INTEGRAL POINTS OF FIXED DEGREE AND BOUNDED HEIGHT

MARTIN WIDMER

ABSTRACT. By Northcott's Theorem there are only finitely many algebraic points in affine n-space of fixed degree e over a given number field and of height at most X. Finding the asymptotics for these cardinalities as X becomes large is a long standing problem which is solved only for $e = 1$ by Schanuel, for $n = 1$ by Masser and Vaaler, and for n "large enough" by Schmidt, Gao, and the author. In this paper we study the case where the coordinates of the points are restricted to algebraic integers, and we derive the analogues of Schanuel's, Schmidt's, Gao's and the author's results. The proof invokes tools from dynamics on homogeneous spaces, algebraic number theory, geometry of numbers, and a geometric partition method due to Schmidt.

1. INTRODUCTION

In this article we count algebraic points of bounded Weil height with integral coordinates, generating an extension of given degree over a fixed number field.

Let k be a number field, let $\overline{k}$ be an algebraic closure of k, and let H be the absolute multiplicative (affine) Weil height on $\overline{k}^n$ (for the definition see (1.4) below). One of the most fundamental and important properties of the height asserts that subsets of $\overline{k}^n$ of uniformly bounded height and degree are finite. This result was shown by Northcott [20] in 1950, and his proof provides explicit upper bounds. However, for big n these estimates are rather poor, and even nowadays, the correct order of magnitude is known only in some special cases.

In 1962 Lang [15] proposed the problem of asymptotically counting points of bounded height in a fixed number field, i.e., to count points in $\overline{k}^n$ of degree 1 over k. This problem has been solved by Schanuel [22] in 1964, with a detailed proof [23] published 15 years later. The problem of counting points of bounded height and of fixed degree $e > 1$ over a given number field k appears to be much more difficult. Indeed, it took over 40 years before the first significant improvement of Northcott's Theorem was established. In 1991 Schmidt [24] obtained upper bounds that greatly improved upon Northcott's bounds. However, when the degree and the dimension are both bigger than 1 Schmidt's bounds are still significantly larger than what one expects. Later, in [25] Schmidt established the asymptotics for points quadratic over $\mathbb{Q}$, and this in all dimensions n. This in turn yield new results on a generalized version of Manin's conjecture (the special case $n = 2$ provides one of the rare examples of a cubic four fold for which the Batyrev-Manin conjecture is established and, as observed by Le Rudulier [17], leads to a counterexample to Peyre's predicted constant). Soon afterwards Gao [14] gave asymptotics for points in n dimensions of degree e over $\mathbb{Q}$, subject to the constraint $n > e$. The case $n = 1$ was treated by Masser and Vaaler in [18], and was generalized in [19] by the same authors to allow arbitrary ground fields k. The author [30] has established asymptotic estimates for points in n dimensions of fixed degree e over an arbitrary number field, provided

Date: August 12, 2015.
2010 *Mathematics Subject Classification.* Primary 11R04; Secondary 11G50, 11G35.
Key words and phrases. Heights, integral points, algebraic integers, Northcott's Theorem, counting, lattice points, flows on homogeneous spaces, Pisot numbers.

$n > 5e/2 + 5$. A short survey on counting points of fixed degree is given in Section 4 of Bombieri's article [5].

Regarding integral points of fixed degree $e > 1$ the subject is less developed. For a number field k let us write $N(\mathcal{O}_k(n;e), X)$ for the number of points $\boldsymbol{\alpha} = (\alpha_1, \ldots, \alpha_n)$ of absolute multiplicative Weil height no larger than X, whose coordinates are algebraic integers with $[k(\alpha_1, \ldots, \alpha_n) : k] = e$. In [16, p.81] Lang has stated without proof

$$N(\mathcal{O}_k(1;1), X) = \gamma_k X^m (\log X)^{q_k} + O(X^m (\log X)^{q_k - 1}). \tag{1.1}$$

Here $m = [k : \mathbb{Q}]$, q_k is the rank of the group of units and γ_k is an unspecified positive constant depending on k. The formula (1.1) can easily be deduced from a counting principle of Davenport [11], but it is not a straightforward application of counting lattice points in homogeneously expanding domains (cf. [16, p.81]). The asymptotics for $N(\mathcal{O}_k(n;1), X)$ can also be obtained from [8, Theorem 3.11.3]. Regarding higher degrees Chern and Vaaler [9] proved asymptotic estimates for the number of monic polynomials of fixed degree with rational integral coefficients and bounded Mahler measure. As these estimates are of polynomial growth, and since the Mahler measure is multiplicative, one can easily see that the reducible polynomials do not effect the asymptotics. Thus Chern and Vaaler's result implies asymptotics for $N(\mathcal{O}_{\mathbb{Q}}(1;e), X)$. More precisely, their Theorem 6 yields

$$N(\mathcal{O}_{\mathbb{Q}}(1;e), X) = c_e X^{e^2} + O(X^{e^2 - 1}), \tag{1.2}$$

with a positive and explicit constant c_e depending on e. Very recently, Barroero [1] has generalized (1.2) to arbitrary ground fields k, and then further generalized this to S-integers [2]. Barroero's approach follows the one in [19] of counting polynomials of degree e. This strategy is more straightforward and easier than ours but, unfortunately, works only for $n = 1$.

One of our goals here is to deduce statements about points with integral coordinates analogous to the results of Schanuel, Schmidt, Gao, and the author alluded to above. This is the first attempt to prove asymptotic estimates for $N(\mathcal{O}_k(n;e), X)$ with the exception of the special cases $e = 1$ or $n = 1$.

Another new aspect of this article is that our methods allow us to prove a multi-term expansion of $N(\mathcal{O}_k(n;e), X)$. For instance, we are able to find the first $q_k + 1$ leading terms in (1.1), and an error term of order $X^{m-1}(\log X)^{q_k}$. This is in contrast to the results on points of fixed degree, mentioned in the previous paragraph. The $q_k + 1$ different main terms of decreasing order have a simple geometric interpretation which we shall explain later in Section 2. The main terms can be expressed using Laguerre polynomials, e.g.,

$$N(\mathcal{O}_k(n;1), X) = B_k^n X^{mn} L_{q_k}(-\log X^{mn}) + O(X^{mn-1}(\log X)^{q_k}). \tag{1.3}$$

Here $L_{q_k}(x)$ is the q_k-th Laguerre polynomial, and B_k is a field invariant defined later on. The somewhat unexpected appearance of the Laguerre polynomial in the main term is another new feature of our result.

It is typical with these types of asymptotic expansions for the main term to be of the form $X^a P(\log X)$ for some polynomial $P(x)$. This polynomial is often obtained via a meromorphic continuation of the corresponding height zeta function and a suitable Tauberian theorem; see, e.g., Franke, Manin, and Tschinkel's pioneering article [13, Corollary] for the case of rational points on Flag manifolds V. In their case the degree $\deg P$ is also related to the rank of a group, more precisely, $\deg P$ is the rank of the Picard group $\mathrm{Pic}(V)$ minus 1[1]. Franke, Manin, and Tschinkel obtained their result

[1]There is a misprint in their Corollary, t should read $t - 1$.

by expressing the corresponding height zeta function as an Eisenstein series and then using Langland's work to study its analytic properties. Similar, technically intricate, methods have been used in [7] and [8]. Our proof makes no use of complex analysis. Indeed, we reverse the situation here, and we say something about the analytic properties of the height zeta function $\zeta_{k,n,e}(s) = \sum_{\boldsymbol{\alpha}\in\mathcal{O}_k(n;e)} H(\boldsymbol{\alpha})^{-s}$ using our estimates for $N(\mathcal{O}_k(n;e), X)$.

To state our first result we need some notation. Let $K \subset \overline{k}$ be a number field, write $d = [K : \mathbb{Q}]$ for its degree, and let M_K denote the set of places of K. For each place v we choose the unique representative $|\cdot|_v$ that either extends the usual Archimedean absolute value on $\mathbb{Q}$ or a usual p-adic absolute value on $\mathbb{Q}$. Let K_v be the completion of K with respect to v, and let $\mathbb{Q}_v$ the completion with respect to the place of $\mathbb{Q}$ below v, and write $d_v = [K_v : \mathbb{Q}_v]$ for the local degree at v. For a point $\boldsymbol{\alpha} \in K^n$ we define the absolute multiplicative (affine) Weil height of $\boldsymbol{\alpha}$ as

$$H(\boldsymbol{\alpha}) = \prod_{v\in M_K} \max\{1, |\alpha_1|_v, \ldots, |\alpha_n|_v\}^{\frac{d_v}{d}}. \tag{1.4}$$

As is well-known $H(\boldsymbol{\alpha})$ is independent of the number field K containing the coordinates α_i, and hence $H(\cdot)$ defines a genuine function on $\overline{k}^n$.

For a subset S of $\overline{k}^n$ of uniformly bounded degree and real numbers $X \geq 1$ we define the counting function

$$N(S, X) = |\{\boldsymbol{\alpha} \in S; H(\boldsymbol{\alpha}) \leq X\}|.$$

Thanks to Northcott's Theorem the quantity above is finite for each X. For positive rational integers e and n we define the set of integral points in n dimensions of degree e over the field k

$$\mathcal{O}_k(n;e) = \{\boldsymbol{\alpha} \in \mathcal{O}_{\overline{k}}^n; [k(\boldsymbol{\alpha}) : k] = e\}.$$

Here $\mathcal{O}_{\overline{k}} \subset \overline{k}$ denotes the ring of algebraic integers, and $k(\boldsymbol{\alpha}) = k(\alpha_1, \ldots, \alpha_n)$. Let $\mathcal{C}_e(k)$ be the collection of all field extensions of k of degree e, i.e.,

$$\mathcal{C}_e(k) = \{K \subset \overline{k}; [K : k] = e\}.$$

For a number field K we write Δ_K for the discriminant of K, r_K for the number of real, s_K for the number of pairs of complex conjugate embeddings of K, and $q_K = r_K + s_K - 1$ for the rank of the group of units. Moreover, we set

$$t_e(k) = \sup\{q_K; K \in \mathcal{C}_e(k)\} = e(q_k + 1) - 1,$$
$$B_K = \frac{2^{r_K}(2\pi)^{s_K}}{\sqrt{|\Delta_K|}},$$

and for $0 \leq i \leq t_e(k)$ we introduce the formal sum

$$D_i = D_i(k, n, e) = \sum_{\substack{K\in\mathcal{C}_e(k)\\ q_K\geq i}} \frac{B_K^n}{i!}\binom{q_K}{i}. \tag{1.5}$$

For $e > 1$ we define

$$C_{e,m} = \max\{2 + \frac{4}{e-1} + \frac{1}{m(e-1)}, 7 - \frac{e}{2} + \frac{2}{me}\} \leq 7.$$

Finally, we put $\log^+ X = \max\{1, \log X\}$. Now we can state our first result.

Theorem 1.1. *Let k be a number field and $m = [k : \mathbb{Q}]$. Suppose that either $e = 1$ or that $n > e + C_{e,m}$, and set $t = t_e(k)$. Then the sums in (1.5) converge, and for $X \geq 1$ we have*

$$\left| N(\mathcal{O}_k(n;e), X) - \sum_{i=0}^{t} D_i X^{men} (\log X^{men})^i \right| \leq c_1 X^{men-1} (\log^+ X)^t \tag{1.6}$$

for some positive constant $c_1 = c_1(n, m, e)$ depending only on n, m and e.

We remark that the sum in (1.6) can be written as the weighted sum of Laguerre polynomials $X^{men} \sum_q \beta_q L_q(-\log X^{men})$. Here q runs over the finite set $\{q_K; K \in \mathcal{C}_e(k)\}$, and $\beta_q = \beta_q(k, e, n) = \sum_K B_K^n$, where the sum is taken over all $K \in \mathcal{C}_k(e)$ with $q_K = q$.

Note that for $e \geq 9$ the condition $n > e + C_{e,m}$ is equivalent to $n > e + 2$. Unfortunately, this is probably not the sharp bound. However, as $N(\mathcal{O}_k(1;e), X) \leq N(\mathcal{O}_k(n;e), X)$ we see by comparing with (1.2) that if $m = 1$ then (1.6) cannot hold for $n < e$. Borrowing ideas of Masser and Vaaler from [19], Theorem 1.1, combined with standard estimates for the Mahler measure, shows that $N(\mathcal{O}_k(1;e), X) \gg X^{me^2} (\log X)^{q_k}$. Hence, (1.6) cannot hold for $n < e$, even if $m > 1$. Note also that for $e = n = 2$ the sums in (1.5) diverge.

Next let us choose $e = 1$. Then we get the formula (1.3) which is a new result, even for $n = 1$. Here the multi-term expansion could probably be worked out from the results in [7], but it is unlikely that the same error term can be obtained.

It is probably not too difficult to extend our theorem to the context of Lipschitz heights as in [19] or even adelic Lipschitz heights as in [30]. These generalizations would have further applications such as refined asymptotic estimates for $N(\mathcal{O}_k(1;e), X)$, improving upon Barroero's result, or for the number of integral solutions of fixed degree to a system of linear equations, analogous to the main result in [31]. However, to keep the technical difficulties and the required notation at a minimal level, and to emphasize the main ideas and novelties of this work, we decided not to include these generalizations.

Let us formally define the height zeta function of $\mathcal{O}_k(n;e)$ as

$$\zeta_{k,n,e}(s) = \sum_{\boldsymbol{\alpha} \in \mathcal{O}_k(n;e)} H(\boldsymbol{\alpha})^{-s}.$$

The upper bound of order $X^{men} (\log X)^t$ implies that $\zeta_{k,n,e}(s)$ converges in the complex half plane $\Re(s) > men$. But Theorem 1.1 implies also that $\zeta_{k,n,e}(s)$ has a meromorphic continuation to $\Re(s) > men - 1$ with a pole at $s = men$ of order $t + 1$. More precisely, setting $D_{t+1} = 0$, and using summation by parts, we find that the principal part of the Laurent series at $s = men$ is given by

$$\sum_{i=1}^{t+1} \frac{(men)^i (i-1)! (D_{i-1} + i D_i)}{(s - men)^i}.$$

Theorem 1.1 will be proved via our main result Theorem 2.1 which we present in the next section.

