Mh. Math. 115, 169—181 (1993)

Monatshefte für
Mathematik

Northcott's Theorem on Heights
I. A General Estimate

By

Wolfgang M. Schmidt[†], Boulder, CO

(Received 1 June 1992)

Abstract. Given a point $P = (\alpha_0 : \ldots : \alpha_n)$ of projective space $\mathbb{P}^n = \mathbb{P}^n(A)$ where A is the field of algebraic numbers, let $d(P)$ be its degree and $H(P)$ its absolute multiplicative height. Northcott's Theorem says that given d, n and X, there are only finitely many points $P \in \mathbb{P}^n$ with $d(P) \leqq d$ and $H(P) \leqq X$. We will show that there are at most $c(d, n) X^{d(d+n)}$ such points.

1. Introduction

The distribution of rational or algebraic points on algebraic varieties is most simply described in terms of asymptotics of their heights. Here we will study points in projective space $\mathbb{P}^n = \mathbb{P}^n(A)$, where A is the field of algebraic numbers.

When $P = (\alpha_0 : \ldots : \alpha_n)$ lies in $\mathbb{P}^n(A)$, let $\mathbb{Q}(P)$ be the field obtained from $\mathbb{Q}$ by adjoining the quotients α_i/α_j with $0 \leqq i, j \leqq n$ and $\alpha_j \neq 0$, and let $d(P)$ be the degree of $\mathbb{Q}(P)$. Let $H(P)$ denote the absolute multiplicative height (as defined in [2], [4], [6] or [8], and also below). Northcott's Theorem [3] says that given d, n, X, there are only finitely many points $P \in \mathbb{P}^n$ with $d(P) \leqq d$ and $H(P) \leqq X$. Here we will show that the number of such points is at most

$$c_1 X^{d(d+n)} \tag{1.1}$$

with $c_1 = c_1(d, n) = 2^{(2d+n)(d+n+10)}$.

Let $K \subset A$ be a number field of degree k, and $M(K)$ a set of properly

[†] Supported in part by NSF grant DMS-9108581.

normalized absolute values of K, such that they extend the standard or a p-adic absolute value of $\mathbb{Q}$. Then the product formula

$$\prod_{v \in M(K)} |\alpha|_v^{n_v} = 1$$

holds for $\alpha \in K^\times$, where the n_v are the local degrees. Given $\boldsymbol{\alpha} = (\alpha_0, \alpha_1, \ldots, \alpha_n) \in K^{n+1}$, we set $|\boldsymbol{\alpha}|_v = \max(|\alpha_0|_v, \ldots, |\alpha_n|_v)$ and

$$H_K(\boldsymbol{\alpha}) = \prod_{v \in M(K)} |\boldsymbol{\alpha}|_v^{n_v}.$$

By the product formula, $H_K(P)$ is in fact defined for $P = (\alpha_0 : \alpha_1 : \ldots : \alpha_n) \in \mathbb{P}^n(K)$; it is called the (multiplicative) *field height* of P. It is well known that $H_L(P) = H_K(P)^\delta$ if $L \supseteq K$ with $[L:K] = \delta$ and $P \in \mathbb{P}^n(K) \subseteq \mathbb{P}^n(L)$. Therefore if $P \in \mathbb{P}^n$, and if in fact $P \in \mathbb{P}^n(K)$ with a number field K of degree k, the *absolute height*

$$H(P) = H_K(P)^{1/k}$$

is independent of the field K.

Given a number field K of degree k, and given $P \in \mathbb{P}^n$ as above, let $K(P)$ be the field obtained from K by adjoining the quotients α_i/α_j ($0 \leqq i, j \leqq n$; $\alpha_j \neq 0$), and let $d_K(P)$ be the degree $[K(P):K]$. The formula

$$H_K(P) = H(P)^{k d_K(P)} \tag{1.2}$$

is valid for $P \in \mathbb{P}^n(K)$, since such P have $d_K(P) = 1$. In general, we define $H_K(P)$ by (1.2). Let $Z(K, d, n, X)$ be the number of $P \in \mathbb{P}^n$ having

$$d_K(P) = d \quad \text{and} \quad H_K(P) \leqq X. \tag{1.3}$$

We will prove the following

Theorem. *We have*

$$Z(K, d, n, X) \leqq c_2(K, d, n) X^{d+n}, \tag{1.4}$$

$$Z(K, d, n, X) \geqq c_3(K, n) X^{n+1} \text{ when } X > X_1(K, d, n), \tag{1.5}$$

$$Z(K, d, n, X) \geqq c_4(K, d) X^{d+1} \text{ when } X > X_2(K, d). \tag{1.6}$$

The constants c_2, c_3, c_4, like all the constants in this paper, are positive. In particular, we may take

$$c_2(K, d, n) = 2^{kd(d+n+3)+d^2+n^2+10d+10n}.$$

For $K = \mathbb{Q}$ we have the explicit lower bounds

$$Z(\mathbb{Q}, 1, n, X) > \frac{1}{4} X^{n+1} \text{ when } X \geqq 1, \tag{1.7}$$

$$Z(\mathbb{Q}, d, n, X) > 6^{-d(d+1)} X^{d+1} \text{ when } X \geqq 2. \tag{1.8}$$

