EFFECTIVE EQUIDISTRIBUTION OF NORM ONE ELEMENTS IN CM-FIELDS

SHABNAM AKHTARI, JEFFREY D. VAALER, AND MARTIN WIDMER

ABSTRACT. For a number field K let $\mathcal{S}_K$ be the maximal subgroup of the multiplicative group $K^\times$ that embeds into the unit circle under each embedding of K into the complex numbers. The group $\mathcal{S}_K$ can be seen as an archimedean counterpart to the group of units $\mathcal{O}_K^\times$ of the ring of integers $\mathcal{O}_K$. If $K = \mathbb{Q}(\mathcal{S}_K)$ is a CM-field then $\mathcal{S}_K/\mathrm{Tor}(K^\times)$ is a free abelian group of infinite rank. If $K = \mathbb{Q}(\mathcal{S}_K)$ is not a CM-field then $\mathcal{S}_K = \{\pm 1\}$. In the former case $\mathcal{S}_K$ is the kernel of the relative norm map from $K^\times$ to the multiplicative subgroup $k^\times$ of the maximal totally real subfield k of K.

We prove an effective equidistribution result for the elements of $\mathcal{S}_K$ embedded into the complex unit circle and enumerated by the Weil height. Our result also includes a specific rate of convergence.

For imaginary quadratic fields an ineffective version of the equidistribution result has been proven by Petersen and Sinclair.

1. INTRODUCTION

Let K be a number field. We choose a representative $|\cdot|_v$ for each place v of K and write $v|\infty$ if v is archimedean and $v \nmid \infty$ if v is non-archimedean. The torsion subgroup of the ring of integers $\mathcal{O}_K$ consists of all roots of unity in $K^\times$, and is given by

$$\mathrm{Tor}(K^\times) = \{\alpha \in K^\times ; |\alpha|_v = 1 \ \text{ for all } v\}.$$

The group of units of the ring of integers $\mathcal{O}_K$ is

$$\mathcal{O}_K^\times = \{\alpha \in K^\times ; |\alpha|_v = 1 \ \text{ for all } v \text{ such that } v \nmid \infty\}.$$

In this article we study its "archimedean counterpart" defined by

$$\mathcal{S}_K = \{\alpha \in K^\times ; |\alpha|_v = 1 \ \text{ for all } v \text{ such that } v|\infty\}.$$

It is clear that $\mathcal{S}_K$ is also a subgroup of the multiplicative group $K^\times$ and that

$$\{\pm 1\} \subseteq \mathrm{Tor}(K^\times) = \mathcal{S}_K \cap \mathcal{O}_K^\times. \tag{1.1}$$

Our main result is concerned with the distribution of elements in $\mathcal{S}_K$ when enumerated by the Weil height.

But first let us clarify the basic structure of the group $\mathcal{S}_K$ and its connection to CM-fields. Recall that a number field K is a CM-field if it is totally complex and contains a totally real subfield k of index 2.

2020 *Mathematics Subject Classification.* 11R06, 11R21, 11G50, 11D45.

Key words and phrases. CM-fields, equidistribution, norm one, counting, Weil height, Hilbert 90.

Proposition 1.1. *Let K be a number field, and let $\mathbb{Q}(\mathcal{S}_K)$ be the intersection of all subfields of K that contain $\mathcal{S}_K$. If $\mathbb{Q}(\mathcal{S}_K)$ is not a CM-field then $\mathcal{S}_K = \{\pm 1\}$. If $\mathbb{Q}(\mathcal{S}_K)$ is a CM-field then $\mathcal{S}_K/\mathrm{Tor}(K^\times)$ is a free abelian group of countably infinite rank.*

Obviously we have $\mathcal{S}_{\mathbb{Q}(\mathcal{S}_K)} = \mathcal{S}_K$ for each number field K. For the purposes of studying the group $\mathcal{S}_K$ we can and will therefore assume that K is a CM-field, and we write k for its maximal totally real subfield.

The norm map $N_{K/k} : K^\times \to k^\times$ is a homomorphism of groups and it is closely related to the group $\mathcal{S}_K$ via the following proposition. The proof follows easily from a characterisation of CM-fields due to Shimura, and stated here as Proposition 2.1.

Proposition 1.2. *Let K be a CM-field, and let k be its maximal totally real subfield. Then $\mathcal{S}_K$ is the kernel of the norm map $N_{K/k} : K^\times \to k^\times$.*

We now describe our main result. In short, it provides the asymptotics, and a power saving error term, for the number of elements in $\mathcal{S}_K$ with bounded height whose embeddings lie in given arcs of the unit circle in $\mathbb{C}$.

Let $2N$ be the degree of the CM-field K, and recall that k is its maximal totally real subfield. For $1 \le n \le N$ let σ_n, σ_{n+N} be the N pairs of complex conjugate embeddings of K into $\mathbb{C}$, so that

$$\mathcal{S}_K = \{\alpha \in K; |\sigma_n(\alpha)| = 1 \ \text{ for } 1 \le n \le N\}.$$

For a non-zero complex number x we write $\arg(x)$ for the unique argument of x in $[0, 2\pi)$, so that $x = |x|e^{i\arg(x)}$. For a product of intervals $\mathcal{I} = \mathcal{I}_1 \times \cdots \times \mathcal{I}_N$ with each interval $\mathcal{I}_j \subseteq [0, 2\pi)$ we define

$$\mathcal{S}_K(\mathcal{I}) = \{\alpha \in \mathcal{S}_K; (\arg(\sigma_n(\alpha)))_n \in \mathcal{I}\},$$

and we write $|\mathcal{I}|$ for the product of the lengths of the intervals $\mathcal{I}_1, \dots, \mathcal{I}_N$.

For each place v of K we choose the unique representative $|\cdot|_v$ that either extends the usual archimedean absolute value or one of the usual p-adic absolute values on $\mathbb{Q}$, and we write $[K_v : \mathbb{Q}_v]$ for the local degree at v. Let

$$H(\alpha) = \prod_v \max\{1, |\alpha|_v\}^{\frac{[K_v:\mathbb{Q}_v]}{[K:\mathbb{Q}]}}$$

denote the absolute (multiplicative) Weil height on K. We refer the reader to [4, Section 1.5] for more details on the Weil height. For $\mathcal{H} \ge 1$ we define

$$\mathcal{S}_K(\mathcal{I}, \mathcal{H}) = \{\alpha \in \mathcal{S}_K(\mathcal{I}); H(\alpha) \le \mathcal{H}\}. \tag{1.2}$$

We set

$$A_K = \left(\prod_{P | D_{K/k}} \frac{2N_{k/\mathbb{Q}}(P)}{N_{k/\mathbb{Q}}(P) + 1}\right) \frac{1}{\sqrt{N_{k/\mathbb{Q}}(D_{K/k})}} \frac{h_k R_k}{\omega_k \zeta_k(2) |\Delta_k|}, \tag{1.3}$$

where the product[1] runs over all prime ideals P of $\mathcal{O}_k$ dividing the relative discriminant $D_{K/k}$ of K/k, and $N_{k/\mathbb{Q}}(P) = [\mathcal{O}_k : P]$ denotes the (absolute) norm of the ideal P, h_k denotes the class number, R_k is the regulator, $\omega_k = 2$ is the number of roots of unity, and Δ_k is the discriminant of k.

We are now in position to state the main result.

[1] As usual, the empty product is interpreted as 1.

Theorem 1.1. *Let K be a CM-field of degree $2N$. There exists $C_K > 0$, depending only on K, such that for every $\mathcal{H} \geq 2$ we have*

$$\left| \#\mathcal{S}_K(\mathcal{I}, \mathcal{H}) - A_K |\mathcal{I}| \mathcal{H}^{2N} \right| \leq C_K \mathcal{H}^{2N-1} \mathcal{L}, \tag{1.4}$$

where $\mathcal{L}$ is defined to be $\log \mathcal{H}$ if $N = 1$ and 1 if $N \geq 2$.

The simplest CM-field is $K = \mathbb{Q}(i) \subseteq \mathbb{C}$. Let $\alpha = a/c + ib/c$ with $\gcd(a, b, c) = 1$ and $c > 0$. Now $\alpha \in \mathcal{S}_K$ means $a^2 + b^2 = c^2$ and it easily follows that $H(\alpha) = \sqrt{c}$. Hence, $\#\mathcal{S}_K(\mathcal{I}, \mathcal{H}) \sim (2/\pi^2)|\mathcal{I}|\mathcal{H}^2$ counts the number of primitive Pythagorean triples (a, b, c) with $0 < c \leq \mathcal{H}^2$ and $\alpha = a/c + ib/c \in \exp(i\mathcal{I})$.

Taking $\mathcal{I} = [0, 2\pi)^N$ the function $\#\mathcal{S}_K(\mathcal{I}, \mathcal{H})$ counts all elements of $\mathcal{S}_K$ of height at most $\mathcal{H}$. To simplify the notation let us write $\mathcal{S}_K(\mathcal{H}) = \{\alpha \in \mathcal{S}_K; H(\alpha) \leq \mathcal{H}\}$.

Corollary 1.1. *Let K be a CM-field of degree $2N$. There exists $C_K > 0$, depending only on K, such that for every $\mathcal{H} \geq 2$ we have*

$$\left| \#\mathcal{S}_K(\mathcal{H}) - A_K (2\pi)^N \mathcal{H}^{2N} \right| \leq C_K \mathcal{H}^{2N-1} \mathcal{L},$$

where A_K and $\mathcal{L}$ are as in Theorem 1.1.

The main term in Corollary 1.1 could possibly be derived from work of Batyrev and Tschinkel ([2, Corollary 4.7] or even its precursor [1]). However, this would require some effort. While very general, the methods from [2] do not provide effective results. To obtain an explicit power saving error term we develop another method, more in the spirit of [8], which we explain at the end of this section.

Next we consider the discrepancy

$$D_{\mathcal{H}}(\mathcal{S}_K) = \sup_{\mathcal{I}} \left| \frac{\#\mathcal{S}_K(\mathcal{I}, \mathcal{H})}{\#\mathcal{S}_K(\mathcal{H})} - \frac{|\mathcal{I}|}{(2\pi)^N} \right| \subseteq [0, 1],$$

where the supremum is taken over all products of intervals

$$\mathcal{I} = \mathcal{I}_1 \times \cdots \times \mathcal{I}_N \subseteq [0, 2\pi)^N.$$

Let $\sigma_1, \ldots, \sigma_N$ be the complete collection of independent embeddings of K. Theorem 1.1 implies not only that the points of $\mathcal{S}_K$ are simultaneously and independently equidistributed on the unit circle under these embeddings (when enumerated by the Weil height) but we also get a an explicit upper bound on the discrepancy (at least up to the constant C'_K).

