Asymptotically Counting Points of Bounded Height

Inauguraldissertation
zur
Erlangung der Würde eines Doktors der Philosophie

vorgelegt der
Philosophisch-Naturwissenschaftlichen Fakultät
der Universität Basel

von

Martin Lucien Widmer

aus
Mosnang SG

Basel, 2007

Genehmigt von der Philosophisch-Naturwissenschaftlichen Fakultät auf Antrag von

Prof. Dr. D.W. Masser und Prof. Dr. J.L. Thunder.

Basel, den 16. Oktober 2007

Prof. Dr. Hans-Peter Hauri
Dekan

Contents

Acknowledgements

First I would like to thank my advisor Prof. David Masser for his indispensable support and all his patience. Without his detailed suggestions and his continuous encouragement this Thesis would not exist. I would like also to thank Prof. Jeffrey Thunder for carefully reading this manuscript.

I am grateful to the Swiss National Science Foundation and the Mathematical Institute of the University of Basel for the financial aid during the time I worked on my Thesis.

Thanks also to my friends Christian, Guido, Irene, Jonas, Philipp, Reto and Vincent for the mental support and for all the discussions during the coffee breaks. I dedicate this Thesis to my mother to whom I owe what I am. Thanks also to my father who encouraged me in many ways. Finally I want to express my gratitude to Renata for the wonderful time we spend together.

Introduction

In this Thesis we shall count points of bounded height, with particular emphasis on asymptotic estimates. We begin by defining the standard example of a height and some of its basic properties, then we will state some important known results and finally we briefly describe the main results of this work.

We start with a short account of heights; for more details we refer to [**3**] or [**22**].

Let K be a finite extension of $\mathbb{Q}$ of degree $[K:\mathbb{Q}]=d$. By a place v of K we mean an equivalence class of non-trivial absolute values on K. The set of all places of K will be denoted by M_K. For each v in M_K we write K_v for the completion of K with respect to the place v and d_v for the local degree defined by $d_v=[K_v:\mathbb{Q}_w]$ where w denotes the place in $M_{\mathbb{Q}}$ we get by restricting v to $\mathbb{Q}$. A place v in M_K corresponds either to a non-zero prime ideal $\mathfrak{p}_v$ in the ring of integers $\mathcal{O}_K$ or to a complex embedding σ_v of K into $\mathbb{C}$. If v comes from a prime ideal we call v a finite or non-archimedean place indicated by $v\nmid\infty$ and if v corresponds to an embedding we say v is a infinite or archimedean place abbreviated to $v\mid\infty$. For each place in M_K we choose a representative $|\cdot|_v$, normalized in the following way: if v is finite and $\alpha\neq 0$ we set by convention

$$|\alpha|_v = N\mathfrak{p}_v^{-\frac{ord_{\mathfrak{p}_v}(\alpha\mathcal{O}_K)}{d_v}}$$

where $N\mathfrak{p}_v$ denotes the norm of $\mathfrak{p}_v$ from K to $\mathbb{Q}$ and $ord_{\mathfrak{p}_v}(\alpha\mathcal{O}_K)$ is the power of $\mathfrak{p}_v$ in the prime ideal decomposition of the fractional ideal $\alpha\mathcal{O}_K$. Moreover we set

$$|0|_v = 0.$$

And if v is infinite we define

$$|\alpha|_v = |\sigma_v(\alpha)|.$$

Suppose α is in $K^* = K\backslash\{0\}$ then $|\alpha|_v \neq 1$ holds only for a finite number of places v.

Throughout the Introduction n will denote a natural number, which in this Thesis always means a positive rational integer. The height on K^{n+1} is defined by

$$H(\alpha_0, ..., \alpha_n) = \prod_{M_K} \max\{|\alpha_0|_v, ..., |\alpha_n|_v\}^{\frac{d_v}{d}}. \tag{0.0.1}$$

Due to the remark above this is in fact a finite product. Furthermore this definition is independent of the field K containing the coordinates (see [**3**] Lemma 1.5.2 or [**22**] p.51,52) and therefore defines a height on $\overline{\mathbb{Q}}^{n+1}$ for an algebraic closure $\overline{\mathbb{Q}}$ of $\mathbb{Q}$. Immediately from the definition we get

$$H(1, \alpha_1, ..., \alpha_n) \geq \max\{H(1, \alpha_1), ..., H(1, \alpha_n)\}. \tag{0.0.2}$$

The height $H(1, \alpha)$ of a number α can be expressed using the minimal polynomial $a_0x^d + ... + a_d$ in $\mathbb{Z}[x]\backslash\{0\}$ with coprime coefficents, $a_0 > 0$ and of minimal degree which has α as a root. We call d the degree of α. Over the complex numbers the minimal polynomial of α factors as, say $a_0(x - \zeta_1)...(x - \zeta_d)$, and then

$$H(1, \alpha) = (a_0 \prod_{i=1}^{d} \max\{1, |\zeta_i|\})^{\frac{1}{d}}. \tag{0.0.3}$$

This formula is a consequence of Proposition 1.6.5 and Proposition 1.6.6 in [**3**].

The well-known *product formula* (see [**3**] Proposition 1.4.4) says that

$$\prod_{M_K} |\alpha|_v^{d_v} = 1 \text{ for each } \alpha \text{ in } K^*.$$

This has important consequences, two of them are: for $\boldsymbol{\alpha} \in \overline{\mathbb{Q}}^{n+1}\backslash\{\mathbf{0}\}$ we have $H(\boldsymbol{\alpha}) \geq 1$, and the value of the height in (0.0.1) does not change if we multiply each coordinate with a fixed element of K^*. Therefore one can define a height on points $P = (\alpha_0 : ... : \alpha_n)$ in $\mathbb{P}^n(\overline{\mathbb{Q}})$ by

$$H(P) = H(\alpha_0, ..., \alpha_n).$$

This is the absolute non-logarithmic projective Weil height or simpler Weil height. A projective point $P = (\alpha_0 : ... : \alpha_n)$ in $\mathbb{P}^n(\overline{\mathbb{Q}})$ has also a

natural degree defined as

$$[\mathbb{Q}(P):\mathbb{Q}]$$

where $\mathbb{Q}(P)$ denotes the extension we get by adjoining all ratios α_i/α_j $(0 \leq i,j \leq n, \alpha_j \neq 0)$ to $\mathbb{Q}$. At this point we have a finiteness statement usually associated with the name of Northcott due to his result Theorem 1 in [**37**]: *for each positive real number X and each natural number d there are only finitely many points P in $\mathbb{P}^n(\overline{\mathbb{Q}})$ of degree d with $H(P) \leq X$.* If P has degree d then clearly α_i/α_j $(0 \leq i,j \leq n, \alpha_j \neq 0)$ have degree at most d. Appealing to (0.0.2) we see that the above finiteness statement follows from the fact that the number of α's in $\overline{\mathbb{Q}}$ of degree d with $H(1,\alpha) \leq X$ is finite. The latter can be seen using (0.0.3) to bound the number of polynomials $a_0x^d + ... + a_d$ in $\mathbb{Z}[x]$ (see [**3**] Theorem 1.6.8). In this way one gets a trivial upper bound of order of magnitude $X^{(d^2+d)n}$ for the number of points in $\mathbb{P}^n(\overline{\mathbb{Q}})$ of degree d with height not exceeding X. The above finiteness property is fundamental for the concept of heights in particular it allows to associate a counting function

$$Z_H(\mathbf{P},X) = |\{P \in \mathbf{P}; H(P) \leq X\}|$$

to each subset $\mathbf{P}$ of $\mathbb{P}^n(\overline{\mathbb{Q}})$ of bounded degree. If the height is unbounded one might investigate the counting function if the height gets large. More precisely one might try to find an asymptotic estimate for $Z_H(\mathbf{P},X)$.

We will now recapitulate some important well-known results in the context of this Thesis.

Franke, Manin and Tschinkel [**20**] started a program where they investigate the counting functions for rational points on certain classes of varieties. The general thought here is that the asymptotics should reflect geometric properties of the variety. However we stick to rather special varieties and indeed the central set of investigation in our work is

$$\mathbb{P}^n(k;e)$$

the set of points P in $\mathbb{P}^n$ over an algebraic closure $\overline{k}$ of the number field k with relative degree $[k(P):k] = e$. The most well-known result in this direction is probably Schanuel's Theorem [**43**] for $e = 1$, which gives the asymptotics for $\mathbb{P}^n(k;1) = \mathbb{P}^n(k)$ the projective space of dimension n over a number field k. Denote by m the degree of k.

THEOREM 0.1 (Schanuel). *As X tends to infinity one has*

$$Z_H(\mathbb{P}^n(k), X) = S_k(n)X^{m(n+1)} + O(X^{m(n+1)-1}\log X). \tag{0.0.4}$$

The logarithm can be omitted in all cases except for $n = m = 1$. The constant $S_k(n)$ involves all classical field invariants more precisely

$$S_k(n) = \frac{h_k R_k}{w_k \zeta_k(n+1)} \left(\frac{2^{r_k}(2\pi)^{s_k}}{\sqrt{|\Delta_k|}}\right)^{n+1} (n+1)^{r_k+s_k-1}.$$

Here h_k is the class number, R_k the regulator, w_k the number of roots of unity in k, ζ_k the Dedekind zeta-function of k, Δ_k the discriminant, r_k is the number of real embeddings of k and s_k is the number of pairs of distinct complex conjugate embeddings of k. Several authors including Evertse [**15**], Schmidt [**48**], Loher [**28**] and Loher-Masser [**29**] proved explicit upper bounds for $Z_H(\mathbb{P}^n(k), X)$ which are independent of the detailed field structure.

What is known for $e > 1$? Let P be in $\mathbb{P}^n(k; e)$ then $[\mathbb{Q}(P) : \mathbb{Q}] \leq me$. The trivial bound mentioned on the previous page yields therefore a bound for $Z_H(\mathbb{P}^n(k; e), X)$ involving the exponent $((me)^2 + me)n$ of X. The first non-trivial bounds for $Z_H(\mathbb{P}^n(k; e), X)$ are due to Schmidt [**48**].

THEOREM 0.2 (Schmidt). *There are positive constants $c = c(k, e, n)$, $C = C(k, e, n)$ depending on k, e, n such that*

$$cX^{me(\max\{e,n\}+1)} \leq Z_H(\mathbb{P}^n(k; e), X) \leq CX^{me(e+n)} \tag{0.0.5}$$

where the upper bound holds for $X > 0$ and the lower bound holds for $X \geq X_0(k, e, n)$ depending also on k, e, n.

So it turned out that the central problem is the following (see also [**47**] p.27).

PROBLEM 0.1. *Find (when possible) an asymptotic estimate for the counting function $Z_H(\mathbb{P}^n(k; e), X)$ as X tends to infinity.*

Schanuel's Theorem yields the asymptotics for $e = 1$ but already with $e = 2$ the problem becomes far more difficult even if one replaces the arbitrary k in Schanuel's Theorem by $\mathbb{Q}$. And indeed for arbitrary k and $e, n > 1$ not even the correct order of magnitude is known. Nevertheless Schmidt [**49**] made a first big step towards solving Problem 0.1.

THEOREM 0.3 (Schmidt). *As X tends to infinity one has*

$$Z_H(\mathbb{P}^n(\mathbb{Q};2),X) = \begin{cases} D_1X^6 + O(X^4\log X) & \text{if } n=1 \\ D_2X^6\log X + O(X^6\sqrt{\log X}) & \text{if } n=2 \\ D_nX^{2(n+1)} + O(X^{2n+1}) & \text{if } n>2 \end{cases}.$$

In fact Schmidt's result was more precise since it gave the asymptotics for real and imaginary quadratic points separately. Here $D_1 = \frac{8}{\zeta(3)}$, $D_2 = \frac{8(12+\pi^2)}{\zeta(3)^2}$ and $D_n = D(\mathbb{Q},2,n)$ is given by the sum

$$D(\mathbb{Q},2,n) = \sum_K S_K(n)$$

where the sum runs over all quadratic extensions K. The reader might be confused by the different style of representation for these constants but this partially reflects the different nature of the proofs. Schmidt proved also a similar result for a more general definition of height and showed that this leads to asymptotic formulae for the number of decomposable quadratic forms $f(x_0,...,x_n) = \sum_{0\le i\le j\le n} a_{ij}x_ix_j$ with coefficients a_{ij} in $\mathbb{Z}$ having $|a_{ij}| \le X$ and moreover for the number of symmetric $(n+1)\times(n+1)$ matrices with rank ≤ 2 such that $b_{ii}\in\mathbb{Z}$, $|b_{ii}|\le X$ and $2b_{ij}\in\mathbb{Z}$, $2|b_{ij}|\le X$ for $i\ne j$. Already way back in 1967 Schmidt [**16**] introduced more general classes of heights where the max-norm in (0.0.1) at the infinite places is replaced by an arbitrary but fixed distance function. More recently Thunder [**59**] and Roy-Thunder [**40**] introduced "twisted heights" which allow also modifications at the finite places.

One year after Schmidt's article on quadratic points his Ph.D. student Gao [**17**] covered all cases where $n > e > 2$ but still with $k = \mathbb{Q}$ only. Unfortunately Gao's result was not published but we are very grateful to Gao Xia for showing us his work.

THEOREM 0.4 (Gao). *For $n > e > 2$ and as X tends to infinity one has*

$$Z_H(\mathbb{P}^n(\mathbb{Q};e),X) = D(\mathbb{Q},e,n)X^{e(n+1)} + O(X^{e(n+1)-1}).$$

The constant $D(\mathbb{Q},e,n)$ is given by the infinite sum $D(\mathbb{Q},e,n) = \sum_K S_K(n)$ where the sum runs over all extensions K of $\mathbb{Q}$ of degree e.

The audacious strategy of Schmidt and Gao was to prove a result similar to (0.0.4) but with $\mathbb{P}^n(K)$ replaced by $\mathbb{P}^n(K/\mathbb{Q})$ the subset of primitive points in $\mathbb{P}^n(K)$; by definition these satisfy $K = \mathbb{Q}(P)$. Now $\mathbb{P}^n(\mathbb{Q};e)$ is a disjoint union of the sets $\mathbb{P}^n(K/\mathbb{Q})$ where K runs over all number fields of degree e. For each $\mathbb{P}^n(K/\mathbb{Q})$ the main term remains

the same as in (0.0.4) but Schmidt (for $e = 2$) could replace the error term by

$$O(\frac{\sqrt{h_K R_K \log(3 + h_K R_K)}}{|\Delta_K|^{n/2}} X^{2n+1}) \tag{0.0.6}$$

where the constant in O depends only on n but is independent of the field K (for a completely explicit version see [**61**]). This is the major step of the proof and involves many very clever new ideas. Now one can sum over all quadratic number fields and the Theorem of Siegel-Brauer ensures that the sum over the main terms $S_K(n)$ as well as over the error terms converges provided $n > 2$. For similar reasons the restriction $n > e$ in Gao's result appears. However for $1 \leq n \leq e$ Gao found also that the correct order of magnitude of $Z_H(\mathbb{P}^n(\mathbb{Q}; e), X)$ is $X^{e(e+1)}$. Here the asymptotics are still unknown, even in the case $e = 3$ and $n = 2$ of cubic points in two dimensions.

A completely different strategy was used first by Schmidt for $e = 2$ and then by Masser and Vaaler [**33**] for arbitrary e to find the asymptotics for $n = 1$. Here the quadratic case is rather easy using (0.0.3) and expressing the height via coefficients of its minimal polynomial. But for degree 3 one needs Cardano's quite complicated formula and already for $e > 4$ there is no analogue of the latter. However Masser and Vaaler [**34**] realized that Chern and Vaaler's intricate volume computations in [**8**] lead to the asymptotics for numbers of fixed degree not only of fixed degree over $\mathbb{Q}$ but in fact also for the number of fixed degree over any fixed number field k.

THEOREM 0.5 (Masser, Vaaler). *Let k be a number field with $[k : \mathbb{Q}] = m$. Then as X tends to infinity one has*

$$Z_H(\mathbb{P}(k; e), X) = eV_{\mathbb{R}}(e)^{r_k} V_{\mathbb{C}}(e)^{s_k} S_k(e) X^{me(e+1)} + O(X^{me(e+1)-e} \log X).$$

The constants $V_{\mathbb{R}}(e), V_{\mathbb{C}}(e)$ have their origins in [**8**]. Moreover the logarithm can be omitted in all cases except $(m, e) = (1, 1)$ and $(m, e) = (1, 2)$. Theorem 0.5 was the first asymptotic result for arbitrary number fields k and $e > 1$. Very roughly speaking Masser and Vaaler's idea was to interpret the height of the root of an irreducible polynomial in $k[x]$ of fixed degree e as a suitable height of the coefficient vector of this polynomial and to proceed by counting minimal polynomials with respect to this modified height. To carry out this plan they had to generalize the class of heights introduced by Schmidt allowing now different distance functions at the infinite places not only one as Schmidt did. On the other hand Masser and Vaaler had to impose a technical

condition, associated with the name of Lipschitz, on the boundaries of the unit balls given by the respective distance function. They therefore introduced so-called Lipschitz systems, giving what one could call Lipschitz heights.

Unfortunately the proof of Masser and Vaaler's Theorem shed no light on the case $n > 1$ and we emphasize that for $k \neq \mathbb{Q}$ and $e, n > 1$ not even the correct order of magnitude is known. But Schmidt already conjectured that for (0.0.5) his lower bounds are nearer the truth than the upper bounds.

We now describe our own main results. In short; we will establish asymptotic estimates for the counting functions of $\mathbb{P}^n(k; e) \cap \mathbb{P}^n(K)$, $\mathbb{P}^n(k; e)$ and $\mathbb{P}^n(k; e) \cap \mathbb{V}(\overline{k})$ where K is an extension of k of degree e and $\mathbb{V}$ is a linear projective variety. These results are contained in Chapter 3, 4 and 5. We proceed with a more detailed account of each of these chapters.

In Chapter 3 we investigate $\mathbb{P}^n(K/k) = \mathbb{P}^n(k; e) \cap \mathbb{P}^n(K)$ the set of points in $\mathbb{P}^n(K)$ generating K over k. We start by generalizing Masser and Vaaler's Lipschitz systems (see [**34**]) to Arakelov-Lipschitz systems $\mathcal{N}$ on K of dimension n. These provide heights $H_{\mathcal{N}}$ on $\mathbb{P}^n(K)$ where one allows also arbitrary norms at a finite number of finite places. First of all this is natural in view of the equal status of all places on a number field. But it is also essential to deduce the results in Chapter 5. We then investigate the counting function $Z_{\mathcal{N}}$ of $\mathbb{P}^n(K/k)$ with respect to the height $H_{\mathcal{N}}$. Having in mind the above plan of summing these counting functions over all extensions K of k of fixed relative degree we derive an error term which is particular good with respect to the field K. Schmidt (see (0.0.6)) and Gao [**17**] expressed the error term using the discriminant whereas we need a new invariant $\delta(K/k)$. This is a slight generalization of an invariant $\delta(K) = \delta(K/\mathbb{Q})$ introduced by Roy and Thunder [**39**]. The reason for this is that the summatory properties for $\delta(K/k)$ are much easier to prove than those for the discriminants, which are still governed by difficult conjectures such as Linnik's Conjecture (see [**14**]). The latter is proved only for very special cases although great progress was achieved by the recent work of Ellenberg and Venkatesh [**14**].

We can now state the first result of Chapter 3.

COROLLARY 0.1. *Let k, K be number fields with $k \subseteq K$ and $[K : k] = e$, $[k : \mathbb{Q}] = m$, $[K : \mathbb{Q}] = d$. Let $\mathcal{N}$ be an Arakelov-Lipschitz system of dimension n on K. Then as X tends to infinity we have*

$$\begin{aligned} Z_{\mathcal{N}}(\mathbb{P}^n(K/k), X) =& 2^{-r_K(n+1)}\pi^{-s_K(n+1)}V_{\mathcal{N}}S_K(n)X^{d(n+1)} \\ &+O(A_{\mathcal{N}}\frac{h_K R_K}{\delta(K/k)^{\frac{d(n+1)}{2}-1}}X^{d(n+1)-1}\log X) \end{aligned}$$

where the implied constant in O depends only on n and d.

We will define neither $A_{\mathcal{N}}$ nor $V_{\mathcal{N}}$ here but let us point out that the dependence on $\mathcal{N}$ in the error term is explicitly given by $A_{\mathcal{N}}$. The quantity $V_{\mathcal{N}}$ can be considered as some sort of global volume which, for a height $H_{\mathcal{N}}$ with max-norms at all finite places, reduces just to the product of the volumes of the unit balls with respect to the distance functions appearing at the infinite places. Just as Schmidt's error term (0.0.6) for $k = \mathbb{Q}$ and $e = 2$ the error term in Corollary 0.1 converges if summed over all extensions K of relative degree e, at least if $n > 4e$.

The previous corollary follows from the main result of Chapter 3, Theorem 3.1. Here we express the error term in terms of a bunch of new invariants $\delta_g(K/k)$ which are refinements of $\delta(K/k)$. Thus for a fixed K each error term splits up in a sum of $\delta_g(K/k)$. This refinement enables us to reduce n from $4e$ to about $5e/2$ in Chapter 4, and we will further discuss the advantage of these invariants in Chapter 4. Theorem 3.1 is the main technical theorem and somehow the core of this work. It has various applications such as the results in Chapter 4 and Chapter 5. Moreover one can derive the asymptotics for algebraic numbers generating a field over $\mathbb{Q}$ of degree mn containing an unspecified subfield of degree m provided n is much larger than m. This leads also to information on the distribution of number fields of degree d containing a proper intermediate field if ordered via the function δ, for more details we refer to [**62**]. Furthermore one gets a generalized version of Proposition in [**34**] with a particularly good error term. It is most likely that using this generalized Proposition and following the ideas of Masser and Vaaler in [**34**] one can deduce the asymptotics for points of fixed degree on arbitrary lines. Also the somewhat degenerate case $k = K$ (here Theorem 3.1 and Corollary 0.1 coincide) has applications using in an essential way the explicit dependence on $\mathcal{N}$ in the error term (see the announcements below).

Theorem 3.1 could be proved in a slightly more general form (using AGL-heights as in Appendix B) but only at the expense that more

effort is needed to apply the Theorem. However this slight generalization would provide asymptotic results for the number of decomposable forms as shown by Schmidt [**49**] and Gao [**17**]. But they considered only forms defined over $\mathbb{Q}$ while the modified Theorem 3.1 would give asymptotic results for forms defined over arbitrary number fields. What is more, counting results for decomposable forms sometimes easily translate into counting results for symmetric matrices of bounded rank (see for example [**49**] p.346). We expect this list of applications to Theorem 3.1 not to be exhaustive.

We now move to Chapter 4. It deals with the set $\mathbb{P}^n(k;e)$ and contains the main result of this Thesis. First we take up the definition of an Arakelov-Lipschitz system on a number field and we define a uniform Arakelov-Lipschitz system on the collection of all extensions of k of degree e. This then gives rise to a class of heights $H_{\mathcal{N}}$ defined on $\mathbb{P}^n(k;e)$. The Main Theorem asymptotically estimates the counting function of $\mathbb{P}^n(k;e)$ with respect to the height $H_{\mathcal{N}}$. Here we state it only in the simplest form choosing a special uniform Arakelov-Lipschitz system by taking max-norms at all places. Then the corresponding Arakelov-Lipschitz height $H_{\mathcal{N}}$ becomes just the Weil height H. Write

$$D = D(k,e,n) = \sum_K S_K(n)$$

where the sum runs over all extensions of k of degree e.

THEOREM 0.6. *Let e, n be positive integers and k a number field of degree m and suppose that $n > 5e/2 + 4 + 2/(me)$. Then the sum defining D converges and as X tends to infinity we have*

$$Z_H(\mathbb{P}^n(k;e), X) = DX^{me(n+1)} + O(X^{me(n+1)-1}\log X).$$

Thus Theorem 0.6 solves Problem 0.1 for arbitrary k but under the restriction $n > 5e/2 + 4 + 2/(me)$. In particular it determines the correct order of magnitude under the above conditions on e and n. Since Schmidt's and Gao's constraints are only $n > e$ our Theorem 0.6 does not imply their full result. On the other hand it is the first asymptotic result for arbitrary k and $e, n > 1$. Let us give a single new example. We take $n = 11$, $k = \mathbb{Q}(i)$, $e = 2$, so that we are counting points in eleven dimensions quadratic over $\mathbb{Q}(i)$. For the number $Z = Z_H(\mathbb{P}^{11}(\mathbb{Q}(i);2), X)$ of points of height at most X, the Schmidt bounds are $X^{48} \ll Z \ll X^{52}$ for $X \geq X_0$, with absolute implied constants. Our result implies that

$$Z = DX^{48} + O(X^{47}\log X)$$

with

$$D = 12 \cdot (2\pi)^{24} \sum_{\substack{K \\ [K:\mathbb{Q}(i)]=2}} \frac{h_K R_K}{w_K \zeta_K(12) |\Delta_K|^6}.$$

The Main Theorem is quite general since it holds for the wide class of Arakelov-Lipschitz heights. It is in Chapter 5 that we see the advantage of working in such generality. Here we are concerned with some non-trivial subvarieties of projective space.

Various people especially Franke, Manin, Tschinkel, Batyrev, Salberger, Peyre, Thunder and Heath-Brown made progress in estimating the number of rational points of bounded height on certain classes of varieties. Much of this work can probably be extended to points defined over number fields k. But a fundamental obstacle underlies all the work because the points over $\mathbb{Q}$ or k are necessarily restricted via diophantine constraints like Faltings's Theorem [**16**] or the various conjectural generalizations. Indeed the points are often restricted to proper Zariski-closed subsets. However any variety defined over say $\mathbb{Q}$ has a Zariski-dense set of points over $\overline{\mathbb{Q}}$ of sufficiently large fixed degree. Thus one can hope that the behaviour of points of fixed degree should be easier to study.

The case of points over k on a linear variety was treated in great detail by Thunder [**58**] and can be considered as a kind of standard example. We generalize this to points of fixed degree. Thus our Theorem 0.7 below is a first step in estimating the counting function for points of fixed degree on a non-trivial variety.

Let $\mathbb{V}$ be a projective variety in $\mathbb{P}^{N-1}$ and define

$$\mathbb{V}(k;e) = \mathbb{P}^{N-1}(k;e) \cap \mathbb{V}(\overline{k})$$

the set of points on $\mathbb{V}$ of degree e over k. For natural numbers e, n we define the sum

$$\alpha = \alpha(k,e,n) = \sum_K (2^{-r_K} \pi^{-s_K})^{n+1} V(n+1)^{r_K} V(2n+2)^{s_K} S_K(n)$$

where the sum runs over all extensions of k with relative degree e and $V(p)$ denotes the volume of the euclidean ball in $\mathbb{R}^p$ with radius one. A linear projective variety $\mathbb{V}$ defined over a number field has a natural height, for example for a hypersurface it is simply the height of the coefficient vector of any equation defining $\mathbb{V}$. Here it is especially convenient, as Thunder did, to take l^2-heights, which are a very special

case of our Arakelov-Lipschitz heights obtained by taking l^2-norms instead of max-norms at the infinite places. So we write $H_2(\mathbb{V})$ instead of $H(\mathbb{V})$. Similarly we count points of bounded l^2-height, and similarly we abbreviate the counting function to Z_2.

THEOREM 0.7. *Let k be a number field of degree m, let n, e and $N \geq n+2$ be natural numbers, and let $\mathbb{V}$ be a linear subvariety of $\mathbb{P}^{N-1}$ of dimension n defined over k. Suppose that either $e = 1$ or*

$$n > 5e/2 + 4 + 2/(me).$$

Then the sum defining α converges and as X tends to infinity we have

$$Z_2(\mathbb{V}(k;e), X) = \alpha H_2(\mathbb{V})^{-me} X^{me(n+1)} + O(X^{me(n+1)-1} \log X).$$

The constant in O depends only on k, e, n.

The case $e = 1$ was known before and is due to Thunder ([**58**] Theorem 1) but Thunder's proof is different from ours.

Let us illustrate this result with two new examples. The equation

$$x_1 + x_2 + x_3 + x_4 + x_5 + x_6 + x_7 + x_8 + x_9 + x_{10} + x_{11} + x_{12} + x_{13} = 0$$

has

$$\frac{1}{13} \left(\sum_{\substack{K \\ [K:\mathbb{Q}]=2}} (\frac{\pi^6}{2949120})^{r_K} (\frac{1}{479001600})^{s_K} S_K(11) \right) X^{24} + O(X^{23} \log X)$$

pairwise non-proportional solutions of degree 2 over $\mathbb{Q}$ with height less or equal X. Next we take an equation defined over a rather large field:

$$\sqrt{1}x_1 + \sqrt{2}x_2 + \sqrt{3}x_3 + \sqrt{4}x_4 + \sqrt{5}x_5 + \sqrt{6}x_6$$
$$+\sqrt{7}x_7 + \sqrt{8}x_8 + \sqrt{9}x_9 + \sqrt{10}x_{10} + \sqrt{11}x_{11} + \sqrt{12}x_{12} = 0$$

defined over the field $k = \mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5}, \sqrt{7}, \sqrt{11})$. Here we find

$$\frac{1}{78^{32}} \left(\sum_{\substack{K \\ [K:k]=2}} (\frac{\pi^5}{332640})^{r_K} (\frac{1}{39916800})^{s_K} S_K(10) \right) X^{704} + O(X^{703} \log X)$$

pairwise non-proportional solutions of degree 2 over k with height less or equal X.

So much for the new results of this Thesis. But we should also comment on the preliminary Chapters 1 and 2.

Chapter 1 is dedicated to the counting of lattice points in bounded domains of the euclidean space $\mathbb{R}^n$ and lays the ground for all subsequent counting results. In the literature two principles appear. The older one is associated with the name of Lipschitz and is applicable if the boundary of the set can be covered by the images of finitely many maps from $[0,1]^{n-1}$ to $\mathbb{R}^n$ each one satisfying a Lipschitz condition. This principle has been applied by Schanuel [**43**] and was further developed by Schmidt [**51**] and Masser and Vaaler [**34**]. The other method, but formulated for $\mathbb{Z}^n$ only, comes from Davenport [**10**]. It has been generalized to arbitrary lattices by Schmidt [**49**] and [**17**] (see Theorem 1.3 in Chapter 1) and by Thunder [**56**] and [**58**]. The counting principles based on Davenport's method involve conditions which can be difficult to check; one has to control the number of connected components of the intersection of the set with arbitrary lines and what is more not only for the set itself but also for any projection of the set on any subspace. Therefore we are using the Lipschitz approach. The main result of Chapter 1 is Theorem 1.2 which can be seen as the perfect analogue in the Lipschitz context of Schmidt's powerful Theorem 1.3. However the Lipschitz method also involves conditions which are not so straightforward to check but we have carried out this checking very carefully in Chapter 3 and to the best of the author's knowledge this is the first detailed account of such matters in the literature, published and unpublished.

Chapter 2 contains hardly any new results but provides a source of references for results needed in Chapter 4. Furthermore it serves as warm-up for the somewhat technical topic of Arakelov-Lipschitz systems.

In Appendix A we take up Chapter 1 and we compare the Lipschitz conditions with the Davenport conditions. It becomes clear that the former does not imply the latter but that the opposite implication probably does hold in some form. We render this precise by formulating a conjecture, which we prove in some special cases.

In Appendix B we briefly recall Gao's definition of heights [**17**]. His definition is in some sense less general for two reasons: first he allows only the max-norm at the finite places and second he uses the Davenport method which is perhaps more restrictive. But from another point of view Gao's heights are more general and have applications (such as counting decomposable forms) which cannot be deduced directly using our definition of heights. Therefore we generalize our definition of

heights such that they include Gao's heights and we attempt a conjectural version of the Main Theorem for this new definition of heights.

In Chapter 3,4 and 5 we use the O-notation and we will clarify this symbol in Chapter 3. In Chapter 3 and 4 it will be convenient to use $\ll$ and $\gg$ in order to avoid unimportant constants. An expression $A \ll B$ ($A \gg B$) is to be understood as follows: there exists a positive constant c depending only on a specified set of parameters such that $A \leq cB$ ($B \leq cA$). In Chapter 3 the constants in $\ll, \gg$ will depend only on e, n and in Chapter 4 they will depend on e, n and k but we will recall such matters in each chapter.

Finally we would like to announce results which are not further mentioned in this Thesis.

The first result takes up on Masser and Vaaler's Theorem. Let m, n be natural numbers with $n > \max\{6m + 2 + 2/m, m^2 + m\}$. Then as X tends to infinity the number of algebraic numbers α of degree mn such that $\mathbb{Q}(\alpha)$ contains a subfield of degree m and $H(1, \alpha) \leq X$ is asymptotically equal to

$$D'(m, n)X^{mn(n+1)}$$

where $D'(m, n) = \sum_K nV_{\mathbb{R}}(n)^{r_k}V_{\mathbb{C}}(n)^{s_k}S_k(n)$ and the sum runs over all number fields of degree m.

Note that the subfield condition reduces the order of magnitude from $X^{mn(mn+1)}$ to $X^{mn(n+1)}$. As a by-product of the proof we find the following amusing fact: when ordered via the invariant δ then the density of the number fields of degree d containing a proper intermediate field in the set of all number fields of degree d is zero, at least if $d > 6$. This is in stark contrast to when ordered via modulus of the discriminant since Linnik's Conjecture implies one would have positive density provided $d > 1$ is not a prime. For $d = 4$ much more is known: a quartic field has a quadratic subfield if and only if its Galois closure is D_4 or an abelian group of order four. Malle [**31**] has given conjectural asymptotics for $\Delta_G(e, X)$ the number of fields of degree e having Galois closure isomorphic to G and modulus of the discriminant not larger than X. But this is proved only in very special cases. However Bhargava's work [**2**] implies $\Delta_{S_4}(4, X)$ is asymptotically equal to λX

for

$$\lambda = \frac{5}{6}\prod_{p}\left(1+\frac{1}{p^2}-\frac{1}{p^3}-\frac{1}{p^4}\right) = 1.01389....$$

And according to Cohen, Diaz y Diaz and Olivier [**12**] the number $\Delta_{D_4}(4,X)$ with dihedral group is asymptotically equal to μX where $\mu = 0.1046520224....$ It is also known that abelian groups G of order four occur rarely more precisely $\Delta_G(4,X) = o(X)$. Thus when we order by absolute value of the discriminant the probability that a quartic field has a quadratic subfield is the positive number

$$\frac{\mu}{\mu+\lambda} = 0.09356....$$

The second result solves a problem due to Loher and Masser. In [**29**] they give upper bounds for the number of α in a number field k with $H(1,\theta\alpha) \leq X$ for a fixed non-zero algebraic number θ and they state: *"It would be interesting to know if there are asymptotic formulae like Schanuel's for the cardinalities here, at least for fixed θ not in k."* We have the following result which implies an affirmative answer on Loher and Masser's question. Let n be a natural number and let θ be a non-zero algebraic number. Then as X tends to infinity the number of $(\alpha_0 : \alpha_1 : ... : \alpha_n)$ in $\mathbb{P}^n(k)$ with $H(\theta\alpha_0, \alpha_1, ..., \alpha_n) \leq X$ is asymptotically equal to

$$g(\theta,k,n)X^{m(n+1)}.$$

The constant $g(\theta,k,n)$ can be explicitly given but has a rather complex structure.

After all we briefly explain how Theorem 3.1 can be applied to obtain the asymptotics for special types of non-linear varieties. For example if a variety defined over a number field k is a disjoint union of lines (also defined over k) we can easily estimate the counting functions of these lines by Theorem 3.1 and then try to sum them to get asymptotic estimates for the given variety. This idea can be found in Heath-Brown's articles [**18**] and [**19**] but see especially McKinnon [**35**] for the approach with lines. McKinnon found the correct order of magnitude for many algebraic varieties (see [**35**] Theorem 1.3) but he did not provide the asymptotics. Some of them can be deduced from our Theorem 3.1. For example, let $r > 1$ be a fixed natural number. Then as X tends to infinity the number of points (x,y,z) on the hypersurface

in $\mathbb{A}^3(k)$ defined by

$$z = xy^r$$

with $H(1,x,y,z) \leq X$ is asymptotically equal to

$$S_k(1)\zeta_{k,H}(m(r+1))X^{2m}.$$

Here $m = [k:\mathbb{Q}]$ and $\zeta_{k,H}(s)$ denotes the height zeta function defined by $\sum_{\alpha \in k} H(1,\alpha)^{-s}$, which converges for $s > 2m$, thanks to Schanuel's Theorem. The asymptotics for this example are possibly already known but with Theorem 3.1 we can also make an attempt to count points of fixed degree. So suppose we have a variety which is a union of disjoint linear subvarieties (of positive dimension and defined over k). Then we can use Theorem 3.1 to estimate the number of primitive points on each linear subvariety. Summing these estimates over the linear subvarieties one can hope to get the asymptotics for primitive points on the given variety. Due to the particular good dependence of the error term in Theorem 3.1 with respect to the underlying field, one can now try to sum the asymptotic estimates for primitive points over all number fields of fixed degree. Indeed sometimes this summation converges and one gets asymptotics for the number of points of fixed degree and bounded height on a non-linear variety. To the best of the author's knowledge the following example is new. We consider the affine subvariety of $\mathbb{A}^{2n+1}(\overline{\mathbb{Q}})$ given by the n equations

$$\begin{aligned} x_{n+2} - x_1 x_{n+1}^r &= 0 \\ &\vdots \\ x_{2n+1} - x_n x_{n+1}^r &= 0 \end{aligned}$$

where $r > 1$ is a natural number. If we suppose that $n > 5e/2 + 5$ then we can use Theorem 3.1 to prove: as X tends to infinity there are asymptotically

$$\left(\sum_K S_K(n)\zeta_{K,H}(e(nr+1)) \right) X^{e(n+1)}$$

points $(x_1, ..., x_{2n+1})$ on the above variety with $[\mathbb{Q}(x_1, ..., x_{2n+1}) : \mathbb{Q}] = e$ and $H(1, x_1, ..., x_{2n+1}) \leq X$. Here the sum runs over all number fields K of degree e.

CHAPTER 1

Counting lattice points

In this chapter we will prove an easy but important theorem, which will be used in almost all of the following results. It estimates the number of lattice points in a bounded subset of $\mathbb{R}^n$. To get nontrivial estimates it is necessary to ask for some additional conditions on the set. Classically two different approaches are known; one is associated with the name Lipschitz and the other one goes back to Davenport [**10**]. The chapter is organized as follows. In the first section we introduce the conditions on the set. Section 2 is devoted to the orthogonality defect, which plays a crucial role in the study of lattices. Finally in the third section we state and prove the main result.

1. Preliminaries

For a vector $\mathbf{x}$ in $\mathbb{R}^n$ we write $|\mathbf{x}|$ for the euclidean length of $\mathbf{x}$.

DEFINITION 1.1. *Let S be a subset of $\mathbb{R}^n$ and let $0 \leq k \leq n$. We say S is in Lip(n,k,M,L) if there are M maps $\phi : [0,1]^{n-k} \longrightarrow \mathbb{R}^n$ satisfying a Lipschitz condition*

$$|\phi(\mathbf{x}) - \phi(\mathbf{y})| \leq L|\mathbf{x} - \mathbf{y}| \tag{1.1.1}$$

such that S is covered by the images of the ϕ's. For $k = n$ this is to be interpreted simply as the finiteness of the set S.

We call L a Lipschitz constant for ϕ. If $k = n$ then M is interpreted as an upper bound for the cardinality of S and any non-negative L is allowed. By definition the empty set lies in Lip(n,k,M,L) for any positive integer n, any k in $\{0,1,2,...,n\}$ any M in $\{0,1,2,3,...\}$ and any non-negative L. However in our applications k will be 1 or 2.

The closed euclidean ball centered at $\mathbf{z}$ with radius r will be denoted by $B_{\mathbf{z}}(r)$. Let Λ be a lattice of rank n in $\mathbb{R}^n$ then we define the *successive minima* $\lambda_1(\Lambda), ..., \lambda_n(\Lambda)$ of Λ as the successive minima in the sense of Minkowski with respect to the unit ball. That is

$$\lambda_i = \inf\{\lambda;\ \lambda B_0(1) \cap \Lambda \text{ contains } i \text{ linear independent vectors}\}.$$

By definition we have

$$0 < \lambda_1 \leq \lambda_2 \leq ... \leq \lambda_n < \infty. \tag{1.1.2}$$

REMARK 1. *Minkowski's successive minima can be defined with respect to any convex, symmetric, bounded subset of* $\mathbb{R}^n$*, which contains the origin in its interior.*

Next we prove a simple but useful lemma. Let Λ be a lattice in $\mathbb{R}^n$ with successive minima $\lambda_1, ..., \lambda_n$.

LEMMA 1.1. *Suppose* V *is a subspace of* $\mathbb{R}^n$ *of dimension* $i-1 \geq 1$ *and contains* $i-1$ *linearly independent elements* $v_1, ..., v_{i-1}$ *of* Λ *with* $|v_k| = \lambda_k$ *for* $1 \leq k \leq i-1$*. Then any* v *in* Λ *not in* V *satisfies*

$$|v| \geq \lambda_i.$$

Proof. Suppose v is in Λ but not in V. Then $v_1, ..., v_{i-1}, v$ are linearly independent. Hence one of these vectors has length at least λ_i. If $\lambda_{i-1} < \lambda_i$ the claim follows at once since $|v_1| \leq ... \leq |v_{i-1}| = \lambda_{i-1}$. Now let j in $\{1, ..., i\}$ be minimal with $\lambda_j = \lambda_i$. If $j = 1$ then the result is clear from the definition of λ_1. If $j > 1$ then $v_1, ..., v_{j-1}, v$ are linearly independent and again we conclude one of these vectors has length at least $\lambda_j = \lambda_i$. But $v_1, ..., v_{j-1}$ have length at most $\lambda_{j-1} < \lambda_i$, so $|v| \geq \lambda_i$ as claimed. □

LEMMA 1.2. *Suppose* $n = dm$ *and* $\Lambda = \Lambda_0^m$ *for a lattice* Λ_0 *in* $\mathbb{R}^d$*. Then the successive minima of* Λ *are given by*

$$\lambda_1(\Lambda_0), ..., \lambda_1(\Lambda_0), \lambda_2(\Lambda_0), ..., \lambda_2(\Lambda_0), ..., \lambda_d(\Lambda_0), ..., \lambda_d(\Lambda_0)$$

where each minimum is repeated m *times.*

Proof. A typical minimum $\lambda_i(\Lambda_0)$ occurs above in the positions $(i-1)m+1, ..., im$. Thus it suffices to verify

$$\lambda_{im}({\Lambda_0}^m) \leq \lambda_i(\Lambda_0) \leq \lambda_{(i-1)m+1}({\Lambda_0}^m) \tag{1.1.3}$$

for $1 \leq i \leq d$. For the first inequality we note that there is a subspace V_i in $\mathbb{R}^d$ of dimension i containing i linearly independent elements $v_1, ..., v_i$ of Λ_0 with length $\lambda_1(\Lambda_0), ..., \lambda_i(\Lambda_0)$. Now V_i^m in $\mathbb{R}^{dm}$ of dimension im contains im linearly independent elements of Λ_0^m like $(v_1, 0, ..., 0)$ also with length at most $\lambda_i(\Lambda_0)$. The first inequality in (1.1.3) follows at once.

