Rom18] or [FK07] in order to identify the main term of their sums of combinations of Legendre symbols.

1327

7.1 Multiquadratic case

Define

$$\mathcal{I} := \{(S,T) : S,T \in \mathbb{F}_2^n, S \notin B, \langle \gamma, T \rangle = 0 \; \forall \gamma \in B_S\}.$$

For a subspace V of $\mathbb{F}_2^n$ we write

$$V^\top = \{S \in \mathbb{F}_2^n : \langle S, v \rangle = 0 \; \forall v \in V\}$$

for the complement under the pairing $\langle \cdot, \cdot \rangle$. We have the following crucial lemma.

LEMMA 7.1. *Let $X \subseteq \mathcal{I}$ with $|X| \geq 2^n - |B|$. Suppose that*

$$\langle S_1, T_2 \rangle + \langle S_2, T_1 \rangle = 0 \tag{7.1}$$

for all $(S_1, T_1), (S_2, T_2) \in X$. Then we have

$$X = \{(S, f(S)) : S \in \mathbb{F}_2^n - B\}$$

for some function $f : \mathbb{F}_2^n - B \to B^\top$ which is alternating with respect to the bilinear pairing $\langle \cdot, \cdot \rangle$, in the sense that

$$\langle S, f(T) \rangle = \langle T, f(S) \rangle \quad \text{and} \quad \langle S, f(S) \rangle = 0.$$

Proof. Denote by π_1 and π_2 the natural projection maps from $\mathcal{I}$ to $\mathbb{F}_2^n$. Write V_1 for the subspace generated by $\pi_1(X)$ and write V_2 for the subspace generated by $\pi_2(X)$. By construction of $\mathcal{I}$ we have that

$$V_2 \subseteq B^\top. \tag{7.2}$$

By the pigeonhole principle there exists some $T_0 \in \pi_2(X)$ such that

$$|\pi_2^{-1}(T_0) \cap X| \geq \frac{2^n - |B|}{|V_2|}. \tag{7.3}$$

List the elements of $\pi_2^{-1}(T_0) \cap X$ as

$$(S_1, T_0), \ldots, (S_\alpha, T_0).$$

Suppose that there exists $T_1 \in \pi_2(X)$ such that

$$\langle S_i, T_1 \rangle + \langle S_j, T_1 \rangle = 1$$

for some $1 \leq i, j \leq \alpha$. We claim that this contradicts (7.1). Indeed, take such a T_1 and such i, j. Let U be such that $(U, T_1) \in X$. Then either (U, T_1) and (S_i, T_0) contradict (7.1) or (U, T_1) and (S_j, T_0) do.

Therefore, we may assume from now on that for all $T_1 \in \pi_2(X)$ and all $1 \leq i, j \leq \alpha$,

$$\langle S_i, T_1 \rangle + \langle S_j, T_1 \rangle = 0.$$

We conclude that $S_i - S_j \in V_2^\top$. We now claim that V_1 contains $V_2^\top$, so it contains in particular B by (7.2). Since we have $S_i - S_j \in V_2^\top$, we now consider the elements

$$\{S_j - S_1 : 2 \leq j \leq \alpha\}.$$

This gives $\alpha - 1 = |\pi_2^{-1}(T_0) \cap X| - 1$ non-zero elements of $V_2^\top \cap V_1$. Therefore, we get from (7.3) that

$$|V_2^\top \cap V_1| \geq \alpha \geq \frac{2^n - |B|}{|V_2|} = |V_2^\top| - \frac{|B|}{|V_2|}$$

1328

after also taking into account the zero element of $V_2^\top \cap V_1$. If B has codimension zero or one, then the lemma is trivial. Otherwise we have

$$|V_2^\top| - \frac{|B|}{|V_2|} \geq |V_2^\top| - \frac{|V_2^\top|}{4}.$$

We conclude that

$$|V_2^\top \cap V_1| \geq \frac{3|V_2^\top|}{4},$$

which readily implies the claim. Thanks to the claim we see that V_1 contains B.

We next claim that V_1 equals $\mathbb{F}_2^n$. We now fix some $S_0 \in \pi_1(X)$. Arguing as before, we see that

$$\langle S_1, T_i \rangle + \langle S_1, T_j \rangle = 0$$

for all $S_1 \in \pi_1(X)$ and all i and j such that $(S_0, T_i), (S_0, T_j) \in X$. In particular, we deduce that $|\pi_1^{-1}(S_0) \cap X| \leq |V_1^\top|$. We now sum to obtain

$$2^n - |B| \leq |X| = \sum_{S_0 \in \pi_1(X)} |\pi_1^{-1}(S_0) \cap X| \leq \sum_{S_0 \in \pi_1(X)} |V_1^\top| \leq (|V_1| - |B|) \cdot |V_1^\top| = 2^n - |B| \cdot |V_1^\top|,$$

because V_1 contains B. But this is only possible if $|V_1^\top| = 1$ or equivalently $V_1 = \mathbb{F}_2^n$. Therefore, there exists a function $f : \mathbb{F}_2^n - B \to B^\top$ such that

$$X = \{(S, f(S)) : S \in \mathbb{F}_2^n - B\}.$$

It is readily verified that f must be alternating, completing the proof. $\qquad \square$

7.2 Multicyclic case

Define

$$\mathcal{I} := \{(a, b) : a, b \in \mathbb{F}_\ell^n, a \notin B, \langle \gamma, b \rangle = 0 \ \forall \gamma \in B_a\},$$

where we recall that $\langle \cdot, \cdot \rangle$ is the standard bilinear form. We have the following crucial lemma.

LEMMA 7.2. *Let $X \subseteq \mathcal{I}$ with $|X| \geq \ell^n - |B|$. Suppose that*

$$\langle a_2, b_1 \rangle = 0 \tag{7.4}$$

for all $(a_1, b_1), (a_2, b_2) \in X$. Then we have

$$X = \{(a, 0) : a \in \mathbb{F}_\ell^n - B\}.$$

Proof. The proof is similar to the proof of Lemma 7.1. We write π_1 and π_2 for the natural projection maps from $\mathcal{I}$ to $\mathbb{F}_\ell^n$. We denote by N the number of elements in the subspace generated by $\pi_2(X)$. If $N = 1$, then we have

$$X = \{(a, 0) : a \in \mathbb{F}_\ell^n - B\}.$$

From now on we may and will assume that $N > 1$ and seek a contradiction.

Take some $b_0 \in \pi_2(X)$ and suppose that $|\pi_2^{-1}(b_0) \cap X| \geq (\ell^n - |B|)/N$. The existence of such a b_0 is guaranteed by the pigeonhole principle and our assumption $|X| \geq \ell^n - |B|$. We enumerate the elements of $\pi_2^{-1}(b_0) \cap X$ as

$$(a_1, b_0), \ldots, (a_k, b_0)$$

with $k \geq (\ell^n - |B|)/N$. Then we have, thanks to (7.4), the equality

$$\langle a_i, b \rangle = 0$$

for all $b \in \pi_2(X)$ and all $1 \leq i \leq k$. Since $\langle \cdot, \cdot \rangle$ is non-degenerate and N is the cardinality of the subspace generated by $\pi_2(X)$, it follows that there exists a subspace V of dimension $n - \log_\ell N$

1329

containing B such that $a_i \in V$ for all $1 \le i \le k$. Furthermore, we know that the a_i are not in B. This gives the inclusion

$$\{a_i : 1 \le i \le k\} \subseteq V \setminus B$$

and therefore the bound $k \le \ell^n/N - |B|$. Therefore, we conclude that

$$\frac{\ell^n}{N} - |B| \ge k = |\pi_2^{-1}(b_0) \cap X| \ge \frac{\ell^n - |B|}{N},$$

which is a contradiction for $N > 1$. $\qquad\square$

8. Oscillation of characters

We now return to (6.5). We say that an integer x is large if

$$|x| > \exp\big((\log X)^{A_1}\big),$$

where $A_1 > 0$ is a small constant that we will choose later.

8.1 Large variables

We split the character sum $N(X)$ in two subsums

$$N(X) = N_{\text{small}}(X) + N_{\text{large}}(X),$$

where $N_{\text{small}}(X)$ is by definition the contribution to $N(X)$, where at most $\ell^n - |B| - 1$ of the variables $w_{a,b}$ are large, and $N_{\text{large}}(X)$ is by definition the remaining contribution. We will make use of the following well-known lemma.

LEMMA 8.1. *Let $\kappa, C > 0$ be fixed real numbers. Then we have the bounds*

$$\sum_{\substack{1 \le n \le x \\ p|n \Rightarrow p \bmod M \in H}} \mu^2(n) \kappa^{\omega(n)} \ll_{\kappa,C} x(\log x)^{(|H| \cdot \kappa)/\varphi(M) - 1}$$

and

$$\sum_{\substack{1 \le n \le x \\ p|n \Rightarrow p \bmod M \in H}} \frac{\mu^2(n) \kappa^{\omega(n)}}{n} \ll_{\kappa,C} (\log x)^{(|H| \cdot \kappa)/\varphi(M)}$$

for all $M \le (\log x)^C$ and all subsets H of $(\mathbb{Z}/M\mathbb{Z})^*$.

Proof. The first bound follows from Theorem 4.1 with

$$f(n) := \mu^2(n) \kappa^{\omega(n)} \mathbf{1}_{p|n \Rightarrow p \bmod M \in H}, \quad \alpha := \frac{|H| \cdot \kappa}{\varphi(M)}, \quad k := \kappa, \quad Q := \exp\big((\log x)^{\min(1/4\kappa, 1/2)}\big)$$

and $J := 1$, $\epsilon := 1/10$. Assumption (4.1) is guaranteed by the Siegel–Walfisz theorem. The second bound follows from partial summation and the first bound. $\qquad\square$

After choosing the constant $A_1 > 0$ to be sufficiently small, it follows from Lemma 8.1 that we have the bound

$$N_{\text{small}}(X) = O\big(X(\log X)^{\alpha - 1 - \delta}\big)$$

for some $\delta > 0$. It is precisely at this step that we make fundamental use of the assumptions $|H_a| = |H_{a'}|$ for all $a, a' \in A - B$ and $[(\mathbb{Z}/M\mathbb{Z})^* : H_a] \le C$.