Corollary 1.2. *Let K and $\mathcal{L}$ be as in Theorem 1.1. There exists $C'_K > 0$ such that for $\mathcal{H} \geq 2$ we have*

$$D_{\mathcal{H}}(\mathcal{S}_K) \leq C'_K \frac{\mathcal{L}}{\mathcal{H}}. \tag{1.5}$$

A precursor of Corollary 1.2 was proven in 2011 by Petersen and Sinclair [9, Theorem 2.1] in the case of imaginary quadratic fields K. It is conceivable that equidistribution can be deduced for arbitrary CM-fields by combining an observation of Peyre [10, Proposition 5.0.1] with the aforementioned work of Batyrev and Tschinkel [2]. However, neither Batyrev, Tschinkel and Peyre's nor Petersen and Sinclair's work yields an effective equidistribution result. Petersen and Sinclair's work is analytic in nature and uses Weyl's equidistribution criterion, the

Wiener-Ikehara Tauberian Theorem, and properties of Hecke L-functions. Our approach is quite different and the basic strategy is explained at the end of this section.

It is worthwhile to note that equidistribution fails if we consider many quadratic CM-fields simultaneously. Let us consider the set of all rational and all imaginary quadratic points on the unit circle

$$\mathcal{S}_2 = \bigcup_K \mathcal{S}_K,$$

where the union is taken over all imaginary quadratic fields K (here we consider each K as subfield of $\mathbb{C}$), and set

$$\mathcal{S}_2(\mathcal{I}, \mathcal{H}) = \{e^{i\theta} \in \mathcal{S}_2; \theta \in \mathcal{I}, H(e^{i\theta}) \leq \mathcal{H}\} = \bigcup_K \mathcal{S}_K(\mathcal{I}, \mathcal{H}).$$

If $\mathcal{I} \subseteq (\pi, 2\pi)$ then $\#\mathcal{S}_2(\mathcal{I}, \mathcal{H}) = \#\mathcal{S}_2(\mathcal{I} - \pi, \mathcal{H})$ as $H(\alpha) = H(-\alpha)$. Therefore, it suffices to consider the case $\mathcal{I} \subseteq [0, \pi]$. A point $e^{i\theta} \neq \pm 1$ on the unit circle is imaginary quadratic if and only if $\cos(\theta) = -b/2a$, for coprime integers $a > 0, b$. In this case the minimal polynomial is

$$f(x) = ax^2 - 2a\cos(\theta)x + a = ax^2 + bx + a \in \mathbb{Z}[x]$$

and $H(e^{i\theta}) = \sqrt{a}$ (see [4, Propositions 1.6.5 and 1.6.6]). Writing $|\cos(\mathcal{I})|$ for the length of the interval $\cos(\mathcal{I})$, we get

$$\#\mathcal{S}_2(\mathcal{I}, \mathcal{H}) = O(1) + \sum_{a=1}^{\mathcal{H}^2} \sum_{\substack{b \in -2a\cos(\mathcal{I}) \\ (a,b)=1}} 1 = \frac{|\cos(\mathcal{I})|}{\zeta(2)} \mathcal{H}^4 + O(\mathcal{H}^2 \log \mathcal{H}).$$

In particular, $\mathcal{S}_2$ is not equidistributed on the unit circle, when ordered by the Weil height $H(\cdot)$.

We conclude this section with a brief overview of the remaining sections. In Section 2 we recall some basic facts about CM-fields, and we deduce the first part of Proposition 1.1 and Proposition 1.2.

It follows from Proposition 1.2 that Hilbert's Theorem 90 provides a surjective group homomorphism $\psi : K^\times \to \mathcal{S}_K$ with kernel $k^\times$. In Section 3 we use this, in conjunction with results of Brandis [5], Lawrence [7], Steprāns [13], and Zorzitto [16], to deduce that $\mathcal{S}_K/\mathrm{Tor}(K^\times)$ is a free abelian group of (countably) infinite rank, proving the second part of Proposition 1.1.

Sections 4-7 are preparations for the proof of Theorem 1.1. Section 4 provides the counting principle Lemma 4.2 based on geometry of numbers to count lattice points. In Section 5 we introduce the counting domain, and we prove that it satisfies the technical conditions needed to apply Lemma 4.2.

Section 6 can be seen as the core of the proof. The homomorphism ψ induces an isomorphism $\hat{\psi} : K^\times/k^\times \to \mathcal{S}_K$. Therefore we need to construct a suitable fundamental domain of $K^\times$ under the action of $k^\times$. "Suitable" means that the height bound cuts out a subset that is accessible to our counting techniques. All this is done in detail in Section 6 and (modulo minor modifications) this part is applicable to counting elements of bounded height in the kernel of the norm map for any quadratic extension K/k of number fields.

The next step is to transform the counting problem to an ordinary lattice point counting problem, and this is carried out in Section 7. We then have all in place to finalise the proof of Theorem 1.1, which is done in Section 8.

In the final section we consider the quotient group $K^\times/k^\times$. We show that if a coset $k^\times$ in $K^\times$ intersects $\mathcal{S}_K$ then the minimal height of all elements in that coset is the height of the elements that lie in $\mathcal{S}_K$ (clearly they all have equal height). More generally we show that this holds true whenever K/k is a quadratic extension and $\mathcal{S}_K$ is the kernel of the norm map $N_{K/k} : K^\times \to k^\times$. Furthermore, we show that the cosets that intersect $\mathcal{S}_K$ are precisely the images of the squares in $\mathcal{S}_K$ under the inverse map of the isomorphism $\hat{\psi}$.

ACKNOWLEDGEMENTS

The authors thank the referee for helpful comments. Parts of this work were done during a Summer Collaborators Program at the Institute for Advanced Study in Princeton in 2024. The authors gratefully acknowledge support from the IAS.

M.W. would like to thank Tim Browning, Christopher Frei, Daniel Loughran, Nick Rome, and Tim Santens for helpful discussions and additional references.

2. BASICS ON CM-FIELDS

Let $\rho : \mathbb{C} \to \mathbb{C}$ be the complex conjugation. A basic observation made already by Shimura [11, 18.2. Lemma (i)] is the following very useful characterisation of CM-fields.

Lemma 2.1 (Shimura)**.** *A number field K is a CM-field if and only if there exists a non-trivial automorphism τ of K such that $\sigma \circ \tau = \rho \circ \sigma$ for all homomorphisms $\sigma : K \to \mathbb{C}$.*

If K is a CM-field and k its maximal totally real subfield then the automorphism τ from Lemma 2.1 satisfies

$$\tau = \sigma^{-1} \circ \rho \circ \sigma \tag{2.6}$$

for every homomorphisms $\sigma : K \to \mathbb{C}$, and it is a non-trivial automorphism of K fixing k (we drop $\circ$ and simply write $\sigma^{-1}\rho\sigma$). Consequently, τ is the unique non-trivial element of $\mathrm{Gal}(K/k)$, and

$$\mathrm{Gal}(K/k) = \langle \tau \rangle. \tag{2.7}$$

Shimura [11, 18.2. Lemma (ii)] also observed that Lemma 2.1 implies the following result.

Lemma 2.2 (Shimura)**.** *The composite field of finitely many CM-fields is also a CM-field.*

Blanksby and Loxton [3, Theorem 1] proved a characterisation of CM-fields that connects them to the group $\mathcal{S}_K$.

Theorem 2.1 (Blanksby, Loxton)**.** *Let K be a number field of degree $d > 1$. Then K is a CM-field if and only if $K = \mathbb{Q}(\alpha)$ for some $\alpha \in \mathcal{S}_K$.*

In fact [3, Theorem 1] is stated slightly differently and we are using the fact that if the maximal modulus of the conjugates (over $\mathbb{Q}$) of an algebraic number

$\alpha \in \mathbb{C}$ is equal to 1, then all conjugates lie on the unit circle. This is because the complex conjugate $\rho(\alpha)$ is also a conjugate (over $\mathbb{Q}$) of α. Hence α is reciprocal.

Theorem 2.1 in conjunction with Lemma 2.2 yields the first part of Proposition 1.1.

Lemma 2.3. *Let K be a number field. Then $\mathcal{S}_K \neq \{\pm 1\}$ if and only if $\mathbb{Q}(\mathcal{S}_K)$ is a CM-field.*

Proof. Suppose $\alpha_1, \dots, \alpha_n \in \mathcal{S}_K \backslash \{\pm 1\}$ with $\mathbb{Q}(\mathcal{S}_K) = \mathbb{Q}(\alpha_1, \dots, \alpha_n)$. By Theorem 2.1 we see that $K_i = \mathbb{Q}(\alpha_i)$ is CM for $1 \leq i \leq n$. By Lemma 2.2 we conclude that $\mathbb{Q}(\mathcal{S}_K) = K_1 \cdots K_n$ is also CM. The other direction is trivial. □

Next we restate the Proposition 1.2 and we prove it.

Proposition 2.1. *Let K be a CM-field and k its maximal totally real subfield. Then $\mathcal{S}_K$ is the kernel of the norm map $N_{K/k} : K^\times \to k^\times$.*

Proof. Let $\alpha \in K^\times$ be in the kernel of the norm map. Using (2.7) and (2.6) gives

$$1 = N_{K/k}(\alpha) = \alpha\tau(\alpha) = \alpha\sigma^{-1}(\rho(\sigma(\alpha)))$$

for all homomorphisms $\sigma : K \to \mathbb{C}$. Applying σ on both sides gives

$$1 = \sigma(\alpha)\rho(\sigma(\alpha)) = |\sigma(\alpha)|^2.$$

Hence, $|\alpha|_v = 1$ for all archimedean places v of K, and so $\alpha \in \mathcal{S}_K$.

Now suppose $\beta \in \mathcal{S}_K$. Then $|\sigma(\beta)|^2 = \sigma(\beta)\rho(\sigma(\beta)) = 1$ for all homomorphism $\sigma : K \to \mathbb{C}$. Applying σ^{-1} on both sides gives $1 = \beta\sigma^{-1}(\rho(\sigma(\beta))) = \beta\tau(\beta)$. Thus $N_{K/k}(\beta) = 1$. □

We also learn from this proof that if $\alpha \in K^\times$ then $\sigma(N_{K/k}(\alpha)) = |\sigma(\alpha)|^2 > 0$ for any homomorphism $\sigma : K \to \mathbb{C}$. Hence, the norm $N_{K/k}$ maps to the subset of $k^\times$ of totally positive elements.

