

Werk

Titel: Journal für die reine und angewandte Mathematik

Verlag: de Gruyter

Jahr: 1993

Kollektion: Mathematica

Digitalisiert: Niedersächsische Staats- und Universitätsbibliothek Göttingen

Werk Id: PPN243919689_0442

PURL: http://resolver.sub.uni-goettingen.de/purl?PPN243919689_0442

LOG Id: LOG_0005

LOG Titel: Logarithmic forms and group varieties.

LOG Typ: article

Übergeordnetes Werk

Werk Id: PPN243919689

PURL: <http://resolver.sub.uni-goettingen.de/purl?PPN243919689>

Terms and Conditions

The Goettingen State and University Library provides access to digitized documents strictly for noncommercial educational, research and private purposes and makes no warranty with regard to their use for other purposes. Some of our collections are protected by copyright. Publication and/or broadcast in any form (including electronic) requires prior written permission from the Goettingen State- and University Library.

Each copy of any part of this document must contain there Terms and Conditions. With the usage of the library's online system to access or download a digitized document you accept the Terms and Conditions.

Reproductions of material on the web site may not be made for or donated to other repositories, nor may be further reproduced without written permission from the Goettingen State- and University Library.

For reproduction requests and permissions, please contact us. If citing materials, please give proper attribution of the source.

Contact

Niedersächsische Staats- und Universitätsbibliothek Göttingen
Georg-August-Universität Göttingen
Platz der Göttinger Sieben 1
37073 Göttingen
Germany
Email: gdz@sub.uni-goettingen.de

Logarithmic forms and group varieties

By *A. Baker* at Cambridge and *G. Wüstholz* at Zürich

1. Introduction

The past decade has seen some spectacular progress concerning multiplicity estimates on group varieties. The first substantial work in this context is due to Masser and Wüstholz [18]; they considered a single differential operator on such a variety and their results led, amongst other things, to the new theory of large transcendence degree. One of the main ingredients was the use of effective commutative algebra which was introduced into the subject by Nesterenko [20] through the study of E -functions and which was subsequently extended by Brownawell and Masser [10]. In 1983, Wüstholz [29] succeeded in obtaining a general theorem on multiplicity estimates appertaining to arbitrarily many differential operators and, up to a constant multiple, the results are best possible. The work has already found application to yield an abelian analogue of the famous Lindemann theorem and to solve a long-standing problem concerning periods of elliptic integrals (see [26], [27], [28]). The key result in this context is now the analytic subgroup theorem established in Wüstholz [30] which includes as special cases most of the classical theorems in transcendence theory. In particular it furnishes a generalisation in terms of algebraic groups of the qualitative version of Baker's theorem on linear forms in the logarithms of algebraic numbers.

The purpose of the present paper is to prove a quantitative version of Baker's theorem which is fully explicit with respect to all the parameters and which we believe to be a basically definitive result. Our work has evolved from a long series of earlier researches in the subject stretching over some twenty-five years and with roots going back to the celebrated Gelfond-Schneider solution to Hilbert's seventh problem.

Throughout the paper we shall denote by $\alpha_1, \dots, \alpha_n$ algebraic numbers, not 0 or 1, and by $\log \alpha_1, \dots, \log \alpha_n$ we shall mean fixed determinations of the logarithms. Let K be the field generated by $\alpha_1, \dots, \alpha_n$ over the rationals $\mathbb{Q}$ and let d be the degree of K . For each α in K and any given determination of $\log \alpha$ we define the modified height $h'(\alpha)$ by

$$h'(\alpha) = \frac{1}{d} \max(h(\alpha), |\log \alpha|, 1),$$

where $h(\alpha)$ is the standard logarithmic Weil height of α (for the definition see § 2). We shall be concerned with the linear form

$$L(z_1, \dots, z_n) = b_1 z_1 + \dots + b_n z_n,$$

where $b_1, \dots, b_n$ are rational integers, not all 0. In analogy with the modified height introduced above, we define

$$h'(L) = \frac{1}{d} \max(h(L), 1),$$

where $h(L)$ is the logarithmic Weil height of L (again see § 2). We shall prove the following theorem.