1330

8.2 Linked variables

We will now turn our attention to $N_{\text{large}}(X)$. We say that an integer x is medium if

$$|x| > (\log X)^{A_2},$$

where $A_2 > 0$ is a large constant to be chosen later. We also split the sum $N_{\text{large}}(X)$ into two subsums, namely

$$N_{\text{large}}(X) = N_{\text{linked}}(X) + N_{\text{main}}(X).$$

Here $N_{\text{linked}}(X)$ is the contribution to $N_{\text{large}}(X)$ for which the following assertions hold.

- If $\ell > 2$, then there exists $(a_1, b_1), (a_2, b_2) \in \mathcal{I}$ such that the following conditions hold:
  (1) we have $\langle a_2, b_1 \rangle \neq 0$ or $\langle a_1, b_2 \rangle \neq 0$;
  (2) we have that w_{a_1,b_1} and w_{a_2,b_2} are both medium or we have that $|w_{a_1,b_1}|, |w_{a_2,b_2}| > 1$ and one of the w_{a_i,b_i} is large.
- If $\ell = 2$, then there exists $(a_1, b_1), (a_2, b_2) \in \mathcal{I}$ such that the following conditions hold:
  (1) we have $\langle a_2, b_1 \rangle + \langle a_1, b_2 \rangle = 1$;
  (2) we have that w_{a_1,b_1} and w_{a_2,b_2} are both medium or we have that $|w_{a_1,b_1}|, |w_{a_2,b_2}| > 2$ and one of the w_{a_i,b_i} is large.

Furthermore, $N_{\text{main}}(X)$ is by definition the remaining contribution.

Our next goal is to bound $N_{\text{linked}}(X)$. Our two principal tools are the large sieve, as presented in Proposition 4.3, and the Siegel–Walfisz theorem over number fields as presented in the main theorem of [Gol70].

8.2.1 *Equidistribution with the large sieve.* We will now bound $N_{\text{linked}}(X)$. We will first suppose that there exist $(a_1, b_1), (a_2, b_2) \in \mathcal{I}$ with w_{a_1,b_1} and w_{a_2,b_2} both medium and satisfying the aforementioned conditions. So fix such a choice of (a_1, b_1) and (a_2, b_2). Define $\mathcal{I}' := \mathcal{I} - \{(a_1, b_1), (a_2, b_2)\}$. The corresponding contribution to $N_{\text{linked}}(X)$ is bounded by

$$\sum_{(v_a)_{a \in B - \{0\}}} \sum_{(w_{a,\bullet})} \sum_{(w_{a,b})_{(a,b) \in \mathcal{I}'}} \ell^{-m \sum_{(a,b) \in \mathcal{I}'} \tilde{\omega}(w_{a,b})}$$

$$\times \left| \sum_{\substack{w_{a_1,b_1}, w_{a_2,b_2} \\ \Delta(|w_{a_1,b_1} w_{a_2,b_2}|) \leq X/(\prod_a \Delta(|v_a|) \prod_{(a,b) \in \mathcal{I}'} \Delta(|w_{a,b}|))}} \alpha_{w_{a_1,b_1}} \beta_{w_{a_2,b_2}} \psi^{\langle b_1, a_2 \rangle}_{w_{a_2,b_2}, \ell, 1}(\text{Frob}_{w_{a_1,b_1}}) \psi^{\langle b_2, a_1 \rangle}_{w_{a_1,b_1}, \ell, 1}(\text{Frob}_{w_{a_2,b_2}}) \right|,$$

$$(8.1)$$

where $\alpha_{w_{a_1,b_1}}$ and $\beta_{w_{a_2,b_2}}$ are complex numbers of absolute value bounded by 1 depending only on respectively w_{a_1,b_1} and w_{a_2,b_2} (and $w_{a,b}$ for $(a, b) \in \mathcal{I}'$). By changing the coefficients if necessary, we may assume from now on that w_{a_1,b_1} and w_{a_2,b_2} are coprime to ℓ.

We now work towards our goal of applying Proposition 4.3. We take $K = \mathbb{Q}(\zeta_\ell)$ and take the M of Proposition 4.3 to be a sufficiently large power of ℓ. Critically, the field K depends only on the abelian group A. Write $(\cdot / \cdot)_{\mathbb{Q}(\zeta_\ell), \ell}$ for the ℓth power residue symbol in $\mathbb{Q}(\zeta_\ell)$. We define

$$\gamma(w, z) := \left(\frac{N_{\mathbb{Q}(\zeta_\ell)/\mathbb{Q}}(w)}{z} \right)^{\langle b_1, a_2 \rangle}_{\mathbb{Q}(\zeta_\ell), \ell} \left(\frac{N_{\mathbb{Q}(\zeta_\ell)/\mathbb{Q}}(z)}{w} \right)^{\langle b_2, a_1 \rangle}_{\mathbb{Q}(\zeta_\ell), \ell}. \tag{8.2}$$

Note that if we define $\tilde{\gamma}(w, z) := \gamma(z, w)$, then $\tilde{\gamma}(w, z)$ is still of the form (8.2). Therefore, if we check properties (P1)–(P3) for all $\gamma(w, z)$, then these properties will also hold for $\tilde{\gamma}(w, z)$. This allows us to circumvent the condition $X \leq Y$ in Proposition 4.3 by applying Proposition 4.3

1331

to $\gamma(w,z)$ or $\widetilde{\gamma}(w,z)$ depending on whether X or Y is larger. Let us now verify (P1)–(P3).

Property (P1) is clear. We take A_{bad} to be the set of squarefull integers. In particular, property (P3) is immediate for $C_2 = 1/2$ if we take C_1 sufficiently large. The first part of property (P2) follows from reciprocity and the periodicity of power residue symbols provided that we take the M from Proposition 4.3 to be a sufficiently large power of ℓ. It remains to prove the final part of property (P2).

To this end, fix some w. Then the application $z \mapsto \gamma(w,z)$ is a multiplicative character with period $MN_{\mathbb{Q}(\zeta_\ell)/\mathbb{Q}}(w)$ by assumption. Therefore, by orthogonality of characters, it suffices to show that the character $z \mapsto \gamma(w,z)$ is not the principal character. By assumption, we have that $N_{\mathbb{Q}(\zeta_\ell)/\mathbb{Q}}(w)$ is not squarefull. Therefore, we may take a prime ideal $\mathfrak{p}$ of $\mathbb{Q}(\zeta_\ell)$ of degree one that divides w such that none of the conjugates of $\mathfrak{p}$ divides w. By the Chinese remainder theorem, we may find an element $z \in \mathbb{Z}[\zeta_\ell]$ such that

$$z \equiv 1 \bmod M, \quad z \equiv 1 \bmod \mathfrak{q} \text{ for all } \mathfrak{q} \mid N_{\mathbb{Q}(\zeta_\ell)/\mathbb{Q}}(w) \text{ with } \mathfrak{q} \neq \mathfrak{p}, \quad z \equiv \alpha \bmod \mathfrak{p},$$

where α is any generator of the cyclic group $(\mathbb{Z}[\zeta_\ell]/\mathfrak{p})^* \cong \mathbb{F}_p^*$. Using our assumptions on $\langle b_1, a_2 \rangle$ and $\langle b_2, a_1 \rangle$, it is not hard to show now that $z \mapsto \gamma(w,z)$ is not the principal character. We have finished checking that $\gamma(\cdot, \cdot)$ satisfies all the conditions of Proposition 4.3.

However, in (8.1), we are at the moment summing over rational integers and not over elements of $\mathbb{Z}[\zeta_\ell]$. Therefore, we aim to replace the sum over the integers by a sum taking place in $\mathbb{Q}(\zeta_\ell)$. The following lemma is critical.

LEMMA 8.2. *Fix a root of unity $\zeta_\ell \in \mathbb{C}$ inducing an identification between $\mathbb{F}_\ell$ and $\langle \zeta_\ell \rangle$ by sending 1 to ζ_ℓ. Let p be a prime number such that $p \equiv 1 \bmod \ell$. Then there are canonical bijections*

$$\{\phi \in \text{Epi}(G_\mathbb{Q}, \mathbb{F}_\ell) : \phi \text{ ramified only at } p\} \leftrightarrow \{\text{Dirichlet characters modulo } p \text{ of order } \ell\}$$

$$\leftrightarrow \{\text{prime ideals of } \mathbb{Q}(\zeta_\ell) \text{ above } p\}.$$

Proof. Given a map $\phi \in \text{Epi}(G_\mathbb{Q}, \mathbb{F}_\ell)$ that is only ramified at p, class field theory implies that ϕ factors through $\text{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q})$, which is canonically isomorphic to $(\mathbb{Z}/p\mathbb{Z})^*$. Therefore, we may associate to ϕ an epimorphism from $(\mathbb{Z}/p\mathbb{Z})^*$ to $\mathbb{F}_\ell$. Using our identification between $\mathbb{F}_\ell$ and $\langle \zeta_\ell \rangle$, ϕ induces a map $(\mathbb{Z}/p\mathbb{Z})^* \to \mathbb{C}^*$. Extending ϕ in the usual way to $\mathbb{Z}$ gives a Dirichlet character modulo p of order equal to ℓ. This defines the first bijection.

For the second bijection, suppose that we are given an ideal $\mathfrak{p}$ of $\mathbb{Q}(\zeta_\ell)$ above p. Since $\mathfrak{p}$ has degree one, one readily verifies that the map

$$n \mapsto \left(\frac{n}{\mathfrak{p}} \right)_{\mathbb{Q}(\zeta_\ell), \ell}$$

is a Dirichlet character. One directly shows that this is a bijection as well, completing the proof of the lemma. $\qquad \square$

By Lemma 8.2, the choice of $\psi_{p,\ell,1}$ from § 2 is equivalent to choosing a prime ideal $\mathfrak{p}$ of $\mathbb{Q}(\zeta_\ell)$ above p. Observe that p indeed splits in $\mathbb{Q}(\zeta_\ell)$, because we have the congruence $p \equiv 1 \bmod \ell$ if $\psi_{p,\ell,1}$ is a homomorphism. We write this unique ideal $\mathfrak{p}$ as $\text{Pref}_\ell(p)$. We extend the definition of $\text{Pref}_\ell(p)$ multiplicatively to a function $\text{Pref}_\ell(x)$ for all squarefree integers x supported in primes congruent to 1 modulo ℓ.