2. THE MAIN RESULT

Suppose K is a field extension of k of degree $e = [K : k]$, and put $[K : \mathbb{Q}] = d$, so that $d = em$. We denote by $\sigma_1, \ldots, \sigma_d$ the embeddings from K to $\mathbb{R}$ or $\mathbb{C}$ respectively, ordered such that $\sigma_{r+s+i} = \overline{\sigma}_{r+i}$ for $1 \leq i \leq s$, i.e., σ_{r+s+i} and σ_{r+i} are complex conjugate. Let $\mathcal{O}$ be a submodule of the free $\mathbb{Z}$-module $\mathcal{O}_K$ of full rank. Let $\mathfrak{A}_{\mathcal{O}}$ be the smallest ideal in $\mathcal{O}_K$ that contains $\mathcal{O}$, i.e., $\mathfrak{A}_{\mathcal{O}}$ is the intersection over all ideals in $\mathcal{O}_K$ that contain $\mathcal{O}$. Set

$$\eta_{\mathcal{O}} = \mathfrak{N}(\mathfrak{A}_{\mathcal{O}})^{1/d} \geq 1, \tag{2.1}$$

where $\mathfrak{N}(\mathfrak{A}) = |\mathcal{O}_K/\mathfrak{A}|$ denotes the norm of a nonzero ideal $\mathfrak{A}$ of $\mathcal{O}_K$. Furthermore, we define

$$G(K/k) = \{[K_0 : k]; k \subset K_0 \subsetneq K\}$$

if $K \neq k$, and we put

$$G(K/k) = \{1\}$$

if $K = k$. Then for an integer $g \in G(K/k)$ we define

$$\delta_g(K/k) = \inf\{H(\alpha, \beta); k(\alpha, \beta) = K, [k(\alpha) : k] = g\},$$

and we set

$$\mu_g = mn(e - g) - 1. \tag{2.2}$$

We remark that $\delta_g(K/k)$ refines the invariant $\delta(K)$ introduced by Roy and Thunder [21]. For a point $\boldsymbol{\alpha} \in \overline{k}^n \backslash \{\mathbf{0}\}$ we write $k(\ldots, \alpha_i/\alpha_j, \ldots)$ for the extension of k generated by all possible ratios α_i/α_j $(1 \leq i, j \leq n, \alpha_j \neq 0)$ of the coordinates of $\boldsymbol{\alpha}$. Next we introduce the set of "projectively primitive" points in $\mathcal{O}^n$

$$\mathcal{O}^n(K/k) = \{\boldsymbol{\alpha} \in \mathcal{O}^n \backslash \{\mathbf{0}\}; K = k(\ldots, \alpha_i/\alpha_j, \ldots)\}.$$

Note that for $n = 1$ the set $\mathcal{O}^n(K/k)$ is empty if $K \neq k$ and equals $\mathcal{O}\backslash\{0\}$ if $K = k$. For a subset $I \subset \{1, \ldots, r_K + s_K\}$ and $I^c = \{1, \ldots, r_K + s_K\}\backslash I$ we define

$$\mathcal{O}_I^n(K/k) = \{\boldsymbol{\alpha} \in \mathcal{O}^n(K/k); |\sigma_i(\boldsymbol{\alpha})|_\infty \geq 1 \text{ for } i \in I, \text{ and } |\sigma_i(\boldsymbol{\alpha})|_\infty < 1 \text{ for } i \in I^c\},$$

where $|\sigma_i(\boldsymbol{\alpha})|_\infty = \max\{|\sigma_i(\alpha_1)|, \ldots, |\sigma_i(\alpha_n)|\}$. Finally, let $Z_I(T)$ be the measurable set in Euclidean space, defined in (5.1), and set $q' = |I| - 1$. In Section 16 we will show that for $X \geq 1$

$$\text{Vol} Z_I(X^d) = (2^{r_K}\pi^{s_K})^n(-1)^{q'}\left(-1 + X^{dn}\sum_{i=0}^{q'}\frac{(-\log X^{dn})^i}{i!}\right).$$

Recall that K/k is an extension of number fields and $d = [K : \mathbb{Q}]$. We can now state the main result of this article. All our results will be deduced from this theorem.

Theorem 2.1. *Suppose $q' = |I| - 1 \geq 0$, $X \geq 1$ and either $n > 1$ or $K = k$. Then*

$$\left|N(\mathcal{O}_I^n(K/k), X) - \frac{2^{s_K n}\text{Vol} Z_I(X^d)}{(\sqrt{|\Delta_K|}[\mathcal{O}_K : \mathcal{O}])^n}\right| \leq c_2 \sum_{g \in G(K/k)} \frac{X^{dn-1}(\log^+ X)^{q'}}{\eta_{\mathcal{O}}^{dn-1}\delta_g(K/k)^{\mu_g}},$$

where $c_2 = c_2(n, d)$ is a positive constant depending only on n and d.

Using $P_{q'}(x) = \sum_{i=0}^{q'} \frac{x^i}{i!}$ we can rewrite the main term as

$$\left(\frac{B_K}{[\mathcal{O}_K : \mathcal{O}]}\right)^n (-1)^{q'}\left(X^{dn}P_{q'}(-\log X^{dn}) - 1\right).$$

Note that this expression depends only on the cardinality of I but not on the particular choice of I itself. Next let us consider some special cases. We start with the case $K = k$, i.e., $d = m$. Then the statement takes the form

$$\left|N(\mathcal{O}_I^n(k/k), X) - \frac{2^{s_k n}\text{Vol} Z_I(X^m)}{(\sqrt{|\Delta_k|}[\mathcal{O}_k : \mathcal{O}])^n}\right| \leq c_2(n, m)\frac{X^{mn-1}(\log^+ X)^{q'}}{\eta_{\mathcal{O}}^{mn-1}}.$$

Now we take $n = 1$, $\mathcal{O} = \mathcal{O}_k$, and let us assume $r_k \geq 1$. If we choose $I = \{1\}$ and assume $m > 1$, then $N(\mathcal{O}_I^n(k/k), X) = N(\mathcal{O}_I, X)$ counts the primitive Pisot numbers in the real field $\sigma_1(k)$. Here the primitivity is induced by the choice of the set I. The non-primitive Pisot numbers lie in a strict subfield of $\sigma_1(k)$, and so their number has order of magnitude at most $X^{m/2}$. Thus for the total number of Pisot numbers in $\sigma_1(k)$ of height no larger than X we get

$$B_k X^m + O(X^{m-1}).$$

Still with $K = k$, $\mathcal{O} = \mathcal{O}_k$, and $n = 1$ we now take $I = \{1, \ldots, r_k + s_k\}$. Then we are counting the nonzero elements $\alpha \in \mathcal{O}_k$ with $H(\alpha) = |Nm_{k/\mathbb{Q}}(\alpha)|^{1/m} \leq X$. Their number is given by

$$\sum_{i=0}^{q_k} (-1)^{q_k} B_k X^m \frac{(-\log X^m)^i}{i!} + O(X^{m-1}(\log^+ X)^{q_k}).$$

Next note that

$$\mathcal{O}^n(K/k) = \cup_I \mathcal{O}_I^n(K/k), \tag{2.3}$$

taken over all non-empty subsets of I of $\{1, \ldots, r_K + s_K\}$, is a disjoint union. Thus we may sum the estimate in Theorem 2.1 over all non-empty sets I to get estimates for the counting function of $\mathcal{O}^n(K/k)$. We even get a geometric interpretation of the main terms. The highest order main term comes from the points in $\mathcal{O}_I^n(K/k)$ with maximal I, i.e., points satisfying $|\sigma_i(\boldsymbol{\alpha})|_\infty \geq 1$ for all i. For the second order main term there is a negative contribution from $\mathcal{O}_I^n(K/k)$ with maximal I and a positive contribution for each $\mathcal{O}_I^n(K/k)$ with $|I| = r_K + s_K - 1$, and so forth.

Let $Z(T) = \cup_I Z_I(T)$, where this time I runs over all subsets of $\{1, \ldots, r_K + s_K\}$, and again this is a disjoint union. In Section 16 we will show that for $X \geq 1$

$$\text{Vol}Z(X^d) = (2^{r_K}\pi^{s_K})^n X^{dn} \sum_{i=0}^{q_K} \frac{(\log X^{dn})^i}{i!}\binom{q_K}{i} = (2^{r_K}\pi^{s_K})^n X^{dn} L_{q_K}(-\log X^{dn}).$$

As $\mathcal{O}_\emptyset^n(K/k) = \emptyset$ we see that the union in (2.3) taken over all subsets remains equals $\mathcal{O}^n(K/k)$. In Section 15 we show that Theorem 2.1 remains valid for $I = \emptyset$, provided $(\log^+ X)^{q'}$ in the error term is replaced by 1. From this and Theorem 2.1 we may deduce the following result.

Corollary 2.1. *Suppose $X \geq 1$ and either $n > 1$ or $K = k$. Then*

$$\left| N(\mathcal{O}^n(K/k), X) - \frac{2^{s_K n}\text{Vol}Z(X^d)}{(\sqrt{|\Delta_K|}[\mathcal{O}_K : \mathcal{O}])^n} \right| \leq c_3 \sum_{g \in G(K/k)} \frac{X^{dn-1}(\log^+ X)^{q_K}}{\eta_{\mathcal{O}}^{dn-1}\delta_g(K/k)^{\mu_g}},$$

where $c_3 = c_3(n, d)$ is a positive constant depending only on n and d.

Note that here, opposed to in Theorem 2.1, all main terms are positive. Let us briefly explain the strategy of the proof of Theorem 1.1. To this end we define the set of "non-projectively primitive" points in $\mathcal{O}_K^n$

$$\mathcal{O}_{npp}^n(K/k) = \{\boldsymbol{\alpha} \in \mathcal{O}_K^n \backslash \mathcal{O}_K^n(K/k); k(\boldsymbol{\alpha}) = K\}.$$

Now any $\boldsymbol{\alpha}$ in $\mathcal{O}_k(e, n)$ lies either in $\mathcal{O}_K^n(K/k)$ or in $\mathcal{O}_{npp}^n(K/k)$, with $K = k(\boldsymbol{\alpha}) \in \mathcal{C}_e(k)$. Hence we have the following disjoint union

$$\mathcal{O}_k(e, n) = \bigcup_{\mathcal{C}_e(k)} \mathcal{O}_K^n(K/k) \cup \mathcal{O}_{npp}^n(K/k).$$

Therefore, we just have to sum $N(\mathcal{O}_K^n(K/k), X)$ and $N(\mathcal{O}_{npp}^n(K/k), X)$ over all K in $\mathcal{C}_e(k)$. And indeed, we will show that the sum over all main terms as well as the sum over all error terms of $N(\mathcal{O}_K^n(K/k), X)$ converges, provided $n > e + C_{e,m}$, while the sum over $N(\mathcal{O}_{npp}^n(K/k), X)$ has smaller order of magnitude.

It now is obvious that a crucially important feature of Corollary 2.1 (and so of Theorem 2.1) is the good dependence of the error term on the extension K/k; note that by Northcott's Theorem $\delta_g(K/k)^{-\mu_g}$ tends to zero as K runs over the subset $\mathcal{C}_e^{(g)}(k)$ of those $K \in \mathcal{C}_e(k)$ with $g \in G(K/k)$. To compare with the discriminant we can apply a well-known inequality of Silverman [27, Theorem 2] to get $\delta_g(K/k) \geq c_k|\Delta_K|^{1/(2me(e-1))}$ for some positive constant c_k.

Unfortunately, bounding the number of extensions K/k of fixed degree e and bounded discriminant is a difficult problem, satisfactorily solved only for $e \leq 5$, thanks to the deep work of Datskowsky and Wright [10], and Bhargava [3, 4]. We surmount this impasse by deviating from the standard route and working with the new invariant $\delta_g(K/k)$ instead of the classical discriminant. As it turns out we have almost sharp bounds for the number of fields $K \in \mathcal{C}_e^{(g)}(k)$ with $\delta_g(K/k) \leq T$, opposed to the case when we enumerate by the discriminant. Furthermore, as larger g gets, which means as larger the error terms get, the better our upper bounds for the number of $K \in \mathcal{C}_e^{(g)}(k)$ with $\delta_g(K/k) \leq T$ become. These observations have already been used in [30].

Our method leads also to asymptotics for more specific sets, e.g., points $\boldsymbol{\alpha}$ of degree d whose coordinates are primitive Pisot numbers of $\mathbb{Q}(\boldsymbol{\alpha})$, provided $n > d + C_{e,m} + 1$. Here the "+1" is required to exclude the points with some coordinates equal zero.

The special case $K = k$ in Corollary 2.1 yields a generalization of (1.3) (to arbitrary submodules of $\mathcal{O}_k$ of full rank) with a more precise error term. We have

$$\left| N(\mathcal{O}^n \backslash \{\mathbf{0}\}, X) - \frac{2^{s_k n} \mathrm{Vol} Z(X^m)}{(\sqrt{|\Delta_k|}[\mathcal{O}_k : \mathcal{O}])^n} \right| \leq c_3(n,m) \left(\frac{X}{\eta_{\mathcal{O}}}\right)^{mn-1} (\log^+ X)^{q_k}. \tag{2.4}$$

Now let us choose $\mathcal{O} = \mathfrak{A}$ for a nonzero ideal $\mathfrak{A}$. Then we have $\eta_{\mathcal{O}} = \mathfrak{N}(\mathfrak{A})^{1/m}$. This allows one to carry out a Möbius inversion to count $\boldsymbol{\alpha} \in \mathfrak{A}^n$ satisfying another type of primitivity, namely $\alpha_1\mathcal{O}_k + \cdots + \alpha_n\mathcal{O}_k = \mathfrak{A}$. Here we need $n \geq 2$ to get for the number of such $\boldsymbol{\alpha}$

$$\frac{2^{s_k n} \mathrm{Vol} Z(X^m)}{\zeta_k(n)(\sqrt{|\Delta_k|}\mathfrak{N}(\mathfrak{A}))^n} + O\left(\frac{X^{mn-1}(\log^+ X)^{\overline{q}}}{\mathfrak{N}(\mathfrak{A})^{n-1/m}}\right),$$

where $\overline{q} = q_k$ if $(n,m) \neq (2,1)$ and $\overline{q} = 1$ if $(n,m) = (2,1)$.

3. Techniques and plan of the paper

The paper is organized as follows. We start with a section on elementary counting principles. Here we recall and provide some basic results on counting lattice points. Then in Section 5 we state a precise estimate (Theorem 5.1) of the quantity $|\Lambda \cap Z_I(T)|$, for lattices Λ that have a bounded orbit under the flow induced by a certain subgroup $\mathcal{T}$ of the diagonal endomorphisms with determinant 1.

In Section 6 we introduce some notation and state some simple properties of the sets $Z_I(T)$ and $Z(T)$ which are required for the proof of Theorem 5.1.