Note that the exponents of X in (1.4) and (1.5) are the same when $d = 1$, and they are the same in (1.4) and (1.6) when $n = 1$. In the other cases there is a considerable gap between the upper and lower bounds. The number of $P \in \mathbb{P}^n$ with $d(P) = e$ and $H(P) \leqq X$ is $\leqq \leqslant c_2(\mathbb{Q}, e, n) X^{e(e+n)}$, since $H_{\mathbb{Q}}(P) = H(P)^e \leqq X^e$ for such P. Applying this estimate for $e = 1, \ldots, d$ and taking the sum, we obtain (1.1).

There is an asymptotic estimate due to SCHANUEL [4]: For given K and n,

$$Z(K, 1, n, X) \sim c_5(K, n) X^{n+1} \quad \text{as} \quad X \to \infty. \tag{1.9}$$

In proving the lower bounds (1.5), (1.6), we will use Schanuel's result. With extra effort it would be possible to give explicit values for the constants c_3, c_4, X_1, X_2 depending only on n, d, $k = \deg K$ and the discriminant of K.

Note that $H_{\mathbb{Q}}(P) = H(P)^{d(P)}$. An alternative to $Z(K, d, n, X)$ is the number $Z^*(K, d, n, X)$ of $P \in \mathbb{P}^n$ with

$$d_K(P) = d \quad \text{and} \quad H_{\mathbb{Q}}(P) \leqq X \quad (\text{i.e., } H(P) \leqq X^{1/d}).$$

As we will point out in Section 7, our theorem holds for Z^* in place of Z, but with a new constant $c_2^*(K, d, n)$ in place of $c_2(K, d, n)$.

In a subsequent paper [7] we will give an asymptotic formula for the case when the ground field $K = \mathbb{Q}$ and when $d = 2$, i.e., the quadratic case. This formula will suggest that $Z(K, d, n, X)$ should have order of magnitude near $X^{\max(d+1, n+1)}$. In other words, the combined lower bounds in (1.5), (1.6) are likely to be nearer the truth than the upper bound (1.4).

2. Lower Bounds

Given K, d, let L be an extension of K with $[L:K] = d$. By Schanuel's formula (1.9), $Z(L, 1, n, X) \sim c_5(L, n) X^{n+1}$ as $X \to \infty$. Here

$Z(L, 1, n, X)$ counts the number of $P \in \mathbb{P}^n$ with $H_L(P) \leqq X$ and $\mathbb{Q}(P) \subseteq L$. The number $Z'(L, 1, n, X)$ of elements $P \in \mathbb{P}^n$ with $H_L(P) \leqq X$ and $\mathbb{Q}(P) = L$ satisfies the same asymptotic formula:

$$Z'(L, 1, n, X) \sim c_5(L, n) X^{n+1} \quad \text{as} \quad X \to \infty. \tag{2.1}$$

This is so, because when $P \in \mathbb{P}^n(M)$ where M is a proper subfield of L, then $H_M(P) = H_L(P)^{m/l} \leqq X^{m/l}$ with $l = \deg L$, $m = \deg M$, and (again by Schanuel) the number of such P is of smaller order of magnitude than X^{n+1}.

But when $\mathbb{Q}(P) = L$, then $K(P) = L$ and $[K(P):K] = d$, therefore $H_K(P) = H(P)^{d \cdot [K:\mathbb{Q}]} = H(P)^l = H_L(P)$. This implies $Z(K, d, n, X) \geqq Z'(L, 1, n, X)$, so that (1.5) follows from (2.1).

Note that we used only a single field L with $[L:K] = d$. It appears to be difficult to improve upon (1.5) by using various fields. The quadratic case to be dealt with in [7] suggests that often a single field already gives the correct order of magnitude.

Let $N(K, d, X)$ be the number of irreducible monic polynomials $f(x) = x^d + a_1 x^{d-1} + \cdots + a_d$ in $K[x]$ of degree d and with $H_K(f) \leqq X$. Here the height of a polynomial is defined as the height of its coefficient vector. If $\alpha_1, \ldots, \alpha_d$ are the roots of such a polynomial f, then we have (see, e.g., [8], Ch. VIII, Theorem 5.9)

$$H(\alpha_i)^d = H(\alpha_1) \cdots H(\alpha_d) \leqq 2^d H(f) \leqq 2^d X^{1/k},$$

where $k = \deg K$. This gives $H_K(\alpha_i) = H(\alpha_i)^{dk} \leqq 2^{dk} X$. Since f has d roots in A,

$$Z(K, d, 1, 2^{dk} X) \geqq d N(K, d, X). \tag{2.2}$$

By (1.9), the number of points $P = (1 : a_1 : \ldots : a_d) \in \mathbb{P}^d(K)$ with $H_K(P) \leqq X$ is $\sim c_5(K, d) X^{d+1}$. Therefore the number of monic polynomials $f \in K[x]$ of degree d and with $H_K(f) \leqq X$ is $\sim c_5(K, d) X^{d+1}$ as $X \to \infty$. It is easily seen that the number of reducible polynomials is of a smaller order of magnitude, so that

$$N(K, d, X) \sim c_5(K, d) X^{d+1} \quad \text{as} \quad X \to \infty. \tag{2.3}$$

In conjunction with (2.2) this yields $Z(K, d, 1, 2^{dk} X) \geqq c_5(K, d) X^{d+1}$ when $X > X_3(K, d)$, therefore (1.6).