We fix a set of integral ideals $I_1, \ldots, I_t$ representing every ideal class of $\text{Cl}(\mathbb{Q}(\zeta_\ell))$. We now split (8.1) into t^2 sums, where we insert the additional condition that

$$\text{Pref}_\ell(w_{a_1,b_1}) \sim I_{s_1}, \quad \text{Pref}_\ell(w_{a_2,b_2}) \sim I_{s_2},$$

where we fixed some integers $1 \leq s_1, s_2 \leq t$. We introduce new variables w and z in the fundamental domain of K such that

$$(w)I_{s_1} = \mathrm{Pref}_\ell(w_{a_1,b_1}), \quad (z)I_{s_2} = \mathrm{Pref}_\ell(w_{a_2,b_2}).$$

We also define new coefficients

$$\alpha_w = \begin{cases} \alpha_{N_{\mathbb{Q}(\zeta_\ell)/\mathbb{Q}}(wI_{s_1})} \cdot \left(\dfrac{N_{\mathbb{Q}(\zeta_\ell)/\mathbb{Q}}(w)}{I_{s_2}} \right)_{\mathbb{Q}(\zeta_\ell),\ell}^{\langle b_2,a_1 \rangle} \cdot \left(\dfrac{N_{\mathbb{Q}(\zeta_\ell)/\mathbb{Q}}(I_{s_2})}{w} \right)_{\mathbb{Q}(\zeta_\ell),\ell}^{\langle b_1,a_2 \rangle}, & \text{if } (w)I_{s_1} \in \mathrm{Im}(\mathrm{Pref}_\ell), \\ 0, & \text{otherwise} \end{cases}$$

and

$$\beta_z = \begin{cases} \beta_{N_{\mathbb{Q}(\zeta_\ell)/\mathbb{Q}}(zI_{s_2})} \cdot \left(\dfrac{N_{\mathbb{Q}(\zeta_\ell)/\mathbb{Q}}(z)}{I_{s_1}} \right)_{\mathbb{Q}(\zeta_\ell),\ell}^{\langle b_1,a_2 \rangle} \cdot \left(\dfrac{N_{\mathbb{Q}(\zeta_\ell)/\mathbb{Q}}(I_{s_1})}{z} \right)_{\mathbb{Q}(\zeta_\ell),\ell}^{\langle b_2,a_1 \rangle}, & \text{if } (z)I_{s_2} \in \mathrm{Im}(\mathrm{Pref}_\ell), \\ 0, & \text{otherwise.} \end{cases}$$

Then the inner sum of (8.1) becomes t^2 sums of the form

$$\frac{1}{(\ell-1)^2} \left| \sum_w \sum_z \alpha_w \beta_z \gamma(w,z) \right|, \tag{8.3}$$

where we divide by $1/(\ell-1)^2$, because the fundamental domain of $\mathbb{Q}(\zeta_\ell)$ contains $\ell - 1 = \varphi(\ell)$ generators for each principal ideal.

Finally, there is one more barrier to overcome before we are ready to apply Proposition 4.3. The implicit condition in (8.3) is that

$$N_{\mathbb{Q}(\zeta_\ell)/\mathbb{Q}}(wz) \leq B$$

for some bound $B > 0$, while Proposition 4.3 applies only to box shapes given by $N_{\mathbb{Q}(\zeta_\ell)/\mathbb{Q}}(w) \leq W$ and $N_{\mathbb{Q}(\zeta_\ell)/\mathbb{Q}}(z) \leq Z$. To this end, we split w and z into intervals of the form

$$W \leq N_{\mathbb{Q}(\zeta_\ell)/\mathbb{Q}}(w) \leq W\left(1 + \frac{1}{(\log X)^{A_3}}\right), \quad Z \leq N_{\mathbb{Q}(\zeta_\ell)/\mathbb{Q}}(z) \leq Z\left(1 + \frac{1}{(\log X)^{A_3}}\right).$$

This does not cover the entire region, but for sufficiently large A_3 one may bound the resulting leftover trivially. Inserting the bound of Proposition 4.3 for each such sum into (8.1) and summing trivially shows that $N_{\mathrm{linked}}(X)$ ends up in the error term, in the case where w_{a_1,b_1} and w_{a_2,b_2} are both medium, upon choosing A_2 sufficiently large in terms of A_3.

8.2.2 *Equidistribution with Siegel–Walfisz.* It is now time to bring the Siegel–Walfisz theorem into play. Let $(a_1, b_1) \in \mathcal{I}$ be such that w_{a_1,b_1} is large. By definition of $N_{\mathrm{linked}}(X)$, we know that there exists $(a_2, b_2) \in \mathcal{I}$ satisfying

- $|w_{a_2,b_2}| > 2$;
- $\langle a_2, b_1 \rangle \neq 0$ or $\langle a_1, b_2 \rangle \neq 0$ if $\ell > 2$;
- $\langle a_2, b_1 \rangle + \langle a_1, b_2 \rangle = 1$ if $\ell = 2$.

Furthermore, by the work done in §8.2.1, we may assume that all pairs (a_2, b_2) satisfying the above properties are such that w_{a_2,b_2} is not medium. Define $\mathcal{I}' := \mathcal{I} - \{(a_1, b_1)\}$. We now expand

1333

the product over the primes p dividing M'. Then we bound the corresponding contribution by

$$\sum_{(\alpha_p)_{p|M'}} \sum_{(\mathbf{x}_p)_{p|M'}} \sum_{(v_a)_{a \in B - \{0\}}} \sum_{(w_{a,\bullet})} \sum_{(w_{a,b})_{(a,b) \in \mathcal{I}'}} \ell^{-m \sum_{(a,b) \in \mathcal{I}'} \tilde{\omega}(w_{a,b})}$$

$$\times \left| \sum_{\substack{\Delta(|w_{a_1,b_1}|) \leq X/(\prod_a \Delta(|v_a|) \prod_{(a,b) \in \mathcal{I}'} \Delta(|w_{a,b}|)) \\ w_{a_1,b_1} \equiv c' \bmod d(\ell) \\ \gcd(w_{a_1,b_1},M)=1 \\ p|w_{a_1,b_1} \Rightarrow p \bmod M \in H_{a_1}}} \ell^{-m\tilde{\omega}(w_{a_1,b_1})} \left(\prod_{j \in [n]} \prod_{p|w_{a_1,b_1}} \delta_{a_1,p \bmod M,j,f}^{\pi_j(b_1)} \right) \right.$$

$$\times \left(\prod_{(a_2,b_2) \in \mathcal{I}'} \psi_{w_{a_2,b_2},\ell,1}^{\langle b_1,a_2 \rangle}(\mathrm{Frob}_{w_{a_1,b_1}}) \psi_{w_{a_1,b_1},\ell,1}^{\langle b_2,a_1 \rangle}(\mathrm{Frob}_{w_{a_2,b_2}}) \right)$$

$$\left. \times \left(\prod_{p|M'} \prod_{j \in [n]} \psi_{w_{a_1,b_1},\ell,1}(\mathrm{Frob}_p)^{\pi_j(\mathbf{x}_p)\pi_j(a_1)} \overline{\chi_j(\alpha_p)}^{\pi_j(\mathbf{x}_p)} \right) \right|, \tag{8.4}$$

where we also stipulate that the $w_{a,b}$ are squarefree, pairwise coprime and satisfy $p \mid w_{a,b} \Rightarrow p \equiv 0, 1 \bmod \ell$. We now define the multiplicative function h supported on squarefree integers and given on the primes coprime to ℓ by

$$h(q) = \ell^{-m} \times \mathbf{1}_{\gcd(q,M \prod_a v_a \prod_{(a,b) \in \mathcal{I}'} w_{a,b})=1} \times \mathbf{1}_{q \bmod M \in H_{a_1}} \times \mathbf{1}_{q \equiv 1 \bmod \ell}$$

$$\times \prod_{j \in [n]} \delta_{a_1,q \bmod M,j,f}^{\pi_j(b_1)} \times \prod_{(a_2,b_2) \in \mathcal{I}'} \psi_{w_{a_2,b_2},\ell,1}^{\langle b_1,a_2 \rangle}(\mathrm{Frob}_q) \psi_{q,\ell,1}^{\langle b_2,a_1 \rangle}(\mathrm{Frob}_{w_{a_2,b_2}})$$

$$\times \prod_{p|M'} \prod_{j \in [n]} \psi_{q,\ell,1}(\mathrm{Frob}_p)^{\pi_j(\mathbf{x}_p)\pi_j(a_1)} \overline{\chi_j(\alpha_p)}^{\pi_j(\mathbf{x}_p)}.$$

We claim that

$$\sum_{1 \leq q \leq X} h(q) \log q = O_A\left(\frac{X}{(\log X)^A} \right) \tag{8.5}$$

for every $A > 0$. Applying Theorem 4.1 then shows that

$$\sum_{1 \leq n \leq X} h(n) = O_A\left(\frac{X}{(\log X)^A} \right)$$

for every $A > 0$. Using this for a sufficiently large A and inserting it into (8.4) gives the desired upper bound for (8.4) after a trivial summation.

1334

It remains to prove (8.5). For now we assume that $\ell > 2$, and we will later sketch the modifications to get the case $\ell = 2$. Before we proceed, let us remark that the sum

$$\sum_{1 \leq q \leq X} \psi_{q,\ell,1}(\mathrm{Frob}_{w_{a_2,b_2}})$$

need not oscillate. Indeed, recall that $\psi_{q,\ell,1}$ depends on our choice of σ_q, and for a dramatically poor choice we might (for example) have

$$\psi_{q,\ell,1}(\mathrm{Frob}_{w_{a_2,b_2}}) \in \{1, \zeta_\ell\}.$$

With this in mind, let us now work towards the proof of (8.5). We now pass to $\mathbb{Q}(\zeta_\ell)$. We have already seen in Lemma 8.2 that the choice of $\psi_{q,\ell,1}$ is equivalent to a choice of prime ideal $\mathfrak{p}$ of $\mathbb{Q}(\zeta_\ell)$ above q. We also remind the reader that this ideal was called $\mathrm{Pref}_\ell(q)$. Consider the Hecke character ρ of $\mathbb{Q}(\zeta_\ell)$ defined as

$$\rho(\mathfrak{p}) = \mathbf{1}_{\gcd(N_{\mathbb{Q}(\zeta_\ell)/\mathbb{Q}}(\mathfrak{p}), M \prod_a v_a \prod_{(a,b) \in \mathcal{I}'} w_{a,b}) = 1}$$
$$\times \prod_{(a_2,b_2) \in \mathcal{I}'} \left(\frac{N_{\mathbb{Q}(\zeta_\ell)/\mathbb{Q}}(\mathfrak{p})}{\mathrm{Pref}_\ell(w_{a_2,b_2})} \right)_{\mathbb{Q}(\zeta_\ell),\ell}^{\langle b_1, a_2 \rangle} \left(\frac{w_{a_2,b_2}}{\mathfrak{p}} \right)_{\mathbb{Q}(\zeta_\ell),\ell}^{\langle b_2, a_1 \rangle} \times \prod_{p | M'} \prod_{j \in [n]} \left(\frac{p}{\mathfrak{p}} \right)_{\mathbb{Q}(\zeta_\ell),\ell}^{\pi_j(\mathbf{x}_p)\pi_j(a_1)}.$$