As before let τ be the unique non-trivial automorphism of K fixing k, and let $\psi : K^\times \to K^\times$ be the group homomorphism defined by

$$\psi(\beta) = \frac{\beta}{\tau(\beta)}. \tag{2.8}$$

We note that the kernel of ψ is $k^\times$. Since K/k is a cyclic extension and $\mathrm{Gal}(K/k) = \langle\tau\rangle$ it follows from Hilbert's Theorem 90 that $\ker N_{K/k} = \mathrm{Im}\,\psi$. Hence, the maps ψ and the norm $N_{K/k}$ yield an exact sequence

$$k^\times \xrightarrow{\mathrm{id}} K^\times \xrightarrow{\psi} K^\times \xrightarrow{N_{K/k}} k^\times, \tag{2.9}$$

and we know from Proposition 2.1 that the group $\mathcal{S}_K$ is given by the kernel of the norm map $N_{K/k}$ which in turn is equal to the image of ψ. Hence,

$$\mathcal{S}_K = \mathrm{Im}\,\psi \cong K^\times/k^\times. \tag{2.10}$$

3. The group structure of $\mathcal{S}_K$

In this section we prove that $\mathcal{S}_K/\mathrm{Tor}(K^\times)$ is a free abelian group of countably infinite rank, proving the second claim of Proposition 1.1.

Lemma 3.1. *Let K be a CM-field and let k be its maximal totally real subfield. Then $\mathcal{S}_K/\mathrm{Tor}(K^\times)$ is a free abelian group of countably infinite rank.*

Proof. It follows from the exact sequence (2.9) that the induced homomorphism

$$\widehat{\psi} : K^\times/k^\times \to \mathcal{S}_K \tag{3.11}$$

is an isomorphism of multiplicative groups. By a result of Brandis [5] the group $K^\times/k^\times$ is not finitely generated. Because (3.11) is an isomorphism, we conclude that the group $\mathcal{S}_K$ is not finitely generated.

From (1.1) we get

$$\mathrm{Tor}(\mathcal{S}_K) = \mathrm{Tor}(K^\times), \tag{3.12}$$

and therefore $\mathrm{Tor}(\mathcal{S}_K)$ is a finite cyclic group of order $2q$ where $q|\Delta_K$. Hence, the torsion-free abelian group $\mathcal{S}_K/\mathrm{Tor}(K^\times)$ is not finitely generated.

We note that the absolute, logarithmic Weil height $h(\cdot) = \log H(\cdot)$ is well defined on the multiplicative quotient group

$$K^\times/\mathrm{Tor}(K^\times) = \mathcal{G}_K.$$

Moreover, the Weil height

$$h : \mathcal{G}_K \to [0, \infty)$$

satisfies (here we write α and β for coset representatives in $\mathcal{G}_K$):

(i) $0 \leq h(\alpha)$ for α in $\mathcal{G}_K$, and $0 = h(\alpha)$ if and only if $\alpha = 1$,

(ii) $h(\alpha^m) = |m|h(\alpha)$ for each $m \in \mathbb{Z}$ and α in $\mathcal{G}_K$,

(iii) $h(\alpha\beta) \leq h(\alpha) + h(\beta)$ for each α and β in $\mathcal{G}_K$,

(iv) there exists $0 < \varepsilon(K)$ so that $\varepsilon(K) \leq h(\alpha)$ for each $\alpha \neq 1$ in $\mathcal{G}_K$.

These four conditions imply that h is a discrete norm on the abelian group $\mathcal{G}_K$, and on all of its subgroups. It follows from the results of [7], [13], and [16], that an abelian group with a discrete norm must be a free group. As

$$\mathcal{S}_K/\mathrm{Tor}(K^\times) \subseteq \mathcal{G}_K,$$

we find that the quotient group $\mathcal{S}_K/\mathrm{Tor}(K^\times)$ is a free group and not finitely generated. Hence, $\mathcal{S}_K/\mathrm{Tor}(K^\times)$ has (countably) infinite rank. □

4. Lattice point counting

Throughout this section let $D \geq 2$ be an integer. By a lattice Λ in $\mathbb{R}^D$ we mean a discrete, free $\mathbb{Z}$-module of rank D. Let $\lambda_1(\Lambda)$ be the shortest euclidean length of a non-zero vector of Λ

$$\lambda_1 = \min\{|\boldsymbol{x}|; \boldsymbol{x} \in \Lambda, \boldsymbol{x} \neq 0\}.$$

Let M be a positive integer, and let L be a non-negative real number. We say that a set S is in $\mathrm{Lip}(D, M, L)$ if S is a subset of $\mathbb{R}^D$, and if there are M maps

$$\phi_1, \ldots, \phi_M : [0,1]^{D-1} \longrightarrow \mathbb{R}^D$$

satisfying a Lipschitz condition

$$|\phi_i(\boldsymbol{x}) - \phi_i(\boldsymbol{y})| \leq L|\boldsymbol{x} - \boldsymbol{y}| \text{ for } \boldsymbol{x}, \boldsymbol{y} \in [0,1]^{D-1}, i = 1, \ldots, M$$

such that S is covered by the images of the maps ϕ_i.

If the boundary ∂S is in $\mathrm{Lip}(D, M, L)$ then ∂S has measure zero and thus S is measurable (see, e.g., [12]).

The following Lemma is [15, Lemma 3.1].

Lemma 4.1. *Let Λ be a lattice in $\mathbb{R}^D$ Let S be a set in $\mathbb{R}^D$ such that the boundary ∂S of S is in Lip(D, M, L), and suppose S lies in the closed euclidean ball with centre P. Then S is measurable, and moreover,*

$$\left| \#(\Lambda \cap S) - \frac{\mathrm{Vol} S}{\det \Lambda} \right| \leq D^{3D^2/2} M \left(\left(\frac{L}{\lambda_1} \right)^{D-1} + 1^*(S \cap \Lambda) \right),$$

where $1^*(S \cap \Lambda) = 0$ if $S \cap \Lambda = \emptyset$ and $1^*(S \cap \Lambda) = 1$ otherwise.

If we can choose P to be the origin and the latter is not contained in S then we can get rid of the extra 1^* in the error term, and this gives a slightly more convenient version for our purposes.

Lemma 4.2. *Let Λ be a lattice in $\mathbb{R}^D$ and $\lambda_1 = \lambda_1(\Lambda)$. Let S be a set in $\mathbb{R}^D$ such that the boundary ∂S of S is in Lip(D, M, L). Suppose S is contained in the closed euclidean ball about the origin of radius L, and the origin is not contained in S. Then*

$$\left| \#(\Lambda \cap S) - \frac{\mathrm{Vol} S}{\det \Lambda} \right| \leq 2D^{3D^2/2} M \left(\frac{L}{\lambda_1} \right)^{D-1}.$$

Proof. The claim follows from Lemma 4.1 upon noticing that if $L < \lambda_1$ then $\Lambda \cap S = \emptyset$ so that $1^*(\Lambda \cap S) = 0$. And if $L \geq \lambda_1$ then $L/\lambda_1 \geq 1^*(\Lambda \cap S)$. □

5. Preliminaries

For $1 \leq n \leq N$ let σ_n, σ_{n+N} be the N pairs of complex conjugate embeddings of K into $\mathbb{C}$. Write $\boldsymbol{\sigma} : K \to \mathbb{C}^N$ for the Minkowski-embedding defined by

$$\boldsymbol{\sigma}(\beta) = (\sigma_1(\beta), \dots, \sigma_N(\beta)).$$

Recall that k, the maximal totally real subfield of K, has degree N, and its N distinct embeddings into $\mathbb{C}$ are given by the restrictions of $\sigma_1, \dots, \sigma_N$ to k. Let $l : k^\times \to \mathbb{R}^N$ be the usual logarithmic mapping defined by

$$l(\beta) = (2\log|\sigma_1(\beta)|, \dots, 2\log|\sigma_N(\beta)|).$$

Let F be a fundamental domain of $\Sigma = \{(z_n)_n \in \mathbb{R}^N; \sum_n z_n = 0\}$ for the action of the subgroup $\mathbb{U}_k = l(\mathcal{O}_k^\times)$ on Σ. If $N = 1$ (i.e., $k = \mathbb{Q}$) we have $\mathbb{U}_k = \{0\}$, and so there is no choice except $F = \Sigma = \{0\}$. If $N > 1$ then $\mathbb{U}_k$ is a lattice in Σ and we have many choices for F. It is convenient to have an F with "simple" geometry, therefore we take

$$F = [0, 1)u_1 + \cdots + [0, 1)u_{N-1}$$

where $(u_1, \dots, u_{N-1})$ is a reduced basis of the unit lattice $\mathbb{U}_k$, in the sense that $|u_1| \leq \cdots \leq |u_{N-1}| \leq c_N R_k$ for some constant $c_N > 0$. The existence of such a reduced basis follows from the general reduction theory and the additional fact $|u_1| \gg_N 1$ which is a consequence of Northcott's Theorem. Let $T \geq 1$. Let $([K_v : \mathbb{Q}_v])_{v|\infty} = (2, \dots, 2)$, and consider the vector sum

$$F(T) = F + (2, \dots, 2)(-\infty, \log T].$$

Then $F(\infty) = F + (2, \dots, 2)(-\infty, \infty)$ is a fundamental domain for the action of the subgroup $\mathbb{U}_K$ on $\mathbb{R}^N$.

Let $\mathcal{J} = \mathcal{J}_1 \times \cdots \times \mathcal{J}_N$ where each $\mathcal{J}_j$ is an arbitrary subset of $[0, 2\pi)$. We define the set

(5.13)

$$S_F(\mathcal{J}; T) = \{\boldsymbol{x} = (x_n)_n \in (\mathbb{C}^\times)^N; (2\log|x_n|)_n \in F(T), \text{ and } (\arg(x_n))_n \in \mathcal{J}\}.$$

We note that $S_F(\mathcal{J}; T)$ is homogeneously expanding, i.e.,

$$S_F(\mathcal{J}; T) = TS_F(\mathcal{J}; 1). \tag{5.14}$$

Now let $\mathcal{I} = \mathcal{I}_1 \times \cdots \times \mathcal{I}_N \subseteq [0, 2\pi)^N$ be a product of intervals as in Theorem 1.1, and let

$$\mathcal{I}^* = \frac{1}{2}\mathcal{I}_1 \times \prod_{n=2}^{N} \left(\frac{1}{2}\mathcal{I}_n \cup \left(\frac{1}{2}\mathcal{I}_n + \pi\right)\right) \tag{5.15}$$

One step in the proof of Theorem 1.1 is to count lattice points inside the set $S_F(\mathcal{I}^*; T)$ for suitable T. To this end we will need the following two lemmas. Recall from Section 4 that a set $S \subseteq \mathbb{R}^D$ is in $\mathrm{Lip}(D, M, L)$ if if there are M maps

$$\phi_1, \dots, \phi_M : [0, 1]^{D-1} \longrightarrow \mathbb{R}^D$$

satisfying a Lipschitz condition

$$|\phi_i(\boldsymbol{x}) - \phi_i(\boldsymbol{y})| \leq L|\boldsymbol{x} - \boldsymbol{y}| \text{ for } \boldsymbol{x}, \boldsymbol{y} \in [0, 1]^{D-1}, i = 1, \dots, M$$

such that S is covered by the images of the maps ϕ_i.