Skriganov [28, 29] obtained very good estimates for the number of lattice points inside aligned boxes, provided the lattice orbit under the above mentioned flow is bounded. However, our set $Z_I(T)$ has hyperbolic spikes and is far away from box-shaped. To overcome this hurdle we adapt a geometric partition method that goes back to Schmidt [25], and combine it with tools from dynamics on homogeneous spaces. An extensions of Schmidt's partition method is applied in Section 7 and Section 8. To apply the simple counting principles we still have to check some technical conditions such as the Lipschitz parameterizability of the boundary, and this is done in Section 9. In Section 10 we are finally in position to apply the elementary counting principles, and we can conclude the proof of Theorem 5.1.

The most important aspect of Theorem 2.1 is the good error term, in particular, with respect to the extension K/k. This particular feature imposes serious additional challenges. Instead of the boundedness of the orbit of Λ under the flow of $\mathcal{T}$ we have to prove that the orbit of Λ (scaled to have determinant 1) lies in a certain subset of the space of lattices $SL_{dn}(\mathbb{R})/SL_{dn}(\mathbb{Z})$ which is defined in terms of the higher successive minima and involves a critical successive minimum λ_I. To show that this condition implies the desired error term we need to utilize the machinery developed in [32]. However, the latter can only be applied to the set $\mathcal{O}_K^n(K/k)$ of projectively primitive points, and this is exactly why we have to restrict the counting in Theorem 2.1 to these points. Thus, to prove Theorem 1.1 we have to deal with the set $\mathcal{O}_{npp}^n(K/k)$ separately. In Section 11 we show that the orbits of the lattices coming from embeddings of $\mathcal{O}^n$ under the flow of $\mathcal{T}$ are bounded, and satisfy the refined conditions involving the higher successive minima as well. The entire Section 11 is heavily based on [32, Section 9]. In Section 12 we prove an upper bound for the number of lattice points that are not projectively primitive. With this upper bound we are ready in Section 13 to prove a precise asymptotic estimate for the number of projectively primitive lattice points for all components that arise from the partition method. Section 14 finishes the proof of Theorem 2.1.

Corollary 2.1 is essentially an immediate consequence of Theorem 2.1. However, the present statement requires an analogue of Theorem 2.1 in the case $q' = -1$. The latter is stated an proved in Section 15. The volumes of the sets $Z_I(T)$ and $Z(T)$ are computed in Section 16. In Section 17 we prove that the sum over $N(\mathcal{O}_{npp}^n(K/k), X)$ taken over all fields $K \in \mathcal{C}_e(k)$ is covered by the error term in Theorem 1.1. Finally, Section 18 is devoted to the proof of Theorem 1.1.

We will use Vinogradov's notation $\ll$. The implied constants depend only on n, m, e and d. Throughout this article T and X denote real numbers ≥ 1.

4. General counting principles

For a vector $\mathbf{x}$ in $\mathbb{R}^D$ we write $|\mathbf{x}|$ for the Euclidean length of $\mathbf{x}$. The closed Euclidean ball centered at $\mathbf{x}$ with radius r will be denoted by $B_{\mathbf{x}}(r)$. Let Λ be a lattice of rank D in $\mathbb{R}^D$ then we define the *successive minima* $\lambda_1(\Lambda), ..., \lambda_D(\Lambda)$ of Λ as the successive minima in the sense of Minkowski with respect to the unit ball. That is

$$\lambda_i = \inf\{\lambda;\ B_0(\lambda) \cap \Lambda \text{ contains } i \text{ linearly independent vectors}\}.$$

Definition 1. *Let M and D be positive integers, and let L be a non-negative real. We say that a set Z is in $Lip(D, M, L)$ if Z is a subset of $\mathbb{R}^D$, and if there are M maps $\varrho_1, \ldots, \varrho_M : [0,1]^{D-1} \longrightarrow \mathbb{R}^D$ satisfying a Lipschitz condition*

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

such that Z is covered by the images of the maps ϱ_i. For $D = 1$ this is to be interpreted as the finiteness of the set Z, and the maps ϱ_i are considered points in $\mathbb{R}^D$ such that $Z \subset \{\varrho_i; 1 \leq i \leq M\}$.

We will apply the following counting result from [32, Theorem 5.4].

Theorem 4.1. *Let Λ be a lattice in $\mathbb{R}^D$ with successive minima $\lambda_1, \ldots, \lambda_D$. Let Z be a bounded set in $\mathbb{R}^D$ such that the boundary ∂Z of Z is in $Lip(D, M, L)$. Then Z is measurable, and,* *moreover,*

$$\left| |Z \cap \Lambda| - \frac{\mathrm{Vol} Z}{\det \Lambda} \right| \leq c_4(D) M \max_{0 \leq i < D} \frac{L^i}{\lambda_1 \cdots \lambda_i}.$$

For $i = 0$ the expression in the maximum is to be understood as 1. Furthermore, one can choose $c_4(D) = D^{3D^2/2}$.

If Λ is a lattice in $\mathbb{R}^D$ and a is an integer with $1 \leq a \leq D$ then we put

$$\Lambda(a) = \{\mathbf{x} \in \Lambda; |\mathbf{x}| \geq \lambda_a\}. \tag{4.1}$$

Corollary 4.1. *Let Λ be a lattice in $\mathbb{R}^D$ with successive minima $\lambda_1, \ldots, \lambda_D$. Let Z be a bounded set in $\mathbb{R}^D$ such that the boundary ∂Z of Z is in $Lip(D, M, L)$, and $Z \subset B_0(\kappa L)$ with $\kappa \geq 1$. Then Z is measurable and we have*

$$\left| |Z \cap \Lambda(a)| - \frac{\mathrm{Vol} Z}{\det \Lambda} \right| \leq c_5(D) M \frac{(\kappa L)^{D-1}}{{\lambda_1}^{a-1} {\lambda_a}^{D-a}}.$$

One can choose $c_5(D) = c_4(D)(2\pi D)^D$.

Proof. The measurability comes directly from Theorem 4.1. First suppose $\kappa L \geq \lambda_a$. By the triangle inequality we get

$$\left| |Z \cap \Lambda(a)| - \frac{\mathrm{Vol} Z}{\det \Lambda} \right| \leq \left| |Z \cap \Lambda| - \frac{\mathrm{Vol} Z}{\det \Lambda} \right| + |B_0(\lambda_a) \cap \Lambda|.$$

We apply Theorem 4.1. Since $\kappa \geq 1$, we have

$$\left| |Z \cap \Lambda| - \frac{\mathrm{Vol} Z}{\det \Lambda} \right| \leq c_4(D) M \max_{0 \leq i < D} \frac{L^i}{\lambda_1 \cdots \lambda_i} \leq c_4(D) M \frac{(\kappa L)^{D-1}}{{\lambda_1}^{a-1} {\lambda_a}^{D-a}}.$$

To estimate $|B_0(\lambda_a) \cap \Lambda|$ we observe that $\partial B_0(\lambda_a)$ lies in $\mathrm{Lip}(D, 1, 2\pi D \lambda_a)$. Applying Theorem 4.1 gives

$$|B_0(\lambda_a) \cap \Lambda| \leq \frac{\mathrm{Vol} B_0(\lambda_a)}{\det \Lambda} + c_4(D) \max_{0 \leq i < D} \frac{(2\pi D \lambda_a)^i}{\lambda_1 \cdots \lambda_i}.$$

Using Minkowski's second Theorem we get

$$\frac{\mathrm{Vol} B_0(\lambda_a)}{\det \Lambda} \leq 2^D \frac{\lambda_a^D}{\lambda_1 \cdots \lambda_D} \leq 2^D \frac{\lambda_a^{D-1}}{\lambda_1^{a-1} \lambda_a^{D-a}} \leq 2^D \frac{(\kappa L)^{D-1}}{{\lambda_1}^{a-1} {\lambda_a}^{D-a}}.$$

Moreover,

$$\max_{0 \leq i < D} \frac{(2\pi D \lambda_a)^i}{\lambda_1 \cdots \lambda_i} \leq (2\pi D)^{D-1} \frac{\lambda_a^{D-1}}{\lambda_1^{a-1} \lambda_a^{D-a}} \leq (2\pi D)^{D-1} \frac{(\kappa L)^{D-1}}{{\lambda_1}^{a-1} {\lambda_a}^{D-a}}.$$

Next suppose $\kappa L < \lambda_a$. Then, as $Z \subset B_0(\kappa L)$, we have $|Z \cap \Lambda(a)| = 0$. Again, by Minkowski's second Theorem and by $Z \subset B_0(\kappa L)$ we get

$$\frac{\mathrm{Vol} Z}{\det \Lambda} \leq \frac{(2\kappa L)^D}{\lambda_1 \cdots \lambda_D} \leq 2^D \left(\frac{\kappa L}{\lambda_1} \right)^{a-1} \left(\frac{\kappa L}{\lambda_a} \right)^{D-a+1} \leq 2^D \frac{(\kappa L)^{D-1}}{{\lambda_1}^{a-1} {\lambda_a}^{D-a}}.$$

This completes the proof. $\square$

5. Counting via flows and partition techniques

Let r and s be non-negative integers not both zero, and put $d = r + 2s$ and $q = r + s - 1$. For $1 \leq i \leq r + s$ we set $d_i = 1$ if $i \leq r$ and $d_i = 2$ otherwise. We write $\mathbf{z}_i = (z_{i1}, \ldots, z_{in})$ for variables in K_i^n, where $K_i = \mathbb{R}$ if $i \leq r$ and $K_i = \mathbb{C}$ if $i > r$. Moreover, we write

$$|\mathbf{z}_i|_\infty = \max\{|z_{i1}|, \ldots, |z_{in}|\},$$
$$|(1, \mathbf{z}_i)|_\infty = \max\{1, |z_{i1}|, \ldots, |z_{in}|\}.$$

For $T \geq 1$ we define the set

$$Z(T) = \left\{ (\mathbf{z}_1, \ldots, \mathbf{z}_{r+s}) \in \prod_{i=1}^{r+s} K_i^n; \prod_{i=1}^{r+s} |(1, \mathbf{z}_i)|_\infty^{d_i} \leq T \right\}.$$

For each subset $I \subset \{1, 2, \ldots, r+s\}$ and $I^c = \{1, 2, \ldots, r+s\} \backslash I$ we define

$$Z_I(T) = \{(\mathbf{z}_1, \ldots, \mathbf{z}_{r+s}) \in Z(T); |\mathbf{z}_i|_\infty \geq 1 \text{ for } i \in I \text{ and } |\mathbf{z}_i|_\infty < 1 \text{ for } i \in I^c\}. \tag{5.1}$$

We put

$$d' = \sum_I d_i,$$

and

$$q' = |I| - 1.$$

Let $\mathcal{T}$ be the group of $\mathbb{R}$-linear maps ϕ on $\prod_{i=1}^{r+s} K_i^n$ of the form

$$\phi(\mathbf{z}_1, \ldots, \mathbf{z}_{r+s}) = (\xi_1 \mathbf{z}_1, \ldots, \xi_{r+s} \mathbf{z}_{r+s}) \tag{5.2}$$

with positive real ξ_i satisfying

$$\prod_{i=1}^{r+s} \xi_i^{d_i} = 1, \tag{5.3}$$

so that $\det \phi = 1$. The following theorem is an important intermediate step.

Theorem 5.1. *Suppose $q' = |I| - 1 \geq 0$. Let Λ be a lattice in the Euclidean space $\prod_{i=1}^{r+s} K_i^n$ and suppose there exist positive real numbers $\eta_1, \ldots, \eta_{nd}$ such that $\lambda_p(\phi(\Lambda)) \geq \eta_p$ for $1 \leq p \leq nd$ and all $\phi \in \mathcal{T}$. Then, for $T \geq 1$, one has*

$$\left| |\Lambda \cap Z_I(T)| - \frac{\mathrm{Vol} Z_I(T)}{\det \Lambda} \right| \leq c_6 (\log^+ T)^{q'} \max_{0 \leq p < nd} \frac{T^{p/d}}{\eta_1 \cdots \eta_p},$$
$$\left| |\Lambda \cap Z_I(T)| - \frac{\mathrm{Vol} Z_I(T)}{\det \Lambda} \right| \leq c_7 (\log^+ T)^{q'} \frac{T^{n-1/d}}{\eta_1^{nd-1}},$$

where $c_6 = c_6(n, d)$ and $c_7 = c_7(n, d)$ depend only on n and d. For $p = 0$ the expression in the maximum is to be understood as 1. Moreover, if $T < (\eta_1/\kappa)^d$ we have

$$|\Lambda \cap Z_I(T)| = 0,$$

where $\kappa = \sqrt{dn} \exp(\sqrt{q})$.

