ACTA ARITHMETICA
111.3 (2004)

# Uniformly counting points of bounded height

by

Thomas Loher (Zürich) and David Masser (Basel)

**1. Introduction.** In this paper we give some new uniform estimates for the cardinalities of certain sets involving algebraic numbers of bounded height. The estimates are nearly optimal with respect to the degree of the number field. We mention some applications to problems about multiplicatively independent and dependent numbers in situations occurring in the recent theory of linear forms in logarithms associated with the name of Matveev. We also extend our counting estimates to algebraic vectors.

Let $K$ be a number field of degree $d=[K:\mathbb{Q}]$ over the rational field $\mathbb{Q}$. We use the absolute height function defined for $\alpha$ in $K$ by

$$H(\alpha)^d=\prod_v \max\{1,|\alpha|_v\}, \tag{1.1}$$

where the product is over all representatives $v$ of equivalence classes of valuations on $K$. These representatives are normalized in such a way that $H(a)=a$ for all positive $a$ in $\mathbb{Q}$; this is possible in a unique way. For example, if $v$ corresponds to an embedding $\sigma$ of $K$ into the complex field, then $|\alpha|_v=|\sigma(\alpha)|^f$, where $f=1$ if $\sigma(K)$ is in the real field $\mathbb{R}$ and $f=2$ otherwise. In general see Lang [La2, pp. 19–21, 50–52] or Waldschmidt [W, pp. 67–75].

To begin with, we are interested for real numbers $H\ge 1$ in the sets $K(H)$ consisting of all $\alpha$ in $K$ with $H(\alpha)\le H$. A classical theorem of Northcott [N] from 1949 implies that $K(H)$ is a finite set. And a more recent theorem of Schanuel [Scha] from 1979 (usually stated for projective space) implies that its cardinality $\#K(H)$ is asymptotic as $H\to\infty$ to $S_KH^{2d}$, where $S_K$ is independent of $H$. In fact

$$S_K=h_KR_K\{2^{r_K}(2\pi)^{s_K}/\sqrt{|\Delta_K|}\}^2\cdot 2^{r_K+s_K-1}/\{w_K\zeta_K(2)\} \tag{1.2}$$

involves several standard field constants; namely, the class number $h_K$, the regulator $R_K$, the discriminant $\Delta_K$, the number $w_K$ of roots of unity in $K$,

2000 *Mathematics Subject Classification*: 11G50, 11R04, 14G40.

and the Dedekind zeta-function $\zeta_K(s)$, as well as the number $r_K$ of real embeddings of $K$ and the number $s_K$ of pairs of complex conjugate embeddings.

Schanuel gave an error term bounded by $C_K H^{2d-1} \log H$ (where the logarithm can be omitted if $d \geq 2$), but no published estimates for $C_K$ appeared until 1995. They apply only to $d = 2$ (the case $d = 1$ being easy), and are due to Schmidt [Schm3, Theorem 2, p. 345 for $n = 1$].

It was Evertse in 1984 who first proved the general existence of simple explicit upper bounds for $\#K(H)$ and any $H \geq 1$. His Lemma 1 (p. 570) in [E] implies the bound $5 \cdot 2^d H^{3d} + 1$. In 1991 his argument was modified by Schmidt [Schm1] to get the correct exponent $2d$ of $H$ (see Lemma 8B, p. 29, which however applies to a slightly different height). Shortly afterwards in 1993 Schmidt gave the upper bound $2^{5d+22} H^{2d}$; see the Theorem (p. 170) of [Schm2] (in particular equation (1.4) for his $d = n = 1$ and $X = H^d$). In fact his equation (4.3) on p. 176 (with $s = 1$, $\theta = 1$) gives the slightly better inequality

$$\#K(H) \leq 2^{d+5} H^{2d} \tag{1.3}$$

for any $H \geq 1$.

All these uniform estimates provide valuable alternatives to the asymptotic formulae, because they are independent of the complicated field structure of $K$; for example Evertse used them in [E] to prove his celebrated uniform bounds for the number of solutions of $S$-unit equations over $K$.

But for small $H$ they are not too accurate in view of the exponential dependence on $d$. Thus if $H = 1$ is as small as possible then, by Kronecker's Theorem [K], $\#K(H) - 1$ is just the number $w_K$ of roots of unity in $K$. This satisfies $\phi(w_K) \leq d$ for Euler's totient function $\phi$. Now $\phi(x)/\sqrt{x} \to \infty$ as $x \to \infty$, for example, and so $w_K$ is certainly of order at most $d^2$.

And it was stated without proof by the second author in 1989 that there is a positive constant $C$ such that for the small value $H = \exp(1/Cd)$ one has

$$\#K(H) \leq Cd \log d \tag{1.4}$$

provided $d \geq 2$. See [Mas, p. 263].

A proof of (1.4), and indeed much more, was recently given by the first author in 2001 in his Basel Ph.D. thesis [Lo]. In his Theorem 1 (p. 9) he proved for any $H \geq 1$ that

$$\#K(H) \leq 37(d \log d) H^{2d} \tag{1.5}$$

provided $d \geq 2$. This improves (1.3) and implies (1.4) with say $C = 39$.

For $H = 1$ it yields the upper bound $w_K < 37 d \log d$. As remarked in [Lo, p. 4], this compares quite well with the estimate $\phi(w_K) \leq d$ mentioned above. For it is known (see for example [HW, Theorem 328, pp. 267, 353, 354]) that $\phi(x)$ is asymptotically as small as $e^{-\gamma}x/\log\log x$ when $x = 2\cdot 3\cdot 5\dots$ is a product of consecutive primes, with Euler's constant $\gamma$. So we get an upper bound asymptotically $e^{\gamma}d(\log\log d)$. Furthermore if $K$ is cyclotomic then $\phi(w_K) = d$, and we can take $w_K$ as such a product of primes, so this asymptotic bound is best possible. It follows that (1.5) would be false with $O(d\log d)$ replaced by $o(d\log\log d)$.

Loher's Theorem 1 also contains the estimate

$$\#K(H) \le 13(d\log d)H^{2d} \tag{1.6}$$

if $K$ has a real embedding ($r_K \ge 1$). And if $K$ has a prime ideal of norm 2, he proved $\#K(H) \le 16(d\log d)H^{2d}$; coincidentally one might expect $S_K$ also to be slightly smaller in this case, as now $\zeta_K(2) > 5/4$ in (1.2) is bounded away from 1.

Indeed an amusing consequence of (1.5) is the inequality

$$S_K \le 37d\log d \tag{1.7}$$

for Schanuel's constant when $d \ge 2$. It does not seem easy to prove this directly from the definition; indeed the term $2^{r_K+s_K}$ alone in (1.2) exceeds $2^{d/2}$.

As remarked in [Lo, p. 10] these asymptotic considerations show that we cannot hope for similar uniform lower bounds for $\#K(H)$. In fact there is no positive constant $C = C(d)$ such that $\#K(H) \ge C^{-1}H^{2d}$ for all $H \ge 1$. For this would imply $S_K \ge C^{-1}$. But on the other hand $\zeta_K(2) > 1$, and by the Siegel–Brauer Theorem (see for example [La1, Corollary, p. 328]) we have $h_K R_K \le |\Delta_K|^{3/4}$ if $|\Delta_K|$ is large enough. It follows that $S_K < C_1|\Delta_K|^{-1/4}$ for some $C_1 = C_1(d)$, leading to a contradiction if further $|\Delta_K| \ge (CC_1)^4$.

In fact the results of Evertse [E] and Schmidt [Schm1] apply to a slightly more general situation. It is well known that the height $H(\alpha)$ extends to all $\alpha$ in the algebraic closure $\overline{\mathbb{Q}}$. These authors take an arbitrary non-zero $\theta$ in $\overline{\mathbb{Q}}$ and obtain similar uniform upper bounds, independent even of $\theta$, for the number of $\alpha$ in $K$ with $H(\theta\alpha) \le H$. For $\theta = 1$ (or indeed for any $\theta$ in $K$) this number is none other than $\#K(H)$.

Our first main result is a similar generalization of (1.5).

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

It would be interesting to know if there are asymptotic formulae like Schanuel's for the cardinalities here, at least for fixed $\theta$ not in $K$. At any rate the known formula for $\theta = 1$ leads to the small improvement $S_K \le 31d\log d$ of (1.7). With a bit more effort we can prove

THEOREM 2. *For Schanuel's constant we have*

$$S_K \leq 21 d \log d$$

*provided* $d \geq 2$.