Theorem. *If $A = L(\log \alpha_1, \dots, \log \alpha_n) \neq 0$ then*

$$\log |A| > -C(n, d) h'(\alpha_1) \dots h'(\alpha_n) h'(L),$$

where

$$C(n, d) = 18(n+1)! n^{n+1} (32d)^{n+2} \log(2nd).$$

In order to compare with previous results we suppose that $B \geq \max |b_j|$ and, for any α as above, we take A as an upper bound for the absolute values of the relatively prime integer coefficients in the minimal defining polynomial for α . Then (see § 2) if $A \geq e$, $B \geq e$ and $\log \alpha$ has its principal value we have

$$h'(L) \leq \log B, \quad h'(\alpha) \leq \pi + \log A \leq 4 \cdot 2 \log A.$$

Since $n! \leq n^{n+1} e^{-n+1}$ we obtain

$$C(n, d) \leq 2400(3 \cdot 5n)^{2n+3} d^{n+2} \log(2nd),$$

whence

$$\log |A| > -(16nd)^{2(n+2)} \log A_1 \dots \log A_n \log B,$$

where A_j is defined like A with $\alpha = \alpha_j$. A result of this kind was established for the first time by Baker [3], but with an extra factor $\log(\log A_1 \dots \log A_{n-1})$ on the right and with an exponent $200n$ in place of $2(n+2)$. The deletion of the logarithmic factor is a consequence of the work on multiplicity estimates discussed earlier and it was developed particularly for this problem in the series of papers of Wüstholz [31], [32]. Here, especially, the Geometry of Numbers played an important role. Based on these ideas, Wüstholz [32] and Philippon and Waldschmidt [21] succeeded in giving inequalities of the desired type though without establishing an explicit expression for $C(n, d)$. The Philippon-Waldschmidt approach originates from Waldschmidt's paper [25] where certain improvements were obtained in the constants occurring in one of the theorems of Baker [3]. It is not clear to us, at the time of writing, exactly what form for $C(n, d)$ can be derived from their exposition. Studies of a group located at Bowling Green State University in Ohio [8] have yielded some refinements in the work of Waldschmidt [25] but without changing the general shape.

The first part of our proof follows on classical lines (see [4]). After the construction of an auxiliary function of several variables one applies an inductive extrapolation algorithm to increase the number of zeros of the function counted with multiplicities. By a suitable choice of the size of the inductive steps one could now apply the result of [31] directly so as to yield a theorem of the same kind as that quoted above; but the numerical values of the constants occurring in our expression for $C(n, d)$ would be greater. In order to obtain the version given here we apply Kummer descent as in [3] so as to furnish a new function with a larger proportion of zeros; the result then follows at once as in [32]. The extent of the descent is determined by the multiplicity estimates and depends here only on n and d ; in previous applications it depended also on the heights of the α 's and this explains the occurrence of the extra factor referred to above.

An important consideration in deriving our result has been the widespread application of the theory of linear forms in logarithms to the solution of Diophantine problems. The precision of $C(n, d)$ is particularly significant in computations and it would seem that our expression strengthens substantially all previous expressions in this context. Our aim has been to establish a sharp result of general type useful in specific calculations. It should be noted, however, that in special circumstances, for instance when n is small or when all the α 's are near to 1, careful analysis adapted to the particular case would certainly yield some improvements.

It is possible to extend our result to an arbitrary inhomogeneous linear form

$$\beta_0 + \beta_1 z_1 + \dots + \beta_n z_n$$

with algebraic coefficients and we would expect essentially the same estimate for $\log |A|$ with $h'(L)$ replaced by $h'(L) + \log(h'(\alpha_1) \dots h'(\alpha_n))$. The work can further be generalised in the direction of [2] (Sharpening II). The latter has been fundamental to several developments in Diophantine analysis; see, for example, Baker and Stewart [6] which includes a particularly efficient Kummer descent. Furthermore it is clear that analogous theorems can be proved in the p -adic domain; we leave the details for future publications.

2. Heights

We give here the definition and basic properties of the logarithmic Weil height that we use in our work.

Let K be an algebraic number field of degree d over the rationals $\mathbb{Q}$. We signify by v an arbitrary place of K and we denote by K_v the completion of K at v . Then $\mathbb{Q}_v$ denotes the closure of $\mathbb{Q}$ in K_v and we put $d_v = [K_v : \mathbb{Q}_v]$. We normalise the absolute value $|\cdot|_v$ by defining $|p|_v = p^{-d_v}$ when v is non-Archimedean (written $v \nmid \infty$) and divides the rational prime p (written $v|p$), and by putting $|x|_v = |\tau(x)|^{d_v}$ when v is an Archimedean place (written $v|\infty$). Here τ denotes the embedding of K into $\mathbb{C}$ which defines v and $|\tau(x)|$ is the Euclidean absolute value on $\mathbb{R}$ or $\mathbb{C}$ according as v is real or complex. Note that, when $v|p$, $\mathbb{Q}_v$ is isomorphic to $\mathbb{Q}_p$ and, when $v|\infty$, it is isomorphic to $\mathbb{R}$.