For the second inequality note that any $(i-1)m+1$ independent points w of Λ_0^m cannot all lie in V_{i-1}^m. So some w has the form $w = (w_1, ..., w_m)$ with some w_j not in V_{i-1}. By the previous lemma we see that $|w| \geq |w_j| \geq \lambda_i(\Lambda_0)$ and the second inequality is proved. □

2. Orthogonality defect

Given a lattice, we would like to choose a good basis of this lattice. Intuitively one might say an orthogonal basis is good. Usually we will not find an orthogonal basis but we may look for a basis as orthogonal as possible. To quantify the deficiency from being orthogonal we define the *orthogonality defect* Ω *of a set of linearly independent vectors* $v_1, ..., v_n$ in $\mathbb{R}^n$ as

$$\Omega(v_1, ..., v_n) = \frac{|v_1|...|v_n|}{\det \Lambda}$$

where Λ is the lattice generated by $v_1, ..., v_n$. The Theorem of Hadamard tells us that this quantity is bounded below by 1 and is 1 if and only if the system of vectors is orthogonal. From a geometrical point of view this is obvious since the product of the length of the edges can not exceed the volume of a parallelepiped. But how small can it get for a fixed Λ? For this we define the *orthogonality defect of the lattice* Λ as

$$\Omega(\Lambda) = \inf_{(v_1,...,v_n)} \frac{|v_1|...|v_n|}{\det \Lambda}$$

where the infimum runs over all bases $(v_1, ..., v_n)$ of Λ. Since Λ is discrete the infimum will be attained. Due to its importance it is worth to state Minkowski's Theorem before we go on. Since we need only a special case we do not give the full theorem (see [**7**] p.218 Theorem V).

THEOREM 1.1 (Minkowski's Second Theorem for balls). *Let* Λ *be a lattice in* $\mathbb{R}^n$ *with successive minima* $\lambda_1, ..., \lambda_n$. *Then*

$$\frac{2^n}{n!} \det \Lambda \leq \lambda_1 ... \lambda_n \text{Vol } B_0(1) \leq 2^n \det \Lambda$$

where Vol $B_0(1) = \frac{\pi^{n/2}}{\Gamma(n/2+1)}$.

Proof. See [**7**] p.205. □

By Minkowski's Second Theorem we obtain n linearly independent vectors $u_1, ..., u_n$ in Λ, such that $|u_1|...|u_n|/\det \Lambda = \lambda_1 ... \lambda_n / \det \Lambda$ is bounded below and above in terms of n only. Unfortunately these vectors usually fail to build a basis of the lattice but they can be used to construct a reduced basis (see Lemma 1.3 below). However there are several basis reduction algorithms: Minkowski, Mahler-Weyl, Korkine-Zolotarev, LLL just to name a few. A common property is, that the orthogonality defect of these reduced bases is bounded above in terms of the rank only (see Lemma 1.3 below). Therefore we can define

$$\Omega(n) = \sup_{\Lambda} \Omega(\Lambda)$$

where the supremum runs over all lattices of rank n.

QUESTION 1. *Is there an algorithm to compute $\Omega(n)$?*

Being more pragmatic one may ask for upper bounds on $\Omega(n)$. This suffices for most applications. We use the Mahler-Weyl basis reduction to prove the following bound:

LEMMA 1.3. *Let $n > 1$ be a natural number then*

$$\Omega(n) \leq \frac{n^{\frac{3}{2}n}}{(2\pi)^{\frac{n}{2}}}.$$

Proof. Let Λ be a lattice of rank n. By Theorem 1.1

$$\lambda_1 ... \lambda_n \text{Vol } B_0(1) \leq 2^n \det \Lambda.$$

It is known from the definition of the λ_i that there are linearly independent vectors $u_1, ..., u_n$, such that $|u_i| = \lambda_i$ for $1 \leq i \leq n$. Using a lemma of Mahler and Weyl ([**7**] p.135 Lemma 8) we obtain a basis $v_1, ..., v_n$ of Λ satisfying

$$|v_i| \leq \max\{|u_i|, \frac{1}{2}(|u_1| + ... + |u_i|)\} \leq \max\{1, \frac{i}{2}\}\lambda_i$$

for $1 \leq i \leq n$. Since $\Gamma(m+1) = m!$ and $\Gamma(m+1/2) = (m-1/2)(m-3/2)(m-5/2)...(1/2)\sqrt{\pi}$ for positive integers m, we see that $\Gamma(\frac{n}{2}+1) \leq (\frac{n}{2})^{\frac{n}{2}}$ provided $n \geq 2$. Using also $n! \leq n^{n-1}$ this yields

$$\Omega(\Lambda) \leq \frac{|v_1|...|v_n|}{\det \Lambda} \leq \frac{nn!\Gamma(\frac{n}{2}+1)}{\pi^{\frac{n}{2}}} \leq \frac{n^{\frac{3}{2}n}}{(2\pi)^{\frac{n}{2}}}$$

and proves the statement. □

Using the Korkine-Zolotarev algorithm instead of "Mahler and Weyl" gives probably a better upper bound for $\Omega(n)$. On the other hand for powers of lattices Λ_0^m we have $\Omega(\Lambda_0^m) = (\Omega(\Lambda_0))^m$. The hexagonal lattice generated by $(1,0), (1/2, \sqrt{3}/2)$ has orthogonality defect $2/\sqrt{3} > 1$. So by restricting to powers of lattices we see that the growth of $\Omega(n)$ is at least exponential. This lower bound gives rise to the following question.

QUESTION 2. *Is the function*

$$\frac{\log \Omega(n)}{n} \tag{1.2.1}$$

bounded above?

3. Counting

What is the idea behind the approach using Lipschitz parameterization? A set F is called a *fundamental domain* of Λ if there is a basis $v_1, ..., v_n$ of Λ such that

$$F = [0,1)v_1 + ... + [0,1)v_n.$$

Let Λ be a lattice in $\mathbb{R}^n$ and $v_1, ..., v_n$ a basis of Λ with corresponding fundamental domain F. For a set S in $\mathbb{R}^n$ write $\mathfrak{T} = \mathfrak{T}_S(F)$ for the number of translates by lattice points having non-empty intersection with the boundary ∂S. The following inequality is well-known but crucial. Therefore we state it as a lemma.

LEMMA 1.4. *Suppose S is measurable and bounded. Then*

$$||\Lambda \cap S| - \frac{\text{Vol } S}{\det \Lambda}| \leq \mathfrak{T}. \tag{1.3.1}$$

Proof. Clearly the translates $F_v = F + v$ ($v \in \Lambda$) define a partition of $\mathbb{R}^n$. Moreover every F_v contains exactly one lattice point - namely v. Denote by $\mathfrak{m} = \mathfrak{m}_S(F)$ the number of translates of F by lattice points, which have empty intersection with the complement of S. In particular we have $\mathfrak{m} \leq |\Lambda \cap S|$. Now suppose v lies in S. So either F_v lies in S or F_v contains a point of S and a point of its complement. But F_v is convex and therefore connected. So if F_v contains a point of S and a point of its complement then it contains a point of the boundary ∂S. Hence $|\Lambda \cap S| \leq \mathfrak{m} + \mathfrak{T}$.

Now $\det \Lambda$ is the volume of F_v. So the union of all translates F_v lying in S has volume $\mathfrak{m} \det \Lambda$. And the union of all translates having non-empty intersection with S has volume at most $(\mathfrak{m}+\mathfrak{T}) \det \Lambda$. Thus we have proven the following inequalities:

$$\mathfrak{m} \leq |\Lambda \cap S| \leq \mathfrak{m} + \mathfrak{T},$$
$$\mathfrak{m} \det \Lambda \leq \text{Vol } S \leq (\mathfrak{m} + \mathfrak{T}) \det \Lambda.$$

Hence

$$||\Lambda \cap S| - \frac{\text{Vol } S}{\det \Lambda}| \leq \mathfrak{T}.$$

□

The inequality above explains why the following proposition is crucial for the subsequent counting results of this chapter.

PROPOSITION 1.1 (Masser). *Assume $n > 1$, let $\Lambda \subseteq \mathbb{R}^n$ be a lattice and let $\lambda_1, ..., \lambda_n$ be the successive minima of Λ with respect to the unit ball. Assume S is a bounded subset of $\mathbb{R}^n$ with boundary ∂S in Lip$(n, 1, M, L)$. Let $v_1, ..., v_n$ be a basis of Λ with fundamental domain*

F and $\mathfrak{T}_S(F)$ the number of translates $F_v = F + v$ ($v \in \Lambda$), which have non-empty intersection with ∂S. Then for any natural number Q we have

$$\mathfrak{T}_S(F) \leq MQ^{n-1} \prod_{i=1}^{n} (\frac{\sqrt{n-1}\Omega(v_1, ..., v_n)L}{\lambda_i Q} + 2).$$

Proof. We certainly may assume that ∂S is not empty. Choose one of the parameterizing maps ϕ and split $I = [0, 1]$ in Q intervals of length $1/Q$. Then $\phi(I^{n-1})$ splits in Q^{n-1} subsets $\phi(C)$ where C is a hypercube in $\mathbb{R}^{n-1}$ of side $1/Q$. Due to the Lipschitz condition the distance between any two points in $\phi(C)$ does not exceed $\frac{\sqrt{n-1}L}{Q}$. Now F is the fundamental domain corresponding to the given basis so $F = [0, 1)v_1 + ... + [0, 1)v_n$. We have to count the v in Λ such that F_v meets ∂S. Thus F_v meets one of the $\phi(C)$ say in a point $\mathbf{x}$. Writing $v = r_1v_1 + ... + r_nv_n$ for $r_1, ..., r_n$ in $\mathbb{Z}$, we see that there are $\vartheta_1, ..., \vartheta_n$ in $[0, 1)$ such that

$$\mathbf{x} = (r_1 + \vartheta_1)v_1 + ... + (r_n + \vartheta_n)v_n.$$

We now show that there are not too many other v' in Λ such that $F_{v'}$ meets this same $\phi(C)$. Let $\mathbf{x}'$ be in $\phi(C) \cap F_{v'}$ then we get corresponding r_i', ϑ_i'. To estimate the length of $\mathbf{x} - \mathbf{x}'$ write $\varrho_i = r_i + \vartheta_i - (r_i' + \vartheta_i')$ for the coefficient of the basis element v_i. Hence

$$|\varrho_1v_1 + ... + \varrho_nv_n| = |\mathbf{x} - \mathbf{x}'| \leq \frac{\sqrt{n-1}L}{Q}. \tag{1.3.2}$$

After permuting the indices we may assume that $|v_i| \leq |v_{i+1}|$ and therefore $|v_i| \geq \lambda_i$. Now by Cramer's rule and the definition of $\Omega(v_1, ..., v_n) = \Omega$ we get

$$|\varrho_i| = |\frac{\det[v_1...\mathbf{x} - \mathbf{x}'...v_n]}{\det[v_1...v_i...v_n]}| = \frac{|\det[v_1...\mathbf{x} - \mathbf{x}'...v_n]|}{|v_1|...|v_i|...|v_n|}\Omega.$$

Now we apply Hadamard's inequality to find the upper bound

$$\frac{|v_1|...|\mathbf{x} - \mathbf{x}'|...|v_n|}{|v_1|...|v_n|}\Omega$$
$$= \frac{|\mathbf{x} - \mathbf{x}'|}{|v_i|}\Omega.$$

Due to (1.3.2) the latter is

$$\leq \frac{\sqrt{n-1}\Omega L}{\lambda_i Q}.$$

Notice that $|\vartheta_i - \vartheta_i'| < 1$ therefore all the r_i lie in an interval of length

$$\frac{\sqrt{n-1}\Omega L}{\lambda_i Q} + 1.$$

So the number of $(r_1, ..., r_n)$ is at most

$$\prod_{i=1}^{n}([\frac{\sqrt{n-1}\Omega L}{\lambda_i Q}] + 2),$$

provided there are at least two of them. However it is trivially true if there is just one of them. On recalling that we have M parameterizing maps and Q^{n-1} subsets $\phi(C)$ for each map we get the desired upper bound for the number of translates having non-empty intersection with the boundary of S. □

The Proposition 1.1 leads to an explicit version of Lemma 2 [**34**].

COROLLARY 1.1. *Let S be a bounded set in $\mathbb{R}^n$ such that the boundary ∂S of S is in Lip$(n, 1, M, L)$. Let Λ be a lattice in $\mathbb{R}^n$. Then S is measurable and moreover*

$$||S \cap \Lambda| - \frac{\text{Vol } S}{\det \Lambda}| \leq 3^n M(\frac{\sqrt{n}\Omega(\Lambda)L}{\lambda_1} + 1)^{n-1}. \tag{1.3.3}$$

Proof. For $n = 1$ the set S is a union of at most M intervals (or single points) in which case the statement is trivial. So we may assume $n > 1$. For the measurability we refer to [**25**] p.294 Satz 7. To prove the second statement we choose a basis with minimal orthogonality defect. Thanks to (1.3.1) it suffices to estimate $\mathfrak{T}$ corresponding to this basis. Using Proposition 1.1 we see that $\mathfrak{T}$ is bounded above by $MQ^{n-1}(\frac{\sqrt{n-1}\Omega(\Lambda)L}{\lambda_1 Q} + 2)^n$. Now let us choose $Q = [\frac{\sqrt{n}\Omega(\Lambda)L}{\lambda_1}] + 1$. This leads straightforwardly to

$$\mathfrak{T} \leq 3^n M(\frac{\sqrt{n}\Omega(\Lambda)L}{\lambda_1} + 1)^{n-1}$$

and the theorem is proved. □

Sometimes another choice of Q is more reasonable. However the reader interested only in the theorems needed for the following chapters may skip the next remark.

REMARK 2. *Assume $n > 1$. If we estimate every λ_i by λ_1 then we obtain*

$$\begin{aligned}\mathfrak{T} &\leq MQ^{n-1}(\frac{\sqrt{n-1}\Omega(\Lambda)L}{\lambda_1 Q}+2)^n \\ &= M(\frac{\sqrt{n-1}\Omega(\Lambda)L}{\lambda_1 Q}+2)(\frac{\sqrt{n-1}\Omega(\Lambda)L}{\lambda_1}+2Q)^{n-1}.\end{aligned}$$

Now we choose $Q = [\frac{\Omega(\Lambda)L}{2\sqrt{n-1}\lambda_1}]+1$ and deduce

$$\begin{aligned}\mathfrak{T} &\leq 2nM(\frac{n\Omega(\Lambda)L}{\sqrt{n-1}\lambda_1}+2)^{n-1} \\ &\leq 2n^nM(\frac{\Omega(\Lambda)L}{\sqrt{n-1}\lambda_1}+1)^{n-1}.\end{aligned}$$

So

$$||S\cap\Lambda| - \frac{\text{Vol } S}{\det\Lambda}| \leq 2n^nM(\frac{\Omega(\Lambda)L}{\sqrt{n-1}\lambda_1}+1)^{n-1}. \tag{1.3.4}$$

This bound is sharper if for example $\frac{\Omega(\Lambda)L}{\lambda_1} \geq 2\sqrt{n}$.

In some cases it is necessary to take into account not only the first but also the other minima. Therefore the following more precise result is often very useful and indeed it can be considered as the main result of this chapter.

THEOREM 1.2. *Let Λ be a lattice in $\mathbb{R}^n$ with successive minima (with respect to the unit ball) $\lambda_1, ..., \lambda_n$. Let S be a bounded set in $\mathbb{R}^n$ such that the boundary ∂S of S is in Lip$(n, 1, M, L)$. Then S is measurable and moreover*

$$||S\cap\Lambda| - \frac{\text{Vol } S}{\det\Lambda}| \leq c_0(n)M\max_{0\leq i<n}\frac{L^i}{\lambda_1...\lambda_i}.$$

For $i = 0$ the expression in the maximum is to be understood as 1. Furthermore one can choose $c_0(n) = n^{3n^2/2}$.

Proof. For the measurability see Corollary 1.1. Since the case $n = 1$ is straightforward we assume $n > 1$. As in the proof of Corollary 1.1 it suffices to estimate $\mathfrak{T}$ corresponding to a basis with minimal orthogonality defect. To simplify notation we write κ for $\sqrt{n-1}\Omega(\Lambda)$. It is convenient to distinguish two cases:

(1) $L < \lambda_n$:
We use Proposition 1.1 with $Q = 1$. We estimate the n-th term of the

product by $\kappa+2$. So

$$\mathfrak{T} \le M(\kappa+2)\prod_{i=1}^{n-1}(\frac{\kappa L}{\lambda_i}+2) \le M(\kappa+2)\prod_{i=1}^{n-1}(\kappa+2)(\frac{L}{\lambda_i}+1)$$
$$= M(\kappa+2)^n\prod_{i=1}^{n-1}(\frac{L}{\lambda_i}+1).$$

Now we expand the remaining product and estimate each of the 2^{n-1} terms in the resulting sum by $\max_{0\le i<n}\frac{L^i}{\lambda_1\ldots\lambda_i}$. Hence

$$\mathfrak{T} \le M(\kappa+2)^n 2^{n-1}\max_{0\le i<n}\frac{L^i}{\lambda_1\ldots\lambda_i}. \tag{1.3.5}$$

Next we use Lemma 1.3 and recall that $n>1$ to estimate

$$\kappa+2 \le \frac{\sqrt{n-1}n^{3n/2}}{(2\pi)^{n/2}}+2 \le \frac{1}{2\pi}n^{3n/2}+\frac{1}{4}n^{3n/2} < \frac{1}{2}n^{3n/2}.$$

Hence

$$\mathfrak{T} \le Mn^{3n^2/2}\max_{0\le i<n}\frac{L^i}{\lambda_1\ldots\lambda_i},$$

which proves the theorem in the first case.

(2) $L \ge \lambda_n$:
Note that in particular $L>0$. Here we choose $Q=[\frac{L}{\lambda_n}]+1$ and we get

$$\mathfrak{T} \le \frac{M}{Q}\prod_{i=1}^{n}(\frac{\kappa L}{\lambda_i}+2Q) \le \frac{M\lambda_n}{L}\prod_{i=1}^{n}(\frac{(\kappa+2)L}{\lambda_i}+2)$$
$$\le M(\kappa+4)^n\frac{L^{n-1}}{\lambda_1\ldots\lambda_{n-1}}$$
$$\le M2^n(\kappa+2)^n\frac{L^{n-1}}{\lambda_1\ldots\lambda_{n-1}}$$

where this last $\frac{L^{n-1}}{\lambda_1\ldots\lambda_{n-1}}$ is now the maximum term in (1.3.5). We have already seen that (for $n>1$) $\kappa+2 \le 2^{-1}n^{3n/2}$ and so the result drops out. □

The following remark is not used in the sequel but it might be of some independent interest.

REMARK 3. *For $L \ge \lambda_{n-1}$ one can deduce by Theorem 1.1*

$$||S\cap\Lambda| - \frac{\text{Vol } S}{\det\Lambda}| \le c_0'(n)M\frac{L^{n-1}\lambda_n}{\det\Lambda},$$

where one can choose $c_0'(n) = (\frac{\sqrt{\pi}}{2})^n \frac{\Gamma(n+1)}{\Gamma(n/2+1)} c_0(n)$.

Theorem 1.2 can be considered as a version of Schmidt's Theorem 1.3 (see below) with different and probably weaker conditions on the set. Since we would like to compare these two theorems the exact statement of Schmidt's theorem is needed. This requires another definition originally coming from p.347 in [**49**] (using compact instead of bounded and measurable) and later defined in the following way in [**17**] p.14.

DEFINITION 1.2. *A subset* S *of* $\mathbb{R}^n$ *is called of narrow class* s *if*
(a) S *is bounded, measurable and intersects every line in at most* s *intervals or single points.*
(b) The same is true for any projection of S *on any linear subspace of* $\mathbb{R}^n$.

THEOREM 1.3 (Schmidt). *Let* S *be a set in* $\mathbb{R}^n$ *of narrow class* s *and assume* $S \subseteq B_0(R)$. *Let* Λ *be a lattice in* $\mathbb{R}^n$. *Then we have*

$$||S \cap \Lambda| - \frac{\text{Vol } S}{\det \Lambda}| \leq c_1(n,s) \max_{0 \leq i < n} \frac{R^i}{\lambda_1 ... \lambda_i} \tag{1.3.6}$$

where one can choose $c_1(n,s) = (s + \frac{2}{\sqrt{3}} 3^n n)^n$.

Proof. See [**17**] p.15. □

We will attempt a more detailed comparison in Appendix A.

CHAPTER 2

Some uniform upper bounds

This chapter is dedicated to some uniform upper bounds due to Schmidt and Loher and Masser for the number of algebraic points of bounded height in projective space either restricted to a fixed number field or of bounded degree. The bounds will depend only on the dimension of the projective space and the bounds for the degree and the height. Our own contribution in this chapter is modest and consists of Theorem 2.4, which is a small improvement in a special case of Schmidt's upper bound. For our application coming in Chapter 4 only the original bounds due to Schmidt, Loher and Masser are used. However a good reason to include Theorem 2.4 is that the proof involves Lipschitz systems. Lipschitz systems are the origin of the more general Arakelov-Lipschitz systems following in Chapter 3. Therefore the proof of Theorem 2.4 can be considered as a first and simple example dealing with Arakelov-Lipschitz systems.

1. Introduction and results

It was Evertse who first gave uniform upper bounds for the number of elements α in a fixed number field K with absolute Weil height $H(1,\alpha)$ not exceeding a parameter X. His bound $c(d)X^{3d}$ (d is the degree of K) is uniform in two different senses. First it depends only on the degree of K but not on the field structure of K itself. Moreover it holds not only for the height but also for "shifted heights" more precisely his bound holds for the number of α's in K with $H(1,\theta\alpha) \leq X$ where θ is an arbitrary but fixed non-zero algebraic number. The need for such a result came up in the final step in the proof of his famous result on the unit-equation [**15**] Theorem 1, to bound the solutions with small height. In [**47**] Lemma 8B p.29 Schmidt refined his arguments to get the correct exponent $2d$. Behind both of these theorems there is a simple principle. We sketch the proof in the simplest case where $\theta = 1$ and K has a real embedding σ but the attentive reader will easily adapt the proof for arbitrary non-zero θ. For each place v we denote by K_v the completion of K at v. Let $X \geq 1$ be a real and suppose $\alpha_1, ..., \alpha_N$ are pairwise distinct numbers in K with absolute Weil height not exceeding

X. Due to $H(1,\alpha)^d \geq |\sigma(\alpha)|$ the real numbers $\sigma(\alpha_1),...,\sigma(\alpha_N)$ lie in an interval of length $2X^d$ and so we get by the Box Principle (after changing indices)

$$|\sigma(\alpha_1) - \sigma(\alpha_2)| \leq 2X^d/N.$$

Now we may suppose w corresponds to the real embedding σ. We apply the product formula to find

$$\begin{aligned} 1 = \prod_v |\alpha_1 - \alpha_2|_v^{d_v} &= |\alpha_1 - \alpha_2|_w^{d_w} \prod_{v \neq w} |\alpha_1 - \alpha_2|_v^{d_v} \\ &\leq |\alpha_1 - \alpha_2|_w^{d_w} \prod_v \max\{1, |\alpha_1 - \alpha_2|_v\}^{d_v} \\ &= |\sigma(\alpha_1) - \sigma(\alpha_2)| H(1, \alpha_1 - \alpha_2)^d \end{aligned}$$

Now $H(1,\alpha+\beta) \leq 2H(1,\alpha)H(1,\beta)$ holds for any α, β in K. Hence we have the following estimate

$$1 \leq |\sigma(\alpha_1) - \sigma(\alpha_2)| 2^d X^{2d} \leq 2^{d+1} \frac{X^{3d}}{N}$$

so $N \leq 2^{d+1} X^{3d}$.

Here the constant $c(d) = 2^{d+1}$ is exponential in d and this was the case in Evertse's as well as Schmidt's result. However for $X = 1$ we are counting roots of unity in K and it is clear that the number N of these satisfies $\phi(N) \leq d$ for Euler's totient function ϕ, leading to an upper bound for N that is polynomial in d. Therefore the above estimates seem to be inadequate for small height. Already in 1989 Masser stated (without proof) that there is a positive effective absolute constant C such that for $X \leq \exp\{1/Cd\}$ one has not more than $Cd \log d$ numbers in K with height not exceeding X. A more refined version of the idea above is needed to eliminate the exponential dependence on d. Recently Masser and Loher ([**29**] Theorem 1) proved

THEOREM 2.1 (Loher, Masser). *Let $\theta \neq 0$ be in $\overline{\mathbb{Q}}$, let K be a number field of degree d, and let $X \geq 0$ be real. If $d \geq 2$ there are at most $68(d \log d)X^{2d}$ elements α in K with $H(1,\theta\alpha) \leq X$; further if θ is in K this can be improved to $31(d \log d)X^{2d}$. If $d = 1$ the expression $68(d \log d)$ can be replaced by 17.*

Loher and Masser ([**29**] Theorem 4) gave also new bounds for vectors. Write $Z_H(K^n, X)$ for the number of elements $(\alpha_1,...,\alpha_n)$ in K^n with $H(1,\alpha_1,...,\alpha_n) \leq X$.

THEOREM 2.2 (Loher, Masser). *Let K be a number field of degree $d \geq 2$, let $n \geq 1$ and let $X \geq 0$ be real. Then one has $Z_H(K^n, X) \leq (1088 d \log d)^n X^{(n+1)d}$.*

Up to now we fixed the number field. Now we focus on the case of fixed degree only. Let k be a number field and fix an algebraic closure $\overline{k}$ of k. Let $P = (\alpha_0 : ... : \alpha_n)$ be a point in $\mathbb{P}^n(\overline{k})$. By adjoining all the ratios α_i/α_j $(0 \leq i, j \leq n,\ \alpha_j \neq 0)$ to k, we get an extension $k(P) = k(..., \alpha_i/\alpha_j, ...)$. For natural numbers e, n we define the subset $\mathbb{P}^n(k; e)$ of $\mathbb{P}^n(\overline{k})$ as the set of points P with $[k(P) : k] = e$. The corresponding counting function $Z_H(\mathbb{P}^n(k; e), X)$ denotes the number of points in $\mathbb{P}^n(k; e)$ with $H(P) \leq X$. As far as we know Schmidt [**48**] was the first giving upper and lower bounds for the number of projective points of bounded height and fixed degree over an arbitrary but fixed number field k.

THEOREM 2.3 (Schmidt). *Let k be a number field of degree m. Then*

(2.1.1) $Z_H(\mathbb{P}^n(k; e), X) \leq c_2(k, e, n)X^{me(n+e)}$,

(2.1.2) $Z_H(\mathbb{P}^n(k; e), X) \geq c_3(k, e, n)X^{me(n+1)}$ *when* $X \geq X_3(k, e, n)$,

(2.1.3) $Z_H(\mathbb{P}^n(k; e), X) \geq c_4(k, e, n)X^{me(e+1)}$ *when* $X \geq X_4(k, e)$.

The constants c_2, c_3, c_4 are positive. In particular, we may take

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

Following the strategy of Masser and Vaaler in [**34**] Theorem 2.2 provides a slight improvement on the dependence on m in Schmidt's upper bound for $n = 1$.

THEOREM 2.4. *Let k be a number field of degree m over $\mathbb{Q}$ and $X \geq 0$ a real. Then*

$$Z_H(\mathbb{P}^1(k; e), X) \leq \begin{cases} 2e(1088m \log m)^e 2^{me(e+1)} X^{me(e+1)} & \text{if } m > 1 \\ e3^{e+1} \cdot 2^{e(e+1)} X^{e(e+1)} & \text{if } m = 1 \end{cases}.$$

As above, the case $X = 1$ counts roots of unity of degree e over k. It was noted in [**32**] that the number of roots of unity of degree at most d is asymptotically $\frac{315\zeta(3)}{4\pi^4}d^2$ as d tends to infinity. So certainly $Z_H(\mathbb{P}^1(k; e), 1)$ is of order at most $d^2 = e^2m^2$. Taking $m = 1$ shows that the exponent 2 of e here is best possible; however the exponent 2 of m can be lowered to $1 + \epsilon$ for any $\epsilon > 0$. Taking $e = 1$ shows that no further improvement is possible. So for $X = 1$ the exponential dependence on m and e can be removed. For $X > 1$ we get a hint if we look at the asymptotics. According to Theorem [**34**] they are $eV_{\mathbb{R}}(e)^{r_k}V_{\mathbb{C}}(e)^{s_k}S_k(e)X^{me(e+1)}$ for certain constants $V_{\mathbb{R}}(e), V_{\mathbb{C}}(e)$ depending only on e and non-negative integers r_k, s_k with $r_k + 2s_k = m$. By Corollary 4.1 of [**29**] one has $S_k(e) \leq (1088m \log m)^e$ (provided

$m > 1$) and it turns out that $V_{\mathbb{R}}(e), V_{\mathbb{C}}(e) \leq 1$. In fact these numbers tend to zero if e gets large. So one might hope to remove the exponential dependence on m in the factor $2^{me(e+1)}$ of Theorem 2.4 entirely.

2. Lipschitz heights

Here we recall the definition of Lipschitz systems and their corresponding heights introduced by Masser and Vaaler [**34**] in order to prove counting results for the numbers of fixed degree and bounded height. We briefly describe their strategy; this will also motivate the more general definitions of Lipschitz systems that we will provide in Chapter 3.

An algebraic number α is of degree e over the rationals if and only if it is a zero of a non-zero polynomial f of degree e irreducible over the rationals with integer coefficients. If we fix an α of degree e all these corresponding polynomials are proportional and the zeros are pairwise distinct. Now $H(1,\alpha)^e$ is simply the Mahler-measure of f divided by the greatest common factor of the coefficients. But what is this Mahler-measure $\mathcal{M}$? Let f be any polynomial in $\mathbb{C}[x]$. If f is constant then $\mathcal{M}(f) = |f|$. If f is not constant we may factor f over $\mathbb{C}$ so $f = z_0(x-\alpha_1)(x-\alpha_2)...(x-\alpha_e)$. And now

$$\mathcal{M}(f) = |z_0| \prod_{i=1}^{e} \max\{1, |\alpha_i|\}.$$

We define a modified height on $\mathbb{Q}^{e+1}$

$$H_{\mathcal{N}}(\mathbf{z}) = \mathcal{M}(z_0 x^e + ... + z_e) \prod_{v \nmid \infty} \max\{|z_0|_v, ..., |z_e|_v\}^{d_v}.$$

Here v runs over all finite places in $M_{\mathbb{Q}}$. Due to the product formula this defines a height on $\mathbb{P}^e(\mathbb{Q})$. Clearly

$$H_{\mathcal{N}}(\mathbf{z}) = \mathcal{M}(z_0 x^e + ... + z_e) \gcd\{z_0, ..., z_e\}^{-1}$$

for integer coordinates $z_0, ..., z_e$. So the number of α's of degree e over $\mathbb{Q}$ and $H(1,\alpha) \leq X$ is nothing but e times the number of projective points $P = (z_0 : ... : z_e)$ in $\mathbb{P}^e(\mathbb{Q})$ where $z_0 \neq 0$, $f = (z_0 x^e + ... + z_e)/z_0$ is irreducible over the rationals and $H_{\mathcal{N}}(P) \leq X^e$. So one just has to count projective points in $\mathbb{P}^e(\mathbb{Q})$ corresponding to irreducible polynomials with first coordinate non-zero and with modified height not larger than X^e. The points coming from reducible polynomials or with first

coordinate zero cause no trouble since their number is of smaller magnitude and so one just has to adapt Schanuel's proof for the new height.

We now define the more general settings following almost literally section 2 in [**34**]. Let n be a natural number and let N be a continuous function from $\mathbb{R}^{n+1}$ or $\mathbb{C}^{n+1}$ to $[0,\infty)$ with

(*i*) $N(\mathbf{z}) = 0$ if and only if $\mathbf{z} = \mathbf{0}$,

(*ii*) $N(\omega\mathbf{z}) = |\omega|N(\mathbf{z})$ for all ω in $\mathbb{R}$ or $\mathbb{C}$,

(*iii*) the set $\{\mathbf{z}; N(\mathbf{z}) = 1\}$ in $\mathbb{R}^{n+1}$ or $\mathbb{C}^{n+1} = \mathbb{R}^{2n+2}$ is in $\mathrm{Lip}(n+1, 1, M, L)$ or in $\mathrm{Lip}(2n+2, 1, M, L)$ for some M and L.

As in [**34**] we call N a *Lipschitz distance function* (of dimension n). A standard example is given by

$$N(\mathbf{z}) = \max\{|z_0|, |z_1|, ..., |z_n|\}. \tag{2.2.1}$$

The set defined in (*iii*) is the boundary of the set $\mathbf{B} = \{\mathbf{z}; N(\mathbf{z}) < 1\}$ and therefore $\mathbf{B}$ is a bounded symmetric open star-body in $\mathbb{R}^{n+1}$ or $\mathbb{C}^{n+1}$ respectively (see [**34**] p.6). This implies $\mathbf{B}$ has a finite volume V_N (see [**7**], Chapter IV, Section 2). Since $\mathbf{B}$ is bounded open and contains the origin we see by (*ii*) that all N are equivalent in the following sense: For each N there are positive constants c_N, C'_N such that

$$c_N \max\{|z_0|, |z_1|, ..., |z_n|\} \leq N(\mathbf{z}) \leq C'_N \max\{|z_0|, |z_1|..., |z_n|\}. \tag{2.2.2}$$

for all $\mathbf{z}$ in $\mathbb{R}^{n+1}$ or $\mathbb{C}^{n+1}$ (see also Subsection 1.2 Chapter 3). Next let r, s be non-negative integers not both zero and let $\mathcal{N}$ be a system of $r+s$ Lipschitz-distance functions, one for each of the factors in the product $\mathbb{R}^r \times \mathbb{C}^s$. Masser and Vaaler call such a system an (r,s)-*Lipschitz system (of dimension n)*. The volume $V_{\mathcal{N}}$ is defined as the product of the $r+s$ volumes V_N. Now we can consider number fields.

Let K be a number field with r real embeddings and s pairs of complex conjugate embeddings. Thus an (r,s)-Lipschitz system (of dimension n) gives a system of Lipschitz distance functions N_v on K_v^{n+1} for each infinite place v. For the finite places Masser and Vaaler choose

$$N_v(\mathbf{z}) = \max\{|z_0|_v, |z_1|_v, ..., |z_n|_v\}. \tag{2.2.3}$$

They proceed by defining a height $H_{\mathcal{N}}$ on K^{n+1} by

$$H_{\mathcal{N}}(\boldsymbol{\alpha})^d = \prod_v N_v(\sigma_v(\boldsymbol{\alpha}))^{d_v} \tag{2.2.4}$$

taken over all places v, where σ_v denotes the canonical embedding of K in K_v extended componentwise to K^{n+1}, $d = [K:\mathbb{Q}]$ and $d_v = [K_v :$

$\mathbb{Q}_v]$ denote the global and local degree. For any β in K^* we have the product formula

$$\prod_v |\sigma_v(\beta)|_v^{d_v} = 1. \tag{2.2.5}$$

Combined with (ii) it implies that (2.2.4) defines a height on $\mathbb{P}^n(K)$. We call $H_{\mathcal{N}}$ a *Lipschitz height*. To measure how much $H_{\mathcal{N}}$ differs from the absolute Weil height we use the estimate (2.2.2) for each factor $N_v(\cdot)$ and obtain

$$C_{\mathcal{N}}^{-1} H(\boldsymbol{\alpha}) \leq H_{\mathcal{N}}(\boldsymbol{\alpha}) \leq C'_{\mathcal{N}} H(\boldsymbol{\alpha}) \tag{2.2.6}$$

where

$$\begin{aligned} C_{\mathcal{N}} &= \max_v c_{N_v}^{-1} \\ C'_{\mathcal{N}} &= \max_v C'_{N_v}. \end{aligned} \tag{2.2.7}$$

Here v runs over all infinite places. For our purpose only $C_{\mathcal{N}}$ is important and we can forget $C'_{\mathcal{N}}$.

3. A general upper bound

Recall that K is a number field of degree d. Suppose we have a function $\mathcal{F} : \mathbb{P}^n(K) \longrightarrow [0, \infty)$ and a positive constant C such that $\mathcal{F}(P) \geq C^{-1} H(P)$ for all P in $\mathbb{P}^n(K)$. Let $Z_{\mathcal{F}}(\mathbb{P}^n(K), X)$ be the function that counts the points P in $\mathbb{P}^n(K)$ with $\mathcal{F}(P) \leq X$. The following corollary is almost an immediate consequence of Theorem 2.2.

Corollary 2.1. *Let $X \geq 0$ be real then*

$$Z_{\mathcal{F}}(\mathbb{P}^n(K), X) \leq \begin{cases} 2(1088 d \log d)^n (CX)^{d(n+1)} & \text{if } d > 1 \\ 3^{n+1}(CX)^{n+1} & \text{if } d = 1 \end{cases}.$$

Proof. By hypothesis $\mathcal{F}(P) \geq C^{-1} H(P)$ we have

$$Z_{\mathcal{F}}(\mathbb{P}^n(K), X) \leq Z_H(\mathbb{P}^n(K), CX). \tag{2.3.1}$$

Now every projective point $(\alpha_0 : \alpha_1 : ... : \alpha_n)$ has $\alpha_{n-i} \neq 0$ for some unique maximal i with $0 \leq i \leq n$. It follows that

$$Z_H(\mathbb{P}^n(K), CX) = \sum_{i=0}^{n} Z_H(K^i, CX)$$

where we interpret K^0 as $\{1\}$. For $d > 1$ we can apply Theorem 2.2 to estimate the right-hand side. In this way we derive the following upper bound

$$Z_{\mathcal{F}}(\mathbb{P}^n(K), X) \leq 1 + \sum_{i=1}^{n} (1088 d \log d)^i (CX)^{d(i+1)} \leq (CX)^d \sum_{i=0}^{n} Y^i$$

with $Y = (1088d\log d)(CX)^d$. Since $H(P) \geq 1$ we see by (2.3.1) that $Z_{\mathcal{F}}(\mathbb{P}^n(K), X) = 0$ if $CX < 1$. Therefore we may assume $CX \geq 1$. Since $d \geq 2$ we have $Y \geq 2$ and so

$$\sum_{i=0}^{n} Y^i = Y^n \sum_{i=0}^{n-1} Y^{-(n-i)} < 2Y^n.$$

Hence we have found the upper bound $2(1088d\log d)^n(CX)^{d(n+1)}$. The excluded case $K = \mathbb{Q}$ is trivial since the number of non-zero lattice points of $\mathbb{Z}^{n+1}$ in the set defined by $-CX \leq x_i \leq CX$ $(0 \leq i \leq n)$ is certainly an upper bound for $Z_H(\mathbb{P}^n(\mathbb{Q}), CX)$. On the other hand the number of such lattice points is $(2[CX]+1)^{n+1}-1$ which does not exceed $(3CX)^{n+1}$. Appealing to inequality (2.3.1) proves the claim for $d = 1$. □

4. Proof of Theorem 2.4

Every α of degree e over k is a zero of a monic polynomial irreducible over k with coefficients in k. We choose a height on $\mathbb{P}^e(k)$ as in Section 2 of this chapter but now for the more general case with arbitrary number field k and we will see in a moment that it is indeed a Lipschitz height. Let r be the number of real and s the number of complex conjugate pairs of embeddings of k. For each of the factors in $\mathbb{R}^r \times \mathbb{C}^s$ we choose

$$N(\mathbf{z}) = \mathcal{M}(z_0x^e + z_1x^{e-1} + ... + z_e).$$

We can choose $c_N = 2^{-e}$ (see [**22**] Lemma 2.2 p.56 or [**44**] Corollary 11 (38), p.248) and so $C_{\mathcal{N}}$ becomes

$$C_{\mathcal{N}} = 2^e. \tag{2.4.1}$$

Masser and Vaaler [**34**] proved that this defines an (r, s)-Lipschitz system $\mathcal{N}$. Moreover their equation (2.15) tells us that

$$H(1, \alpha)^e = H_{\mathcal{N}}(\mathbf{z}) \tag{2.4.2}$$

provided α is of degree e over k and $f = z_0x^e + ... + z_e$ is a non-zero polynomial of degree e with coefficients in k and vanishing in α. Hence e times the number of projective points in $\mathbb{P}^e(k)$ with $H_{\mathcal{N}}$ not larger than X^e is an upper bound for the number of α's in question. Thus Corollary 2.1 with $\mathcal{F} = H_{\mathcal{N}}$, $C = C_{\mathcal{N}} = 2^e$, $K = k$, $d = m$, $n = e$ and X replaced by X^e applies and we find exactly the desired upper bound.

CHAPTER 3

Counting over a fixed number field

In the first section we define a generalization of the Lipschitz systems of the previous chapter. This gives rise to a new height defined on $\mathbb{P}^n(K)$. In the second section we state Theorem 3.1, which is the main result of this chapter, and we deduce two corollaries. The last section is devoted to the proof of Theorem 3.1.

1. Arakelov-Lipschitz systems I

1.1. Motivation. In the last chapter we introduced Masser and Vaaler's Lipschitz systems. They led us to a quite general class of heights useful to prove counting results for points in $\mathbb{P}^n(K)$ but also for the number of algebraic numbers of fixed degree. Now we consider a simple example where a similar strategy works. Let V in K^3 be the vector space defined by the equation $2x + 3y - z = 0$. How many solutions (x, y, z) with height bounded above by X are there? We identify proportional solutions so that we have to count projective points $P = (x : y : z)$ were $z = 2x + 3y$ with $H(P) \leq X$ or what is the same count the number of $(x : y)$ in $\mathbb{P}^2(K)$ with $H_{\mathcal{N}}((x : y)) \leq X$. Here

$$H_{\mathcal{N}}((x : y)) = \prod_v \max\{|x|_v, |y|_v, |2x + 3y|_v\}^{d_v/d}$$

where $d = [K : \mathbb{Q}]$, $d_v = [K_v : \mathbb{Q}_v]$. Due to the ultrametric inequality we have

$$H_{\mathcal{N}}((x : y)) = \prod_{v|\infty} \max\{|x|_v, |y|_v, |2x + 3y|_v\}^{d_v/d} \prod_{v\nmid\infty} \max\{|x|_v, |y|_v\}^{d_v/d}.$$

Now it is easy to see that $H_{\mathcal{N}}$ defines a Lipschitz height in the sense of Masser and Vaaler and hence their Proposition answers the question. But what happens for the equation $2x + 3y + 5z = 0$? Here $\max\{|x|_v, |y|_v, |2x/5 + 3y/5|_v\} = \max\{|x|_v, |y|_v\}$ fails not only for the archimedean valuations but also for those lying above the prime 5. Hence we must be prepared to allow modifications on the max-norm not only at the infinite places but also at a finite number of finite places. We now switch to the general setting.

1.2. Arakelov-Lipschitz systems on a number field. Let K be a number field of degree d with r real embeddings and s pairs of complex conjugate embeddings. Recall that we identify M_K with the set of places of K. For a non-zero fractional ideal $\mathfrak{A}$ of K we abbreviate the norm $N_{K/\mathbb{Q}}(\mathfrak{A})$ to $N\mathfrak{A}$, which we consider as a rational number (not as an ideal) if not specified otherwise.
For every place v we fix a completion K_v of K at v. There is a value set

$$\Gamma_v = \{|\alpha|_v; \alpha \in K_v\}.$$

It is $[0,\infty)$ for v archimedean and

$$\{0, (N\mathfrak{p}_v)^0, (N\mathfrak{p}_v)^{\pm 1/d_v}, (N\mathfrak{p}_v)^{\pm 2/d_v}, ...\}$$

otherwise where $[K_v : \mathbb{Q}_v] = d_v$ denotes the local degree and $\mathbb{Q}_v$ is a completion with respect to the place which extends to v. For brevity we use $v \mid \infty$ if v is archimedean and $v \nmid \infty$ otherwise. For $v \mid \infty$ we identify K_v with $\mathbb{R}$ or $\mathbb{C}$ respectively and we identify $\mathbb{C}$ with $\mathbb{R}^2$ via $\xi \longrightarrow (\Re(\xi), \Im(\xi))$ where we used $\Re$ for the real and $\Im$ for the imaginary part of a complex number.
As usual n, M will always stand for a natural number. But L will denote a non-negative real number.

Definition 3.1 (Arakelov-Lipschitz system). *An Arakelov-Lipschitz system (ALS) $\mathcal{N}_K$ or simply $\mathcal{N}$ on K (of dimension n) is a set of continuous maps*

$$N_v : K_v^{n+1} \to \Gamma_v \quad v \in M_K \tag{3.1.1}$$

such that

(*i*) $N_v(\mathbf{z}) = 0$ *if and only if* $\mathbf{z} = \mathbf{0}$,

(*ii*) $N_v(\omega\mathbf{z}) = |\omega|_v N_v(\mathbf{z})$ *for all* ω *in* K_v *and all* $\mathbf{z}$ *in* K_v^{n+1},

(*iii*) $\begin{cases} \{\mathbf{z}; N_v(\mathbf{z}) = 1\} \text{ is in } Lip(d_v(n+1), 1, M, L) \text{ for some } M, L & : v \mid \infty \\ N_v(\mathbf{z}_1 + \mathbf{z}_2) \le \max\{N_v(\mathbf{z}_1), N_v(\mathbf{z}_2)\} \text{ for all } \mathbf{z}_1, \mathbf{z}_2 \text{ in } K_v^{n+1} & : v \nmid \infty \end{cases}$.