We can also deduce some reasonable lower bounds for heights; for example in [Lo, Corollary 1, p. 23] it is shown that the logarithmic height

$$h(\alpha) = \log H(\alpha)$$

satisfies $h(\alpha) \geq (1/37) d^{-2} (\log d)^{-1}$ if $d \geq 2$ and $\alpha \neq 0$ in $K$ is not a root of unity. The present paper allows a small numerical improvement; however if $d \geq 4$ this is inferior to Voutier's [V] inequality

$$h(\alpha) \geq \tfrac{1}{4} d^{-1} (\log d / \log\log d)^{-3}.$$

It was pointed out to us by Amoroso that results like Theorem 1 for $\theta = 1$ imply lower bounds for products $h(\alpha_1) \ldots h(\alpha_n)$ that improve some work of Matveev. This work is designed for applications to linear forms in logarithms of algebraic numbers, for which it is important to have no worse than exponential dependence on the number $n$. Using Theorem 1 for a certain $\theta \neq 1$ (which actually appears at first sight to be transcendental!), we can improve this dependence even further.

During a lecture at Boulder in March 2001, Yu explained that Matveev's application involves a certain lattice defined for $\alpha_1, \ldots, \alpha_n$ in $K$, together with an upper bound for a related lattice index. Conversations with Yu led us to define a more intrinsic lattice, and we prove an index bound that includes Matveev's index bound. It also implies the lower bound for $h(\alpha_1) \ldots h(\alpha_n)$ just mentioned.

Thus for $n \geq 1$ let $\alpha_1, \ldots, \alpha_n$ be non-zero elements of our field $K$. We look at $r_1, \ldots, r_n$, $s \geq 1$ in the ring $\mathbb{Z}$ of all rational integers, and we define $\mathcal{M}_K(\alpha_1, \ldots, \alpha_n)$ as the set of all $(r_1/s, \ldots, r_n/s)$ in $\mathbb{Q}^n$ such that $\alpha_1^{r_1} \ldots \alpha_n^{r_n}$ is a perfect $s$th power in $K$. Taking $s = 1$ we see that this set contains $\mathbb{Z}^n$. Alternatively $\mathcal{M}_K(\alpha_1, \ldots, \alpha_n)$ is the set of all $(\xi_1, \ldots, \xi_n)$ in $\mathbb{Q}^n$ such that some (and therefore every) determination of $\alpha_1^{\xi_1} \ldots \alpha_n^{\xi_n}$ has the form $\mu\beta$ for some root of unity $\mu$ in $\overline{\mathbb{Q}}$ and some $\beta$ in $K$.

THEOREM 3. *For* $n \geq 1$ *let* $\alpha_1, \ldots, \alpha_n$ *be multiplicatively independent non-zero elements of a number field* $K$ *of degree* $d$. *Then the set* $\mathcal{M} = \mathcal{M}_K(\alpha_1, \ldots, \alpha_n)$ *is an additive subgroup of* $\mathbb{Q}^n$ *and the index* $[\mathcal{M} : \mathbb{Z}^n]$ *is finite. If* $d \geq 2$ *we have*

$$w_K [\mathcal{M} : \mathbb{Z}^n] \leq 58 (n! e^n / n^n) d^{n+1} (\log d) h(\alpha_1) \ldots h(\alpha_n),$$

*and if* $d = 1$ *the expression* $58 d^{n+1} (\log d)$ *may be replaced by* 17.

The quantity $n! e^n / n^n$ is at most $e\sqrt{n}$ and is asymptotic to $\sqrt{2\pi n}$, so apart from $d^{n+1}$ there is no exponential dependence on $n$ at all.

The consequence for heights is immediate.

Corollary 3.1. *For $n \geq 1$ let $\alpha_1, \ldots, \alpha_n$ be multiplicatively independent non-zero elements of a number field $K$ of degree $d \geq 2$. Then*

$$h(\alpha_1)\ldots h(\alpha_n) \geq (w_K/58)(n!e^n/n^n)^{-1}d^{-n-1}(\log d)^{-1}. \tag{1.8}$$

A result similar to (1.8), without the $w_K$ and weaker essentially by an extra exponential factor $2^n$, occurs as Theorem 4 (p. 23) of [Lo]. It is precisely the possibility $\theta \neq 1$ in our Theorem 1 which eliminates the $2^n$.

Matveev's work [Mat2], especially equation (6.5) on p. 418, implies a result like (1.8) with an extra $(3.053\ldots)^n$, provided $K$ has a real embedding. If $K$ has no real embedding then his substitute (6.4) appears to involve additional complex logarithms of $\alpha_1, \ldots, \alpha_n$; see also equation (5.1) on p. 1228 of his later paper [Mat3].

And in equation (6.3) of [Mat2] (p. 418) there is a lattice index $[\Lambda_n : \Lambda_n']$, which also appears to involve complex logarithms.

Regarding (1.8), we should mention that for $d \to \infty$ and fixed $n$ much sharper lower bounds of the form

$$h(\alpha_1)\ldots h(\alpha_n) \geq C(n)^{-1}d^{-1}(\log d)^{-\Lambda(n)} \tag{1.9}$$

were established by Amoroso and David; see Théorème 1.6 (p. 148) of [AD]. Here $\Lambda(n)$ behaves like $(n!)^n$, and $C(n) > 0$ is not yet explicitly calculated.

Amoroso has also remarked that conversely any lower bound like (1.9) implies via Minkowski's Second Theorem an index bound of the shape

$$[\mathcal{M} : \mathbb{Z}^n] \leq C'(n)d(\log d)^{\Lambda(n)}h(\alpha_1)\ldots h(\alpha_n) \tag{1.10}$$

like Theorem 3 but without the factor $w_K$. An extra $w_K$ in (1.10) would have interesting consequences for lower bounds of heights over cyclotomic fields. Otherwise (1.10) is much better than Theorem 3 for large $d$.

In this context one should also point out that an observation of Bilu [Bi] leads to a lower bound

$$h(\alpha_1)\ldots h(\alpha_n) \geq c^{-n/2}d^{-n/2}(\log d)^{-\lambda n/2}$$

with $c = C(2)$ and $\lambda = \Lambda(2)$ in (1.9). This is a nice compromise between (1.8) and (1.9), and indeed it beats (1.8) as soon as $d$ exceeds a certain absolute constant.

Here is another consequence of Theorem 3, now for multiplicatively dependent algebraic numbers. The idea for this came from Yu, and we are grateful to him for permission to include the details in the present paper.

Corollary 3.2 (Yu). *For $n \geq 1$ let $\alpha_0, \ldots, \alpha_n$ be multiplicatively dependent non-zero elements of a number field $K$ of degree $d \geq 2$. Suppose that any $n$ from $\alpha_0, \ldots, \alpha_n$ are multiplicatively independent. Then there are* *non-zero rational integers* $b_0, \ldots, b_n$ *with* $\alpha_0^{b_0} \ldots \alpha_n^{b_n} = 1$; *further if* $d \geq 2$ *one can take*

$$|b_i| \leq 58(n!e^n/n^n)d^{n+1}(\log d)h(\alpha_0)\ldots h(\alpha_n)/h(\alpha_i) \qquad (0 \leq i \leq n),$$

*and if* $d = 1$ *the expression* $58d^{n+1}(\log d)$ *may be replaced by* $17$.

Such results are also familiar in the theory of linear forms in logarithms. Some particularly good recent versions occur in the work [Mat1] of Matveev (for example Theorem 4, p. 423); compare also Bertrand's paper [Be] (for example p. 207). These supply bounds for all relations. See also the references in [W] (p. 222).

The result above for a single relation is especially favourable as a function of $n$. It would actually become false if there are more relations, that is, without the extra independence hypothesis. For then we could take $\alpha_0, \ldots, \alpha_n$ all equal to some $\alpha$ in $K$ not a root of unity, and the inequalities in this case would trivially imply $1 \leq 58(n!e^n/n^n)d^{n+1}(\log d)(h(\alpha))^n$; but now making $n \to \infty$ would yield $h(\alpha) \geq 1/d$, easily seen to be an impossibly strong version of the Lehmer inequality.

So much for counting $K(H)$ and applications. Our arguments lead naturally to analogous counting results in higher dimensions.