Now let $\mathbb{P}^n$ be the projective space of dimension n over K , and let

$$x = (x_0 : x_1 : \dots : x_n)$$

be a K -rational point of $\mathbb{P}^n$. We define the logarithmic Weil height of x as

$$h(x) = \sum_v \log(\max |x_j|_v).$$

The expression is independent of the projective co-ordinates of x by virtue of the product formula. For any α in K the point $x = (1 : \alpha)$ is a K -rational point of $\mathbb{P}^1$ and we define $h(\alpha) = h(x)$. Similarly, for any linear form

$$L(z_1, \dots, z_n) = l_1 z_1 + \dots + l_n z_n$$

with coefficients in K , the point $x = (l_1 : \dots : l_n)$ is a K -rational point of $\mathbb{P}^{n-1}$ and we define $h(L) = h(x)$. It is customary to define the absolute logarithmic Weil height of a K -rational point x in $\mathbb{P}^n$ as $h_0(x) = (1/d) h(x)$; this is independent of the choice of K , that is, if K' is a finite extension of K then h_0 defined with respect to K and K' is the same. Plainly the modified height occurring in our theorem is essentially the absolute logarithmic Weil height. As obvious consequences of the definition of $h(x)$ we have for any algebraic numbers α, β in K

$$h(\alpha\beta) \leq h(\alpha) + h(\beta),$$

and, for non-zero α and any integer m ,

$$h(\alpha^m) = mh(\alpha).$$

The classical results in the subject were expressed in terms of a different height, that is, the least function A indicated in §1. They can be readily related; indeed we have

$$(1) \quad \delta h_0(\alpha) = \log a_0 + \sum_{j=1}^{\delta} \log \max(1, |\alpha^{(j)}|),$$

where the minimal polynomial for α is

$$a_0 x^{\delta} + a_1 x^{\delta-1} + \dots + a_{\delta} = a_0 \prod_{j=1}^{\delta} (x - \alpha^{(j)}), \quad a_0 > 0.$$

By a well known inequality of Landau [14] (see also Mahler [16], [17]) we have

$$h_0(\alpha) \leq \frac{1}{2\delta} \log \left(\sum_{j=0}^{\delta} a_j^2 \right).$$

The right hand side does not exceed $\log(\sqrt{2}A)$. Further, if $\log \alpha$ has its principal value, then clearly $|\log \alpha| \leq \pi + \log(\delta A)$. Hence we obtain the asserted estimate $h'(\alpha) \leq \pi + \log A$.

3. Siegel's lemma

As usual in this context we shall need to establish the existence of small solutions of a system of homogeneous linear equations

$$(2) \quad L_i(x_1, \dots, x_N) = \sum_{j=1}^N a_{ij} x_j = 0 \quad (1 \leq i \leq M).$$

An argument for deriving such solutions was implicit in the research of Thue but the first explicit formulation is due to Siegel. He discussed the case when the a_{ij} are rational integers and he specified a bound for a non-trivial solution in integers $x_1, \dots, x_N$ by means of Dirichlet's box principle. Here we shall be concerned with the more general situation where the a_{ij} are elements of an algebraic number field K of degree d and we seek a small non-trivial solution in the ring of integers $\mathcal{O}_K$ of K . Such studies are already well known in the literature, the sharpest bound to date being due to Bombieri and Vaaler [9]. Their exposition is based on the Geometry of Numbers and, in particular, on an adelic analogue of Minkowski's successive minima theorem (see the reference to work of Macfeat in the addendum to [9]).

The result that we shall use is the following:

Lemma 1. *If $N > M$ then the equations (2) have a non-trivial solution $x = (x_1, \dots, x_N)$ with co-ordinates in $\mathcal{O}_K$ such that*

$$h(x) \leq \frac{1}{2} \log |\mathcal{D}| + \frac{1}{N-M} \sum_{i=1}^M \left(\frac{1}{2} d \log N + h(L_i) \right),$$

where $\mathcal{D}$ denotes the discriminant of K .

The lemma is a consequence of Theorem 9 of [9]. For on writing A for the matrix (a_{ij}) and A_i for the row vector $(a_{i1}, \dots, a_{iN})$ we have

$$H(A) \leq H(A_1) \dots H(A_M),$$

where H is the height defined in [9]. Hence Theorem 9 gives a non-trivial solution x with

$$h(x) \leq \frac{1}{2} \log |\mathcal{D}| + \frac{1}{N-M} \sum_{i=1}^M \log H(A_i).$$

But we have

$$\log H(A_i) \leq \frac{1}{2} d \log N + h(A_i);$$

indeed $\log H$ and our h differ only at the infinite places and there the local difference is at most $\frac{1}{2} \log N$ or $\log N$ according as the place is real or complex.