We have the fundamental identity

$$\ell^m \cdot h(q) = \mathbf{1}_{q \bmod M \in H_{a_1}} \cdot \rho(\mathrm{Pref}_\ell(q)) \cdot \zeta(q), \tag{8.6}$$

where $\zeta(q)$ is an ℓth root of unity depending only on $q \bmod M$. Since $|w_{a_2,b_2}| > 2$ and since w_{a_2,b_2} is coprime to M, we see that ρ is a non-trivial character and so is $\rho\chi$ for any Dirichlet character χ modulo M. Then the main theorem of Goldstein [Gol70] yields

$$\sum_{N_{\mathbb{Q}(\zeta_\ell)/\mathbb{Q}}(\mathfrak{p}) \leq X} (\rho\chi)(\mathfrak{p}) = O_A\left(\frac{X}{(\log X)^A} \right) \tag{8.7}$$

for every $A > 0$. Note that Goldstein's result formally only applies to primitive characters, but one readily passes to non-primitive characters by trivially bounding the contribution of the primes dividing the conductor. Here we use that the norm of the conductor is bounded by a suitable power of $\log X$ depending only on our starting abelian group.

Our goal is now to deduce (8.5) from (8.6) and (8.7). But as we have emphasised before, this may not be possible if we made a dramatically poor choice of σ_q. We say that a choice $(\mathrm{Pref}_\ell(q))_{q \equiv 1 \bmod \ell, q \leq X}$ is poor if there exists some integer $\exp((\log X)^{A_1}) \leq n \leq X$, some Hecke character ψ of $\mathbb{Q}(\zeta_\ell)$ of order ℓ such that the norm of the conductor is bounded by X and some $a \in \mathbb{F}_\ell^*$ such that

$$\left| |\{q \leq n : \psi(\mathrm{Pref}_\ell(q)) = \zeta_\ell^a\}| - \frac{|\{q \leq n : \psi(\mathrm{Pref}_\ell(q)) \neq 1\}|}{\ell - 1} \right| \geq n^{3/4}. \tag{8.8}$$

For fixed n, ψ and a, observe that this is an entirely combinatorial condition. Indeed, $\psi(\mathrm{Pref}_\ell(q))$ runs through all values of ζ_ℓ^a with $a \in \mathbb{F}_\ell^*$ exactly once as we run through the choices of $\mathrm{Pref}_\ell(q)$. For fixed n, ψ and a, we bound the event (8.8) using Hoeffding's inequality with the probability space corresponding to the set of choices $(\mathrm{Pref}_\ell(q))_{q \equiv 1 \bmod \ell, q \leq X}$. This also gives a bound for the event that $(\mathrm{Pref}_\ell(q))_{q \equiv 1 \bmod \ell, q \leq X}$ is poor by using the union bound. This shows that for X large enough, we may pick σ_q such that $(\mathrm{Pref}_\ell(q))_{q \equiv 1 \bmod \ell, q \leq X}$ is not poor. In particular, we may pick

one such choice of σ_q at the start of our proof. Then we have that

$$\sum_{1 \leq q \leq X} (\rho\chi)(\mathrm{Pref}_\ell(q)) = O_A\left(\frac{X}{(\log X)^A}\right),$$

which implies that

$$\sum_{\substack{1 \leq q \leq X \\ q \equiv a \bmod M}} \rho(\mathrm{Pref}_\ell(q)) = O_A\left(\frac{X}{(\log X)^A}\right)$$

for every invertible class $a \bmod M$.

Thanks to the above equation and (8.6), we obtain that

$$\ell^m \cdot \sum_{1 \leq q \leq X} h(q) = \sum_{\substack{\lambda \in (\mathbb{Z}/M\mathbb{Z})^* \\ \lambda \in H_{a_1}}} \zeta(\lambda) \sum_{\substack{1 \leq q \leq X \\ q \equiv \lambda \bmod M}} \rho(\mathrm{Pref}_\ell(q)) = O_A\left(\frac{X}{(\log X)^A}\right).$$

We deduce that (8.5) holds by partial summation.

In the case $\ell = 2$, we must also contend with the congruence condition $w_{a_1,b_1} \equiv c' \bmod 16$. We detect this congruence condition using Dirichlet characters and may now proceed as above.

8.3 The main term

We now use the results from § 7 to finish the proof. We distinguish two cases.

Let us start with the case $\ell > 2$. We apply Lemma 7.2 with

$$Y = \{(a,b) \in \mathcal{I} : w_{a,b} \text{ large}\}.$$

By construction of $N_{\mathrm{main}}(X)$ we have that:

– $|Y| \geq \ell^n - |B|$ thanks to § 8.1;
– $\langle a_2, b_1 \rangle = 0$ for all $(a_1, b_1), (a_2, b_2) \in Y$ thanks to § 8.2.

Therefore, all conditions of Lemma 7.2 are satisfied. We conclude that

$$Y = \{(a,0) : a \in \mathbb{F}_\ell^n - B\}.$$

We now observe that for every $(a_1, b_1) \in \mathcal{I}$ with $b_1 \neq 0$ there exists some $(a,0) \in Y$ such that $\langle a, b_1 \rangle \neq 0$. By § 8.2 and by definition of $N_{\mathrm{main}}(X)$, this forces $w_{a,b} = 1$ for all $b \neq 0$. Therefore, $N_{\mathrm{main}}(X)$ becomes

$$N_{\mathrm{main}}(X) = \sum_{\substack{(v_a)_{a \in B-\{0\}} \\ p|v_a \Rightarrow p \bmod M \in H_a}} \sum_{\substack{(w_{a,0})_a \\ w_{a,0} \text{ large} \\ \prod_a \Delta(|v_a|) \prod_a \Delta(|w_{a,0}|) \leq X \\ v_a \equiv c_a \bmod d(\ell) \\ \gcd(w_{a,0}, M) = 1 \\ p|w_{a,0} \Rightarrow p \bmod M \in H_a}} \mathbf{1}_{\mathbf{v} \in \mathcal{A}} \times \ell^{-m \sum_{a,0} \tilde\omega(w_{a,0})}$$

$$\times \prod_{p|M'}\left(\frac{1}{\ell^n} \sum_{\alpha \in g(p)} \sum_{\mathbf{x} \in \mathbb{F}_\ell^n} \prod_{j \in [n]} \psi_j(\mathrm{Frob}_p)^{\pi_j(\mathbf{x})} \overline{\chi_j(\alpha)}^{\pi_j(\mathbf{x})}\right),$$

where we also demand that all $w_{a,0}$ are large. Expanding the product over M', we get a combination of non-principal characters of small conductor unless $\mathbf{x}$ is the zero vector. Another application of Siegel–Walfisz, where we sum over an appropriate variable $w_{a,0}$ depending on $\mathbf{x}$,

1336

yields the asymptotic

$$
N_{\mathrm{main}}(X) = \sum_{\substack{(v_a)_{a \in B-\{0\}} \\ p|v_a \Rightarrow p \bmod M \in H_a}} \sum_{\substack{(w_{a,0})_a \\ w_{a,0} \text{ large} \\ \mathbf{v} \in \mathcal{A} \\ \prod_a \Delta(|v_a|) \prod_a \Delta(|w_{a,0}|) \leq X \\ v_a \equiv c_a \bmod d(\ell) \\ \gcd(w_{a,0},M)=1 \\ p|w_{a,0} \Rightarrow p \bmod M \in H_a}} \ell^{-m \sum_{a,0} \tilde{\omega}(w_{a,0})} \prod_{p|M'} \frac{|g(p)|}{\ell^n} + O_A\left(\frac{X}{(\log X)^A}\right).
$$

We may also remove the condition that $w_{a,0}$ is large with an acceptable error term. Therefore, we conclude that

$$
N(X) = \sum_{\substack{(v_a)_{a \in B-\{0\}} \\ p|v_a \Rightarrow p \bmod M \in H_a}} \sum_{\substack{(w_{a,0})_a \\ \mathbf{v} \in \mathcal{A} \\ \prod_a \Delta(|v_a|) \prod_a \Delta(|w_{a,0}|) \leq X \\ v_a \equiv c_a \bmod d(\ell) \\ \gcd(w_{a,0},M)=1 \\ p|w_{a,0} \Rightarrow p \bmod M \in H_a}} \ell^{-m \sum_{a,0} \tilde{\omega}(w_{a,0})} \prod_{p|M'} \frac{|g(p)|}{\ell^n} + O_A\left(X(\log X)^{\alpha-1-\delta}\right)
$$

for some $\delta > 0$. Since ℓ is odd, we have $d(\ell) = 1$. We directly evaluate the above sum using Theorem 4.1 with

$$
\alpha = \sum_{a \in B-\{0\}} \frac{1}{\varphi(\mathrm{lcm}(M,\ell))} \sum_{\lambda \in (\mathbb{Z}/\mathrm{lcm}(M,\ell)\mathbb{Z})^*} \mathbf{1}_{\lambda \equiv 1 \bmod \ell} \cdot \mathbf{1}_{\lambda \bmod M \in H_a}
$$
$$
+ \frac{1}{\ell^m} \sum_{a \in A-B} \frac{1}{\varphi(\mathrm{lcm}(M,\ell))} \sum_{\lambda \in (\mathbb{Z}/\mathrm{lcm}(M,\ell)\mathbb{Z})^*} \mathbf{1}_{\lambda \equiv 1 \bmod \ell} \cdot \mathbf{1}_{\lambda \bmod M \in H_a},
$$

which is readily verified to be the correct exponent for the logarithm. One also finds that the leading constant equals the conditionally convergent product

$$
C_{\mathrm{lead}} = \prod_{\substack{p \equiv 1 \bmod \ell \\ \gcd(p,M)=1}} \left(1 + \frac{\sum_{\substack{a \in B-\{0\} \\ p \bmod M \in H_a}} 1 + \sum_{\substack{a \in A-B \\ p \bmod M \in H_a}} 1/\ell^m}{p}\right) \cdot \prod_p \left(1 - \frac{1}{p}\right)^\alpha
$$
$$
\cdot \left(\prod_{p|M'} \frac{|g(p)|}{\ell^n}\right) \cdot \frac{1}{\Gamma(\alpha)} \cdot \left(\sum_{\substack{(d_a)_{a \in A-\{0\}} \\ d_a|\ell \\ \gcd(d_a,M)=1}} \frac{\mu^2\left(\prod_{a \in A-\{0\}} d_a\right)}{\prod_{a \in A-\{0\}} d_a^2}\right).
$$

In particular, if $\ell > 2$, we always have $C_{\mathrm{lead}} > 0$. It is also clear from the above expression that C_{lead} is uniformly bounded.