Thus for $m \geq 1$ and $\alpha_1, \ldots, \alpha_m$ in $K$ one defines

$$(1.11) \qquad H(\alpha_1, \ldots, \alpha_m)^d = \prod_v \max\{1, |\alpha_1|_v, \ldots, |\alpha_m|_v\}$$

generalizing (1.1), and for $H \geq 1$ correspondingly $K^m(H)$ as the set of all $(\alpha_1, \ldots, \alpha_m)$ in $K^m$ with $H(\alpha_1, \ldots, \alpha_m) \leq H$. Again Northcott's Theorem implies that $K^m(H)$ is finite; and Schanuel's Theorem leads to the asymptotic expression

$$(1.12) \qquad S_K(m)H^{(m+1)d}$$

for $\#K^m(H)$ as $H \to \infty$, where now

$$(1.13) \quad S_K(m) = h_K R_K \{2^{r_K}(2\pi)^{s_K}/\sqrt{|\Delta_K|}\}^{m+1}(m+1)^{r_K+s_K-1}/\{w_K \zeta_K(m+1)\}$$

generalizes (1.2). Again the shape of the error term is known, but the only published estimates are for $d = 2$, also due to Schmidt [Schm3] (p. 345, just after Theorem 2).

And in 1993 Schmidt [Schm2] was the first to obtain uniform upper bounds in higher dimensions. His equation (1.4) of the Theorem (p. 170) implies the estimate

$$(1.14) \qquad \#K^m(H) \leq 2^{m^2+10m+11} \cdot 2^{(m+4)d} \cdot H^{(m+1)d}$$

for any $H \geq 1$.

The first step towards removing the above exponential factor in $d$ was taken by the first author [Lo] in dimension $m = 2$. His Theorem 4 (p. 26) states that

$$\#K^2(H) \leq 2^{17}(d\log d)^2 H^{7d/2} \tag{1.15}$$

provided $d \geq 2$. As the exponent $7d/2$ is not the exponent $(m+1)d = 3d$ of (1.12), there are no immediate consequences for the associated Schanuel constant $S_K(2)$. However (1.15) does improve the estimate $\{37(d\log d)H^{2d}\}^2$ arising from (1.5) and the elementary inequality $H(\alpha_1, \alpha_2) \geq \max\{H(\alpha_1), H(\alpha_2)\}$.

Here we obtain the correct exponent in (1.15) and generalize to arbitrary $m$.

Theorem 4. *Let $K$ be a number field of degree $d \geq 2$, let $m \geq 1$, and let $H \geq 1$ be real. Then there are at most $(1088d\log d)^m H^{(m+1)d}$ elements $(\alpha_1, \ldots, \alpha_m)$ in $K^m$ with $H(\alpha_1, \ldots, \alpha_m) \leq H$.*

As in (1.5), the roots of unity mean that the factor $(d\log d)^m$ is fairly near best possible; $K^m$ contains at least $w_K^m$ elements with height 1.

The following is an immediate consequence after comparing with (1.12).

Corollary 4.1. *For Schanuel's constant we have*

$$S_K(m) \leq (1088d\log d)^m$$

*provided $d \geq 2$.*

Another curious consequence is the following. If $\Delta$ is the discriminant of a number field of degree $d \geq 2$ with $r$ real embeddings and $s$ pairs of complex conjugate embeddings then

$$|\Delta| \geq 4^r(2\pi)^{2s}/(1088d\log d)^2. \tag{1.16}$$

This comes from making $m \to \infty$ in the above corollary and noting that $\zeta_K(m+1) \to 1$ in (1.13). It may be compared with the classical Minkowski bound $(d^d/d!)^2(\pi/4)^{2s}$, which behaves asymptotically like $(e^2)^r(\pi e^2/4)^{2s}$. Although our 4 is inferior to $e^2 = 7.389\ldots$, our $2\pi = 6.283\ldots$ is superior to $\pi e^2/4 = 5.803\ldots$ So (1.15) is sometimes better, for example if $r < (.1146\ldots)d$ and $d \to \infty$.

This consequence (1.16) is actually no more than curious, because the Minkowski bound has been sharpened by several authors, including Blichfeldt [Bl], Rogers [Ro], Mulholland [Mu], and most recently Odlyzko [O]; the last-named with an asymptotic lower bound of $60^r 22^{2s}$. And even Blichfeldt's result (from 1939) is asymptotically much better than (1.16).

We close this introduction with some remarks about the proofs of our results. The main idea behind (1.3) is the following. If $\#K(H)$ is very large the Box Principle gives two different $\alpha_1$ and $\alpha_2$ in $K(H)$ which are very close with respect to some embedding of $K$. Then the Product Formula on $\alpha_1 - \alpha_2$ yields a contradiction. The $2^d$ in (1.3) arises specifically from the coefficient 2 in the inequality

$$|z_1 - z_2| \leq 2\max\{1, |z_1|\}\max\{1, |z_2|\} \tag{1.17}$$

for the other conjugates $z_1, z_2$ of $\alpha_1, \alpha_2$. The first author's main idea in [Lo] was to find not just two but $N$ different numbers $\alpha_1, \ldots, \alpha_N$ which are close. The corresponding quantity $\prod_{1\leq i<j\leq N} |z_i - z_j|$ can then be estimated using Hadamard's inequality on the Vandermonde determinant, leading to a coefficient $N^{N/2}$ instead of 2. This is a lot better than the coefficient $2^{N(N-1)/2}$ which would arise from applying (1.17) to each $|z_i - z_j|$ separately. In Section 2 we record such estimates as well as a suitable version of the Box Principle.

Then in Section 3 we use these results to prove a basic technical counting Proposition. In Section 4 we deduce Theorems 1 and 2.

In Section 5 we prove Theorem 3, and finally in Section 6 we deduce Theorem 4 from the Proposition using essentially the same ingenious inductive argument of Schmidt in [Schm2]. This replaces the original argument in Chapter 2 of [Lo], which proves (1.15) by means of a generalization of the Vandermonde determinant associated with Laurent's method in transcendence theory and the Bombieri–Pila method for counting points on curves.

After most of this paper was completed we realized that our underlying proof strategy is not really all that different from that introduced by Matveev in [Mat2]. Thus our Proposition in Section 3 plays a role similar to that of his Lemma 7.2 (p. 419), except that we build in the Box Principle while he applies it separately on p. 421. Both proofs are based on the Vandermonde determinant. We estimate it directly using our Lemmas 1 and 2 of Section 2, while he uses the Maximum Modulus Principle on p. 420.

We wish to thank Francesco Amoroso for his many comments on [Lo] and in particular about the applications to Matveev's estimates. We are also grateful to Yu Kunrui for conversations about these applications, and especially for permission to include his Corollary 3.2.

**2. Geometric preparations.** We require two results on the "discriminant function"

$$\Delta(t_1, \ldots, t_N) = \prod_{1\leq i<j\leq N} (t_i - t_j)$$

for an integer $N \geq 2$. This function also plays an important role in [Ro] and [Mu] (but not [O]). Our results can be found in [Lo], but for the convenience of the reader we reproduce everything here.

Lemma 1. *For any real $r > 0$ and any complex $t_1, \ldots, t_N$ in any disc of radius $r$ we have*

$$|\Delta(t_1, \ldots, t_N)| \le N^{N/2} r^{N(N-1)/2}.$$

*Proof.* This is Lemma 1 (p. 11) of [Lo]. By translation we may assume that the centre of the disc is 0; and by replacing each $t_i$ by $t_i/r$ using homogeneity we may further assume that $r = 1$. Now the result is an immediate consequence of the Hadamard inequality for the Vandermonde determinant for $(-1)^{N(N-1)/2}\Delta(t_1, \ldots, t_N)$, in which the $i$th row $(1, t_i, \ldots, t_i^{N-1})$ has squared length

$$1 + |t_i|^2 + \ldots + |t_i^{N-1}|^2 \le N \quad (1 \le i \le N).$$

The theory of the transfinite diameter (see for example [Ra]) shows that Lemma 1 is quite sharp. In fact an upper bound of the shape $\exp\{o(N^2)\}x^{N(N-1)/2}$ for any $x < r$ independent of $N$ would imply that the transfinite diameter of a complex disc of radius $r$ is at most $x$; but this transfinite diameter is exactly $r$.

And even any bound $N^{c(N)N/2} r^{N(N-1)/2}$ with $\lim c(N) < 1$ is also false, because $|\Delta(1, \mu, \ldots, \mu^{p-2})| = p^{(p-2)/2}$ if $p = N + 1$ is prime and $\mu = e^{2\pi i/p}$.

If $t_1, \ldots, t_N$ are real then of course the estimate of Lemma 1 remains valid. But the transfinite diameter of a real interval of half-length $r$ is $r/2$, not $r$. So some improvement can be expected, as in the following result.