Take the special case $K = \mathbb{Q}$. When $X \in \mathbb{N}$, the number of points $\boldsymbol{\alpha} \in \mathbb{Z}^{n+1}$ with $1 \leqq |\alpha_i| \leqq X$ $(i = 1, \ldots, n)$ is $(2X)^{n+1}$. The number of such points whose coordinates are multiples of a prime p is $\leqq (2X/p)^{n+1}$, so that the number of primitive points $\boldsymbol{\alpha} \in \mathbb{Z}^{n+1}$ with $|\boldsymbol{\alpha}| \leqq X$ is

$$\geqq (2X)^{n+1}\left(1 - \sum_p \frac{1}{p^{n+1}}\right) > \frac{1}{2}(2X)^{n+1}.$$

Since each point in $\mathbb{P}^n(\mathbb{Q})$ corresponds to a pair $\boldsymbol{\alpha}$, $-\boldsymbol{\alpha}$ of primitive points in $\mathbb{Z}^{n+1}$, we have $Z(\mathbb{Q}, 1, n, X) > \frac{1}{4}(2X)^{n+1}$. When $X \geqq 1$ is real, with integer part $[X]$, we have

$$Z(\mathbb{Q}, 1, n, X) \geqq Z(\mathbb{Q}, n, 1, [X]) > \frac{1}{4}(2[X])^{n+1} > \frac{1}{4}X^{n+1},$$

i.e., (1.7).

It is well known that the constant $c_5(\mathbb{Q}, n)$ in (1.9) is given by $c_5(\mathbb{Q}, n) = 2^n/\zeta(n+1)$. Therefore (2.3) becomes

$$N(\mathbb{Q}, d, X) \sim (2^d/\zeta(d+1))\, X^{d+1} \quad \text{as} \quad X \to \infty.$$

An explicit lower bound may be obtained as follows. $N(\mathbb{Q}, d, X)$ is the number of irreducible polynomials $f(x) = a_0 x^d + \cdots + a_d$ in $\mathbb{Q}[x]$ with coefficients $a_i \in \mathbb{Z}$ having $a_0 > 0$, $\gcd(a_0, \ldots, a_d) = 1$ and $|a_i| \leqq X$. By Eisenstein's Theorem, this number is bounded from below by the number of polynomials $f(x) = b_0 x^d + 2b_1 x^{d-1} + \cdots + 2b_{d-1}x + 2b_d$ with $2 \nmid b_0 b_d$ and with $1 \leqq b_0 \leqq X$, $|b_1|, \ldots, |b_d| \leqq X/2$, having $\gcd(b_0, \ldots, b_d)$ not divisible by a prime $p > 2$. If we ignore the last condition, there are precisely

$$\left[\frac{X+1}{2}\right] \cdot (1 + 2[X/2])^{d-1} \cdot 2\left[\frac{(X/2)+1}{2}\right] = g(X), \qquad (2.4)$$

say, such polynomials. Thus

$$N(\mathbb{Q}, d, X) \geqq g(X) - \sum_{\substack{p \text{ prime} \\ p > 2}} g(X/p). \qquad (2.5)$$

By considering residue classes of $X \bmod 4$, we see that $g(X) \geqq \frac{1}{4}X^{d+1}$, except when $X \equiv 1 \pmod 4$, when we have $g(X) = \frac{1}{4}X^{d+1}(1 - X^{-2})$. Thus when $X > 1$,

$$g(X) \geqq \frac{1}{4}X^{d+1}(1 - 5^{-2}) = \frac{6}{25}X^{d+1}. \qquad (2.6)$$