Lemma 5.1. *The set $S_F(\mathcal{I}^*; 1)$ is contained in the closed euclidean ball about the origin of radius L, and its boundary $\partial(S_F(\mathcal{I}^*; 1))$ is in Lip$(2N, M, L)$ with $M = M(N)$ and $L = L(K)$ depending only on K. Further, the origin is not contained in $S_F(\mathcal{I}^*; 1)$.*

Proof. The last assertion is clear from the definition (5.13). The first and the second assertion are easy to see for $N = 1$, so we assume $N \geq 2$. Thus $F = [0, 1)u_1 + \cdots + [0, 1)u_{N-1}$ and $|u_i| \leq c_N R_k$ for $1 \leq i \leq N - 1$.

For the first assertion we note that if $\boldsymbol{x} \in S_F(\mathcal{I}^*; 1)$ then $|x_n|^2 = \exp(z_n + 2t)$ for some $\boldsymbol{z} \in F$ and $t \in (-\infty, 0]$. Hence, $|z_n| \leq (N - 1)c_N R_k \leq Nc_N R_k$, and so the first claim holds for any $L \geq L_0 := (N \exp(Nc_N R_k))^{1/2}$.

Now let us prove the second claim. The boundary $\partial(S_F(\mathcal{I}^*; 1))$ comes in two flavours. Firstly, those points $\boldsymbol{x}$ in the topological closure of $S_F(\mathcal{I}^*; 1)$ with $(|x_n|^2)_n \in \exp(\partial F(1))$, where we used exp for the diagonal exponential map from $\mathbb{R}^N$ to $(0, \infty)^N$. And secondly, those points $\boldsymbol{x}$ in the closure of $S_F(\mathcal{I}^*; 1)$ with $\boldsymbol{x} \in [0, 1] \cdot L_0 \exp(i\partial\mathcal{I}^*)$, where exp denotes the complex diagonal exponential map, and $\partial\mathcal{I}^*$ denotes the boundary of the set $\mathcal{I}^* \subseteq \mathbb{R}^N$.

The latter are covered by 2^N Lipschitz maps as follows. Choose $1 \leq m \leq N$, and let γ be one of the two endpoints of $\mathcal{I}_m$. Sending $t_m \in [0, 1]$ to $t_m L_0 \exp(i\gamma)$ and, for $n \neq m$, sending $(t_n, \gamma_n) \in [0, 1]^2$ to $t_n L_0 \exp(i2\pi\gamma_n)$ defines a map from $[0, 1]^{2N-1}$ to $\mathbb{C}^N$. In this way we get 2^N maps whose images cover $[0, 1] \cdot L_0 \exp(i\partial\mathcal{I}^*)$, and each one satisfies Lipschitz condition with Lipschitz constant $L \ll_K 1$ (see [14, (1)-(3) Appendix A]).

Parametrising the points of the first kind is more involved but this has been done (in a more general setting) in [8, Lemma 3] and, with explicit constants,

in [14, Lemma A.1] (with the irrelevant difference that the coordinates x_n are in some $\mathbb{C}^m$ instead of $\mathbb{C}$). □

Lemma 5.2. *The set $S_F(\mathcal{I}^*; 1)$ is measurable and we have*

$$\mathrm{Vol}(S_F(\mathcal{I}^*; 1)) = \frac{|\mathcal{I}|R_k}{2^N \omega_k}.$$

Proof. We note that the $(N-1)$-volume of F is $\sqrt{N}R_k$. The proof is now nearly identical to the proof of [8, Lemma 4] and left to the reader. □

6. Constructing a suitable fundamental domain

We use the letters A, B, C to denote non-zero ideals in $\mathcal{O}_k$, and P, Q to denote non-zero prime ideals in $\mathcal{O}_k$. And we use the letters $\mathfrak{A}, \mathfrak{B}, \mathfrak{C}, \mathfrak{D}, \mathcal{P}$ to denote non-zero ideals in $\mathcal{O}_K$, and the letters $\mathfrak{p}, \mathfrak{q}$ to denote non-zero prime ideals in $\mathcal{O}_K$. We write $A\mathcal{O}_K$ for the extension of the ideal $A \subseteq \mathcal{O}_k$ to an ideal of $\mathcal{O}_K$, and we note that $(AB)\mathcal{O}_K = (A\mathcal{O}_K)(B\mathcal{O}_K)$. Let

$$\mathcal{R}_k = \{C_1, \dots, C_h\}$$

be a complete system of integral inequivalent representatives of the class group Cl_k of k. Let

$$P_1, \dots, P_s$$

be the (possibly empty) list of prime ideals of $\mathcal{O}_k$ that ramify in K, so that

$$P_1\mathcal{O}_K = \mathfrak{p}_1^2, \dots, P_s\mathcal{O}_K = \mathfrak{p}_s^2$$

for certain distinct prime ideals $\mathfrak{p}_1, \dots, \mathfrak{p}_s$ of $\mathcal{O}_K$. We note that $P_1, \dots, P_s$ are precisely the prime ideals that divide $D_{K/k}$. We set

$$\mathcal{P} = \mathfrak{p}_1 \cdots \mathfrak{p}_s,$$

for the square-free part of $D_{K/k}$, and the empty product (i.e., $s = 0$) is understood as $\mathcal{O}_K$.

We let $I_{\mathcal{P}}$ be the set of non-zero ideals of $\mathcal{O}_K$ that have no ideal divisors A defined over the subfield k and are coprime to $\mathcal{P}$, i.e.,

$$I_{\mathcal{P}} = \{\mathfrak{B} \subseteq \mathcal{O}_K; \mathfrak{B} \neq \{0\}, (\mathfrak{B}, \mathcal{P}) = 1, \text{ and } A\mathcal{O}_K \nmid \mathfrak{B} \text{ for all } A \subsetneq \mathcal{O}_k\}.$$

Lemma 6.1. *Let A, A' be non-zero ideals of $\mathcal{O}_k$, let $\mathfrak{D}, \mathfrak{D}'$ be ideals of $\mathcal{O}_K$ both dividing $\mathcal{P}$, and let $\mathfrak{B}$ and $\mathfrak{B}'$ both be in $I_{\mathcal{P}}$. If $A\mathcal{O}_K\mathfrak{D}\mathfrak{B} = A'\mathcal{O}_K\mathfrak{D}'\mathfrak{B}'$ then $A = A'$, $\mathfrak{D} = \mathfrak{D}'$ and $\mathfrak{B} = \mathfrak{B}'$.*

Proof. If $\mathfrak{p}|\mathcal{P}$ then $\mathrm{ord}_{\mathfrak{p}}(A\mathcal{O}_K\mathfrak{B})$ and $\mathrm{ord}_{\mathfrak{p}}(A'\mathcal{O}_K\mathfrak{B}')$ are even. This implies that $\mathfrak{D} = \mathfrak{D}'$, and thus $A\mathcal{O}_K\mathfrak{B} = A'\mathcal{O}_K\mathfrak{B}'$. Let $P \subseteq \mathcal{O}_k$, and suppose $\mathrm{ord}_P(A) \geq \mathrm{ord}_P(A')$. Dividing both sides by $P^{\mathrm{ord}_P(A')}\mathcal{O}_K$, and assuming $\mathrm{ord}_P(A) > \mathrm{ord}_P(A')$ we conclude $P\mathcal{O}_K|\mathfrak{B}'$ which is impossible as $\mathfrak{B}' \in I_{\mathcal{P}}$. This proves that $A = A'$, and hence $\mathfrak{B} = \mathfrak{B}'$. □

Recall that τ is the unique non-trivial automorphism of K fixing k, and

$$\psi : K^\times \to K^\times \tag{6.16}$$

denotes the group homomorphism defined by $\psi(\beta) = \beta/\tau(\beta)$. The kernel of ψ is $k^\times$ and $\tau^2 = \mathrm{id}$.

Lemma 6.2. *Let $C \in \mathcal{R}_k$, $\mathfrak{D}|\mathcal{P}$ and $\mathfrak{B} \in I_{\mathcal{P}}$. Then $\tau(C\mathcal{O}_K\mathfrak{D}\mathfrak{B}) = C\mathcal{O}_K\mathfrak{D}\tau(\mathfrak{B})$, and $(\mathfrak{B}, \tau(\mathfrak{B})) = 1$.*

Proof. We have $\tau(C\mathcal{O}_K) = \tau(C)\mathcal{O}_K = C\mathcal{O}_K$. Further, $\tau(\mathfrak{p}_j)^2 = \tau(\mathfrak{p}_j^2) = \tau(P_j\mathcal{O}_K) = \tau(P_j)\mathcal{O}_K = P_j\mathcal{O}_K = \mathfrak{p}_j^2$, and thus $\tau(\mathfrak{p}_j) = \mathfrak{p}_j$, and so $\tau(\mathfrak{D}) = \mathfrak{D}$. Now suppose the prime ideal $\mathfrak{q}$ divides $\mathfrak{B}$ and $\tau(\mathfrak{B})$. Then $\tau(\mathfrak{q})$ also divides $\tau^2(\mathfrak{B}) = \mathfrak{B}$. As $\mathfrak{B} \in I_{\mathcal{P}}$ it follows that $\mathfrak{q} \cap k$ must split in K, but then $\mathfrak{q}$ and $\tau(\mathfrak{q})$ are distinct prime ideals and thus $Q\mathcal{O}_K = \mathfrak{q}\tau(\mathfrak{q})$ divides $\mathfrak{B}$, contradicting that $\mathfrak{B} \in I_{\mathcal{P}}$. Hence $\mathfrak{B}$ and $\tau(\mathfrak{B})$ are coprime. □

Lemma 6.3. *If $\beta \in K^\times$ and $1 \leq n \leq N$, then*

$$\sigma_n(\psi(\beta)) = \frac{\sigma_n(\beta)}{\rho(\sigma_n(\beta))}.$$

In particular, $\arg(\sigma_n(\psi(\beta)))$ *and* $2\arg(\sigma_n(\beta))$ *differ by an integer multiple of* 2π.