We remark that a result of the same kind as above sufficient for our purpose can be obtained directly from Dirichlet's principle after reduction to the rational case, but it is plainly convenient to appeal to the existing literature.

4. Discriminant

Let $\alpha_1, \dots, \alpha_n$ be algebraic numbers, let $K = \mathbb{Q}(\alpha_1, \dots, \alpha_n)$ and let d be the degree of K . We establish here an estimate for the discriminant $\mathcal{D}$ of K . Estimates of this kind are widely used in Diophantine problems but we could not find a convenient reference to our particular result.

We define $K_j = \mathbb{Q}(\alpha_j)$ and we denote by d_j the degree of K_j . Then $K = K_1 \dots K_n$ and d_j divides d . We shall use Lemma 7 of [23]; this asserts that $\mathcal{D}$ divides $\mathcal{D}_1^{d/d_1} \dots \mathcal{D}_n^{d/d_n}$, where $\mathcal{D}_j$ is the discriminant of K_j . We proceed to prove that

$$\log |\mathcal{D}_j| \leq d_j(d_j - 1)(2h_0(\alpha_j) + \log 2).$$

This implies that $\log |\mathcal{D}|$ is at most

$$\sum_{j=1}^n (d_j - 1)(2h(\alpha_j) + d \log 2).$$

Hence we have:

Lemma 2. $\log |\mathcal{D}| \leq 2(d - 1)(h(\alpha_1) + \dots + h(\alpha_n) + \frac{1}{2}nd \log 2).$

To establish the estimate for $|\mathcal{D}_j|$ we put $\alpha = \alpha_j$ and we signify by a_0 the leading coefficient in the minimal polynomial for α . Then $\mathcal{D}_j$ divides

$$a_0^{d_j(d_j-1)} \prod_{k < l} (\alpha^{(k)} - \alpha^{(l)})^2,$$

where $\alpha^{(k)}$ runs through the conjugates of α . Clearly

$$|\alpha^{(k)} - \alpha^{(l)}| \leq 2 \max(1, |\alpha^{(k)}|) \max(1, |\alpha^{(l)}|)$$

and thus the product is at most

$$2^{d_j(d_j-1)} \left(\prod_k \max(1, |\alpha^{(k)}|) \right)^{2(d_j-1)}.$$

The desired estimate now follows at once from (1).

The lemma gives a best possible estimate with respect to the dependence on d , as has recently been demonstrated by Masser and Wüstholz.

5. Liouville estimate

An elementary lower bound for a non-vanishing logarithmic form with integer coefficients can be obtained at once from simple manipulations of heights. The result corresponds to Liouville's inequality on rational approximations to algebraic numbers. We prove the following lemma.

Lemma 3. *Let $\alpha_1, \dots, \alpha_n$ be non-zero algebraic numbers, let $K = \mathbb{Q}(\alpha_1, \dots, \alpha_n)$ and let d be the degree of K . Then for any rational integers $y_1, \dots, y_n$ such that the logarithmic form*

$$A = y_1 \log \alpha_1 + \dots + y_n \log \alpha_n$$

does not vanish, we have

$$\log |A| \geq -|y_1|h(\alpha_1) - \dots - |y_n|h(\alpha_n) - d \log 2.$$

Proof. Let $\alpha = \alpha_1^{y_1} \dots \alpha_n^{y_n}$ and let the branch of $\log \alpha$ be defined such that $\log \alpha = A$. Put $\alpha' = \alpha - 1$. We first observe that

$$h(\alpha') \leq h(\alpha) + \max(\log |\alpha'|, 0) + (d-1) \log 2.$$

For if $v \nmid \infty$ then

$$\max(\log |\alpha'|_v, 0) \leq \log \max(|\alpha|_v, 1) = \max(\log |\alpha|_v, 0),$$

and if $v \mid \infty$ then

$$\max(\log |\alpha'|_v, 0) \leq d_v \log(1 + |\alpha|_v^{1/d_v}) \leq \max(\log |\alpha|_v, 0) + d_v \log 2.$$

Secondly we note that

$$\log |\alpha'| + h(\alpha') \geq \max(\log |\alpha'|, 0).$$

This is obvious if $\log |\alpha'| \geq 0$, and it holds if $\log |\alpha'| < 0$ since by definition

$$h(\alpha') = \sum_v \max(\log |\alpha'|_v, 0)$$

and this is at least

$$\sum_v \log |\alpha'|_v - \log |\alpha'| = -\log |\alpha'|$$

by the product formula.