Moreover we assume that only a finite number of the functions $N_v(\cdot)$ are different from

$$N_v(\mathbf{z}) = \max\{|z_0|_v, ..., |z_n|_v\}. \tag{3.1.2}$$

If we consider only the functions N_v for $v|\infty$ then we get an (r,s)-Lipschitz system (of dimension n) in the sense of Masser and Vaaler [**34**]. If (*iii*) holds for some $M = M_{\mathcal{N}}, L = L_{\mathcal{N}}$ for every $v \mid \infty$, then we will say that $\mathcal{N}$ is a *ALS* with associated constants $M_{\mathcal{N}}, L_{\mathcal{N}}$. For $v|\infty$ we call N_v as in Chapter 2 a *Lipschitz distance function* (of dimension

n). We have already seen in Chapter 2 that the set defined in (iii) is the boundary of the set $\mathbf{B}_v = \{\mathbf{z}; N_v(\mathbf{z}) < 1\}$ and that therefore $\mathbf{B}_v$ is a bounded symmetric open star-body in $\mathbb{R}^{n+1}$ or $\mathbb{C}^{n+1}$. In particular $\mathbf{B}_v$ has a finite volume V_v.

Let us consider the system where N_v is as in (3.1.2) for all places v. If v is an infinite place then $\mathbf{B}_v$ is a cube for $d_v = 1$ and the complex analogue if $d_v = 2$. Their boundaries are clearly in $\mathrm{Lip}(d_v(n+1), 1, M, L)$ most naturally with $M = 2n+2$ maps and $L = 2$ if $d_v = 1$ and with $M = n+1$ maps and for example $L = 2\pi\sqrt{2n+1}$ if $d_v = 2$. This system is somehow the standard example for an Arakelov-Lipschitz system.

1.3. Preliminaries. For any $v \in M_K$ there is c_v in the value group $\Gamma_v^* = \Gamma_v \backslash \{0\}$ with

$$N_v(\mathbf{z}) \geq c_v \max\{|z_0|_v, ..., |z_n|_v\} \tag{3.1.3}$$

for all $\mathbf{z} = (z_0, ..., z_n)$ in K_v^{n+1}. For if v is archimedean then $\mathbf{B}_v$ is bounded open and contains the origin. Since Γ_v^* contains arbitrary small positive numbers the claim follows by (ii). Now for v non-archimedean N_v and $\max\{|z_0|_v, ..., |z_n|_v\}$ define norms on the vector space K_v^{n+1} over the complete field K_v. But on a finite dimensional vector space over a complete field all norms are equivalent ([**5**] Corollary 5. p.93) hence (3.1.3) remains true for a suitable choice of c_v.

So let $\mathcal{N}$ be an ALS on K of dimension n. For every v in M_K let c_v be an element of Γ_v^*, such that $c_v \leq 1$ and (3.1.3) holds. Due to (3.1.2) we can assume that $c_v \neq 1$ only for a finite number of $v's$. Define

$$C_{\mathcal{N}}^{fin} = \prod_v c_v^{-\frac{d_v}{d}} \geq 1 \tag{3.1.4}$$

where the product runs over all finite v. Next for the infinite part we define

$$C_{\mathcal{N}}^{inf} = \max_v\{c_v^{-1}\} \geq 1 \tag{3.1.5}$$

where now v runs over all infinite v.

Multiplying the finite and the infinite part gives rise to another constant

$$C_{\mathcal{N}} = C_{\mathcal{N}}^{fin} C_{\mathcal{N}}^{inf}. \tag{3.1.6}$$

It will turn out that besides $M_{\mathcal{N}}$ and $L_{\mathcal{N}}$ this is another important quantity for an *ALS*. So we say that $\mathcal{N}$ *is an ALS with associated constants* $C_{\mathcal{N}}, M_{\mathcal{N}}, L_{\mathcal{N}}$.

REMARK 4. *Let v be an infinite place. Suppose $N_v : K_v^{n+1} \longrightarrow [0,\infty)$ defines a norm, so that $N_v(\mathbf{z}_1+\mathbf{z}_2) \leq N_v(\mathbf{z}_1)+N_v(\mathbf{z}_2)$. Then $\mathbf{B}_v$ is convex and (3.1.3) combined with (3.1.4), (3.1.5) and (3.1.6) shows that $\mathbf{B}_v$ lies in $B_0(C_{\mathcal{N}}\sqrt{n+1})$. From Theorem A.1 in Appendix A it follows immediately that $\partial\mathbf{B}_v$ lies in Lip$(d_v(n+1),1,1,8{d_v}^2(n+1)^{5/2}C_{\mathcal{N}})$.*

We denote by $\sigma_1,...,\sigma_d$ the embeddings from K to $\mathbb{R}$ or $\mathbb{C}$ respectively, ordered such that $\sigma_{r+s+i}=\overline{\sigma}_{r+i}$ for $1\leq i\leq s$. We write

$$\sigma : K \longrightarrow \mathbb{R}^r\times\mathbb{C}^s \tag{3.1.7}$$

$$\sigma(\alpha)=(\sigma_1(\alpha),...,\sigma_{r+s}(\alpha)). \tag{3.1.8}$$

Sometimes it will be more readable to omit the brackets and simply write $\sigma\alpha$. We identify $\mathbb{C}$ in the usual way with $\mathbb{R}^2$ and extend σ componentwise to get a map

$$\sigma : K^{n+1} \longrightarrow \mathbb{R}^D \tag{3.1.9}$$

where $D=d(n+1)$. On $\mathbb{R}^D$ we use $|\cdot|$ for the usual euclidean norm. Let σ_v be the canonical embedding of K in K_v again extended componentwise on K^{n+1}.

DEFINITION 3.2. *Let $\mathfrak{D}\neq 0$ be a fractional ideal in K and $\mathcal{N}$ an ALS of dimension n. We define*

$$\Lambda_{\mathcal{N}}(\mathfrak{D})=\{\sigma(\boldsymbol{\alpha});\boldsymbol{\alpha}\in K^{n+1}, N_v(\sigma_v\boldsymbol{\alpha})\leq|\mathfrak{D}|_v \text{ for all finite } v\} \tag{3.1.10}$$

where $|\mathfrak{D}|_v = N\mathfrak{p}_v^{-\frac{ord_{\mathfrak{p}_v}\mathfrak{D}}{d_v}}$.

It is easy to see that $\Lambda_{\mathcal{N}}(\mathfrak{D})$ is a additive subgroup of $\mathbb{R}^D$ (the origin lies in $\Lambda_{\mathcal{N}}(\mathfrak{D})$, thanks to (*iii*) the set is closed under addition and by $|-1|_v=1$ and (*ii*) we get an additive inverse for every element). Now assume $B\geq 1$ and $|\sigma(\boldsymbol{\alpha})|\leq B$; then (3.1.3) implies $H(\boldsymbol{\alpha})^d\leq (BC_{\mathcal{N}}^{fin})^d N\mathfrak{D}^{-1}$ and by Northcott's Theorem we deduce that $\Lambda_{\mathcal{N}}(\mathfrak{D})$ is discrete. Hence it is a lattice.

Notice that for ε in K^* one has

$$\det\Lambda_{\mathcal{N}}((\varepsilon)\mathfrak{D})=|N_{K/\mathbb{Q}}(\varepsilon)|^{n+1}\det\Lambda_{\mathcal{N}}(\mathfrak{D}). \tag{3.1.11}$$

Therefore

$$\Delta_{\mathcal{N}}(\mathcal{D})=\frac{\det\Lambda_{\mathcal{N}}(\mathfrak{D})}{N\mathfrak{D}^{n+1}} \tag{3.1.12}$$

is independent of the choice of the representative $\mathfrak{D}$ but depends only on the ideal class $\mathcal{D}$ of $\mathfrak{D}$. Let Cl be the set of ideal classes. We define

$$V_{\mathcal{N}}^{fin} = 2^{-s(n+1)}|\Delta_K|^{\frac{n+1}{2}} h_K^{-1} \sum_{\mathcal{D}\in Cl} \Delta_{\mathcal{N}}(\mathcal{D})^{-1} \tag{3.1.13}$$

for the finite part. By s we denote the number of pairs of complex conjugate embeddings of K, h_K stands for the class number of K and Δ_K is the discriminant of K. The infinite part is defined by

$$V_{\mathcal{N}}^{inf} = \prod_{v|\infty} V_v.$$

By virtue of (3.1.3) we observe that

$$V_{\mathcal{N}}^{inf} = \prod_{v|\infty} V_v \leq \prod_{v|\infty} (2C_{\mathcal{N}}^{inf})^{d_v(n+1)} = (2C_{\mathcal{N}}^{inf})^{d(n+1)}. \tag{3.1.14}$$

We multiply the finite and the infinite part to get a global volume

$$V_{\mathcal{N}} = V_{\mathcal{N}}^{inf} V_{\mathcal{N}}^{fin}. \tag{3.1.15}$$

1.4. Arakelov-Lipschitz heights on a number field. In Subsection 1.2 we gave a slightly more general version of Masser and Vaaler's Lipschitz systems, which they used in [**34**] to define a class of heights. We proceed as in their article to obtain a generalization of these heights. So let $\mathcal{N}$ be an ALS on K of dimension n. Then the height $H_{\mathcal{N}}$ on K^{n+1} is defined by

$$H_{\mathcal{N}}(\boldsymbol{\alpha}) = \prod_{v} N_v(\sigma_v(\boldsymbol{\alpha}))^{\frac{d_v}{d}}$$

where the product is taken over all $v \in M_K$. The product over the archimedean absolute values will be denoted by $H_{\mathcal{N}}^{inf}(\cdot)$ and the one over the non-archimedean absolute values by $H_{\mathcal{N}}^{fin}(\cdot)$. The product formula (2.2.5) together with (ii) implies that $H_{\mathcal{N}}$ is well-defined on $\mathbb{P}^n(K)$.

Remark 5. *Multiplying (3.1.3) over all places with suitable multiplicities yields*

$$H_{\mathcal{N}}(\boldsymbol{\alpha}) \geq C_{\mathcal{N}}^{-1} H(\boldsymbol{\alpha}). \tag{3.1.16}$$

Thanks to Northcott's Theorem it follows that $\{P \in \mathbb{P}^n(K); H_{\mathcal{N}}(P) \leq X\}$ *is a finite set for each* X *in* $[0, \infty)$.

2. Introduction and results

We will investigate the set

$$\mathbb{P}^n(K/k) = \{P \in \mathbb{P}^n(K); k(P) = K\}$$

and its counting function

$$Z_{\mathcal{N}}(\mathbb{P}^n(K/k), X) = |\{P \in \mathbb{P}^n(K/k); H_{\mathcal{N}}(P) \leq X\}|.$$

In [**39**] Roy and Thunder introduced the quantity

$$\delta(K) = \inf_{\alpha}\{H(1,\alpha); K = \mathbb{Q}(\alpha)\}.$$

We generalize this definition for extensions K/k of number fields k, K

$$\delta(K/k) = \inf_{\alpha}\{H(1,\alpha); K = k(\alpha)\}.$$

The reader may wonder why we use the Weil height H and not $H_{\mathcal{N}}$ but for our purpose the choice of the height is not significant as long as one has (3.1.16) with some $C_{\mathcal{N}}$. Writing $[K : k] = e$ we define the integer

$$g_{\max} = g_{\max}(K/k) = \sup_{K_0}\{[K_0 : k]; k \subseteq K_0 \subsetneq K\} \leq \frac{e}{2}$$

if $k \neq K$, and we define

$$g_{\max} = g_{\max}(K/k) = 1$$

if $k = K$. Note that $1 \leq g_{\max} \leq \max\{1, e/2\}$. Finally write $m = [k : \mathbb{Q}]$ and

$$\mu = m(e - g_{\max})(n+1) - 1.$$

Recall the definition of the Schanuel constant

$$S_K(n) = \frac{h_K R_K}{w_K \zeta_K(n+1)}\left(\frac{2^{r_K}(2\pi)^{s_K}}{\sqrt{|\Delta_K|}}\right)^{n+1}(n+1)^{r_K+s_K-1}. \tag{3.2.1}$$

Here h_K is the class number, R_K the regulator, w_K the number of roots of unity in K, ζ_K the Dedekind zeta-function of K, Δ_K the discriminant, r_K is the number of real embeddings of K and s_K is the number of pairs of distinct complex conjugate embeddings of K. For non-negative real functions $f(X), g(X), h(X)$ we say that $f(X) = g(X) + O(h(X))$ as $X > X_0$ tends to infinity if there is a constant C_0 (independent of X) such that $|f(X) - g(X)| \leq C_0 h(X)$ for each $X > X_0$. The main result of this chapter is Theorem 3.1 below. But first we give an important consequence.

COROLLARY 3.1. *Let k, K be number fields with $k \subseteq K$ and $[K : k] = e$, $[k : \mathbb{Q}] = m$, $[K : \mathbb{Q}] = d$. Let $\mathcal{N}$ be an Arakelov-Lipschitz system of dimension n on K with associated constants $C_{\mathcal{N}}, L_{\mathcal{N}}, M_{\mathcal{N}}$ and write*

$$A_{\mathcal{N}} = M_{\mathcal{N}}^{d}(C_{\mathcal{N}}(L_{\mathcal{N}} + 1))^{d(n+1)-1}. \tag{3.2.2}$$

Then as $X > 0$ tends to infinity we have

$$\begin{aligned} Z_{\mathcal{N}}(\mathbb{P}^n(K/k), X) =& 2^{-r_K(n+1)}\pi^{-s_K(n+1)}V_{\mathcal{N}}S_K(n)X^{d(n+1)} \\ &+O(A_{\mathcal{N}}R_K h_K \delta(K/k)^{-\mu}X^{d(n+1)-1}\mathfrak{L}) \end{aligned}$$

where

$$\mathfrak{L} = \log \max\{2, 2C_{\mathcal{N}}X\} \text{ if } (n, d) = (1, 1) \text{ and } \mathfrak{L} = 1 \text{ otherwise}$$

and the implied constant in O depends only on n and d.

Now with $k = K$ the above corollary leads to a version of the Proposition in [**34**] with explicit error term regarding the field K. In particular we get Schanuel's Theorem with an explicit error term with respect to the field. A more precise version can be obtained by counting primitive points (over $\mathbb{Q}$) for all subfields of K (see Corollary 3.2 below). However the main purpose of Corollary 3.1 is to improve Schmidt's upper bound (2.1.1) in Theorem 2.3 from Chapter 2 when n and X are large. To prove the asymptotics in the Main Theorem of Chapter 4 we need a more precise theorem using a slightly more sophisticated quantity than $\delta(K/k)$.

First for fields k, K with $k \subseteq K$ and $[K : k] = e$ define the set

$$G(K/k) = \{g; \text{there is a field } K_0 \text{ with } k \subseteq K_0 \subsetneq K \text{ and } [K_0 : k] = g\}$$

if $k \neq K$, and define

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

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

$$\delta_g(K/k) = \inf_{\alpha,\beta}\{H(1, \alpha, \beta); k(\alpha, \beta) = K, [k(\alpha) : k] = g\} \geq 1 \tag{3.2.3}$$

and

$$\mu_g = m(e - g)(n + 1) - 1. \tag{3.2.4}$$

Note that $\delta_1(K/k) = \delta(K/k)$. Furthermore $g_{\max}$ and μ in Corollary 3.1 are simply the maximal g and the minimal μ_g

$$g_{\max} = \max_{g \in G} g, \qquad \mu = \min_{g \in G} \mu_g.$$

THEOREM 3.1. *Let k, K be number fields with $k \subseteq K$ and $[K:k] = e$, $[k:\mathbb{Q}] = m$, $[K:\mathbb{Q}] = d$. Let $\mathcal{N}$ be an Arakelov-Lipschitz system of dimension n on K with associated constants $C_{\mathcal{N}}, L_{\mathcal{N}}, M_{\mathcal{N}}$. Write*

$$A_{\mathcal{N}} = M_{\mathcal{N}}^{d}(C_{\mathcal{N}}(L_{\mathcal{N}}+1))^{d(n+1)-1} \tag{3.2.5}$$

and

$$B = A_{\mathcal{N}} R_K h_K \sum_{g \in G(K/k)} \delta_g(K/k)^{-\mu_g}.$$

Then as $X > 0$ tends to infinity we have

$$Z_{\mathcal{N}}(\mathbb{P}^n(K/k), X) = 2^{-r_K(n+1)}\pi^{-s_K(n+1)} V_{\mathcal{N}} S_K(n) X^{d(n+1)} + O(BX^{d(n+1)-1}\mathfrak{L}),$$

where

$$\mathfrak{L} = \log \max\{2, 2C_{\mathcal{N}}X\} \text{ if } (n,d) = (1,1) \text{ and } \mathfrak{L} = 1 \text{ otherwise}$$

and the implied constant in O depends only on n and d.

To see that Theorem 3.1 implies Corollary 3.1 we need the following well-known argument. Since it will be frequently used in the sequel we are not ashamed to give a proof here.

LEMMA 3.1. *Let F be a field of characteristic zero and L a finite extension of relative degree e generated by $\alpha_1, ..., \alpha_t$. Then there are integers $0 \leq m_1, ..., m_t < e$ such that $F(\alpha) = L$ for $\alpha = \sum_{j=1}^{t} m_j \alpha_j$. Moreover we may assume at most $\log_2(e)$ of the m_j are non-zero.*

Proof. It is well-known and easily seen (e.g. by induction on r) that for a polynomial $P(X_1, ..., X_r) \in F[X_1, ..., X_r]$ not identically zero with total degree p we can find integers $m_1, ..., m_r$ among $0, ..., p$ such that $P(m_1, ..., m_r) \neq 0$. Now the case $e = 1$ is trivial and moreover when $e \geq 2$ we may choose elements, say $\alpha_1, ..., \alpha_r$, among $\alpha_1, ..., \alpha_t$ with

$$F \subsetneq F(\alpha_1) \subsetneq F(\alpha_1, \alpha_2) \subsetneq ... \subsetneq F(\alpha_1, ..., \alpha_r) = L. \tag{3.2.6}$$

Thus $r \leq \log_2 e$. Denote the conjugates of α_j over F by $\alpha_j^{(i)}$ for $1 \leq i \leq e$. We consider the polynomial

$$P(X_1, ..., X_r) = \prod_{i=2}^{e} (\sum_{j=1}^{r} (\alpha_j^{(1)} - \alpha_j^{(i)}) X_j). \tag{3.2.7}$$

Since $L = F(\alpha_1, ..., \alpha_r)$ none of the factors $\sum_{j=1}^{r}(\alpha_j^{(1)} - \alpha_j^{(i)})X_j$ are zero and so P is not identically zero and of total degree $e-1$. Using the observation of the beginning we get integers $m_1, ..., m_r$ with $0 \leq m_j < e$ such that $P(m_1, ..., m_r) \neq 0$. But this implies $\alpha = \sum_{j=1}^{r} m_j \alpha_j$ generates L over F. □

Now let us prove that Theorem 3.1 implies Corollary 3.1. We have to show that the error term in the former is bounded above by the error term in the latter. If $K = k$ then $\delta = \delta(K/k) = 1$, while $G(K/k) = \{1\}$ and $\delta_1(K/k) = 1$, $\mu_1 = -1$. So we are done. If $K \neq k$ then each g in $G(K/k)$ satisfies $g \leq g_{\max}$ and so $\mu_g \geq \mu$. Thus we have to compare $\delta_g = \delta_g(K/k)$ with δ. Let α_1, α_2 be any numbers in K such that $k(\alpha_1, \alpha_2) = K$. By the previous lemma we deduce that there are rational integers $0 \leq m_1, m_2 < e$ such that $\xi = m_1\alpha_1 + m_2\alpha_2$ is primitive, so $K = k(\xi)$. Hence $\delta(K/k) \leq H(1, \xi)$. On the other hand an easy calculation shows $H(1, \xi) \leq 2H(1, m_1, m_2)H(1, \alpha_1, \alpha_2) \leq 2eH(1, \alpha_1, \alpha_2)$. Hence $\delta \leq 2e\delta_g$ for all g in $G(K/k)$. This suffices to deduce Corollary 3.1 from Theorem 3.1.

As mentioned after Corollary 3.1 we may obtain a version of Proposition in [**34**] with a good error term regarding the field K by using

$$Z_{\mathcal{N}}(\mathbb{P}^n(K), X) = \sum_{\mathbb{Q} \subseteq K_0 \subseteq K} Z_{\mathcal{N}}(\mathbb{P}^n(K_0/\mathbb{Q}), X).$$

The terms with $K_0 = K$ are dealt with by Corollary 3.1 and those with $K_0 \neq K$ by Corollary 2.1 with $\mathcal{F} = H_{\mathcal{N}}$, $C = C_{\mathcal{N}}$ and $[K_0 : \mathbb{Q}] \leq g_{\max}(K/\mathbb{Q})$. It is well-known that the number of subfields of K is bounded only in terms of $d = [K : \mathbb{Q}]$ (for example counting subsets of the group of the galois closure gives $2^{d!}$ and realizing that an intermediate group of two groups $H \subseteq G$ is a union of cosets of H gives even 2^d). This leads immediately to

Corollary 3.2. *Let K be a number field of degree d. Let $\mathcal{N}$ be an Arakelov-Lipschitz system of dimension n on K with associated constants $C_{\mathcal{N}}, L_{\mathcal{N}}, M_{\mathcal{N}}$. Then as $X > 0$ tends to infinity we have*

$$\begin{aligned} Z_{\mathcal{N}}(\mathbb{P}^n(K), X) =& 2^{-r_K(n+1)}\pi^{-s_K(n+1)}V_{\mathcal{N}}S_K(n)X^{d(n+1)} \\ &+O(A_{\mathcal{N}}R_Kh_K\delta(K/\mathbb{Q})^{-(d-g_{\max}(K/\mathbb{Q}))(n+1)+1}X^{d(n+1)-1}\mathfrak{L}) \\ &+O((C_{\mathcal{N}}X)^{g_{\max}(K/\mathbb{Q})(n+1)}) \end{aligned}$$

where the constants in O depend only on n, d and $A_{\mathcal{N}}, \mathfrak{L}$ are defined in Theorem 3.1. Moreover for $K = \mathbb{Q}$ the second error term can be omitted.

3. Proof of Theorem 3.1

Here all constants involved in $\ll$ or $\gg$ depend only on n, d (so are independent of K, k and $\mathcal{N}$). The constants $C_{\mathcal{N}}, M_{\mathcal{N}}, L_{\mathcal{N}}$ will be abbreviated to C, M, L. Lemma 3.2 and Lemma 3.9 have much in common with Lemma 3 and Lemma 4 respectively of [**34**]. To minimize

confusion we tried to use the original notations whenever possible. So let $q = r+s-1$, Σ the hyperplane in $\mathbb{R}^{q+1}$ defined by $x_1+...+x_{q+1} = 0$ and $\boldsymbol{\delta} = (d_1, ..., d_{q+1})$ with $d_i = 1$ for $1 \leq i \leq r$ and $d_i = 2$ for $r+1 \leq i \leq r+s = q+1$. The map $l(\eta) = (d_1 \log|\sigma_1(\eta)|, ..., d_{q+1}\log|\sigma_{q+1}(\eta)|)$ sends K^* to $\mathbb{R}^{q+1}$. The image of the unit group $\mathbb{U} = \mathcal{O}_K^*$ under l is a lattice in Σ with determinant $\sqrt{q+1}R_K$ (for $q = 0$ we consider $\mathbf{0}$ as a lattice in $\mathbf{0}$).

Let F be a bounded set in Σ and for real, positive T let $F(T)$ be the vector sum

$$F(T) = F + \boldsymbol{\delta}(-\infty, \log T]. \tag{3.3.1}$$

We denote by exp the diagonal exponential map from $\mathbb{R}^{q+1}$ to $[0,\infty)^{q+1}$. We have $r+s$ Lipschitz distance functions $N_1, ..., N_{q+1}$ one for each factor of $\mathbb{R}^r \times \mathbb{C}^s$. We use variables $\mathbf{z}_1, ..., \mathbf{z}_{q+1}$ with $\mathbf{z}_i$ in $\mathbb{R}^{d_i(n+1)}$. Now we define $S_F(T)$ in $\mathbb{R}^D$ for $D = \sum_{i=1}^{q+1} d_i(n+1) = d(n+1)$ as the set of all $\mathbf{z}_1, ..., \mathbf{z}_{q+1}$ such that

$$(N_1(\mathbf{z}_1)^{d_1}, ..., N_{q+1}(\mathbf{z}_{q+1})^{d_{q+1}}) \in \exp F(T). \tag{3.3.2}$$

3.1. The boundary of $S_F(1)$ is Lipschitz parameterizable. The archimedean condition (iii) in Subsection 1.2 was introduced by Masser and Vaaler to ensure that the set $S_F(T)$ has Lipschitz parameterizable boundary of codimension one. The latter is shown in [**34**] Lemma 3. To see the dependence on F, L, M for the Lipschitz constant corresponding to $\partial S_F(T)$, we need an explicit (up to dependence on n, d) version of this Lemma 3. We worked out a completely explicit lemma to the cost that the proof gets a bit tedious. Notice that for $q = 0$ the boundary of $S_F(1)$ is nothing but the set defined in (iii) Subsection 1.2 (for $v|\infty$) and so in that case we have $\partial S_F(1)$ lies in $\mathrm{Lip}(D, 1, M, L)$.

LEMMA 3.2. *Suppose $q \geq 1$ and let F be a set in Σ such that ∂F is in Lip$(q+1, 2, M', L')$ and moreover assume F lies in $B_0(r_F)$. Then $\partial S_F(1)$ is in Lip$(D, 1, \widetilde{M}, \widetilde{L})$ where one can choose*

$$\widetilde{M} = (M'+1)M^{q+1}$$
$$\widetilde{L} = 3\sqrt{D}(L'+r_F+1)\exp\{\sqrt{q}(L'+r_F)\}(L + C_{\mathcal{N}}^{inf}).$$

Proof. For $1 \leq i \leq M'$ let

$$\psi^{(i)} : [0,1]^{q-1} \longrightarrow \mathbb{R}^{q+1}$$

be the parameterizing maps of ∂F with Lipschitz constants L'. Choose an orthonormal basis $e_1, ..., e_q$ of Σ. The affine map $\nu : [0,1]^q \longrightarrow \Sigma$ defined by

$$\nu(\mathbf{t}) = (1-2t_1)r_F e_1 + ... + (1-2t_q)r_F e_q \tag{3.3.3}$$

is a Lipschitz parameterization covering the topological closure $\overline{F}$ with Lipschitz constant $2r_F$. Since $\boldsymbol{\delta}$ is not in Σ the boundary $\partial F(1)$ consists of two parts

$$\partial(F(1)) = (\partial(F) + (-\infty, 0]\boldsymbol{\delta}) \cup \overline{F}.$$

So we see that $\partial(F(1))$ is parameterized by $M'+1$ maps. Here the parameter domain is not compact anymore but this problem can easily be eliminated as we shall see in a moment. Since F is bounded we may use (3.3.1) to get

$$\begin{aligned} \partial(\exp(F(1))) &= \exp(\partial(F(1))) \cup \{\mathbf{0}\} \\ &= \exp(\partial(F) + (-\infty, 0]\boldsymbol{\delta}) \cup \exp(\overline{F}) \cup \{\mathbf{0}\}. \end{aligned} \tag{3.3.4}$$

With a $\psi = (\psi_1, ..., \psi_{q+1}) = \psi^{(i)}$ as above, the first part is covered by

$$\Phi = \exp(\psi + t\boldsymbol{\delta}) = (e^{\psi_1 + td_1}, ..., e^{\psi_{q+1}+td_{q+1}}) = (e^{\psi_1}u^{d_1}, ..., e^{\psi_{q+1}}u^{d_{q+1}}) \tag{3.3.5}$$

with parameter domain $[0,1]^{q-1} \times (-\infty, 0]$ and $u = e^t$ in $(0,1]$. Now we simply choose u as parameter instead of t and extend its parameter range from $(0,1]$ to $[0,1]$ to cover the origin. The remaining part of (3.3.4) is covered by

$$\Phi = \exp(\nu). \tag{3.3.6}$$

We use $\mathbf{t}$ for the parameter variables in $[0,1]^q$, not just for (3.3.6) as in (3.3.3) but also for (3.3.5). So until now we have $M'+1$ maps. We denote them by $\Phi^{(i)}$ for $1 \leq i \leq M'+1$ or more simply Φ. The N_i are continuous functions and therefore $\partial S_F(1)$ consists of these $(\mathbf{z}_1, ..., \mathbf{z}_{q+1})$ in $\prod_{i=1}^{q+1} \mathbb{R}^{d_i(n+1)} = \mathbb{R}^{d(n+1)}$ such that

$$(N_1(\mathbf{z}_1)^{d_1}, ..., N_{q+1}(\mathbf{z}_{q+1})^{d_{q+1}}) \in \partial(\exp(F(1))).$$

By our assumptions on $\mathcal{N}$ there are maps

$$\eta_i^{(j)} : [0,1]^{d_i(n+1)-1} \longrightarrow \mathbb{R}^{d_i(n+1)} \tag{3.3.7}$$

for $1 \leq i \leq q+1$ and $1 \leq j \leq M$ satisfying a Lipschitz condition and whose images cover the sets

$$\{\mathbf{z} \in \mathbb{R}^{d_i(n+1)}; N_i(\mathbf{z}) = 1\}. \tag{3.3.8}$$

We write more simply η_i. For real $\zeta \geq 0$ the images of $\zeta\eta_i$ cover the sets $\{\mathbf{z} \in \mathbb{R}^{d_i(n+1)}; N_i(\mathbf{z}) = \zeta\}$ and with $\Phi = (\Phi_1, ..., \Phi_{q+1})$ we obtain a parameterization of $\partial S_F(1)$ by maps

$$(\Phi_1(\mathbf{t})^{\frac{1}{d_1}}\eta_1(\underline{\mathbf{t}}^{(\mathbf{1})}), ..., \Phi_{q+1}(\mathbf{t})^{\frac{1}{d_{q+1}}}\eta_{q+1}(\underline{\mathbf{t}}^{(\mathbf{q+1})})). \tag{3.3.9}$$

We have $M'+1$ possibilities for Φ and M possibilities for each η_i. Hence the total number of parameterization maps is $(M'+1)M^{q+1}$ and the number of parameters is $q+\sum_{i=1}^{q+1}(d_i(n+1)-1) = d(n+1)-1 = D-1$ as desired.

To verify the Lipschitz conditions and to compute a Lipschitz constant we make use of the following assertions.

(1) Suppose $f_i : [0,1]^{D-1} \longrightarrow \mathbb{R}^{n_i}$ have Lipschitz constants L_i $(1 \leq i \leq q+1)$. Then $f = (f_1, .., f_{q+1}) : [0,1]^{D-1} \longrightarrow \mathbb{R}^{n_1+...+n_{q+1}}$ has a Lipschitz constant $\sqrt{L_1^2 + ... + L_{q+1}^2}$.

(2) Suppose $f : [0,1]^{E-1} \longrightarrow \mathbb{R}^n$ has a Lipschitz constant L. Then for any $D > E$ the function $f' : [0,1]^{D-1} \longrightarrow \mathbb{R}^n$ defined by $f'(\mathbf{x}, \mathbf{x}') = f(\mathbf{x})$ also has a Lipschitz constant L.

(3) Assume $f : [0,1]^E \longrightarrow \mathbb{R}$, $f' : [0,1]^{E'} \longrightarrow \mathbb{R}^n$ are functions with Lipschitz constants L, L'. Then $\sqrt{2}\max\{\|f'\|_\infty L, \|f\|_\infty L'\}$ is a Lipschitz constant of the function $g : [0,1]^{E+E'} \longrightarrow \mathbb{R}^n$ defined by $g(\mathbf{x}, \mathbf{x}') = f(\mathbf{x})f'(\mathbf{x}')$, where $\|f\|_\infty = \sup|f|, \|f'\|_\infty = \sup|f'|$ for the euclidean norms $|f|, |f'|$.

Here (1) and (2) are clear. To prove (3) we write $f' = (f'_1, ..., f'_n)$ so that

$$|g(\mathbf{x}, \mathbf{x}') - g(\mathbf{y}, \mathbf{y}')|^2 = \sum_{i=1}^{n}(f(\mathbf{x})f'_i(\mathbf{x}') - f(\mathbf{y})f'_i(\mathbf{y}'))^2$$

which because of

$$(aa' - bb')^2 = (a'(a-b) + b(a'-b'))^2 \leq 2(a'^2(a-b)^2 + b^2(a'-b')^2)$$

is at most

$$\begin{aligned} &2\sum_{i=1}^{n}(f'_i(\mathbf{x}')^2(f(\mathbf{x}) - f(\mathbf{y}))^2 + (f(\mathbf{y})^2(f'_i(\mathbf{x}') - f'_i(\mathbf{y}'))^2) \\ \leq &2(\|f'\|_\infty^2 L^2|\mathbf{x} - \mathbf{y}|^2 + \|f\|_\infty^2 L'^2|\mathbf{x}' - \mathbf{y}'|^2). \end{aligned}$$

Now (3) follows because the squared distance between $(\mathbf{x}, \mathbf{x}')$ and $(\mathbf{y}, \mathbf{y}')$ is $|\mathbf{x} - \mathbf{y}|^2 + |\mathbf{x}' - \mathbf{y}'|^2$.

Back to (3.3.9). First we will apply (3) to compute Lipschitz constants of the the single components in (3.3.9) and then we will make use of (2) and (1) to establish the final Lipschitz constant. According to (3.3.5) and (3.3.6) respectively two cases for Φ may arise. For the first case we have

$$\|\Phi_i^{\frac{1}{d_i}}\|_\infty = \|e^{\frac{\psi_i}{d_i}}u\|_\infty \leq \|e^{\frac{\psi_i}{d_i}}\|_\infty \leq e^{\|\frac{\psi_i}{d_i}\|_\infty} = E_i, \tag{3.3.10}$$

say. We may assume that the image $Im\psi$ of ψ meets ∂F in a point P (for if not then we can omit ψ) and so by assumption $|P| \leq r_F$. Let P' be an arbitrary point in $Im\psi$. Using the Lipschitz condition and the triangle inequality yields $|P'| \leq r_F + \sqrt{q-1}L'$ and therefore

$$\|\psi_i\|_\infty \leq \sqrt{q-1}L' + r_F. \tag{3.3.11}$$

If we plug this in (3.3.10) we obtain

$$\begin{aligned} \|\Phi_i^{\frac{1}{d_i}}\|_\infty \leq E_i &\leq \exp(\frac{\sqrt{q-1}L'}{d_i} + \frac{r_F}{d_i}) \\ &\leq \exp(\frac{\sqrt{q}}{d_i}(L' + r_F)). \end{aligned} \tag{3.3.12}$$

Now notice that $\|\nu\|_\infty = \sqrt{q}r_F$ and therefore $\|\exp(\nu/d_i)\|_\infty \leq \exp(\sqrt{q}r_F/d_i)$. This shows that the estimate (3.3.12) holds also in the second case (3.3.6).

Next let us compute a Lipschitz constant L_i of $\Phi_i^{\frac{1}{d_i}}$. We proceed by distinguishing the cases (3.3.5) and (3.3.6). For the first case we observe that 1 is a Lipschitz constant of $f = u$ and furthermore $\|u\|_\infty = 1$. Also for $f' = e^{\frac{\psi_i}{d_i}}$ we have $\|f'\|_\infty \leq E_i$, and the Mean Value Theorem leads to a Lipschitz constant for f' of the form E_iL'/d_i. So by (3) we get a Lipschitz constant for ${\Phi_i}^{\frac{1}{d_i}} = ff'$ of the form

$$\sqrt{2}(\frac{L'}{d_i} + 1)E_i \leq \sqrt{2}(L' + 1)\exp(\frac{\sqrt{q}}{d_i}(L' + r_F))$$

using (3.3.12).
Similarly we recover the Lipschitz constant

$$\frac{2r_F}{d_i}\exp(\frac{\sqrt{q}r_F}{d_i})$$

for $\Phi_i^{\frac{1}{d_i}}$ in the second case (3.3.6). We choose

$$L_i = 2(L' + r_F + 1)\exp(\frac{\sqrt{q}}{d_i}(L' + r_F)) \tag{3.3.13}$$

to cover both cases at once.

Back to (3.3.9) again. We intend to apply (3) to $\Phi_i(\mathbf{t})^{\frac{1}{d_i}}\eta_i(\underline{\mathbf{t}}^{(\mathbf{i})}) = ff'$. We may assume that (3.3.8) and the image of η_i have a common point, say Q. Hence by (3.1.3) and (3.1.5) we get $|Q| \leq \sqrt{n+1}C_{\mathcal{N}}^{inf}$. Since L is a Lipschitz constant of η_i we see as in (3.3.11) that

(3.3.14)

$$\|\eta_i\|_\infty \leq \sqrt{d_i(n+1)-1}L + \sqrt{n+1}C_{\mathcal{N}}^{inf} \leq \sqrt{d_i(n+1)}(L + C_{\mathcal{N}}^{inf}).$$

Now using (3) with (3.3.12), (3.3.13) and (3.3.14) yields the Lipschitz constant

$$3\sqrt{d_i(n+1)}(L' + r_F + 1)\exp(\frac{\sqrt{q}}{d_i}(L' + r_F))(L + C_{\mathcal{N}}^{inf})$$

for the component functions in (3.3.9). Finally we extend the component functions as in (2) on $[0,1]^{d(n+1)-1}$ to use (1). This leads to the final Lipschitz constant

$$3\sqrt{D}(L' + r_F + 1)\exp\{\sqrt{q}(L' + r_F)\}(L + C_{\mathcal{N}}^{inf}).$$

□

In our first application F will have the form

$$[0,1)v_1 + ... + [0,1)v_q \tag{3.3.15}$$

for $v_1, ..., v_q$ in $\mathbb{R}^{q+1}$ with $|v_1|, ..., |v_q| < 1$. It is easy to see that ∂F is Lipschitz parameterizable; a typical boundary point has the form $x_1v_1 + ... + x_qv_q$ with some $x_i = 0$ or 1, so for example if $i = q$ then this expression gives a parameterization on the variables $x_1, ..., x_{q-1}$. We find in this way that ∂F is in $\mathrm{Lip}(q+1, 2, 2q, q-1)$.

3.2. Schmidt's partition method. First suppose $q > 0$. We choose F as a fundamental domain of the unit lattice $l(\mathbb{U})$ more precisely $F = [0,1)u_1 + ... + [0,1)u_q$, where $U = (u_1, ..., u_q)$ is a basis of $l(\mathbb{U})$. The major step of the proof is counting lattice points in the set $S_F(T)$. This will be carried out with the help of Theorem 1.2. But here the relevant Lipschitz constants may depend on the units in a fatal way. In fact F has volume $\sqrt{q+1}R_K$ and so if we are unlucky then it might not lie in a ball of radius much smaller than R_K. Thus $\exp(F)$ might not lie in a ball of radius much smaller than $\exp(R_K)$. This might introduce Lipschitz constants of this size and consequently the error terms in the counting could be this large. That however is far from what we claim in Theorem 3.1. And such an exponential dependence on R_K would be disastrous for the summation techniques in Chapter 4. To overcome this problem we extend an idea of Schmidt

[**49**] from the real-quadratic case $d = 2$ to arbitrary d (see also [**17**] for $d > 2$).

Let us carry out the details. First we define the $q + 1$ natural numbers

$$n_j = [|u_j|] + 1 \quad (1 \le j \le q), \tag{3.3.16}$$

$$t = n_1 ... n_q. \tag{3.3.17}$$

Let $Q = |\{\beta \in \overline{\mathbb{Q}}; [\mathbb{Q}(\alpha) : \mathbb{Q}] \le d, \log H(1, \alpha) \le 1\}|$. If α of degree at most d is neither zero nor a root of unity then the $Q + 1$ numbers $1, \alpha, ..., \alpha^Q$ are pairwise distinct and therefore $\log H(1, \alpha^Q) > 1$ or

$$\log H(1, \alpha) > Q^{-1}.$$

We take $\alpha = \eta_j$ for $l(\eta_j) = u_j$ to deduce

$$\exp(d/Q) \le H(1, \eta_j)^d = \prod_{i=1}^{q+1} \max\{1, |\sigma_i(\eta_j)|^{d_i}\}.$$

It follows that $|\sigma_i(\eta_j)| \ge \exp(1/Q)$ for some i. Thus

$$|u_j|^2 = \sum_{k=1}^{q+1} d_k^2 \log^2 |\sigma_k(\eta_j)| \ge (1/Q)^2$$

and so

$$|u_j| \ge 1/Q > 0,$$

where Q depends only on d. The inequality above implies $[|u_j|] + 1 \le (1 + Q)|u_j|$. Recalling the definition of the orthogonality defect $\Omega(U)$ of U and not forgetting that $\det l(\mathbb{U}) = \sqrt{q+1} R_K$ yields

$$\sqrt{q+1} R_K < t \le (1 + Q)^q \Omega(U) \sqrt{q+1} R_K.$$

Now we choose a reduced basis U; that is, $\Omega(U) \ll 1$. Hence

$$R_K \ll t \ll R_K. \tag{3.3.18}$$

Let us define

$$F(\mathbf{i}) = i_1 \frac{u_1}{n_1} + ... + i_q \frac{u_q}{n_q} + [0, 1)\frac{u_1}{n_1} + ... + [0, 1)\frac{u_q}{n_q} \tag{3.3.19}$$

with $\mathbf{i} = (i_1, ..., i_q)$ for $0 \le i_j < n_j$ $(1 \le j \le q)$. Then the partition $F = \bigcup_{\mathbf{i}} F(\mathbf{i})$ leads to a partition

$$S_F(T) = \bigcup_{\mathbf{i}} S_{F(\mathbf{i})}(T) \tag{3.3.20}$$

in t subsets. For each of these t vectors $\mathbf{i}$ we define a translation $tr_{\mathbf{i}}$ on $\mathbb{R}^{q+1}$ by

$$tr_{\mathbf{i}}(x) = x - \sum_{j=1}^{q} \frac{i_j u_j}{n_j}.$$

This translation sends Σ to Σ and $F(\mathbf{i})$ to $F(\mathbf{0})$. It has an exponential counterpart $etr_{\mathbf{i}}$ defined by $etr_{\mathbf{i}}(\exp(x)) = \exp(tr_{\mathbf{i}}(x))$ and this takes the form

$$etr_{\mathbf{i}}(X_1, ..., X_{q+1}) = (\gamma_1^{d_1} X_1, ..., \gamma_{q+1}^{d_{q+1}} X_{q+1})$$

for positive real $\gamma_1, ..., \gamma_{q+1}$, depending on $\mathbf{i}$, with

$$\gamma_1^{d_1} ... \gamma_{q+1}^{d_{q+1}} = 1. \tag{3.3.21}$$

We define the automorphism $\tau_{\mathbf{i}}$ of $\mathbb{R}^D$ by

$$\tau_{\mathbf{i}}(\mathbf{z}_1, ..., \mathbf{z}_{q+1}) = (\gamma_1 \mathbf{z}_1, ..., \gamma_{q+1} \mathbf{z}_{q+1}), \tag{3.3.22}$$

so that

$$\det \tau_{\mathbf{i}} = 1. \tag{3.3.23}$$

Now

$$etr_{\mathbf{i}}(\exp(F(\mathbf{i})(T))) = \exp(tr_{\mathbf{i}}(F(\mathbf{i})(T))) = \exp(F(\mathbf{0})(T))$$

and so (3.3.2) together with (ii) of Subsection 1.2 gives

$$\tau_{\mathbf{i}} S_{F(\mathbf{i})}(T) = S_{F(\mathbf{0})}(T). \tag{3.3.24}$$

The identity

$$S_F(T) = T S_F(1) \tag{3.3.25}$$

holds for any F in Σ whatsoever and in particular

$$S_{F(\mathbf{0})}(T) = T S_{F(\mathbf{0})}(1). \tag{3.3.26}$$

Thanks to (3.3.16) and the triangle inequality, $|\theta_1 \frac{u_1}{n_1} + ... + \theta_q \frac{u_q}{n_q}| \leq q$ holds for any $\theta_j \in [0, 1)$. From the definition of $F(\mathbf{0})$ and $S_{F(\mathbf{0})}$ it follows that

$$S_{F(\mathbf{0})}(1) \subseteq \{(\mathbf{z}_1, ..., \mathbf{z}_{q+1}); N_i(\mathbf{z}_i)^{d_i} \leq e^q \text{ for } 1 \leq i \leq q+1\}. \tag{3.3.27}$$

On recalling the definition (3.1.5) of $C_{\mathcal{N}}^{inf}$ the above inclusion together with (3.3.26) yields

$$S_{F(\mathbf{0})}(T) \subseteq B_0(\kappa T) \tag{3.3.28}$$

where $\kappa = \sqrt{d(n+1)} C_{\mathcal{N}}^{inf} \exp\{q\}$ and $B_0(\kappa T)$ denotes the euclidean ball centered at the origin with radius κT.