Proof. Using (2.6) with $\sigma = \sigma_n$ gives

$$\sigma_n(\psi(\beta)) = \frac{\sigma_n(\beta)}{\sigma_n(\tau(\beta))} = \frac{\sigma_n(\beta)}{\rho(\sigma_n(\beta))}.$$

□

Next we define

$$Z^*(\mathfrak{A}) = \{\beta \in \mathfrak{A}\backslash\{0\}; \beta\mathcal{O}_K = \mathfrak{A}\mathfrak{B} \text{ for some } \mathfrak{B} \in I_{\mathcal{P}}\}.$$

Lemma 6.4. *Let $C \in \mathcal{R}_k$ and $\mathfrak{D}|\mathcal{P}$. Let β be in $Z^*(C\mathcal{O}_K\mathfrak{D})$). Then*

$$H(\psi(\beta)) = \left(\frac{N_{K/\mathbb{Q}}(\beta)}{N_{K/\mathbb{Q}}(C\mathcal{O}_K\mathfrak{D})}\right)^{1/(2N)}.$$

Proof. By Lemma 6.3 $\psi(\beta) \in \mathcal{S}_K$, and so there are no archimedean contributions to the height of $\psi(\beta)$. Writing v for the places of K and $d_v = [K_v : \mathbb{Q}_v]$, we have

$$H(\psi(\beta)) = \prod_{v\nmid\infty} \max\left\{1, \left|\frac{\beta}{\tau(\beta)}\right|_v\right\}^{d_v/(2N)}.$$

By Lemma 6.2 we have

$$\frac{\beta\mathcal{O}_K}{\tau(\beta\mathcal{O}_K)} = \frac{\mathfrak{B}}{\tau(\mathfrak{B})},$$

and $\mathfrak{B}$ and $\tau(\mathfrak{B})$ are coprime. It follows that

$$\prod_{v\nmid\infty} \max\left\{1, \left|\frac{\beta}{\tau(\beta)}\right|_v\right\}^{d_v/(2N)} = \left(N_{K/\mathbb{Q}}(\tau(\mathfrak{B}))\right)^{1/(2N)}.$$

Now $N_{K/\mathbb{Q}}(\tau(\mathfrak{B}) = N_{K/\mathbb{Q}}(\mathfrak{B})$, and thus

$$H(\psi(\beta)) = \left(N_{K/\mathbb{Q}}(\mathfrak{B})\right)^{1/(2N)} = \left(\frac{N_{K/\mathbb{Q}}(\beta)}{N_{K/\mathbb{Q}}(C\mathcal{O}_K\mathfrak{D})}\right)^{1/(2N)}.$$

□

As $F, \mathcal{I}$ and $\mathcal{H}$ are kept fixed we may simplify the notation and write

$$\mathbb{S}_{C,\mathfrak{D}} = \{\beta \in C\mathcal{O}_K\mathfrak{D}; \boldsymbol{\sigma}(\beta) \in S_F(\mathcal{I}^*; \mathcal{H}N_{K/\mathbb{Q}}(C\mathcal{O}_K\mathfrak{D}))^{1/(2N)}\}, \tag{6.17}$$

where $\mathcal{I}^*$ was defined in (5.15).

Lemma 6.5. *The restriction of the map ψ defined in (6.16) to the subset*

$$\bigcup_{C\in\mathcal{R}_k}\bigcup_{\mathfrak{D}|\mathcal{P}}(Z^*(C\mathcal{O}_K\mathfrak{D}))\cap\mathbb{S}_{C,\mathfrak{D}}$$

maps to the set $\mathcal{S}_K(\mathcal{I},\mathcal{H})$.

Proof. Let $C \in \mathcal{R}_k$ and $\mathfrak{D}|\mathcal{P}$, and let β be in $Z^*(C\mathcal{O}_K\mathfrak{D}))\cap\mathbb{S}_{C,\mathfrak{D}}$. Recalling (6.17) and (5.15) we see that for $1 \le n \le N$

$$\arg(\sigma_n(\beta)) \in \mathcal{I}_n^* \subseteq \frac{1}{2}\mathcal{I}_n \cup \left(\frac{1}{2}\mathcal{I}_n + \pi\right),$$

so that $2\arg(\sigma_n(\beta)) \in \mathcal{I}_n \cup (\mathcal{I}_n + 2\pi)$. It follows from Lemma 6.3 that $\arg(\sigma_n(\psi(\beta))) \in \mathcal{I}_n$ for $1 \le n \le N$. And it follows from Lemma 6.4 that

$$H(\psi(\beta)) = \left(\frac{N_{K/\mathbb{Q}}(\beta)}{N_{K/\mathbb{Q}}(C\mathcal{O}_K\mathfrak{D})}\right)^{1/(2N)} \le \mathcal{H}.$$

This proves that $\psi(\beta) \in \mathcal{S}_K(\mathcal{I};\mathcal{H})$. □

Lemma 6.5 shows that we have the map

$$\psi : \bigcup_{C\in\mathcal{R}_k}\bigcup_{\mathfrak{D}|\mathcal{P}}(Z^*(C\mathcal{O}_K\mathfrak{D}))\cap\mathbb{S}_{C,\mathfrak{D}} \to \mathcal{S}_K(\mathcal{I},\mathcal{H}) \tag{6.18}$$

Lemma 6.6. *The map ψ defined in (6.18) is surjective.*

Proof. Let α be in $\mathcal{S}_K(\mathcal{I},\mathcal{H})$. Since $\mathcal{S}_K$ is the kernel of the norm map $N_{K/k}$ it follows from the exact sequence (2.9) that $\psi : K^\times \to K^\times$ has image $\mathcal{S}_K$ and kernel $k^\times$. Hence there is $\beta \in \mathcal{O}_K$ that maps to α. Now let $A \subseteq \mathcal{O}_k$ be of maximal norm with $A\mathcal{O}_K|\beta\mathcal{O}_K$. Hence, $\mathfrak{p}^2 \nmid \beta\mathcal{O}_K(A\mathcal{O}_K)^{-1}$ whenever $\mathfrak{p}|\mathcal{P}$. Therefore there exists $\mathfrak{D}|\mathcal{P}$ and $\mathfrak{B} \in I_{\mathcal{P}}$ such that

$$\beta\mathcal{O}_K = A\mathcal{O}_K\mathfrak{D}\mathfrak{B}.$$

There exists $\xi \in k^\times$, unique up to units of $\mathcal{O}_k$, such that $\xi A \in \mathcal{R}_k$, say $\xi A = C$. Replacing β by $\xi\beta$ we get

$$\beta\mathcal{O}_K = \xi\mathcal{O}_K A\mathcal{O}_K\mathfrak{D}\mathfrak{B} = (\xi A)\mathcal{O}_K\mathfrak{D}\mathfrak{B} = C\mathcal{O}_K\mathfrak{D}\mathfrak{B},$$

and this shows that $\beta \in Z^*(C\mathcal{O}_K\mathfrak{D})$. Multiplying β with a unit of $\mathcal{O}_k$, unique up to sign, we get $(2\log|\sigma_n(\beta)|)_n \in F(\infty)$ and, of course, still $\beta \in Z^*(C\mathcal{O}_K\mathfrak{D})$. Replacing β by $-\beta$ if needed we get $\boldsymbol{\sigma}(\beta) \in S_F(\mathcal{I}^*;\infty)$. Finally, by Lemma 6.4

$$H(\psi(\beta)) = \left(\frac{N_{K/\mathbb{Q}}(\beta)}{N_{K/\mathbb{Q}}(C\mathcal{O}_K\mathfrak{D})}\right)^{1/(2N)}.$$

Since $H(\psi(\beta)) = H(\alpha) \le \mathcal{H}$, we conclude that $\beta \in \mathbb{S}_{C,\mathfrak{D}}$. This proves the surjectivity of (6.18). □

Lemma 6.7. *The map ψ defined in (6.18) is injective.*

Proof. Suppose β, β' are both in the domain and have the same image. Then $\beta'/\beta \in k^\times$ and so $\beta' = \xi\beta$ for some $\xi \in k^\times$. Further

$$\beta\mathcal{O}_K = C\mathcal{O}_K\mathfrak{D}\mathfrak{B}, \quad \text{and} \quad \beta'\mathcal{O}_K = C'\mathcal{O}_K\mathfrak{D}'\mathfrak{B}'$$

for certain C, C' both in $\mathcal{R}_k$, $\mathfrak{D}, \mathfrak{D}'$ both dividing $\mathcal{P}$, and $\mathfrak{B}, \mathfrak{B}'$ both in $I_\mathcal{P}$. Hence,

$$\xi C\mathcal{O}_K\mathfrak{D}\mathfrak{B} = C'\mathcal{O}_K\mathfrak{D}'\mathfrak{B}'.$$

Writing $\xi = \xi_1/\xi_0$ with non-zero $\xi_0, \xi_1 \in \mathcal{O}_k$, and $A = \xi_1 C$, $A' = \xi_0 C'$ it follows that

$$A\mathcal{O}_K\mathfrak{D}\mathfrak{B} = A'\mathcal{O}_K\mathfrak{D}'\mathfrak{B}'.$$

Now Lemma 6.1 tells us that that $A = A'$, $\mathfrak{D} = \mathfrak{D}'$ and $\mathfrak{B} = \mathfrak{B}'$. This implies that C and C' both lie in the same ideal class of k and so must be equal. Consequently $\beta' = \eta\beta$ for a unit η in $\mathcal{O}_K^\times \cap k = \mathcal{O}_k^\times$. As β and β' are both in $\mathbb{S}_{C,\mathfrak{D}}$ we conclude that $l(\eta) = 0$ and thus $\eta = \pm 1$. Finally, since $\arg(\sigma_1(\beta))$ and $\arg(\sigma_1(\beta'))$ are both in $(1/2)\mathcal{I}_1 \subseteq [0, \pi)$ the case $\beta' = -\beta$ is ruled out. This proves the injectivity. □

Lemma 6.8. *The union*

$$\bigcup_{C\in\mathcal{R}_k} \bigcup_{\mathfrak{D}|\mathcal{P}} (Z^*(C\mathcal{O}_K\mathfrak{D}))$$

is disjoint. In particular,

$$\bigcup_{C\in\mathcal{R}_k} \bigcup_{\mathfrak{D}|\mathcal{P}} (Z^*(C\mathcal{O}_K\mathfrak{D})) \cap \mathbb{S}_{C,\mathfrak{D}}$$

is a disjoint union.

Proof. Let $C_1, C_2 \in \mathcal{R}_k$, let $\mathfrak{D}_1, \mathfrak{D}_2$ both be divisors of $\mathcal{P}$ and suppose

$$\beta \in Z^*(C_1\mathcal{O}_K\mathfrak{D}_1) \cap Z^*(C_2\mathcal{O}_K\mathfrak{D}_2).$$

Hence, there exist $\mathfrak{B}_1, \mathfrak{B}_2 \in I_\mathcal{P}$ such that $C_1\mathcal{O}_K\mathfrak{D}_1\mathfrak{B}_1 = C_2\mathcal{O}_K\mathfrak{D}_2\mathfrak{B}_2$. Now Lemma 6.1 implies that $C_1 = C_2$ and $\mathfrak{D}_1 = \mathfrak{D}_2$ and this proves the lemma. □

Lemma 6.9. *We have*

$$\#\mathcal{S}_K(\mathcal{I}, \mathcal{H}) = \sum_{C\in\mathcal{R}_k} \sum_{\mathfrak{D}|\mathcal{P}} \#Z^*(C\mathcal{O}_K\mathfrak{D}) \cap \mathbb{S}_{C,\mathfrak{D}}.$$

Proof. Follows immediately from Lemma 6.6, 6.7, and 6.8. □

7. Sieving

Lemma 6.9 shows that we simply need to compute $\#Z^*(C\mathcal{O}_K\mathfrak{D}) \cap \mathbb{S}_{C,\mathfrak{D}}$. In this section we apply simple sieving arguments to reduce this task to an ordinary lattice point counting problem.