Let us now see how to modify the above argument for $\ell = 2$. In this case we apply Lemma 7.1 with

$$
Y = \{(a,b) \in \mathcal{I} : w_{a,b} \text{ large}\}.
$$

By construction of $N_{\mathrm{main}}(X)$ we have that:

- $|Y| \geq 2^n - |B|$ due to §8.1;
- $\langle a_1, b_2 \rangle + \langle a_2, b_1 \rangle = 0$ for all $(a_1, b_1), (a_2, b_2) \in Y$ due to §8.2.

1337

Lemma 7.1 yields

$$Y = \{(a, f(a)) : a \in \mathbb{F}_2^n\}$$

for some alternating map f. The case $B = \mathbb{F}_2^n$ is easy, so let us suppose that B is a proper subspace of $\mathbb{F}_2^n$. We now observe that for every $(a_1, b_1) \in \mathcal{I}$ with $b_1 \neq f(a_1)$ there exists some $(a, f(a)) \in Y$ such that

$$\langle a_1, f(a) \rangle + \langle a, b_1 \rangle \neq 0.$$

Indeed, take any $a \notin B$ such that $\langle a, f(a_1) - b_1 \rangle \neq 0$.

By §8.2 and by definition of $N_{\text{main}}(X)$, this forces $|w_{a,b}| \leq 2$ for all $(a, b) \in \mathcal{I} - Y$ and therefore $w_{a,b} \in \{-2, -1, 1, 2\}$ and thus $w_{a,b} = 1$ unless $b = \bullet$. We now analyze $N_{\text{main}}(X)$ by splitting over congruence conditions on $w_{a,f(a)}$ modulo $16M$ and the parity of the number of prime divisors p such that $p \bmod M$ lies in a given coset of G. Crucially, this fixes both

$$\prod_{j \in [n]} \prod_{p | w_{a_1, f(a_1)}} \delta_{a_1, p \bmod M, j, f}^{\pi_j(f(a_1))}$$

and

$$\prod_{p | M'} \left(\frac{1}{2^n} \sum_{\alpha \in g(p)} \sum_{\mathbf{x} \in \mathbb{F}_2^n} \prod_{j \in [n]} \psi_j(\text{Frob}_p)^{\pi_j(\mathbf{x})} \overline{\chi_j(\alpha)}^{\pi_j(\mathbf{x})} \right).$$

Therefore, using quadratic reciprocity and the values of c_a modulo 16 to also eliminate the terms of the form

$$\psi_{w_{a_2, b_2}, \ell, 1}(\text{Frob}_{w_{a_1, b_1}}) \psi_{w_{a_1, b_1}, \ell, 1}(\text{Frob}_{w_{a_2, b_2}}),$$

our main term $N_{\text{main}}(X)$ becomes

$$N_{\text{main}}(X) = \sum_f \sum_{(c_a)} \sum_{(e_{a, \lambda})} \sum_{\substack{(v_a)_{a \in B - \{0\}} \\ p | v_a \Rightarrow p \bmod M \in H_a}} \epsilon((c_a), (e_a)) \sum_{\substack{(w_{a, f(a)})_a \\ \mathbf{v} \in \mathcal{A} \\ \prod_a \Delta(|v_a|) \prod_a \Delta(|w_{a, f(a)}|) \leq X \\ v_a \equiv c_a \bmod 16M \\ \gcd(w_{a, f(a)}, M) = 1 \\ p | w_{a, f(a)} \Rightarrow p \bmod M \in H_a \\ \omega_\lambda(v_a) \equiv e_{a, \lambda} \bmod 2}} 2^{-m \sum_a \tilde{\omega}(w_{a, f(a)})},$$

where $\epsilon((c_a), (e_a))$ is a real number, bounded in absolute value by 1, depending only on c_a and e_a, where $\omega_\lambda(v_a)$ denotes the number of prime divisors p of v_a such that $p \bmod M$ is in the coset $\lambda + G$ and where the sum over f is over all alternating maps. We now detect the congruence condition $v_a \equiv c_a \bmod 16M$ using Dirichlet characters and the condition $\omega_\lambda(v_a) \equiv e_{a, \lambda} \bmod 2$ using

$$\tfrac{1}{2}\left(1 + (-1)^{e_{a, \lambda} + \omega_\lambda(v_a)}\right).$$

To finish the proof, we proceed as in the case $\ell = 2$ to get the asymptotic formula for $N_{\text{main}}(X)$ by several applications of Theorem 4.1.

Let us now check the final part of Theorem 5.2. It is still readily verified that C_{lead} is bounded in terms of n only. For the final part, one gets that $C_{\text{lead}} > 0$ by directly adapting the above argument for $\ell > 2$ (including the application of Siegel–Walfisz to get the main term for the

conditions on the primes p dividing M'), observing that

$$\delta^{\pi_j(f(a_1))}_{a_1, p \bmod M, j, f} = 1$$

and

$$\psi_{w_{a_2, b_2}, 2, 1}(\mathrm{Frob}_{w_{a_1, b_1}}) \psi_{w_{a_1, b_1}, 2, 1}(\mathrm{Frob}_{w_{a_2, b_2}}) = 1$$

under the assumptions of the final part of Theorem 5.2.

9. Explicit constants

In general, the leading constant in Theorem 1.2 is an infinite sum of Euler products, which is unlikely to be expressible in a simple fashion. However, in specific cases it is possible to write down an explicit description of the leading constant. In particular, for purely multicyclic extensions, since C_{lead} in Theorem 5.2 can be made explicit so can the leading constant in the count of extensions satisfying the weak approximation property. As a further example, in this section we will also compute the leading constant for $C_2 \times C_3 \times C_3$ as this is the smallest group A for which a positive proportion of fields, when ordered by discriminant, have the weak approximation property.

9.1 Multicyclic extensions

Before writing down the explicit asymptotic for the number of $\mathbb{F}_\ell^n$-extensions of $\mathbb{Q}$ whose norm one torus satisfies weak approximation, we start by explicitly enumerating the $\mathbb{F}_\ell^n$-extensions of bounded absolute discriminant, for the purpose of comparison. While the asymptotic formula, with an inexplicit constant, dates back to the work of Wright [Wri89], to the authors' knowledge, the only examples where the leading constant is explicitly known are following the cases:

– $\ell = 2$ (due independently to de la Bretèche, Kurlberg and Shparlinski [dlBKS21] and Fritsch [Fri19]),
– $\ell = 3$, $n = 2$ (due to Mammo [Mam10]),
– $n = 1$, for any prime ℓ over any base field (due to Cohen, Diaz-y-Diaz and Olivier [CDO02]).

For a survey of some of the results known about explicit constants in Malle's conjecture, see Cohen, Diaz-y-Diaz and Olivier [CDO06]. We restrict attention to the case $\ell > 2$, to avoid the additional complications of the oddest prime, and $n \geq 2$, since weak approximation always holds on the norm one torus of a cyclic extension. In this setting, every case of the following theorem but the simplest is new.

THEOREM 9.1. *Let $\ell > 2$ be a prime and $n > 0$ an integer. For a real number $X > 1$, denote by $N_{\ell, n}(X)$ the number of field extensions $K/\mathbb{Q}$ such that $\mathrm{Gal}(K/\mathbb{Q}) \cong \mathbb{F}_\ell^n$ and $\mathrm{Disc}(K/\mathbb{Q}) \leq X$. Then, as $X \to \infty$, we have*

$$N_{\ell, n}(X) = \frac{C}{\Gamma((\ell^n - 1)/(\ell - 1))} X^{1/(\ell^n - \ell^{n-1})} (\log X)^{(\ell^n - 1)/(\ell - 1) - 1}$$
$$+ O\big(X^{1/(\ell^n - \ell^{n-1})} (\log X)^{(\ell^n - 1)/(\ell - 1) - 2}\big),$$

where

$$C = \frac{1}{\prod_{i=0}^{n-1}(\ell^n - \ell^i)} \frac{(1 + (\ell^n - 1)/\ell^2)}{(\ell^n - \ell^{n-1})^{(\ell^n - 1)/(\ell - 1) - 1}} \prod_{p \equiv 1 \bmod \ell} \left(1 + \frac{\ell^n - 1}{p}\right) \prod_p \left(1 - \frac{1}{p}\right)^{(\ell^n - 1)/(\ell - 1)}.$$

1339

Remark. The authors are fairly confident that one could prove an asymptotic with an explicit degree $(\ell^n - 1)/(\ell - 1) - 1$ polynomial in $\log X$ and power-saving error term by replacing the application of Theorem 4.1 in the proof with a customised application of the Selberg–Delange approach (perhaps multidimensional in nature, as in [dlBKS21]).

Proof. To begin, we parametrise $\mathbb{F}_\ell^n$-extensions of $\mathbb{Q}$ as in §2. That is to say, each such extension corresponds to a tuple $(v_a)_{a \in \mathbb{F}_\ell^n - \{0\}}$, where the entries are squarefree and pairwise coprime. Furthermore, we stipulate that the v_a must satisfy:

– for all prime divisors p of v_a,

$$p \equiv 1 \mod \frac{\mathrm{ord}(a)}{p^{v_p(\mathrm{ord}(a))}};$$

– if $\mathrm{ord}(a) > 2$, then $v_a > 0$.

The latter condition forces each entry in the tuple to be positive, while the former requires each prime divisor of v_a which is not equal to ℓ to be congruent to 1 modulo ℓ. Finally, we observe that the discriminant of the field associated to such a tuple is given by

$$\begin{cases} \prod v_a^{\ell^n - \ell^{n-1}}, & \text{if } \ell \nmid v_a \text{ for all } a, \\ \ell^{2(\ell^n - \ell^{n-1})} \prod (v_a')^{\ell^n - \ell^{n-1}}, & \text{if } \exists a \text{ s.t. } \ell \mid v_a, \end{cases}$$

where $v_a' = v_a \ell^{-v_\ell(v_a)}$.