From now on let $\mathbf{i}$ be fixed so that we may drop the index and write

τ. The $\mathbf{z}_i$ lie in $\mathbb{R}^{n+1}$ or $\mathbb{C}^{n+1}$. By abuse of notation we set $n = 0$ so that we may interpret these vectors for a moment as numbers in $\mathbb{R}$ or $\mathbb{C}$. Then the right hand side of (3.3.22) defines an automorphism of $\mathbb{R}^d$, say p_τ with

$$\det p_\tau = 1. \tag{3.3.29}$$

Notice that for a set X in $\mathbb{R}^d$ one has $\tau(X^{n+1}) = (p_\tau(X))^{n+1}$ in $\mathbb{R}^{d(n+1)} = \mathbb{R}^D$. However it will be more convenient to write τ for p_τ, just as the σ in (3.1.7) is simply the σ in (3.1.9) with $n = 0$.

Now suppose $q = 0$. In this case the only units are roots of unity and we set $F = \mathbf{0}$. Here we may apply the counting principles of Chapter 1 to the set $S_F(T)$ directly without running into the difficulty of getting huge Lipschitz constants. In order to treat this rather easy case simultaneously with the more interesting case $q > 0$ it will be convenient to define the set of $\mathbf{i}$'s as the set $\{\mathbf{0}\}$ consisting only of the single vector $\mathbf{0} = (0)$ and we set $t = 1$. Then we define $S_{F(\mathbf{i})}(T) = S_{F(\mathbf{0})}(T) = S_F(T)$ and moreover $\tau_\mathbf{i} = \tau_\mathbf{0}$ is the identity automorphism. Hence an expression like $\bigcup_\mathbf{i} S_{F(\mathbf{i})}(T)$ is to be understood as $S_F(T)$. With these conventions (3.3.18), (3.3.20) and also (3.3.24), (3.3.25), (3.3.26), (3.3.27), (3.3.28) and (3.3.29) remain valid.

3.3. Estimates for the minima. We define the non-zero ideal $\mathfrak{C}_0$ by

$$\mathfrak{C}_0 = \prod_{v \nmid \infty} \mathfrak{p}_v^{-\frac{d_v \log c_v}{\log N\mathfrak{p}_v}} \tag{3.3.30}$$

with c_v as in (3.1.4). Thus $|\mathfrak{C}_0|_v = c_v$ and

$$N\mathfrak{C}_0 = (C_\mathcal{N}^{fin})^d. \tag{3.3.31}$$

Let $\mathfrak{D} \neq 0$ be a fractional ideal. Clearly $|\alpha|_v \leq |\mathfrak{C}_0^{-1}\mathfrak{D}|_v$ for all non-archimedean v is equivalent to $\alpha \in \mathfrak{C}_0^{-1}\mathfrak{D}$. By (3.1.3) we conclude

$$\Lambda_\mathcal{N}(\mathfrak{D}) \subseteq \sigma(\mathfrak{C}_0^{-1}\mathfrak{D})^{n+1}. \tag{3.3.32}$$

Since $\mathcal{N}$ is fixed we can omit the index and simply write $\Lambda(\mathfrak{D})$ for $\Lambda_\mathcal{N}(\mathfrak{D})$. Certainly $\tau\sigma(\mathfrak{C}_0^{-1}\mathfrak{D})$ is a lattice in $\mathbb{R}^d$. For each $\mathfrak{D}$ we choose linearly independent vectors

$$v_1 = \tau\sigma(\theta_1), ..., v_d = \tau\sigma(\theta_d)$$

of the lattice $\tau\sigma(\mathfrak{C}_0^{-1}\mathfrak{D})$ with

$$|v_i| = \lambda_i(\tau\sigma(\mathfrak{C}_0^{-1}\mathfrak{D})) \qquad (1 \leq i \leq d) \tag{3.3.33}$$

for the successive minima. Since $v_1, ..., v_d$ are $\mathbb{R}$-linearly independent, $\tau^{-1}v_1, ..., \tau^{-1}v_d$ are also $\mathbb{R}$-linearly independent. Hence $\theta_1, ..., \theta_d$ are $\mathbb{Q}$-linearly independent and therefore $\frac{\theta_1}{\theta_1}, ..., \frac{\theta_d}{\theta_1}$ are $\mathbb{Q}$-linearly independent. Now $[K : \mathbb{Q}] = d$ implies $K = \mathbb{Q}(\frac{\theta_1}{\theta_1}, ..., \frac{\theta_d}{\theta_1}) = k(\frac{\theta_1}{\theta_1}, ..., \frac{\theta_d}{\theta_1})$ and this allows the following definition.

DEFINITION 3.3. *Let $l \in \{1, ..., d\}$ be minimal with $K = k(\frac{\theta_1}{\theta_1}, ..., \frac{\theta_l}{\theta_1})$.*

In principle l depends on k, on the lattice $\tau\sigma(\mathfrak{C}_0^{-1}\mathfrak{D})$ and on the choice of $v_1, ..., v_d$. So it depends on k, on τ and on $\mathfrak{C}_0$, $\mathfrak{D}$. But $\tau = \tau(\mathbf{i})$ itself depends on $\mathbf{i}$ and on the basis U of the unit lattice. However k, $\mathfrak{C}_0$ and the choice of U are fixed and for every $\tau\sigma(\mathfrak{C}_0^{-1}\mathfrak{D})$ the choice of $v_1, ..., v_d$ is fixed also such that $l = l(\mathbf{i}, \mathfrak{D})$ depends only on the ideal $\mathfrak{D}$ and on the vector $\mathbf{i}$. Moreover we have the following statement which for $k = \mathbb{Q}$ is Lemma 2.1 of [**17**].

LEMMA 3.3. *We have*

$$l \leq [\frac{d}{2}] + 1.$$

Proof. Assume the statement is false then there exists a proper subfield K_0 of K containing the $[\frac{d}{2}]+1$ $\mathbb{Q}$-linear independent numbers $\frac{\theta_i}{\theta_1}$ for $1 \leq i \leq [\frac{d}{2}] + 1$. But $[K_0 : \mathbb{Q}] \leq d/2$ and so K_0 contains no more than $d/2$ $\mathbb{Q}$-linear independent numbers contradicting the fact $[\frac{d}{2}] + 1 > d/2$. □

We abbreviate

$$\lambda_i = \lambda_i(\tau\sigma(\mathfrak{C}_0^{-1}\mathfrak{D})) \tag{3.3.34}$$

for $1 \leq i \leq d$.

LEMMA 3.4. *Assume $a \in \{1, ..., d\}$ and $\mu_1, ..., \mu_a$ in $\mathbb{R}$ with $\mu_a \neq 0$ are such that $w = \mu_1 v_1 + ... + \mu_a v_a$ lies in $\tau\sigma(\mathfrak{C}_0^{-1}\mathfrak{D})$. Then we have*

$$|w| \geq \lambda_a.$$

Proof. For $a = 1$ it is clear. For $a > 1$ we apply Lemma 1.1 of Chapter 1 with $V = \mathbb{R}v_1 + ... + \mathbb{R}v_{a-1}$. □

LEMMA 3.5. *Assume $l \geq 2$, and let $\omega_0, ..., \omega_n$ in K be not all zero with $k(\omega_0 : ... : \omega_n) = K$. Then not all of the $\omega_0, ..., \omega_n$ are in $k\theta_1 + ... + k\theta_{l-1}$.*

Proof. Set $K_0 = k(\frac{\theta_1}{\theta_1}, ..., \frac{\theta_{l-1}}{\theta_1})$. By definition of l we have $K_0 \subsetneq K$. Let a, b be in $\{0, ..., n\}$ with $\omega_b \neq 0$. Suppose ω_a, ω_b are in $k\theta_1 + ... + k\theta_{l-1}$. Then there are α_j, β_j $(1 \leq j \leq l-1)$ in k such that

$$\frac{\omega_a}{\omega_b} = \frac{\sum_{j=1}^{l-1} \alpha_j \theta_j}{\sum_{j=1}^{l-1} \beta_j \theta_j} = \frac{\sum_{j=1}^{l-1} \alpha_j \frac{\theta_j}{\theta_1}}{\sum_{j=1}^{l-1} \beta_j \frac{\theta_j}{\theta_1}}.$$

But numerator and denominator of the last fraction are in K_0 and so $\frac{\omega_a}{\omega_b}$ is in K_0. So if all $\omega_0, ..., \omega_n$ are in $k\theta_1 + ... + k\theta_{l-1}$ then $k(\omega_0 : ... : \omega_n) \subseteq K_0$ - a contradiction. □

LEMMA 3.6. *Let $\omega_0, ..., \omega_n$ be in $\mathfrak{C}_0^{-1}\mathfrak{D}$ not all zero with $k(\omega_0 : ... : \omega_n) = K$. Then for $v = (\tau\sigma\omega_0, ..., \tau\sigma\omega_n)$ in $\mathbb{R}^D$ we have*

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

Proof. Each of the $\tau\sigma\omega_0$,..., $\tau\sigma\omega_n$ lies in the lattice $\tau\sigma(\mathfrak{C}_0^{-1}\mathfrak{D})$. The sublattice generated by $v_1, ..., v_d$ has finite index in $\tau\sigma(\mathfrak{C}_0^{-1}\mathfrak{D})$. Hence there are $\mu_j^{(i)} \in \mathbb{Q}$ such that

$$v = (\sum_{j=1}^{d} \mu_j^{(0)} v_j, ..., \sum_{j=1}^{d} \mu_j^{(n)} v_j).$$

Lemma 3.5 and the condition $K = k(\omega_0 : ... : \omega_n)$ imply at least one of the numbers $\mu_j^{(i)}$ for $l \leq j \leq d$, $0 \leq i \leq n$ is non-zero and so the result follows by Lemma 3.4. □

LEMMA 3.7. *If $l \geq 2$ then*

$$\frac{l-1}{m} \leq [k(\frac{\theta_1}{\theta_1}, ..., \frac{\theta_{l-1}}{\theta_1}) : k] \leq \max\{1, e/2\}. \tag{3.3.35}$$

Proof. The $l-1$ numbers $\frac{\theta_1}{\theta_1}, ..., \frac{\theta_{l-1}}{\theta_1}$ are $\mathbb{Q}$-linearly independent. Hence $[K_0 : \mathbb{Q}] \geq l-1$ for $K_0 = k(\frac{\theta_1}{\theta_1}, ..., \frac{\theta_{l-1}}{\theta_1})$. The first inequality follows at once, since $m = [k : \mathbb{Q}]$. But the second one follows immediately from the definition of l since $[K : k] = e$. □

LEMMA 3.8. *One has*

$$\lambda_1 \geq \sqrt{d/2}(C_{\mathcal{N}}^{fin})^{-1} N(\mathfrak{D})^{\frac{1}{d}}.$$

Moreover with $K_0 = k(\frac{\theta_1}{\theta_1}, ..., \frac{\theta_{l-1}}{\theta_1})$ if $l \geq 2$ and $K_0 = k$ if $l = 1$ and $g = [K_0 : k] \in G(K/k)$ one has

$$\lambda_l \geq \frac{1}{\sqrt{2}ed}(C_{\mathcal{N}}^{fin})^{-1} N(\mathfrak{D})^{\frac{1}{d}} \delta_g(K/k).$$

Proof. For the first statement observe that by definition

$$\tau\sigma\alpha = (\gamma_1\sigma_1\alpha, ..., \gamma_{q+1}\sigma_{q+1}\alpha).$$

So the squared length of an element $\tau\sigma\alpha$ of $\tau\sigma(\mathfrak{C}_0^{-1}\mathfrak{D})$ is

$$\sum_{i=1}^{q+1} |\gamma_i\sigma_i\alpha|^2 \geq \frac{1}{2} \sum_{i=1}^{q+1} d_i |\gamma_i\sigma_i\alpha|^2.$$

Next we use the AGM-inequality to deduce that this is at least

$$(d/2)\prod_{i=1}^{q+1}|\gamma_i\sigma_i\alpha|^{2d_i/d}.$$

By (3.3.21) we see that the latter is $(d/2)\prod_{i=1}^{q+1}|\sigma_i\alpha|^{2d_i/d}$. Here $\prod_{i=1}^{q+1}|\sigma_i\alpha|^{d_i}$ is the absolute value of the norm of α from K to $\mathbb{Q}$ which is at least $N\mathfrak{C}_0{}^{-1}\mathfrak{D}$ provided $\alpha\neq 0$. Recalling (3.3.31) we see that $N\mathfrak{C}_0{}^{-1}\mathfrak{D} = (C_{\mathcal{N}}^{fin})^{-d}N\mathfrak{D}$ which leads to the first statement.

Now let us prove the second estimate. First note that $l=1$ is equivalent to $K=k$. Thus $l=1$ implies $k=K$, $g=1$, $\delta_g(K/k)=1$ and so the claim follows from the first statement. Next suppose $l>1$. We apply Lemma 3.1 twice to obtain a primitive element $\beta=\sum_{i=1}^{l}m_i\frac{\theta_i}{\theta_1}$ for the extension K/k where m_i are in $\mathbb{Z}$ and $0\leq m_i<e$ $(1\leq i\leq l)$. And once more to get a primitive element $\alpha=\sum_{i=1}^{l-1}m_i'\frac{\theta_i}{\theta_1}$ for the extension $k(\frac{\theta_1}{\theta_1},...,\frac{\theta_{l-1}}{\theta_1})/k$ with $m_1',...,m_{l-1}'$ in $\mathbb{Z}$ and $0\leq m_i'<e$ $(1\leq i\leq l-1)$. So $k(\alpha,\beta)=K$ and $[k(\alpha):k]=g$. Using the product formula we get

$$\delta_g(K/k)^d\leq H(1,\alpha,\beta)^d=\prod_{v\nmid\infty}\max\{|\theta_1|_v,|\sum_{i=1}^{l-1}m_i'\theta_i|_v,|\sum_{i=1}^{l}m_i\theta_i|_v\}^{d_v}$$
$$\prod_{j=1}^{q+1}\max\{|\sigma_j\theta_1|,|\sigma_j(\sum_{i=1}^{l-1}m_i'\theta_i)|,|\sigma_j(\sum_{i=1}^{l}m_i\theta_i)|\}^{d_j}.$$

Because $\theta_1,...,\theta_l$ are in $\mathfrak{C}_0^{-1}\mathfrak{D}$ this is

$$\leq N(\mathfrak{C}_0^{-1}\mathfrak{D})^{-1}\prod_{j=1}^{q+1}(le)^{d_j}\max\{|\sigma_j\theta_1|,...,|\sigma_j\theta_l|\}^{d_j},$$

and since $\prod_{j=1}^{q+1}\gamma_j^{d_j}=1$ this in turn is

$$=(le)^dN(\mathfrak{C}_0^{-1}\mathfrak{D})^{-1}\prod_{j=1}^{q+1}\max\{\gamma_j|\sigma_j\theta_1|,...,\gamma_j|\sigma_j\theta_l|\}^{d_j}$$

$$=(le)^d(C_{\mathcal{N}}^{fin})^dN(\mathfrak{D})^{-1}\left(\prod_{j=1}^{q+1}\max\{\gamma_j|\sigma_j\theta_1|,...,\gamma_j|\sigma_j\theta_l|\}^{2d_j}\right)^{\frac{1}{2}}$$

$$=(le)^d(C_{\mathcal{N}}^{fin})^dN(\mathfrak{D})^{-1}\left(\prod_{j=1}^{q+1}|w_j|_\infty^{2d_j}\right)^{\frac{1}{2}}$$

where w_j is the vector $(\gamma_j\sigma_j\theta_1, ..., \gamma_j\sigma_j\theta_l)$ in $\mathbb{R}^{ld_j}$ and $|\cdot|_\infty$ denotes the max-norm. Now using the AGM-inequality and $|\cdot| \geq |\cdot|_\infty$ for the l^2-norm $|\cdot|$ we may estimate the above by

$$\leq (le)^d (C_{\mathcal{N}}^{fin})^d N(\mathfrak{D})^{-1} \left(\frac{1}{d} \sum_{j=1}^{q+1} d_j |w_j|^2 \right)^{\frac{d}{2}}$$

$$\leq (le)^d (2/d)^{d/2} (C_{\mathcal{N}}^{fin})^d N(\mathfrak{D})^{-1} \left(\sum_{j=1}^{q+1} |w_j|^2 \right)^{\frac{d}{2}}. \tag{3.3.36}$$

The vector $(\tau\sigma\theta_1, ..., \tau\sigma\theta_l)$ in $\mathbb{R}^{ld}$ has squared length exactly

$$\sum_{j=1}^{q+1} |(\gamma_j\sigma_j\theta_1, ..., \gamma_j\sigma_j\theta_l)|^2,$$

so that the right-hand side of (3.3.36) is

$$= (le)^d (2/d)^{d/2} (C_{\mathcal{N}}^{fin})^d N(\mathfrak{D})^{-1} |(\tau\sigma\theta_1, ..., \tau\sigma\theta_l)|^d. \tag{3.3.37}$$

Moreover by (3.3.33) one has

$$|(\tau\sigma\theta_1, ..., \tau\sigma\theta_l)| = (|v_1|^2 + ... + |v_l|^2)^{\frac{1}{2}} \leq \sqrt{l}\lambda_l. \tag{3.3.38}$$

Note that by definition $l \leq d$. Combining (3.3.37) and (3.3.38) yields the desired result. □

3.4. Counting. Recall the partition (3.3.20) of $S_F(T)$. In this subsection we concentrate on the component $S_{F(\mathbf{0})}(T)$. We will use the main result of Chapter 1 to estimate the number of points in $\tau\Lambda(\mathfrak{D}) \cap S_{F(\mathbf{0})}(T)$ satisfying a certain primitivity condition. Let $S_1 \subseteq \sigma K^{n+1}$ and $S_2 \subseteq \mathbb{R}^D$ be sets with $|S_1 \cap S_2|$ or $|\tau S_1 \cap S_2|$ finite. We use the following notation

$$Z^*(S_1, S_2) = |\{\sigma\omega \in S_1 \cap S_2; \omega \neq \mathbf{0}, k(\omega_0 : ... : \omega_n) = K\}| \tag{3.3.39}$$

$$Z_\tau^*(\tau S_1, S_2) = |\{\tau\sigma\omega \in \tau S_1 \cap S_2; \omega \neq \mathbf{0}, k(\omega_0 : ... : \omega_n) = K\}|. \tag{3.3.40}$$

We recall that τ and σ are injective. Hence (3.3.39) and (3.3.40) are well-defined and moreover

$$Z^*(S_1, S_2) = Z_\tau^*(\tau S_1, \tau S_2). \tag{3.3.41}$$

It might be worth to repeat (3.3.34) namely

$$\lambda_i = \lambda_i(\tau\sigma(\mathfrak{C}_0^{-1}\mathfrak{D}))$$

for $1 \leq i \leq d$.
Recall also definition (3.2.4)

$$\mu_g = m(e-g)(n+1) - 1.$$

Inclusion (3.3.28) tells us in particular $S_{F(\mathbf{0})}(T)$ is bounded. First suppose $q > 0$. We apply Lemma 3.2 not to F but to

$$F(\mathbf{0}) = [0,1)\frac{u_1}{n_1} + ... + [0,1)\frac{u_q}{n_q}.$$

Remember that by (3.3.16)

$$|\frac{u_j}{n_j}| = \frac{|u_j|}{[|u_j|]+1} < 1.$$

We refer to (3.3.15) and the observations just after to conclude that $\partial F(\mathbf{0})$ lies in $\mathrm{Lip}(q+1, 2, 2q, q-1)$. Furthermore it is clear that $F(\mathbf{0})$ lies in a ball of radius $r_{F(\mathbf{0})} = q$. Applying Lemma 3.2 gives that the boundary

$$\partial S_{F(\mathbf{0})}(1) \text{ lies in } \mathrm{Lip}(D, 1, \widetilde{M}, \widetilde{L}) \tag{3.3.42}$$

where

$$\widetilde{M} = (2q+1)M^{q+1} \ll M^d,$$
$$\widetilde{L} = 3\sqrt{D}(2q)\exp(\sqrt{q}(2q-1))(L + C_{\mathcal{N}}^{inf}) \ll L + C_{\mathcal{N}}^{inf}.$$

Now suppose $q = 0$. So we have $S_{F(\mathbf{0})}(1) = S_F(1)$. Recalling the observation just before Lemma 3.2 shows directly that (3.3.42) holds with $\widetilde{M} = M \leq M^d$ and $\widetilde{L} = L \leq L + C_{\mathcal{N}}^{inf}$.

By Theorem 1.2 we deduce that $S_{F(\mathbf{0})}(1)$ is measurable. Since by (3.3.26) $S_{F(\mathbf{0})}(T) = TS_{F(\mathbf{0})}(1)$ we conclude that the latter remains true for $S_{F(\mathbf{0})}(T)$. So the quantities $|\tau\Lambda(\mathfrak{D}) \cap S_{F(\mathbf{0})}(T)|$ and Vol $S_{F(\mathbf{0})}(T)$ are well-defined and finite.

Proposition 3.1. *With $A = A_{\mathcal{N}}$ as in Theorem 3.1, $T > 0$ and $g = [K_0 : k]$ as in Lemma 3.8 we have*

$$|Z_\tau^*(\tau\Lambda(\mathfrak{D}), S_{F(\mathbf{0})}(T)) - \frac{\text{Vol } S_{F(\mathbf{0})}(T)}{\det \tau\Lambda(\mathfrak{D})}| \ll \frac{AT^{d(n+1)-1}}{N\mathfrak{D}^{n+1-1/d}\delta_g(K/k)^{\mu_g}}.$$

Proof. Recall that $A = M^d(C(L+1))^{d(n+1)-1}$. We have

$$\mu_g = (d-mg)(n+1) - 1 \leq (d-l+1)(n+1) - 1$$

by Lemma 3.7 provided $l \geq 2$. But if $l = 1$ then $K = k$ and thus $G(K/k) = \{1\}$ so $g = 1$. Hence for $l = 1$ the inequality remains valid.

Thanks to Lemma 3.8 and (3.1.6) relating $C = C_{\mathcal{N}}$ and $C_{\mathcal{N}}^{inf}$ it is enough to verify the claim

$$|Z_\tau^*(\tau\Lambda(\mathfrak{D}), S_{F(\mathbf{0})}(T)) - \frac{\text{Vol } S_{F(\mathbf{0})}(T)}{\det \tau\Lambda(\mathfrak{D})}| \ll M^d \frac{(C_{\mathcal{N}}^{inf}(L+1)T)^{d(n+1)-1}}{\lambda_1^{(l-1)(n+1)}\lambda_l^{(d-l+1)(n+1)-1}}.$$

Remember also inclusion (3.3.28) telling us

$$S_{F(\mathbf{0})}(T) \subseteq B_0(\kappa T) \tag{3.3.43}$$

where $\kappa = \sqrt{d(n+1)}C_{\mathcal{N}}^{inf}\exp\{q\}$.

We consider two cases.

(1) $T < \kappa^{-1}\lambda_l$.

Now (3.3.43) shows that $|v| < \lambda_l$ for each v in $S_{F(\mathbf{0})}(T)$. From (3.3.32) we get $\tau\Lambda(\mathfrak{D}) \subseteq \tau(\sigma(\mathfrak{C}_0^{-1}\mathfrak{D})^{n+1})$ and so Lemma 3.6 implies

$$Z_\tau^*(\tau\Lambda(\mathfrak{D}), S_{F(\mathbf{0})}(T)) = 0.$$

On the other hand

$$\frac{\text{Vol } S_{F(\mathbf{0})}(T)}{\det \tau\Lambda(\mathfrak{D})} \leq \frac{\text{Vol } B_0(\kappa T)}{\det \tau(\sigma(\mathfrak{C}_0^{-1}\mathfrak{D})^{n+1})}.$$

Since $\det(\Lambda_0^{n+1}) = (\det \Lambda_0)^{n+1}$ for any lattice Λ_0 in $\mathbb{R}^d$ the latter is

$$= \frac{\text{Vol } B_0(\kappa T)}{\det(\tau\sigma(\mathfrak{C}_0^{-1}\mathfrak{D}))^{n+1}}.$$

Because of Vol $B_0(R) \ll R^{d(n+1)}$, Minkowski's Second Theorem and (1) this in turn is

$$\ll \frac{(\kappa T)^{d(n+1)}}{\det(\tau\sigma(\mathfrak{C}_0^{-1}\mathfrak{D}))^{n+1}} \ll \frac{(\kappa T)^{d(n+1)}}{(\lambda_1 \ldots \lambda_d)^{n+1}}$$
$$\ll \frac{\lambda_l(\kappa T)^{d(n+1)-1}}{(\lambda_1 \ldots \lambda_d)^{n+1}} \qquad \ll \frac{(C_{\mathcal{N}}^{inf}T)^{d(n+1)-1}}{\lambda_1^{(l-1)(n+1)}\lambda_l^{(d-l+1)(n+1)-1}}.$$

This implies the claim in case (1) because $M \geq 1$.

(2) $T \geq \kappa^{-1}\lambda_l$.

Thus for $1 \leq i \leq l$ one has

$$C_{\mathcal{N}}^{inf}\frac{T}{\lambda_i} \gg 1. \tag{3.3.44}$$

Set

$$S = \tau\Lambda(\mathfrak{D}) \cap S_{F(\mathbf{0})}(T).$$

Notice that by definition (3.3.2) $\mathbf{0}$ is not in $S_{F(\mathbf{0})}(T)$ for all $T > 0$. Thus we can define

$$S' = \{v \in S; v = (\tau\sigma\omega_0, ..., \tau\sigma\omega_n), k(\omega_0 : ... : \omega_n) \subsetneq K\}.$$

Clearly

$$Z^*_\tau(\tau\Lambda(\mathfrak{D}), S_{F(\mathbf{0})}(T)) = |S| - |S'|.$$

Let us estimate $|S|$ first. Due to (3.3.42) we know that $\partial S_{F(\mathbf{0})}(1)$ lies in $\mathrm{Lip}(D, 1, \widetilde{M}, \widetilde{L})$ where $\widetilde{M} \ll M^d$ and $\widetilde{L} \ll L + C_{\mathcal{N}}^{inf}$. By (3.3.26) we see that $\partial S_{F(\mathbf{0})}(T)$ is in $\mathrm{Lip}(D, 1, \widetilde{M}, \widetilde{L}T)$. Next we apply Theorem 1.2 of Chapter 1 to deduce

$$\begin{aligned} ||S| - \frac{\mathrm{Vol}\ S_{F(\mathbf{0})}(T)}{\det \tau\Lambda(\mathfrak{D})}| &\ll \widetilde{M} \max_{0\le j\le d(n+1)-1} \frac{(\widetilde{L}T)^j}{\lambda_1(\tau\Lambda(\mathfrak{D}))...\lambda_j(\tau\Lambda(\mathfrak{D}))} \\ &\ll M^d \max_{0\le j\le d(n+1)-1} \frac{((L + C_{\mathcal{N}}^{inf})T)^j}{\lambda_1(\tau\Lambda(\mathfrak{D}))...\lambda_j(\tau\Lambda(\mathfrak{D}))}. \end{aligned} \tag{3.3.45}$$

From (3.3.32) we get

$$\lambda_j(\tau\Lambda(\mathfrak{D})) \ge \lambda_j((\tau\sigma(\mathfrak{C}_0^{-1}\mathfrak{D}))^{n+1}) \tag{3.3.46}$$

for $1 \le j \le d(n+1)$. We abbreviate the right-hand side of (3.3.46) to ν_j. Inserting this estimate in (3.3.45) and then using $C_{\mathcal{N}}^{inf} \ge 1$ in the form $L + C_{\mathcal{N}}^{inf} \le (L+1)C_{\mathcal{N}}^{inf}$ yields the bound

$$\ll M^d(L+1)^{d(n+1)-1} \max_{0\le j\le d(n+1)-1} \frac{(C_{\mathcal{N}}^{inf}T)^j}{\nu_1...\nu_j}. \tag{3.3.47}$$

Consider the expressions

$$E_j = \frac{(C_{\mathcal{N}}^{inf}T)^j}{\nu_1...\nu_j} \tag{3.3.48}$$

in (3.3.47). From Lemma 1.2 we see that $\nu_1, ..., \nu_D$ are

$$\lambda_1, ..., \lambda_1, \lambda_2, ..., \lambda_2, ..., \lambda_d, ..., \lambda_d$$

in blocks of $n+1$. Thus for $j \le (l-1)(n+1)$ we have $\nu_j \le \lambda_l$. So in this case

$$E_j = E_{j-1}\frac{C_{\mathcal{N}}^{inf}T}{\nu_j} \gg E_{j-1}. \tag{3.3.49}$$

Therefore the maximum over these j in (3.3.48) is

$$\ll E_{(l-1)(n+1)} = \frac{(C_{\mathcal{N}}^{inf}T)^{(l-1)(n+1)}}{(\lambda_1...\lambda_{l-1})^{n+1}} \leq \frac{(C_{\mathcal{N}}^{inf}T)^{(l-1)(n+1)}}{\lambda_1^{(l-1)(n+1)}}. \tag{3.3.50}$$

For the other $j > (l-1)(n+1)$ we get $\nu_j \geq \lambda_l$ so

$$E_j \leq E_{j-1}\frac{C_{\mathcal{N}}^{inf}T}{\lambda_l} \tag{3.3.51}$$

which contribute an extra

$$\left(\frac{C_{\mathcal{N}}^{inf}T}{\lambda_l}\right)^{d(n+1)-1-(l-1)(n+1)}$$

to the maximum in (3.3.50). This yields the bound

$$\ll M^d(C_{\mathcal{N}}^{inf}(L+1))^{d(n+1)-1}\frac{T^{d(n+1)-1}}{\lambda_1^{(l-1)(n+1)}\lambda_l^{(d-l+1)(n+1)-1}} \tag{3.3.52}$$

for (3.3.47).

Next we shall obtain an upper bound for $|S'|$. For $(\tau\sigma\omega_0, ..., \tau\sigma\omega_n)$ in S' the field $K_1 = k(\omega_0 : ... : \omega_n)$ satisfies $K_1 \subsetneq K$. 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 $(\tau\sigma\omega_0, ..., \tau\sigma\omega_n) \neq \mathbf{0}$ hence at least one of the numbers $\omega_0, ..., \omega_n$ is non-zero. By symmetry we lose only a factor $n+1$ if we assume $\omega_0 \neq 0$. So let us temporarily regard $\omega_0 \neq 0$ as fixed; then every ω_j for $1 \leq j \leq n$ satisfies

$$\sigma_a\frac{\omega_j}{\omega_0} = \sigma_b\frac{\omega_j}{\omega_0}.$$

Let z_0, z_1 be in $\mathbb{R}$ with $z_0 + iz_1 = \frac{\sigma_a\omega_0}{\sigma_b\omega_0}$. Then we get

$$\Re\sigma_a\omega_j = z_0\Re\sigma_b\omega_j - z_1\Im\sigma_b\omega_j,$$
$$\Im\sigma_a\omega_j = z_1\Re\sigma_b\omega_j + z_0\Im\sigma_b\omega_j,$$

where we used $\Re$ for the real and $\Im$ for the imaginary part of a complex number. This shows that all $\sigma\omega_j$ for $1 \leq j \leq n$ lie in a hyperplane $\mathcal{P}(\omega_0)$ of $\mathbb{R}^d$ and therefore all $\tau\sigma\omega_j$ lie in the hyperplane $\tau\mathcal{P}(\omega_0)$. The inclusion (3.3.43) implies $|\tau\sigma\omega_j| \leq \kappa T$. 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 $r' \leq r$. It is easy to see that it belongs to the class $\mathrm{Lip}(d, 1, 1, 2\sqrt{d-1}r)$ (for example using (3.3.3) with $q = d-1$ and $r_F = \sqrt{d-1}r'$ if the center

is at the origin). Moreover it has volume zero. Hence by Theorem 1.2 and (3.3.44) we obtain the upper bound

$$\ll \max_{0\leq i<d} \frac{(\kappa T)^i}{\lambda_1 ... \lambda_i} \ll \frac{(C_{\mathcal{N}}^{inf} T)^{d-1}}{\lambda_1^{l-1}\lambda_l^{d-l}}$$

for the number of $\tau\sigma\omega_j$ with $1 \leq j \leq n$.

Next we have to estimate the number of $\tau\sigma\omega_0$. By inclusion (3.3.43) we see once more that $|\tau\sigma\omega_0| \leq \kappa T$. Now by virtue of Theorem 1.2 we deduce the following upper bound

$$\ll \frac{\text{Vol } B_0(\kappa T)}{\det \tau\sigma(\mathfrak{C}_0^{-1}\mathfrak{D})} + \max_{0\leq i<d} \frac{(\kappa T)^i}{\lambda_1 ... \lambda_i}$$

for the number of $\tau\sigma\omega_0$. Going right up to the last minimum, we see that this is bounded by

$$\ll \max_{0\leq i\leq d} \frac{(\kappa T)^i}{\lambda_1 ... \lambda_i}$$

and taking (3.3.44) into account yields the upper bound

$$\ll \frac{(C_{\mathcal{N}}^{inf} T)^d}{\lambda_1^{l-1}\lambda_l^{d-l+1}}.$$

Multiplying the bounds for the number of $\tau\sigma\omega_0$ and $\tau\sigma\omega_j$ leads to

$$|S'| \ll \frac{(C_{\mathcal{N}}^{inf} T)^d}{\lambda_1^{l-1}\lambda_l^{d-l+1}} \left(\frac{(C_{\mathcal{N}}^{inf} T)^{d-1}}{\lambda_1^{l-1}\lambda_l^{d-l}} \right)^n = \frac{(C_{\mathcal{N}}^{inf} T)^{d(n+1)-n}}{\lambda_1^{(l-1)(n+1)}\lambda_l^{(d-l+1)(n+1)-n}}.$$

We appeal once more to (3.3.44) with $i = l$ to see that the latter is

$$\ll \frac{(C_{\mathcal{N}}^{inf} T)^{d(n+1)-1}}{\lambda_1^{(l-1)(n+1)}\lambda_l^{(d-l+1)(n+1)-1}}.$$

Combining the estimates for $|S|$ and $|S'|$ proves the claim in case (2).□

3.5. End of the proof. Let $\Lambda^*(\mathfrak{A})$ be the subset of $\Lambda(\mathfrak{A})$ defined by

$$\Lambda^*(\mathfrak{A}) = \{\sigma(\boldsymbol{\alpha}); \boldsymbol{\alpha} \in K^{n+1}, N_v(\sigma_v\boldsymbol{\alpha}) = |\mathfrak{A}|_v \text{ for all finite } v\}.$$

As in Subsection 3.4 the star * indicates some primitivity condition. However the property defining the set above has nothing to do with the one in Subsection 3.4.

LEMMA 3.9. *For $X > 0$ we have*

$$Z_{\mathcal{N}}(\mathbb{P}^n(K/k), X) = w_K^{-1} \sum_{\mathfrak{A} \in R} Z^*(\Lambda^*(\mathfrak{A}), S_F(N\mathfrak{A}^{\frac{1}{d}} X))$$

where the sum runs over any system R of class representatives of K.

Proof. Let $P \in \mathbb{P}^n(K)$ with homogeneous coordinates $(\alpha_0, ..., \alpha_n) = \boldsymbol{\alpha} \in K^{n+1} \backslash \{\mathbf{0}\}$. Thanks to the uniqueness of the prime factorization for non-zero fractional ideals together with property $N_v(\sigma_v K^{n+1}) \subseteq \Gamma_v$ we may conclude that there is exactly one ideal $\mathfrak{A} = \mathfrak{A}_{\boldsymbol{\alpha}}$ such that

$$N_v(\sigma_v \boldsymbol{\alpha}) = |\mathfrak{A}|_v \tag{3.3.53}$$

for all finite v. Suppose $\varepsilon \in K^*$ then we have

$$N_v(\sigma_v \varepsilon \boldsymbol{\alpha}) = |\sigma_v \varepsilon|_v N_v(\sigma_v \boldsymbol{\alpha})$$

for all finite v. Hence $\mathfrak{A}_{\varepsilon \boldsymbol{\alpha}} = \varepsilon \mathfrak{A}_{\boldsymbol{\alpha}}$; in other words the ideal class of $\mathfrak{A}_{\boldsymbol{\alpha}}$ is independent of the coordinates $\boldsymbol{\alpha}$ we have chosen. In particular we can choose $\boldsymbol{\alpha}$ such that $\mathfrak{A}_{\boldsymbol{\alpha}}$ lies in R and so $\boldsymbol{\alpha}$ is unique up to units η. The set $F(\infty) = F + \mathbb{R}\delta$ is a fundamental set of $\mathbb{R}^{q+1}$ under the action of the additive subgroup $l(\mathbb{U})$. Because of (ii) of Subsection 1.2 we have

$$\log N_i(\sigma_i(\eta \boldsymbol{\alpha}))^{d_i} = \log N_i(\sigma_i \boldsymbol{\alpha})^{d_i} + d_i \log |\sigma_i \eta|$$

for $1 \leq i \leq q+1$. And so there exist exactly w_K representatives $\boldsymbol{\alpha}$ of P with

$$(d_1 \log N_1(\sigma_1 \boldsymbol{\alpha}), ..., d_{q+1} \log N_{q+1}(\sigma_{q+1} \boldsymbol{\alpha})) \in F(\infty).$$

But the above is equivalent with

$$(N_1(\sigma_1 \boldsymbol{\alpha})^{d_1}, ..., N_{q+1}(\sigma_{q+1} \boldsymbol{\alpha})^{d_{q+1}}) \in \exp F(\infty).$$

Furthermore

$$\exp F(T_0) = \{(X_1, ..., X_{q+1}) \in \exp F(\infty); X_1 ... X_{q+1} \leq T_0^d\}.$$

By definition (see Subsection 1.4) $H_{\mathcal{N}}^{inf}(\boldsymbol{\alpha}), H_{\mathcal{N}}^{fin}(\boldsymbol{\alpha})$ are invariant under substitution of $\boldsymbol{\alpha}$ by $\omega \boldsymbol{\alpha}$ where ω denotes a root of unity in K. Hence for all w_K possible choices $\boldsymbol{\alpha}$ of P the inequality

$$H_{\mathcal{N}}^{inf}(\boldsymbol{\alpha}) \leq T_0$$

is equivalent to

$$\sigma \boldsymbol{\alpha} \in S_F(T_0).$$

On the other hand

$$H_{\mathcal{N}}(P) = H_{\mathcal{N}}^{inf}(\boldsymbol{\alpha}) H_{\mathcal{N}}^{fin}(\boldsymbol{\alpha})$$

and by (3.3.53)

$$H_{\mathcal{N}}^{fin}(\boldsymbol{\alpha})^d = \prod_{v\nmid\infty} |\mathfrak{A}|_v^{d_v} = N\mathfrak{A}^{-1},$$

which completes the proof. □

Let Cl be the set of ideal classes and for (non-zero) ideals $\mathfrak{A}$, $\mathfrak{B}$, $\mathfrak{C}$ denote by $\mathcal{A}$, $\mathcal{B}$, $\mathcal{C}$ the ideal classes of $\mathfrak{A}$, $\mathfrak{B}$ and $\mathfrak{C}$. Recall from (3.1.11) that the function $\Delta_{\mathcal{N}}(\cdot)$ is well-defined on Cl.

Lemma 3.10. *We have*

$$\sum_{\mathfrak{A}\in R}\sum_{\mathfrak{B}} \frac{\mu(\mathfrak{B})}{N\mathfrak{B}^{n+1}}\Delta_{\mathcal{N}}(\mathcal{AB})^{-1} = \frac{1}{\zeta_K(n+1)}\sum_{\mathcal{D}\in Cl}\Delta_{\mathcal{N}}(\mathcal{D})^{-1} \tag{3.3.54}$$

where the inner sum on the left-hand side runs over all non-zero ideals $\mathfrak{B}$ in $\mathcal{O}_K$.