Lemma 2. *For any real $r > 0$ and any real $t_1, \ldots, t_N$ in any interval of half-length $r$ we have*

$$|\Delta(t_1, \ldots, t_N)| \le U_N (r/2)^{N(N-1)/2},$$

*where*

$$U_N = \{2^{N(N-1)}(N-1)^{N-1}N^N\}^{1/2} \prod_{k=1}^{N-2} \{k^k/(2k+1)^{(2k+1)/2}\} \quad (N \ge 3)$$

*and $U_2 = 4$.*

*Proof.* This is Lemma 2 (p. 12) of [Lo]. By translation and homogeneity we may assume that the interval is $[-1, 1]$, so that $r = 1$. In this case the true maximum of $|\Delta(t_1, \ldots, t_N)|$ was determined by Schur [Schu, p. 378] as $2^{-N(N-1)/2}U_N$. The result follows.

Thus again any upper bound $\exp\{o(N^2)\}x^{N(N-1)/2}$ for $x < r/2$ would be false.

In fact $U_N$ behaves like $N^{N/2}$ for large $N$. But to estimate it explicitly we need the following remark.

Lemma 3. *For every $N \ge 2$ we have $U_N \le N^{2N}$.*

*Proof.* This is Lemma 3 (p. 12) of [Lo]. If $N = 2$ the inequality is trivial; however $U_2 = 4$ and so it is not good. If $N \geq 3$ we observe that $k^k/(2k+1)^{(2k+1)/2} \leq 2^{-k}$ in $U_N$, so the product is at most $2^{-(N-1)(N-2)/2}$. It follows that $U_N < N^{2N}$ as desired.

In standard applications of the Box Principle say in two dimensions, there is not much of a problem if the boxes are small squares in a large square. But some inefficiency may arise if we use circles. A simple way of dealing with this was given in Lemma 4 (p. 12) of [Lo], which we now reformulate in terms of multiple packings.

Let $f \geq 1$ and $N \geq 2$ be integers. We say that a set of balls forms an $(N-1)$-*fold packing* of a set $\mathcal{S}$ in real Euclidean space $\mathbb{R}^f$ if they are contained in $\mathcal{S}$ and no point of $\mathcal{S}$ lies in $N$ of the interiors; that is, when the balls are $\mathcal{B}_1, \ldots, \mathcal{B}_M$, then there is no subset $\mathcal{I}$ of $\{1, \ldots, M\}$ with cardinality $N$ such that some point of $\mathcal{S}$ is in the interior of all $\mathcal{B}_i$ ($i$ in $\mathcal{I}$). When $N = 2$ this is just the definition of a packing.

Lemma 4. *For any real $r > 0$, $R \geq r$ suppose that we are given $M$ balls of radius $r$ that form an $(N-1)$-fold packing of a ball of radius $R$ in $\mathbb{R}^f$. Then*

$$M \leq (N-1)(R/r)^f. \tag{2.1}$$

*If further $f = 2$ and $N = 2$ then*

$$M \leq \max\{1, (\pi/\sqrt{12})(R/r)^2\}. \tag{2.2}$$

*Proof.* Actually (2.1) is equivalent to Lemma 4 of [Lo], but the packing language makes the proof almost obvious: the sum of all the measures of the small balls cannot exceed $N-1$ times the measure of the large one.

And if $f = N = 2$ then we have a finite packing problem in the plane, solved by Fejes Tóth [FT] (p. 90, see also p. 67): a convex set of area $A \geq \sqrt{12}$ contains at most $A/\sqrt{12}$ disjoint unit discs. If $\pi(R/r)^2 \geq \sqrt{12}$ we apply this to a suitable disc of radius $R/r$ to deduce (2.2). And if $\pi(R/r)^2 < \sqrt{12}$ then (2.2) is trivial.

The constant $\pi/\sqrt{12}$ in (2.2) is the optimal asymptotic packing density of equal discs in the plane, as first proved by Thue, and so it is optimal in our finite non-asymptotic situation. Already in $\mathbb{R}^3$ the determination of the asymptotic density is the Kepler Problem. And in $\mathbb{R}^2$ the asymptotic density for $N = 9$ is not known, even for lattice packings. See for example [GL, pp. 526–527].

**3. The main estimate.** Here we state and prove a Proposition from which all our theorems can be deduced. Apart from the numerical constants, it comes about by combining the considerations in the works [E], [Schm1] and [Schm2] of Evertse and Schmidt.

Let $K$ be a number field of degree $d$ and let $v$ be a valuation on $K$ normalized as in Section 1. We will define a local height $\mathcal{H}_v$ on $\overline{\mathbb{Q}}^m$ as follows. Any $\boldsymbol{\alpha} = (\alpha_1, \dots, \alpha_m)$ in $\overline{\mathbb{Q}}^m$ lies in $L^m$ for some number field $L$ containing $K$. Then

$$\mathcal{H}_v(\boldsymbol{\alpha})^{[L:\mathbb{Q}]} = \prod_w \max\{|\alpha_1|_w, \dots, |\alpha_m|_w\}, \tag{3.1}$$

where the product is taken over all valuations $w$ of $L$, properly normalized with respect to $L$, that lie over $v$. Just as for $H$ this is independent of the choice of $L$. The definition includes a definition of $\mathcal{H}_w$ for any $w$ on $L$; then $\mathcal{H}_w^{[L:\mathbb{Q}]}$ coincides with the corresponding factor on the right-hand side of (3.1). Thus (3.1) could be rewritten as $\mathcal{H}_v = \prod_w \mathcal{H}_w$ over the same $w$.

It is also convenient to define an "anti-local" height $\mathcal{H}^v(\boldsymbol{\alpha})$ by the product (3.1) taken over all $w$ not lying over $v$. Then

$$\mathcal{H}(\boldsymbol{\alpha}) = \mathcal{H}_v(\boldsymbol{\alpha})\mathcal{H}^v(\boldsymbol{\alpha})$$

is not quite the height $H(\alpha_1, \dots, \alpha_m)$ in (1.10), and indeed if $m = 1$ then $\mathcal{H}(\boldsymbol{\alpha}) = 1$ for all $\boldsymbol{\alpha} = (\alpha_1)$ with $\alpha_1 \neq 0$ by virtue of the Product Formula. In general if $\boldsymbol{\alpha}$ is non-zero in $\overline{\mathbb{Q}}^m$ then $\mathcal{H}(\boldsymbol{\alpha}) \geq 1$.

We also define, for $N \geq 2$,

$$u_1(N) = U_N^{2/(N(N-1))}, \quad u_2(N) = N^{1/(N-1)}$$

in the notation of Lemma 2.

Proposition. *Let $v$ be an archimedean valuation of $K$ and put $f = 1$ if it corresponds to a real embedding and $f = 2$ otherwise. Let $l \geq 1$, let $\boldsymbol{\phi}$ in $\overline{\mathbb{Q}}^l$ be non-zero, and let $X \geq 1$, $Y \geq 1$ be real. Then for any integer $N \geq 2$ the number of $\alpha$ in $K$ with*

$$\mathcal{H}_v(\boldsymbol{\phi}, \alpha) \leq X\mathcal{H}_v(\boldsymbol{\phi}), \quad \mathcal{H}^v(\boldsymbol{\phi}, \alpha) \leq Y\mathcal{H}^v(\boldsymbol{\phi}) \tag{3.2}$$

*is at most*

$$(N-1)\left\{1 + \tfrac{1}{2} f u_f(N) Z^{d/f}\right\}^f \tag{3.3}$$

*where*

$$Z = u_2(N) X Y^2 \mathcal{H}(\boldsymbol{\phi}).$$

*Further if $f = 2$ and $N = 2$ then the factor $N-1$ can be replaced by $\pi/\sqrt{12}$.*

*Proof.* Let $\sigma$ be the embedding of $K$ corresponding to $v$, considered as a map from $K$ to $\mathbb{R}^f$. Define

$$R = \{X\mathcal{H}_v(\boldsymbol{\phi})\}^{d/f}$$

and

$$r = 2\{u_2 Y^2 \mathcal{H}^v(\boldsymbol{\phi})\}^{-d/f}/(f u_f),$$

with $u_2 = u_2(N)$, $u_f = u_f(N)$ for brevity. We will verify in a moment that as $\alpha$ runs over all the different elements in $K$ satisfying (3.2), the balls $\mathcal{B}(\alpha)$ with centre $\sigma(\alpha)$ and radius $r$ form an $(N-1)$-fold packing of the ball $\mathcal{B}$ with centre 0 and radius $r+R$. Assuming this, we get from Lemma 4 the estimate

$$M \le (N-1)(1+R/r)^f$$

for their cardinality $M$. But this is just (3.3) of the Proposition.