On the other hand, $g(X) < \frac{1}{4}(X+1)^{d+1}$, and $g(X) = 0$ when $X < 2$. Therefore when $d > 1$,

$$\sum_{\substack{p \text{ prime} \\ p > 2}} g(X/p) \leqq \frac{1}{4} \sum_{\substack{p \text{ prime} \\ 2 < p \leqq x/2}} \left(\frac{X}{p} + 1\right)^{d+1} \leqq$$

$$\leqq \frac{1}{4} \sum_{\substack{p \text{ prime} \\ 2 < p \leqq X/2}} \left(\frac{1}{p^2}(X+1)^{d+1} + \frac{d+1}{p} X + 1\right) <$$

$$< \frac{1}{4}\left(\frac{1}{4}(X+1)^{d+1} + (d+1)\frac{X^2}{4} + \frac{X}{4}\right) \leqq$$

$$\leqq \frac{1}{16}((X+1)^{d+1} + (d+2)X^2).$$

When $X \geqq 2d+4$, then $(d+1)\log(1+X^{-1}) < (d+1)X^{-1} < 1/2$, so that $(X+1)^{d+1} < e^{1/2}X^{d+1}$. Also $(d+2)X^2 \leqq \frac{1}{2}X^{d+1}$, so that our sum is

$$\leqq \left(\frac{1}{16}\right)\left(e^{1/2} + \frac{1}{2}\right) X^{d+1} < (.14)\, X^{d+1}.$$

Comparison with (2.5) and (2.6) gives the explicit bound

$$N(\mathbb{Q}, d, X) > \frac{1}{10} X^{d+1} \quad \text{when } X \geqq 2d+4.$$

When $d \geqq 2$ and $X \geqq 4d \cdot 2^d \geqq (2d+4) \cdot 2^d$, (2.2) yields

$$Z(\mathbb{Q}, d, n, X) \geqq Z(\mathbb{Q}, d, 1, X) > N(\mathbb{Q}, d, 2^{-d}X) >$$

$$> \frac{1}{10}(X/2^d)^{d+1} > (X/6^d)^{d+1}.$$

Now $P = (1 : \sqrt[d]{2})$ is counted by $Z(\mathbb{Q}, d, 1, 2)$, so that $Z(\mathbb{Q}, d, n, X) \geqq$ $\geqq Z(\mathbb{Q}, d, 1, 2) \geqq 1$ when $X \geqq 2$. Thus for X in the range $2 \leqq X < 4d \cdot 2^d$,

$$Z(\mathbb{Q}, d, n, X) \geqq (X/(4d \cdot 2^d))^{d+1} > (X/6^d)^{d+1}.$$

We have established (1.8) for $d \geqq 2$. When $d = 1$, (1.8) follows from (1.7).

3. A Connection with Decomposable Forms

Before embarking on the upper bounds of our theorem, we wish to point out a simple counting argument via decomposable forms.

We will always represent $P \in \mathbb{P}^n$ by a tuple $(\alpha_0 : \alpha_1 : \ldots : \alpha_n)$ with each $\alpha_i \in \mathbb{Q}(P)$. When $[K(P) : K] = d$, let $\tau_1, \ldots, \tau_d$ be the embeddings of $K(P)$ over K into A, and set

$$f(\boldsymbol{x}) = f(x_0, \ldots, x_n) = \prod_{i=1}^{d} (\tau_i(\alpha_0 x_0 + \cdots + \alpha_n x_n));$$

here τ_i is applied to the coefficients. Then $f \in K[\boldsymbol{x}]$ is a form of degree d, and it is irreducible over K. This last assertion is easily seen, or else it may be found in [5, Ch. VII, Lemma 1B]. We have

$$H(f) \leqq c_6(d, n) \prod_{i=1}^{d} H(\tau_i(\alpha_0 x_0 + \cdots + \alpha_n x_n)) = c_6(d, n) H(P)^d$$

by [2, Ch. III, Proposition 2.4], and the fact that conjugate points have the same height. Therefore, with $k = \deg K$,

$$H_K(f) = H(f)^k \leqq c_7(K, d, n) H(P)^{dk} = c_7(K, d, n) H_K(P).$$

When $H_K(P) \leqq X$, this gives

$$H_K(f) \leqq c_7(K, d, n) X. \tag{3.1}$$

The form f is decomposable, i.e., it is a product of linear forms (with coefficients in A). The decomposable forms (modulo constant factors) make up a projective manifold V, embedded in the projective space $\mathbb{P}^m$ with $m = \binom{d+n}{d} - 1$, consisting of all forms (modulo constant factors) in $n + 1$ variables of degree d. Now $\dim V = dn$, so that by (1.9) (and by projecting V on a suitable coordinate space of dimension dn), the number of $f \in V(K)$ (i.e., $f \in V$ with coefficients in K) satisfying (3.1) is $\leqq c_8(K, d, n) X^{dn+1}$. Since f has d linear factors, we may conclude that

$$Z(K, d, n, X) \leqq c_9(K, d, n) X^{dn+1}.$$

4. The Main Lemma

Lemma. *Let K be a number field of degree k, let $s \geqq 1$, $t \geqq 1$, and $\boldsymbol{\theta} = (\theta_1, \ldots, \theta_s) \neq 0$ with components in K. When $\boldsymbol{\alpha} = (\alpha_1, \ldots, \alpha_t) \in K^t$, write $H_K(\boldsymbol{\theta}, \boldsymbol{\alpha}) = H_K(\theta_1, \ldots, \theta_s, \alpha_1, \ldots, \alpha_t)$ and*

$$H_0(\boldsymbol{\alpha}) = H_K(\boldsymbol{\theta}, \boldsymbol{\alpha})/H_K(\boldsymbol{\theta}). \tag{4.1}$$