Proof. We have

$$\begin{aligned}
\sum_{\mathfrak{A}}\sum_{\mathfrak{B}} \frac{\mu(\mathfrak{B})}{N\mathfrak{B}^{n+1}}\Delta_{\mathcal{N}}(\mathcal{AB})^{-1} &= \sum_{\mathcal{A}\in Cl}\sum_{\mathfrak{B}} \frac{\mu(\mathfrak{B})}{N\mathfrak{B}^{n+1}}\Delta_{\mathcal{N}}(\mathcal{AB})^{-1} \\
&= \sum_{\mathcal{A}\in Cl}\sum_{\mathcal{C}\in Cl}\Delta_{\mathcal{N}}(\mathcal{AC})^{-1}\sum_{\mathfrak{B}\in\mathcal{C}}\frac{\mu(\mathfrak{B})}{N\mathfrak{B}^{n+1}} \\
&= \sum_{\mathcal{A}\in Cl}\sum_{\mathcal{D}\in Cl}\Delta_{\mathcal{N}}(\mathcal{D})^{-1}\sum_{\mathfrak{B}\in\mathcal{D}/\mathcal{A}}\frac{\mu(\mathfrak{B})}{N\mathfrak{B}^{n+1}} \\
&= \sum_{\mathcal{D}\in Cl}\Delta_{\mathcal{N}}(\mathcal{D})^{-1}\sum_{\mathcal{A}\in Cl}\sum_{\mathfrak{B}\in\mathcal{D}/\mathcal{A}}\frac{\mu(\mathfrak{B})}{N\mathfrak{B}^{n+1}} \\
&= \sum_{\mathcal{D}\in Cl}\Delta_{\mathcal{N}}(\mathcal{D})^{-1}\sum_{\mathfrak{B}}\frac{\mu(\mathfrak{B})}{N\mathfrak{B}^{n+1}}
\end{aligned}$$

again over all non-zero ideals $\mathfrak{B}$ in $\mathcal{O}_K$. Now we just have to remember the fact that $\sum_{\mathfrak{B}}\frac{\mu(\mathfrak{B})}{N\mathfrak{B}^s} = \zeta_K(s)^{-1}$ for $s > 1$ (so in particular for $s = n+1$) and the result drops out. □

The image of $\sigma_v(K^{n+1}\backslash\{\mathbf{0}\})$ under the map N_v lies in Γ_v^* and for all non-zero $\boldsymbol{\alpha}$ in K^{n+1} there are only finitely many v with $N_v(\sigma_v\boldsymbol{\alpha}) \neq 1$. So assume $\boldsymbol{\alpha}$ is in $K^{n+1}\backslash\{\mathbf{0}\}$; then $N_v(\sigma_v\boldsymbol{\alpha}) \leq |\mathfrak{A}|_v$ for all $v \nmid \infty$ is equivalent with the existence of a unique $\mathfrak{B} = \mathfrak{B}(\boldsymbol{\alpha}) \subseteq \mathcal{O}_K$, $\mathfrak{B} \neq 0$ such that $N_v(\sigma_v\boldsymbol{\alpha}) = |\mathfrak{AB}|_v$ for all $v \nmid \infty$. Hence from (3.1.10) we have the following disjoint union

$$\Lambda(\mathfrak{A}) = \bigcup_{\mathfrak{B}} \Lambda^*(\mathfrak{AB})$$

and therefore

$$Z^*(\Lambda(\mathfrak{A}), S_F(T)) = \sum_{\mathfrak{B}} Z^*(\Lambda^*(\mathfrak{AB}), S_F(T))$$

for any $T > 0$. Using the Möbius function μ_K of K we get by inversion

$$Z^*(\Lambda^*(\mathfrak{A}), S_F(T)) = \sum_{\mathfrak{B}} \mu_K(\mathfrak{B}) Z^*(\Lambda(\mathfrak{AB}), S_F(T)). \tag{3.3.55}$$

Applying (3.3.20) we find

$$Z^*(\Lambda(\mathfrak{AB}), S_F(T)) = \sum_{\mathbf{i}} Z^*(\Lambda(\mathfrak{AB}), S_{F(\mathbf{i})}(T))$$

where $\mathbf{i}$ is taken over the same set as in (3.3.20). Refering to (3.3.41) we see that the latter is

$$= \sum_{\mathbf{i}} Z^*_{\tau_{\mathbf{i}}}(\tau_{\mathbf{i}}\Lambda(\mathfrak{AB}), \tau_{\mathbf{i}} S_{F(\mathbf{i})}(T))$$

and by (3.3.24) this in turn is

$$= \sum_{\mathbf{i}} Z^*_{\tau_{\mathbf{i}}}(\tau_{\mathbf{i}}\Lambda(\mathfrak{AB}), S_{F(\mathbf{0})}(T)).$$

Thus

$$Z^*(\Lambda(\mathfrak{AB}), S_F(T)) = \sum_{\mathbf{i}} Z^*_{\tau_{\mathbf{i}}}(\tau_{\mathbf{i}}\Lambda(\mathfrak{AB}), S_{F(\mathbf{0})}(T)) \tag{3.3.56}$$

and again $\mathbf{i}$ is taken over the same set as in (3.3.20). Next we apply Proposition 3.1 with $\mathfrak{D} = \mathfrak{AB}$. To emphasize the dependence on $\mathbf{i}$ and $\mathfrak{AB}$ we can think of $g = g(\mathbf{i}, \mathfrak{AB})$. We get

$$Z^*_{\tau_{\mathbf{i}}}(\tau_{\mathbf{i}}\Lambda(\mathfrak{AB}), S_{F(\mathbf{0})}(T)) = \frac{\text{Vol } S_{F(\mathbf{0})}(T)}{\det \tau_{\mathbf{i}}\Lambda(\mathfrak{AB})} + O\left(\frac{AT^{d(n+1)-1}}{(N\mathfrak{AB})^{n+1-1/d}\delta_g(K/k)^{\mu_g}}\right).$$

By (3.3.23) we have $\det \tau_{\mathbf{i}}\Lambda(\mathfrak{AB}) = \det \Lambda(\mathfrak{AB})$ and taking also into account (3.3.24) and (3.3.20) gives

$$\sum_{\mathbf{i}} \text{Vol } S_{F(\mathbf{0})}(T) = \sum_{\mathbf{i}} \text{Vol } \tau_{\mathbf{i}} S_{F(\mathbf{i})}(T) = \sum_{\mathbf{i}} \text{Vol } S_{F(\mathbf{i})}(T) = \text{Vol } S_F(T).$$

Refering back to (3.3.56) we conclude

$$Z^*(\Lambda(\mathfrak{AB}), S_F(T)) = \sum_{\mathbf{i}} Z^*_{\tau_{\mathbf{i}}}(\tau_{\mathbf{i}}\Lambda(\mathfrak{AB}), S_{F(\mathbf{0})}(T))$$

$$= \frac{\text{Vol } S_F(T)}{\det \Lambda(\mathfrak{AB})} + O\left(\frac{AT^{d(n+1)-1}}{(N\mathfrak{AB})^{n+1-1/d}} \sum_{\mathbf{i}} \delta_g(K/k)^{-\mu_g}\right). \tag{3.3.57}$$

Let us focus on the error term. Recall that $g = g(\mathbf{i}, \mathfrak{AB}) = [K_0 : k] \in G = G(K/k)$ where $K_0 = k(\theta_1/\theta_1, ..., \theta_{l-1}/\theta_1)$ if $l \geq 2$ and $K_0 = k$ if

$l = 1$. Thus the $\sum_{\mathbf{i}}$ above can be replaced by $t\sum_{g\in G}$ with $t = \sum_{\mathbf{i}} 1$. By (3.3.18) we have

$$t \ll R_K$$

and (3.3.25) says

$$S_F(T) = TS_F(1).$$

Thus by (3.3.55) we get

(3.3.58)

$$Z^*(\Lambda^*(\mathfrak{A}), S_F(T)) = \sum_{\mathfrak{B}} \mu_K(\mathfrak{B}) \frac{\text{Vol } S_F(1) T^{d(n+1)}}{\det \Lambda(\mathfrak{A}\mathfrak{B})} + O\left(\sum_{\mathfrak{B}} \frac{AR_K T^{d(n+1)-1}}{(N\mathfrak{A}\mathfrak{B})^{n+1-1/d}} \sum_{g\in G} \delta_g (K/k)^{-\mu_g} \right).$$

According to Lemma 3.9 we set

$$T = T(\mathfrak{A}) = N\mathfrak{A}^{\frac{1}{d}} X.$$

By (3.1.12) we see that

$$\det \Lambda(\mathfrak{A}\mathfrak{B}) = \Delta_{\mathcal{N}}(\mathcal{A}\mathcal{B})(N\mathfrak{A}\mathfrak{B})^{n+1}$$

for the corresponding ideal classes $\mathcal{A}, \mathcal{B}$. Therefore (3.3.58) is equal

$$\sum_{\mathfrak{B}} \frac{\mu_K(\mathfrak{B})}{N\mathfrak{B}^{n+1}} \Delta_{\mathcal{N}}(\mathcal{A}\mathcal{B})^{-1} \text{Vol } S_F(1) X^{d(n+1)} + O\left(\sum_{\mathfrak{B}} \frac{AR_K X^{d(n+1)-1}}{N\mathfrak{B}^{n+1-1/d}} \sum_{g\in G} \delta_g (K/k)^{-\mu_g} \right).$$

Lemma 3.9 tells us that this quantity has to be summed over a set R of ideal class representatives $\mathfrak{A}$ and divided by the number w_K of roots of unity. Applying Lemma 3.10 yields

$$Z_{\mathcal{N}}(\mathbb{P}^n(K/k), X) = \frac{1}{\zeta_K(n+1) w_K} \sum_{\mathcal{D}\in Cl} \Delta_{\mathcal{N}}(\mathcal{D})^{-1} \text{Vol } S_F(1) X^{d(n+1)} + O\left(\sum_{\mathfrak{B}} \frac{Ah_K R_K X^{d(n+1)-1}}{N\mathfrak{B}^{n+1-1/d}} \sum_{g\in G} \delta_g (K/k)^{-\mu_g} \right).$$

By (3.1.13) we have

$$\sum_{\mathcal{D}\in Cl} \Delta_{\mathcal{N}}(\mathcal{D})^{-1} = 2^{s_K(n+1)} h_K V_{\mathcal{N}}^{fin} |\Delta_K|^{-\frac{n+1}{2}}.$$

The volume of $S_F(1)$ has been computed by Masser and Vaaler in [**34**] Lemma 4

$$\text{Vol } S_F(1) = (n+1)^q R_K V_{\mathcal{N}}^{inf}.$$

On recalling that $V_{\mathcal{N}} = V_{\mathcal{N}}^{fin} V_{\mathcal{N}}^{inf}$ we end up with

$$\begin{aligned}&\frac{1}{\zeta_K(n+1)w_K} 2^{s_K(n+1)} h_K V_{\mathcal{N}}^{fin} |\Delta_K|^{-\frac{n+1}{2}} (n+1)^q R_K V_{\mathcal{N}}^{inf} X^{d(n+1)} \\ =&S_K(n) 2^{-r_K(n+1)} \pi^{-s_K(n+1)} V_{\mathcal{N}} X^{d(n+1)}\end{aligned}$$

for the main term - exactly the main term of the theorem.

To deal with the error term we assume first $(n,d) \neq (1,1)$. It is well-known that $\zeta_K(x) \leq \zeta_{\mathbb{Q}}(x)^d$ for $x > 1$ (see Lang [**23**] p.322). Thus we have

$$\sum_{\mathfrak{B}} N\mathfrak{B}^{-(n+1-1/d)} \ll 1$$

and so we are done. Next assume $(n,d) = (1,1)$ so $k = K = \mathbb{Q}$, $q = 0$ and therefore $S_{F(\mathbf{0})}(T) = S_F(T)$. By (3.3.28) we have $S_F(T) \subseteq B_0(\kappa T)$ and here $\kappa = \sqrt{2} C_{\mathcal{N}}^{inf}$. From Lemma 3.8 we get $\lambda_1 \geq (1/\sqrt{2})(C_{\mathcal{N}}^{fin})^{-1} N\mathfrak{D}$. It follows without difficulty that $B_0(\kappa T)$ contains no point of the lattice $(\sigma \mathfrak{C}_0^{-1}\mathfrak{D})^2$ except the origin provided $T < (1/2) C_{\mathcal{N}}^{-1} N\mathfrak{D}$. But the origin does not lie in $S_F(T)$ and on recalling the inclusion (3.3.32) we deduce $S_F(T) \cap \Lambda_{\mathcal{N}}(\mathfrak{D})$ is empty for $T < (1/2) C_{\mathcal{N}}^{-1} N\mathfrak{D}$. Hence we may restrict the sum over $\mathfrak{B}$ in (3.3.55) to $N\mathfrak{B} \leq 2C_{\mathcal{N}} T N\mathfrak{A}^{-1}$. Thus by (3.3.55)

$$Z^*(\Lambda^*(\mathfrak{A}), S_F(T)) = \sum_{\substack{\mathfrak{B} \\ N\mathfrak{B} \leq 2C_{\mathcal{N}} T N\mathfrak{A}^{-1}}} \mu_K(\mathfrak{B}) Z^*(\Lambda(\mathfrak{A}\mathfrak{B}), S_F(T))$$

and by (3.3.58) we get for the latter

$$\sum_{\substack{\mathfrak{B} \\ N\mathfrak{B} \leq 2C_{\mathcal{N}} T N\mathfrak{A}^{-1}}} \mu_K(\mathfrak{B}) \frac{\text{Vol } S_F(1) T^2}{\det \Lambda(\mathfrak{A}\mathfrak{B})} + O\left(\sum_{\substack{\mathfrak{B} \\ N\mathfrak{B} \leq 2C_{\mathcal{N}} T N\mathfrak{A}^{-1}}} \frac{A R_K T}{N\mathfrak{A}\mathfrak{B}} \sum_{g \in G} \delta_g (K/k)^{-\mu_g} \right).$$

Here $G = \{1\}$ and $\delta_g = 1$. Now in order to get the main term as in the case $(n,d) \neq (1,1)$ we let the sum run over all $\mathfrak{B}$'s in $\mathcal{O}_K$ and correct

by an additional error term

$$\sum_{\mathfrak{B}} \mu_K(\mathfrak{B}) \frac{\text{Vol } S_F(1)T^2}{\det \Lambda(\mathfrak{AB})} + O\left(\sum_{\substack{\mathfrak{B} \\ N\mathfrak{B} > 2C_{\mathcal{N}} T N\mathfrak{A}^{-1}}} \frac{\text{Vol } S_F(1)T^2}{\det \Lambda(\mathfrak{AB})} \right) + O\left(\sum_{\substack{\mathfrak{B} \\ N\mathfrak{B} \leq 2C_{\mathcal{N}} T N\mathfrak{A}^{-1}}} \frac{AR_K T}{N\mathfrak{AB}} \right).$$

We set $T = XN\mathfrak{A}$ and by Lemma 3.9 we see that this quantity has to be summed over a set R of ideal class representatives $\mathfrak{A}$ and divided by the number w_K of roots of unity. But here $K = \mathbb{Q}$ so R consists just of a single class, $w_K = 2$ and $R_K = 1$. Thus

$$Z_{\mathcal{N}}(\mathbb{P}^n(K/k), X) = 2^{-1} \sum_{\mathfrak{B}} \mu_K(\mathfrak{B}) \frac{\text{Vol } S_F(1)(XN\mathfrak{A})^2}{\det \Lambda(\mathfrak{AB})} + O\left(\sum_{\substack{\mathfrak{B} \\ N\mathfrak{B} > 2C_{\mathcal{N}} X}} \frac{\text{Vol } S_F(1)(XN\mathfrak{A})^2}{\det \Lambda(\mathfrak{AB})} \right) + O\left(\sum_{\substack{\mathfrak{B} \\ N\mathfrak{B} \leq 2C_{\mathcal{N}} X}} \frac{AX}{N\mathfrak{B}} \right).$$

As in the previous case the first term leads exactly to the predicted main term. For the first error term we appeal once more to (3.3.28) to get Vol $S_F(1) \ll (C_{\mathcal{N}}^{inf})^2$. Using inclusion (3.3.32) we get $\Lambda_{\mathcal{N}}(\mathfrak{AB}) \subseteq (\sigma \mathfrak{C}_0^{-1} \mathfrak{AB})^2$ and therefore

$$\det \Lambda_{\mathcal{N}}(\mathfrak{AB}) \geq \det(\sigma \mathfrak{C}_0^{-1} \mathfrak{AB})^2 = (C_{\mathcal{N}}^{fin})^{-2} (N\mathfrak{A} N\mathfrak{B})^2.$$

So the first error term is reduced to

$$C_{\mathcal{N}}^2 X^2 \sum_{\substack{\mathfrak{B} \\ N\mathfrak{B} > 2C_{\mathcal{N}} X}} N\mathfrak{B}^{-2}$$

and so is

$$O(C_{\mathcal{N}} X) = O(AX\mathfrak{L}).$$

The second error term is even easier; namely

$$\sum_{\substack{\mathfrak{B} \\ N\mathfrak{B} \leq 2C_{\mathcal{N}} X}} \frac{AX}{N\mathfrak{B}} \leq AX \max\{0, 1 + \log(2C_{\mathcal{N}} X)\} = O(AX\mathfrak{L}).$$

This completes the proof of Theorem 3.1.

CHAPTER 4

Counting points of fixed relative degree

In this chapter we present the main result of this Thesis. It deals with counting points of fixed relative degree and bounded height. As an immediate consequence it will solve Problem 0.1 when n is large compared to e. We state our result for a large class of heights on points of fixed relative degree, which can be considered as heights in the sense of the previous chapter when the degree is one. In Chapter 5 we will give another application of our main result.

1. Arakelov-Lipschitz systems II

Let k be a number field of degree m and $\overline{k}$ an algebraic closure of k. We fix k and $\overline{k}$ throughout this chapter and assume finite extensions of k to lie in $\overline{k}$.

1.1. Arakelov-Lipschitz systems on a collection of number fields. Let $\mathcal{C}$ be a collection of finite extensions of k. We are especially interested in the set of all extensions of fixed relative degree. We denote it by

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

Let $\mathcal{N}$ be a collection of Arakelov-Lipschitz systems $\mathcal{N}_K$ of dimension n - one for each K of $\mathcal{C}$. Then we call $\mathcal{N}$ an *Arakelov-Lipschitz system (ALS) on $\mathcal{C}$ of dimension n.* We say $\mathcal{N}$ is a *uniform ALS* on $\mathcal{C}$ of dimension n with associated constants $C_{\mathcal{N}}, M_{\mathcal{N}}, L_{\mathcal{N}}$ in $\mathbb{R}$ if the following holds: for each *ALS* $\mathcal{N}_K$ of the collection $\mathcal{N}$ we can choose associated constants $C_{\mathcal{N}_K}, M_{\mathcal{N}_K}, L_{\mathcal{N}_K}$ satisfying

$$C_{\mathcal{N}_K} \leq C_{\mathcal{N}}, \quad M_{\mathcal{N}_K} \leq M_{\mathcal{N}}, \quad L_{\mathcal{N}_K} \leq L_{\mathcal{N}}.$$

Notice that a uniform *ALS* $\mathcal{N}$ (of dimension n) on the collection consisting only of a single field K with associated constants $C_{\mathcal{N}}, M_{\mathcal{N}}, L_{\mathcal{N}}$ is simply an *ALS* $\mathcal{N}$ (of dimension n) on K with associated constants $C_{\mathcal{N}}, M_{\mathcal{N}}, L_{\mathcal{N}}$ in the sense of the previous chapter.

Let $\mathcal{N}$ be an *ALS* (of dimension n) on the collection consisting of all finite extensions K of k. We say $\mathcal{N}$ is *consistent* if the following

holds: for all finite extensions K, F of k with $K \subseteq F$ and all places $u \in M_F$, $w \in M_K$ with $u|w$ one has

$$N_u(\sigma_u(\boldsymbol{\alpha})) = N_w(\sigma_w(\boldsymbol{\alpha})) \tag{4.1.1}$$

for the corresponding functions $N_u \in \mathcal{N}_F$, $N_w \in \mathcal{N}_K$ and all $\boldsymbol{\alpha}$ in K^{n+1}. Let $v \in M_k$ and suppose $w|v$ and $v|\infty$. If $d_w = d_v$ then $K_w^{n+1} = k_v^{n+1}$ and the sets $\sigma_w(K^{n+1})$, $\sigma_v(k^{n+1})$ are both dense; it follows that $N_w = N_v$ on $K_w^{n+1} = k_v^{n+1}$. A standard example for a uniform consistent ALS is given as follows: choose N_v as in (3.1.2) for each v in M_K, then clearly $C_{\mathcal{N}} = 1$ is fine. And we know from Subsection 1.2 Chapter 3, right at the end, that we may choose $M_{\mathcal{N}} = 2n + 2$ and $L_{\mathcal{N}} = 2\pi\sqrt{2n+1}$. Alternatively we could use Remark 4, coming from the more subtle arguments in Appendix A. Choosing l^2-norms at all infinite places and N_v as in (3.1.2) for all finite places yields another important uniform consistent ALS.

1.2. Arakelov-Lipschitz heights on a collection of number fields. Let $\mathcal{C}$ be a collection of finite extensions of k and let $\mathcal{N}$ be an ALS of dimension n on $\mathcal{C}$. Now we can define heights on $\mathbb{P}^n(K/k)$ (the set of primitive projective points) for K in $\mathcal{C}$. Let $P = (\alpha_0 : ... : \alpha_n) \in \mathbb{P}^n(K/k)$, so that $k(P) = K$. According to Chapter 3 we know that $H_{\mathcal{N}_K}(\cdot)$ defines a projective height on $\mathbb{P}^n(K)$. Now we define

$$H_{\mathcal{N}}(P) = H_{\mathcal{N}_K}(P). \tag{4.1.2}$$

Set $\boldsymbol{\alpha} = (\alpha_0, ..., \alpha_n)$. From the previous chapter we know

$$H_{\mathcal{N}_K}(P) = \prod_{v \in M_K} N_v(\sigma_v(\boldsymbol{\alpha}))^{\frac{d_v}{d}} \tag{4.1.3}$$

for the functions N_v of $\mathcal{N}_K$ and $[K : \mathbb{Q}] = d$, $[K_v : \mathbb{Q}_v] = d_v$. Notice that in Chapter 3 we had only a single ALS $\mathcal{N}_K$ to define the height on all points of $\mathbb{P}^n(K)$. By definition (4.1.2) $\mathcal{N}_K$ suffices only to define the height on the set of (projective) primitive points, which for $K \neq k$ is a strict subset of $\mathbb{P}^n(K)$. Now suppose $\mathcal{N}$ is consistent and let P be in $\mathbb{P}^n(K)$, not necessarily primitive. Then

$$H_{\mathcal{N}_K}(P) = H_{\mathcal{N}_{k(P)}}(P),$$

so that $\mathcal{N}_K$ defines the height on all points of $\mathbb{P}^n(K)$. For the standard example in Subsection 1.1 we see that $H_{\mathcal{N}}$ is the (absolute, non-logarithmic) Weil height H, which will be called also l^∞-height. For the other example at the end of Subsection 1.1, using l^2-norms at the infinite places, we denote $H_{\mathcal{N}}$ by H_2. The l^2-height H_2 will appear again in Chapter 5.

2. Introduction and results

Let $\mathcal{N}$ be an ALS on $\mathcal{C}_e$ of dimension n. Then $H_{\mathcal{N}}(\cdot)$ defines a height on $\mathbb{P}^n(k;e)$, the set of points $P = (\alpha_0 : ... : \alpha_n)$ in $\mathbb{P}^n(\overline{k})$ with $[k(P) : k] = e$ where $k(P) = k(..., \alpha_i/\alpha_j, ...)$ for $0 \leq i, j \leq n$, $\alpha_j \neq 0$. The associated counting function $Z_{\mathcal{N}}(\mathbb{P}^n(k;e), X)$ denotes the number of points P in $\mathbb{P}^n(k;e)$ with $H_{\mathcal{N}}(P) \leq X$. Assume $\mathcal{N}$ is a uniform ALS on $\mathcal{C}_e$ (of dimension n). Then due to Northcott and (3.1.16) $Z_{\mathcal{N}}(\mathbb{P}^n(k;e), X)$ is finite for all X in $[0, \infty)$. Recall the definition of the Schanuel constant $S_K(n)$ (see (3.2.1)) and those of $V_{\mathcal{N}_K}$ (see (3.1.15)). By r_K we denote the number of real embeddings of K and s_K is the number of pairs of distinct complex conjugate embeddings of K. Now we define the sum

$$D_{\mathcal{N}} = D_{\mathcal{N}}(k, e, n) = \sum_K 2^{-r_K(n+1)} \pi^{-s_K(n+1)} V_{\mathcal{N}_K} S_K(n) \tag{4.2.1}$$

where the sum runs over all extensions of k with relative degree e. We will prove that the sum in (4.2.1) converges if n is large enough compared to e.

After all this we are ready to state the main theorem.

Main Theorem
Let e, n be positive integers and k a number field of degree m. Suppose $\mathcal{N}$ is a uniform Arakelov-Lipschitz system of dimension n on $\mathcal{C}_e$, the collection of all finite extensions of k of relative degree e, with associated constants $C_{\mathcal{N}}, M_{\mathcal{N}}$ and $L_{\mathcal{N}}$. Write

$$A_{\mathcal{N}} = M_{\mathcal{N}}^{me} (C_{\mathcal{N}}(L_{\mathcal{N}} + 1))^{me(n+1)-1}.$$

(a) For every positive ϵ there is a constant $c_1 = c_1(k, e, n, \epsilon)$ depending only on k, e, n, ϵ such that for $X > 0$

$$Z_{\mathcal{N}}(\mathbb{P}^n(k;e), X) \leq c_1 C_{\mathcal{N}} A_{\mathcal{N}} X^{me(n+1)} \max\{1, (C_{\mathcal{N}} X)^{me(2e - \frac{n+1}{2}) + \epsilon}\}.$$

Moreover with $c_2 = c_2(k, e, n)$ as in Theorem 2.3 one has

$$Z_{\mathcal{N}}(\mathbb{P}^n(k;e), X) \leq c_2 (C_{\mathcal{N}} X)^{me(n+e)}.$$

(b) Suppose that either $e = 1$ or

$$n > 5e/2 + 4 + 2/(me).$$

Then the sum in (4.2.1) converges and as $X > 0$ tends to infinity we have

$$Z_{\mathcal{N}}(\mathbb{P}^n(k;e), X) = D_{\mathcal{N}} X^{me(n+1)} + O(A_{\mathcal{N}} X^{me(n+1)-1} \mathfrak{L}),$$

where $\mathfrak{L} = \log\max\{2, 2C_{\mathcal{N}}X\}$ *if* $(me, n) = (1, 1)$ *and* $\mathfrak{L} = 1$ *otherwise. The constant in* O *depends only on* k, e *and* n.

In Chapter 5 we will explore some applications of the Main Theorem. Here we are content with some immediate consequences. First let us consider part (b). For $e = 1$ we recover a version of Proposition [**34**], which allows more general norms at the finite places (this generalization will be essential to deduce the results of Chapter 5). Now choose the standard uniform ALS at the end of Subsection 1.1 so that $H_{\mathcal{N}}$ becomes the Weil height. Schanuel's Theorem implies $S_K(n) = D_{\mathcal{N}}(K, 1, n) = 2^{-r_K(n+1)}\pi^{-s_K(n+1)}V_{\mathcal{N}_K}S_K(n)$. We can verify

$$V_{\mathcal{N}_K} = 2^{r_K(n+1)}\pi^{s_K(n+1)} \tag{4.2.2}$$

directly by noting that $\Lambda_{\mathcal{N}}(\mathfrak{D}) = (\sigma\mathfrak{D})^{n+1}$ in (3.1.10), so that $\det\Lambda_{\mathcal{N}}(\mathfrak{D}) = (2^{-s_K}N\mathfrak{D}\sqrt{|\Delta_K|})^{n+1}$ (see [**34**] Lemma 5). Inserting the latter in definition (3.1.13) we get $V^{fin}_{\mathcal{N}_K} = 1$ and it is clear that $V^{inf}_{\mathcal{N}_K} = 2^{r_K(n+1)}\pi^{s_K(n+1)}$. Then (4.2.2) follows from $V_{\mathcal{N}_K} = V^{inf}_{\mathcal{N}_K}V^{fin}_{\mathcal{N}_K}$. For $k = \mathbb{Q}$ and $e = 2$ we recover essentially Theorem 3 on p.345 in [**49**] but only for $n > 10$ while Schmidt does it for all $n \geq 3$ and even (in a modified form) for $n = 1, 2$. For $k = \mathbb{Q}$ and $e > 2$ we find Theorem 4.1 a) on p.73 in [**17**] applied to the Weil height but again with the stronger restriction $n > 5e/2 + 4 + 2/(me)$ instead of Gao's $n > e$.

Now let us return from $\mathbb{Q}$ to arbitrary number fields k and assume $e > 1$. In this case rather little was known; namely Schmidt's upper and lower bounds (Theorem 2.3) implying that

$$cX^{me(\max\{e,n\}+1)} \leq Z_H(\mathbb{P}^n(k; e), X) \leq CX^{me(n+e)}$$

for $X \geq X_0(k, e, n)$ and certain positive constants c, C depending on k, e, n (in fact the upper bound holds for any nonnegative X). For $n = 1$ this established the correct order of magnitude and recently Masser and Vaaler (Theorem 0.5) found even the correct asymptotics. However their work shed no light on the case when $n > 1$ and even worse there is a considerable gap between the two exponents in Schmidt's bounds. Therefore for $n > 1$ not even the correct order of magnitude was known (see also [**34**] p.428). The Main Theorem part (a) improves upon Schmidt's upper bound when $n > 2e + 1$. On the other hand Schmidt's bound is completely explicit. Here this could be achieved with some extra effort by proving an explicit version of Theorem 3.1. Now if $n > 5e/2 + 4 + (2/me)$ we even get the correct asymptotics confirming Schmidt's suggestion (at least for n large) that his lower

bounds are likely to be nearer the truth than the upper bound.

Let us illustrate this with a single new example. We take $n = 11$, $k = \mathbb{Q}(i)$, $e = 2$, so that we are counting points in eleven dimensions quadratic over $\mathbb{Q}(i)$. For the number $Z = Z_H(\mathbb{P}^{11}(\mathbb{Q}(i); 2), X)$ of points of height at most X, the Schmidt bounds are

$$X^{48} \ll Z \ll X^{52}$$

for $X \geq X_0$, with absolute implied constants. Our result implies that

$$Z = DX^{48} + O(X^{47})$$

with

$$D = 12 \cdot (2\pi)^{24} \sum_{\substack{K \\ [K:\mathbb{Q}(i)]=2}} \frac{h_K R_K}{w_K \zeta_K(12) |\Delta_K|^6}$$

where we used that $r_K = 0, s_K = 2$ for all these K's.

It is likely that the main result part (b) is valid for $n > e$. Gao showed, at least for his definition of height (see Appendix B), that for $k = \mathbb{Q}$ the bound $n > e$ suffices. On the other hand Schmidt's lower bound implies that part (b) in the Main Theorem cannot hold for $e > 1$ and $n < e$. However there is a good possibility of obtaining the asymptotics for $e > 1$ and $n = 1$ using a kind of generalized Mahler measure.

3. Proof of Main Theorem

Usually the constants involved in $\ll$ and $\gg$ will depend only on k, n, e. If the constants depend also on additional parameters then we emphasize the dependence by adding these parameters as an index. The case $e = 1$ is already covered by the work of the previous chapters. Part (b) comes directly from Corollary 3.1 in Chapter 3 by choosing $K = k$. Part (a) is covered by Corollary 2.1 with $\mathcal{F} = H_{\mathcal{N}}$ and $C = C_{\mathcal{N}}$ so that we conclude $Z_{\mathcal{N}}(\mathbb{P}^n(k; 1), X) = Z_{\mathcal{N}}(\mathbb{P}^n(k), X) \leq c(m)(C_{\mathcal{N}} X)^{m(n+1)} \leq c(m) A_{\mathcal{N}} C_{\mathcal{N}} X^{m(n+1)}$ for a constant $c(m)$ depending only on m.

For the rest of this chapter we assume

$$e > 1.$$

3.1. Preliminaries. Let K be in $\mathcal{C}_e$. Then by definition $H_{\mathcal{N}}(P) = H_{\mathcal{N}_K}(P)$ for all P in $\mathbb{P}^n(K/k)$. Since

$$\mathbb{P}^n(k;e) = \bigcup_{K\in\mathcal{C}_e} \mathbb{P}^n(K/k) \tag{4.3.1}$$

where the right hand side is a disjoint union, we get

$$Z_{\mathcal{N}}(\mathbb{P}^n(k;e),X) = \sum_{K\in\mathcal{C}_e} Z_{\mathcal{N}_K}(\mathbb{P}^n(K/k),X). \tag{4.3.2}$$

For a non-zero ideal $\mathfrak{A}$ in K let $D_{K/k}(\mathfrak{A})$ be the discriminant-ideal of $\mathfrak{A}$ relative to k and write $D_{K/k}$ for $D_{K/k}(\mathcal{O}_K)$ (for definitions see [**36**] p.212 or [**23**]) where $\mathcal{O}_K$ denotes the ring of integers in K. By assumption we have $\mathbb{Q}\subseteq k\subseteq K$ hence

$$D_{K/\mathbb{Q}} = D_{k/\mathbb{Q}}^{[K:k]} N_{k/\mathbb{Q}}(D_{K/k}) \tag{4.3.3}$$

(here the norm is interpreted as an ideal). A good reference is for example [**36**] (2.10) Korollar p.213. Let P be in $\mathbb{P}^n(K/k)$, so $K = k(P)$. We use a theorem of Silverman ([**54**] Theorem 2) with Silverman's S_F (for $F = k$) as the set of archimedean absolute values. Then Silverman's $L_F(\cdot)$ is simply the usual norm $N(\cdot)$. Hence we deduce

$$H(P)^m \geq \exp(-\frac{\delta_k \log e}{2(e-1)}) N_{k/\mathbb{Q}}(D_{K/k})^{\frac{1}{2e(e-1)}} \tag{4.3.4}$$

where δ_k is the number of archimedean places in M_k (here the norm is back as a rational number). Since Silverman uses not an absolute height but rather an "absolute height relative to k", we had to take the m-th power on the left hand side of (4.3.4).

Clearly $D_{K/\mathbb{Q}}$ is the principal ideal generated by Δ_K. Combining (4.3.3) and (4.3.4) yields

$$\begin{aligned} H(P) &\geq \exp(-\frac{\delta_k \log e}{2(e-1)m}) |\Delta_k|^{-\frac{1}{2(e-1)m}} |\Delta_K|^{\frac{1}{2e(e-1)m}} \\ &\gg |\Delta_K|^{\frac{1}{2e(e-1)m}}. \end{aligned} \tag{4.3.5}$$

Recalling the definitions of δ, δ_g and $G(K/k)$ from Chapter 3 and taking $P = (1:\alpha_1:\alpha_2)$ in $\mathbb{P}^2(K/k)$ we get

$$\delta_g(K/k) \gg |\Delta_K|^{\frac{1}{2e(e-1)m}} \tag{4.3.6}$$

for any $g \in G(K/k)$; and similarly

$$\delta(K/k) \gg |\Delta_K|^{\frac{1}{2e(e-1)m}}. \tag{4.3.7}$$

Actually we have already seen in Section 2 Chapter 3 that $\delta \leq 2e\delta_g$ and so (4.3.6) implies (4.3.7). Here it might be worth to point out

that (4.3.5) can be used to prove a version of Theorem 3.1 where B is redefined in terms of the discriminants; namely

$$B = B_K = A_{\mathcal{N}} R_K h_K \sum_{g \in G(K/k)} (|\Delta_k|^{-e} |\Delta_K|)^{-\frac{\mu_g}{2e(e-1)m}}. \tag{4.3.8}$$

At the first glance this error term looks more appropriate due to the unavoidable appearance of Δ_K in the main term. In the next subsection we will explain why it is more convenient to use δ_g instead of Δ_K. Thanks to the well-known Theorem of Siegel-Brauer ([**23**] p.328 Corollary or [**53**] p.67 Satz 1 for a more precise version) we can use the inequalities (4.3.6) and (4.3.7) to bound the product of regulator and class number. More precisely we have

$$R_K h_K \ll_\beta \delta_g (K/k)^\beta \tag{4.3.9}$$

and

$$R_K h_K \ll_\beta \delta (K/k)^\beta. \tag{4.3.10}$$

for any $\beta > e(e-1)m$ and any $g \in G(K/k)$. The next argument is rather simple but will be used a lot. It is known as dyadic summation and we state it as a lemma.

LEMMA 4.1 (Dyadic summation). *Let $\mathcal{C}$ be a non-empty subset of $\mathcal{C}_e$ and let ι be a map $\iota : \mathcal{C} \longrightarrow [1, \infty)$. Write $N_\iota(T) = |\{K \in \mathcal{C}; \iota(K) \leq T\}|$ and suppose there are nonnegative real numbers b, c (independent of T) with*

$$N_\iota(T) \leq cT^b$$

for every $T > 0$. Let $\mathcal{C}'$ be a non-empty subset of $\mathcal{C}$. Set $\mathfrak{M} = [\log_2 \max_{\mathcal{C}'} \iota(K)] + 1$ if $\mathcal{C}'$ is finite and $\mathfrak{M} = \infty$ otherwise. Moreover suppose α is a real number such that $\sum_{i=1}^{\mathfrak{M}} 2^{i(\alpha+b)}$ converges. Then we have

$$\sum_{K \in \mathcal{C}'} \iota(K)^\alpha \leq c 2^{|\alpha|} \sum_{i=1}^{\mathfrak{M}} 2^{i(\alpha+b)}.$$

Proof. From the definition of $\mathfrak{M}$ and since $\mathcal{C}' \subseteq \mathcal{C}$ we have

$$\sum_{K \in \mathcal{C}'} \iota(K)^\alpha = \sum_{i=1}^{\mathfrak{M}} \sum_{\substack{K \in \mathcal{C}' \\ 2^{i-1} \leq \iota(K) < 2^i}} \iota(K)^\alpha \leq \sum_{i=1}^{\mathfrak{M}} \sum_{\substack{K \in \mathcal{C} \\ 2^{i-1} \leq \iota(K) < 2^i}} \iota(K)^\alpha.$$

First suppose $\alpha < 0$. Then the latter is

$$\leq \sum_{i=1}^{\mathfrak{M}} 2^{(i-1)\alpha} N_\iota(2^i) \leq c 2^{-\alpha} \sum_{i=1}^{\mathfrak{M}} 2^{i(\alpha+b)}.$$

If $\alpha \geq 0$ then we even get

$$\sum_{K \in \mathcal{C}'} \iota(K)^{\alpha} \leq c \sum_{i=1}^{\mathfrak{M}} 2^{i(\alpha+b)}.$$

This proves the lemma. □

Recall the definition of $G(K/k)$ from Chapter 3. In our applications ι will be δ_g and $\mathcal{C}$ will be

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

the set of extensions K of k of relative degree e containing an intermediate field $K_0 \subsetneq K$ with $[K_0 : k] = g$. Let G_u be the union of all $G(K/k)$'s

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

so that $\mathcal{C}_e^{(g)}$ is non-empty if and only if $g \in G_u$. In fact G_u is simply the set of positive, proper divisors of e but we need only

$$\{1\} \subseteq G_u \subseteq \{1, ..., [e/2]\}.$$

To apply the Dyadic summation Lemma we need information about the growth rate of $N_{\delta_g}(T)$. In accordance with the notation in Lemma 4.1 we define for an integer $g \in G_u$ and real positive T

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

The set on the right-hand side is finite. More precisely we have

LEMMA 4.2. *Set $\gamma_g = m(g^2 + g + e^2/g + e)$. Then for real positive T and g in G_u we have*

$$N_{\delta_g}(T) \ll T^{\gamma_g}$$

Proof. Since $H(1, \alpha_1, \alpha_2) \geq \max\{H(1, \alpha_1), H(1, \alpha_2)\}$ it suffices to show that the number of $(\alpha_1, \alpha_2) \in \overline{k}^2$ with

$$[k(\alpha_1) : k] = g \tag{4.3.11}$$

$$[k(\alpha_1, \alpha_2) : k(\alpha_1)] = e/g \tag{4.3.12}$$

$$H(1, \alpha_1), H(1, \alpha_2) \leq T \tag{4.3.13}$$

is $\ll T^{\gamma_g}$. The number of projective points in $\mathbb{P}(k; g)$ with height not exceeding T is an upper bound for the number of α_1 in $\overline{k}$ of relative degree g with $H(1, \alpha_1) \leq T$. Thus by Theorem 2.3 we get the upper bound

$$\ll T^{mg(g+1)} \tag{4.3.14}$$

for the number of α_1. Next for each α_1 we count the number of α_2. By (4.3.12) we have $[k(\alpha_1,\alpha_2):k(\alpha_1)]=e/g$ and moreover $H(1,\alpha_2)\le T$. Applying Theorem 2.3 (note that the constant $c_2(k,e,n)$ in Theorem 2.3 depends only on $[k:\mathbb{Q}],e,n$) once more yields the upper bound

$$\ll T^{[k(\alpha_1):\mathbb{Q}](e/g)(e/g+1)}=T^{me(e/g+1)} \tag{4.3.15}$$

for the number of α_2 provided α_1 is fixed. Multiplying the bound (4.3.14) for the number of α_1 and (4.3.15) gives the upper bound

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

for the number of (α_1,α_2) and thereby proves the lemma. □

Recall that $\delta_1=\delta$ and that $N_\delta(T)$ denotes the number of number fields K in $\overline{k}$ of relative degree e with $\delta(K/k)\le T$. So Lemma 4.2 with $g=1$ yields an upper bound for the growth rate of $N_\delta(T)$ but applying Theorem 2.3 directly gives a slightly better result.

LEMMA 4.3. *Set $\gamma=me(e+1)$ and let $C_\delta=c_2(k,e,1)$ be as in Theorem 2.3. Then for $T>0$ we have*

$$N_\delta(T)\le C_\delta T^\gamma. \tag{4.3.16}$$

Proof. The number of points in $\mathbb{P}(k;e)$ with height not larger than T is clearly an upper bound for $N_\delta(T)$. Thus the lemma follows from (2.1.1) in Theorem 2.3. □

In fact Lemma 4.2 would suffice to prove the full Main Theorem, so one could omit Lemma 4.3. We did not because γ looks nicer than γ_1 and the proof above is essentially simply a reference.

3.2. Proof of part (b)**.** For brevity we write

$$D_K=2^{-r_K(n+1)}\pi^{-s_K(n+1)}V_{\mathcal{N}_K}S_K(n) \tag{4.3.17}$$

for the constant in the main term of Theorem 3.1 and

$$B_K=A_{\mathcal{N}_K}R_Kh_K\sum_{g\in G(K/k)}\delta_g(K/k)^{-\mu_g} \tag{4.3.18}$$

for the constant in the error term of Theorem 3.1. Thanks to (4.3.2) and Theorem 3.1 it suffices to show that $\sum D_K$ and $\sum B_K$ are convergent (here the sum runs over the same fields as in (4.2.1) and (4.3.2)).

Before proving part (b) let us explain why we use B_K involving δ_g as in (4.3.18) instead of B_K with Δ_K as in (4.3.8). Recall that $\mathcal{C}_e^{(g)}$ is nonempty if and only if $g\in G_u$. Suppose we have a map $\iota_g:\mathcal{C}_e^{(g)}\longrightarrow[1,\infty)$

for each g in G_u with

$$\delta_g(K/k) \gg \iota_g(K)^{\kappa_g}, \tag{4.3.19}$$

$$\iota_g(K)^{\kappa'_g} \gg R_K h_K \tag{4.3.20}$$

for positive κ_g, κ'_g depending only on k, e and g. Then we deduce from (4.3.18)

$$\sum_{K\in\mathcal{C}_e} B_K \ll A_{\mathcal{N}} \sum_{g\in G_u} \sum_{K\in\mathcal{C}_e^{(g)}} \iota_g^{-\mu_g\kappa_g+\kappa'_g}. \tag{4.3.21}$$

Suppose we have a nonnegative real number b_g for each $g \in G_u$ with

$$N_{\iota_g}(T) = |\{K \in \mathcal{C}_e^{(g)}; \iota_g(K) \le T\}| \ll T^{b_g}.$$

In order to deduce convergence for (4.3.21) from the Dyadic summation Lemma we need $-\mu_g\kappa_g+\kappa'_g+b_g < 0$ for each $g \in G_u$, which is equivalent to

$$n > \frac{(b_g + \kappa'_g)}{\kappa_g m(e-g)} + \frac{1}{m(e-g)} - 1 \tag{4.3.22}$$

for each $g \in G_u$. We will now investigate for different choices of the invariants ι_g how this lower bound for n grows if e gets large. First let us suppose that $\iota_g = |\Delta_K|$. By (4.3.6) we see that $\kappa_g = 1/(2e(e-1)m)$ is admissible (Masser showed [**39**] Proposition 1, at least for $k = \mathbb{Q}$, that κ_1 cannot be increased). Using the Theorem of Siegel-Brauer we see that any $\kappa'_g > 1/2$ is fine and no $\kappa'_g < 1/2$ is possible. What about b_g? Since $\mathcal{C}_e^{(1)} = \mathcal{C}_e$ we see that b_g can be estimated by b_1. Now counting fields with respect to the discriminant is a major unsolved problem. The asymptotics of $N_\Delta(T) = |\{K \in \mathcal{C}_e; |\Delta_K| \le T\}|$ are predicted by a classical conjecture, which is possibly due to Linnik and states that if $T > 0$ tends to infinity one has

$$N_\Delta(T) = c_\Delta T + o(T) \tag{4.3.23}$$

for a positive constant c_Δ depending on k, e. This would imply that $b_1 = 1$ is an admissible choice providing the bound $n > 6e - 7 + 2/(me)$. But Linnik's Conjecture is proved only for $e \le 3$ (Davenport and Heilbronn [**11**] for $k = \mathbb{Q}$ and Datskovsky and Wright [**9**] for arbitrary k) and for $e = 4, 5$ (Bhargava [**2**]) but restricted to $k = \mathbb{Q}$. It might come as a surprise that this approach, together with the fact $G_u = \{1\}$ for e prime, leads to the better bounds $n > 5 + 1/m$ and $n > 8 + 1/(2m)$ for $e = 2$ and $e = 3$ respectively. Schmidt was probably the first (see [**50**]) making a considerable approach to (4.3.23) for arbitrary

degree. His result implies

$$N_\Delta(T) \ll T^{\frac{e+2}{4}}. \tag{4.3.24}$$

Setting $b_g = (e+2)/4$ and inserted in (4.3.22) provides the bound $n > e^2+3e-5+2/(me)$. In fact estimating b_g by b_1 is a loss since Schmidt's result even implies that we can choose $b_g = (\max\{g, e/g\}+2)/4$. Then we get a better bound for n, but still of quadratic order. The recent work [**14**] of Ellenberg and Venkatesh makes great progress towards (4.3.23). Their result (Theorem 1.1) gives a bound for n of order $e\exp(C\sqrt{\log(e/2)})$ for an effective, positive, absolute constant C. Note that any exponent b_g independent of e would give even a linear bound for n. Next we consider the invariant δ. Counting fields with respect to δ seems to be easier. Here upper and lower bound for the order of magnitude are rather close (see Section 4), which is in stark contrast to when counted via $|\Delta_K|$. But using only $\iota = \delta$ with $\kappa_g = 1$, $\kappa_g' > e(e-1)m$ from (4.3.10) and $b_g = \gamma$ from Lemma 4.3 we could prove the Main Theorem part (b) only for $n > 4e$. For e prime we can use $G_u = \{1\}$ to relax the constraint to $n > 2e+1+2/(e-1)+1/(m(e-1))$. But we did not include this improvement in the Main Theorem to keep the statement simpler. Note that if b_g, κ_g, κ_g' are independent of g then the right-hand side of (4.3.22) gets large if g gets large ($1 \le g \le e/2$). For δ the quantities b_g, κ_g, κ_g' from above are independent of g. Using a more sophisticated invariant one could hope to reduce b_g, κ_g' or increase κ_g if g gets bigger. Indeed choosing $\iota_g = \delta_g$ we may use the same values for κ_g, κ_g' as for δ but we see from Lemma 4.2 that $b_g = \gamma_g$ gets smaller if g gets large, for example $\gamma_{e/2} = me(e/4+5/2) < me(e+1) = \gamma$ provided $e > 2$. Therefore we can relax the constraint $n > 4e$ to $n > 5e/2 + 4 + 2/(me)$.