And if $f = N = 2$ we get

$$M \le \max\{1, (\pi/\sqrt{12})(1+R/r)^2\}.$$

However, now

$$R/r = 2Z^{d/2} \ge 2^{1+d/2} \ge 2^{3/2}$$

and so the 1 in the maximum can be omitted. This also leads to the bound of the Proposition.

It remains to prove the above packing assertion. Let $L$ be a number field containing $K$ and the components of $\boldsymbol{\phi}$. Throwing away these components on the left-hand side of the first inequality in (3.2) yields $\mathcal{H}_v(\alpha) \le X\mathcal{H}_v(\boldsymbol{\phi})$. As $\alpha$ is in $K$ we have $\mathcal{H}_v(\alpha) = |\alpha|_v^{1/d} = |\sigma(\alpha)|^{f/d}$. So $|\sigma(\alpha)| \le R$ and this implies that the ball $\mathcal{B}(\alpha)$ of radius $r$ is contained in the ball $\mathcal{B}$ of radius $r+R$.

Finally it will suffice to deduce a contradiction from the existence of different $\alpha_1, \dots, \alpha_N$ such that $\mathcal{B}(\alpha_1), \dots, \mathcal{B}(\alpha_N)$ have a common point $z$ in their interiors. But this would imply that $\sigma(\alpha_1), \dots, \sigma(\alpha_N)$ lie in some ball (with centre $z$) of radius strictly less than $r$. Our contradiction will come from applying the Product Formula to the number $\Delta = \Delta(\alpha_1, \dots, \alpha_N)$ in $K$.

Certainly the above together with Lemma 1 (if $f = 2$) or Lemma 2 (if $f = 1$) implies

$$|\Delta|_v < (fu_f r/2)^{fQ}$$

with $Q = N(N-1)/2$ for brevity. However we want to work over $L$ and so this should be written as

$$\prod_w |\Delta|_w < (fu_f r/2)^{fQe/d} \tag{3.4}$$

for $e = [L : \mathbb{Q}]$, where the product is over all $w$ lying over $v$.

Next suppose that $w$ is any non-archimedean valuation (thus certainly not lying over $v$) of $L$. We use the fact that $\Delta$ is a sum of terms $\delta = \pm\alpha_1^{i_1} \dots \alpha_N^{i_N}$ with $0 \le i_j \le N-1$ $(1 \le j \le N)$ and $i_1 + \dots + i_N = Q$. For each of these, and any real $\lambda > 0$, we have

$$|\delta|_w = \lambda^Q(|\alpha_1|_w/\lambda)^{i_1} \dots (|\alpha_N|_w/\lambda)^{i_N},$$

which is at most

$$\lambda^Q \max\{1, |\alpha_1|_w/\lambda\}^{N-1} \ldots \max\{1, |\alpha_N|_w/\lambda\}^{N-1}$$
$$= \lambda^{-Q} \max\{\lambda, |\alpha_1|_w\}^{N-1} \ldots \max\{\lambda, |\alpha_N|_w\}^{N-1}.$$

Choosing $\lambda = \mathcal{H}_w(\boldsymbol{\phi})^e$ and noting that

$$\max\{\mathcal{H}_w(\boldsymbol{\phi})^e, |\alpha_j|_w\} = \mathcal{H}_w(\boldsymbol{\phi}, \alpha_j)^e \quad (1 \le j \le N), \tag{3.5}$$

we end up with upper bounds for each $|\delta|_w$ that lead to the same upper bound

$$|\varDelta|_w \le \mathcal{H}_w(\boldsymbol{\phi})^{-eQ} \cdot \mathcal{H}_w(\boldsymbol{\phi}, \alpha_1)^{e(N-1)} \ldots \mathcal{H}_w(\boldsymbol{\phi}, \alpha_N)^{e(N-1)} \tag{3.6}$$

for the sum $\varDelta$ of the $\delta$.

Finally suppose that $w$ is any archimedean valuation of $L$. The same argument leads to extra powers of $N!$ but we prefer to use Hadamard's inequality. If $w$ corresponds to an embedding $\tau$ of $L$ then again for any real $\lambda > 0$ we have

$$|\tau(\varDelta)| = |\varDelta(\tau(\alpha_1), \ldots, \tau(\alpha_N))| = \lambda^Q |\varDelta(\tau(\alpha_1)/\lambda, \ldots, \tau(\alpha_N)/\lambda)|,$$

which is at most

$$\lambda^Q N^{N/2} \max\{1, |\tau(\alpha_1)|/\lambda\}^{N-1} \ldots \max\{1, |\tau(\alpha_N)|/\lambda\}^{N-1}$$
$$= \lambda^{-Q} N^{N/2} \max\{\lambda, |\tau(\alpha_1)|\}^{N-1} \ldots \max\{\lambda, |\tau(\alpha_N)|\}^{N-1}.$$

Choosing now $\lambda = \mathcal{H}_w(\boldsymbol{\phi})^{e/f(\tau)}$ for the local degree $f(\tau)$ of $\tau$ and using again (3.5), we end up with

$$|\varDelta|_w \le \mathcal{H}_w(\boldsymbol{\phi})^{-eQ} \cdot N^{f(\tau)N/2} \cdot \mathcal{H}_w(\boldsymbol{\phi}, \alpha_1)^{e(N-1)} \ldots \mathcal{H}_w(\boldsymbol{\phi}, \alpha_N)^{e(N-1)}. \tag{3.7}$$

We now take the product of (3.4) together with (3.6) and (3.7) for $w$ not lying over $v$. The product of the $\mathcal{H}_w$ terms gives just $\mathcal{H}^v$, for which the second inequality in (3.2) is available. Also $\sum f(\tau) \le e$, and $N^{eN/2} = u_2^{eQ}$. We find for the product over all $w$ that

$$\prod_w |\varDelta|_w < \{(fu_f r/2)^{f/d} \cdot u_2 Y^2 \mathcal{H}^v(\boldsymbol{\phi})\}^{eQ}.$$

From the definition of $r$ the right-hand side is 1, and as $\varDelta \ne 0$ this contradicts the Product Formula, according to which the left-hand side is 1. The proof of the Proposition is thereby complete.

**4. Proofs of Theorems 1 and 2.** We start with some numerical estimates which will be useful also in later sections. For an integer $N \ge 2$ define $\chi(N) = N - 1$ $(N \ge 3)$ and $\chi(2) = \pi/\sqrt{12}$. For an integer $d \ge 2$ set

$$A = A(N, d) = \chi(N)/(d \log d),$$
$$B = B(N, d) = 2\chi(N) u_2(N)^{1+d/2}/(d \log d),$$
$$C = C(N, d) = \chi(N) u_2(N)^{2+d}/(d \log d).$$

We will also need the linear combinations

$$\begin{aligned} B' &= B'(N,d) = A + 2B/(\sqrt{2}-1), \\ C' &= C'(N,d) = B' + 4C, \\ C'' &= C''(N,d) = 2A + 2B + 2C, \\ C''' &= C'''(N,d) = B'/\sqrt{e} + 4C. \end{aligned}$$

None of these are constants, but we will see that they can be treated as such.

Lemma 5. *For each $d \ge 2$ there exists $N = N(d)$ such that*

(a) $C \le C(2,2) = (\pi/\sqrt{12})(8/\log 2) = 10.46\ldots$,
(b) $B' \le B'(9,4) = 33.20\ldots$,
(c) $C' \le C'(2,2) = 67.79\ldots$,
(d) $C'' \le C''(12,5) = 28.07\ldots\,(d \ne 2,4)$,
(e) $C''' \le C'''(2,2) = 57.59\ldots$

*Proof.* We choose $N = N(d)$ so as to minimize $C(N,d)$, at least approximately. If $d = 2,3,4,5,6,7$ the inequalities can be checked directly with the values $N = 2,2,9,12,15,19$ respectively.

For $d \ge 8$ we take $N = 1 + [d\log d] \ge 17$ and note that $\chi(N) = N-1 \le d\log d$ in $A,B,C$. Also the function $F(x) = x^{1/x}$ decreases as $x \ge e$ increases. So

$$u_2(N) = F(N)^{N/(N-1)} \le F(d\log d)^{\nu}$$

for $\nu = 17/16$. Substituting this into $V = u_2(N)^{2+d}$ we get

$$V \le (d\log d)^{\nu/\log d} \cdot F(d\log d)^{2\nu} \le c(d\log d)^{\nu/\log d}$$

for $c = F(8\log 8)^{2\nu}$. Finally $F(x)$ increases as $x$ increases from 1 to $e$, so $\log d$ is

$$\exp\{(\log d)(\log F(\log d))\} \le \exp\{(\log d)(\log F(e))\} = d^{1/e},$$

leading to

$$V \le ce^{\nu(1+1/e)} \le 6.13. \tag{4.1}$$

Now $A \le 1$, $B \le 2\sqrt{V}$, $C \le V$ and the estimates (a)–(e) follow.