6. Preliminaries

Unless explicitly mentioned otherwise (which will be the case only in Section 15) we always assume $I \neq \emptyset$. Suppose $I = \{i_1, \ldots, i_p\}$ with $i_1 < \cdots < i_p$ then we put $(\mathbf{z}_i)_I = (\mathbf{z}_{i_1}, \ldots, \mathbf{z}_{i_p})$. For subsets $\mathcal{Z}_1 \subset \prod_I K_i^n$ and $\mathcal{Z}_2 \subset \prod_{I^c} K_i^n$ we identify the Cartesian product $\mathcal{Z}_1 \times \mathcal{Z}_2$ with $\mathcal{Z}_1$ if I^c is empty. It is more convenient to group the coordinate vectors according to their maximum norm, and thus we redefine

$$Z_I(T) = \left\{ (\mathbf{z}_i)_I \in \prod_I K_i^n; \prod_I |\mathbf{z}_i|_\infty^{d_i} \leq T, |\mathbf{z}_i|_\infty \geq 1 \text{ for } i \in I \right\} \times \left\{ (\mathbf{z}_i)_{I^c} \in \prod_{I^c} K_i^n; |\mathbf{z}_i|_\infty < 1 \text{ for } i \in I^c \right\}. \tag{6.1}$$

As we study the cardinality $|\Lambda \cap Z_I(T)|$ we shall permute the coordinates of Λ in the same manner, and we modify $\phi \in \mathcal{T}$ accordingly to act on $\prod_I K_i^n \times \prod_{I^c} K_i^n$. Of course, this leaves the volume $\mathrm{Vol} Z_I(T)$ and the values $\lambda_i(\phi(\Lambda))$ invariant. Let Σ be the hyperplane in $\mathbb{R}^{q'+1}$ defined by $x_1 + \cdots + x_{q'+1} = 0$ and

$$\delta = (d_i/d')_I.$$

Let F be a set in Σ and put $F(T)$ for the vector sum

$$F(T) = F + \delta(-\infty, \log T]. \tag{6.2}$$

The map $(\mathbf{z}_i)_I \longrightarrow (d_i \log |\mathbf{z}_i|_\infty)_I$ sends $\prod_I K_i^n \backslash \{\mathbf{0}\}$ to $\mathbb{R}^{q'+1}$. Now we define

$$S_F(T) = \left\{ (\mathbf{z}_i)_I \in \prod_I K_i^n \backslash \{\mathbf{0}\}; (d_i \log |\mathbf{z}_i|_\infty)_I \in F(T) \right\}. \tag{6.3}$$

Directly from the definition we get

$$S_F(T) = T^{1/d'} S_F(1). \tag{6.4}$$

Moreover, if F lies in a ball centered at zero of radius r_F, then for any $(\mathbf{z}_i)_I \in S_F(T)$

$$|\mathbf{z}_i|_\infty \leq \exp(r_F) T^{1/d'} \quad (i \in I). \tag{6.5}$$

For non-negative reals a_i ($i \in I$) let us write

$$E((a_i)_I) = \left\{ (\mathbf{z}_i)_I \in \prod_I K_i^n; |\mathbf{z}_i|_\infty \geq a_i \text{ for } i \in I \right\}. \tag{6.6}$$

7. Partitioning and transforming $Z_I(T)$

In Section 10 we will prove that for $q' > 0$ we have

$$Z_I(T) = (S_F(T) \cap E((1)_I)) \times \{(\mathbf{z}_i)_{I^c}; |\mathbf{z}_i|_\infty < 1 \text{ for } i \in I^c\}$$

for a certain $F \subset \Sigma$. In this section we focus on the first component $S_F(T) \cap E((1)_I)$ but we will allow arbitrary sets $F \subset \Sigma$. Throughout this section we assume

$$q' > 0.$$

Fix once and for all an orthonormal basis $e_1, \ldots, e_{q'}$ of $\Sigma \subset \mathbb{R}^{q'+1}$. For $\mathbf{j} = (j_1, \ldots, j_{q'}) \in \mathbb{Z}^{q'}$ we define the fundamental cell

$$C_{\mathbf{j}} = j_1 e_1 + [0,1) e_1 + \cdots + j_{q'} e_{q'} + [0,1) e_{q'}.$$

For $F \subset \Sigma$ we define

$$F_{\mathbf{j}} = C_{\mathbf{j}} \cap F.$$

Let $\mathfrak{m}_F$ be the set of those $\mathbf{j}$ that satisfy $F_{\mathbf{j}} \neq \emptyset$. Clearly,

$$F = \bigcup_{\mathfrak{m}_F} F_{\mathbf{j}}, \tag{7.1}$$

and the latter is a disjoint union.

Lemma 7.1. *Suppose F is a subset of Σ and $F \subset B_0(r_F)$ with $r_F \geq 1$. Then*

$$|\mathfrak{m}_F| \ll {r_F}^{q'}.$$

Proof. Clearly, F lies in the cube $[-r_F, r_F]e_1 + \cdots + [-r_F, r_F]e_{q'}$ which has non-empty intersection with at most $(2\lceil r_F \rceil + 1)^{q'}$ fundamental cells $C_{\mathbf{j}}$ (here $\lceil r_F \rceil$ denotes the smallest integer not smaller than r_F). Since $r_F \geq 1$ the lemma follows. □

Now (7.1) leads to

$$S_F(T) = \bigcup_{\mathfrak{m}_F} S_{F_{\mathbf{j}}}(T), \tag{7.2}$$

which again is a disjoint union. For each vector $\mathbf{j} = (j_1, \ldots, j_{q'}) \in \mathbb{Z}^{q'}$ we define a translation $tr_{\mathbf{j}}$ on $\mathbb{R}^{q'+1}$ by

$$tr_{\mathbf{j}}(x) = x - \sum_{p=1}^{q'} j_p e_p = x - u(\mathbf{j}),$$

where $u(\mathbf{j}) = (u_i)_I = \sum_{p=1}^{q'} j_p e_p$. This translation sends Σ to Σ and $C_{\mathbf{j}}$ to $C_{\mathbf{0}}$. For $i \in I$ set $\gamma_i = \gamma_i(\mathbf{j}) = \exp(-u_i/d_i)$, so that $\gamma_i > 0$,

$$\prod_I \gamma_i^{d_i} = 1, \tag{7.3}$$

and

$$(d_i \log |\gamma_i \mathbf{z}_i|_\infty)_I = tr_{\mathbf{j}}((d_i \log |\mathbf{z}_i|_\infty)_I).$$

Hence, for the automorphism $\tau_{\mathbf{j}}$ of $\prod_I K_i^n$ defined by

$$\tau_{\mathbf{j}}(\mathbf{z}_i)_I = (\gamma_i \mathbf{z}_i)_I,$$

we have

$$\tau_{\mathbf{j}} S_F(T) = S_{tr_{\mathbf{j}}(F)}(T).$$

As $tr_{\mathbf{j}}(F_{\mathbf{j}}) = tr_{\mathbf{j}}(F) \cap C_{\mathbf{0}}$ we get

$$\tau_{\mathbf{j}} S_{F_{\mathbf{j}}}(T) = S_{tr_{\mathbf{j}}(F) \cap C_{\mathbf{0}}}(T). \tag{7.4}$$

Moreover, we have

$$\tau_{\mathbf{j}} E(1)_I = \left\{ (\mathbf{z}_i)_I \in \prod_I K_i^n; |\mathbf{z}_i|_\infty \geq \gamma_i \text{ for } i \in I \right\} = E((\gamma_i)_I).$$

As $C_{\mathbf{0}} \subset B_0(\sqrt{q'})$ we get from (6.5) that for any $(\mathbf{z}_i)_I \in S_{C_{\mathbf{0}}}(T)$

$$|\mathbf{z}_i|_\infty \leq \exp(\sqrt{q'}) T^{1/d'} \quad (i \in I). \tag{7.5}$$

We extend $\tau_{\mathbf{j}}$ to a diagonal endomorphism $\phi_{\mathbf{j}}$ on $\prod_I K_i^n \times \prod_{I^c} K_i^n$ by setting

$$\phi_{\mathbf{j}}(((\mathbf{z}_i)_I, (\mathbf{z}_i)_{I^c})) = (\tau_{\mathbf{j}}(\mathbf{z}_i)_I, (\mathbf{z}_i)_{I^c}) = ((\gamma_i \mathbf{z}_i)_I, (\mathbf{z}_i)_{I^c}). \tag{7.6}$$

Next we put

$$Z_{F_{\mathbf{j}}} = \Big(S_{F_{\mathbf{j}}}(T) \cap E((1)_I) \Big) \times \{ (\mathbf{z}_i)_{I^c}; |\mathbf{z}_i|_\infty < 1 \text{ for } i \in I^c \}. \tag{7.7}$$

8. FURTHER TRANSFORMING $Z_I(T)$

We define a map

$$\psi : \prod_I K_i^n \times \prod_{I^c} K_i^n \longrightarrow \prod_I K_i^n \times \prod_{I^c} K_i^n \tag{8.1}$$

by

$$\psi(((\mathbf{z}_i)_I, (\mathbf{z}_i)_{I^c})) = (\psi_1((\mathbf{z}_i)_I), \psi_2((\mathbf{z}_i)_{I^c})),$$

where

$$\psi_1((\mathbf{z}_i)_I) = ((T^{-1/d'+1/d}\mathbf{z}_i)_I),$$
$$\psi_2((\mathbf{z}_i)_{I^c}) = ((T^{1/d}\mathbf{z}_i)_{I^c}).$$

For $q' = q$ (i.e., for $I^c = \emptyset$) we interpret, of course, $\psi = \psi_1$ as the identity on $\prod_I K_i^n = \prod_{i=1}^{r+s} K_i^n$. As $d' = \sum_I d_i$ we see that

$$\det \psi = \prod_I T^{d_i n(-1/d'+1/d)} \prod_{I^c} T^{d_i n/d} = 1. \tag{8.2}$$

Therefore, ψ lies in $\mathcal{T}$.

First suppose $q' = 0$, so that $I = \{i\}$ is a singleton. Then

$$\psi Z_I(T) = \tag{8.3}$$

$$\left\{\mathbf{z}_i \in K_i^n; T^{-1/d'+1/d} \le |\mathbf{z}_i|_\infty \le T^{1/d}\right\} \times \left\{(\mathbf{z}_{i'})_{i' \neq i} \in \prod_{i' \neq i} K_{i'}{}^n; |\mathbf{z}_{i'}|_\infty < T^{1/d} \text{ for } i' \neq i\right\}.$$

Now suppose $q' > 0$. For $\mathbf{j} \in \mathbb{Z}^{q'}$ we set

$$\mathcal{Z}_1 = \psi_1\left(\tau_{\mathbf{j}} S_{F_{\mathbf{j}}}(T) \cap \tau_{\mathbf{j}} E((1)_I)\right) \subset \prod_I K_i^n, \tag{8.4}$$

and, with $\phi_{\mathbf{j}}$ as in (7.6), we define

$$\psi_{\mathbf{j}} = \psi \circ \phi_{\mathbf{j}}. \tag{8.5}$$

Moreover, we set

$$\mathcal{Z}_2 = \psi_2\left\{(\mathbf{z}_i)_{I^c}; |\mathbf{z}_i|_\infty < 1 \text{ for } i \in I^c\right\} = \left\{(\mathbf{z}_i)_{I^c}; |\mathbf{z}_i|_\infty < T^{1/d} \text{ for } i \in I^c\right\} \subset \prod_{I^c} K_i^n, \tag{8.6}$$

so that

$$\mathcal{Z}_1 \times \mathcal{Z}_2 = \psi_{\mathbf{j}} Z_{F_{\mathbf{j}}}.$$

Lemma 8.1. *Let $\kappa = \sqrt{dn}\exp(\sqrt{q})$ be as in Theorem 5.1. If $q' = 0$ then we have*

$$\psi Z_I(T) \subset B_0(\kappa T^{1/d}). \tag{8.7}$$

If $q' > 0$ and $\mathbf{j} \in \mathbb{Z}^{q'}$ then we have

$$\psi_{\mathbf{j}} Z_{F_{\mathbf{j}}} \subset B_0(\kappa T^{1/d}). \tag{8.8}$$

In particular,

$$\mathcal{Z}_p \subset B_0(\kappa T^{1/d}) \quad (1 \le p \le 2) \tag{8.9}$$

for the respective balls $B_0(\kappa T^{1/d})$.

Proof. As $\kappa \geq \sqrt{(q+1)n}$ the claim (8.7) follows immediately from (8.3). Next suppose $q' > 0$. Recall from (7.4) that $\tau_{\mathbf{j}} S_{F_{\mathbf{j}}}(T) \subset S_{C_{\mathbf{0}}}(T)$. From (7.5), and not forgetting the effect of ψ_1, we see that for any $(\mathbf{z}_i)_I$ in $\mathcal{Z}_1$ we have $|\mathbf{z}_i|_\infty \leq \exp(\sqrt{q'})T^{1/d}$ $(i \in I)$. And, obviously, we also have $|\mathbf{z}_i|_\infty \leq \exp(\sqrt{q'})T^{1/d}$ $(i \in I^c)$ for any $(\mathbf{z}_i)_{I^c}$ in $\mathcal{Z}_2$. This proves (8.8). □

9. Lipschitz parameterizations

In this section we shall prove that the sets $\psi Z_I(T)$ (if $q' = 0$), and $\psi_{\mathbf{j}} Z_{F_{\mathbf{j}}}$ (if $q' > 0$) have Lipschitz parameterizable boundaries with Lipschitz constant $L \ll T^{1/d}$. To this end we need a few simple lemmas. For $q' > 0$ we will identify Σ with $\mathbb{R}^{q'}$ via the basis $e_1, \ldots, e_{q'}$ from Section 7. For a subset $\mathcal{Z}$ of Euclidean space we write $\partial\mathcal{Z}$ for its topological boundary.

Lemma 9.1. *Suppose $q' > 0$, and let F be a set in Σ such that ∂F is in $Lip(q', M', L')$, and, moreover, assume F lies in $B_0(r_F)$. Then $\partial S_F(1)$ is in $Lip(d'n, \widetilde{M}, \widetilde{L})$ with $\widetilde{M}$ and $\widetilde{L}$ depending only on n, q', M', L', r_F.*

Proof. The case $n > 1$ follows directly from [19, Lemma 3] (see also [32, Lemma 7.1] for a more detailed and completely explicit version). However, for $n = 1$ the proof remains correct without change. □

Lemma 9.2. *Suppose $q' > 0$, and recall the definition of $tr_{\mathbf{j}}$ and $F_{\mathbf{j}}$ from Section 7. Let $Y \geq 1$ be a real number and suppose the boundary of $tr_{\mathbf{j}} F_{\mathbf{j}}$ lies in $Lip(q', M', L')$ with $M' \ll 1$ and $L' \ll 1$. Then the boundary of $\tau_{\mathbf{j}} S_{F_{\mathbf{j}}}(Y)$ lies in $Lip(d'n, M, L)$ with $M \ll 1$ and $L \ll Y^{1/d'}$.*

Proof. Clearly, $tr_{\mathbf{j}}(F_{\mathbf{j}}) = tr_{\mathbf{j}}(F) \cap C_{\mathbf{0}}$ is contained in $B_0(\sqrt{q'})$. Now $\tau_{\mathbf{j}} S_{F_{\mathbf{j}}}(Y) = S_{tr_{\mathbf{j}}(F_{\mathbf{j}})}(Y)$ and thus the lemma follows from (6.4) and Lemma 9.1. □

Lemma 9.3. *If $q' = 0$ then $\partial\psi Z_I(T)$ lies in $Lip(dn, M, L)$ with $M \ll 1$ and $L \ll T^{1/d}$. If $q' > 0$ and $\partial tr_{\mathbf{j}} F_{\mathbf{j}}$ lies in $Lip(q', M', L')$ with $M' \ll 1$ and $L' \ll 1$ then the set $\partial\psi_{\mathbf{j}} Z_{F_{\mathbf{j}}}$ lies in $Lip(dn, M, L)$ with $M \ll 1$ and $L \ll T^{1/d}$.*

Proof. Fist suppose $q' = 0$. The sets in K_i^n defined by $|\mathbf{z}_i|_\infty = \zeta$ are in $\mathrm{Lip}(d_i n, 2n, \zeta')$ with $\zeta' \ll \zeta$, e.g., we can take $2n$ linear (if $i \leq r$) or n trigonometrical (if $i > r$) maps. Then one easily gets a parameterization of the sets $|\mathbf{z}_i|_\infty = \zeta_1$, $|\mathbf{z}_{i'}|_\infty \leq \zeta_2$ $(i' \neq i)$ in $\prod_I K_i^n \times \prod_{I^c} K_i^n$ with $M \ll 1$ maps and Lipschitz constants $L \ll \max\{\zeta_1, \zeta_2\}$. In view of (8.3) this proves the lemma for $q' = 0$.