Note that the parametrisation just discussed does not parametrise $\mathbb{F}_\ell^n$-extensions of $\mathbb{Q}$ but rather homomorphisms from $G_\mathbb{Q}$ to $\mathbb{F}_\ell^n$. However, for each field there are several such homomorphisms. In order to correct this overcount, we need to divide by the size of the automorphism group of $\mathbb{F}_\ell^n$.

Hence, splitting up the two cases where $\ell \nmid \prod v_a$ and $\ell \mid \prod v_a$, we find that the count for $N_{\ell,n}(X)$ may be given by the sum

$$\frac{1}{|\mathrm{Aut}(\mathbb{F}_\ell^n)|} \left[\sum_{\substack{\mathbf{v} \in \mathbb{Z}_{>0}^{\ell^n - 1} \\ p|v_i \Rightarrow p \equiv 1 \bmod \ell \\ \gcd(v_i, 2\ell) = 1 \\ \prod_i v_i^{\ell^n - \ell^{n-1}} \leq X}} \mu^2\left(\prod_i v_i\right) + (\ell^n - 1) \sum_{\substack{\mathbf{v} \in \mathbb{Z}_{>0}^{\ell^n - 1} \\ p|v_i \Rightarrow p \equiv 1 \bmod \ell \\ \gcd(v_i, 2\ell) = 1 \\ \prod_i v_i^{\ell^n - \ell^{n-1}} \leq X/\ell^{2(\ell^n - \ell^{n-1})}}} \mu^2\left(\prod_i v_i\right) \right].$$

We can compute the size of the sums appearing here using Theorem 4.1. Indeed, for any V, we may write

$$\sum_{\substack{\mathbf{v} \in \mathbb{Z}_{>0}^{\ell^n - 1} \\ p|v_i \Rightarrow p \equiv 1 \bmod \ell \\ \gcd(v_i, 2\ell) = 1 \\ \prod_i v_i \leq V}} \mu^2\left(\prod_i v_i\right) = \sum_{\substack{v \in \mathbb{Z}_{>0} \\ v \leq V}} \mu^2(v) g(v),$$

where $g(v)$ is the $(\ell^n - 1)$-fold convolution of the indicator function $\mathbf{1}_{p|v \Rightarrow p \equiv 1 \bmod \ell}(v)$. Note that we have dropped the coprimality condition $\gcd(v_i, 2\ell) = 1$, since it is already implied by the constraint that prime divisors of v must be congruent to 1 mod ℓ. On primes, we can estimate

the sum

$$\sum_{p \le x} g(p) \log p = \sum_{p \le x} (\ell^n - 1) \mathbf{1}_{p|v \Rightarrow p \equiv 1 \bmod \ell}(v) \log p$$

$$= (\ell^n - 1) \sum_{\substack{p \le x \\ p \equiv 1 \bmod \ell}} \log p = \frac{\ell^n - 1}{\ell - 1} x + O_A\left(\frac{x}{(\log x)^A}\right)$$

by the classical Siegel–Walfisz theorem. Therefore, applying Theorem 4.1, we have

$$\sum_{\substack{v \in \mathbb{Z}_{>0} \\ v \le V}} \mu^2(v) g(v) = \frac{V(\log V)^{(\ell^n - 1)/(\ell - 1) - 1}}{\Gamma((\ell^n - 1)/(\ell - 1))} \prod_{p \equiv 1 \bmod \ell} \left(1 + \frac{\ell^n - 1}{p}\right) \prod_p \left(1 - \frac{1}{p}\right)^{(\ell^n - 1)/(\ell - 1)}$$

$$+ O\left(V(\log V)^{(\ell^n - 1)/(\ell - 1) - 2}\right).$$

Combining this with our previous expression for $N_{\ell,n}(X)$ completes the claim. $\qquad \square$

Remark. To compare with Mammo's result, set $\ell = 3$ and $n = 2$. Then the main term for $N_{3,2}(X)$ is given by

$$\frac{1}{(3^2 - 1)(3^2 - 3)}\left(1 + \frac{3^2 - 1}{3^2}\right) \frac{X^{1/6}(\log X)^3}{6^3 \Gamma(4)} \prod_{p \equiv 1 \bmod 3} \left(1 + \frac{8}{p}\right) \prod_p \left(1 - \frac{1}{p}\right)^4$$

$$= \frac{1}{48} \frac{17}{9} \frac{X^{1/6}(\log X)^3}{6^4}\left(\frac{2}{3}\right)^4 \prod_{p \equiv 1 \bmod 3} \left(1 + \frac{8}{p}\right)\left(1 - \frac{1}{p}\right)^4 \prod_{p \equiv 2 \bmod 3} \left(1 - \frac{1}{p}\right)^4.$$

This Euler product can be simplified by comparison with $L(1, \chi)^4$ for χ the non-principal Dirichlet character mod 3. Thus our leading constant becomes

$$\frac{17 X^{1/6}(\log X)^3}{2^4 3^{11}} L(1, \chi)^4 \prod_{p \equiv 1 \bmod 3} \left(1 + \frac{8}{p}\right)\left(1 - \frac{1}{p}\right)^8 \prod_{p \equiv 2 \bmod 3} \left(1 - \frac{1}{p^2}\right)^4.$$

By the analytic class number formula, $L(1, \chi) = 2\pi/6\sqrt{3}$. This means that we have

$$N_{3,2}(X) \sim \frac{17 \pi^4 X^{1/6}(\log X)^3}{2^4 3^{17}} \prod_{p \equiv 1 \bmod 3} \left(1 + \frac{8}{p}\right)\left(1 - \frac{1}{p}\right)^8 \prod_{p \equiv 2 \bmod 3} \left(1 - \frac{1}{p^2}\right)^4,$$

which recovers the result of [Mam10, § 7, Case 2]. Since the proof in [Mam10] relies on an application of the Ikehara–Delange Tauberian theorem, there is no error term given, so our result represents an improvement in that respect.

We now turn to the problem of weak approximation on the norm one torus. Our count will be provided by Theorem 5.2; however, many of the complications arising in the case of general abelian extensions are not necessary for multicyclic extensions. In particular, we may set $M = 1$, which makes the subgroups H_a trivial, and we have by definition that $d(\ell) = 1$. Note also that $m := n - 1 - \dim_{\mathbb{F}_\ell} B = n - 1$. Thus, by the work of the previous section in concluding the proof of Theorem 5.2, the number of $\mathbb{F}_\ell^n$-extensions of $\mathbb{Q}$ with absolute discriminant at most X whose norm one torus satisfies weak approximation is equal to

$$\frac{1}{\prod_{i=0}^{n-1}(\ell^n - \ell^i)} C_{\text{lead}} X^{1/(\ell^n - \ell^{n-1})} \log(X^{1/(\ell^n - \ell^{n-1})})^{\alpha - 1} + O\left(X^{1/(\ell^n - \ell^{n-1})}(\log X)^{\alpha - 1 - \delta}\right)$$

for some $\delta > 0$, where

$$C_{\text{lead}} = \prod_{p \equiv 1 \bmod \ell} \left(1 + \frac{\sum_{a \in \mathbb{F}_\ell^n - \{0\}} \ell^{-n}}{p} \right) \prod_p \left(1 - \frac{1}{p} \right)^\alpha \frac{1}{\Gamma(\alpha)} \left(\sum_{\substack{(d_a)_{a \in \mathbb{F}_\ell^n - \{0\}} \\ d_a | \ell}} \frac{\mu^2(\prod_a d_a)}{\prod_a d_a^2} \right),$$

$$\alpha = 0 + \frac{1}{\ell^{n-1}} \sum_{a \in \mathbb{F}_\ell^n - \{0\}} \frac{1}{\varphi(\ell)} \sum_{\lambda \in (\mathbb{Z}/\ell\mathbb{Z})^*} \mathbf{1}_{\lambda \equiv 1 \bmod \ell} = \frac{\ell^n - 1}{\ell^{n-1}(\ell - 1)}.$$

We observe that, as in the proof of Theorem 9.1, we have divided by a factor of $|\text{Aut}(\mathbb{F}_\ell^n)| = \prod_{i=0}^{n-1}(\ell^n - \ell^i)$. Using the fact that

$$\left(\sum_{\substack{(d_a)_{a \in \mathbb{F}_\ell^n - \{0\}} \\ d_a | \ell}} \frac{\mu^2(\prod_a d_a)}{\prod_a d_a^2} \right) = 1 + \frac{\ell^n - 1}{\ell^2},$$

the main term becomes

$$\frac{X^{1/(\ell^n - \ell^{n-1})}(\log X)^{(\ell^n - 1)/(\ell^{n-1}(\ell-1)) - 1}}{\Gamma((\ell^n - 1)/(\ell^{n-1}(\ell - 1)))} \frac{(1 + (\ell^n - 1)/\ell^2)}{(\ell^n - \ell^{n-1})^{(\ell^n - 1)/(\ell^{n-1}(\ell-1)) - 1} \prod_{i=0}^{n-1}(\ell^n - \ell^i)}$$

$$\times \prod_{p \equiv 1 \bmod \ell} \left(1 + \frac{\ell^n - 1}{\ell^{n-1} p} \right) \prod_p \left(1 - \frac{1}{p} \right)^{(\ell^n - 1)/(\ell^{n-1}(\ell-1))}$$

as desired.

9.2 A positive proportion of fields satisfying weak approximation

In order to parametrise $A = (C_2 \times C_3 \times C_3)$-extensions, using the method of §2, we need a 17-tuple of squarefree, pairwise coprime integers. The tuple is indexed by the non-identity elements of $C_2 \times C_3 \times C_3$ and hence we will write the tuple as $(u_1, \ldots, u_8, v_1, \ldots, v_8, w)$ where the u_i are those components indexed by elements of order 3 in $C_2 \times C_3 \times C_3$, the v_i are those components indexed by elements of order 6, and w is the component indexed by the order two element. The u_i and v_i must be positive, but w can be either positive or negative. To complete the parametrisation we must impose the further conditions that:

– $p \mid u_i \Rightarrow p \equiv 0, 1 \bmod 3$;
– $p \mid v_i \Rightarrow p \equiv 1, 3 \bmod 6$.