We also need

$$\begin{aligned} \widetilde{C} &= \widetilde{C}(N,d) = (N-1)\{1 + 2u_1(N)u_2(N)^d\}/(d\log d), \\ \widetilde{C}' &= \widetilde{C}'(N,d) = (N-1)\bigl\{1 + \tfrac{1}{2}u_1(N)u_2(N)^d\bigr\}/(d\log d). \end{aligned}$$

Lemma 6. *For each $d \ge 2$ there exists $N = \widetilde{N}(d)$ such that*

$$\begin{aligned} \widetilde{C} &\le \widetilde{C}(2,2) = 33/(2\log 2) = 23.80\ldots, \\ \widetilde{C}' &\le \widetilde{C}'(2,2) = 9/(2\log 2) = 6.49\ldots \end{aligned}$$

*Proof.* For $2 \le d \le 7$ these come from taking $N = 1 + [d \log d]$ and a direct calculation. If $d \ge 8$ we use Lemma 3 to see that $u_1(N) \le u_2(N)^4$, so again, with $N = 1 + [d \log d]$,

$$\widetilde{C} \le 1 + 2u_2(N)^{4+d} = 1 + 2V^{(4+d)/(2+d)}.$$

Using (4.1) and bounding the exponent by $6/5$ we find $\widetilde{C} < 18.7$. Similarly for $\widetilde{C}' \le 1 + \frac{1}{2}V^{6/5} < 5.5$. This completes the proof.

With these numerical preparations out of the way, we turn to the proofs proper. Let $\theta$, $K$, $d$, $H$ be as in Theorem 1. Fix any archimedean valuation $v$ of $K$, and let $f$ be as in the Proposition. Now

$$H(\theta\alpha) = \mathcal{H}(1, \theta\alpha) = \mathcal{H}_v(1, \theta\alpha)\mathcal{H}^v(1, \theta\alpha) \le H,$$

and so there is an integer $i \ge 1$ with

$$2^{(i-1)/d} \le \mathcal{H}_v(1, \theta\alpha) < 2^{i/d}. \tag{4.2}$$

Thus $\mathcal{H}^v(1, \theta\alpha) \le 2^{-(i-1)/d}H$. With $\phi = 1/\theta$ these inequalities imply

$$\mathcal{H}_v(\phi, \alpha) < X\mathcal{H}_v(\phi), \qquad \mathcal{H}^v(\phi, \alpha) \le Y\mathcal{H}^v(\phi),$$

where

$$X = 2^{i/d} > 1, \qquad Y = 2^{-(i-1)/d}H \ge 1.$$

As $\mathcal{H}(\phi) = 1$ the Proposition shows that for this value of $i$ the number of $\alpha$ is at most

$$(N-1)\left\{1 + \tfrac{1}{2}fu_f u_2^{d/f} \cdot 2^{-(i-2)/f}H^{2d/f}\right\}^f \tag{4.3}$$

where $u_f = u_f(N)$, $u_2 = u_2(N)$ for an arbitrary integer $N \ge 2$. Further if $f = N = 2$ then $N - 1$ can be replaced with $\pi/\sqrt{12}$.

It turns out that the worst numerical constants arise from the case $f = 2$ (and $N = 2$, which is why we went to the trouble with [FT]). So we treat this case $f = 2$ first. Then $d \ge 2$, and the number of $\alpha$ for fixed $i$ is at most

$$(d \log d)\{A + 2^{-(i-2)/2}BH^d + 2^{-(i-2)}CH^{2d}\} \tag{4.4}$$

with $A$, $B$, $C$ as above. So summing over all integers $i$ with

$$1 \le i \le 1 + [(\log H^d)/(\log 2)] \le H^d \tag{4.5}$$

we find the bound

$$(d \log d)(B'H^d + 4CH^{2d}) \tag{4.6}$$

for the total number of $\alpha$ in $K$ with $H(\theta\alpha) \le H$, at least if $f = 2$ (so $d \ge 2$). For the purposes of Theorem 1 it suffices to estimate this by

$$C'(d \log d)H^{2d} \le C'(2,2)(d \log d)H^{2d} \tag{4.7}$$

using Lemma 5(c).

We said that the case $f = 1$ gives better results. If $d \geq 2$ then (4.3) is $(N-1)\bigl\{1+\frac{1}{2}u_1u_2^d\cdot 2^{-(i-2)}H^{2d}\bigr\}$. Now summing over $i$ as in (4.5) and using Lemma 6 gives the estimate

$$\widetilde{C}(2,2)(d\log d)H^{2d} \tag{4.8}$$

for the number of $\alpha$ in $K$ with $H(\theta\alpha) \leq H$, at least if $f = 1$ and $d \geq 2$. This is well within the bound of Theorem 1.

The missing case $d = 1$ (so $f = 1$) comes directly from choosing $N = 2$, so that (4.3) becomes $1 + 4\cdot 2^{-(i-2)}H^2$, and summing over $i$ to yield $17H^2$.

Now all the assertions for arbitrary $\theta$ in Theorem 1 follow from this and (4.7), (4.8).

If however $\theta$ lies in $K$ we can assume $\theta = 1$, and now the "Inverse Trick" of [Lo, p. 14] can be used to avoid the summation over $i$.

Namely the $\alpha$ in $K$ with $H(\alpha) \leq H$ include 0 and $\pm 1$, and apart from these they come in pairs $(\alpha, \alpha^{-1})$ with $\alpha \neq \alpha^{-1}$, thanks to $H(\alpha) = H(\alpha^{-1})$. Suppose there are $M - 3 \geq 0$ such pairs; then the total number $\#K(H) = 2M - 3$. Fixing $v$ as above, and noting that at least one of $|\alpha|_v$, $|\alpha^{-1}|_v$ is no greater than 1, we obtain $M$ different $\beta$ in $K$ with $|\beta|_v \leq 1$ and $H(\beta) \leq H$. We can therefore apply the Proposition with $\phi = 1$, $X = 1$, $Y = H$. It shows that

$$M \leq (N-1)\bigl\{1+\tfrac{1}{2}fu_fu_2^{d/f}\cdot H^{2d/f}\bigr\}^f \tag{4.9}$$

and if $f = N = 2$ the $N - 1$ can be replaced by $\pi/\sqrt{12}$. If $f = 2$ the same calculations as before give

$$M \leq (d\log d)(A + BH^d + CH^{2d}). \tag{4.10}$$

If $d \neq 2, 4$ it is enough to use $\#K(H) \leq 2M$ and appeal to Lemma 5(d). If $d = 2, 4$ we take $N = 2$ and shamelessly exploit the extra "3" in $\#K(H) = 2M - 3$. We get $2M - 3 \leq a + bx + cx^2$ for

$$a = 2A(d\log d) - 3, \qquad b = 2B(d\log d), \qquad c = 2C(d\log d)$$

and $x = H^d \geq 1$. But the elementary inequality $a + bx \leq (a + b)x^2$ is easily verified for all $x \geq 1$ provided $a + b \geq 0$ and $2a + b \geq 0$; and this is the case here. It follows that

$$\#K(H) \leq (a + b + c)H^{2d} < 31(d\log d)H^{2d}$$

for $d = 2, 4$.

This completes the proof of Theorem 1 for $\theta$ in $K$ and $f = 2$.

If $f = 1$ then (4.9) gives

$$M \leq (N-1)\bigl(1+\tfrac{1}{2}u_1u_2^d\cdot H^{2d}\bigr) \leq \widetilde{C}'(d\log d)H^{2d}$$

and it is enough to use $\#K(H) \leq 2M$ and Lemma 6 to get $\#K(H) \leq 13(d\log d)H^{2d}$. This completes the proof of Theorem 1 and by the way establishes Loher's improved estimate (1.6) if $K$ has a real embedding.

Theorem 2 comes out quickly now. If $f = 2$ it suffices to use (4.10) with $H \to \infty$ and Lemma 5(a). And if $f = 1$ we already got the coefficient 13 just above.