Now from our estimate for $h(\alpha')$ above we have

$$\log |\alpha'| \geq -h(\alpha) - (d-1) \log 2.$$

But clearly from the basic properties of heights

$$h(\alpha) \leq |y_1|h(\alpha_1) + \dots + |y_n|h(\alpha_n).$$

Further, since

$$|\alpha - 1| \leq |\log \alpha| e^{|\log \alpha|},$$

we have

$$\log |\alpha'| \leq \log |A| + |A|.$$

The lemma follows at once for plainly one can assume that $|A| < \log 2$.

As an immediate consequence of Lemma 3 we have

$$\log |A| \geq -d(h'(\alpha_1) + \dots + h'(\alpha_n) + \log 2) \exp(h'(L)),$$

where $L = y_1 z_1 + \dots + y_n z_n$. This is clear on writing $L = yL'$, where y is the greatest common divisor of $y_1, \dots, y_n$, and noting that

$$h'(L) = h'(L') \geq \log \max(|y_j|/y);$$

we then apply the lemma to $A' = L'(\log \alpha_1, \dots, \log \alpha_n)$. On observing that

$$n \max(h'(\alpha_j)) + \log 2 \leq d^{n-1}(n+d) h'(\alpha_1) \dots h'(\alpha_n),$$

it follows that it suffices to establish our theorem under the assumption

$$h'(L) \geq \log C(n, d) - n \log d - \log(n+d).$$

Note that, for $d \geq 2$, we have $\log(n+d)$ at most $\log n + \log d$, whence our estimate for $h'(L)$ exceeds the asymptotic bound $\log(d \log d)$ as $d \rightarrow \infty$.

6. Logarithmic independence

We show here that it suffices to establish our theorem on the further assumption that $\log \alpha_1, \dots, \log \alpha_n$ are linearly independent over the rationals.

For suppose that they are linearly dependent. Then there is a smallest subset of $\log \alpha_1, \dots, \log \alpha_n$ with this property. Without loss of generality we can assume that it is given by $\log \alpha_1, \dots, \log \alpha_m$ and furthermore that $h'(\alpha_m) \geq h'(\alpha_j)$ for $j = 1, \dots, m$. By [25], Lemma 4.1, there exists a non-zero linear form $L' = y_1 z_1 + \dots + y_m z_m$ with relatively prime integer coefficients such that

$$L'(\log \alpha_1, \dots, \log \alpha_m) = 0$$

and

$$\exp(h'(L')) \leq (9md^3)^m h'(\alpha_1) \dots h'(\alpha_m).$$

This type of result was first obtained in the study of logarithmic forms (see [1]); a more elementary derivation based on the Geometry of Numbers was subsequently given by A. J. van der Poorten and J. H. Loxton and this was improved by M. Waldschmidt to give the form quoted here (a further small numerical improvement is given by Yu Kunrui [33]).

By our assumption on m , none of the y_j are zero. We eliminate z_m from

$$L = b_1 z_1 + \dots + b_n z_n$$

and get a new linear form

$$L^{(m)} = y_m L - b_m L'$$

with

$$h'(L^{(m)}) \leq h'(L) + h'(L') + \log 2.$$

We now assume that our theorem is valid for linear forms in at most $n - 1$ variables. Then for $A^{(m)} = L^{(m)}(\log \alpha_1, \dots, \log \alpha_n)$ we have

$$\log |A^{(m)}| \geq -C(n-1, d) h'(\alpha_1) \dots h'(\alpha_n) h'(L^{(m)})/h'(\alpha_m).$$

Since $h'(\alpha_m)$ is maximal, we have

$$h'(L') \leq m(\log(9md^3) + \log h'(\alpha_m)).$$

Hence, on recalling that $h'(\alpha_m) \geq 1/d$, we get

$$h'(L^{(m)})/h'(\alpha_m) \leq d(h'(L) + 3m \log(9md)).$$

Now by the assumption at the end of §5 it is clear that $h'(L) \geq \log(9md)$ whence

$$\log |A^{(m)}| \geq -(3m+1)dC(n-1, d) h'(\alpha_1) \dots h'(\alpha_n) h'(L).$$

Finally we note that

$$\log |A| = \log |A^{(m)}| - \log |y_m|,$$

and the above estimates plainly give

$$\log |y_m| \leq 3md^m h'(L) h'(\alpha_1) \dots h'(\alpha_m).$$

The required result now follows since

$$(3m+1)dC(n-1, d) + 3md^m \leq C(n, d).$$

7. Successive minima

We shall show in §9 that it suffices to establish a modified version of our theorem subject to the familiar Kummer condition. The approach is based as usual on the classical Kummer lemma but we develop here a new argument; it depends on the theory of successive minima in the Geometry of Numbers, and it seems to us to be conceptually well adapted not only with respect to the Kummer descent but also in connection with the multiplicity estimates that we shall introduce later.