The proof will proceed by fixing the u_i and v_i and thus determining a $(C_3 \times C_3)$-extension F of small discriminant, after which we will vary w. To ensure that the extension $K/\mathbb{Q}$ is such that the norm one torus satisfies weak approximation we must turn to the criteria in §3. The subset $2A \cap A[2]$ contains only the identity and therefore, by Theorem 3.4, once the u_i and v_i are chosen, there is no additional condition on w. In other words, $R_{K/\mathbb{Q}}^1 \mathbb{G}_m$ satisfies weak approximation if and only if $R_{F/\mathbb{Q}}^1 \mathbb{G}_m$ does. Hence, in the general setup in §5, we can take H_a to be the full group $(\mathbb{Z}/M\mathbb{Z})^*$. This means that in order to compute $A = (C_2 \times C_3 \times C_3)$-extensions of bounded absolute discriminant satisfying the weak approximation condition, we must consider

sums of the form

$$\sum_{\substack{\mathbf{u},\mathbf{v}\in\mathbb{Z}_{>0}^8 \\ \mathrm{Par}(\mathbf{u},\mathbf{v})\text{ satisfies WA} \\ \mathrm{disc}(\mathrm{Par}(\mathbf{u},\mathbf{v}))\leq(\log X)^{100} \\ p|u_i\Rightarrow p\equiv 0,1 \bmod 3 \\ p|v_i\Rightarrow p\equiv 1,3 \bmod 6}} \quad \sum_{\substack{w\in\mathbb{Z}_{\neq 0} \\ \mathrm{disc}(\mathrm{Par}(\mathbf{u},\mathbf{v},w))\leq X}} \mu^2\Big(w\prod_i u_i\prod_j v_j\Big).$$

Next, we describe the discriminant of the extension $K/\mathbb{Q}$. We observe that the valuation of the discriminant at the primes 3 and p for p any prime greater than 3 are given by

$$v_3(\Delta_{K/\mathbb{Q}}) = \begin{cases} 0, & \text{if } 3\nmid u_1\cdots u_8 v_1\cdots v_8 w, \\ 9, & \text{if } p\mid w, \\ 24, & \text{if } p\mid u_i, \\ 27, & \text{if } p\mid v_i, \end{cases}$$

and

$$v_p(\Delta_{K/\mathbb{Q}}) = \begin{cases} 0, & \text{if } p\nmid u_1\cdots u_8 v_1\cdots v_8 w, \\ 9, & \text{if } p\mid w, \\ 12, & \text{if } p\mid u_i, \\ 15, & \text{if } p\mid v_i. \end{cases}$$

Finally, at 2 (noting that 2 never ramifies in a $C_3\times C_3$-extension), we find that the discriminant has valuation

$$v_2(\Delta_{K/\mathbb{Q}}) = \begin{cases} 0, & \text{if } w\equiv 1 \bmod 4, \\ 18, & \text{if } w\equiv 3 \bmod 4, \\ 27, & \text{if } w\equiv 2 \bmod 4. \end{cases}$$

The innermost sum will be handled using the well-known estimate for odd d,

$$\sum_{\substack{\gcd(w,d)=1 \\ w\equiv a \bmod 4 \\ 0<w^9\leq W}} \mu^2(w) = \frac{3}{\pi^2}W^{1/9}\prod_{p|2d}\Big(1+\frac{1}{p}\Big)^{-1} + O\big(W^{1/18}\tau(d)\big). \tag{9.1}$$

To compute the count for A-extensions whose norm one torus satisfies weak approximation, we will consider four cases:

(i) $3\nmid u_1\cdots u_8 v_1\cdots v_8 w$;
(ii) there is some i such that $3\mid u_i$;
(iii) there is some i such that $3\mid v_i$;
(iv) $3\mid w$.

Note that these cases are both disjoint and exhaustive.

We start with case (i). In this case, the sum that has to be computed can be written as

$$\Sigma_1(X) := \sum_{\substack{\mathbf{u},\mathbf{v}\in\mathbb{Z}_{>0}^8 \\ \mathrm{Par}(\mathbf{u},\mathbf{v})\text{ satisfies WA} \\ \prod_i u_i^{12}\prod_j v_j^{15}\leq(\log X)^{100} \\ p|u_i\Rightarrow p\equiv 1 \bmod 3 \\ p|v_i\Rightarrow p\equiv 1 \bmod 6}} \quad \sum_{a\in\{1,2,3\}} \quad \sum_{\substack{w\in\mathbb{Z}_{\neq 0} \\ w\equiv a \bmod 4 \\ (c(a)|w|)^9\leq X/(\prod_i u_i^{12}\prod_j v_j^{15})}} \mu^2\Big(3w\prod_i u_i\prod_j v_j\Big),$$

1343

where $c(1) = 1, c(2) = 4$ and $c(3) = 4$. We can express this as

$$\Sigma_1(X) = \sum_{\substack{\mathbf{u},\mathbf{v}\in\mathbb{Z}_{>0}^8 \\ \mathrm{Par}(\mathbf{u},\mathbf{v})\ \mathrm{satisfies\ WA} \\ \prod_i u_i^{12}\prod_j v_j^{15}\leq(\log X)^{100} \\ p|u_i\Rightarrow p\equiv 1\bmod 3 \\ p|v_i\Rightarrow p\equiv 1\bmod 6}} \mu^2\left(\prod_i u_i \prod_j v_j\right) \sum_{a\in\{1,2,3\}} \sum_{\substack{w\in\mathbb{Z}_{\neq 0} \\ w\equiv a\bmod 4 \\ |w|\leq(c(a))^{-1}(X/(\prod_i u_i^{12}\prod_j v_j^{15}))^{1/9} \\ \gcd\left(w,3\prod_i u_i\prod_j v_j\right)=1}} \mu^2(w).$$

Applying (9.1) to the inner sums over a and w, we see that they are equal to

$$2\times\frac{3}{\pi^2}\left(\frac{X}{\prod_i u_i^{12}\prod_j v_j^{15}}\right)^{1/9}\left(1+\frac{1}{4}+\frac{1}{4}\right)\prod_{p|6\prod_i u_i\prod_j v_j}\left(1+\frac{1}{p}\right)^{-1} + O_\epsilon\left(\left(\frac{X}{\prod_i u_i^{12}\prod_j v_j^{15}}\right)^{1/18+\epsilon}\right).$$

Since the u_i and v_j all have log power size, this error term is negligible when summed over the remaining variables. Thus

$$\Sigma_1(X) \sim \frac{9}{\pi^2}X^{1/9}\sum_{\substack{\mathbf{u},\mathbf{v}\in\mathbb{Z}_{>0}^8 \\ \mathrm{Par}(\mathbf{u},\mathbf{v})\ \mathrm{satisfies\ WA} \\ p|u_i\Rightarrow p\equiv 1\bmod 3 \\ p|v_i\Rightarrow p\equiv 1\bmod 6}} \frac{\mu^2\left(\prod_i u_i\prod_j v_j\right)}{\prod_i u_i^{4/3}\prod_j v_j^{5/3}}\prod_{p|\prod_i u_i\prod_j v_j}\left(1+\frac{1}{p}\right)^{-1}.$$

Unfortunately, at this stage it seems that no further simplification is possible. The condition that $\mathrm{Par}(\mathbf{u},\mathbf{v})$ satisfies WA is not a multiplicative condition on the variables $\mathbf{u}$ and $\mathbf{v}$ and thus this convergent sum cannot be expressed as an Euler product. One could detect this condition using character sums as discussed in §6, but it is unclear that doing so will give a path towards writing the sum in any kind of simpler form. Henceforth, we will simply refer to this infinite sum as κ.

We now move to case (ii). Suppose that $3 \mid u_{i_0}$ and write $\widetilde{u}_i = u_i$ for all $i \neq i_0$ and $\widetilde{u}_{i_0} = u_{i_0}/3$. Then the sum which has to be computed is

$$\Sigma_2(X) := \sum_{\substack{\widetilde{\mathbf{u}},\mathbf{v}\in\mathbb{Z}_{>0}^8 \\ \mathrm{Par}(\mathbf{u},\mathbf{v})\ \mathrm{satisfies\ WA} \\ \prod_i \widetilde{u}_i^{12}\prod_j v_j^{15}\leq(\log X)^{100} \\ p|\widetilde{u}_i\Rightarrow p\equiv 1\bmod 3 \\ p|v_i\Rightarrow p\equiv 1\bmod 6}} \sum_{a\in\{1,2,3\}} \sum_{\substack{w\in\mathbb{Z}_{\neq 0} \\ w\equiv a\bmod 4 \\ (c(a)|w|)^9\leq X/3^{24}(\prod_i \widetilde{u}_i^{12}\prod_j v_j^{15})}} \mu^2\left(3w\prod_i\widetilde{u}_i\prod_j v_j\right).$$

Evidently, we have $\Sigma_2 = 3^{-24/9}\Sigma_1$. The argument in case (iii) is almost exactly the same. We find that the sum we need to compute in this setting, $\Sigma_3(X)$ satisfies $\Sigma_3 = 3^{-27/9}\Sigma_1$. Finally, in case (iv), write $\widetilde{w} = w/3$. Then we consider

$$\Sigma_4(X) := \sum_{\substack{\mathbf{u},\mathbf{v}\in\mathbb{Z}_{>0}^8 \\ \mathrm{Par}(\mathbf{u},\mathbf{v})\ \mathrm{satisfies\ WA} \\ \prod_i u_i^{12}\prod_j v_j^{15}\leq(\log X)^{100} \\ p|u_i\Rightarrow p\equiv 1\bmod 3 \\ p|v_i\Rightarrow p\equiv 1\bmod 6}} \sum_{a\in\{1,2,3\}} \sum_{\substack{\widetilde{w}\in\mathbb{Z}_{\neq 0} \\ \widetilde{w}\equiv a\bmod 4 \\ (c(a)|\widetilde{w}|)^9\leq X/3^9(\prod_i u_i^{12}\prod_j v_j^{15})}} \mu^2\left(3\widetilde{w}\prod_i u_i\prod_j v_j\right),$$

and thus $\Sigma_4 = 3^{-9/9}\Sigma_1$. Combining these, we have

$$\Sigma_1 + \Sigma_2 + \Sigma_3 + \Sigma_4 = \left(1+\frac{1}{3^{8/3}}+\frac{1}{81}+\frac{1}{3}\right)\Sigma_1(X)$$

1344

Just as in the last subsection, this sum counts each field extension multiple times and hence we must divide by the order of the automorphism group of $A = C_2 \times C_3 \times C_3$ which is 48.

Our work so far has lead us to the following result.