For the entire section we fix a non-zero ideal $\mathfrak{A}$ in $\mathcal{O}_K$ (playing the role of $C\mathcal{O}_K\mathfrak{D}$), and an arbitrary finite subset $\mathfrak{S}$ of $\mathcal{O}_K$ (playing the role of $\mathbb{S}_{C,\mathfrak{D}}$). For a non-zero ideal $A \subseteq \mathcal{O}_k$ we write

$$Z_A = \left(\mathfrak{A}A\mathcal{O}_K \setminus \bigcup_{\mathfrak{p}|\mathcal{P}} \mathfrak{A}\mathfrak{p}A\mathcal{O}_K \right) \cap \mathfrak{S}.$$

We note that

$$Z_A = \{\beta \in \mathfrak{A}A\mathcal{O}_K \setminus \{0\}; \beta\mathcal{O}_K = \mathfrak{A}A\mathcal{O}_K\mathfrak{B} \text{ for some } \mathfrak{B} \subseteq \mathcal{O}_K \text{ with } (\mathcal{P}, \mathfrak{B}) = 1\} \cap \mathfrak{S}.$$

Lemma 7.1. *We have*

$$Z^*(\mathfrak{A}) \cap \mathfrak{S} = Z_{\mathcal{O}_k} \setminus \bigcup_{A \subsetneq \mathcal{O}_k} (Z_{\mathcal{O}_k} \cap \mathfrak{A}A\mathcal{O}_K)$$

Proof. If $\beta \in Z^*(\mathfrak{A})$ then clearly $\beta \in Z_{\mathcal{O}_k}$ and $\beta \notin \mathfrak{A}A\mathcal{O}_K$ whenever $A \subsetneq \mathcal{O}_k$. Hence, $\beta \in Z_{\mathcal{O}_k} \setminus \bigcup_{A \subsetneq \mathcal{O}_k} (Z_{\mathcal{O}_k} \cap \mathfrak{A}A\mathcal{O}_K)$.

Now suppose $\beta \in Z_{\mathcal{O}_k} \setminus \bigcup_{A \subsetneq \mathcal{O}_k} (Z_{\mathcal{O}_k} \cap \mathfrak{A}A\mathcal{O}_K)$. As $\beta \in Z_{\mathcal{O}_k}$ we have $\beta\mathcal{O}_K = \mathfrak{A}\mathcal{O}_K\mathfrak{B}$ for some $\mathfrak{B} \subseteq \mathcal{O}_K$ with $(\mathcal{P}, \mathfrak{B}) = 1$. And since $\beta \notin \bigcup_{A \subsetneq \mathcal{O}_k} \mathfrak{A}A\mathcal{O}_K$ we see that $A\mathcal{O}_K \nmid \mathfrak{B}$ for all $A \subsetneq \mathcal{O}_k$. Hence, $\mathfrak{B} \in I_{\mathcal{P}}$, and thus $\beta \in Z^*(\mathfrak{A})$. □

Lemma 7.2. *We have*

$$\bigcup_{A \subsetneq \mathcal{O}_k} (Z_{\mathcal{O}_k} \cap \mathfrak{A}A\mathcal{O}_K) = \bigcup_{\substack{Q \\ (Q, P_1 \cdots P_s) = 1}} Z_Q,$$

where the union is taken over all prime ideals $Q \subseteq \mathcal{O}_k$ different from the prime ideals $P_1, \ldots, P_s$.

Proof. We have

$$\bigcup_{A \subsetneq \mathcal{O}_k} (Z_{\mathcal{O}_k} \cap \mathfrak{A}A\mathcal{O}_K) = \bigcup_{Q} (Z_{\mathcal{O}_k} \cap \mathfrak{A}Q\mathcal{O}_K),$$

and if $(Q, P_1 \cdots P_s) \neq 1$ then

$$Z_{\mathcal{O}_k} \cap \mathfrak{A}Q\mathcal{O}_K = \emptyset.$$

Therefore

$$\bigcup_{A \subsetneq \mathcal{O}_k} (Z_{\mathcal{O}_k} \cap \mathfrak{A}A\mathcal{O}_K) = \bigcup_{\substack{Q \\ (Q, P_1 \cdots P_s) = 1}} (Z_{\mathcal{O}_k} \cap \mathfrak{A}Q\mathcal{O}_K),$$

and further,

$$\begin{aligned} Z_{\mathcal{O}_k} \cap \mathfrak{A}Q\mathcal{O}_K &= \mathfrak{S} \cap \left(\mathfrak{A} \setminus \bigcup_{\mathfrak{p} \mid \mathcal{P}} \mathfrak{A}\mathfrak{p} \right) \cap \mathfrak{A}Q\mathcal{O}_K \\ &= \mathfrak{S} \cap \mathfrak{A}Q\mathcal{O}_K \setminus \bigcup_{\mathfrak{p} \mid \mathcal{P}} (\mathfrak{A}\mathfrak{p} \cap \mathfrak{A}Q\mathcal{O}_K). \end{aligned}$$

Finally, for prime Q with $(Q, P_1 \cdots P_s) = 1$ we have $(Q\mathcal{O}_K, \mathcal{P}) = 1$ and thus $\mathfrak{A}\mathfrak{p}\mathcal{O}_K \cap \mathfrak{A}Q\mathcal{O}_K = \mathfrak{A}\mathfrak{p}Q\mathcal{O}_K$ whenever $\mathfrak{p} \mid \mathcal{P}$. Hence,

$$Z_{\mathcal{O}_k} \cap \mathfrak{A}Q\mathcal{O}_K = \mathfrak{S} \cap \mathfrak{A}Q\mathcal{O}_K \setminus \bigcup_{\mathfrak{p} \mid \mathcal{P}} (\mathfrak{A}\mathfrak{p}Q\mathcal{O}_K) = Z_Q,$$

and this completes the proof. □

Lemma 7.3. *If $Q_1, \ldots, Q_m$ are distinct prime ideals of $\mathcal{O}_k$ all coprime to $P_1 \cdots P_s$ then*

$$\bigcap_{i=1}^{m} Z_{Q_i} = Z_{Q_1 \cdots Q_m}.$$

Proof. For arbitrary sets A_i and subsets B_{ij}, and $A = \cap_i A_i$ one has

$$\cap_i (A_i \backslash \cup_j B_{ij}) = A \backslash (\cup_{i,j} B_{ij} \cap A).$$

Applying this with $A_i = \mathfrak{A} Q_i \mathcal{O}_K$, and $B_{ij} = \mathfrak{A}\mathfrak{p}_j Q_i \mathcal{O}_K$, so that $Z_{Q_i} = \mathfrak{S} \cap A_i \backslash \cup_j B_{ij}$, and noting that $B_{ij} \cap A = \mathfrak{A}\mathfrak{p}_j Q_1 \cdots Q_m$, as $(\mathfrak{p}_j, Q_1 \cdots Q_m \mathcal{O}_K) = 1$, we get

$$\bigcap_{i=1}^{m} Z_{Q_i} = \mathfrak{S} \cap \bigcap_{i=1}^{m} A_i \backslash \cup_j B_{ij} = \mathfrak{S} \cap \mathfrak{A} Q_1 \cdots Q_m \backslash (\cup_{i,j} \mathfrak{A}\mathfrak{p}_j Q_1 \cdots Q_m).$$

Finally, we note that $\cup_{i,j} \mathfrak{A}\mathfrak{p}_j Q_1 \cdots Q_m = \cup_{\mathfrak{p}|\mathcal{P}} \mathfrak{A}\mathfrak{p} Q_1 \cdots Q_m$, and thus the claim drops out. □

Let $\mu_k(\cdot)$ and $\mu_K(\cdot)$ be the Möbius functions on non-zero ideals of $\mathcal{O}_k$ and $\mathcal{O}_K$ respectively.

Lemma 7.4. *We have*

$$\# \bigcup_{\substack{Q \\ (Q, P_1 \cdots P_s)=1}} Z_Q = \sum_{\substack{A \subsetneq \mathcal{O}_k \\ (A, P_1 \cdots P_s)=1}} -\mu_k(A) \# Z_A,$$

where the left union is taken over all prime ideals $Q \subseteq \mathcal{O}_k$ different from the prime ideals $P_1, \ldots, P_s$.

Proof. As the set $\mathfrak{S}$ is finite there are only finitely many non-zero ideals $A \subsetneq \mathcal{O}_k$ for which $Z_A \neq \emptyset$. Among those A only finitely many prime ideals divisors Q occur. Let $Q_1, \ldots, Q_m$ be those that are coprime to $P_1 \cdots P_s$ (if no such Q exists then evidently both sides are 0). Applying the inclusion-exclusion principle, and then using Lemma 7.3 we find

$$\begin{aligned} \# \bigcup_{\substack{Q \\ (Q, P_1 \cdots P_s)=1}} Z_Q = \# \bigcup_{i=1}^{m} Z_{Q_i} &= \sum_{\emptyset \neq I \subseteq \{1,2,\ldots,m\}} (-1)^{\# I - 1} \# \bigcap_{i \in I} Z_{Q_i} \\ &= \sum_{\emptyset \neq I \subseteq \{1,2,\ldots,m\}} (-1)^{\# I - 1} \# Z_{\prod_{i \in I} Q_i} \\ &= \sum_{\substack{A \subsetneq \mathcal{O}_k \\ (A, P_1 \cdots P_s)=1}} -\mu_k(A) \# Z_A. \end{aligned}$$

□

Lemma 7.5. *Let A be a non-zero ideal in $\mathcal{O}_k$. Then we have*

$$\# Z_A = \sum_{\mathfrak{E} | \mathcal{P}} \mu_K(\mathfrak{E}) \# (\mathfrak{A}\mathfrak{E} A \mathcal{O}_K \cap \mathfrak{S}).$$

Proof. The inclusion-exclusion principle yields

$$\# \bigcup_{\mathfrak{p} | \mathcal{P}} \mathfrak{A}\mathfrak{p} A \mathcal{O}_K \cap \mathfrak{S} = \sum_{\substack{\mathfrak{E} | \mathcal{P} \\ \mathfrak{E} \neq \mathcal{O}_K}} -\mu_K(\mathfrak{E}) \# (\mathfrak{A}\mathfrak{E} A \mathcal{O}_K \cap \mathfrak{S}).$$

As $\# Z_A = \# (\mathfrak{A} A \mathcal{O}_K \cap \mathfrak{S}) - \# \bigcup_{\mathfrak{p} | \mathcal{P}} \mathfrak{A}\mathfrak{p} A \mathcal{O}_K \cap \mathfrak{S}$ the result follows at once. □

Lemma 7.6. *We have*

$$Z^*(\mathfrak{A}) \cap \mathfrak{S} = \sum_{\mathfrak{E} | \mathcal{P}} \mu_K(\mathfrak{E}) \left(\# (\mathfrak{A}\mathfrak{E} \cap \mathfrak{S}) + \sum_{\substack{A \subsetneq \mathcal{O}_k \\ (A, P_1 \cdots P_s)=1}} \mu_k(A) \# (\mathfrak{A}\mathfrak{E} A \mathcal{O}_K \cap \mathfrak{S}) \right).$$