Now suppose $q' > 0$. We need to show that $\partial(\mathcal{Z}_1 \times \mathcal{Z}_2)$ lies in $\mathrm{Lip}(dn, M, L)$. Clearly, $\partial(\mathcal{Z}_1 \times \mathcal{Z}_2)$ is contained in the union of $\overline{\mathcal{Z}_1} \times \partial\mathcal{Z}_2$ and $\partial\mathcal{Z}_1 \times \overline{\mathcal{Z}_2}$, where the bar denotes the topological closure. Moreover, by (8.9) we know $\overline{\mathcal{Z}_1}$ and $\overline{\mathcal{Z}_2}$ lie both in a ball $B_0(\kappa T^{1/d})$. Therefore, it suffices to show that $\partial\mathcal{Z}_1 \in \mathrm{Lip}(d'n, M'', L'')$ and, if $d - d' > 0$, also $\partial\mathcal{Z}_2 \in \mathrm{Lip}((d-d')n, M'', L'')$ with some $M'' \ll 1$ and some $L'' \ll T^{1/d}$. Next note that

$$\psi_1 \tau_{\mathbf{j}}(S_{F_{\mathbf{j}}}(T)) = T^{1/d} S_{tr_{\mathbf{j}} F_{\mathbf{j}}}(1),$$
$$\psi_1 \tau_{\mathbf{j}}\,(E((1)_I)) = E((T^{1/d - 1/d'}\gamma_i)_I).$$

As $\mathcal{Z}_1$ is the intersection of these two sets, we see that $\partial\mathcal{Z}_1$ is covered by the union of $\partial E((T^{1/d-1/d'}\gamma_i)_I) \cap \overline{\mathcal{Z}_1}$ and $\partial T^{1/d} S_{tr_{\mathbf{j}} F_{\mathbf{j}}}(1)$. Regarding the latter recall that $tr_{\mathbf{j}} F_{\mathbf{j}} \subset C_{\mathbf{0}} \subset B_0(\sqrt{q'})$ and $\partial tr_{\mathbf{j}} F_{\mathbf{j}}$ lies in $\mathrm{Lip}(q', M', L')$. Therefore, we can apply Lemma 9.1 to conclude $\partial T^{1/d} S_{tr_{\mathbf{j}} F_{\mathbf{j}}}(1)$ lies in $\mathrm{Lip}(d'n, M'', L'')$ with some $M'' \ll 1$ and some $L'' \ll$

$T^{1/d}$. And for $\partial E((T^{1/d-1/d'}\gamma_i)_I) \cap \overline{\mathcal{Z}_1}$ we use the same argument as for $q' = 0$ to see that it is in $\mathrm{Lip}(d'n, M'', L'')$ with an $M'' \ll 1$ and an $L'' \ll T^{1/d}$. And again, the same argument shows that, for $d > d'$, $\partial\mathcal{Z}_2$ lies in $\mathrm{Lip}((d-d')n, M'', L'')$ with an $M'' \ll 1$ and an $L'' \ll T^{1/d}$. This proves the Lemma 9.3. □

10. Proof of Theorem 5.1

To simplify the notation we write Z_I for $Z_I(T)$. First we assume $q' = 0$.
Recall that ψ lies in $\mathcal{T}$, and, clearly, we have $|Z_I \cap \Lambda| = |\psi Z_I \cap \psi\Lambda|$. By (8.7) we have $\psi(Z_I) \subset B_0(\kappa T^{1/d})$, and by hypothesis of Theorem 5.1 we have $\lambda_i(\psi\Lambda) \geq \eta_i$ for $1 \leq i \leq dn$. Thanks to Lemma 9.3 we can apply Theorem 4.1 which gives the first inequality of Theorem 5.1. For the second inequality we apply Corollary 4.1 with $a = 1$ and note that $\mathbf{0} \notin \psi(Z_I)$. And finally, as $\mathbf{0} \notin \psi(Z_I)$ and $\psi(Z_I) \subset B_0(\kappa T^{1/d})$ we see that $|\Lambda \cap Z_I| = 0$ if $T^{1/d} < (1/\kappa)\eta_1$. This finishes the proof of Theorem 5.1 for $q' = 0$.

For the rest of this section we assume $q' > 0$, and, for the rest of the paper, we fix F as

$$F = (\mathbb{R}_{\geq 0}^{q'+1} - \delta \log T) \cap \Sigma. \tag{10.1}$$

Lemma 10.1. *We have*

$$Z_I = (S_F(T) \cap E((1)_I)) \times \{(\mathbf{z}_i)_{I^c}; |\mathbf{z}_i|_\infty < 1 \text{ for } i \in I^c\}.$$

Proof. In view of (6.1) it suffices to show

$$\left\{(\mathbf{z}_i)_I \in \prod_I K_i^n; \prod_I |\mathbf{z}_i|_\infty^{d_i} \leq T, |\mathbf{z}_i|_\infty \geq 1 \text{ for } i \in I\right\} = S_F(T) \cap E((1)_I) \tag{10.2}$$

From the definitions (6.3) and (6.6) we see immediately that the right hand-side is contained in the left hand-side for any choice of $F \subset \Sigma$ whatsoever. Now for the other inclusion note that the left hand-side in (10.2) means

$$(d_i \log |\mathbf{z}_i|_\infty)_I \in \mathbb{R}_{\geq 0}^{q'+1} \cap (\Sigma + \delta(-\infty, \log T]).$$

Thus we need to show

$$\mathbb{R}_{\geq 0}^{q'+1} \cap (\Sigma + \delta(-\infty, \log T]) \subset F(T) = \left(\left(\mathbb{R}_{\geq 0}^{q'+1} - \delta \log T\right) \cap \Sigma\right) + \delta(-\infty, \log T].$$

Any element in the set on the left hand-side can be written as $\mathbf{x} + \delta t$ with $\mathbf{x} \in \Sigma$ and $t \in (-\infty, \log T]$. As $\mathbf{x} + \delta t \in \mathbb{R}_{\geq 0}^{q'+1}$ we get $\mathbf{x} \in \mathbb{R}_{\geq 0}^{q'+1} - \delta \log T \cap \Sigma$, and therefore

$$\mathbf{x} + \delta t \in \left(\left(\mathbb{R}_{\geq 0}^{q'+1} - \delta \log T\right) \cap \Sigma\right) + \delta(-\infty, \log T].$$

This concludes the proof. □

Lemma 10.2. *We have*

$$F \subset B_0(2 \log T) \tag{10.3}$$

Proof. Suppose $(x_1, \ldots, x_{q'+1}) \in F$. As $x_1 + \cdots + x_{q'+1} = 0$ we see that the sum over the positive coordinates equals minus the sum over the negative coordinates and thus $|x_1| + \cdots + |x_{q'+1}| \leq 2\sum_I (d_i/d') \log T = 2 \log T$. This proves the lemma. □

Recall the definition of $Z_{F_{\mathfrak{j}}}$ from (7.7). The disjoint union (7.2), in conjunction with Lemma 10.1, leads to the disjoint union

$$Z_I = \bigcup_{\mathfrak{m}_F} Z_{F_{\mathfrak{j}}}, \tag{10.4}$$

which in turn yields

$$|Z_I \cap \Lambda| = \sum_{\mathfrak{m}_F} |Z_{F_{\mathbf{j}}} \cap \Lambda|.$$

As the $\psi_{\mathbf{j}}$ are automorphisms we conclude

$$|Z_I \cap \Lambda| = \sum_{\mathfrak{m}_F} |\psi_{\mathbf{j}} Z_{F_{\mathbf{j}}} \cap \psi_{\mathbf{j}} \Lambda|. \tag{10.5}$$

We will apply Lemma 9.3 with our choice of F given in (10.1). We start off by verifying the necessary conditions.

Lemma 10.3. *Let F be as in (10.1). There exist $M' \ll 1$ and $L' \ll 1$ such that $\partial tr_{\mathbf{j}} F_{\mathbf{j}}$ lies in $Lip(q', M', L')$.*

Proof. Clearly, F, and therefore also $tr_{\mathbf{j}} F$, is convex. And, clearly, $C_{\mathbf{0}}$ is convex and contained in $B_0(\sqrt{q'})$. Hence $tr_{\mathbf{j}} F_{\mathbf{j}} = tr_{\mathbf{j}} F \cap C_{\mathbf{0}}$ is convex and lies in $B_0(\sqrt{q'})$. Now if $q' = 1$ the lemma is trivial, and if $q' > 1$ it follows immediately from [33, Theorem 2.6]. □

Lemma 10.4. *The set $\partial \psi_{\mathbf{j}}(Z_{F_{\mathbf{j}}})$ lies in $Lip(dn, M, L)$ with some $M \ll 1$ and some $L \ll T^{1/d}$.*

Proof. This is an immediate consequence of Lemma 10.3 and Lemma 9.3. □

Lemma 10.5. *We have*

$$\left| |\psi_{\mathbf{j}}(Z_{F_{\mathbf{j}}}) \cap \psi_{\mathbf{j}}(\Lambda)| - \frac{\mathrm{Vol} Z_{F_{\mathbf{j}}}}{\det \Lambda} \right| \ll \max_{0 \le p < dn} \frac{T^{p/d}}{\eta_1 \cdots \eta_p},$$

$$\left| |\psi_{\mathbf{j}}(Z_{F_{\mathbf{j}}}) \cap \psi_{\mathbf{j}}(\Lambda)| - \frac{\mathrm{Vol} Z_{F_{\mathbf{j}}}}{\det \Lambda} \right| \ll \frac{T^{n-1/d}}{\eta_1^{nd-1}},$$

$$|\psi_{\mathbf{j}}(Z_{F_{\mathbf{j}}}) \cap \psi_{\mathbf{j}}(\Lambda)| = 0 \text{ if } T^{1/d} < (1/\kappa)\eta_1.$$

Proof. Again, we want to apply Theorem 4.1 and Corollary 4.1. First recall that $\psi_{\mathbf{j}} \in \mathcal{T}$, in particular, $\mathrm{Vol} \psi_{\mathbf{j}} Z_{F_{\mathbf{j}}} = \mathrm{Vol} Z_{F_{\mathbf{j}}}$ and $\det \psi_{\mathbf{j}}(\Lambda) = \det(\Lambda)$. By Lemma 10.4 we know $\partial \psi_{\mathbf{j}}(Z_{F_{\mathbf{j}}})$ lies in $\mathrm{Lip}(dn, M, L)$ with some $M \ll 1$ and some $L \ll T^{1/d}$. By (8.8) we have $\psi_{\mathbf{j}} Z_{F_{\mathbf{j}}} \subset B_0(\kappa T^{1/d})$ with $1 \le \kappa \ll 1$, and as $\mathbf{0} \notin Z_I$ we also have $\mathbf{0} \notin \psi_{\mathbf{j}} Z_{F_{\mathbf{j}}}$. Applying Theorem 4.1 and Corollary 4.1, and using the hypothesis $\lambda_p(\psi_{\mathbf{j}}(\Lambda)) \ge \eta_p$ yields the inequalities of the lemma. And the last statement follows just as in the case $q' = 0$. □

Lemma 10.6. *We have*

$$|\mathfrak{m}_F| \ll (\log^+ T)^{q'}.$$

Proof. This follows immediately from (10.3) and Lemma 7.1. □

We can now easily conclude the proof of Theorem 5.1. Combining (10.5) and Lemma 10.5 with (10.4) implies

$$\left| |Z_I \cap \Lambda| - \frac{\mathrm{Vol} Z_I}{\det \Lambda} \right| \ll \sum_{\mathfrak{m}_F} \max_{0 \le p < dn} \frac{T^{p/d}}{\eta_1 \cdots \eta_p},$$

$$\left| |Z_I \cap \Lambda| - \frac{\mathrm{Vol} Z_I}{\det \Lambda} \right| \ll \sum_{\mathfrak{m}_F} \frac{T^{n-1/d}}{\eta_1^{nd-1}}.$$

And, if $T^{1/d} < (1/\kappa)\eta_1$, we have

$$|Z_I \cap \Lambda| = \sum_{\mathfrak{m}_F} 0 = 0.$$

Finally, we use Lemma 10.6 to deduce

$$\sum_{\mathfrak{m}_F} 1 \ll (\log^+ T)^{q'}.$$

This proves Theorem 5.1.

11. Estimates for the successive minima

In this section, we state the fact that the successive minima of the lattice $\phi\sigma\mathcal{O}^n$ are bounded away from zero, uniformly in $\phi \in \mathcal{T}$. We also state a crucial refinement involving a critical higher successive minimum λ_l and two other results. All these results are slight generalizations of those in [32, Section 9] but they are proved by exactly the same arguments. Therefore we skip the proofs and simply state the lemmas.

As in Section 2 let K/k be an extension of number fields, and $d = [K : \mathbb{Q}]$. Recall that $\sigma_1, \ldots, \sigma_d$ denote the embeddings from K to K_i, ordered such that $\sigma_{r+s+i} = \overline{\sigma}_{r+i}$ for $1 \leq i \leq s$. We write

$$\sigma : K \longrightarrow \prod_{i=1}^{r+s} K_i \qquad (11.1)$$
$$\sigma(\alpha) = (\sigma_1(\alpha), \ldots, \sigma_{r+s}(\alpha)).$$

Let ϕ be as in (5.2). By abuse of notation we may regard ϕ also as an automorphism of $\mathbb{R}^r \times \mathbb{C}^s$, and from now on, depending on the argument, we view ϕ as an automorphism of $\mathbb{R}^r \times \mathbb{C}^s$ or $\mathbb{R}^{rn} \times \mathbb{C}^{sn}$. Applying ϕ to the lattice $\sigma\mathcal{O}$ gives a new lattice $\phi\sigma\mathcal{O}$ in $\mathbb{R}^r \times \mathbb{C}^s$. As is well-known, see, e.g., [6, Chapter VIII, Lemma 1], we can choose linearly independent vectors

$$v_1 = \phi\sigma(\theta_1), \ldots, v_d = \phi\sigma(\theta_d)$$

of the lattice $\phi\sigma\mathcal{O}$ with

$$|v_i| = \lambda_i(\phi\sigma\mathcal{O}) \qquad (1 \leq i \leq d) \qquad (11.2)$$

for the successive minima $\lambda_i(\phi\sigma\mathcal{O})$. The $v_1, \ldots, v_d$ are $\mathbb{R}$-linearly independent. Hence, $\theta_1, \ldots, \theta_d$ are $\mathbb{Q}$-linearly independent, and therefore $\frac{\theta_1}{\theta_1}, \ldots, \frac{\theta_d}{\theta_1}$ are $\mathbb{Q}$-linearly independent. As $[K : \mathbb{Q}] = d$ we get $K = \mathbb{Q}(\frac{\theta_1}{\theta_1}, \ldots, \frac{\theta_d}{\theta_1}) = k(\frac{\theta_1}{\theta_1}, \ldots, \frac{\theta_d}{\theta_1})$, and this allows the following definition.