In preparation for the following section we would like to draw attention to the estimate (4.6), which for any $N \geq 2$ is an upper bound for the number of $\alpha$ in $K$ with $H(\theta\alpha) \leq H$, valid for any $\theta$ in $\overline{\mathbb{Q}}$ provided $K$ has a non-real embedding (so $d \geq 2$). If $K$ has a real embedding and $d \geq 2$ we can use (4.8) instead. Finally if $d = 1$ the bound $17H^2$ is valid.

**5. Proof of Theorem 3.** Let $n \geq 1$ and let $\alpha_1, \ldots, \alpha_n$ be non-zero multiplicatively independent elements of $K$. The set $\mathcal{M} = \mathcal{M}_K(\alpha_1, \ldots, \alpha_n)$ was defined as the set of all $(\xi_1, \ldots, \xi_n)$ in $\mathbb{Q}^n$ such that some (and therefore every) determination of $\alpha_1^{\xi_1} \ldots \alpha_n^{\xi_n}$ has the form $\mu\beta$ for some root of unity $\mu$ in $\overline{\mathbb{Q}}$ and some $\beta$ in $K$. It is easy to see that this is an additive subgroup containing $\mathbb{Z}^n$. The finiteness of the index $[\mathcal{M} : \mathbb{Z}^n]$ comes implicitly out of our proof of Theorem 3, but it could also be verified directly by noting that an infinite index would imply non-discreteness and so arbitrarily small non-zero $(\xi_1, \ldots, \xi_n)$ in $\mathcal{M}$; but then any determination of $\alpha_1^{\xi_1} \ldots \alpha_n^{\xi_n} = \mu\beta$ would have arbitrarily small logarithmic height $h(\mu\beta) = h(\beta)$; on the other hand $\beta$ in $K$ is not a root of unity and so $h(\beta)$ is bounded away from 0.

In other words, $\mathcal{M}$ is a lattice in $\mathbb{R}^n$.

For the actual upper bound we use the Geometry of Numbers. Write for brevity $h_i = h(\alpha_i)$ $(1 \leq i \leq n)$ and for $H \geq 1$ consider the subset $\mathcal{S}$ of $\mathbb{R}^n$ defined by

$$h_1|x_1| + \ldots + h_n|x_n| < \log H. \tag{5.1}$$

Its measure is

$$V = (2^n/n!)(\log H)^n/(h_1 \ldots h_n). \tag{5.2}$$

The lattice $\mathcal{M}$ has determinant

$$D = d(\mathcal{M}) = d(\mathbb{Z}^n)/[\mathcal{M} : \mathbb{Z}^n] = 1/[\mathcal{M} : \mathbb{Z}^n]. \tag{5.3}$$

We apply Blichfeldt's Theorem (see [C, Theorem I, p. 69]) with the greatest integer $M < V/D$. We obtain

$$M + 1 \geq V/D \tag{5.4}$$

different points $P_0, \ldots, P_M$ of $\mathcal{S}$ such that the differences $P_i - P_0$ $(1 \leq i \leq M)$ are in $\mathcal{M}$. Since $\mathcal{S}$ is open, by moving $P_0$ slightly we can assume that it is also in $\mathbb{Q}^n$.

Thus if $P_0 = (\xi_{10}, \ldots, \xi_{n0})$ then all determinations of the number $\alpha_1^{\xi_{10}} \ldots \alpha_n^{\xi_{n0}}$ are in $\overline{\mathbb{Q}}$; choose any such determination $\theta_0$. Similarly if $P_i = (\xi_{1i}, \ldots, \xi_{ni})$ choose any determination $\theta_i$ of $\alpha_1^{\xi_{1i}} \ldots \alpha_n^{\xi_{ni}}$ in $\overline{\mathbb{Q}}$ $(1 \leq i \leq M)$.

As $P_i - P_0$ is in $\mathcal{M}$, we deduce that $\theta_i/\theta_0 = \mu_i\beta_i$ for some root of unity $\mu_i$ in $\overline{\mathbb{Q}}$ and some $\beta_i$ in $K$; this trivially holds for $i = 0$ as well. And

$$h(\theta_0\beta_i) = h(\theta_i) < \log H$$

by (5.1), since $P_i$ is in $\mathcal{S}$ $(0 \le i \le M)$.

So $\beta_0, \dots, \beta_M$ lie in $K$ with $H(\theta_0\beta_i) < H$ $(0 \le i \le M)$. The multiplicative independence of $\alpha_1, \dots, \alpha_n$ implies that $\beta_0, \dots, \beta_M$ are different and even different modulo roots of unity in $K$. From (4.6) we therefore deduce an upper bound for $(M+1)w_K$ which in view of (5.4), (5.2) and (5.3) implies

$$w_K[\mathcal{M} : \mathbb{Z}^n](2^n/n!)(\log H)^n/(h_1 \dots h_n) \\ \le (d \log d)(B'H^d + 4CH^{2d}) \tag{5.5}$$

with $B' = B'(N, d)$ and $C = C(N, d)$ for any $N \ge 2$, provided $K$ has a non-real embedding (so $d \ge 2$). In this case we choose $H = e^{n/2d}$ to get

$$w_K[\mathcal{M} : \mathbb{Z}^n] \le C_n(n!e^n/n^n)d^{n+1}(\log d)h_1 \dots h_n. \tag{5.6}$$

Here

$$C_n = B'e^{-n/2} + 4C \le B'/\sqrt{e} + 4C = C'''$$

as in Section 4. So we can choose $N$ by Lemma 5(e) to make $C_n < 58$.

If $K$ has a real embedding (and still $d \ge 2$) we use (4.8) on the right-hand side of (5.5) to get (5.6) with $C_n = \widetilde{C}(2, 2) < 24$. This proves Theorem 3 whenever $d \ge 2$; and the case $d = 1$ follows equally easily using the corresponding part of Theorem 1.

We already proved Corollary 3.1. For the proof of Corollary 3.2 consider the set of all $(r_0, \dots, r_n)$ in $\mathbb{Z}^{n+1}$ for which there exists a root of unity $\mu$ in $K$ with

$$\alpha_0^{r_0} \dots \alpha_n^{r_n} = \mu. \tag{5.7}$$

This set is an additive group, and our hypotheses imply that its rank is 1. Thus there is a single generator, which we could also denote by $(r_0, \dots, r_n)$. Further $r_0, \dots, r_n$ are all non-zero and also coprime.

Now the vector $\boldsymbol{\xi} = (r_1/r_0, \dots, r_n/r_0)$ lies in $\mathcal{M} = \mathcal{M}_K(\alpha_1, \dots, \alpha_n)$. Thus $[\mathcal{M} : \mathbb{Z}^n]\boldsymbol{\xi}$ lies in $\mathbb{Z}^n$. It follows that $|r_0| \le [\mathcal{M} : \mathbb{Z}^n]$. And $\alpha_0^{b_0} \dots \alpha_n^{b_n} = 1$ with $b_i = r_i w_K$ $(0 \le i \le n)$, and this yields the required upper bound for $|b_0|$ using Theorem 3. The bounds for the other $|b_i|$ follow on grounds of symmetry.

## 6. Proof of Theorem 4.

This proceeds via two lemmas. Again we use the height $\mathcal{H}$ of Section 3. But from now on we work only over $K$, with $d = [K : \mathbb{Q}] \ge 2$.

Lemma 7. *Let $l \geq 1$ and let $\boldsymbol{\phi}$ in $K^l$ be non-zero. Then for any real $T \geq 1$ the number of $\alpha$ in $K$ with*

$$\mathcal{H}(\boldsymbol{\phi}, \alpha) \leq T\mathcal{H}(\boldsymbol{\phi}) \tag{6.1}$$

*is at most $68(d \log d)T^{2d}\mathcal{H}(\boldsymbol{\phi})^d$.*

*Proof.* Taking $l = 1$ and $\boldsymbol{\phi} = (1/\theta)$ we recover the first part of Theorem 1, at least for $\theta$ in $K$. The present proof runs on the same lines.