Proof. Combining Lemma 7.1, Lemma 7.2, Lemma 7.4, and Lemma 7.5 the result drops out. □

Lemma 7.7. *The following two identities hold*

$$\sum_{\mathfrak{E}|\mathcal{P}} \frac{\mu_K(\mathfrak{E})}{N_{K/\mathbb{Q}}(\mathfrak{E})} = \prod_{P|D_{K/k}} \left(1 - \frac{1}{N_{k/\mathbb{Q}}(P)}\right),$$

$$\sum_{\substack{A\subseteq\mathcal{O}_k \\ (A,P_1\cdots P_s)=1}} \frac{\mu_k(A)}{N_{k/\mathbb{Q}}(A)^2} = \frac{1}{\zeta_k(2)} \prod_{P|D_{K/k}} \left(1 - \frac{1}{N_{k/\mathbb{Q}}(P)^2}\right)^{-1}.$$

Proof. Recall that $\mathcal{P} = \mathfrak{p}_1 \cdots \mathfrak{p}_s$. If $s = 0$ (i.e., $\mathcal{P} = \mathcal{O}_K$) then both statements are obvious; the first sum is 1 and the second one is $\zeta_k(2)^{-1}$. Note that $N_{k/\mathbb{Q}}(P_i) = N_{K/\mathbb{Q}}(\mathfrak{p}_i)$. The first statement follows by induction from the following simple identity

$$\sum_{\mathfrak{E}|\mathfrak{p}_1\cdots\mathfrak{p}_s} \frac{\mu_K(\mathfrak{E})}{N_{K/\mathbb{Q}}(\mathfrak{E})} = \sum_{\mathfrak{E}|\mathfrak{p}_1\cdots\mathfrak{p}_{s-1}} \frac{\mu_K(\mathfrak{E})}{N_{K/\mathbb{Q}}(\mathfrak{E})} \left(1 + \frac{\mu_K(\mathfrak{p}_s)}{N_{K/\mathbb{Q}}(\mathfrak{p}_s)}\right).$$

Now let us prove the second identity. We have

$$\begin{aligned}\sum_{\substack{A\subseteq\mathcal{O}_k \\ (A,P_1\cdots P_s)=1}} \frac{\mu_k(A)}{N_{k/\mathbb{Q}}(A)^2} &= \prod_{\substack{P \\ P\nmid P_1\cdots P_s}} \left(\mu_k(1) + \mu_k(P)N_{k/\mathbb{Q}}(P)^{-2} + \mu_k(P^2)N_{k/\mathbb{Q}}(P)^{-4} + \cdots\right) \\ &= \prod_{\substack{P \\ P\nmid P_1\cdots P_s}} \left(1 - \frac{1}{N_{k/\mathbb{Q}}(P)^2}\right) = \frac{1}{\zeta_k(2)} \prod_{P|D_{K/k}} \left(1 - \frac{1}{N_{k/\mathbb{Q}}(P)^2}\right)^{-1}.\end{aligned}$$

In the last step we have used that a prime ideal P divides $P_1 \cdots P_s$ if and only if it divides $D_{K/k}$. □

8. Proof of Theorem 1.1

Here we finalise the proof of Theorem 1.1. Combining Lemma 6.9 and Lemma 7.6 we are led to the problem of counting elements of an ideal satisfying certain archimedean conditions.

Let $\mathfrak{F} \subseteq \mathcal{O}_K$ be a non-zero ideal; then $\sigma(\mathfrak{F})$ is a lattice in $\mathbb{C}^N \cong \mathbb{R}^{2N}$ of determinant

$$\det(\sigma(\mathfrak{F})) = 2^{-N} N_{K/\mathbb{Q}}(\mathfrak{F}) \sqrt{|\Delta_K|}, \tag{8.19}$$

and the shortest non-zero vector has euclidean length

$$\lambda_1(\sigma(\mathfrak{F})) \geq N_{K/\mathbb{Q}}(\mathfrak{F})^{1/(2N)} \tag{8.20}$$

(see [8, Lemma 5]). For brevity let us write

$$V = \mathrm{Vol}(S_F(\mathcal{I}^*; 1)),$$
$$T = \mathcal{H} N_{K/\mathbb{Q}}(C\mathcal{O}_K\mathfrak{D})^{1/(2N)}.$$

Now

$$\sigma(\mathcal{S}_{C,\mathfrak{D}})) = \sigma(C\mathcal{O}_K\mathfrak{D}) \cap S_F(\mathcal{I}^*; T), \tag{8.21}$$

and it follows from (5.14) that

$$\mathrm{Vol}\left(S_F(\mathcal{I}^*;T)\right) = VT^{2N} = V\mathcal{H}^{2N}N_{K/\mathbb{Q}}(C\mathcal{O}_K\mathfrak{D}).$$

Lemma 8.1. *Let $C \in \mathcal{R}_k$, $\mathfrak{E}|\mathcal{P}$, $\mathfrak{D}|\mathcal{P}$, $A \subseteq \mathcal{O}_K$, and let $\mathcal{H} \geq 2$. Then there exists a constant $c_1 = c_1(K)$ such that*

$$\left|\#(C\mathcal{O}_K\mathfrak{D}\mathfrak{E}A\mathcal{O}_K \cap \mathrm{S}_{C,\mathfrak{D}}) - \frac{2^N V\mathcal{H}^{2N}}{\sqrt{|\Delta_K|}N_{K/\mathbb{Q}}(\mathfrak{E})N_{k/\mathbb{Q}}(A)^2}\right| \leq c_1\frac{\mathcal{H}^{2N-1}}{N_{k/\mathbb{Q}}(A)^{2-1/N}}.$$

Proof. Using the injectivity of the map $\sigma(\cdot)$ and (8.21) we get

$$\begin{aligned}\#(C\mathcal{O}_K\mathfrak{D}\mathfrak{E}A\mathcal{O}_K \cap \mathrm{S}_{C,\mathfrak{D}}) &= \#\left(\sigma(C\mathcal{O}_K\mathfrak{D}\mathfrak{E}A\mathcal{O}_K) \cap \sigma(\mathrm{S}_{C,\mathfrak{D}})\right)\\ &= \#\left(\sigma(C\mathcal{O}_K\mathfrak{D}\mathfrak{E}A\mathcal{O}_K) \cap \sigma(C\mathcal{O}_K\mathfrak{D}) \cap S_F(\mathcal{I}^*;T)\right)\\ &= \#\left(\sigma(C\mathcal{O}_K\mathfrak{D}\mathfrak{E}A\mathcal{O}_K) \cap S_F(\mathcal{I}^*;T)\right).\end{aligned}$$

Combining Lemma 5.1 and (5.14) we see that $\partial(S_F(\mathcal{I}^*;T))$ is in $\mathrm{Lip}(2N, M, LT)$, and that $S_F(\mathcal{I}^*;T)$ does not contain the origin but is contained in the zero centred ball of radius LT. We apply Lemma 4.2 with $\Lambda = \sigma(C\mathcal{O}_K\mathfrak{D}\mathfrak{E}A\mathcal{O}_K)$, and we use (8.19) and (8.20). Since

$$N_{K/\mathbb{Q}}(\mathfrak{E}A\mathcal{O}_K) = N_{K/\mathbb{Q}}(\mathfrak{E})N_{k/\mathbb{Q}}(A)^2 \geq N_{k/\mathbb{Q}}(A)^2$$

the result drops out. □

Lemma 8.2. *Let $C \in \mathcal{R}_k$, $\mathfrak{D}|\mathcal{P}$, $\mathfrak{E}|\mathcal{P}$, and $\mathcal{H} \geq 2$. Then there exists a constant $c_2 = c_2(K)$ such that*

$$\left|\sum_{\substack{A\subsetneq\mathcal{O}_k\\(A,P_1\cdots P_s)=1}}\mu_k(A)\#(C\mathcal{O}_K\mathfrak{D}\mathfrak{E}A\mathcal{O}_K \cap \mathrm{S}_{C,\mathfrak{D}}) - \frac{2^N V\mathcal{H}^{2N}}{\sqrt{|\Delta_K|}N_{K/\mathbb{Q}}(\mathfrak{E})}\sum_{\substack{A\subsetneq\mathcal{O}_k\\(A,P_1\cdots P_s)=1}}\frac{\mu_k(A)}{N_{k/\mathbb{Q}}(A)^2}\right| \leq c_2\mathcal{H}^{2N-1}\mathcal{L},$$

where $\mathcal{L} = \log\mathcal{H}$ if $N = 1$ and $\mathcal{L} = 1$ if $N \geq 2$.

Proof. For $N \geq 2$ this follows immediately from Lemma 8.1. If $N = 1$ then we use that $C\mathcal{O}_K\mathfrak{D}\mathfrak{E}A\mathcal{O}_K \cap \mathrm{S}_{C,\mathfrak{D}}$ is empty whenever $N_{K/\mathbb{Q}}(\mathfrak{E}A\mathcal{O}_K) > \mathcal{H}$. In particular, we can restrict the sum to those A with $N_{k/\mathbb{Q}}(A) \leq \mathcal{H}$. Applying Lemma 8.1 yields the error term

$$\sum_{\substack{A\subsetneq\mathcal{O}_k\\(A,P_1\cdots P_s)=1\\N_{k/\mathbb{Q}}(A)\leq\mathcal{H}}} c_1\frac{\mathcal{H}}{N_{k/\mathbb{Q}}(A)} \ll_K \mathcal{H}\log\mathcal{H}.$$

Restricting the sum also introduces the additional error term

$$\left|\sum_{\substack{A\subsetneq\mathcal{O}_k\\(A,P_1\cdots P_s)=1\\N_{k/\mathbb{Q}}(A)>\mathcal{H}}}\frac{2^N V\mathcal{H}^2}{\sqrt{|\Delta_K|}N_{K/\mathbb{Q}}(\mathfrak{E})}\frac{\mu_k(A)}{N_{k/\mathbb{Q}}(A)^2}\right| \ll_K \mathcal{H}.$$

This completes the proof of Lemma 8.2. □

Using Lemma 7.6, and then plugging in the estimates from Lemma 8.1 and Lemma 8.2 yields

$$\#Z^*(C\mathcal{O}_K\mathfrak{D}) \cap \mathcal{S}_{C,\mathfrak{D}} = \sum_{\mathfrak{E}|\mathcal{P}} \frac{\mu_K(\mathfrak{E})2^N V\mathcal{H}^{2N}}{\sqrt{|\Delta_K|}N_{K/\mathbb{Q}}(\mathfrak{E})} \left(1 + \sum_{\substack{A\subsetneq\mathcal{O}_k \\ (A,P_1\cdots P_s)=1}} \frac{\mu_k(A)}{N_{k/\mathbb{Q}}(A)^2}\right) + O_K\left(\mathcal{H}^{2N-1}\mathcal{L}\right).$$