Then the number of $\boldsymbol{\alpha} \in K^t$ *with* $H_0(\boldsymbol{\alpha}) \leqq X$ *is*

$$\leqq 2^{kt + t(t+15)/2} H_K(\boldsymbol{\theta})^t X^{t+1}. \tag{4.2}$$

Proof. We begin with case $t = 1$. Here we will prove the slightly stronger estimate that the number of $\alpha \in K$ with $H_0(\alpha) \leqq X$ is

$$\leqq 2^{k+5} H_K(\boldsymbol{\theta}) X^2. \tag{4.3}$$

Our argument will be similar to one in [1]. Fix an Archimedean absolute value $v_0 \in M(K)$. We may suppose that K is embedded in $\mathbb{C}$ and that $|\xi|_{v_0} = |\xi|$ for $\xi \in K$. We have

$$H_0(\alpha) = \left(\frac{\max(|\boldsymbol{\theta}|, |\alpha|)}{|\boldsymbol{\theta}|}\right)^{n_{v_0}} \prod_{\substack{v \in M(k) \\ v \neq v_0}} \left(\frac{\max(|\boldsymbol{\theta}|_v, |\alpha|_v)}{|\boldsymbol{\theta}|_v}\right)^{n_v} = H_1(\alpha) H_2(\alpha),$$

say. Given $X_1 \geqq 1$, $X_2 \geqq 1$, we first wish to estimate the number N of elements $\alpha \in K$ with

$$H_1(\alpha) \leqq X_1, \qquad H_2(\alpha) \leqq X_2. \tag{4.4}$$

Such α have $|\alpha| \leqq |\boldsymbol{\theta}| X_1^{1/n_{v_0}}$.

Let us suppose that v_0 corresponds to a complex (i.e., non-real) embedding of K. Then $n_{v_0} = 2$ and $|\alpha| \leqq |\boldsymbol{\theta}| X_1^{1/2}$, so that in particular α lies in the square in the complex plane given by $|\mathcal{Re}\,\alpha|$, $|\mathcal{Im}\,\alpha| \leqq$ $\leqq |\boldsymbol{\theta}| X_1^{1/2}$. Suppose $N \geqq 16$, and choose the integer m with $m^2 < N \leqq$ $\leqq (m+1)^2$, so that $2m^2 > N$. We divide the square into m^2 squares of side $2|\boldsymbol{\theta}| X_1^{1/2}/m$. There will be two of our N elements α in the same subsquare, say α, α'. Then $|\alpha - \alpha'| \leqq 2\sqrt{2}|\boldsymbol{\theta}| X_1^{1/2}/m$, and

$$|\alpha - \alpha'|^2 \leqq 8|\boldsymbol{\theta}|^2 X_1/m^2 < 2^4|\boldsymbol{\theta}|^2 X_1/N.$$

A similar argument can be made when v_0 corresponds to a real embedding, and in both cases we get $\alpha \neq \alpha'$ in our set with

$$|\alpha - \alpha'|_{v_0}^{n_{v_0}} < 2^4 |\boldsymbol{\theta}|_{v_0}^{n_{v_0}} X_1/N. \tag{4.5}$$

When v is ultrametric

$$|\alpha - \alpha'|_v \leqq |\boldsymbol{\theta}|_v \max\left(\frac{|\alpha|_v}{|\boldsymbol{\theta}|_v}, \frac{|\alpha'_v|}{|\boldsymbol{\theta}|_v}\right) \leqq$$

$$\leqq |\boldsymbol{\theta}|_v \max\left(1, \frac{|\alpha|_v}{|\boldsymbol{\theta}|_v}\right) \max\left(1, \frac{|\alpha'|_v}{|\boldsymbol{\theta}|_v}\right),$$

so that

$$|\alpha - \alpha'|_v \leqq |\boldsymbol{\theta}|_v \frac{\max(|\boldsymbol{\theta}|_v, |\alpha|_v)}{|\boldsymbol{\theta}|_v} \frac{\max(|\boldsymbol{\theta}|_v, |\alpha'|_v)}{|\boldsymbol{\theta}|_v}.$$

This estimate, but with an extra factor 2, is still valid when v is Archimedean. In conjunction with the product formula and with (4.4), (4.5) we obtain

$$1 = \prod_{v \in M(K)} |\alpha - \alpha'|_v^{n_v} \leqq 2^{k+3} \left(\prod_{v \in M(K)} |\boldsymbol{\theta}|_v^{n_v} \right) X_1 X_2^2 / N,$$

so that

$$N \leqq 2^{k+3} H_K(\boldsymbol{\theta}) X_1 X_2^2. \tag{4.6}$$

This estimate is also true when $N < 16$.