After this discussion let us come back to the proof of the Main Theorem part (b). Since $\mathcal{N}$ is a uniform ALS on $\mathcal{C}_e$ with associated constants $C_\mathcal{N}, M_\mathcal{N}$ and $L_\mathcal{N}$ we can assume that

$$C_{\mathcal{N}_K} \le C_\mathcal{N}, \tag{4.3.25}$$

$$M_{\mathcal{N}_K} \le M_\mathcal{N}, \tag{4.3.26}$$

$$L_{\mathcal{N}_K} \le L_\mathcal{N}. \tag{4.3.27}$$

This implies in particular

$$A_{\mathcal{N}_K} \le A_\mathcal{N}. \tag{4.3.28}$$

Let us now prove that $\sum_K B_K$ converges. We set $\beta = e(e-1)m+1/8$. Using (4.3.9) and (4.3.28) we get

$$\sum_{K\in\mathcal{C}_e} B_K \ll A_{\mathcal{N}} \sum_{K\in\mathcal{C}_e} \sum_{g\in G(K/k)} \delta_g (K/k)^{\beta-\mu_g}.$$

Recall that $G_u = \bigcup_{\mathcal{C}_e} G(K/k)$. So the term on the right-hand side above is

$$\begin{aligned} &= A_{\mathcal{N}} \sum_{g\in G_u} \sum_{\substack{K\in\mathcal{C}_e \\ g\in G(K/k)}} \delta_g (K/k)^{\beta-\mu_g} \\ &= A_{\mathcal{N}} \sum_{g\in G_u} \sum_{K\in\mathcal{C}_e^{(g)}} \delta_g (K/k)^{\beta-\mu_g} \end{aligned} \tag{4.3.29}$$

provided the sum converges. This will be verified in a moment (see (4.3.30)). Applying the Dyadic summation Lemma with $\iota = \delta_g$ and $b = \gamma_g$ from Lemma 4.2 we see that the latter is

$$\ll A_{\mathcal{N}} \sum_{g\in G_u} \sum_{i=1}^{\infty} 2^{i(\gamma_g+\beta-\mu_g)}.$$

The next lemma will tell us that the exponent $\gamma_g + \beta - \mu_g$ is negative. Assuming this for a moment we see that the inner sum above is $\ll 1$. Thus we derive the upper bound

$$\ll A_{\mathcal{N}} \sum_{g\in G_u} 1 \leq A_{\mathcal{N}}[e/2], \tag{4.3.30}$$

confirming that the whole sum in (4.3.29) converges. This verifies the convergence of $\sum_K B_K$ on the assumption that $\gamma_g + \beta - \mu_g < 0$ for all $g \in G_u$. The following lemma shows that indeed $\gamma_g + \beta - \mu_g < -1/8$ holds for all $g \in G_u$. Recall that we assume $e > 1$ and therefore by hypothesis of the Main Theorem part (b) $n > 5e/2 + 4 + 2/(me)$.

Lemma 4.4. *Let g be in G_u. Then*

$$\gamma_g + \beta - \mu_g \leq -\frac{1}{8}. \tag{4.3.31}$$

Proof. Recall that $G_u \subseteq \{1, ..., [e/2]\}$ and $\mu_g = m(e-g)(n+1) - 1$. Write

$$F(g) = \frac{1}{m(e-g)}(\gamma_g + \beta + 1).$$

So (4.3.31) claims that $m(e-g)(F(g)-(n+1)) \leq -1/8$ for all $g \in G_u$. Hence it suffices to show that

$$F(g) - (n+1) \leq -\frac{1}{4me}$$

for $1 \le g \le e/2$. By definition

$$F(g) = \frac{g^2 + g + e^2/g + e}{e-g} + \frac{e(e-1)}{e-g} + \frac{1+1/8}{m(e-g)}.$$

We claim that the second derivative $F''(g)$ is positive for $1 \le g \le e/2$. One finds

$$\begin{aligned} F''(g) =& \frac{2(e^2/g^3+1)(e-g) + 2(2g+1-e^2/g^2)}{(e-g)^2} + \frac{2e(e-1)}{(e-g)^3} \\ &+ \frac{2(g^2+g+e^2/g+e)}{(e-g)^3} + \frac{2(1+1/8)}{m(e-g)^3}. \end{aligned}$$

For $1 \le g \le e/2$ the last three fractions are certainly positive and so we may focus on the numerator of the first fraction. Now if $2g+1-e^2/g^2 \ge 0$ the claim follows at once. If $2g + 1 - e^2/g^2 < 0$ it suffices to show that

$$(e^2/g^3+1)(e-g) \ge e^2/g^2 - 2g - 1.$$

With $u = e/g$ the latter is equivalent to $u^3 - u^2 + e - g \ge u^2 - 2g - 1$ and this is equivalent to $u^2(u-2) + e + g + 1 \ge 0$, which is certainly true since $1 \le g \le e/2$ and therefore $2 \le u \le e$.

Thus we have shown that $F''(g) > 0$ for $1 \le g \le e/2$ so that F is here convex upwards; and we now consider $F(1)$ and $F(e/2)$. First we use a simple arithmetic argument. Since n is an integer and $n > E = 5e/2+4+2/(me)$ with denominator dividing $2me$ we see that

$$n + 1 \ge E + 1 + 1/(2me). \tag{4.3.32}$$

Now $F(e/2) = 5e/2 + 5 + 2/(me) + 1/(4me) = E + 1 + 1/(4me)$ and thus

$$F(e/2) - (n+1) \le 1/(4me) - 1/(2me) = -1/(4me).$$

Finally

$$F(1) = 2e + 2 + 4/(e-1) + 9/(8m(e-1)).$$

Using (4.3.32) again yields

$$F(1) - (n+1) \le \frac{4}{e-1} + \frac{9}{8m(e-1)} - \frac{e}{2} - 3 - \frac{2}{me} - \frac{1}{2me}. \tag{4.3.33}$$

First suppose $e = 2$. Then (4.3.33) says $F(1) - (n+1) \le -1/(8m) = -1/(4em)$. Next suppose $e > 2$. Then the right-hand side in (4.3.33) is $\le 4/2 + 9/(16m) - e/2 - 3 - 5/(2me) < -5/(2me) < -1/(4em)$. This completes the proof of the lemma. □

To show convergence for $\sum_K D_K$ we may use similar arguments but here as in the proof of part (a) we use only $\delta = \delta_1$ instead of δ_g. As in Chapter 3 let $d = me$ so that $[K : \mathbb{Q}] = d$. To estimate $V_{\mathcal{N}_K}$ in (4.3.17) we proceed as in the proof of Theorem 3.1 as we had to bound the first error term in the case $(n, d) = (1, 1)$. First recall $V_{\mathcal{N}_K} = V^{inf}_{\mathcal{N}_K} V^{fin}_{\mathcal{N}_K}$. By (3.1.14) we have

$$V^{inf}_{\mathcal{N}_K} \ll (C^{inf}_{\mathcal{N}_K})^{d(n+1)}.$$

To estimate $V^{fin}_{\mathcal{N}_K}$ we note that by (3.3.32)

$$\det \Lambda_{\mathcal{N}_K}(\mathfrak{D}) \geq \det \sigma(\mathfrak{C}_0^{-1}\mathfrak{D})^{n+1}.$$

It is well-known (see [**36**] p.33 (5.2) Satz) that

$$\det \sigma(\mathfrak{C}_0^{-1}\mathfrak{D}) = 2^{-s_K}\sqrt{|\Delta_K|}N(\mathfrak{D})N(\mathfrak{C}_0)^{-1}.$$

Combining the latter with (3.3.31) we see that

$$\det \sigma(\mathfrak{C}_0^{-1}\mathfrak{D})^{n+1} = 2^{-s_K(n+1)}|\Delta_K|^{(n+1)/2}N\mathfrak{D}^{n+1}(C^{fin}_{\mathcal{N}_K})^{-d(n+1)}.$$

Inserting the latter in definition (3.1.13) yields

$$V^{fin}_{\mathcal{N}_K} \ll (C^{fin}_{\mathcal{N}_K})^{d(n+1)}.$$

Now on recalling that $C_{\mathcal{N}_K} = C^{inf}_{\mathcal{N}_K} C^{fin}_{\mathcal{N}_K}$ and using (4.3.25) we conclude

$$V_{\mathcal{N}_K} \ll C^{d(n+1)}_{\mathcal{N}_K} \leq C^{d(n+1)}_{\mathcal{N}}.$$

The number of roots of unity w_K in (3.2.1) is at least 2. Furthermore $\zeta_K(n+1) > 1$. Hence $S_K(n) \ll R_K h_K |\Delta_K|^{-\frac{n+1}{2}}$. This together with the above estimate for $V_{\mathcal{N}_K}$ implies $D_K \ll C^{d(n+1)}_{\mathcal{N}} R_K h_K |\Delta_K|^{-\frac{n+1}{2}}$ and since by Siegel-Brauer $R_K h_K \ll_\epsilon |\Delta_K|^{\frac{1}{2}+\epsilon}$ for any positive ϵ we get

$$D_K \ll_\epsilon C^{d(n+1)}_{\mathcal{N}} |\Delta_K|^{-\frac{n}{2}+\epsilon}. \tag{4.3.34}$$

At this point we could apply the Dyadic summation Lemma with $\iota = |\Delta_K|$ and $b = (e+2)/4$ from Schmidt's bound (4.3.24) to see that $\sum_K D_K$ converges for $n > e/2 + 1$. Note that Linnik's Conjecture implies convergence even for $n > 2$ but we already pointed out that for $n < e$ the main term (provided there is an asymptotic estimate as in our Main Theorem) cannot be of the form $\sum_K D_K X^{em(n+1)}$. However we may use Lemma 4.3 instead Schmidt's result if we have a lower bound for $|\Delta_K|$ in terms of $\delta(K/k)$. This lower bound is of interest for its own sake.

Lemma 4.5. *We have*

$$\delta(K/k) \leq \delta(K/\mathbb{Q}) \ll |\Delta_K|^{\frac{1}{d}}. \tag{4.3.35}$$

Proof. The lemma is trivially true for $K = k = \mathbb{Q}$. However we have by assumption $e \geq 2$ and so $[K : \mathbb{Q}] = em \geq 2$. The first inequality follows immediately from the definition. Let σ be as in (3.1.7) and suppose α is a non-zero integer of K. One gets

$$\begin{aligned} H(1,\alpha) &= \prod_{i=1}^{d} \max\{1, |\sigma_i(\alpha)|\}^{1/d} \\ &\leq \max\{1, \max_{1\leq i\leq d}\{|\sigma_i(\alpha)|\}\} \\ &\leq |\sigma(\alpha)| \end{aligned}$$

because $|\sigma(\alpha)| \geq 1$. Let $v_1 = \sigma(\alpha_1), ..., v_d = \sigma(\alpha_d)$ be linearly independent vectors of the lattice $\sigma\mathcal{O}_K$ with $|v_i| = \lambda_i$ for the successive minima λ_i of $\sigma\mathcal{O}_K$. Let us temporarily denote by b the maximal degree of all proper subfields of K. Therefore $K = \mathbb{Q}(\alpha_1, ..., \alpha_{b+1})$. Next we need to construct a primitive element in $\mathcal{O}_K$ with small height. We apply Lemma 3.1 to obtain a primitive $\alpha = \sum_{j=1}^{b+1} m_j\alpha_j$. Now

$$H(1,\alpha) \leq |\sigma(\sum_{j=1}^{b+1} m_j\alpha_j)| \leq \sum_{j=1}^{b+1} m_j|\sigma(\alpha_j)| \ll \lambda_{b+1}.$$

We shall estimate λ_{b+1}:

$$\begin{aligned} \lambda_{b+1} &= \left(\frac{\lambda_1...\lambda_b\lambda_{b+1}^{d-b}}{\lambda_1...\lambda_b}\right)^{\frac{1}{d-b}} \\ &\leq \left(\frac{\lambda_1...\lambda_d}{\lambda_1...\lambda_b}\right)^{\frac{1}{d-b}} \\ &\ll \left(\frac{\det(\sigma\mathcal{O}_K)}{\lambda_1...\lambda_b}\right)^{\frac{1}{d-b}} \\ &= \left(\frac{|\Delta_K|^{\frac{1}{2}}}{2^{s_K}\lambda_1...\lambda_b}\right)^{\frac{1}{d-b}} \\ &\ll |\Delta_K|^{\frac{1}{2(d-b)}} \end{aligned}$$

where we used again that $\lambda_1 = |\sigma(\alpha_1)| \geq H(1,\alpha_1) \geq 1$. So all this together implies

$$\delta(K/\mathbb{Q}) \ll |\Delta_K|^{\frac{1}{2(d-b)}}. \tag{4.3.36}$$

Now b is the degree of a proper subfield. Thus $b \leq d/2$ and we get (4.3.35). □

Using Lemma 4.5 and (4.3.34) with ϵ replaced by ϵ/d we deduce

$$D_K \ll_\epsilon C_{\mathcal{N}}^{d(n+1)} \delta(K/k)^{-\frac{dn}{2}+\epsilon} \tag{4.3.37}$$

for any positive ϵ. Choosing $\epsilon = 1/2$ we get

$$D_K \ll C_{\mathcal{N}}^{d(n+1)} \delta(K/k)^{-\frac{dn}{2}+\frac{1}{2}}.$$

Applying the Dyadic summation Lemma with $\iota = \delta$ and $b = \gamma$ from Lemma 4.3 we conclude

$$\begin{aligned}\sum_{K\in\mathcal{C}_e} D_K &\ll C_{\mathcal{N}}^{d(n+1)} \sum_{K\in\mathcal{C}_e} \delta(K/k)^{-\frac{dn}{2}+\frac{1}{2}} \\ &\ll C_{\mathcal{N}}^{d(n+1)} \sum_{i=1}^{\infty} 2^{(-\frac{dn}{2}+\frac{1}{2}+\gamma)i} \\ &\ll C_{\mathcal{N}}^{d(n+1)}\end{aligned}$$

provided $-\frac{dn}{2} + \frac{1}{2} + \gamma < 0$, which is equivalent to $n > 2e + 2 + 1/d$. But the latter holds since $n > 5e/2 + 4 + 2/(me)$. This completes the proof of part (b) of the Main Theorem.

3.3. Proof of part (a)**.** First note that unlike in part (b) there are no conditions on e and n except $e > 1$ from page 75. To prove part (a) let us consider the analogues of the quantities (4.3.17) and (4.3.18) for Corollary 3.1. The first is again D_K but the second changes to

$$\widetilde{B_K} = A_{\mathcal{N}_K} R_K h_K \delta(K/k)^{-\mu}.$$

Remember that $\mu = m(e - g_{\max})(n + 1) - 1 \geq d(n + 1)/2 - 1$ and $A_{\mathcal{N}_K} \leq A_{\mathcal{N}}$. Thus

$$\widetilde{B_K} \leq A_{\mathcal{N}} R_K h_K \delta(K/k)^{-d(n+1)/2+1}. \tag{4.3.38}$$

Let P be in $\mathbb{P}^n(k; e)$. So P lies in $\mathbb{P}^n(K/k)$ for some K in $\mathcal{C}_e$. By (3.1.16) we know $H_{\mathcal{N}}(P) = H_{\mathcal{N}_K}(P) \geq C_{\mathcal{N}_K}^{-1} H(P)$ and from (4.3.25) we know $C_{\mathcal{N}} \geq C_{\mathcal{N}_K}$. Thus $Z_{\mathcal{N}}(\mathbb{P}^n(k; e), X) = 0$ for $C_{\mathcal{N}} X < 1$. So we may assume

$$C_{\mathcal{N}} X \geq 1.$$

Set

$$\mathcal{B} = neC_{\mathcal{N}} X$$

and

$$\mathcal{C}' = \{K \in \mathcal{C}_e; \delta(K/k) \leq \mathcal{B}\}.$$

Note that by Lemma 4.3 the set $\mathcal{C}'$ is finite. As in Chapter 3 abbreviate $d(n + 1)$ to D.

LEMMA 4.6. *We have*

$$Z_{\mathcal{N}}(\mathbb{P}^n(k;e),X) \ll X^D \sum_{K\in\mathcal{C}'} D_K + X^{D-1}\sum_{K\in\mathcal{C}'}\widetilde{B_K}. \tag{4.3.39}$$

Proof. We claim $Z_{\mathcal{N}_K}(\mathbb{P}^n(K/k),X)=0$ for $\delta(K/k)>\mathcal{B}$. From this we could deduce

$$\begin{aligned} Z_{\mathcal{N}}(\mathbb{P}^n(k;e),X) &= \sum_{K\in\mathcal{C}_e} Z_{\mathcal{N}_K}(\mathbb{P}^n(K/k),X) \\ &= \sum_{K\in\mathcal{C}'} Z_{\mathcal{N}_K}(\mathbb{P}^n(K/k),X). \end{aligned} \tag{4.3.40}$$

Now using the estimates coming from Corollary 3.1 the statement of the lemma follows immediately. It remains to prove the claim. Let P be in $\mathbb{P}^n(K/k)$ with homogeneous coordinates $\omega_0,...,\omega_n$. We may assume $\omega_0\neq 0$ and $\omega_i\in\mathcal{O}_K$ for $0\leq i\leq n$. Applying Lemma 3.1 shows that there exist $m_1,...,m_n$ in $\mathbb{Z}$ with $0\leq m_i<e$ for $1\leq i\leq n$, such that $\beta=\sum_{i=1}^n m_i\omega_i/\omega_0$ is primitive. Using the product formula it is easily seen that $H(1,\beta)\leq neH(P)$ and by (3.1.16) we deduce $\delta(K/k)\leq H(1,\beta)\leq neC_{\mathcal{N}_K}H_{\mathcal{N}_K}(P)\leq neC_{\mathcal{N}}H_{\mathcal{N}}(P)$. In particular the fields K with $\delta(K/k)>neC_{\mathcal{N}}X=\mathcal{B}$ satisfy $Z_{\mathcal{N}_K}(\mathbb{P}^n(K/k),X)=0$, which verifies the claim. □

LEMMA 4.7. *For any positive ϵ and $\alpha_\epsilon=d(e+1-n/2)+\epsilon$ we have*

$$\sum_{K\in\mathcal{C}'} D_K \ll_\epsilon C_{\mathcal{N}}^D \max\{1,(C_{\mathcal{N}}X)^{\alpha_\epsilon}\} \tag{4.3.41}$$

Proof. We use (4.3.37) with $\epsilon/2$ instead of ϵ to get the upper bound

$$\ll_\epsilon C_{\mathcal{N}}^D \sum_{K\in\mathcal{C}'}\delta(K/k)^{-\frac{dn}{2}+\frac{\epsilon}{2}} \tag{4.3.42}$$

for the left-hand side of (4.3.41). We may assume that $\mathcal{C}'$ is not empty otherwise the lemma is trivially true. Applying the Dyadic summation Lemma with $\iota=\delta$, $b=\gamma$ from Lemma 4.3 and $\mathfrak{M}=[\log_2\mathcal{B}]+1$ we find that the above is bounded by

$$\ll_\epsilon C_{\mathcal{N}}^D \sum_{i=1}^{\mathfrak{M}} 2^{-i\eta} \tag{4.3.43}$$

with $\eta=\frac{dn}{2}-\gamma-\frac{\epsilon}{2}$. First suppose $\eta>0$. Then this is

$$\leq C_{\mathcal{N}}^D\sum_{i=1}^{\infty}2^{-i\eta}\ll_\epsilon C_{\mathcal{N}}^D.$$

Next suppose $\eta \leq 0$. Then the right-hand side of (4.3.43) becomes

$$\leq C_{\mathcal{N}}^{D} 2^{-\eta\mathfrak{M}}\mathfrak{M}.$$

Since $\mathfrak{M} = [\log_2 \mathcal{B}] + 1 = [\log_2(2neC_{\mathcal{N}}X)]$ this in turn is

$$\begin{aligned}
&\leq C_{\mathcal{N}}^{D}(2neC_{\mathcal{N}}X)^{-\eta}\log_2(2neC_{\mathcal{N}}X) \\
&\ll_{\epsilon} C_{\mathcal{N}}^{D}(C_{\mathcal{N}}X)^{-\eta+\frac{\epsilon}{2}} \\
&= C_{\mathcal{N}}^{D}\max\{1, C_{\mathcal{N}}X\}^{-\eta+\frac{\epsilon}{2}} \\
&= C_{\mathcal{N}}^{D}\max\{1, (C_{\mathcal{N}}X)^{\alpha_\epsilon}\}.
\end{aligned}$$

□

LEMMA 4.8. *For any positive ϵ and $\beta_\epsilon = d(2e - (n+1)/2) + \epsilon$ we have*

$$\sum_{K\in\mathcal{C}'} \widetilde{B_K} \ll_{\epsilon} A_{\mathcal{N}}C_{\mathcal{N}}X\max\{1, (C_{\mathcal{N}}X)^{\beta_\epsilon}\}. \tag{4.3.44}$$

Proof. By (4.3.10) we find

$$R_K h_K \ll_{\epsilon} \delta(K/k)^{d(e-1)+\epsilon/2}. \tag{4.3.45}$$

Thus (4.3.38) implies

$$\widetilde{B_K} \ll_{\epsilon} A_{\mathcal{N}}\delta(K/k)^{d(e-1)+\frac{\epsilon}{2}-\frac{d(n+1)}{2}+1}. \tag{4.3.46}$$

Hence

$$\sum_{K\in\mathcal{C}'} \widetilde{B_K} \ll_{\epsilon} A_{\mathcal{N}} \sum_{K\in\mathcal{C}'} \delta(K/k)^{d(e-1)+\frac{\epsilon}{2}-\frac{d(n+1)}{2}+1}.$$

Applying the Dyadic summation Lemma just as in (4.3.42) we deduce that the above is

$$\ll A_{\mathcal{N}} \sum_{i=1}^{\mathfrak{M}} 2^{-i\eta} \tag{4.3.47}$$

this time with

$$\begin{aligned}
\eta &= \frac{d(n+1)}{2} - 1 - d(e-1) - \frac{\epsilon}{2} - \gamma \\
&= d((n+1)/2 - 2e) - 1 - \frac{\epsilon}{2}
\end{aligned}$$

and $\mathfrak{M} = [\log_2 \mathcal{B}] + 1$ as before. Now if $\eta > 0$ then (4.3.47) is

$$\ll_{\epsilon} A_{\mathcal{N}} \leq A_{\mathcal{N}}C_{\mathcal{N}}X$$

just as for (4.3.43). If $\eta \le 0$ we similarly get the bound

$$\begin{aligned}
&\le A_{\mathcal{N}} 2^{-\eta\mathfrak{M}}\mathfrak{M} \\
&\le A_{\mathcal{N}}(2neC_{\mathcal{N}}X)^{-\eta}\log_2(2neC_{\mathcal{N}}X) \\
&\ll_\epsilon A_{\mathcal{N}}(C_{\mathcal{N}}X)^{-\eta}\log_2(2C_{\mathcal{N}}X) \\
&\ll_\epsilon A_{\mathcal{N}}(C_{\mathcal{N}}X)^{-\eta+\epsilon/2} \\
&= A_{\mathcal{N}}C_{\mathcal{N}}X\max\{1,(C_{\mathcal{N}}X)^{\beta_\epsilon}\}.
\end{aligned}$$

□

Combining Lemma 4.6, Lemma 4.7 and Lemma 4.8 we conclude: for any positive ϵ there is a constant $c_1 = c_1(k,e,n,\epsilon)$ depending only on k, e, n and ϵ such that

$$\begin{aligned}
Z_{\mathcal{N}}(\mathbb{P}^n(k;e),X) \le c_1\max\{&(C_{\mathcal{N}}X)^D\max\{1,(C_{\mathcal{N}}X)^{\alpha_\epsilon}\}, \\
&A_{\mathcal{N}}C_{\mathcal{N}}X^D\max\{1,(C_{\mathcal{N}}X)^{\beta_\epsilon}\}\}.
\end{aligned}$$

Recall that $A_{\mathcal{N}} = M_{\mathcal{N}}^d(L_{\mathcal{N}}+1)^{D-1}C_{\mathcal{N}}^{D-1}$ and $M_{\mathcal{N}} \ge 1$, $L_{\mathcal{N}} \ge 0$. Thus we get

$$Z_{\mathcal{N}}(\mathbb{P}^n(k;e),X) \le c_1A_{\mathcal{N}}C_{\mathcal{N}}X^D\max\{1,(C_{\mathcal{N}}X)^{\alpha_\epsilon},(C_{\mathcal{N}}X)^{\beta_\epsilon}\}.$$

Now $\alpha_\epsilon = d(e+1-n/2)+\epsilon < d(2e-(n+1)/2)+\epsilon = \beta_\epsilon$ and we end up with

$$Z_{\mathcal{N}}(\mathbb{P}^n(k;e),X) \le c_1A_{\mathcal{N}}C_{\mathcal{N}}X^D\max\{1,(C_{\mathcal{N}}X)^{\beta_\epsilon}\}.$$

This proves the first statement of Main Theorem part (a). The second statement is a simple consequence of Theorem 2.3 and (3.1.16). For any P in $\mathbb{P}^n(k;e)$ we have $C_{\mathcal{N}}H_{\mathcal{N}}(P) \ge H(P)$. Thus

$$Z_{\mathcal{N}}(\mathbb{P}^n(k;e),X) \le Z_H(\mathbb{P}^n(k;e),C_{\mathcal{N}}X) \le c_2(k,e,n)(C_{\mathcal{N}}X)^{d(e+n)}.$$

This completes the proof of the Main Theorem.

4. Counting number fields

Using results of the previous section and Chapter 2 we give simple lower bounds for the growth rate of $N_\delta(T)$ and $N_\Delta(T)$, the number of field extensions K of k of degree e with $\delta(K/k) \le T$ or $|\Delta_K| \le T$. The lower bound for $N_\delta(T)$ shows that Lemma 4.3 is not very far from the truth.

COROLLARY 4.1. *With $c_4 = c_4(k,e,1), c_2 = c_2(k,e,1)$ and $X_4(k,e)$ from Theorem 2.3 set*

$$c_\delta = 2^{-5em-22}c_4,\ C_\delta = c_2 \text{ and } T_0 = X_4(k,e).$$

Then we have

$$c_\delta T^{me(e-1)} \leq N_\delta(T) \leq C_\delta T^{me(e+1)}$$

where the upper bounds holds for $T > 0$ *and the lower bound holds for* $T \geq T_0$.

Proof. From the definition it is clear that $Z_H(\mathbb{P}(K/k), T) > 0$ if and only if $\delta(K/k) \leq T$. Therefore we have

$$N_\delta(T) = \sum_{\substack{K \in \mathcal{C}_e \\ \delta(K/k) \leq T}} 1 = \sum_{\substack{K \in \mathcal{C}_e \\ \delta(K/k) \leq T}} \frac{Z_H(\mathbb{P}(K/k), T)}{Z_H(\mathbb{P}(K/k), T)}. \tag{4.4.1}$$

Using the equivalence above once again, we see that the term on the far right-hand side of (4.4.1) is

$$\begin{aligned}
&\geq (\sup_{K \in \mathcal{C}_e} \{Z_H(\mathbb{P}(K/k), T)\})^{-1} \sum_{\substack{K \in \mathcal{C}_e \\ \delta(K/k) \leq T}} Z_H(\mathbb{P}(K/k), T) \\
&= (\sup_{K \in \mathcal{C}_e} \{Z_H(\mathbb{P}(K/k), T)\})^{-1} \sum_{K \in \mathcal{C}_e} Z_H(\mathbb{P}(K/k), T) \\
&= (\sup_{K \in \mathcal{C}_e} \{Z_H(\mathbb{P}(K/k), T)\})^{-1} Z_H(\mathbb{P}(k; e), T)
\end{aligned}$$

Now $Z_H(\mathbb{P}(K/k), T) \leq Z_H(\mathbb{P}(K; 1), T)$ and by (2.1.1) of Theorem 2.3 and recalling that $[K : \mathbb{Q}] = em$ we get

$$Z_H(\mathbb{P}(K; 1), T) \leq c_2(K, 1, 1) T^{2me} = 2^{5em+22} T^{2me}.$$

Furthermore (2.1.3) of Theorem 2.3 with $c_4 = c_4(k, e, 1)$ yields

$$Z_H(\mathbb{P}(k; e), T) \geq c_4 T^{me(e+1)}$$

for $T \geq X_4(k, e) = T_0$. Hence

$$N_\delta(T) \geq (2^{5em+22} T^{2me})^{-1} c_4 T^{me(e+1)} = c_\delta T^{me(e-1)}$$

for $T \geq T_0$. On the other hand Lemma 4.3 tells us that

$$N_\delta(T) \leq C_\delta T^{me(e+1)}$$

for $T > 0$. □

Corollary 4.1 combined with the lower bound (4.3.7) for δ in terms of $|\Delta_K|$ yields

COROLLARY 4.2. *There are constants* $c_5 = c_5(k, e)$ *and* $T_1 = T_1(k, e)$ *depending only on* k, e *such that*

$$N_\Delta(T) \geq c_5 T^{1/2}$$

for $T \geq T_1$.

Proof. From (4.3.7) we know that there is a positive constant $c_6 = c_6(k,e)$ depending only on $k, e > 1$ such that $\delta(K/k) \geq c_6|\Delta_K|^{1/(2e(e-1)m)}$. Using Corollary 4.1 and setting $c_5 = c_\delta c_6^{me(e-1)}$, $T_1 = (T_0/c_6)^{2e(e-1)m}$ we conclude

$$N_\Delta(T) \geq N_\delta(c_6 T^{1/(2e(e-1)m)}) \geq c_5 T^{1/2}$$

provided $T \geq T_1$. □

Ellenberg and Venkatesh's Theorem 1.1 in [**14**] shows that the exponent $1/2$ in Corollary 4.2 can be replaced by $1/2 + 1/e^2$ and Linnik's Conjecture implies that it can be replaced even by 1. Although Linnik's Conjecture is known only for $e \leq 3$ the following argument, mentioned by Ellenberg and Venkatesh (see [**14**] p. 723), shows that for e even the exponent $1/2$ can always be increased to 1. So suppose e is even and let F be an extension of k of relative degree $e/2$. For degree 2 Linnik's Conjecture is true and thus $|\{K \subseteq \overline{F}; [K:F] = 2, |\Delta_K| \leq T\}| = c_7 T + o(T)$ where the positive constant c_7 and the implied constant in o depend only on F. This shows that $N_\Delta(T) \geq (c_7/2)T$ for $T > T_2(F)$ and since F was an arbitrary extension of k of degree $e/2$ we can choose even $c_7 = c_7(k,e)$ and $T_2 = T_2(k,e)$ depending only on k, e, for example $T_2 = \inf_{[F:k]=e/2} T_2(F) + 1$ and then $c_7 = 1/2 \sup_{[F:k]=e/2, T_2(F) \leq T_2} c_7(F)$. Linnik's Conjecture is also true for degree 3. Thus the same argument can be used if 3 divides e.

What about upper bounds for $N_\Delta(T)$? From (4.3.35) we know that there is a positive constant $c_8 = c_8(d)$ depending only on $d = em$ such that

$$\delta(K/k) \leq c_8 |\Delta_K|^{\frac{1}{em}}.$$

Thus we get

$$N_\Delta(T) \leq N_\delta(c_8 T^{\frac{1}{em}}) \leq C_\delta c_8^{me(e+1)} T^{e+1}$$

for $T > 0$. This bound is far from Schmidt's bound (4.3.24) and so of no relevance.

CHAPTER 5

One-dimensional subspaces of fixed degree

In this chapter we apply the Main Theorem to prove a counting result for points of fixed degree on linear projective varieties. The special case of degree one is a well-known Theorem of Thunder. As usual k will denote a number field and we fix an algebraic closure $\overline{k}$ of k. We recall that finite extensions of k are assumed to lie in $\overline{k}$.

1. Introduction and results

Let N, M be positive integers and let

$$\begin{array}{rl} a_{11}x_1 + a_{12}x_2 + ... + a_{1N}x_N & = 0 \\ \vdots & \vdots \\ a_{M1}x_1 + a_{M2}x_2 + ... + a_{MN}x_N & = 0 \end{array} \tag{5.1.1}$$

be a system of $M < N$ linearly independent linear homogeneous equations defined over a number field k. In Transcendence theory or Diophantine approximation one often needs to know the existence of non-trivial solutions to (5.1.1), which are small in an appropriate sense. These problems have been investigated by many people (Thue [**55**], Siegel [**52**], Bombieri and Vaaler [**4**], Roy and Thunder [**39**], [**40**], Thunder [**60**] and many others) and are usually associated with the name "Siegel's Lemma". In contrast to that one could ask how many large solutions does one have. The quantification of the size will be done via the concept of heights. Any non-zero multiple of a non-trivial solution $\mathbf{x}$ is again a non-trivial solution but not essentially different and so we do consider it as the same solution. To measure the size of a solution $\mathbf{x} = (x_1, ..., x_N)$ we use a projective height so that the size does not depend on the choice of the representative $\mathbf{x}$. It will turn out that the l^2-height H_2 is in this set up slightly more natural than the Weil height.

From Subsection 1.1 and Subsection 1.2 Chapter 4 we know that

$$H_2(\mathbf{x}) = \prod_{v|\infty}(|\sigma_v(x_1)|_v^2 + ... + |\sigma_v(x_N)|_v^2)^{d_v/d} \prod_{v\nmid\infty} \max\{|\sigma_v(x_1)|_v, ..., |\sigma_v(x_N)|_v\}^{d_v/d} \tag{5.1.2}$$

where K is any number field containing the coordinates, the v's run over M_K and $[K:\mathbb{Q}] = d$. Furthermore we know that this is a projective height and thus defined on $\mathbb{P}^{N-1}(\overline{k})$.

To get finiteness for the number of pairwise non-proportional solutions of bounded height we have to impose further restrictions. It suffices to demand that $[k((x_1 : ... : x_N)) : k] \leq e$ where $k((x_1 : ... : x_N) = k(..., x_i/x_j, ..)$; $1 \leq i, j \leq N, x_j \neq 0$ and e is an arbitrary but fixed natural number. Now we can state our problem a little bit more precisely. Can one give the asymptotics as X tends to infinity for the number of projective points $(x_1 : ... : x_N)$ in $\mathbb{P}^{N-1}(k; e)$ with $\mathbf{x}$ satisfying (5.1.1) and $H_2(\mathbf{x}) \leq X$? Now of course it makes sense to assume $N > M + 1$.

A related problem comes from an early work [**46**] of Schmidt where he gave asymptotic estimates for the number of subspaces of $\mathbb{Q}^N$ of arbitrary but fixed dimension and bounded height. This result was generalized to the affine space over arbitrary number fields by Thunder in [**56**] (see also [**57**] for a further generalization). The relation becomes clearer using a more intrinsic formulation of our counting problem by considering the $(N-M)$-dimensional $\overline{k}$-vector space, say S, defined by (5.1.1), namely: count the one-dimensional subspaces $\overline{k}\mathbf{x}$ of S of fixed degree over k with $H_2(\mathbf{x}) \leq X$.

One would expect that complicated vector spaces do not have many simple one-dimensional subspaces but what exactly do complicated and simple mean here? A vector space defined over a number field k has also a height, which in the case of a one-dimensional space reduces just to the height above and it can be interpreted as a measure for the complexity of the space. So let S be a subspace of $\overline{k}^N$ of dimension $n+1$ over $\overline{k}$ and let $v_1, ..., v_{n+1}$ be a basis of S over $\overline{k}$. We form the wedge-product ([**47**] paragraph 5)

$$v_1 \wedge ... \wedge v_{n+1} \in \overline{k}^{\binom{N}{n+1}}. \tag{5.1.3}$$

Since the vectors are linearly independent it is non-zero ([**47**] Lemma 5C). Let $v'_1, ..., v'_{n+1}$ be linearly independent vectors in $\overline{k}^N$ then $v_1 \wedge ... \wedge v_{n+1}$ is proportional to $v'_1 \wedge ... \wedge v'_{n+1}$ if and only if $v'_1, ..., v'_{n+1}$ and $v_1, ..., v_{n+1}$ span the same space ([**47**] p.14 Lemma 5D). Hence we may define

$$H_2(S) = H_2(v_1 \wedge ... \wedge v_{n+1}).$$

Moreover we set

$$H_2(\{\mathbf{0}\}) = H_2(\overline{k}^N) = 1.$$

The wedge product in (5.1.3) is called a tuple of Grassmann coordinates for S. Up to a non-zero scalar multiple and permutations of the coordinates such a tuple is determined by S.

We may avoid the wedge product by the following equivalent definition using the matrix A of (5.1.1) with entries a_{ij} $(1 \leq i \leq M, 1 \leq j \leq N)$. We denote by A_0 the various maximal minors of A. Let K be any number field containing k. Then with v as in (5.1.2)

$$H^{fin}(A) = \prod_{v \nmid \infty} \max_{A_0} |\sigma_v(\det A_0)|_v^{\frac{d_v}{d}},$$

$$H^{inf}(A) = \prod_{v|\infty} (\sum_{A_0} |\sigma_v(\det A_0)|_v^2)^{\frac{d_v}{2d}}$$

and as always $d = [K : \mathbb{Q}]$ and $d_v = [K_v : \mathbb{Q}_v]$. Using an analogue of the Cauchy-Binet formula over number fields one can prove (see [**4**] p.15 (iv)) that

$$H^{inf}(A) = \prod_{v|\infty} |\det(\sigma_v(A)\overline{\sigma_v(A)}^t)|_v^{\frac{d_v}{2d}} \tag{5.1.4}$$

where over-line means complex conjugation, $\overline{\sigma_v(A)}^t$ is the transpose of $\overline{\sigma_v(A)}$ and σ_v acts on each entry. Multiplying the finite and infinite parts yields the height of the matrix

$$H_2(A) = H^{fin}(A)H^{inf}(A).$$

Notice that a tuple of determinants of all maximal minors is a tuple of Grassmann coordinates of S. Hence $H_2(A)$ is nothing else than $H_2(S)$.

Now let us return to the counting problem for one-dimensional subspaces. Besides the special cases covered directly by Schanuel's Theorem (with a slightly different choice of the height) Thunder was the first who gave answers to the problem. His Theorem 1 in [**58**] settles

the case where $e = 1$. We give a generalization of Thunder's Theorem 1 [**58**] by counting one-dimensional subspaces of "small" relative degree over k. Let us recall what we mean by the degree of a one-dimensional subspace of S. Choose a one-dimensional subspace $\overline{k}\mathbf{x}$ where $\mathbf{x} = (x_1, ..., x_N)$. We define the degree of $\overline{k}\mathbf{x}$ over k simply as the degree of the projective point $(x_1 : ... : x_N)$ over k. Hence we may fix a natural number say e and ask for the number of one-dimensional subspaces $\overline{k}\mathbf{x}$ of S with degree e over k and $H_2(\mathbf{x}) \leq X$.

We choose a slightly different formulation, which is more appropriate in the context of the work of Franke, Manin, Tschinkel [**20**], Peyre [**38**], Salberger, Thunder [**57**] and many others. These authors usually take a projective variety $\mathbb{X}$ (of a very special type) defined over $\mathbb{Q}$ or k and then count points of bounded height in $\mathbb{X}(\mathbb{Q})$ or $\mathbb{X}(k)$. Let us point out that any variety defined over k has a Zariski-dense set of points over $\overline{k}$ of sufficiently large degree, whereas the points over $\mathbb{Q}$ or k are necessarily restricted via diophantine constraints like Faltings's Theorem (see [**16**]) or the various conjectural generalizations.

So suppose $N > M + 1$ and let $\mathbb{V}$ be a linear subvariety of $\mathbb{P}^{N-1}$ of dimension $N - M - 1$ and defined over k. Then there are coefficients $a_{11}, ..., a_{MN}$ in k such that $\mathbb{V}$ is the set of $(x_1 : ... : x_N)$ in $\mathbb{P}^{N-1}$ with $\mathbf{x} = (x_1, ..., x_N)$ solving the system (5.1.1). Let $S \subseteq \overline{k}^N$ be the vector space defined by the same system (5.1.1), so that $(x_1 : ... : x_N)$ lies in $\mathbb{V}$ if and only if $(x_1, ..., x_N)$ lies in $S\backslash\{\mathbf{0}\}$. Then we define of course $H_2(\mathbb{V}) = H_2(S)$. Moreover we define

$$\mathbb{V}(k; e) = \mathbb{P}^{N-1}(k; e) \cap \mathbb{V}(\overline{k}). \tag{5.1.5}$$

Denote by $Z_{H_2}(\mathbb{V}(k; e), X)$ the associated counting function abbreviated to $Z_2(\mathbb{V}(k; e), X)$ so that

$$Z_2(\mathbb{V}(k; e), X) = |\{P \in \mathbb{V}(k; e); H_2(P) \leq X\}. \tag{5.1.6}$$

For a number field k and natural numbers e, n we define the sum

(5.1.7)
$$\alpha = \alpha(k, e, n) = \sum_K (2^{-r_K}\pi^{-s_K})^{n+1} V(n+1)^{r_K} V(2n+2)^{s_K} S_K(n)$$

where the sum runs over all extensions of k with relative degree e and $V(p)$ denotes the volume of the euclidean ball in $\mathbb{R}^p$ with radius one. As in Chapter 4, we will shortly see that this sum sometimes converges. The main result of this chapter is Theorem 5.1.

THEOREM 5.1. *Let k be a number field of degree m, let n, e and $N \geq n+2$ be natural numbers, and let $\mathbb{V}$ be a linear subvariety of $\mathbb{P}^{N-1}$ of dimension n defined over k. Suppose that either $e = 1$ or*

$$n > 5e/2 + 4 + 2/(me).$$

Then the sum in (5.1.7) converges and as $X > 0$ tends to infinity we have

$$Z_2(\mathbb{V}(k;e), X) = \alpha H_2(\mathbb{V})^{-me} X^{me(n+1)} + O(X^{me(n+1)-1}\mathfrak{L}_0).$$

Here $\mathfrak{L}_0 = \log\max\{2, 2X\}$ if $(me, n) = (1, 1)$ and $\mathfrak{L}_0 = 1$ otherwise, and the constant in O depends only on k, e, n.

Note that the error term does not depend on the variety $\mathbb{V}$. This may be found surprising, especially because the proof of the result involves an Arakelov-Lipschitz systems $\mathcal{N} = \mathcal{N}(\mathbb{V})$ which does depend on $\mathbb{V}$.