Fix an archimedean valuation $v$ on $K$. If $\alpha$ satisfies (6.1) there is an integer $i \geq 1$ with

$$2^{(i-1)/d} \leq \mathcal{H}_v(\boldsymbol{\phi}, \alpha)/\mathcal{H}_v(\boldsymbol{\phi}) < 2^{i/d}.$$

So

$$\mathcal{H}^v(\boldsymbol{\phi}, \alpha)/\mathcal{H}^v(\boldsymbol{\phi}) \leq 2^{-(i-1)/d}T.$$

We are therefore back in the situation of the Proposition, with $X = 2^{i/d} > 1$ and $Y = 2^{-(i-1)/d}T \geq 1$. So for this value of $i$ the number of $\alpha$ is at most

$$(N-1)\bigl\{1 + \tfrac{1}{2}fu_f u_2^{d/f} \cdot 2^{-(i-2)/f} \cdot T^{2d/f} \cdot \mathcal{H}^{d/f}\bigr\}^f$$

for any $N \geq 2$ and $\mathcal{H} = \mathcal{H}(\boldsymbol{\phi})$. This coincides with the expression (4.3) if $H = T\mathcal{H}^{1/2}$, and so if $f = 2$ the arguments following (4.3) give the estimate

$$68(d \log d)H^{2d} = 68(d \log d)T^{2d}\mathcal{H}^d$$

just as in (4.7). And if $f = 1$ we get the better estimate (4.8). This completes the proof.

After all the counting in $K$, we can now start to count points of $K^m$.

Lemma 8. *Let $l \geq 1$, $m \geq 1$, and let $\boldsymbol{\phi}$ in $K^l$ be non-zero. Then for any real $H \geq 1$ the number of $\boldsymbol{\alpha} = (\alpha_1, \ldots, \alpha_m)$ in $K^m$ with*

$$\mathcal{H}(\boldsymbol{\phi}, \boldsymbol{\alpha}) \leq H\mathcal{H}(\boldsymbol{\phi}) \tag{6.2}$$

*is at most*

$$(1088 d \log d)^m H^{(m+1)d}\mathcal{H}(\boldsymbol{\phi})^{md}.$$

*Proof.* We use induction on $m$, just as in the proof of the "Main Lemma" of [Schm2, p. 175]. The case $m = 1$ is slightly weaker than Lemma 7. So it suffices to prove the present lemma for $m \geq 2$ assuming that the counting works as stated in $K^{m-1}$.

Again fix an archimedean valuation $v$. Fix also $E = E(m, d) > 1$. If $\boldsymbol{\alpha} = (\alpha_1, \ldots, \alpha_m)$ satisfies (6.2), write $\boldsymbol{\alpha}' = (\alpha_1, \ldots, \alpha_{m-1})$. Then there is an integer $i \geq 1$ with

$$E^{i-1} \leq \mathcal{H}(\boldsymbol{\phi}, \boldsymbol{\alpha}')/\mathcal{H}(\boldsymbol{\phi}) < E^i \tag{6.3}$$

and furthermore

$$E^{i-1} \leq H. \tag{6.4}$$

Now

$$\mathcal{H}(\boldsymbol{\phi},\boldsymbol{\alpha})/\mathcal{H}(\boldsymbol{\phi},\boldsymbol{\alpha}') \le E^{-(i-1)}H. \tag{6.5}$$

By the induction hypothesis the number of $\boldsymbol{\alpha}'$ satisfying (6.3) for this $i$ is at most

$$(1088d\log d)^{m-1} \cdot E^{imd} \cdot \mathcal{H}(\boldsymbol{\phi})^{(m-1)d}. \tag{6.6}$$

For each such $\boldsymbol{\alpha}'$ we can apply Lemma 7 to (6.5) to count the number of $\alpha_m$, and we find the upper bound

$$68(d\log d)\{E^{-(i-1)}H\}^{2d}\mathcal{H}(\boldsymbol{\phi},\boldsymbol{\alpha}')^{d}. \tag{6.7}$$

Substituting the right-hand inequality of (6.3) into (6.7) and multiplying by (6.6), we find for the number of $\boldsymbol{\alpha} = (\boldsymbol{\alpha}', \alpha_m)$ with fixed $i$ the upper bound

$$(1/16)(1088d\log d)^m \cdot E^{i(m-1)d+2d} \cdot H^{2d} \cdot \mathcal{H}(\boldsymbol{\phi})^{md}.$$

Choose now $E = 2^{1/((m-1)d)}$ and sum over all $i$ from $i = 1$ to the biggest value, say $I$, satisfying (6.4). Since $E^{2d} = 2^{2/(m-1)} \le 4$ and

$$\sum_{i=1}^{I} E^{i(m-1)d} = 2^{I+1} - 1 < 4 \cdot 2^{I-1} \le 4H^{(m-1)d}$$

the conclusion of the present lemma drops out.

The proof of Theorem 4 is immediate on taking $l = 1$ and $\boldsymbol{\phi} = (1)$.

## References

[AD] F. Amoroso et S. David, *Le problème de Lehmer en dimension supérieure*, J. Reine Angew. Math. 513 (1999), 145–179.

[Be] D. Bertrand, *Duality on tori and multiplicative dependence relations*, J. Austral. Math. Soc. Ser. A 62 (1997), 198–216.

[Bi] Y. Bilu, Math. Rev. 2000g:11058.

[Bl] H. Blichfeldt, *Note on the minimum value of the discriminant of an algebraic field*, Monatsh. Math. und Phys. 48 (1939), 531–533.

[C] J. W. S. Cassels, *An Introduction to the Geometry of Numbers*, Grundlehren Math. Wiss. 99, Springer, 1959.

[E] J.-H. Evertse, *On equations in S-units and the Thue–Mahler equation*, Invent. Math. 75 (1984), 561–584.

[FT] L. Fejes Tóth, *Lagerungen in der Ebene, auf der Kugel und im Raum*, Grundlehren Math. Wiss. 65, Springer, 1953.

[GL] P. M. Gruber and C. G. Lekkerkerker, *Geometry of Numbers*, North-Holland, 1987.

[HW] G. H. Hardy and E. M. Wright, *An Introduction to the Theory of Numbers*, Oxford Univ. Press, 1960.

[K] L. Kronecker, *Zwei Sätze über Gleichungen mit ganzzahligen Coeffizienten*, J. Reine Angew. Math. 53 (1857), 173–175.

[La1] S. Lang, *Algebraic Number Theory*, Addison-Wesley, 1970.

[La2] S. Lang, *Fundamentals of Diophantine Geometry*, Springer, 1983.

[Lo] T. Loher, *Counting points of bounded height*, Ph.D. thesis, Basel, 2001.

[Mas] D. W. Masser, *Counting points of small height on elliptic curves*, Bull. Soc. Math. France 117 (1989), 247–265.

[Mat1] E. M. Matveev, *On linear and multiplicative relations*, Russian Acad. Sci. Sb. Math. 78 (1994), 411–425.

[Mat2] —, *On the successive minima of the extended logarithmic height of algebraic numbers*, Sb. Math. 190 (1999), 407–425.

[Mat3] —, *An explicit lower bound for a homogeneous rational linear form in logarithms of algebraic numbers II*, Izv. Math. 64 (2000), 1217–1269.

[Mu] H. P. Mulholland, *On the product of $n$ complex homogeneous linear forms*, J. London Math. Soc. 35 (1960), 241–250.

[N] D. G. Northcott, *An inequality in the theory of arithmetic on algebraic varieties*, Proc. Cambridge Philos. Soc. 45 (1949), 502–509.

[O] A. M. Odlyzko, *Some analytic estimates of class numbers and discriminants*, Invent. Math. 29 (1975), 275–286.

[Ra] T. Ransford, *Potential Theory in the Complex Plane*, Cambridge Univ. Press, 1995.

[Ro] C. A. Rogers, *The product of $n$ real homogeneous linear forms*, Acta Math. 82 (1950), 185–208.

[Scha] S. Schanuel, *Heights in number fields*, Bull. Soc. Math. France 107 (1979), 433–449.

[Schm1] W. M. Schmidt, *Diophantine Approximations and Diophantine Equations*, Lecture Notes in Math. 1467, Springer, 1991.

[Schm2] —, *Northcott's theorem on heights I. A general estimate*, Monatsh. Math. 115 (1993), 169–181.

[Schm3] —, *Northcott's theorem on heights II. The quadratic case*, Acta Arith. 70 (1995), 343–375.

[Schu] I. Schur, *Über die Verteilung der Wurzeln bei gewissen algebraischen Gleichungen mit ganzzahligen Koeffizienten*, Math. Z. 1 (1918), 377–402.

[V] P. Voutier, *An effective lower bound for the height of algebraic numbers*, Acta Arith. 74 (1996), 81–95.

[W] M. Waldschmidt, *Diophantine Approximation on Linear Algebraic Groups*, Grundlehren Math. Wiss. 326, Springer, 2000.

Institut für Operations Research
Moussonstrasse 15
8044 Zürich, Switzerland
E-mail: loher@ior.unizh.ch

Mathematisches Institut
Universität Basel
Rheinsprung 21
4051 Basel, Switzerland
E-mail: masser@math.unibas.ch

*Received on 26.8.2002* (4356)