For the main term we observe that

$$\sum_{\mathfrak{E}|\mathcal{P}} \frac{\mu_K(\mathfrak{E})2^N V\mathcal{H}^{2N}}{\sqrt{|\Delta_K|}N_{K/\mathbb{Q}}(\mathfrak{E})} \left(1 + \sum_{\substack{A\subsetneq\mathcal{O}_k \\ (A,P_1\cdots P_s)=1}} \frac{\mu_k(A)}{N_{k/\mathbb{Q}}(A)^2}\right)$$
$$= \frac{2^N V\mathcal{H}^{2N}}{\sqrt{|\Delta_K|}} \left(\sum_{\mathfrak{E}|\mathcal{P}} \frac{\mu_K(\mathfrak{E})}{N_{K/\mathbb{Q}}(\mathfrak{E})}\right) \left(\sum_{\substack{A\subseteq\mathcal{O}_k \\ (A,P_1\cdots P_s)=1}} \frac{\mu_k(A)}{N_{k/\mathbb{Q}}(A)^2}\right).$$

Now using Lemma 6.9 and summing over the 2^s divisors $\mathfrak{D}|\mathcal{P}$, and then over $C \in \mathcal{R}_k$ we get

$$\mathcal{S}_K(\mathcal{H};\mathcal{I}) = \frac{h_k 2^{s+N} V\mathcal{H}^{2N}}{\sqrt{|\Delta_K|}} \left(\sum_{\mathfrak{E}|\mathcal{P}} \frac{\mu_K(\mathfrak{E})}{N_{K/\mathbb{Q}}(\mathfrak{E})}\right) \left(\sum_{\substack{A\subseteq\mathcal{O}_k \\ (A,P_1\cdots P_s)=1}} \frac{\mu_k(A)}{N_{k/\mathbb{Q}}(A)^2}\right) + O_K\left(2^s h_k \mathcal{H}^{2N-1}\mathcal{L}\right).$$

Using Lemma 7.7 and recalling that $D_{K/k}$ has exactly s prime ideal factors gives

$$2^s \left(\sum_{\mathfrak{E}|\mathcal{P}} \frac{\mu_K(\mathfrak{E})}{N_{K/\mathbb{Q}}(\mathfrak{E})}\right) \left(\sum_{\substack{A\subseteq\mathcal{O}_k \\ (A,P_1\cdots P_s)=1}} \frac{\mu_k(A)}{N_{k/\mathbb{Q}}(A)^2}\right) = \left(\prod_{P|D_{K/k}} \frac{2N_{k/\mathbb{Q}}(P)}{N_{k/\mathbb{Q}}(P)+1}\right) \frac{1}{\zeta_k(2)}.$$

Plugging in the value for V from Lemma 5.2, and using

$$|\Delta_K| = |\Delta_k|^2 N_{k/\mathbb{Q}}(D_{K/k})$$

(see [6, p.24]) shows that the leading constant of the main term is given by $A_K|\mathcal{I}|$. This completes the proof of Theorem 1.1.

9. Minimal heights in cosets of $k^\times$

In this section we generalise the previous CM-field setting. We assume throughout that K/k is an arbitrary quadratic extension of number fields.

Let $\tau : K \to K$ be the unique automorphism that fixes k, so that $\mathrm{Gal}(K/k) = \langle\tau\rangle$, and $N_{K/k}(\alpha) = \alpha\tau(\alpha)$. As in Section 2 we let $\psi : K^\times \to K^\times$ be the group homomorphism defined by

$$\psi(\beta) = \frac{\beta}{\tau(\beta)},$$

so that $\ker \psi = k^\times$. We write $\mathcal{S}_{K/k}$ for the kernel of the norm map $N_{K/k}$. Hence, Hilbert's Theorem 90 implies $\operatorname{Im} \psi = \mathcal{S}_{K/k}$, and we get an induced isomorphism

$$\hat{\psi} : K^\times/k^\times \to \mathcal{S}_{K/k}. \tag{9.22}$$

We will determine elements of minimal height for those cosets of $k^\times$ in $K^\times$ that intersect $\mathcal{S}_{K/k}$.

Lemma 9.1. *If α belongs to $\mathcal{S}_{K/k}$ then the inequality*

$$H(\alpha) \leq H(\alpha\gamma) \tag{9.23}$$

holds for each γ in $k^\times$. In particular, the minimum value of the Weil height on elements of the multiplicative coset $\alpha k^\times$ is given by

$$\min\{H(\alpha\gamma) : \gamma \in k^\times\} = H(\alpha).$$

Proof. Assume that α is in $\mathcal{S}_{K/k}$ and γ is in $k^\times$. The automorphism τ preserves the height of points in $K^\times$. Therefore $\alpha\gamma$ and

$$\tau(\alpha\gamma) = \tau(\alpha)\tau(\gamma) = \tau(\alpha)\gamma = \alpha^{-1}\gamma$$

have the same height. Similarly, $\alpha^{-1}\gamma$ and

$$(\alpha^{-1}\gamma)^{-1} = \alpha\gamma^{-1}$$

have the same height. That is, the three elements

$$\alpha\gamma, \quad \alpha^{-1}\gamma, \quad \text{and} \quad \alpha\gamma^{-1},$$

satisfy the identity

$$H(\alpha\gamma) = H(\alpha^{-1}\gamma) = H(\alpha\gamma^{-1}).$$

Now by well known properties of the height we get

$$\begin{aligned} H(\alpha)^2 = H(\alpha^2) &= H((\alpha\gamma)(\alpha\gamma^{-1})) \\ &\leq H(\alpha\gamma)H(\alpha\gamma^{-1}) = H(\alpha\gamma)^2. \end{aligned}$$

This verifies the inequality (9.23). □

Consider the inverse of the isomorphism (9.22)

$$\hat{\psi}^{-1} : \mathcal{S}_{K/k} \to K^\times/k^\times.$$

Lemma 9.1 raises the following question. Which elements of $\mathcal{S}_{K/k}$ are mapped under $\hat{\psi}^{-1}$ to cosets that intersect $\mathcal{S}_{K/k}$? This question is answered by Lemma 9.3 which follows easily from the following simple observation.

Lemma 9.2. *An element $\alpha \in K^\times$ lies in $\mathcal{S}_{K/k}$ if and only if $\psi(\alpha) = \alpha^2$.*

Proof. Since $\psi^2(\beta) = \psi(\beta)^2$ for any $\beta \in K^\times$ we get $\psi(\alpha) = \alpha^2$ whenever $\alpha \in \mathcal{S}_{K/k}$. And if $\psi(\alpha) = \alpha^2$ then $\alpha\tau(\alpha) = 1$, and thus $\alpha \in \mathcal{S}_{K/k}$. This proves the lemma. □

Lemma 9.3. *A coset of $k^\times$ in $K^\times$ intersects $\mathcal{S}_{K/k}$ if and only if it is the image of a square in $\mathcal{S}_{K/k}$ under the isomorphism $\hat{\psi}^{-1}$.*

Proof. First suppose $\beta \in \mathcal{S}_{K/k}$. Then $\psi(\beta) = \beta^2$ by Lemma 9.2, and we get

$$\hat{\psi}^{-1}(\beta^2) = \hat{\psi}^{-1}(\psi(\beta)) = \beta k^{\times},$$

proving that the image of a square is a coset that intersects $\mathcal{S}_{K/k}$.

Next suppose that the image $\beta k^{\times}$ intersects $\mathcal{S}_{K/k}$. We can assume $\beta \in \mathcal{S}_{K/k}$, and thus $\psi(\beta) = \beta^2$ by Lemma 9.2. We conclude

$$\beta k^{\times} = \hat{\psi}^{-1}(\psi(\beta)) = \hat{\psi}^{-1}(\beta^2),$$

which proves the other direction. □

REFERENCES

[1] V. V. Batyrev and Y. Tschinkel, *Rational points of bounded height on compactifications of anisotropic tori*, Internat. Math. Res. Notices (1995), no. 12, 591–635.

[2] V. V. Batyrev and Y. Tschinkel, *Manin's conjecture for toric varieties*, J. Algebraic Geom. **7** (1998), no. 1, 15–53.

[3] P. E. Blanksby and J. H. Loxton, *A note on the characterization of CM-fields*, J. Austral. Math. Soc. (Series A) **26** (1978), 26–30.

[4] E. Bombieri and W. Gubler, *"Heights in Diophantine Geometry"*, Cambridge University Press, 2006.

[5] A. Brandis, *Über die multiplikative Struktur von Körpererweiterungen*, Math. Z. (1965), 71–73.

[6] S. Lang, *"Algebraic Number Theory"*, Springer, 1994.

[7] J. Lawrence, *Countable abelian groups with a discrete norm are free*, Proc. Amer. Math. Soc. **297** (1984), 352–354.

[8] D. W. Masser and J. D. Vaaler, *Counting algebraic numbers with large height II*, Trans. Amer. Math. Soc. **359** (2007), 427–445.

[9] K. Petersen and C. Sinclair, *Equidistribution of algebraic numbers of norm one in quadratic number fields*, Int. J. Number Theory **7** (2011), no. 7, 1841–1861.

[10] E. Peyre, *Hauteurs et mesures de Tamagawa sur les variétés de Fano*, Duke Math. J. **79** (1995), no. 1, 101–218.

[11] G. Shimura, *"Abelian varieties with complex multiplication and modular functions"*, Princeton University Press, Princeton, NJ, 1998.

[12] P. G. Spain, *Lipschitz: A new version of an old principle*, Bull. London Math. Soc. **27** (1995), no. 6, 565–566.

[13] J. Steprāns, *A characterization of free abelian groups*, Proc. Amer. Math. Soc. **93** (1985), 347–349.

[14] M. Widmer, *Counting primitive points of bounded height*, Trans. Amer. Math. Soc. **362** (2010), 4793–4829.

[15] M. Widmer, *Weakly admissible lattices, primitive points, diophantine approximation, and o-minimality*, Mathematika **64** (2018), no. 2, 475–496.

[16] F. Zorzitto, *Discretely normed abelian groups*, Aequationes Math. **29** (1985), 172–174.

DEPARTMENT OF MATHEMATICS, PENNSYLVANIA STATE UNIVERSITY, UNIVERSITY PARK, PA 16802 USA

Email address: akhtari@psu.edu

DEPARTMENT OF MATHEMATICS, UNIVERSITY OF TEXAS, AUSTIN, TX 78712 USA

Email address: vaaler@math.utexas.edu

GRAZ UNIVERSITY OF TECHNOLOGY, INSTITUTE OF ANALYSIS AND NUMBER THEORY, STEYRERGASSE 30/II, 8010 GRAZ, AUSTRIA

Email address: martin.widmer@tugraz.at