Next, consider $\alpha \in K$ with

$$2^{m-1} \leqq H_1(\alpha) < 2^m \quad \text{and} \quad H_0(\alpha) \leqq X. \tag{4.7}$$

They have $H_2(\alpha) \leqq X \cdot 2^{1-m}$. By applying our estimate above with $X_1 = 2^m$, $X_2 = X \cdot 2^{1-m}$, the number N_m of such α is seen to have

$$N_m \leqq 2^{k+5-m} H_k(\boldsymbol{\theta}) X^2.$$

Every α with $H_0(\alpha) \leqq X$ satisfies (4.7) for some integer $m \geqq 1$, so that the bound (4.3) follows by taking the sum over m.

The lemma will now be proved by induction on t. When $t > 1$, write $\boldsymbol{\alpha}' = (\alpha_1, \ldots, \alpha_{t-1})$ and

$$H_0(\boldsymbol{\alpha}) = H_0(\boldsymbol{\alpha}') H^*(\boldsymbol{\alpha})$$

with

$$H_0(\boldsymbol{\alpha}') = \frac{H_K(\boldsymbol{\theta}, \boldsymbol{\alpha}')}{H_K(\boldsymbol{\theta})}, \qquad H^*(\boldsymbol{\alpha}) = \frac{H_K(\boldsymbol{\theta}, \boldsymbol{\alpha})}{H_K(\boldsymbol{\theta}, \boldsymbol{\alpha}')}.$$

Given an integer $m \geqq 1$, consider $\boldsymbol{\alpha} \in K^t$ with

$$2^{m-1} \leqq H_0(\boldsymbol{\alpha}') < 2^m, \qquad H_0(\boldsymbol{\alpha}) \leqq X. \tag{4.8}$$

By the case $t-1$ of the lemma, the number of possibilities for $\boldsymbol{\alpha}'$ is

$$< 2^{k(t-1)+(t-1)(t+14)/2} H_K(\boldsymbol{\theta})^{t-1} \cdot 2^{mt}.$$

But when $\boldsymbol{\alpha}'$ is given, set $H_0(\alpha_t) = H^*(\boldsymbol{\alpha})$, so that $H_0(\alpha_t) = H_0(\boldsymbol{\alpha})/H_0(\boldsymbol{\alpha}') \leqq X \cdot 2^{1-m}$. By the case $t=1$ of the lemma, the number of $\alpha_t \in K$ with this property is

$$\leqq 2^{k+5} H_K(\boldsymbol{\theta}, \boldsymbol{\alpha}')(X \cdot 2^{1-m})^2 = 2^{k+7-2m} H_K(\boldsymbol{\theta}, \boldsymbol{\alpha}') X^2 < 2^{k+7-m} H_K(\boldsymbol{\theta}) X^2$$

in view of (4.8). The total number of $\boldsymbol{\alpha} \in K^t$ with (4.8) is less than

$$2^{kt+t(t+13)/2+m(t-1)} H_K(\boldsymbol{\theta})^t X^2. \tag{4.9}$$

Each $\boldsymbol{\alpha}$ with $H_0(\boldsymbol{\alpha}) \leqq X$ satisfies (4.8) with some m in $1 \leqq m \leqq m_0 = 1 + [\log_2 X]$. Taking the sum of (4.9) over m in this range, we get

$$< 2^{kt+t(t+13)/2+1+m_0(t-1)} H_K(\boldsymbol{\theta})^t X^2 \leqq$$
$$\leqq 2^{kt+t(t+15)/2} H_K(\boldsymbol{\theta})^t X^{t+1}.$$

5. Proof of the Cases $d = 1$ and $n = 1$ of the Theorem

$Z(K, 1, n, X)$ is the number of $P \in \mathbb{P}^n(K)$ with $H_K(P) \leqq X$. We first consider P of the type $(1 : \alpha_1 : \ldots : \alpha_n)$. We apply the Lemma with $s = 1$, $t = n$, $\boldsymbol{\theta} = (1)$, $H_K(\boldsymbol{\theta}) = 1$. The number of points P in question is

$$\leqq 2^{kn+n(n+15)/2} X^{n+1} = g(k, n) X^{n+1},$$

say. By the same reasoning, the number of points $P \in \mathbb{P}^n(K)$ with $H_K(P) \leqq X$ of the type $(0 : \ldots : 0 : 1 : \alpha_{j+1} : \ldots : \alpha_n)$ is $\leqq g(k, n-j) X^{n-j+1}$. Taking the sum over j, $0 \leqq j \leqq n$, we obtain

$$Z(K, 1, n, X) < 2^{kn+n(n+15)/2+1} X^{n+1} \tag{5.1}$$

and the case $d = 1$ of the Theorem.