Let us compare the number of points on $\mathbb{V}$ as counted in Theorem 5.1 with the quantity $Z = Z_{H_2}(\mathbb{P}^n(k;e), X)$. From Subsection 1.1 and Subsection 1.2 in Chapter 4, each time right at the end, we already know that there is a uniform *ALS* $\mathcal{N}$ (of dimension n) on $\mathcal{C}_e(k)$ such that $H_2 = H_{\mathcal{N}}$ on $\mathbb{P}^n(k;e)$. Hence we can use the Main Theorem part (b) to get the asymptotics for Z. Right after (4.2.2) we verified that $V_{\mathcal{N}}^{fin} = 1$ if N_v is the max-norm for all finite places and it is not difficult to see that $V_{\mathcal{N}}^{inf} = V(n+1)^r V(2n+2)^s$ (see also [**34**] p.432). Thus $Z = \alpha X^{me(n+1)} + O(X^{me(n+1)-1}\mathfrak{L})$. So whenever $e = 1$ or $n > 5e/2 + 4 + 2/(me)$ we find that the number of points in $\mathbb{V}(\overline{k})$ of degree e over k and l^2-height $\leq X$ is asymptotically $H_2(\mathbb{V})^{-me} Z_{H_2}(\mathbb{P}^n(k;e), X)$.

Next we look once more at the example of Subsection 1.1 Chapter 3. Here $\mathbb{V}$ was given by the equation $2x_1 + 3x_2 + 5x_3 = 0$ and we get $H_2(\mathbb{V}) = \sqrt{38}$. The constant α is $2^{-2}V(2)S_{\mathbb{Q}}(1) = 3/\pi$. So we have asymptotically

$$\frac{3}{\pi\sqrt{38}} X^2 + O(X \log X)$$

rational points on this projective variety. The example above (and much more) is already covered by Thunder's result. In fact the remark at the end of Section 2 of Chapter 4 means that we could probably obtain the asymptotics for counting points of fixed degree over any k despite $n = 1$ being so small; and this even for arbitrary lines in $\mathbb{P}^{N-1}$.

The novelty in Theorem 5.1 is that we can count also points of fixed degree provided the dimension is much larger than the degree. What about the simple equation

$$x_1 + x_2 + x_3 + x_4 + x_5 + x_6 + x_7 + x_8 + x_9 + x_{10} + x_{11} + x_{12} + x_{13} = 0$$

defined over $\mathbb{Q}$? We compute $H_2(\mathbb{V}) = \sqrt{13}$. Using the formula $V(p) = \pi^{p/2}/\Gamma(p/2+1)$ for $p = n+1$ and $p = 2n+2$ where $n+1 = N - M = 13 - 1 = 12$ we obtain: there are

$$\frac{1}{13}\left(\sum_{\substack{K \\ [K:\mathbb{Q}]=2}} (\frac{\pi^6}{2949120})^{r_K} (\frac{1}{479001600})^{s_K} S_K(11)\right) X^{24} + O(X^{23})$$

pairwise non-proportional solutions of degree 2 over $\mathbb{Q}$ with height less or equal X.

Next consider the equation

$$\begin{aligned} x_1 + 2x_2 + 3x_3 + 4x_4 + 5x_5 + 6x_6 + 7x_7 \\ +8x_8 + 9x_9 + 10x_{10} + 11x_{11} + 12x_{12} + 13x_{13} = 0 \end{aligned}$$

defined over $\mathbb{Q}$. Here we have

$$\frac{1}{819}\left(\sum_{\substack{K \\ [K:\mathbb{Q}]=2}} (\frac{\pi^6}{2949120})^{r_K} (\frac{1}{479001600})^{s_K} S_K(11)\right) X^{24} + O(X^{23})$$

pairwise non-proportional solutions of degree 2 over $\mathbb{Q}$ with height less or equal X.

If we increase the ground field k then we can sometimes even decrease the number of variables. Here is an example actually with rather a large field:

$$\begin{aligned} \sqrt{1}x_1 + \sqrt{2}x_2 + \sqrt{3}x_3 + \sqrt{4}x_4 + \sqrt{5}x_5 + \sqrt{5}x_6 \\ +\sqrt{7}x_7 + \sqrt{8}x_8 + \sqrt{9}x_9 + \sqrt{10}x_{10} + \sqrt{11}x_{11} + \sqrt{12}x_{12} = 0 \end{aligned}$$

defined over the field

$$\begin{aligned} k &= \mathbb{Q}(\sqrt{1}, \sqrt{2}, \sqrt{3}, \sqrt{4}, \sqrt{5}, \sqrt{6}, \sqrt{7}, \sqrt{8}, \sqrt{9}, \sqrt{10}, \sqrt{11}, \sqrt{12}) \\ &= \mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5}, \sqrt{7}, \sqrt{11}). \end{aligned}$$

So we have $m = [k : \mathbb{Q}] = 32$. We find $H_2(\mathbb{V}) = \sqrt{78}$ and setting $e = 2$ we get $H_2(\mathbb{V})^{-me} = 78^{-32}$. As in the previous example we find

$$\frac{1}{78^{32}} \left(\sum_{\substack{K \\ [K:k]=2}} (\frac{\pi^5}{332640})^{r_K} (\frac{1}{39916800})^{s_K} S_K(10) \right) X^{704} + O(X^{703})$$

pairwise non-proportional solutions of degree 2 over k with height less or equal X.

Actually there is no problem to obtain similar results using the l^∞-height H on $\mathbb{V}(k; e)$. For example with rational points on $2x_1 + 3x_2 + 5x_3 = 0$ as above we get a main term $12/(5\pi)^2 X^2$. But already the volume computations for $x_1 + ... + x_{13} = 0$ are more intricate, and in general the dependence on $\mathbb{V}$ will probably not be expressible as any recognizable height function of $\mathbb{V}$.

2. A reformulation of Theorem 5.1

Suppose

$$1 \leq M \leq N - 2. \tag{5.2.1}$$

Set $n = N - M - 1$ so that

$$n = N - M - 1 \geq 1. \tag{5.2.2}$$

Let $\mathbb{V} \subseteq \mathbb{P}^{N-1}$ be a linear subvariety of dimension n and defined over k. Then there are coefficients $a_{11}, ..., a_{MN}$ in k such that a system as in (5.1.1) of M linearly independent equations defines $\mathbb{V}$. Let S be the $\overline{k}$-vector space defined by the same system, so that $(x_1 : ... : x_N)$ lies in $\mathbb{V}(\overline{k})$ if and only if $(x_1, ..., x_N)$ lies in $S \backslash \{\mathbf{0}\}$. Thus the dimension of the vector space S (over $\overline{k}$) is $n + 1$. Since S is defined over k, there are (homogeneous) linear forms $L_1, ..., L_N$ in $k[\mathbf{z}]$ such that there is a $(1 : 1)$-correspondence between $\overline{k}^{n+1}$ and S given by

$$\mathbf{z}^t = (z_0, ..., z_n) \longleftrightarrow (L_1(\mathbf{z}), ..., L_N(\mathbf{z})). \tag{5.2.3}$$

Now (5.2.3) implies a $(1 : 1)$-correspondence between the sets $\mathbb{P}^n(\overline{k})$ and $\mathbb{V}(\overline{k})$

$$(z_0 : ... : z_n) \longleftrightarrow (L_1(\mathbf{z}) : ... : L_N(\mathbf{z})). \tag{5.2.4}$$

If we permute the coordinates in $(L_1(\mathbf{z}) : ... : L_N(\mathbf{z}))$ we will probably no longer parameterize $\mathbb{V}$ but we will parameterize a linear subvariety

with the same number of points of fixed degree and bounded height. Therefore we may assume

$$L_j(\mathbf{z}) = z_{j-1} \quad \text{for } 1 \leq j \leq n+1. \tag{5.2.5}$$

LEMMA 5.1. *The counting function* $Z_2(\mathbb{V}(k;e), X)$ *is given by the number of*

$$(z_0 : ... : z_n) \in \mathbb{P}^n(k;e)$$

with

$$H_2((L_1(\mathbf{z}) : ... : L_N(\mathbf{z}))) \leq X.$$

Proof. By (5.2.4) we see that $Z_2(\mathbb{V}(k;e), X)$ is the number of projective points $(z_0 : ... : z_n)$ in $\mathbb{P}^n(\overline{k})$ with

$$[k((L_1(\mathbf{z}) : ... : L_N(\mathbf{z}))) : k] = e \tag{5.2.6}$$

$$H_2((L_1(\mathbf{z}) : ... : L_N(\mathbf{z}))) \leq X. \tag{5.2.7}$$

Moreover the linear forms L_j have coefficients in k. By (5.2.5) we see that

$$k((L_1(\mathbf{z}) : ... : L_N(\mathbf{z}))) = k((z_0 : ... : z_n)).$$

So the number of points of $\mathbb{V}$ of degree e over k and with l^2-height not exceeding X is the number of $(z_0 : ... : z_n) \in \mathbb{P}^n(k;e)$ with $H_2(L_1(\mathbf{z}) : ... : L_N(\mathbf{z})) \leq X$. □

2.1. The corresponding Arakelov-Lipschitz system. The previous lemma shows that we shall count $(z_0 : ... : z_n) \in \mathbb{P}^n(k;e)$ with $H_2(L_1(\mathbf{z}) : ... : L_N(\mathbf{z})) \leq X$. The strategy is to choose a uniform ALS $\mathcal{N}$ on $\mathcal{C}_e = \mathcal{C}_e(k)$ of dimension n to obtain

$$H_{\mathcal{N}}(\mathbf{z}) = H_2(L_1(\mathbf{z}) : ... : L_N(\mathbf{z})). \tag{5.2.8}$$

We define $\mathcal{N}$ as follows: for each K of $\mathcal{C}_e$ we define an ALS $\mathcal{N}_K$ on K (of dimension n) by

$$N_v(\mathbf{z}) = \max\{|(\sigma_v L_1)(\mathbf{z})|_v, ..., |(\sigma_v L_N)(\mathbf{z})|_v\} : v \nmid \infty \tag{5.2.9}$$

$$N_v(\mathbf{z}) = \sqrt{|(\sigma_v L_1)(\mathbf{z})|_v^2 + ... + |(\sigma_v L_N)(\mathbf{z})|_v^2} \ : v \mid \infty. \tag{5.2.10}$$

Here σ_v acts on the coefficients of the linear forms L_i. With this definition of $\mathcal{N}$, and having (4.1.2) and (4.1.3) in mind, we see that equation (5.2.8) holds. For $v \nmid \infty$ the ultrametric inequality $|(\sigma_v L_1)(\mathbf{z}_1 + \mathbf{z}_2)|_v \leq \max\{|(\sigma_v L_1)(\mathbf{z}_1)|_v, |(\sigma_v L_1)(\mathbf{z}_2)|_v\}$ implies that condition (*iii*) of Subsection 1.2 Chapter 3 is satisfied. For $v \mid \infty$ it is not so obvious that (*iii*) holds and we postpone the proof. But let us describe the set

$\mathbf{B}_v = \{\mathbf{z}; N_v(\mathbf{z}) < 1\}$ and its boundary $\partial\mathbf{B}_v = \{\mathbf{z}; N_v(\mathbf{z}) = 1\}$. We write

$$b_v(\mathbf{z}, \mathbf{z}') = (\sigma_v L_1)(\mathbf{z})\overline{(\sigma_v L_1)(\mathbf{z}')} + ... + (\sigma_v L_N)(\mathbf{z})\overline{(\sigma_v L_N)(\mathbf{z}')}.$$

Let $e_1, ..., e_{n+1}$ be the canonical basis of $\mathbb{R}^{n+1}$ if v is real and of $\mathbb{C}^{n+1}$ if v is non-real. Let $Q = Q_v$ be the matrix with entries q_{ij} $(1 \leq i, j \leq n+1)$ where

$$q_{ij} = b_v(e_i, e_j).$$

At this stage where matrices enter the game we should point out that $\mathbf{z}$ is a column. Using the definition (5.2.10) of $N_v(\cdot)$ we see that

$$N_v(\mathbf{z})^2 = \sum_{j=1}^{N}\sum_{r=0}^{n}\sum_{p=0}^{n} z_r\overline{z_p}(\sigma_v L_j)(e_{r+1})\overline{(\sigma_v L_j)(e_{p+1})} = \overline{\mathbf{z}}^t Q\mathbf{z}.$$

Thus $\mathbf{B}_v = \{\mathbf{z}; \overline{\mathbf{z}}^t Q\mathbf{z} < 1\}$ and $\partial\mathbf{B}_v = \{\mathbf{z}; \overline{\mathbf{z}}^t Q\mathbf{z} = 1\}$. In fact we need that $\mathcal{N}$ defines even a uniform ALS on $\mathcal{C}_e$. This will be verified in the next subsection.

Now notice that according to our choice of $L_1, ..., L_N$

$$\begin{aligned}(5.2.11)\qquad b_v(\mathbf{z}, \mathbf{z}') &= z_0\overline{z_0'} + ... + z_n\overline{z_n'} \\ &+ (\sigma_v L_{n+1})(\mathbf{z})\overline{(\sigma_v L_{n+1})(\mathbf{z}')} + ... + (\sigma_v L_N)(\mathbf{z})\overline{(\sigma_v L_N)(\mathbf{z}')}.\end{aligned}$$

Equation (5.2.11) shows that $Q = E + R$ where E is the identity matrix and R is a hermitian positive semidefinite matrix. Hence all the eigenvalues of R are non-negative reals. There is a unitary matrix U with $\overline{U}^t J'U = R$ for a diagonal matrix J' whose diagonal entries are the eigenvalues of R. Now $\overline{U}^t(J' + E)U = Q$ and so the eigenvalues of Q are real numbers of size at least 1.

2.2. $\mathcal{N}$ is a uniform Arakelov-Lipschitz system. Suppose v is infinite then we just have seen that $Q = Q_v$ is a positive definite matrix so that N_v is a norm on K_v^{n+1}. We could apply the observation in Remark 4 Chapter 3 to deduce that $\partial\mathbf{B}_v$ is Lipschitz parameterizable. But Remark 4 refers to Appendix A and so in order not to distract the reader too much it is convenient to give a direct proof here. More precisely we will show that $\partial\mathbf{B}_v$ lies in $\mathrm{Lip}(d_v(n+1), 1, 1, 2\pi d_v(n+1))$. But first we need a simple lemma.

LEMMA 5.2. *Suppose $p > 1$. Then the $(p-1)$-dimensional unit sphere $\partial B_0(1)$ lies in $Lip(p, 1, 1, 2\pi p)$*

Proof. Let

$$\varphi : [0, 2\pi] \times [0, \pi]^{p-2} \longrightarrow \partial B_0(1)$$

be the standard parameterization of $\partial B_0(1)$ via polar coordinates $\boldsymbol{\theta} = (\theta_1, ..., \theta_{p-1})$ such that

$$\begin{aligned} x_1 &= \cos\theta_1 \cos\theta_2 \cos\theta_3 ... \cos\theta_{p-1} \\ x_2 &= \sin\theta_1 \cos\theta_2 \cos\theta_3 ... \cos\theta_{p-1} \\ x_3 &= \quad \sin\theta_2 \cos\theta_3 ... \cos\theta_{p-1} \\ &\vdots \\ x_p &= \quad \sin\theta_{p-1}. \end{aligned}$$

Using the max-norm $|\cdot|_\infty$ we have $|\partial x_i/\partial\theta_j|_\infty \leq 1$ for $1 \leq i \leq p$ and $1 \leq j \leq p-1$. Applying the Mean-Value Theorem we get $|\varphi(\boldsymbol{\theta}) - \varphi(\boldsymbol{\theta'})| \leq \sqrt{p(p-1)}|\boldsymbol{\theta} - \boldsymbol{\theta'}| \leq p|\boldsymbol{\theta} - \boldsymbol{\theta'}|$. Now normalizing to get a map as in (1.1.1) with parameter domain $[0, 1]^{p-1}$ gives an additional factor 2π and thereby proves the lemma. □

In Appendix A we generalize (up to a slightly different Lipschitz constant) the previous lemma to boundaries of arbitrary bounded convex sets. However with Lemma 5.2 we can prove

LEMMA 5.3. *Suppose $v \mid \infty$. Then the set $\partial\mathbf{B}_v = \{\mathbf{z}; N_v(\mathbf{z}) = 1\}$ lies in Lip$(d_v(n+1), 1, 1, 2\pi d_v(n+1))$.*

Proof. The set $\partial\mathbf{B}_v$ is given by the condition $\overline{\mathbf{z}}^t Q\mathbf{z} = 1$. Since Q is hermitian there is a unitary matrix U with $\overline{U}^t JU = Q$ for a diagonal matrix J where the diagonal entries, say $\lambda_0, ..., \lambda_n$, are the eigenvalues of Q and we have already seen that they are at least 1. Set $\mathbf{y} = U\mathbf{z}$. Then $\partial\mathbf{B}_v = \{\overline{U}^t\mathbf{y}; \overline{\mathbf{y}}^t J\mathbf{y} = 1\} = \overline{U}^t\{\mathbf{y}; \overline{\mathbf{y}}^t J\mathbf{y} = 1\}$. Now $|\overline{U}^t(\mathbf{y}) - \overline{U}^t(\mathbf{y}')| = |\mathbf{y} - \mathbf{y}'|$ so it suffices to check that $\{\mathbf{y}; \overline{\mathbf{y}}^t J\mathbf{y} = 1\}$ lies in Lip$(d_v(n+1), 1, 1, 2\pi d_v(n+1))$. But the latter set is the image of the unit sphere in $K_v^{n+1} = \mathbb{R}^{d_v(n+1)}$ centered at the origin under the K_v^{n+1}-endomorphism say ϕ, defined by

$$\phi((w_0, ..., w_n)) = (\lambda_0^{-1/2} w_0, ..., \lambda_n^{-1/2} w_n).$$

By the previous lemma we know already that the unit sphere lies in Lip$(d_v(n+1), 1, 1, 2\pi d_v(n+1))$. So let φ be the corresponding parameterizing map of the sphere then $\phi(\varphi)$ is a parameterization of

$\{\mathbf{y}; \overline{\mathbf{y}}^t J\mathbf{y} = 1\}$. We compute a Lipschitz constant

$$\begin{aligned}|\phi(\varphi(\mathbf{t})) - \phi(\varphi(\mathbf{t}'))| &= |\phi(\varphi(\mathbf{t}) - \varphi(\mathbf{t}'))| \\ &\leq \sup_{|\boldsymbol{w}|=1} |\phi(\boldsymbol{w})||\varphi(\mathbf{t}) - \varphi(\mathbf{t}')| \\ &= \sup_{|\boldsymbol{w}|=1} (\sum_{i=0}^{n} \frac{|w_i|^2}{\lambda_i})^{1/2} |\varphi(\mathbf{t}) - \varphi(\mathbf{t}')|.\end{aligned}$$

Since $\lambda_i \geq 1$ $(0 \leq i \leq n)$ we deduce the estimates

$$\begin{aligned}&\leq \sup_{|\boldsymbol{w}|=1} (\sum_{i=0}^{n} |w_i|^2)^{1/2} |\varphi(\mathbf{t}) - \varphi(\mathbf{t}')| \\ &= |\varphi(\mathbf{t}) - \varphi(\mathbf{t}')| \\ &\leq 2\pi d_v(n+1)|\mathbf{t} - \mathbf{t}'|.\end{aligned}$$

□

We write

$$\begin{aligned}C_{\mathcal{N}} &= 1, \\ M_{\mathcal{N}} &= 1, \\ L_{\mathcal{N}} &= 4\pi(n+1).\end{aligned}$$

LEMMA 5.4. *The system $\mathcal{N}$ defines a uniform ALS on $\mathcal{C}_e$ of dimension n with associated constants $C_{\mathcal{N}}, M_{\mathcal{N}}, L_{\mathcal{N}}$.*

Proof. Let $\mathcal{N}_K$ be an *ALS* of the collection $\mathcal{N}$. For non-archimedean v in M_K we have

$$\begin{aligned}N_v(\mathbf{z}) &= \max\{|(\sigma_v L_1)(\mathbf{z})|_v, ..., |(\sigma_v L_N)(\mathbf{z})|_v\} \\ &\geq \max\{|(\sigma_v L_1)(\mathbf{z})|_v, ..., |(\sigma_v L_{n+1})(\mathbf{z})|_v\} \\ &= \max\{|z_0|_v, ..., |z_n|_v\}.\end{aligned}$$

The l^2-norm is at least as big as the max-norm and so we get also for v archimedean

$$N_v(\mathbf{z}) \geq \max\{|z_0|_v, ..., |z_n|_v\}.$$

So for the finite part we may choose according to (3.1.3) and (3.1.4)

$$C_{\mathcal{N}_K}^{fin} = 1.$$

For the infinite part we get according to (3.1.5)

$$C_{\mathcal{N}_K}^{inf} = 1.$$

Combining both parts we end up with

$$C_{\mathcal{N}_K} = C_{\mathcal{N}_K}^{fin} C_{\mathcal{N}_K}^{inf} = 1 = C_{\mathcal{N}}.$$

Lemma 5.3 implies that the sets $\partial\mathbf{B}_v = \{\mathbf{z}; N_v(\mathbf{z}) = 1\}$ lie in $\mathrm{Lip}(d_v(n+1), 1, 1, 4\pi(n+1))$ and thus we may choose $M_{\mathcal{N}_K} = 1, L_{\mathcal{N}_K} = 4\pi(n+1)$. This shows that $\mathcal{N}$ is a uniform ALS of dimension n on $\mathcal{C}_e$ with associated constants $C_{\mathcal{N}} = 1$, $M_{\mathcal{N}} = 1$, $L_{\mathcal{N}} = 4\pi(n+1)$. □

3. Proof of Theorem 5.1

We have a uniform ALS $\mathcal{N}$ of dimension n on $\mathcal{C}_e$ with

$$H_{\mathcal{N}}((z_0 : ... : z_n)) = H_{\mathcal{N}}(\mathbf{z}) = H_2((L_1(\mathbf{z}) : ... : L_N(\mathbf{z}))).$$

By Lemma 5.1 we conclude that $Z_2(\mathbb{V}(k;e), X)$ is given by the number of $(z_0 : ... : z_n)$ in $\mathbb{P}^n(k;e)$ with $H_{\mathcal{N}}((z_0 : ... : z_n)) \leq X$, which we denote by $Z_{\mathcal{N}}(\mathbb{P}^n(k;e), X)$. Furthermore we have the hypothesis $e = 1$ or $n > 5e/2 + 4 + 2/(me)$ in Theorem 5.1. This is exactly the situation where we can apply the Main Theorem part (b) from Chapter 4. So we find

$$Z_{\mathcal{N}}(\mathbb{P}^n(k;e), X) = \sum_{\substack{K \\ [K:k]=e}} 2^{-r_K(n+1)}\pi^{-s_K(n+1)}V_{\mathcal{N}_K}S_K(n)X^{me(n+1)} + O(A_{\mathcal{N}}X^{me(n+1)-1}\mathfrak{L}),$$

where $A_{\mathcal{N}} = M_{\mathcal{N}}^{me}(C_{\mathcal{N}}(L_{\mathcal{N}}+1))^{me(n+1)-1}$ with

$$C_{\mathcal{N}} = 1, \quad M_{\mathcal{N}} = 1, \quad L_{\mathcal{N}} = 4\pi(n+1)$$

and $\mathfrak{L} = \log\max\{2, 2C_{\mathcal{N}}X\}$ if $(me, n) = (1, 1)$ and $\mathfrak{L} = 1$ otherwise. Moreover the constant in O depends only on k, e, n. Thus

$$A_{\mathcal{N}} = (4\pi(n+1)+1)^{me(n+1)-1}$$

depends only on m, e, n. All that remains is to compare the main terms. Therefore we are finished once we have shown that

$$V_{\mathcal{N}_K} = \frac{V(n+1)^{r_K}V(2n+2)^{s_K}}{H_2(S)^d}. \tag{5.3.1}$$

At this point we make a simple but crucial remark. Recall the general Definition 3.1 of Chapter 3. Given a positive rational number l and a ALS $\mathcal{N}$ we can define a new ALS $l\mathcal{N}$ by changing each N_v to $|\sigma_v(l)|_v N_v$. However the volume $V_{l\mathcal{N}} = V_{\mathcal{N}}$ is independent of l. This can be computationally verified from the definitions using the product formula. More intuitively it is clear that the height $H_{l\mathcal{N}} = H_{\mathcal{N}}$ is independent of l, and since $V_{l\mathcal{N}}, V_{\mathcal{N}}$ occur in their respective counting functions, their equality follows.

For the purposes of evaluating $V_{\mathcal{N}_K}$ in (5.3.1) we are therefore entitled to use $l\mathcal{N}$. Note that changing $\mathcal{N}$ into $l\mathcal{N}$ (with a positive rational

number l) changes $L_1, ..., L_N$ from (5.2.9) into $lL_1, ..., lL_N$. We choose a positive rational integer l such that $lL_1, ..., lL_N$ have coefficients in $\mathcal{O}_K$. In order to keep the notation simple we will redefine $\mathcal{N}_K$ as $l\mathcal{N}_K$ and $L_1, ..., L_N$ as $lL_1, ..., lL_N$; this will cause no confusion. So from (5.2.5) we get

$$L_j(\mathbf{z}) = lz_{j-1} \quad \text{for } 1 \leq j \leq n+1. \tag{5.3.2}$$

And clearly

$$\mathbf{z}^t = (z_0, ..., z_n) \longleftrightarrow (L_1(\mathbf{z}), ..., L_N(\mathbf{z})) \tag{5.3.3}$$

remains a $(1:1)$-correspondence between $\overline{k}^{n+1}$ and S. For the rest of this chapter $\mathcal{N}_K$ will be fixed. Therefore it is convenient to drop the index and simply write $\mathcal{N}$.

Recall from the definition that $V_{\mathcal{N}}$ splits into a finite and an infinite part. Let $S^{\perp}$ be the orthogonal complement of S consisting of all $\mathbf{y} \in \overline{k}^N$ with $\mathbf{x}^t\mathbf{y} = x_1y_1 + ... + x_Ny_N = 0$ for all $\mathbf{x}$ in S or equivalently $(L_1(\mathbf{z}), ..., L_N(\mathbf{z}))\mathbf{y} = 0$ for all $\mathbf{z}$ in $\overline{k}^{n+1}$. Let $A^{\perp}$ be the $(N-M) \times N$ matrix with columns formed by the coefficients of $L_1, ..., L_N$. Writing $L_r(\mathbf{z}) = \sum_{j=1}^{n+1} l_{j-1}^{(r)} z_{j-1}$ and not forgetting (5.3.2) we have

$$A^{\perp} = \begin{pmatrix} l & & l_0^{(n+2)} & \cdots & l_0^{(N)} \\ & \ddots & \vdots & & \vdots \\ & & l & l_n^{(n+2)} & \cdots & l_n^{(N)} \end{pmatrix}. \tag{5.3.4}$$

So the first $n+1$ columns of $A^{\perp}$ are given by $(l, 0, ..., 0)^t$, ...,$(0, ..., 0, l)^t$. The equations

$$(L_1(\mathbf{z}), ..., L_N(\mathbf{z}))\mathbf{y} = ((A^{\perp})^t\mathbf{z})^t\mathbf{y} = \mathbf{z}^tA^{\perp}\mathbf{y}$$

show that $S^{\perp}$ is given by the equation $A^{\perp}\mathbf{y} = \mathbf{0}$. Now by definition $H_2(S^{\perp}) = H_2(A^{\perp})$ and later on we will use a duality for the height of subspaces (see [**47**] p.28), telling us that $H_2(S^{\perp}) = H_2(S)$. This is no surprise since changing signs of certain coordinates of a tuple of Grassmann coordinates of S yields a tuple of Grassmann coordinates of $S^{\perp}$.

3.1. Computing $V_{\mathcal{N}}^{inf}$. Suppose $v \mid \infty$. The volume V_v is that of the set defined by $\overline{\mathbf{z}}^tQ\mathbf{z} < 1$ where the (i,j) entry of Q is given by

$$b_v(e_i, e_j) = (\sigma_vL_1)(e_i)\overline{(\sigma_vL_1)(e_j)} + ... + (\sigma_vL_N)(e_i)\overline{(\sigma_vL_N)(e_j)}.$$

For v real this is

$$\frac{V(n+1)}{\sqrt{\det Q}}$$

and for v non-real it is

$$\frac{V(2n+2)}{\det Q}$$

Recalling from above that $L_r(\mathbf{z}) = \sum_{j=1}^{n+1} l_{j-1}^{(r)} z_{j-1}$ we get $b_v(e_i, e_j) = \sum_{r=1}^{N} \sigma_v(l_{i-1}^{(r)})\overline{\sigma_v(l_{j-1}^{(r)})}$ which is the (i,j) entry of $\sigma_v(A^\perp)\overline{\sigma_v(A^\perp)}^t$. So

$$Q = \sigma_v(A^\perp)\overline{\sigma_v(A^\perp)}^t.$$

Therefore the denominator is just the local part of the height $H_2(A^\perp)^d$ (see (5.1.4) or [**26**] p.13). This is one of the reasons why it is convenient to choose the l^2-height here. Multiplying V_v over all archimedean places yields

$$V_{\mathcal{N}}^{inf} = \frac{V(n+1)^{r_K} V(2n+2)^{s_K}}{H^{inf}(A^\perp)^d}. \tag{5.3.5}$$

3.2. Computing $V_{\mathcal{N}}^{fin}$. The finite part is more troublesome. Here we will use the fact that the coefficients $l_{j-1}^{(r)}$ of the linear forms $L_1, ..., L_N$ are algebraic integers. Recall also the definition of $A^\perp$. The matrix $A^\perp$ defines two maps. One from K^{n+1} to K^N by multiplication on the right $\mathbf{z} \longrightarrow (\mathbf{z}^t A^\perp)^t$. Now (5.3.3) is a $(1:1)$-correspondence, which tells us that this map is injective. The second map comes from multiplication on the left $\mathbf{x} \longrightarrow A^\perp \mathbf{x}$, which sends the column $\mathbf{x}$ from K^N to K^{n+1}.

Recall the lattice $\Lambda_{\mathcal{N}}$ from (3.1.10)

LEMMA 5.5. *Let $\mathfrak{A} \neq 0$ be a fractional ideal in K. Then*

$$\Lambda_{\mathcal{N}}(\mathfrak{A}) = \sigma(\mathfrak{A}^N A^{\perp -1}) \tag{5.3.6}$$

where $A^\perp$ is considered as a map $K^{n+1} \longrightarrow K^N$ defined by $\mathbf{z}^t \longrightarrow (\mathbf{z}^t A^\perp)^t$ and $A^{\perp -1}$ denotes the set-theoretical inverse.

Proof. The lattice $\Lambda_{\mathcal{N}}(\mathfrak{A})$ is given by the $\sigma\boldsymbol{\alpha}$ where

$$\max\{|(\sigma_v L_1)(\boldsymbol{\alpha})|_v, ..., |(\sigma_v L_N)(\boldsymbol{\alpha})|_v\} \leq |\mathfrak{A}|_v \tag{5.3.7}$$

for all finite v. But (5.3.7) is equivalent to

$$L_1(\boldsymbol{\alpha}), ..., L_N(\boldsymbol{\alpha}) \in \mathfrak{A}$$

and this in turn means nothing else but $(\boldsymbol{\alpha}^t A^{\perp})^t \in \mathfrak{A}^N$. So the $\boldsymbol{\alpha}$'s are exactly the elements of the set $\mathfrak{A}^N A^{\perp -1}$ and therefore $\Lambda_{\mathcal{N}}(\mathfrak{A}) = \sigma(\mathfrak{A}^N A^{\perp -1})$. □

Now $A^{\perp}$ takes $\mathfrak{A}^{n+1}$ to $\mathfrak{A}^N$, thanks to the integrality of its entries, and so

$$\sigma\mathfrak{A}^{n+1} \subseteq \sigma(\mathfrak{A}^N A^{\perp -1}) = \Lambda_{\mathcal{N}}(\mathfrak{A}). \tag{5.3.8}$$

We know $\det \sigma\mathfrak{A}^{n+1} = (2^{-s} N\mathfrak{A}\sqrt{|\Delta_K|})^{n+1}$ (see [**36**] p.33 (5.2) Satz) and so to calculate $\det \Lambda_{\mathcal{N}}(\mathfrak{A})$ it suffices to calculate the index $[\mathfrak{A}^N A^{\perp -1} : \mathfrak{A}^{n+1}]$. This can be done by using some "duality" where the set-up is as follows.

Let W be a finite dimensional $\mathbb{Q}$-vector space and let $b : W \times W \longrightarrow \mathbb{Q}$ be a non-degenerate, symmetric $\mathbb{Q}$-bilinear form. An additive subgroup $G \subset W$ has a dual

$$\widetilde{G} = \{\boldsymbol{w} \in W; b(\boldsymbol{w}, \boldsymbol{g}) \in \mathbb{Z} \text{ for all } \boldsymbol{g} \in G\}, \tag{5.3.9}$$

which is also an additive subgroup. Suppose $\dim W = D$ and from now on assume G is a free $\mathbb{Z}$-module of rank D so that there exist $\boldsymbol{g}_1, ..., \boldsymbol{g}_D$ in W with

$$G = \boldsymbol{g}_1\mathbb{Z} + ... + \boldsymbol{g}_D\mathbb{Z}. \tag{5.3.10}$$

Since $\boldsymbol{g}_1, ..., \boldsymbol{g}_D$ are $\mathbb{Z}$-linearly independent we have

$$W = \boldsymbol{g}_1\mathbb{Q} + ... + \boldsymbol{g}_D\mathbb{Q}. \tag{5.3.11}$$

The following four lemmas are well-known but for the sake of completeness we include the simple proofs.

LEMMA 5.6. *There are $\widetilde{\boldsymbol{g}_1}, ..., \widetilde{\boldsymbol{g}_D}$ in W linearly independent with*

$$b(\widetilde{\boldsymbol{g}_i}, \boldsymbol{g}_j) = \delta_{ij} \tag{5.3.12}$$

for $1 \leq i, j \leq D$.

Proof. By solving a homogeneous linear system of $D-1$ equations in D variables we may find a non-zero $\widetilde{\boldsymbol{g}_1}$ in W with $b(\widetilde{\boldsymbol{g}_1}, \boldsymbol{g}_j) = 0$ for $2 \leq j \leq D$. Now suppose $b(\widetilde{\boldsymbol{g}_1}, \boldsymbol{g}_1) = 0$. Then by (5.3.11) $b(\widetilde{\boldsymbol{g}_1}, \boldsymbol{w}) = 0$ for all $\boldsymbol{w}$ in W but b is non-degenerate and we conclude $\widetilde{\boldsymbol{g}_1} = \boldsymbol{0}$ - a contradiction. Hence $b(\widetilde{\boldsymbol{g}_1}, \boldsymbol{g}_1) \neq 0$ and so after multiplying $\widetilde{\boldsymbol{g}_1}$ with a suitable rational number we get $b(\widetilde{\boldsymbol{g}_1}, \boldsymbol{g}_1) = 1$. In this way we obtain $\widetilde{\boldsymbol{g}_1}, ..., \widetilde{\boldsymbol{g}_D}$ with (5.3.12). The linear independence is immediately implied by (5.3.12). □

LEMMA 5.7. *We have*

$$\widetilde{G} = \widetilde{\boldsymbol{g}_1}\mathbb{Z} + ... + \widetilde{\boldsymbol{g}_D}\mathbb{Z}. \tag{5.3.13}$$

Proof. Clearly the right set is contained in the left one. To prove the other inclusion let $\boldsymbol{w}$ be an element of $\widetilde{G}$. There are $\mu_1, ..., \mu_D$ in $\mathbb{Q}$ with

$$\boldsymbol{w} = \mu_1\widetilde{\boldsymbol{g}_1} + ... + \mu_D\widetilde{\boldsymbol{g}_D}.$$

By definition of $\widetilde{G}$ we have $b(\boldsymbol{w}, \boldsymbol{g})$ in $\mathbb{Z}$ for every $\boldsymbol{g}$ in G. In particular

$$b(\boldsymbol{w}, \boldsymbol{g}_i) \in \mathbb{Z}.$$

But by (5.3.12) we see that $b(\boldsymbol{w}, \boldsymbol{g}_i) = \mu_i$, which proves the second inclusion. □

LEMMA 5.8. *We have*

$$\widetilde{\widetilde{G}} = G.$$

Proof. We have $b(\boldsymbol{g}_i, \widetilde{\boldsymbol{g}_j}) = b(\widetilde{\boldsymbol{g}_j}, \boldsymbol{g}_i) = \delta_{ji}$ for $1 \leq i, j \leq D$. So by Lemma 5.6 and Lemma 5.7 $\widetilde{\widetilde{G}} = \boldsymbol{g}_1\mathbb{Z} + ... + \boldsymbol{g}_D\mathbb{Z} = G$. □

Now let $H \subseteq G$ be a submodule of G also of rank D. We have

LEMMA 5.9. *The indices* $[G : H]$, $[\widetilde{H} : \widetilde{G}]$ *are finite and equal.*

Proof. Using the elementary divisors Theorem (see [**24**] p.153 Th.7.8) we find a basis $\boldsymbol{g}_1, ..., \boldsymbol{g}_D$ of G such that there are rational integers $a_1, ..., a_D$ with $a_1\boldsymbol{g}_1, ..., a_D\boldsymbol{g}_D$ a basis of H. So $[G : H] = |a_1...a_D|$. Let $\widetilde{\boldsymbol{g}_1}, ..., \widetilde{\boldsymbol{g}_D}$ be as in Lemma 5.6. By Lemma 5.7 it is a basis of $\widetilde{G}$. Due to (5.3.12) we have ${a_1}^{-1}\widetilde{\boldsymbol{g}_1}\mathbb{Z} + ... + {a_D}^{-1}\widetilde{\boldsymbol{g}_D}\mathbb{Z} \subseteq \widetilde{H}$. On the other hand every element in $\widetilde{H}$ is of the form $\mu_1\widetilde{\boldsymbol{g}_1} + ... + \mu_D\widetilde{\boldsymbol{g}_D}$ where $\mu_1, ..., \mu_D$ are in $\mathbb{Q}$. Now $a_1\boldsymbol{g}_1 + ... + a_D\boldsymbol{g}_D$ lies in H and therefore by the definition of the dual group and (5.3.12) we see that in fact $\mu_i a_i \in \mathbb{Z}$ for $1 \leq i \leq D$ and so ${a_1}^{-1}\widetilde{\boldsymbol{g}_1}\mathbb{Z} + ... + {a_D}^{-1}\widetilde{\boldsymbol{g}_D}\mathbb{Z} \supseteq \widetilde{H}$ so ${a_1}^{-1}\widetilde{\boldsymbol{g}_1}\mathbb{Z} + ... + {a_D}^{-1}\widetilde{\boldsymbol{g}_D} = \widetilde{H}$. And now we get $[\widetilde{H} : \widetilde{G}] = |a_1...a_D| = [G : H]$. □

From the general context let us return to our specific situation. We define

$$W = K^{n+1} \text{ and} \tag{5.3.14}$$

$$G = \mathfrak{A}^N {A^{\perp}}^{-1}, \quad H = \mathfrak{A}^{n+1} \tag{5.3.15}$$

Clearly $\mathfrak{A}^{n+1} \subseteq G$ and using just the first $n+1$ columns of $A^{\perp}$ we get $G \subseteq l^{-1}\mathfrak{A}^{n+1}$. Now $\mathfrak{A}^{n+1}$ is a free $\mathbb{Z}$-module of rank $D = d(n+1) =$

$\dim_{\mathbb{Q}} K^{n+1}$. Thus G and H are both free $\mathbb{Z}$-modules of rank D. For $b(\cdot,\cdot)$ we choose

$$b(\boldsymbol{w},\boldsymbol{w}') = Tr_{K/\mathbb{Q}}(\boldsymbol{w}^t\boldsymbol{w}'). \tag{5.3.16}$$

Here $\boldsymbol{w}^t\boldsymbol{w}' = w_1w_1' + ... + w_{n+1}w_{n+1}'$ means just the scalar product and $Tr_{K/\mathbb{Q}}$ denotes the trace of K relative to $\mathbb{Q}$, from now on abbreviated to Tr. It is well-known ([**25**] p.214 Satz 3) that $b(\cdot,\cdot)$ defines a non-degenerate, symmetric $\mathbb{Q}$-bilinear form from K^{n+1} to $\mathbb{Q}$ at least for "$n = 0$"; but the extension to any n is clear. Suppose $\boldsymbol{w}$ is such that $Tr(\boldsymbol{w}^t\boldsymbol{w}') \in \mathbb{Z}$ for all $\boldsymbol{w}'$ in $\mathfrak{A}^{n+1}$ and moreover assume $\lambda \in \mathcal{O} = \mathcal{O}_K$. Then $Tr((\lambda\mathbf{x})^t\mathbf{y}) \in \mathbb{Z}$ for all $\mathbf{y}$ in $\mathfrak{A}^{n+1}$. Hence $\widetilde{H}$ is the $(n+1)$-th power of a non-zero fractional ideal, say $\mathfrak{B}$. So

$$\widetilde{H} = \mathfrak{B}^{n+1}. \tag{5.3.17}$$

Lemma 5.10. *We have*

$$\widetilde{G} = A^{\perp}\mathfrak{B}^N. \tag{5.3.18}$$

Here $A^{\perp}$ is considered as a map from K^N to K^{n+1}.

Proof. We abbreviate $A^{\perp}\mathfrak{B}^N$ to G_0. Again using the first $n+1$ columns of $A^{\perp}$ it is easily seen that $l\mathfrak{B}^{n+1} \subseteq A^{\perp}\mathfrak{B}^N$ and clearly $A^{\perp}\mathfrak{B}^N \subseteq \mathfrak{B}^{n+1}$. Therefore G_0 is a $\mathbb{Z}$-module of rank D. Now let us calculate the dual group of G_0

$$\widetilde{G_0} = \{\boldsymbol{\alpha} \in K^{n+1}; Tr(\boldsymbol{\alpha}^tA^{\perp}\boldsymbol{\beta}) \in \mathbb{Z} \text{ for all } \boldsymbol{\beta} \in \mathfrak{B}^N\} \tag{5.3.19}$$

where of course $\boldsymbol{\alpha}$ and $\boldsymbol{\beta}$ are both columns. First consider $\widetilde{G_0}A^{\perp}$ being the set of $(\boldsymbol{\alpha}^tA^{\perp})^t$ with $\boldsymbol{\alpha} \in K^{n+1}$ and $Tr(\boldsymbol{\alpha}^t(A^{\perp}\boldsymbol{\beta})) \in \mathbb{Z}$ for all $\boldsymbol{\beta} \in \mathfrak{B}^N$. Clearly one has $\widetilde{G_0}A^{\perp} \subseteq K^{n+1}A^{\perp}$ and since

$$Tr(((\boldsymbol{\alpha}^tA^{\perp})^t)^t\boldsymbol{\beta}) = Tr((\boldsymbol{\alpha}^tA^{\perp})\boldsymbol{\beta}) = Tr(\boldsymbol{\alpha}^t(A^{\perp}\boldsymbol{\beta})) \tag{5.3.20}$$

we see that $\widetilde{G_0}A^{\perp} \subseteq \widetilde{\mathfrak{B}^N}$ where $\widetilde{\mathfrak{B}^N}$ denotes the dual of $\mathfrak{B}^N$ in K^N with respect to the analogue of (5.3.16). Hence $\widetilde{G_0}A^{\perp} \subseteq \widetilde{\mathfrak{B}^N} \cap K^{n+1}A^{\perp}$. On the other hand suppose $\boldsymbol{\alpha} \in K^{n+1}$ with $(\boldsymbol{\alpha}^tA^{\perp})^t \in \widetilde{\mathfrak{B}^N}$. Then (5.3.20) implies that $\boldsymbol{\alpha}$ is in $\widetilde{G_0}$ and so $(\boldsymbol{\alpha}^tA^{\perp})^t \in \widetilde{G_0}A^{\perp}$. So we conclude $\widetilde{G_0}A^{\perp} \supseteq \widetilde{\mathfrak{B}^N} \cap K^{n+1}A^{\perp}$. Combining both inclusions yields

$$\widetilde{G_0}A^{\perp} = \widetilde{\mathfrak{B}^N} \cap K^{n+1}A^{\perp}.$$

It follows easily using the injectivity of the map $\mathbf{z} \longrightarrow (\mathbf{z}^tA^{\perp})^t$ that

$$\widetilde{G_0} = \widetilde{\mathfrak{B}^N}A^{\perp -1}.$$

By (5.3.15) and (5.3.17) it is clear that $\widetilde{\mathfrak{A}^N} = \mathfrak{B}^N$ where again $\widetilde{\mathfrak{A}^N}$ denotes the dual of $\mathfrak{A}^N$ in K^N. By Lemma 5.8 we have $\widetilde{\widetilde{\mathfrak{A}^N}} = \mathfrak{A}^N$. So $\widetilde{\mathfrak{B}^N} = \mathfrak{A}^N$ and it follows that $\widetilde{G_0} = \mathfrak{A}^N {A^\perp}^{-1} = G$. Appealing once more to Lemma 5.8 we obtain $G_0 = \widetilde{G}$ - exactly the claim. □

We are now in a position to compute the determinant of the lattice $\Lambda_{\mathcal{N}}(\mathfrak{A})$

LEMMA 5.11. *Let $\mathfrak{A} \neq 0$ be a fractional ideal in K. Then we have*

$$\det \Lambda_{\mathcal{N}}(\mathfrak{A}) = (2^{-s} N\mathfrak{A}\sqrt{|\Delta_K|})^{n+1} H^{fin}(A^\perp)^d.$$

Proof. By Lemma 5.10 and Lemma 5.9 we get

$$[\mathfrak{A}^N {A^\perp}^{-1} : \mathfrak{A}^{n+1}] = [\mathfrak{B}^{n+1} : A^\perp \mathfrak{B}^N].$$

Now

$$H^{fin}(A^\perp)^d = [\mathcal{O}^{n+1} : A^\perp \mathcal{O}^N]^{-1}$$

by Lemma 2.1 (p.111) in [**27**]. But here $\mathcal{O}$ can be replaced by any non-zero fractional ideal, which comes out of [**27**] immediately after equation (2.25) (p.114). We conclude

$$\begin{aligned} \det \Lambda_{\mathcal{N}}(\mathfrak{A}) &= \frac{\det \sigma(\mathfrak{A}^{n+1})}{[\mathfrak{A}^N {A^\perp}^{-1} : \mathfrak{A}^{n+1}]} \\ &= (2^{-s} N\mathfrak{A}\sqrt{|\Delta_K|})^{n+1} H^{fin}(A^\perp)^d. \end{aligned}$$

□

So the $\Delta_{\mathcal{N}}(\mathcal{D})$ in (3.1.12) are all equal to

$$(2^{-s}\sqrt{|\Delta_K|})^{n+1} H^{fin}(A^\perp)^d.$$

Hence

$$V_{\mathcal{N}}^{fin} = H^{fin}(A^\perp)^{-d}.$$

3.3. End of the proof. Now the height of $\mathbb{V}$ is defined as the height of the vector space S. But $H_2(S) = H_2(A)$ and $H_2(S^\perp) = H_2(A^\perp)$ also by definition, and the duality for heights of subspaces says $H_2(S^\perp) = H_2(S)$. Finally (5.3.1) comes out after we recall $H_2(A^\perp) = H^{fin}(A^\perp)H^{inf}(A^\perp)$. This finishes the proof of Theorem 5.1.