Definition 2. *Let $l \in \{1, \ldots, d\}$ be minimal with $K = k(\frac{\theta_1}{\theta_1}, \ldots, \frac{\theta_l}{\theta_1})$.*

We abbreviate

$$\lambda_i = \lambda_i(\phi\sigma\mathcal{O}) \qquad (11.3)$$

for $1 \leq i \leq d$. Recall the definition of $\eta_{\mathcal{O}}$ from (2.1).

Lemma 11.1. *We have*

$$\lambda_1 \geq \sqrt{d/2}\,\eta_{\mathcal{O}}.$$

Lemma 11.2. *With $K_0 = k(\frac{\theta_1}{\theta_1}, \ldots, \frac{\theta_{l-1}}{\theta_1})$ if $l \geq 2$ and $K_0 = k$ if $l = 1$, and $g = [K_0 : k] \in G(K/k)$ we have*

$$\lambda_l \geq \frac{1}{\sqrt{2}ed}\eta_{\mathcal{O}}\delta_g(K/k).$$

For the rest of this section we assume that

$$n > 1.$$

Lemma 11.3. *Let* $(\omega_1,\ldots,\omega_n)$ *be in* $\mathcal{O}^n\backslash\{\mathbf{0}\}$ *with* $k(\ldots,\omega_i/\omega_j,\ldots)=K$. *Then for* $v=(\phi\sigma\omega_1,\ldots,\phi\sigma\omega_n)$ *we have*

$$|v|\geq\lambda_l.$$

We remind the reader that $[K:k]=e$, $[k:\mathbb{Q}]=m$, and $d=em$.

Lemma 11.4. *If* $l\geq 2$ *then*

$$\frac{l-1}{m}\leq\left[k\left(\frac{\theta_1}{\theta_1},\ldots,\frac{\theta_{l-1}}{\theta_1}\right):k\right]\leq\max\{1,e/2\}.$$

12. Upper bounds for the projectively non-primitive points

We extend the embeddings σ_i from (11.1) componentwise to get an embedding of K^n

$$\sigma:K^n\longrightarrow\prod_{i=1}^{r+s}K_i^n.$$

Depending on the argument we either see σ as a map on K or on K^n. Again, let ϕ be as in (5.2). In this section we prove an upper bound for the number of nonzero points in $\phi\sigma\mathcal{O}^n$ that (as projective points) do not generate K/k and lie in some ball. For brevity we write

$$\Lambda'=\phi\sigma\mathcal{O}^n\backslash(\phi\sigma\mathcal{O}^n(K/k)\cup\{\mathbf{0}\}).$$

Lemma 12.1. *Suppose* $n>1$, *let* $B_0(R)$ *be the zero centered ball in the Euclidean space* $\mathbb{R}^{nr}\times\mathbb{C}^{ns}$ *of radius* R, *and let* λ_i *be as in (11.3). Then*

$$|\Lambda'\cap B_0(R)|\ll\max_{0\leq i\leq d}\frac{R^i}{\lambda_1\cdots\lambda_i}\left(\max_{0\leq i<d}\frac{R^i}{\lambda_1\cdots\lambda_i}\right)^{n-1}.$$

Proof. We follow the lines of proof in [32, Proposition 10.1]. For $(\phi\sigma\omega_1,\ldots,\phi\sigma\omega_n)$ in Λ' the field $k(\ldots,\omega_i/\omega_j,\ldots)$ lies in a strict subfield, say K_1, of K. Hence, there exist two different embeddings σ_a,σ_b of K with

$$\sigma_a\alpha=\sigma_b\alpha$$

for all α in K_1. Now $(\phi\sigma\omega_1,\ldots,\phi\sigma\omega_n)\neq\mathbf{0}$, and thus, at least one of the numbers $\omega_1,\ldots,\omega_n$ is nonzero. By symmetry we lose only a factor n if we assume $\omega_1\neq 0$. So let us temporarily regard $\omega_1\neq 0$ as fixed; then for $2\leq j\leq n$ every ω_j satisfies

$$\sigma_a\frac{\omega_j}{\omega_1}=\sigma_b\frac{\omega_j}{\omega_1}.$$

Therefore, all these $\sigma\omega_j$ lie in a hyperplane $\mathcal{P}(\omega_1)$ of $\mathbb{R}^d$, and so all these $\phi\sigma\omega_j$ lie in the hyperplane $\phi\mathcal{P}(\omega_1)$. As $(\phi\sigma\omega_1,\ldots,\phi\sigma\omega_n)\in B_0(R)$ we have $|\phi\sigma\omega_j|\leq R$. The intersection of a ball with radius R and a hyperplane in $\mathbb{R}^d$ is a ball in some $\mathbb{R}^{d-1}$ with radius $R'\leq R$ and thus, lies in a cube of edge length $2R$. Thus, this set belongs to the class $\mathrm{Lip}(d,1,2R)$. Moreover, its d-dimensional volume is zero. Hence, by Theorem 4.1 we obtain the upper bound

$$\ll\max_{0\leq i<d}\frac{R^i}{\lambda_1\cdots\lambda_i}$$

for the number of $\phi\sigma\omega_j$ for each j satisfying $2\leq j\leq n$.

Next we have to estimate the number of $\phi\sigma\omega_1$. Again, we have $|\phi\sigma\omega_1| \leq R$. Now by virtue of Theorem 4.1 we deduce the following upper bound

$$\ll \frac{R^d}{\det \phi\sigma\mathcal{O}} + \max_{0\leq i<d} \frac{R^i}{\lambda_1 \cdots \lambda_i}$$

for the number of $\phi\sigma\omega_1$. Going right up to the last minimum, we see that this is bounded by

$$\ll \max_{0\leq i\leq d} \frac{R^i}{\lambda_1 \cdots \lambda_i}.$$

Multiplying the bounds for the number of $\phi\sigma\omega_1$ and $\phi\sigma\omega_j$, and then summing over all (of the at most 2^d) strict subfields K_1 of K leads to

$$|\Lambda'| \ll \max_{0\leq i\leq d} \frac{R^i}{\lambda_1 \cdots \lambda_i} \left(\max_{0\leq i<d} \frac{R^i}{\lambda_1 \cdots \lambda_i} \right)^{n-1}.$$

This completes the proof. □

13. Counting projectively primitive points

The height of an element $\boldsymbol{\alpha} = (\alpha_1, \ldots, \alpha_n) \in \mathcal{O}^n \subset \mathcal{O}_K^n$ is given by

$$H(\boldsymbol{\alpha}) = \prod_{i=1}^{r+s} |(1, \sigma_i(\boldsymbol{\alpha}))|_\infty^{d_i/d}.$$

Therefore, and by the definition (5.1) of $Z_I(X^d)$, we have

$$N(\mathcal{O}_I^n(K/k), X) = |Z_I(X^d) \cap \sigma\mathcal{O}^n(K/k)|. \tag{13.1}$$

Recall the definitions of $Z_{F_\mathbf{j}}$, ψ, $\psi_\mathbf{j}$ and F from (7.7), (8.1), (8.5) and (10.1). Also recall that $q' = |I| - 1$. We permute the coordinates of $\sigma\mathcal{O}^n$ and $\sigma\mathcal{O}^n(K/k)$ as in (6.1), so that they become subsets of $\prod_I K_i^n \times \prod_{I^c} K_i^n$. Just as in (10.5) we conclude

$$|\sigma\mathcal{O}^n(K/k) \cap Z_I(T)| = \begin{cases} |\psi Z_I(T) \cap \psi\sigma\mathcal{O}^n(K/k)| & \text{if } q' = 0 \\ \sum_{\mathfrak{m}_F} |\psi_\mathbf{j} Z_{F_\mathbf{j}} \cap \psi_\mathbf{j}\sigma\mathcal{O}^n(K/k)| & \text{if } q' > 0 \end{cases}. \tag{13.2}$$

Of course, the first equation in (13.2) holds always, although we use it only for $q' = 0$. It is well known that $\sigma\mathcal{O}^n$ is a lattice of determinant

$$\det \sigma\mathcal{O}^n = (2^{-s}\sqrt{|\Delta_K|}[\mathcal{O}_K : \mathcal{O}])^n.$$

Proposition 13.1. *Suppose $T \geq 1$ and $n > 1$, and recall that l was defined in Definition 2 (Section 11). If $q' = 0$ then we have*

$$\left| |\psi\sigma\mathcal{O}^n(K/k) \cap \psi Z_I(T)| - \frac{2^{s_K n} \mathrm{Vol} Z_I(T)}{(\sqrt{|\Delta_K|}[\mathcal{O}_K : \mathcal{O}])^n} \right| \ll \frac{T^{n-1/d}}{\lambda_1^{n(l-1)} \lambda_l^{n(d-l+1)-1}},$$

where $\lambda_i = \lambda_i(\psi\sigma\mathcal{O})$. If $q' > 0$ then we have

$$\left| |\psi_\mathbf{j}\sigma\mathcal{O}^n(K/k) \cap \psi_\mathbf{j} Z_{F_\mathbf{j}}| - \frac{2^{s_K n} \mathrm{Vol} Z_{F_\mathbf{j}}}{(\sqrt{|\Delta_K|}[\mathcal{O}_K : \mathcal{O}])^n} \right| \ll \frac{T^{n-1/d}}{\lambda_1^{n(l-1)} \lambda_l^{n(d-l+1)-1}},$$

where $\lambda_i = \lambda_i(\psi_\mathbf{j}\sigma\mathcal{O})$.

Proof. As the case $q' = 0$ can be proven by exactly the same arguments we restrict ourselves to the case $q' > 0$. Let us write $R = \kappa T^{1/d}$, where κ is as in Lemma 8.1, and thus $R \ll T^{1/d}$, and

$$\psi_{\mathbf{j}} Z_{F_{\mathbf{j}}} \subset B_0(R).$$

Put $\Lambda = \psi_{\mathbf{j}}\sigma\mathcal{O}^n$, and recall that $\psi_{\mathbf{j}} \in \mathcal{T}$. The proof splits in two cases. First we assume

$$R < \lambda_l.$$

By Lemma 11.3, and recalling the definition (4.1), we conclude $\psi_{\mathbf{j}}\sigma\mathcal{O}^n(K/k) \subset \Lambda(l)$. As $\psi_{\mathbf{j}} Z_{F_{\mathbf{j}}} \subset B_0(R)$ we get in particular $0 = |\Lambda(l) \cap \psi_{\mathbf{j}} Z_{F_{\mathbf{j}}}| = |\psi_{\mathbf{j}}\sigma\mathcal{O}^n(K/k) \cap \psi_{\mathbf{j}} Z_{F_{\mathbf{j}}}|$. Using Lemma 10.4, $\det \psi_{\mathbf{j}} = 1$, and applying Corollary 4.1 proves the proposition in the first case. Now we assume

$$R \geq \lambda_l.$$

First we ignore the primitivity condition defining $\mathcal{O}^n(K/k)$ and we count all points in $\Lambda(l) \supset \psi_{\mathbf{j}}\sigma\mathcal{O}^n(K/k)$. Again, using Lemma 10.4 and applying Corollary 4.1 yields

$$\left| |\Lambda(l) \cap \psi_{\mathbf{j}}(Z_{F_{\mathbf{j}}})| - \frac{2^{s_K n}\mathrm{Vol}(Z_{F_{\mathbf{j}}})}{(\sqrt{|\Delta_K|}[\mathcal{O}_K : \mathcal{O}])^n} \right| \ll \frac{T^{n-1/d}}{\lambda_1^{n(l-1)}\lambda_l^{n(d-l+1)-1}}.$$

Next we estimate the number of points in $\Lambda(l) \cap \psi_{\mathbf{j}}(Z_{F_{\mathbf{j}}})$ that do not generate K/k (in the projective sense), i.e., that do not lie in $\psi_{\mathbf{j}}\sigma\mathcal{O}^n(K/k)$. To this end we apply Lemma 12.1. Using $R \geq \lambda_l$ we get the following upper bound for these

$$\ll \max_{0 \leq i \leq d} \frac{R^i}{\lambda_1 \cdots \lambda_i} \left(\max_{0 \leq i < d} \frac{R^i}{\lambda_1 \cdots \lambda_i} \right)^{n-1} \leq \frac{R^d}{\lambda_1^{l-1}\lambda_l^{d-l+1}} \left(\frac{R^{d-1}}{\lambda_1^{l-1}\lambda_l^{d-l}} \right)^{n-1}.$$

As $n > 1$ we see that the latter is

$$\leq \frac{R^{dn-1}}{\lambda_1^{n(l-1)}\lambda_l^{n(d-l+1)-1}} \ll \frac{T^{n-1/d}}{\lambda_1^{n(l-1)}\lambda_l^{n(d-l+1)-1}}.$$

This concludes the proof of the proposition. □

Recall the definitions of $\eta_{\mathcal{O}}$ and μ_g from (2.1) and (2.2) respectively.