Here we record a well known result due essentially to Mahler [15]. Let Ω be a lattice in $\mathbb{R}^n$ and let f be a distance function determined by a bounded convex body symmetric about the origin. We denote by $\lambda_1, \dots, \lambda_n$ the corresponding successive minima and by $u_1, \dots, u_n$ elements of Ω with $f(u_j) = \lambda_j$ for $1 \leq j \leq n$. Plainly the vectors $u_1, \dots, u_n$ generate a

sublattice of Ω but not necessarily Ω itself. In many circumstances, however, one needs a basis for Ω enjoying a similar property as $u_1, \dots, u_n$, and in this connection we have the following lemma.

Lemma 4. *There exists a basis $w_1, \dots, w_n$ for Ω such that $f(w_1) \leq \lambda_1$ and*

$$f(w_j) \leq \frac{1}{2} j \lambda_j$$

for $j \geq 2$.

The proof that follows is a modification of the exposition given in Gruber and Lekkerkerker [13] (see section 10.2) where the result is obtained without the factor $\frac{1}{2}$; for another proof and further references see J. W. S. Cassels, *An introduction to the Geometry of Numbers* (Springer, 1959), section V.4. We observe that in the linear subspace $\mathcal{L}_j$ ($1 \leq j \leq n$) generated by $u_1, \dots, u_j$ there is an element $w_j = \alpha_1 u_1 + \dots + \alpha_j u_j$ in Ω such that w_j has minimal non-zero distance to $\mathcal{L}_{j-1}$; here $\mathcal{L}_0$ is the origin. Then either $w_j = u_j$ has the property, in which case $f(w_j) = \lambda_j$, or we have $0 < |\alpha_j| \leq \frac{1}{2}$. In the latter case, by subtracting the linear combination $a_1 u_1 + \dots + a_{j-1} u_{j-1}$, where $a_1, \dots, a_{j-1}$ are integers nearest to $\alpha_1, \dots, \alpha_{j-1}$, we can suppose that $|\alpha_l| \leq \frac{1}{2}$ for $1 \leq l \leq j$. Thus, since $\lambda_1 \leq \dots \leq \lambda_n$, we have

$$f(w_j) \leq |\alpha_1| f(u_1) + \dots + |\alpha_j| f(u_j) \leq \frac{1}{2} j \lambda_j.$$

Furthermore $w_1, \dots, w_n$ form a basis for Ω . For if Ω' is the lattice generated by these vectors then any element in Ω can be expressed modulo Ω' as $c_1 w_1 + \dots + c_n w_n$ with $0 \leq c_j < 1$, and by the minimal property of the w_j it follows by induction that $c_1 = \dots = c_n = 0$. This establishes the result.

8. A problem of Lehmer

Here and in the next section it will be convenient to work with a semi-modified height $\bar{h}$ defined like the modified height h' but omitting the 1; that is for any α in K we put

$$\bar{h}(\alpha) = \frac{1}{d} \max(h(\alpha), |\log \alpha|).$$

Thus we have $\bar{h}(\alpha) = h'(\alpha)$ unless $\bar{h}$ takes a value less than $1/d$. We have also:

Lemma 5. *If $\alpha \neq 1$ then $h'(\alpha) < c' \bar{h}(\alpha)$, where $c' = 60 d \log(6d)$.*

The lemma is closely connected to a famous problem of Lehmer. He asked whether, for any $\varepsilon > 0$, there exists a non-zero algebraic integer, not a root of unity, such that $M(\alpha) < 1 + \varepsilon$, where $\log M(\alpha)$ denotes the right-hand side of (1) (see § 2). A well known result of Blanksby and Montgomery [7] states that

$$M(\alpha) > 1 + (52\delta \log(6\delta))^{-1}$$

for all non-zero algebraic integers α other than roots of unity and, for these α , Lemma 5 follows readily. For we have $\log M(\alpha) = (\delta/d) h(\alpha)$ and this gives $h(\alpha) > 1/c'$. If α is a root of unity then $\alpha^k = 1$ for some positive integer k such that $\phi(k) \leq d$, where ϕ is Euler's function; moreover, if $\alpha \neq 1$, then $k > 1$ and thus $|\log \alpha| \geq 2\pi/k$. Since $\phi(k) > \frac{1}{4}k/\log k$ for $k > 1$, we obtain $|\log \alpha| > 1/c'$; this proves the lemma when α is an algebraic integer and it holds trivially for non-integral elements of K since then $\alpha_0 \geq 2$, whence $M(\alpha) \geq 2$ and so $h(\alpha) \geq \log 2$.