APPENDIX A

Narrow class and Lipschitz class

The aim of Appendix A is to compare Theorem 1.2 with Schmidt's Theorem 1.3. Theorem 1.3 is ideal in the situation of a bounded, convex (so narrow class 1) set S. But there are sets, which are not of narrow class s for any s and which have a boundary of Lipschitz class $(n, 1, M, L)$ (e.g. take the modified square with side $1/\pi$, where one edge is replaced by a translate of the curve $(x, x^3 \sin(1/x))$ for $0 \leq x \leq 1/\pi$). In our application S was defined by a distance function N (see [**45**] p.431); namely $S = \{\mathbf{x} \in \mathbb{R}^n; N(\mathbf{x}) < 1\}$. Also in this situation it is easy to find an S, which is not of narrow class s for any number s but which has boundary in $\mathrm{Lip}(n, 1, M, L)$ for certain numbers M, L. So if Theorem 1.3 does not apply there is still hope that Theorem 1.2 does. If S is of narrow class s for some s it still might be very arduous to prove it, since one has to check certain intersection conditions of any line not only with S itself but also with all projections of S on any linear subspace of $\mathbb{R}^n$. On the other hand the $\mathrm{Lip}(n, 1, M, L)$ condition on the boundary of S seems to be rather mild. And indeed we believe:

CONJECTURE A.1. *Let S in $\mathbb{R}^n$ be a set of narrow class s and assume S lies in a ball of radius R. Then there is a natural number $M = M(n, s)$ and a real number $C = C(n, s)$ such that ∂S is in $Lip(n, 1, M, CR)$.*

REMARK 6. *The case $n = 1$ is trivial. So assume $n > 1$. If a set in $\mathbb{R}^n$ is in $Lip(n, 1, M, L)$ and lies in a ball of radius R then it can be shown that it is in $Lip(n, 1, 1, L')$ with a new (for example $L' = 8M\sqrt{n-1}(L + R)$) Lipschitz constant L'. Therefore the Conjecture A.1 implies a stronger form of itself with $M = 1$.*

THEOREM A.1. *For $s = 1$ Conjecture A.1 is true. More precisely we have ∂S is in $Lip(1, 1, 2, 0)$ if $n = 1$ and ∂S is in $Lip(n, 1, 1, 8n^2R)$ if $n > 1$.*

For $n = 2$ we prove only a very weak version of Conjecture A.1 (see Subsection 2). The proof of Theorem A.1 requires the following

LEMMA A.1. *Let $n > 1$, S in $\mathbb{R}^n$ be a convex set, P a point in S and r, R positive reals such that*

$$B_P(r) \subseteq S \subseteq B_P(R). \tag{A.0.21}$$

Then the boundary ∂S is in $Lip(n, 1, 1, 8\sqrt{n-1}R^2/r)$.

Proof. We may translate S to get $P = 0$. Let

$$\varphi : [0, 2\pi] \times [0, \pi]^{n-2} \longrightarrow \partial B_P(r) \tag{A.0.22}$$

be the standard parameterization of $\partial B_P(r)$ via polar coordinates such that

$$\begin{aligned}
x_1 &= r\cos\theta_1\cos\theta_2\cos\theta_3 ... \cos\theta_{n-1}\\
x_2 &= r\sin\theta_1\cos\theta_2\cos\theta_3 ... \cos\theta_{n-1}\\
x_3 &= \quad r\sin\theta_2\cos\theta_3 ... \cos\theta_{n-1}\\
&\vdots\\
x_n &= \quad r\sin\theta_{n-1}.
\end{aligned}$$

Let A, B be different points in $\mathbb{R}^n$ then we denote by $[A, B]$ the line segment between A and B (A, B are included) of the line containing A, B. Similar (A, B) denotes the line segment without the points A, B. We claim that intersecting the half-line, which starts in P and contains $\varphi(\boldsymbol{\theta})$ with the boundary of S leads to a parameterization $\widetilde{\varphi}$ of ∂S. It suffices to show that each such half-line contains no more than one boundary point of S. So assume such a half-line contains more than one boundary point, say A and B where A is closer to P. Now consider the union of all line segments (B, F) starting in B and ending on any boundary point F of $B_P(r)$. Then each point of the line segment (B, P) lies in the interior of this union. Due to the convexity of S this set is a subset of the topological closure of S (but not always of S itself) and since A lies in (B, P) we conclude that A lies in the interior of S, a contradiction. This little argument will be used once more at the end of the proof.

The next step of the proof is to show that $\widetilde{\varphi}$ is a Lipschitz parameterization with Lipschitz constant $(4/\pi)\sqrt{n-1}R^2/r$ such that after normalizing properly to get a map as in (1.1.1) one gets the Lipschitz constant $8\sqrt{n-1}R^2/r$.
We use only simple planimetric arguments. Let us write $\overline{AB}$ for the length of the line segment $[A, B]$. Let A, B, C be three different points then we may talk of the angle β between the line-segments $[A, B]$ and $[A, C]$. It is defined as the value in $[0, \pi]$ such that $\cos\beta =$

$\langle B-A, C-A\rangle/(\overline{AB}\cdot\overline{AC})$ where $\langle\cdot,\cdot\rangle$ denotes the euclidean scalar product. If the points do not lie on one line then we may consider the triangle $\triangle(A,B,C)$ with vertices A,B,C.
Let $\widetilde{\varphi}(\boldsymbol{\theta_1})=A, \widetilde{\varphi}(\boldsymbol{\theta_2})=B$ two distinct points on the boundary of S. We may assume

$$0<|\boldsymbol{\theta_2}-\boldsymbol{\theta_1}|<\frac{\pi}{2\sqrt{n-1}} \tag{A.0.23}$$

for otherwise we get automatically

$$\overline{AB}\leq 2R\leq(4/\pi)\sqrt{n-1}R|\boldsymbol{\theta_2}-\boldsymbol{\theta_1}|. \tag{A.0.24}$$

Denote by α the angle between $[P,A]$ and $[P,B]$ and write $|\cdot|_{l_1}$ for the l_1-norm. Then we have

$$\alpha\leq|\boldsymbol{\theta_2}-\boldsymbol{\theta_1}|_{l_1}, \tag{A.0.25}$$

which is a simple consequence of the triangle-inequality in the metric space $\mathbb{S}^{n-1}$ (see p.17 in [**6**]). Hence

$$\alpha\leq\sqrt{n-1}|\boldsymbol{\theta_2}-\boldsymbol{\theta_1}|. \tag{A.0.26}$$

If A,B,P lie on a common line then either $\alpha=\pi$ and so $|\boldsymbol{\theta_2}-\boldsymbol{\theta_1}|\geq\pi/\sqrt{n-1}$ or $A=B$, both contradicting our assumptions. So the lines joining P,A and P,B respectively span a plane say $\mathcal{P}$. Write $\mathcal{B}$ for the interior of $B_P(r)$ and $\mathcal{L}$ for the line joining A and B. The line in $\mathcal{P}$ perpendicular to $\mathcal{L}$ which joins P intersects $\mathcal{L}$ in a point denoted by C.

The proof splits into the following three cases:

(1) $\mathcal{L}$ does not meet $\mathcal{B}$ (C not in $\mathcal{B}$).
(2) $\mathcal{L}$ meets $\mathcal{B}$ between A and B (C is in $[A,B]$ and in $\mathcal{B}$).
(3) The remaining case (A is in $[B,C]$ or B is in $[A,C]$ and C is in $\mathcal{B}$).

We start with the first case. Now $\mathcal{L}$ does not meet $\mathcal{B}$ is equivalent to $\overline{PC}\geq r$. The area of $\triangle(P,A,B)$ is $\overline{PC}\cdot\overline{AB}/2$. It is clear that $\triangle(P,A,B)$ does not exceed the area of a sector of $B_P(R)\cap\mathcal{P}$ with angle α, which is $\alpha R^2/2$. Thus

$$\overline{AB}\leq\frac{R^2}{r}\alpha. \tag{A.0.27}$$

For the second case we have $[A,B]$ contains C. Denote the angle between $[P,C]$ and $[P,A]$ by α_1 and the angle between $[P,C]$ and $[P,B]$ by α_2 such that $\alpha=\alpha_1+\alpha_2$ and $0\leq\alpha_1,\alpha_2\leq\alpha\leq\pi/2$. Hence

$$\overline{AC}=\overline{PA}\sin\alpha_1\leq\overline{PA}\alpha_1\leq R\alpha_1 \tag{A.0.28}$$

and similar $\overline{BC} \leq R\alpha_2$ leading to

$$\overline{AB} \leq R\alpha. \tag{A.0.29}$$

Since A, B lie on the boundary of S none of them can lie in $\mathcal{B}$. Thus the remaining case occurs if either A is in $[B, C]$ or B lies in $[A, C]$. Since C is in $\mathcal{B}$ there is a positive ϵ such that $B_C(\epsilon)$ lies in $\mathcal{B}$. But now we use the same argument as in the beginning of the proof to show that due to the convexity either A or B lies in the interior of S - a contradiction and so the remaining case is impossible.
Recalling (A.0.26) and $R \geq r$ proves that all cases are covered by

$$|\widetilde{\varphi}(\boldsymbol{\theta_1}) - \widetilde{\varphi}(\boldsymbol{\theta_2})| = \overline{AB} \leq (4/\pi)\sqrt{n-1}\frac{R^2}{r}|\boldsymbol{\theta_1} - \boldsymbol{\theta_2}|. \tag{A.0.30}$$

Properly normalizing to get a map as in (1.1.1) gives an additional factor 2π and completes the proof. □

1. Proof of Theorem A.1

Clearly a set of narrow class 1 is convex. For $n = 1$ the set S is just a single interval (maybe even a single point) and so its boundary consists of at most two points proving that ∂S lies in $\mathrm{Lip}(1, 1, 2, 0)$. So assume $n > 1$. Suppose the interior $\mathrm{int}S$ of S is empty. Pick P_0 in S; then the points of $S - P_0$ cannot span $\mathbb{R}^n$ as a $\mathbb{R}$-vector space, else S would contain a small neighbourhood of P_0. Hence S lies in a hyperplane and so ∂S lies in a ball $B_{P'}(R')$ in $\mathbb{R}^{n-1}$ for some $R' \leq R$. So it suffices to know that $B_{P'}(R')$ lies in $\mathrm{Lip}(n, 1, 1, 2R)$, which can be seen by parameterizing a $(n-1)$-dimensional cube containing $B_{P'}(R')$. From now on we may assume $\mathrm{int}S \neq \emptyset$. Therefore we have a point P_1 in $\mathrm{int}S$ and a positive real number $r > 0$ such that $B_{P_1}(r)$ lies in $\mathrm{int}S$. On the other hand there is a point P_2 such that S is in $B_{P_2}(R)$. The triangle-inequality implies S lies in $B_{P_1}(2R)$. Applying Lemma A.1 proves the existence of a Lipschitz parameterization of the boundary. Unfortunately the Lipschitz constant L has still a disallowed dependence on r and moreover the exponent of R should be one not two. We can overcome these problems by the use of John's theorem (see for example [**1**] p.242). Roughly speaking it says that a convex set is not far from an ellipsoid or more precisely; we can find an ellipsoid E with center say P such that

$$E \subseteq S \subseteq nE. \tag{A.1.1}$$

We can translate to get $P = 0$. Now after an orthogonal transformation we can suppose that E is defined by $(x_1/a_1)^2 + ... + (x_n/a_n)^2 = 1$. We may assume that $0 < a_1 \leq a_2 \leq .... \leq a_n$. Moreover E lies in a ball, say

$\mathcal{B}$, of radius R and so $2a_n = \sup_{A,B\in E}|A-B| \leq \sup_{C,D\in\mathcal{B}}|C-D| = 2R$. Hence

$$0 < a_1 \leq a_2 \leq .... \leq a_n \leq R. \tag{A.1.2}$$

Let Φ be the endomorphism which sends $x_i \longrightarrow x_i/a_i$ for $1 \leq i \leq n$. Applying this map to (A.1.1) yields

$$B_0(1) \subseteq \Phi(S) \subseteq B_0(n). \tag{A.1.3}$$

Lemma A.1 with $r = 1$ and $R = n$ yields a map $\widetilde{\varphi} : [0,1]^{n-1} \longrightarrow \mathbb{R}^n$ with image containing $\partial(\Phi(S))$ such that

$$|\widetilde{\varphi}(\mathbf{x}_2) - \widetilde{\varphi}(\mathbf{x}_1)| \leq 8n^2|\mathbf{x}_2 - \mathbf{x}_1|. \tag{A.1.4}$$

Since Φ is linear and bijective the maps Φ and its inverse Φ^{-1} are continuous. So the boundary of S is simple the image under Φ^{-1} of the boundary $\partial\Phi(S)$. Thus $\Phi^{-1}(\widetilde{\varphi}(\cdot))$ is a parameterization of ∂S. Let us calculate a Lipschitz constant:

$$\begin{aligned}
|\Phi^{-1}(\widetilde{\varphi}(\mathbf{x}_2)) - \Phi^{-1}(\widetilde{\varphi}(\mathbf{x}_1))| &= |\Phi^{-1}(\widetilde{\varphi}(\mathbf{x}_2) - \widetilde{\varphi}(\mathbf{x}_1))| \\
&\leq \sup_{|\mathbf{z}|=1} |\Phi^{-1}(\mathbf{z})||\widetilde{\varphi}(\mathbf{x}_2) - \widetilde{\varphi}(\mathbf{x}_1)| \\
&= \sup_{|\mathbf{z}|=1} (\sum_{i=1}^{n} (a_i z_i)^2)^{1/2} |\widetilde{\varphi}(\mathbf{x}_2) - \widetilde{\varphi}(\mathbf{x}_1)| \\
&\leq \sup_{|\mathbf{z}|=1} a_n (\sum_{i=1}^{n} z_i^2)^{1/2} |\widetilde{\varphi}(\mathbf{x}_2) - \widetilde{\varphi}(\mathbf{x}_1)| \\
&= a_n |\widetilde{\varphi}(\mathbf{x}_2) - \widetilde{\varphi}(\mathbf{x}_1)| \\
&\leq a_n 8n^2 |\mathbf{x}_2 - \mathbf{x}_1| \\
&\leq 8n^2 R |\mathbf{x}_2 - \mathbf{x}_1|.
\end{aligned}$$

This agrees with our claim and thereby completes the proof.

2. The 2-dimensional case

For $n = 2$ we can apply Poincaré's formula from integral geometry to prove a weak form of Conjecture A.1. We call Γ a simple curve if there exists a continuous map $\phi : [0,1] \longrightarrow \mathbb{R}^2$ injective on $(0,1)$ such that $\Gamma = \phi([0,1])$. We say Γ is closed if $\phi(0) = \phi(1)$. Let Γ_0, Γ_1 be two rectifiable (see [**6**] p.12), simple curves of length $|\Gamma_0|, |\Gamma_1|$. Poincaré's formula tells us (see [**21**] and [**42**] Chap. 6 and Chap. 7 for more details)

$$\int_{\mathcal{M}} \mathfrak{n} dK = 4|\Gamma_0||\Gamma_1| \tag{A.2.1}$$

where $\mathcal{M}$ is the group of motions ϕ in the plane, $\mathfrak{n} = \mathfrak{n}(\phi) = |\Gamma_1 \cap \phi(\Gamma_0)|$ (possibly infinite) is the intersection number of Γ_1 and $\phi(\Gamma_0)$ and dK is the kinematic density for $\mathcal{M}$ that is the invariant volume element of the space of the group of motions in the plane (therefore the integral is independent of the initial positions of the curves). It seems that formula (A.2.1) has been generalized by Maak ([**30**]) to arbitrary simple curves (for non-rectifiable curves the right hand side has to be interpreted as infinity). In particular if $\mathfrak{n}$ is bounded then Γ_0 and Γ_1 are both rectifiable. But possibly Maak's definition of the intersection number $\mathfrak{n}$ is different from ours so that we prefer not to rely on his result. Now any $\phi = \phi_{a,b,\theta}$ is given by a rotation and a translation

$$\phi(x, y) = (x \cos\theta - y \sin\theta + a, x \sin\theta + y \cos\theta + b)$$

where $-\infty < a < \infty$, $-\infty < b < \infty$, $0 \leq \theta \leq 2\pi$. So $\mathfrak{n} = \mathfrak{n}(\phi(a, b, \theta))$ becomes a function of a, b, θ and we write by abuse of notation $\mathfrak{n}(a, b, \theta)$. In fact (A.2.1) can be written as

$$\int_\theta \int_b \int_a \mathfrak{n} \cdot dadbd\theta = 4|\Gamma_0||\Gamma_1| \tag{A.2.2}$$

see for example [**41**] p.22.

Now consider the following conditions on a set S in $\mathbb{R}^2$.

- (I) The boundary ∂S of S is given by a rectifiable, simple, closed curve.
- (II) Let Γ_0 be a line-segment. Then the subset $\mathcal{M}_0$ of $\mathcal{M}$ defined by $|\partial S \cap \phi(\Gamma_0)| > 2s$ has measure zero, so that $\int_{\mathcal{M}_0} dK = 0$.

A set S in $\mathbb{R}^2$ of narrow class s satisfying (I) and (II) will be called a set of *very narrow class s* .

We can now state our approach to Conjecture A.1 in dimension two.

THEOREM A.2. *Let S in $\mathbb{R}^2$ be a set of very narrow class s and assume S lies in a ball of radius R. Then ∂S is in $Lip(2, 1, 1, (3\pi/2)^2 sR)$.*

Proof. We may assume ∂S lies in $B_0(R)$. Suppose Γ_0 is a line-segment of length R with its middle point on the origin. Let $\mathcal{M}_1 = \mathcal{M}_1(\Gamma_0)$ be the subset of $\mathcal{M}$ defined by $\mathfrak{n}(\phi) = |\partial S \cap \phi(\Gamma_0)| \leq 2s$. Then condition

(II) implies

$$\int_{\mathcal{M}} \mathfrak{n} dK = \int_{\mathcal{M}_1} \mathfrak{n} dK.$$

Hence from (A.2.2)

$$4|\Gamma_0||\partial S| = \int_\Theta \int_{\boldsymbol{\varrho}} \mathfrak{n} \cdot dadbd\theta.$$

with certain subsets $\Theta \subseteq [0, 2\pi]$ and $\boldsymbol{\varrho} \subseteq \mathbb{R}^2$ and

$$\mathfrak{n}(a, b, \theta) \leq 2s$$

for all $(\theta, a, b) \in \Theta \times \boldsymbol{\varrho}$. Now $\partial S \subseteq B_0(R)$ and thus $\partial S \cap \phi_{a,b,\theta}(\Gamma_0) = \emptyset$ if $\sqrt{a^2 + b^2} > 3R/2$. Therefore we have $\mathfrak{n} = \mathfrak{n}(a, b, \theta) = 0$ for $(a, b) \notin B_0(3R/2)$. Hence

$$\begin{aligned} 4R|\partial S| = 4|\Gamma_0||\partial S| = \int_\Theta \int_{\boldsymbol{\varrho}} \mathfrak{n} \cdot dadbd\theta &= \int_\Theta \int_{B_0(3R/2)\cap\boldsymbol{\varrho}} \mathfrak{n} \cdot dadbd\theta \\ &\leq \int_\Theta \int_{B_0(3R/2)\cap\boldsymbol{\varrho}} 2s \cdot dadbd\theta \\ &\leq \int_0^{2\pi} \int_{B_0(3R/2)} 2s \cdot dadbd\theta \\ &= 9\pi^2 sR^2. \end{aligned}$$

Thus $|\partial S| \leq (3\pi/2)^2 sR$. It is well-known that a rectifiable curve can be parameterized by the arc length. Let ψ be such a parameterization of ∂S, scaled from $[0, |\partial S|]$ to $[0, 1]$, then we have $|\psi(t) - \psi(t')| \leq |\partial S||t - t'|$. This shows that ∂S lies in $\mathrm{Lip}(2, 1, 1, (3\pi/2)^2 sR)$. □

The bound $|\partial S| \leq (3\pi/2)^2 sR$ can be improved at least under some regularity conditions. Any line l in the plane is given by a normalized vector $\nu = (\cos\theta, \sin\theta)$ perpendicular to l and the distance $p \geq 0$ of l to the origin. If we restrict the parameter θ to lie in $[0, 2\pi)$ then each line joining the origin has two representations (namely $l(\theta, 0)$ and $l(\theta + \pi, 0)$) and all other lines have exactly one representation. The formula of Cauchy-Croft (see [**13**] Theorem 3 p. 34 and (8) p. 37) for a regular (for definition see [**13**] p.5) curve Γ_1 in the plane tells us that

$$2|\Gamma_1| = \int_0^\infty \int_0^{2\pi} \mathfrak{n}(\theta, p) d\theta dp$$

where $\mathfrak{n}(\theta, p)$ is the intersection number of $l(\theta, p)$ and Γ_1. Now suppose ∂S is regular and for simplicity also $\mathfrak{n}(\theta, p) \leq 2s$ for all (θ, p). Since

$\partial S \subseteq B_0(R)$ we get $\mathfrak{n} = 0$ for $p > R$ and therefore

$$|\partial S| \leq 2\pi s R.$$

The value on the right-hand side cannot be lowered as we can see by the following examples: for $s = 1$ we take S as a circle, for s even we take S as a worm wrapped $s - 1$ times around a circle and for $s > 1$ odd the circle should be considered as the head of the worm and its tail is wrapped $s - 2$ times around the head.

3. Dependence on n

Finally we compare the dependence on n of the error terms in Theorem 1.3 and Theorem 1.2. Since it had no relevance for the original application neither of Theorem 1.3 nor of Theorem 1.2 it is not a surprise that none of them provides optimal dependence on n. However we observe that our $c_0(n)$ is $n^{\frac{3}{2}n^2}$, while for s fixed and n large Schmidt's $c_1(s, n)$ just goes as 3^{n^2}.

APPENDIX B

Gao's and Schmidt's definition of heights

A different approach to define heights than the one of Subsection 1.2 in Chapter 4 goes back to Schmidt [**49**] for degree $d = 2$ and Gao [**17**] for arbitrary degree. We follow Gao. He starts by defining a projective height on $K^{n+1}\backslash\{\mathbf{0}\}$ attached to a subset of $\mathbb{R}^{d(n+1)}$ where $d = [K : \mathbb{Q}]$. The reference set U_0 is defined as the set of $(\mathbf{z}_1, ..., \mathbf{z}_{q+1})$ in $\mathbb{R}^{r(n+1)} \times \mathbb{C}^{s(n+1)}$ with $\prod_{v|\infty} N_v(\mathbf{z_i})^{d_v} \leq 1$ where N_v is as in (3.1.2) Chapter 3 for all v and $q + 1 = r + s$. Recall the meaning of F, Σ and $S_F(1)$ from Chapter 3 Section 3. Notice that $S_\Sigma(1) = U_0$. For a set U in $\mathbb{R}^{r(n+1)} \times \mathbb{C}^{s(n+1)}$ and $F \subseteq \Sigma$ define $U(F)$ as $S_F(\infty) \cap U$. From now on let U be an arbitrary closed set in $\mathbb{R}^{r(n+1)} \times \mathbb{C}^{s(n+1)} = \mathbb{R}^D$ with

(a) $\mu_1 U_0 \subseteq U \subseteq \mu_2 U_0$ for some $\mu_2 \geq \mu_1 > 0$.

(b) For every $\boldsymbol{\eta}$ in $\mathbb{R}^r \times \mathbb{C}^s$ with $|\prod_{i=1}^{q+1} \eta_i^{d_i}| = 1$ we have

$$(\mathbf{z}_1, ..., \mathbf{z}_{q+1}) \in U \text{ if and only if } (\eta_1 \mathbf{z}_1, ..., \eta_{q+1} \mathbf{z}_{q+1}) \in U.$$

If U is measurable and if F is a fundamental domain (see Chapter 1 Section 3) of the unit lattice then $U(F)$ is measurable and the volume is finite. Moreover (b) implies that the volume does not depend on the particular choice of F (see [**17**] p.30), so that we can write

$$V_{U,K} = \text{Vol } (U(F)).$$

Gao defines

$$H_U^K(\boldsymbol{\alpha}) = N\mathfrak{A}^{-1} \inf\{\lambda^d; \lambda \geq 0, \sigma\boldsymbol{\alpha} \in \lambda U\}.$$

Here $\mathfrak{A}$ is the non-zero ideal generated by the coordinates $\alpha_0, ..., \alpha_n$ of $\boldsymbol{\alpha}$ and σ is as in (3.1.9). This is a height relative to K. In order to make it comparable with our height we have to take the d-th root so that

$$H_U(\boldsymbol{\alpha}) = H_U^K(\boldsymbol{\alpha})^{1/d}. \tag{B.0.1}$$

Moreover it is easily seen that the finite part $N\mathfrak{A}^{-1/d}$ can be expressed in the manner of (4.1.3) by choosing (3.1.2) for all finite v. We even may replace (3.1.2) for a finite number of finite places by N_v as in Subsection

1.2 of Chapter 3. This introduces c_v as in (3.1.3) and consequently $C_{\mathcal{N}}^{fin} = \prod_{v\nmid\infty} c_v^{-d_v/d}$. We need only the functions N_v at the finite places v but we do not want to introduce a new terminology and therefore let us stick to the whole ALS. So let $\mathcal{N}$ be an ALS of dimension n on K and U as above. Then we generalize (B.0.1) by setting

$$H_{\mathcal{N},U}(\boldsymbol{\alpha}) = \left(\prod_{v\nmid\infty} N_v(\sigma_v\boldsymbol{\alpha})^{d_v/d}\right) \inf\{\lambda; \lambda \geq 0, \sigma\boldsymbol{\alpha} \in \lambda U\}. \tag{B.0.2}$$

Now (b) and (ii) of Subsection 1.2 Chapter 3 together with the product formula implies that $H_{\mathcal{N},U}$ defines a height on $\mathbb{P}^n(K)$. This height could be referred to as an Arakelov-Gao-Lipschitz-height, short AGL-height. If we take the standard ALS with (3.1.2) for all v we recover Gao's height (B.0.1). Now choose F as in (3.3.19) with $\mathbf{i} = \mathbf{0}$. Then $U(F(\mathbf{0}))$ is the analogue of $S_{F(\mathbf{0})}(1)$ from Chapter 3. To count points of bounded height Gao applied Theorem 1.3 to the set $U(F(\mathbf{0}))$ and so he needs $U(F(\mathbf{0}))$ to be of narrow class s for some s. If we apply Theorem 1.2 we need no narrow class condition. But we need that the boundary $\partial U(F(\mathbf{0}))$ is in $\mathrm{Lip}(D, 1, M, L)$ for some M and L. Notice that by (a) and (3.3.28) we have $U(F(\mathbf{0})) \subseteq (S_{F(\mathbf{0})}(\infty) \cap \mu_2 U_0) = (\mu_2 S_{F(\mathbf{0})}(\infty) \cap \mu_2 U_0) = \mu_2(S_{F(\mathbf{0})}(\infty) \cap U_0) = \mu_2 S_{F(\mathbf{0})}(1) \subseteq B_0(r)$ where $r = \mu_2\sqrt{D}\exp\{q\}$. Suppose Conjecture A.1 in Appendix A is true then our Lipschitz condition condition is strictly weaker than Gao's narrow class condition.

To define a height on points P in $\mathbb{P}^n(\overline{\mathbb{Q}})$ with $[\mathbb{Q}(P) : \mathbb{Q}] = d$ Gao proceeds as follows. Assume for every K of degree d one has a set U_K and corresponding $\mu_2 = \mu_{2U_K}$. After choosing a reduced basis of the unit lattice one gets F and so $U(F(\mathbf{0}))$ and corresponding s. Gao has to assume that $\mu_2, s \ll 1$ whereas we need $\mu_2, L, M \ll 1$ and the implicit constants in $\ll$ depend only on n, d. Now for a point P in $\mathbb{P}^n(\overline{\mathbb{Q}})$ of degree d Gao defined

$$H(P) = H_{U_{\mathbb{Q}(P)}}. \tag{B.0.3}$$

In similar manner we may define Arakelov-Gao-Lipschitz-heights (AGL-heights) on $\mathbb{P}^n(\mathbb{Q}; d)$. Let us consider the more general situation where $\mathbb{Q}$ is replaced by an arbitrary number field k. Recall that $\mathcal{C}_e$ is the collection of all extensions of k of relative degree e and $[k : \mathbb{Q}] = m$ so that $[K : \mathbb{Q}] = me$ for each K in $\mathcal{C}_e$. Suppose we have a uniform ALS $\mathcal{N}$ of dimension n on $\mathcal{C}_e$ and a set U_K in $\mathrm{Lip}(D, 1, M_{U_K}, L_{U_K})$ with (a)

and (b) for each K in $\mathcal{C}_e$. For a point P in $\mathbb{P}^n(k;e)$ we then define

$$H(P) = H_{\mathcal{N}_{k(P)},U_{k(P)}}. \tag{B.0.4}$$

Note that by uniformity of $\mathcal{N}$ we may assume $C_{\mathcal{N}_K} \leq C_{\mathcal{N}}$ for a constant $C_{\mathcal{N}}$ (independent of K). This implies

$$C^{fin}_{\mathcal{N}_K} \leq C^{fin}_{\mathcal{N}_K} C^{inf}_{\mathcal{N}_K} = C_{\mathcal{N}_K} \leq C_{\mathcal{N}}$$

for each K in $\mathcal{C}_e$. Suppose there are constants μ, M, L (independent of K) such that

$$\mu_{2U_K} \leq \mu, \quad M_{U_K} \leq M, \quad L_{U_K} \leq L$$

for each K in $\mathcal{C}_e$. Then we call the resulting height a uniform AGL-height on $\mathbb{P}^n(k;e)$. Next consider

$$V_{\mathcal{N}_K,U_K} = V^{fin}_{\mathcal{N}_K} V^{inf}_{U_K}$$

where $V^{fin}_{\mathcal{N}_K}$ is as in (3.1.13) but $V^{inf}_{U_K}$ is defined as

$$V^{inf}_{U_K} = \frac{V_{U_K,K}}{R_K(n+1)^{r+s-1}}.$$

Now define

$$D_{\mathcal{N},U} = D_{\mathcal{N},U}(k,e,n) = \sum_K 2^{-r_K(n+1)} \pi^{-s_K(n+1)} V_{\mathcal{N}_K,U_K} S_K(n) \tag{B.0.5}$$

where the sum runs over all extensions of k with relative degree e.

Following the proof of the Main Theorem part (b) it is most likely that one can get the following result:

let $H = H_{\mathcal{N},U}$ be a uniform AGL-height on $\mathbb{P}^n(k;e)$ and denote by $Z_{\mathcal{N},U}(\mathbb{P}^n(k;e), X)$ its corresponding counting function. Suppose that either $e = 1$ or $n > 5e/2 + 4 + 2/(me)$. Then the sum in (B.0.5) converges and as $X > 1$ tends to infinity we have

$$Z_{\mathcal{N},U}(\mathbb{P}^n(k;e), X) = D_{\mathcal{N},U} X^{me(n+1)} + O(X^{me(n+1)-1} \log \max\{2, X\}),$$

where the logarithm in the error term can be omitted in all cases except $(me, n) = (1, 1)$. The constant in O depends only on $k, e, n, \mu, C_{\mathcal{N}}, M, L$.

For the proof one has to replace $S_{F(\mathbf{0})}(T)$ by

$$(TU)(F(\mathbf{0})) = (S_{F(\mathbf{0})}(\infty) \cap TU) = T(U(F(\mathbf{0}))).$$

Since by assumption $U(F(\mathbf{0}))$ lies in $\mathrm{Lip}(D, 1, M, L)$ it is clear that $TU(F(\mathbf{0}))$ lies in $\mathrm{Lip}(D, 1, M, LT)$ and thus one can get rid of the tedious Lemma 3.2. On the other hand applying this "theorem" would usually involve much more work than applying the Main Theorem since

proving $U(F(\mathbf{0})) \in \mathrm{Lip}(D, 1, M, L)$ is more difficult than verifying the condition (iii) for each $v \mid \infty$ in Subsection 1.2 of Chapter 3.

Bibliography

1. K. Ball, *Ellipsoids of maximal volume in convex bodies*, Geom. Dedicata **41** (1992), no. 1, 241–250.
2. M. Bhargava, *Higher Composition Laws*, Ph.D. Thesis, Princeton Univ. (2001).
3. E. Bombieri and W. Gubler, *Heights in Diophantine Geometry*, Cambridge University Press, 2006.
4. E. Bombieri and J. D. Vaaler, *On Siegel's lemma*, Invent. Math. **73** (1983), 11–32.
5. S. Bosch, U. Güntzer, and R. Remmert, *Non-Archimedean Analysis*, Springer, 1984.
6. M. R. Bridson and A. Haefliger, *Metric Spaces of Non-Positive Curvature*, Springer, 1999.
7. J. W. S. Cassels, *An Introduction to the Geometry of Numbers*, Springer, 1997.
8. S-J. Chern and J. D. Vaaler, *The distribution of values of mahler's measure*, J. reine angew. Math. **540** (2001), 1–47.
9. B. Datskovsky and D. J. Wright, *Density of discriminants of cubic field extensions*, J. reine angew. Math. **386** (1988), 116–138.
10. H. Davenport, *On a principle of Lipschitz*, J. London Math. Soc. **26** (1951), 179–183.
11. H. Davenport and H. Heilbronn, *On the density of discriminants of cubic field extensions. II*, Proc. London. Math. Soc. **322** (1971), 405–420.
12. H. Cohen F. Diaz Y Diaz and M. Olivier, *Enumerating quartic dihedral extensions of* $\mathbb{Q}$, Comp. Math. **133** (2002), 65–93.
13. M. do Carmo, *Differentialgeometrie von Kurven und Flächen*, Vieweg, 1983.
14. 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.
15. J. H. Evertse, *On equations in S-units and the Thue-Mahler equation*, Invent. Math. **75** (1984), 561–584.
16. G. Faltings, *Endlichkeitssätze für abelsche Varietäten über Zahlkörpern*, Invent. Math. **73** (1983), 349–366.
17. X. Gao, *On Northcott's Theorem*, Ph.D. Thesis, University of Colorado (1995).
18. R. Heath-Brown, *Counting rational surfaces on cubic surfaces*, Astérisque **251** (1998), 13–30.
19. ———, *The density of rational points on curves and surfaces*, Astérisque **155** (2002), 553–598.
20. Y. I. Manin J. Franke and Y. Tschinkel, *Rational points of bounded height on Fano varieties*, Invent. Math. **95** (1989), 421–435.
21. M. Kurita, *An extension of Poincaré's formula in integral geometry*, Nagoya Math. J. **2** (1951), 55–61.
22. S. Lang, *Fundamentals of Diophantine Geometry*, Springer, 1983.

23. ———, *Algebraic Number Theory*, Springer, 1994.
24. ———, *Algebra*, Addison Wesley, 1999.
25. A. Leutbecher, *Zahlentheorie*, Springer, 1996.
26. C. Liebendörfer, *Linear Equations and Heights over Division Algebras*, Ph.D. Thesis, Universität Basel (2002).
27. ———, *Linear equations and heights over division algebras*, J. Number Theory **105** (2004), 101–133.
28. T. Loher, *Counting Points of Bounded Height*, Ph.D. Thesis, Universität Basel (2001).
29. T. Loher and D. W. Masser, *Uniformly counting points of bounded height*, Acta Arith. **111** (2004), 277–297.
30. W. Maak, *Schnittpunktanzahl rektifizierbarer und nichtrektifizierbarer Kurven*, Math. Ann. **118** (1942), 299–304.
31. G. Malle, *On the distribution of Galois groups*, J. Number Theory **92** (2002), 315–329.
32. D. W. Masser, *Counting points with multiplicatively dependent coordinates on a curve*, Diophantine Geometry (ed. U. Zannier), Edizioni della Normale (2007), 221–236.
33. D. W. Masser and J. D. Vaaler, *Counting algebraic numbers of large height I*, submitted (2004).
34. ———, *Counting algebraic numbers of large height II*, Trans. Amer. Math. Soc. **359** (2007), 427–445.
35. D. McKinnon, *Counting rational points on ruled varieties*, Canad. Math. Bull. **47** (2004), 264–270.
36. J. Neukirch, *Algebraische Zahlentheorie*, Springer, 1992.
37. D. G. Northcott, *An inequality in the theory of arithmetic on algebraic varieties*, Proc. Cambridge Phil. Soc. **45** (1949), 502–509 and 510–518.
38. E. Peyre, *Counting points on varieties using universal torsors*, Arithmetic of higher-dimensional algebraic varieties, (B. Poonen, Yu. Tschinkel, eds.), Progress in Mathematics, Birkäuser Boston, Cambridge, MA **226** (2004), 61–81.
39. D. Roy and J. L. Thunder, *A note on Siegel's lemma over number fields*, Monatsh. Math. **120** (1995), 307–318.
40. ———, *An absolute Siegel's lemma*, J. reine angew. Math. **476** (1996), 1–26.
41. L. A. Santaló, *Introduction to Integral Geometry*, Publications de l'institut mathématique de l'université de nancago, 1953.
42. ———, *Integral Geometry and Geometric Probability*, Addison Wesley, 1979.
43. S. H. Schanuel, *Heights in number fields*, Bull. Soc. Math. France **107** (1979), 433–449.
44. A. Schinzel, *Polynomials with Special Regard to Reducibility*, Encyclopedia of Mathematics and its applications, vol. 77, Cambridge University Press, 2000.
45. W. M. Schmidt, *On heights of algebraic subspaces and diophantine approximations*, Ann. of Math. **85** (1967), 430–472.
46. ———, *Asymptotic formulae for point lattices of bounded determinant and subspaces of bounded height*, Duke Math. J. **35** (1968), 327–339.
47. ———, *Diophantine Approximations and Diophantine Equations*, Lecture Notes in Mathematics 1467, Springer, 1991.

48. ———, *Northcott's Theorem on heights I. A general estimate*, Monatsh. Math. **115** (1993), 169–183.
49. ———, *Northcott's Theorem on heights II. The quadratic case*, Acta Arith. **70** (1995), 343–375.
50. ———, *Number fields of given degree and bounded discriminant*, Astérisque **228** (1995), 189–195.
51. ———, *The distribution of sublattices of* $\mathbb{Z}^m$, Monatsh. Math. **125** (1998), 37–81.
52. C. L. Siegel, *Über einige Anwendungen diophantischer Approximationen*, Abh. der Preuss. Akad. der Wissenschaften. Phys.-math. Kl. 1929, Nr.1.
53. ———, *Gesammelte Abhandlungen Band IV*, Springer, 1979.
54. J. Silverman, *Lower bounds for height functions*, Duke Math. J. **51** (1984), 395–403.
55. A. Thue, *Über Annäherungswerte algebraischer Zahlen*, J. reine angew. Math. **135** (1909), 284–305.
56. J. L. Thunder, *An asymptotic estimate for heights of algebraic subspaces*, Trans. Amer. Math. Soc. **331** (1992), 395–424.
57. ———, *Asymptotic estimates for rational points of bounded height on flag varieties*, Comp. Math. **88** (1993), 155–186.
58. ———, *The number of solutions of bounded height to a system of linear equations*, J. Number Theory **43** (1993), 228–250.
59. ———, *An adelic Minkowski-Hlawka theorem and an application to Siegel's lemma*, J. reine angew. Math. **475** (1996), 167–185.
60. ———, *Remarks on adelic geometry of numbers*, Number theory for the millenium III. Proceedings of the millennial conference on number theory, Urbana-Champaign, IL, USA, May 21-26, 2000 (M. A. Bennett et al, ed.) (2002), 253–259.
61. M. Widmer, *Eine effektive Version eines Satzes von Schmidt*, Diplomarbeit, Universität Basel (2003).
62. ———, *On number fields with proper subfields*, In preparation (2007).

Curriculum Vitae

Ich, Martin Lucien Widmer bin am 2. Juni 1978 in Basel geboren. Meine Eltern sind Paul Widmer und Jana Widmer-Köppel. Mein Heimatort ist Mosnang SG.

Ausbildung

Aug. 1994	-	Dez. 1997	Gymnasium Oberwil, Baselland. Grad: Matura.
Okt. 1998	-	Okt. 2000	Grundstudium in Mathematik an der Universität von Basel. Grad: Vordiplom.
Okt. 2000	-	Sept. 2003	Aufbaustudium in Mathematik an der Universität von Basel. Grad: Diplom.
Okt. 2003	-	Okt. 2007	Assistent und Doktorand unter der Anleitung von Prof. D. W. Masser an der Universität Basel.
18. Okt. 2007			Doktorkolloquium.

Ich habe teilgenommen an mathematischen Konferenzen in Marseille, Lausanne, Wien, Oberwolfach und Bonn. Während meines Studiums besuchte ich Vorlesungen und Seminare von Prof. C. Bandle, Prof. Y. Bilu, Prof. W. Gautschi, Prof. J. Königsmann, Prof. H. Kraft, Prof. D. W. Masser, Dr. S. Mohrdieck, Prof. W. Reichel, Prof. B. Scarpellini, Prof. U. Schmock, Prof. A. Shumakovitch, Prof. F. Thielemann, Prof. H. Thomas, Prof. D. Trautmann und Prof. A. Wagner.