Lemma 13.2. *Suppose $X \geq 1$ and $n > 1$. If $q' = 0$ then*

$$\left| |\psi\sigma\mathcal{O}^n(K/k) \cap \psi Z_I(T)| - \frac{2^{s_K n}\mathrm{Vol} Z_I(T)}{(\sqrt{|\Delta_K|}[\mathcal{O}_K : \mathcal{O}])^n} \right| \ll \sum_{g \in G(K/k)} \frac{T^{n-1/d}}{\eta_{\mathcal{O}}^{dn-1}\delta_g(K/k)^{\mu_g}}.$$

If $q' > 0$ then

$$\left| |\psi_{\mathbf{j}}\sigma\mathcal{O}^n(K/k) \cap \psi_{\mathbf{j}} Z_{F_{\mathbf{j}}}| - \frac{2^{s_K n}\mathrm{Vol} Z_{F_{\mathbf{j}}}}{(\sqrt{|\Delta_K|}[\mathcal{O}_K : \mathcal{O}])^n} \right| \ll \sum_{g \in G(K/k)} \frac{T^{n-1/d}}{\eta_{\mathcal{O}}^{dn-1}\delta_g(K/k)^{\mu_g}}.$$

Proof. Recall that ψ and $\psi_{\mathbf{j}}$ are in $\mathcal{T}$, and thus, to estimate the successive minima we can apply the results from Section 11 with $\phi = \psi_{\mathbf{j}}$ and $\phi = \psi$ respectively. Let $K_0 = k(\frac{\theta_1}{\theta_1}, \ldots, \frac{\theta_{l-1}}{\theta_1})$ if $l \geq 2$, and let $K_0 = k$ if $l = 1$, and put $g = [K_0 : k]$. In particular, we have $g \in G(K/k)$. Therefore, and by Proposition 13.1, it suffices to show

$$\lambda_1^{n(l-1)}\lambda_l^{n(d-l+1)-1} \gg \eta_{\mathcal{O}}^{dn-1}\delta_g(K/k)^{\mu_g}. \tag{13.3}$$

First suppose $l = l(\phi) \geq 2$. Then by Lemma 11.4 we have $n(d-l+1)-1 \geq \mu_g$, and thus, (13.3) follows immediately from Lemma 11.2. Now suppose $l = 1$. Then $\delta_g(K/k) = 1$ and thus, (13.3) follows again from Lemma 11.2. This proves the lemma. □

14. PROOF OF THEOREM 2.1

We start with the case $n = 1$. Hence, by hypothesis, we have $k = K$. From (13.1) and since $\mathbf{0} \notin Z_I(X^d)$ we obtain

$$N(\mathcal{O}_I(K/K), X) = |\sigma\mathcal{O}(K/K) \cap Z_I(X^d)| = |\sigma\mathcal{O} \cap Z_I(X^d)|.$$

Applying Theorem 5.1 with $\Lambda = \sigma\mathcal{O}$ and using Lemma 11.1 yields

$$\left| N(\mathcal{O}_I(K/K), X) - \frac{2^{s_K}\mathrm{Vol} Z_I(X^d)}{(\sqrt{|\Delta_K|}[\mathcal{O}_K : \mathcal{O}])} \right| \leq c(1,d)\frac{(\log^+ X)^{q'} X^{d-1}}{\eta_{\mathcal{O}}^{d-1}}.$$

This proves Theorem 2.1 for $n = 1$.

Now we assume $n > 1$. Combining Lemma 13.2, (13.1) and (13.2) yields for $q' = 0$

$$\left| N(\mathcal{O}_I^n(K/k), X) - \frac{2^{s_K n}\mathrm{Vol} Z_I(X^d)}{(\sqrt{|\Delta_K|}[\mathcal{O}_K : \mathcal{O}])^n} \right| \ll \sum_{g \in G(K/k)} \frac{X^{dn-1}}{\eta_{\mathcal{O}}^{dn-1}\delta_g(K/k)^{\mu_g}}.$$

For $q' > 0$ we additionally use (10.4) to get

$$\left| N(\mathcal{O}_I^n(K/k), X) - \frac{2^{s_K n}\mathrm{Vol} Z_I(X^d)}{(\sqrt{|\Delta_K|}[\mathcal{O}_K : \mathcal{O}])^n} \right| \ll \sum_{\mathfrak{m}_F} \sum_{g \in G(K/k)} \frac{X^{dn-1}}{\eta_{\mathcal{O}}^{dn-1}\delta_g(K/k)^{\mu_g}}.$$

By Lemma 10.6 we know $|\mathfrak{m}_F| \ll (\log^+ X)^{q'}$, and this completes the proof of Theorem 2.1.

15. PROOF OF COROLLARY 2.1

Recall that $\mathcal{O}_\emptyset^n(K/k) = \emptyset$, and thus $N(\mathcal{O}^n(K/k), X) = \sum_I N(\mathcal{O}_I^n(K/k), X)$, where the sum runs over all subsets of $\{1, \ldots, r_K + s_K\}$. Also recall the definition of $Z_\emptyset(X^d)$ from (5.1). As the 2^{r+s} sets $Z_I(T)$ define a partition of $Z(T)$ we see that Corollary 2.1 follows immediately from Theorem 2.1 and the following lemma.

Lemma 15.1. *Suppose $X \geq 1$ and either $n > 1$ or $K = k$. Then*

$$\left| N(\mathcal{O}_\emptyset^n(K/k), X) - \frac{2^{s_K n}\mathrm{Vol} Z_\emptyset(X^d)}{(\sqrt{|\Delta_K|}[\mathcal{O}_K : \mathcal{O}])^n} \right| \ll \sum_{g \in G(K/k)} \frac{1}{\eta_{\mathcal{O}}^{dn-1}\delta_g(K/k)^{\mu_g}}.$$

Proof. We have $\mathcal{O}_\emptyset^n(K/k) = \emptyset$, $\mathrm{Vol} Z_\emptyset(X^d) = (2^{r_K}\pi^{s_K})^n$ and $\det \sigma\mathcal{O} = 2^{-s_K}\sqrt{|\Delta_K|}[\mathcal{O}_K : \mathcal{O}]$. As $\eta_{\mathcal{O}}\delta_g(K/k) \geq 1$ and $\mu_g = mn(e-g) - 1$ it suffices to show that for some $g \in G(K/k)$

$$\sqrt{|\Delta_K|}[\mathcal{O}_K : \mathcal{O}] \gg \eta_{\mathcal{O}}^d \delta_g(K/k)^{m(e-g)}. \tag{15.1}$$

Let ϕ be the identity on $\mathbb{R}^r \times \mathbb{C}^s$, let λ_i be as in (11.2), and let l be as in Definition 2. Then

$$\sqrt{|\Delta_K|}[\mathcal{O}_K : \mathcal{O}] \gg \lambda_1 \cdots \lambda_d \geq \lambda_1^{l-1}\lambda_l^{d-l+1}.$$

If $l = 1$ then $K = k$ and $\delta_g(K/k) = 1$, so that (15.1) follows from the above and Lemma 11.1. If $l \geq 2$ we take $g = [k(\theta_1/\theta_1, \ldots, \theta_{l-1}/\theta_1) : k] \in G(K/k)$. Applying Lemma 11.1, Lemma 11.2 and Lemma 11.4 yields (15.1), and thereby proves the lemma. □

16. Volume computations

Lemma 16.1. *Suppose $q' \geq 0$ and $T \geq 1$. Then we have*

$$\mathrm{Vol}Z_I(T) = 2^{rn}\pi^{sn}(-1)^{q'}\left(-1 + T^n \sum_{i=0}^{q'} \frac{(-\log T^n)^i}{i!}\right).$$

Proof. Put $r' = |I \cap \{1,\ldots,r\}|$ and $s' = |I \cap \{r+1,\ldots,r+s\}|$. From (6.1) we see that $\mathrm{Vol}Z_I(T)$ is given by the product of $2^{(r-r')n}\pi^{(s-s')n}$ and the $d'n$-dimensional volume of the set $\{(\mathbf{z}_i)_I \in \prod_I K_i; \prod_I |\mathbf{z}_i|_\infty^{d_i} \leq T, |\mathbf{z}_i|_\infty \geq 1 \text{ for } i \in I\}$. Denote the latter by $V_{r',s'}(T)$. For the sake of readability let us momentarily rewrite the variables $\mathbf{z}_i$ for $i \in I \cap \{1,\ldots,r\}$ as $\mathbf{x}_1,\ldots,\mathbf{x}_{r'}$ and $\mathbf{z}_i$ for $i \in I \cap \{r+1,\ldots,r+s\}$ as $\mathbf{y}_1,\ldots,\mathbf{y}_{s'}$. Clearly, we have $V_{0,1}(T) = \pi^n(T^n - 1)$, and Fubini's Theorem implies

$$\begin{aligned}
V_{0,s'}(T) &= \int_{1\leq|\mathbf{y}_{s'}|_\infty\leq\sqrt{T}} V_{0,s'-1}(T/|\mathbf{y}_{s'}|_\infty^2)d\mathbf{y}_{s'}\\
&= n\int_{1\leq|y_{s'1}|\leq\sqrt{T}}\int_{0\leq|y_{s'2}|\leq|y_{s'1}|}\cdots\int_{0\leq|y_{s'n}|\leq|y_{s'1}|} V_{0,s'-1}(T/|y_{s'1}|^2)dy_{s'n}\cdots dy_{s'1}\\
&= n\int_{1\leq|y_{s'1}|\leq\sqrt{T}}(\pi|y_{s'1}|^2)^{n-1}V_{0,s'-1}(T/|y_{s'1}|^2)dy_{s'1}\\
&= n\int_1^{\sqrt{T}}\int_0^{2\pi}\varrho(\pi\varrho^2)^{n-1}V_{0,s'-1}(T/\varrho^2)d\theta d\varrho\\
&= 2\pi^n n\int_1^{\sqrt{T}}\varrho^{2n-1}V_{0,s'-1}(T/\varrho^2)d\varrho.
\end{aligned}$$

By induction we conclude

$$V_{0,s'}(T) = \pi^{s'n}\left((-1)^{s'} + \sum_{i=0}^{s'-1}\frac{(-1)^{s'-1-i}n^i}{i!}T^n(\log T)^i\right).$$

Again, by Fubini's Theorem we find

$$\begin{aligned}
V_{r',s'}(T) &= \int_{1\leq|\mathbf{x}_{r'}|_\infty\leq T} V_{r'-1,s'}(T/|\mathbf{x}_{r'}|_\infty)d\mathbf{x}_{r'}\\
&= 2^n n\int_1^T x_{r'1}^{n-1}V_{r'-1,s'}(T/x_{r'1})dx_{r'1}.
\end{aligned}$$

Once more a simple induction argument shows

$$\begin{aligned}
V_{r',s'}(T) &= 2^{r'n}\pi^{s'n}\left((-1)^{q'-1} + \sum_{i=0}^{q'}\frac{(-1)^{q'-i}n^i}{i!}T^n(\log T)^i\right)\\
&= 2^{r'n}\pi^{s'n}(-1)^{q'}\left(-1 + T^n\sum_{i=0}^{q'}\frac{(-\log T^n)^i}{i!}\right).
\end{aligned}$$

As $\mathrm{Vol}Z_I(T) = 2^{(r-r')n}\pi^{(s-s')n}V_{r',s'}(T)$ the lemma is proved. □

Lemma 16.2. *Suppose $T \geq 1$. Then we have*

$$\mathrm{Vol}Z(T) = \sum_{i=0}^{q} c_i T^n(\log T^n)^i,$$

where

$$c_i = \frac{2^{rn}\pi^{sn}}{i!}\binom{q}{i}.$$

Proof. Clearly, we have $\mathrm{Vol}Z(T) = \sum_I \mathrm{Vol}Z_I(T)$, where the sum runs over all subsets I of $\{1,\ldots,r+s\}$. Now in order to compute the coefficient c_i we have to sum the contribution from each $\mathrm{Vol}Z_I(T)$. First note that

$$2^{rn}\pi^{sn}\sum_I(-1)^{q'+1} = 2^{rn}\pi^{sn}\sum_{j=0}^{q+1}(-1)^j\binom{q+1}{j} = 0.$$

It remains to compute the coefficients c_i. The contribution of $\mathrm{Vol}Z_I(T)$ is zero if $q' = |I|-1 < i$, and

$$2^{rn}\pi^{sn}\frac{(-1)^{q'+i}}{i!}$$

if $q' \geq i$. As we have $\binom{q+1}{q'+1}$ sets I of cardinality $q'+1$ we conclude

$$c_i = \frac{2^{rn}\pi^{sn}}{i!}\sum_{q'=i}^{q}(-1)^{i+q'}\binom{q+1}{q'+1} = \frac{2^{rn}\pi^{sn}}{i!}\binom{q}{i}.$$

This concludes the proof of the lemma. □

17. Upper bounds for the non-projectively primitive points

Recall the definition of the set of non-projectively primitive points in $\mathcal{O}_K^n$

$$\mathcal{O}_{npp}^n(K/k) = \{\boldsymbol{\alpha} \in \mathcal{O}_K^n \backslash \mathcal{O}_K^n(K/k); k(\boldsymbol{\alpha}) = K\}.$$

Let $k(n;e)$ be the subset of $\overline{k}^n$ of points $\boldsymbol{\alpha}$ with $[k(\boldsymbol{\alpha}):k] = e$. Schmidt [24, Theorem] has shown the following estimate:

$$N(k(n;e),X) \leq c_2(m,e,n)X^{me(n+e)}, \tag{17.1}$$

where $c_2(m,e,n) = 2^{me(e+n+3)+e^2+n^2+10e+10n}$.