We remark that a short, elegant argument of Dobrowolski [11] shows that when α is not a root of unity we have $h(\alpha) > (3d)^{-2}$. Furthermore there is a later paper of Dobrowolski [12], originating from a method of Stewart, that gives an improved lower bound for $h(\alpha)$ of order $(\log \log d/\log d)^3$. Thus since $k \ll d \log \log d$, we obtain

$$h'(\alpha) \ll (d \log \log d) \bar{h}(\alpha)$$

for all large d , where the implied constant is absolute and in fact about 10^3 . Also in this context, Smyth [22] has proved that $M(\alpha) > 1 \cdot 324 \dots$ for all α , not 0 or 1, provided that the minimal polynomial $p(x)$ for α is not reciprocal, that is if $x^{\delta}p(1/x) \neq p(x)$.

9. Kummer condition

We shall say that elements $\eta_1, \dots, \eta_m$ of an algebraic number field K satisfy the Kummer condition with respect to K if the field $K(\eta_1^{1/2}, \dots, \eta_m^{1/2})$ has degree 2^m over K . We remark that although we are using here only the prime $p = 2$, the subsequent theory holds similarly for any prime p provided that K contains the p th roots of unity.

Let now $\alpha_1, \dots, \alpha_n$ and K be as indicated in §1. Our aim in this section is to replace $\alpha_1, \dots, \alpha_n$ by new algebraic numbers $\alpha'_1, \dots, \alpha'_n$ in K which satisfy the Kummer condition and also admit a good estimate for $h'(\alpha'_1) \dots h'(\alpha'_n)$ in terms of $h'(\alpha_1) \dots h'(\alpha_n)$. We do this in two steps; the first is based on the classical Kummer lemma as given in Baker and Stark [5] and the second on the theory of successive minima.

We begin by establishing inductively that for each $v = 0, 1, \dots$ there exists a set of non-zero algebraic numbers $\alpha_1^{(v)}, \dots, \alpha_n^{(v)}$ in K such that for some non-negative integers $v_1, \dots, v_n$ with $v_1 + \dots + v_n \leq v$ we have

$$(3) \quad 2^v \log \alpha_j^{(v)} = \sum_{i=1}^j m_{ij} \log \alpha_i \quad (1 \leq j \leq n),$$

where the m_{ij} are integers with $|m_{ij}| \leq 2^{v-1}$ ($i < j$) and $m_{jj} = 2^{v-v_j}$. The relations (3) hold for some determinations of $\log \alpha_j^{(v)}$ and these will be used in our definition of the heights. By construction, the $\alpha_j^{(v)}$ will satisfy the Kummer condition as soon as the equation $v_1 + \dots + v_n = v$ fails to hold for $v+1$, and we shall prove shortly as a consequence of §6 that the latter must indeed occur for some v .

For $v = 0$ we simply take $\alpha_j^{(v)} = \alpha_j$ ($1 \leq j \leq n$). Now suppose that $\alpha_1^{(v)}, \dots, \alpha_n^{(v)}$ have been constructed to satisfy the inductive hypothesis. Then either the Kummer condition with respect to this set holds or it does not. In the former case we put $\alpha_j^{(v+1)} = \alpha_j^{(v)}$ ($1 \leq j \leq n$) and take the same values of $v_1, \dots, v_n$. In the latter case we appeal to Lemma 3 of [5]; this gives

$$(4) \quad \log \alpha_k^{(v)} = m_1 \log \alpha_1^{(v)} + \dots + m_{k-1} \log \alpha_{k-1}^{(v)} + 2 \log \gamma$$

for some k and some non-zero element γ of K with $m_i = 0$ or 1 . Here we are using the fact that the multiplicative equation determines the value of $\log \gamma^2$ and that, by replacing γ by $-\gamma$ if necessary, we can ensure that $\log \gamma^2 = 2 \log \gamma$; the analogue for an odd prime p , namely $\log \gamma^p = p \log \gamma$, leads to the supposition about the p th roots of unity. From (3) and (4) we see that

$$2^{v+1} \log \gamma = \sum_{i=1}^k m'_{ik} \log \alpha_i$$

for some integers m'_{ik} with $m'_{kk} = m_{kk}$. Now write $m'_{ik} = r_i - 2^{v+1} s_i$ for $i \neq k$, where r_i, s_i are integers with $|r_i| \leq 2^v$. Then define

$$\alpha_k^{(v+1)} = \alpha_1^{s_1} \dots \alpha_{k-1}^{s_{k-1}} \gamma$$

and take $\alpha_j^{(v+1)}$ as $\alpha_j^{(v)}$ for $j \neq k$. This gives (3) with v replaced by $v+1$, with $m_{ik} = r_i$ ($i \neq k$), with $m_{kk} = m'_{kk}$ and with the remaining m_{ij} replaced by $2m_{ij}$. Finally we replace v_k by $v_k + 1$ leaving the other v_j unchanged; then $m'_{kk} = 2^{(v+1)-(v_k+1)}$, as required.