We now turn to the case $n = 1$. We construct a polynomial f as in section 3. In our case, $f = f(x_0, x_1)$ is a binary form of degree d. We may take $c_6(d, 1) = 2^d$ [see 8, Ch. VIII, Thm. 5.9], so that (3.1) becomes

$$H_K(f) \leqq 2^{dk} X.$$

The coefficients of $f = a_d x_0^d + \ldots + a_0 x_1^d$ represent a point $P = (a_d : \ldots : a_0) \in \mathbb{P}^d(K)$. Thus the number of possible forms f (up to constant factors) is $\leqq Z(K, 1, d, 2^{dk}X)$. In view of (5.1), and since f has d linear factors, we get

$$Z(K, d, 1, X) \leqq dZ(K, 1, d, 2^{dk}X) \leqq d \cdot 2^{kd + d(d+15)/2 + 1} \cdot 2^{dk(d+1)} X^{d+1} < \\ < 2^{kd^2 + 2kd + d^2 + 9d} X^{d+1}. \tag{5.2}$$

6. Proof of the Theorem

Let $Z^0(K, d, n, X)$ be the number of $P \in \mathbb{P}^n$ with (1.3) and with $P = (1 : \alpha_1 : \ldots : \alpha_n)$ such that

$$K \subsetneqq K(P_1) \subsetneqq \ldots \subsetneqq K(P_n)$$

where $P_j = (1 : \alpha_1 : \ldots : \alpha_j)$. We will prove that

$$Z^0(K, d, n, X) \leqq 2^{kd^2 + 4kd + d^2 + 9d} X^{d+n}. \tag{6.1}$$

The case $n = 1$ follows from (5.2). In the induction step from $n - 1$ to n, set $L = K(P_{n-1})$ and $d_1 = [L : K]$, $d_2 = [K(P) : L]$, so that $d_1 d_2 = d$ and $d_1 > 1$, $d_2 > 1$. Initially suppose d_1, d_2 to be fixed. Here $H(P_{n-1}) \leqq \leqq H(P_n) = H_K(P_n)^{1/dk} \leqq X^{1/dk}$ by (1.3), and with $k = \deg K$. We obtain $H_K(P_{n-1}) = H(P_{n-1})^{d_1 k} \leqq X^{1/d_2} \leqq X$. By induction, the number of possibilities for $\alpha_1, \ldots, \alpha_{n-1}$ is at most

$$2^{kd_1^2 + 4kd_1 + d_1^2 + 9d_1} X^{d_1 + n - 1}. \tag{6.2}$$

Next, $H(1 : \alpha_n) \leqq H(P) \leqq X^{1/dk}$, so that $H_L(1 : \alpha_n) \leqq X^{[L:\mathbb{Q}]d_2/kd} = X^{kd_1 d_2/kd} = X$. By applying (5.2) with the field L (in place of K) and noting that $[L : \mathbb{Q}] = kd_1$, we see that the number of possibilities for α_n with $[L(\alpha_n) : L] = d_2$ and $H_L(1 : \alpha_n) \leqq X$ is at most

$$2^{kd_1 d_2^2 + 2kd_1 d_2 + d_2^2 + 9d_2} X^{d_2 + 1}. \tag{6.3}$$

Taking the product of (6.2), (6.3) we get

$$2^{k(d_1^2 + d_1 d_2^2) + k(4d_1 + 2d_1 d_2) + d_1^2 + d_2^2 + 9d_1 + 9d_2} X^{d_1 + d_2 + n}. \tag{6.4}$$

Observe that $d_1^2 + d_1 d_2^2 < d^2$, $4d_1 + 2d_1 d_2 \leqq 4d$, $d_1^2 + d_2^2 \leqq d^2/2$ and $d_1 + d_2 \leqq d$. We still have to count the number of possible factorizations $d = d_1 d_2$. This number is $\leqq d \leqq 2^{d^2/2}$. Multiplying (6.4) by $2^{d^2/2}$ we get the bound in (6.1).

Next, let $Z^0(K, d, n, u, X)$ be the number of $P \in \mathbb{P}^n$ with (1.3) and with $P = (1 : \alpha_1 : \ldots : \alpha_n)$ such that

$$K \subsetneqq K(P_1) \subsetneqq \ldots \subsetneqq K(P_u) = K(P).$$

We first count the number of $\alpha_1, \ldots, \alpha_u$ with

$$2^{m-1} < H_K(P_u) \leqq 2^m.$$

By (6.1), this number is

$$Z^0(K, d, u, 2^m) \leqq 2^{kd^2 + 4kd + d^2 + 9d} \cdot 2^{m(d+u)}. \tag{6.5}$$

Given $\boldsymbol{\theta} = (1, \alpha_1, \ldots, \alpha_u)$, the $(n-u)$-tuple $\boldsymbol{\alpha}' = (\alpha_{u+1}, \ldots, \alpha_n)$ has $H_K(\boldsymbol{\theta}, \boldsymbol{\alpha}')/(H_K(\boldsymbol{\theta}) < X \cdot 2^{1-m}$. By the Lemma with $s = u+1$, $t = n-u$, and $K(\boldsymbol{\alpha}_u) = K(P)$ in place of K, the number of possibilities for $\boldsymbol{\alpha}'$ is

$$< 2^{kd(n-u) + (n-u)(n-u+15)/2} \cdot 2^{m(n-u)} (X \cdot 2^{1-m})^{n-u+1}.$$

Taking the product with (6.5) we obtain (on noting $u \geqq 1$)