Lemma 17.1. *Suppose $e > 1$. Then we have*

$$\sum_{\mathcal{C}_e(k)} N(\mathcal{O}_{npp}^n(K/k),X) \ll \sup_{g|e} X^{m(g^2+gn+e^2/g+e)},$$

where the supremum runs over all positive divisors $g < e$ of e. Moreover, for $e = 1$ (and $X \geq 1$) we have

$$\sum_{\mathcal{C}_e(k)} N(\mathcal{O}_{npp}^n(K/k),X) = 1.$$

Proof. If $e = 1$ then $\mathcal{C}_e(k) = \{k\}$ and $\mathcal{O}_{npp}^n(k/k) = \{\mathbf{0}\}$. As $X \geq 1$ the lemma holds. From now on we assume $e > 1$. Then the left-hand side counts points $\boldsymbol{\alpha} = (\alpha_1,\ldots,\alpha_n)$ in $\mathcal{O}_k(e;n)$ with $k(\ldots,\alpha_i/\alpha_j,\ldots) \subsetneq k(\boldsymbol{\alpha})$ and $H(\boldsymbol{\alpha}) \leq X$. First suppose $n = 1$. Then the left-hand side simply counts algebraic integers of degree e over k and height no larger than X. The number of these is by (17.1)

$$\leq c_2(m,e,1)X^{me(e+1)} \ll \sup_{g|e} X^{m(g^2+gn+e^2/g+e)}.$$

This proves the lemma for $n = 1$. Now we assume $n > 1$. As $e > 1$ each $\boldsymbol{\alpha}$ is nonzero, and so we loose only a factor n if we assume $\alpha_1 \neq 0$. Under this assumption $\boldsymbol{\alpha}$ has the form $\boldsymbol{\alpha} = (\theta,\theta\beta_2,\ldots,\theta\beta_n)$ such that with $F = k(\ldots,\alpha_i/\alpha_j,\ldots)$ one has: $k(\boldsymbol{\alpha}) = F(\theta)$ and $k(\beta_2,\ldots,\beta_n) = F$. Furthermore, we have

$$X \geq H(\boldsymbol{\alpha}) = H(\theta,\theta\beta_2,\ldots,\theta\beta_n) = H(1/\theta,\beta_2,\ldots,\beta_n) \geq \max\{H(\theta),H(\beta_2,\ldots,\beta_n)\}.$$

Therefore, it suffices to give an upper bound for the number of $(\beta_2, \ldots, \beta_n, \theta) \in \overline{k}^n$ with

$$[k(\beta_2, \ldots, \beta_n) : k] = g \leq e/2,$$
$$[k(\theta, \beta_2, \ldots, \beta_n) : k(\beta_2, \ldots, \beta_n)] = e/g,$$
$$H(\beta_2, \ldots, \beta_n), H(\theta) \leq X.$$

Let us fix a g as above. From (17.1) we obtain the upper bound

$$c_2(m, g, n-1)X^{mg(g+n)} \tag{17.2}$$

for the number of such vectors $(\beta_2, \ldots, \beta_n)$. Next for each $(\beta_2, \ldots, \beta_n)$ we count the number of θ. Now we have $[k(\theta, \beta_2, \ldots, \beta_n) : k(\beta_2, \ldots, \beta_n)] = e/g$, and, moreover, $H(\theta) \leq X$. Applying (17.1) once more yields the upper bound

$$c_2(mg, e/g, 1)X^{[k(\beta_2,\ldots,\beta_n):\mathbb{Q}](e/g)(e/g+1)} \ll X^{me(e/g+1)} \tag{17.3}$$

for the number of θ, provided $(\beta_2, \ldots, \beta_n)$ is fixed. Multiplying the bound (17.2) for the number of $(\beta_2, \ldots, \beta_n)$ and (17.3) for the number of θ gives the upper bound

$$\ll X^{m(g^2+gn+e^2/g+e)}$$

for the number of tuples $(\beta_2, \ldots, \beta_n, \theta)$. Taking the supremum over all possible values of g proves the lemma. □

18. Proof of Theorem 1.1

We start with a simple lemma. Put

$$\gamma_g = m(g^2 + g + e^2/g + e). \tag{18.1}$$

We remind the reader that $\mu_g = mn(e-g) - 1$ and $C_{e,m} = \max\{2 + \frac{4}{e-1} + \frac{1}{m(e-1)}, 7 - \frac{e}{2} + \frac{2}{me}\}$.

Lemma 18.1. *Suppose $e > 1$, $n > e + C_{e,m}$ and $1 \leq g \leq e/2$. Then we have*

$$\gamma_g - \mu_g \leq -2/e, \tag{18.2}$$

$$m(g^2 + gn + e^2/g + e) \leq men - 1, \tag{18.3}$$

$$(e+2)/4 - n/2 \leq -C_{e,m}/2. \tag{18.4}$$

Proof. Let us write (18.2) as

$$m(g^2 + g + e^2/g + e) - mn(e-g) + 1 + 2/e \leq 0.$$

With

$$F(g) = \frac{g^2 + g + e^2/g + e}{e-g} + \frac{1}{m(e-g)},$$

this means

$$n \geq F(g) + \frac{2}{me(e-g)}. \tag{18.5}$$

As $F(g)$ is a fraction with denominator dividing $mg(e-g)$ we conclude that $n > F(g)$ implies $n \geq F(g) + \frac{1}{mg(e-g)} \geq F(g) + \frac{2}{me(e-g)}$. Hence, it suffices to check $n > F(g)$. Using that $(e-g)e^2/g^3 \geq e^2/g^2$ for $1 \leq g \leq e/2$, one sees that the second derivative $F''(g)$ is positive for $1 \leq g \leq e/2$. Hence, $F(g)$ is here concave, and so it suffices to check that $n > F(1)$ and $n > F(e/2)$, which is equivalent to our hypothesis $n > e + C_{e,m}$. The claim (18.3) is equivalent to

$$n \geq F(g) - \frac{g}{e-g}. \tag{18.6}$$

But we have just seen that (18.5) holds and thus (18.6) holds as well. And, finally, (18.4) follows from the assumptions $n > e + C_{e,m}$ and $e > 1$. This proves the lemma. □

We have the following disjoint union

$$\mathcal{O}_k(n;e) = \bigcup_{\mathcal{C}_e(k)} \mathcal{O}_K^n(K/k) \cup \mathcal{O}_{npp}^n(K/k).$$

Therefore,

$$N(\mathcal{O}_k(n;e), X) = \sum_{\mathcal{C}_e(k)} N(\mathcal{O}_K^n(K/k), X) + \sum_{\mathcal{C}_e(k)} N(\mathcal{O}_{npp}^n(K/k), X). \tag{18.7}$$

Combining Lemma 17.1 and Lemma 18.1 shows that for $e > 1$ and $n > e + C_{e,m}$

$$\sum_{\mathcal{C}_e(k)} N(\mathcal{O}_{npp}^n(K/k), X) \ll X^{men-1}.$$

But by Lemma 17.1 the latter remains trivially true for $e = 1$. Therefore, we may focus on the first sum in (18.7). By virtue of Corollary 2.1 and Lemma 16.2 it suffices to show that the following sums converge

$$\sum_{\mathcal{C}_e(k)} |\Delta_K|^{-n/2}, \tag{18.8}$$

$$\sum_{\mathcal{C}_e(k)} \sum_{g \in G(K/k)} \delta_g(K/k)^{-\mu_g}. \tag{18.9}$$

First suppose $e = 1$. Then $\mathcal{C}_e(k) = \{k\}$ consists of a single field, and, hence, both sums converge. Next we assume

$$e > 1,$$

and thus by hypothesis $n > e + C_{e,m}$. Let us start with the sum in (18.8). Let

$$N_\Delta(\mathcal{C}_e(k), T) = |\{K \in \mathcal{C}_e(k); |\Delta_K| \leq T\}|$$

be the number of fields in $\mathcal{C}_e(k)$ with discriminant no larger than T in absolute value. Schmidt [26] has shown that

$$N_\Delta(\mathcal{C}_e(k), T) \leq c(k,e) T^{(e+2)/4}. \tag{18.10}$$

Ellenberg and Venkatesh [12] have established a better bound for large values of e. However, for our purpose Schmidt's bound is good enough. A simple dyadic summation argument proves the desired convergence. More precisely,

$$\begin{aligned}\sum_{\mathcal{C}_e(k)} |\Delta_K|^{-n/2} = \sum_{i=1}^{\infty} \sum_{\substack{K \in \mathcal{C}_e(k) \\ 2^{i-1} \leq |\Delta_K| < 2^i}} |\Delta_K|^{-n/2} &\leq \sum_{i=1}^{\infty} \frac{N_\Delta(\mathcal{C}_e(k), 2^i)}{2^{(i-1)n/2}} \\ \leq c(k,e) \sum_{i=1}^{\infty} \frac{2^{i(e+2)/4}}{2^{(i-1)n/2}} \qquad &= c(k,e) 2^{n/2} \sum_{i=1}^{\infty} 2^{i((e+2)/4 - n/2)}.\end{aligned}$$

By (18.4) we have $(e+2)/4 - n/2 \leq -C_{e,m}/2 < 0$. Therefore, the last sum converges, and this proves the convergence of (18.8).

To deal with the sum (18.9) we need some more notation and an analogue of (18.10) for the counting function associated to δ_g. We define

$$G_u = \bigcup_{\mathcal{C}_e(k)} G(K/k).$$

Clearly, $G_u \subset \{1,\ldots,[e/2]\}$. Now for any $g \in G_u$ we define

$$\mathcal{C}_e^{(g)}(k) = \{K \in \mathcal{C}_e(k); g \in G(K/k)\}$$

and its counting function

$$N_{\delta_g}(\mathcal{C}_e^{(g)}(k), T) = |\{K \in \mathcal{C}_e^{(g)}(k); \delta_g(K/k) \leq T\}|.$$

Lemma 18.2. *For g in G_u, and γ_g as in (18.1) we have*

$$N_{\delta_g}(\mathcal{C}_e^{(g)}(k), T) \ll T^{\gamma_g}.$$

Proof. Since $H(\alpha_1, \alpha_2) \geq \max\{H(\alpha_1), H(\alpha_2)\}$ it suffices to show that the number of tuples $(\alpha_1, \alpha_2) \in \overline{k}^2$ with

$$\begin{aligned}
&[k(\alpha_1) : k] = g,\\
&[k(\alpha_1, \alpha_2) : k(\alpha_1)] = e/g,\\
&H(\alpha_1), H(\alpha_2) \leq T
\end{aligned}$$

is $\ll T^{\gamma_g}$. But the latter can be shown exactly in the same manner as in the proof of Lemma 17.1. □

Now we can show the convergence of (18.9). We proceed similar as for (18.8).

$$\begin{aligned}
\sum_{K \in \mathcal{C}_e(k)} \sum_{g \in G(K/k)} \delta_g(K/k)^{-\mu_g} &= \sum_{g \in G_u} \sum_{K \in \mathcal{C}_e^{(g)}(k)} \delta_g(K/k)^{-\mu_g}\\
&= \sum_{g \in G_u} \sum_{i=1}^{\infty} \sum_{\substack{K \in \mathcal{C}_e^{(g)}(k)\\ 2^{i-1} \leq \delta_g(K/k) < 2^i}} \delta_g(K/k)^{-\mu_g}\\
&\leq \sum_{g \in G_u} \sum_{i=1}^{\infty} \frac{N_{\delta_g}(\mathcal{C}_e^{(g)}(k), 2^i)}{2^{(i-1)\mu_g}}\\
&\ll \sum_{g \in G_u} \sum_{i=1}^{\infty} 2^{i(\gamma_g - \mu_g)}.
\end{aligned}$$

By (18.2) we have $\gamma_g - \mu_g \leq -2/e$, and this proves the convergence of (18.9). Therefore, the proof of Theorem 1.1 is complete.

Acknowledgements

I would like to thank the referees for carefully reading the manuscript and for providing various helpful comments.

References

1. F. Barroero, *Counting algebraic integers of fixed degree and bounded height*, Monatsh. Math. **175, no.1** (2014), 25–41.
2. ———, *Algebraic S-integers of fixed degree and bounded height*, Acta Arith. **167** (2015), 67–90.
3. M. Bhargava, *The density of discriminants of quartic rings and fields*, Ann. of Math. **162** (2005), 1031–1063.
4. ———, *The density of discriminants of quintic rings and fields*, Ann. of Math. **172** (2010), 1559–1591.
5. E. Bombieri, *Problems and results on the distribution of algebraic points on algebraic varieties*, J. Théor. Nombres Bordeaux **21** (2009), 41–57.
6. J. W. S. Cassels, *An Introduction to the Geometry of Numbers*, Springer, 1997.
7. A. Chambert-Loir and Y. Tschinkel, *Integral points of bounded height on toric varieties*, preprint (2010).
8. ———, *Integral points of bounded height on partial equivariant compactifications of vector groups*, Duke Math. J. **161** (2012), 2799–2836.
9. S-J. Chern and J. D. Vaaler, *The distribution of values of Mahler's measure*, J. reine angew. Math. **540** (2001), 1–47.

10. B. Datskovsky and D. J. Wright, *Density of discriminants of cubic field extensions*, J. reine angew. Math. **386** (1988), 116–138.
11. H. Davenport, *On a principle of Lipschitz*, J. London Math. Soc. **26** (1951), 179–183.
12. J. Ellenberg and A. Venkatesh, *The number of extensions of a number field with fixed degree and bounded discriminant*, Ann. of Math. **163** (2006), 723–741.
13. J. Franke, Y. I. Manin, and Y. Tschinkel, *Rational points of bounded height on Fano varieties*, Invent. Math. **95** (1989), 421–435.
14. X. Gao, *On Northcott's Theorem*, Ph.D. Thesis, University of Colorado (1995).
15. S. Lang, *Diophantine geometry*, New York, Interscience Publishers (Interscience Tracts in pure and applied Mathematics, 11), 1962.
16. ______, *Fundamentals of Diophantine Geometry*, Springer, 1983.
17. C. Le Rudulier, *Points algébriques de hauteur bornée sur une surface*, in preparation (11.12. 2013), 39 pages.
18. D. W. Masser and J. D. Vaaler, *Counting algebraic numbers with large height I*, Diophantine Approximation - Festschrift für Wolfgang Schmidt (eds. H. P. Schlickewei, K. Schmidt, R. F. Tichy), Developments in Mathematics 16, Springer 2008, (pp.237–243).
19. ______, *Counting algebraic numbers with large height II*, Trans. Amer. Math. Soc. **359** (2007), 427–445.
20. D. G. Northcott, *Periodic points on an algebraic variety*, Ann. of Math. **51** (1950), 167–177.
21. D. Roy and J. L. Thunder, *A note on Siegel's lemma over number fields*, Monatsh. Math. **120** (1995), 307–318.
22. S. H. Schanuel, *On heights in number fields*, Bull. Amer. Math. Soc. **70** (1964), 262–263.
23. ______, *Heights in number fields*, Bull. Soc. Math. France **107** (1979), 433–449.
24. W. M. Schmidt, *Northcott's Theorem on heights I. A general estimate*, Monatsh. Math. **115** (1993), 169–183.
25. ______, *Northcott's Theorem on heights II. The quadratic case*, Acta Arith. **70** (1995), 343–375.
26. ______, *Number fields of given degree and bounded discriminant*, Astérisque **228** (1995), 189–195.
27. J. Silverman, *Lower bounds for height functions*, Duke Math. J. **51** (1984), 395–403.
28. M. M. Skriganov, *Constructions of uniform distributions in terms of geometry of numbers*, Algebra i Analiz **6, no.3** (1994), 200–230.
29. ______, *Ergodic theory on SL(n), Diophantine approximations and anomalies in the lattice point problem*, Invent. Math. **132, no.1** (1998), 1–72.
30. M. Widmer, *Counting points of fixed degree and bounded height*, Acta Arith. **140.2** (2009), 145–168.
31. ______, *Counting points of fixed degree and bounded height on linear varieties*, J. Number Theory **130** (2010), 1763–1784.
32. ______, *Counting primitive points of bounded height*, Trans. Amer. Math. Soc. **362** (2010), 4793–4829.
33. ______, *Lipschitz class, narrow class, and counting lattice points*, Proc. Amer. Math. Soc. **140** (2012), 677–689.

DEPARTMENT OF MATHEMATICS, ROYAL HOLLOWAY, UNIVERSITY OF LONDON, TW20 0EX EGHAM, UK

E-mail address: `martin.widmer@rhul.ac.uk`