THEOREM 9.2. *The number of $(C_2 \times C_3 \times C_3)$-extensions $K/\mathbb{Q}$ with absolute discriminant less than or equal to X such that $R^1_{K/\mathbb{Q}}\mathbb{G}_m$ satisfies weak approximation is*

$$\frac{109 + 3\sqrt[3]{3}}{2^4 3^3 \pi^2} \kappa X^{1/9} + O_\epsilon\big(X^{1/18+\epsilon}\big).$$

We can compare this count to the number of A-extensions of bounded absolute discriminant which we compute in a fairly similar manner. The explicit value for the leading constant in the following asymptotic formula is new, as far as the authors are aware.

THEOREM 9.3. *The number of $(C_2 \times C_3 \times C_3)$-extensions $K/\mathbb{Q}$ with absolute discriminant less than or equal to X is*

$$\frac{109 + 3\sqrt[3]{3}}{2^4 3^3 \pi^2} X^{1/9} \prod_{p \equiv 1 \bmod 6} \left(1 + \frac{8}{p^{1/3}(p+1)} + \frac{8}{p^{2/3}(p+1)}\right) + O_\epsilon\left(X^{1/18+\epsilon}\right).$$

Proof. The proof follows exactly the same lines as the previous proof, but we no longer need to impose the condition that weak approximation holds in the $(C_3 \times C_3)$-extension. We will parametrise the extensions in the exact same way and similarly consider four cases depending on the ramification of the prime 3. In the first instance, when 3 does not ramify in the whole extension, we need to compute

$$\widetilde{\Sigma_1}(X) := \sum_{\substack{\mathbf{u},\mathbf{v} \in \mathbb{Z}^8_{>0} \\ \prod_i u_i^{12} \prod_j v_j^{15} \leq (\log X)^{100} \\ p|u_i \Rightarrow p \equiv 1 \bmod 3 \\ p|v_i \Rightarrow p \equiv 1 \bmod 6}} \mu^2\left(\prod_i u_i \prod_j v_j\right) \sum_{a \in \{1,2,3\}} \sum_{\substack{w \in \mathbb{Z}_{\neq 0} \\ w \equiv a \bmod 4 \\ |w| \leq (c(a))^{-1}(X/(\prod_i u_i^{12} \prod_j v_j^{15}))^{1/9} \\ \gcd\left(w, 3\prod_i u_i \prod_j v_j\right)=1}} \mu^2(w).$$

Thus, similarly, we have

$$\widetilde{\Sigma_1}(X) = \frac{9}{\pi^2} X^{1/9} \sum_{\substack{\mathbf{u},\mathbf{v} \in \mathbb{Z}^8_{>0} \\ p|u_i \Rightarrow p \equiv 1 \bmod 3 \\ p|v_i \Rightarrow p \equiv 1 \bmod 6}} \frac{\mu^2\left(\prod_i u_i \prod_j v_j\right)}{\prod_i u_i^{4/3} \prod_j v_j^{5/3}} \prod_{p|\prod_i u_i \prod_j v_j} \left(1 + \frac{1}{p}\right)^{-1} + O_\epsilon\left(X^{1/18+\epsilon}\right)$$

We can express the remaining convergent sum as an Euler product so that

$$\widetilde{\Sigma_1}(X) \sim \frac{9}{\pi^2} X^{1/9} \prod_{p \equiv 1 \bmod 6} \left(1 + 8\frac{1}{p^{1/3}(p+1)} + 8\frac{1}{p^{2/3}(p+1)}\right).$$

The proof now follows exactly the same lines as the previous theorem to conclude. $\square$

Observe that, as we expect, the order of magnitude of these two counts is the same. Therefore, we can combine these results to establish the precise (positive) proportion of A-extensions whose norm one torus satisfies weak approximation.

Corollary 9.4. *The proportion of $(C_2 \times C_3 \times C_3)$-extensions of $\mathbb{Q}$ whose norm one tori satisfy weak approximation is*

$$\kappa \prod_{p \equiv 1 \bmod 6} \left(1 + \frac{8}{p^{1/3}(p+1)} + \frac{8}{p^{2/3}(p+1)} \right)^{-1}.$$

As discussed in §1.1, since we have $H^3(C_2 \times C_3 \times C_3, \mathbb{Z}) \cong C_3$, weak approximation is satisfied if and only if the Hasse norm principle fails. Therefore, we are able to determine the precise proportion of Hasse norm principle failures in this setting as well.

Corollary 9.5. *The proportion of $(C_2 \times C_3 \times C_3)$-extensions of $\mathbb{Q}$ which fail the Hasse norm principle is*

$$\kappa \prod_{p \equiv 1 \bmod 6} \left(1 + \frac{8}{p^{1/3}(p+1)} + \frac{8}{p^{2/3}(p+1)} \right)^{-1}.$$

Conflicts of Interest
None.

References

ASVW21   S. A. Altuğ, A. Shankar, I. Varma and K. H. Wilson, *The number of D_4-fields ordered by conductor*, J. Eur. Math. Soc. **23** (2021), 2733–2785.

Bar81   H.-J. Bartels, *Zur Arithmetik von Diedergruppenerweiterungen*, Math. Ann. **256** (1981), 465–473.

Bha05   M. Bhargava, *The density of discriminants of quartic rings and fields*, Ann. of Math. **162** (2005), 1031–1063.

Bha10   M. Bhargava, *The density of discriminants of quintic rings and fields*, Ann. of Math. **172** (2010), 1559–1591.

BGL14   V. Blomer, L. Goldmakher and B. Louvel, *L-functions with n-th-order twists*, Int. Math. Res. Not. IMRN **2014** (2014), 1925–1955.

CDO02   H. Cohen, F. Diaz-y-Diaz and M. Olivier, *On the density of discriminants of cyclic extensions of prime degree*, J. Reine Angew. Math. **550** (2002), 169–209.

CDO06   H. Cohen, F. Diaz-y-Diaz and M. Olivier, *Counting discriminants of number fields*, J. Théor. Nombres Bordeaux **18** (2006), 573–593.

DY22   R. Darda and T. Yasuda, *The Batyrev-Manin conjecture for DM stacks*, Preprint (2022), arXiv:2207.03645.

dlBKS21 R. de la Bretèche, P. Kurlberg and I. Shparlinski, *On the number of products which form perfect powers and discriminants of multiquadratic extensions*, Int. Math. Res. Not. IMRN **2021** (2021), 17140–17169.

ESZ23   J. Ellenberg, M. Satriano and D. Zureick-Brown, *Heights on stacks and a generalized Batyrev–Manin–Malle conjecture*, Forum Math. Sigma **11** (2023), Paper No. e14.

FK07   E. Fouvry and J. Klüners, *On the 4-rank of class groups of quadratic number fields*, Invent. Math. **167** (2007), 455–513.

FLN18   C. Frei, D. Loughran and R. Newton, *The Hasse norm principle for abelian extensions*, Amer. J. Math. **140** (2018), 1639–1685.

FLN22   C. Frei, D. Loughran and R. Newton, *Number fields with prescribed norms*, Comment. Math. Helv. **97** (2022), 133–181.

Fri19   R. Fritsch, *Counting multi-quadratic number fields of bounded discriminant*, Preprint (2019), arXiv:1902.03202.

GL13   L. Goldmakher and B. Louvel, *A quadratic large sieve inequality over number fields*, Math. Proc. Cambridge Philos. Soc. **154** (2013), 193–212.

Gol70   L. J. Goldstein, *A generalization of the Siegel–Walfisz theorem*, Trans. Amer. Math. Soc. **149** (1970), 417–429.

GK19   A. Granville and D. Koukoulopoulos, *Beyond the LSD method for the partial sums of multiplicative functions*, Ramanujan J. **49** (2019), 287–319.

Hea95   D. R. Heath-Brown, *A mean value estimate for real character sums*, Acta Arith. **72** (1995), 235–275.

Kou19   D. Koukoulopoulos, *The distribution of prime numbers*, Graduate Studies in Mathematics, vol. 203 (American Mathematical Society, Providence, RI, 2019).

KM19   P. Koymans and D. Z. Milovic, *On the 16-rank of class groups of $\mathbb{Q}(\sqrt{-2p})$ for primes $p \equiv 1 \bmod 4$*, Int. Math. Res. Not. IMRN **2019** (2019), 7406–7427.

KP23   P. Koymans and C. Pagano, *On Malle's conjecture for nilpotent groups, I*, Trans. Amer. Math. Soc. Ser. B **10** (2023), 310–354.

KR23   P. Koymans and N. Rome, *A note on the Hasse norm principle*, Bull. Lond. Math. Soc., to appear. Preprint (2023), arXiv:2301.10136.

Mac21   A. Macedo, *Local-global principles for norms*, PhD thesis, University of Reading (2021), https://drive.google.com/file/d/1hx4YUd_FjOxpoYqTxwo7iTKjr-TL6CGl/view.

MN22   A. Macedo and R. Newton, *Explicit methods for the Hasse norm principle and applications to A_n and S_n extensions*, Math. Proc. Cambridge Philos. Soc. **172** (2022), 489–529.

Mam10   B. Mammo, *On the density of discriminants of abelian extensions of a number field*, Int. J. Number Theory **6** (2010), 1273–1291.

Mon22   S. Monnet, *S_4-quartics with prescribed norms*, Preprint (2022), arXiv:2210.06992.

Rom18   N. Rome, *The Hasse norm principle for biquadratic extensions*, J. Théor. Nombres Bordeaux **30** (2018), 947–964.

San81   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.

Vos70   V. E. Voskresenskiĭ, *Birational properties of linear algebraic groups*, Izv. Akad. Nauk SSSR Ser. Mat. **34** (1970), 3–19.

Vos89   V. E. Voskresenskiĭ, *Maximal tori without affect in semisimple algebraic groups*, Mat. Zametki **44** (1988), 309–318; English transl. in *Math. Notes* **44** (1989), 651–655.

Woo10   M. M. Wood, *On the probabilities of local behaviors in abelian field extensions*, Compos. Math. **146** (2010), 102–128.

Wri89   D. J. Wright, *Distribution of discriminants of abelian extensions*, Proc. London Math. Soc. (3) **58** (1989), 17–50.

P. Koymans   peter.koymans@eth-its.ethz.ch

Institute for Theoretical Studies, ETH Zurich, 8006 Zurich, Switzerland

N. Rome   rome@tugraz.at

Graz University of Technology, Institute of Analysis and Number Theory,
Kopernikusgasse 24/II, 8010 Graz, Austria