$$< 2^{k(d^2 + dn + 3d) + d^2 + 9d + n(n+15)/2} X^{n-u+1} \cdot 2^{m(d+u-1)}.$$

We still have to sum over m in $1 \leqq m \leqq m_0 = [\log_2 X] + 1$. The sum of $2^{m(d+u-1)}$ over this range is $\leqq 2^{d+u} X^{d+u-1}$. Therefore

$$Z^0(K, d, n, u, X) < 2^{kd(d+n+3) + d^2 + 10d + n^2 + 9n - 1} X^{d+n}.$$

For any $P = (\alpha_0 : \ldots : \alpha_n)$, there are numbers u and $i_0 < i_1 \ldots < i_u$ such that $\alpha_{i_0} \neq 0$ and $K \subsetneqq K(\alpha_{i_0} : \alpha_{i_1}) \subsetneqq \ldots \subsetneqq K(\alpha_{i_0} : \ldots : \alpha_{i_u}) = K(P)$. After reordering, P will be of the type counted by $Z^0(K, d, n, u, X)$. Given u, the number of $(u+1)$-tuples $i_0 < i_1 < \ldots < i_u$ is $\binom{n+1}{u+1}$, and summing over u we get a factor 2^{n+1}. Therefore

$$Z(K, d, n, X) \leqq 2^{n+1} \cdot 2^{kd(d+n+3) + d^2 + 10d + n^2 + 9n - 1} X^{d+n}.$$

7. The Counting Function Z^*

Given a field K of degree k we have $d(P) \leqq k\, d_K(P)$, therefore $H_{\mathbb{Q}}(P) \leqq H_K(P)$. The inequality

$$Z^*(K, d, n, X) \geqq Z(K, d, n, X) \tag{7.1}$$

follows. Now let $N \supseteq K$ be a field which is normal over $\mathbb{Q}$. We will prove that

$$Z^*(K, d, n, X) \leqq \sum_{L \subseteq N} \sum_{e|d} Z(L, e, n, X), \tag{7.2}$$

where the outer sum is over the subfields L of N.

Clearly $[K(P):K] = d$ implies $[N(P):N] = e$ with $e \mid d$. Construct the form $f = f(x_0, \ldots, x_n)$ as in Section 3, but with respect to the field N. Then f is of degree e, it lies in $N[\boldsymbol{x}]$, and is irreducible. It is the form of least degree in $N[\boldsymbol{x}]$ with the factor $\alpha_0 x_0 + \cdots + \alpha_n x_n$ (which lies in $A[\boldsymbol{x}]$). Let L be the field obtained from $\mathbb{Q}$ by adjoining the coefficients of f. Let $l = \deg L$ and let $\sigma_1, \ldots \sigma_l$ be the embeddings of L into A. The polynomials $\sigma_1 f, \ldots, \sigma_l f$ lie in $N[\boldsymbol{x}]$ and they are pairwise distinct, therefore pairwise coprime since f, and therefore each $\sigma_i f$, is irreducible in $N[\boldsymbol{x}]$. The product $F = (\sigma_1 f) \cdots (\sigma_l f)$ lies in $\mathbb{Q}[\boldsymbol{x}]$. Any nonconstant factor G of F, $G \in \mathbb{Q}[\boldsymbol{x}]$, must be divisible by some $\sigma_i f$, since these are irreducible over N. Therefore G must be divisible by each $\sigma_i f$, hence must be divisible by their product, since they are coprime. Therefore F is irreducible. Since F has the factor $\alpha_0 x_0 + \cdots + \alpha_n x_n$, we may deduce that $d(P) = \deg F = le = l d_L(P)$, and $H_{\mathbb{Q}}(P) = H_L(P)$.

We may conclude that the number of P with given e and L is bounded by $Z(L, e, n, X)$. Now (7.2) follows.

References

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

[2] Lang, S.: Fundamentals of Diophantine Geometry. Berlin—Heidelberg—New York: Springer. 1983.

[3] Northcott, D. G.: An inequality in the theory of arithmetic on algebraic varieties. Proc. Camb. Phil. Soc. **45**, 502—509 and 510—518 (1949).

[4] Schanuel, S. H.: Heights in number fields. Bull. Soc. Math. France **107**, 433—449 (1979).

[5] Schmidt, W. M.: Diophantine Approximation. Lect. Notes Math. **785**. Berlin—Heidelberg—New York: Springer. 1980.

[6] Schmidt, W. M.: Diophantine Approximations and Diophantine Equations. Lect. Notes Math. **1467**. Berlin—Heidelberg—New York: Springer. 1991.

[7] Schmidt, W. M.: Northcott's Theorem on heights. II. The quadratic case. Acta Arithmetica. To appear.

[8] Silverman, J. H.: The Arithmetic of Elliptic Curves. Berlin—Heidelberg—New York: Springer. 1985.

W. M. Schmidt
Department of Mathematics
University of Colorado
Boulder, CO 80309
USA