It is clear from the properties of the heights that, for $v_j \geq 1$, (3) gives

$$h(\alpha_j^{(v)}) \leq \frac{1}{2} (h'(\alpha_1) + \dots + h'(\alpha_j)).$$

For $v_j = 0$ the construction shows that $m_{ij} = 0$ ($1 \leq i < j$) and thus $\alpha_j^{(v)} = \alpha_j$. Hence, if we introduce an ordering, say $h'(\alpha_1) \leq \dots \leq h'(\alpha_n)$, as we may without loss of generality, then we obtain

$$h'(\alpha_j^{(v)}) \leq \frac{1}{2} j h'(\alpha_j) \quad (2 \leq j \leq n)$$

and $h'(\alpha_1^{(v)}) \leq h'(\alpha_1)$. It follows that

$$h'(\alpha_1^{(v)}) \dots h'(\alpha_n^{(v)}) \leq (n!/2^{n-1}) h'(\alpha_1) \dots h'(\alpha_n).$$

We now appeal to the Geometry of Numbers. Consider the distance function

$$F(x) = |x_1| h'(\alpha_1) + \dots + |x_n| h'(\alpha_n)$$

and the convex body $F(x) < 1$ with volume

$$V(F) = (2^n/n!) (h'(\alpha_1) \dots h'(\alpha_n))^{-1}.$$

Let Ω be the lattice in $\mathbb{R}^n$ generated by the vectors $v_1, \dots, v_n$, where

$$v_j = 2^{-v}(m_{1j}, \dots, m_{jj}, 0, \dots, 0) \quad (1 \leq j \leq n).$$

The lattice has determinant $\Delta = 2^{-(v_1 + \dots + v_n)}$. By Minkowski's theorem, the successive minima $\lambda_1, \dots, \lambda_n$ of $F(x) < 1$ satisfy

$$\lambda_1 \dots \lambda_n \leq 2^n \Delta (V(F))^{-1}.$$

Further, by Lemma 4, there exists a basis $w_1, \dots, w_n$ for Ω such that $F(w_j) = \mu_j$, where

$$\mu_1 \dots \mu_n \leq (n!/2^{n-1}) \lambda_1 \dots \lambda_n.$$

We write

$$w_j = 2^{-v}(w_{1j}, \dots, w_{nj}) = u_{1j}v_1 + \dots + u_{nj}v_n;$$

then the u_{ij} are integers and we have

$$w_{ij} = \sum_{l=1}^n m_{il} u_{lj}.$$

This gives

$$2^{-v} \sum_{i=1}^n w_{ij} \log \alpha_i = \sum_{l=1}^n u_{lj} \log \alpha_l^{(v)}.$$

We can express the right hand side as $\log \alpha_j''$ for some element α_j'' of K . Then, since $F(w_j) = \mu_j$, we obtain $\bar{h}(\alpha_j'') \leq \mu_j$. Hence $\bar{h}(\alpha_1'') \dots \bar{h}(\alpha_n'')$ is at most

$$2^{-(v_1 + \dots + v_n) - (n-1)} (n!)^2 h'(\alpha_1) \dots h'(\alpha_n).$$

Note that if $\alpha_1^{(v)}, \dots, \alpha_n^{(v)}$ satisfy the Kummer condition then so do $\alpha_1'', \dots, \alpha_n''$; for, by construction, $w_1, \dots, w_n$ is a basis for Ω whence the u_{ij} have determinant ± 1 and thus the field generated by the square-roots of $\alpha_1^{(v)}, \dots, \alpha_n^{(v)}$ over K is the same as that generated by the square-roots of $\alpha_1'', \dots, \alpha_n''$ over K .

Now, by Lemma 5, if $\alpha \neq 1$ then we have $\bar{h}(\alpha) > (c'd)^{-1}$. From § 6 we know that $\log \alpha_1, \dots, \log \alpha_n$ are linearly independent over the rationals and, since again $w_1, \dots, w_n$ is a basis, we see that $\alpha_j'' \neq 1$ ($1 \leq j \leq n$). Thus we obtain

$$\bar{h}(\alpha_1'') \dots \bar{h}(\alpha_n'') > (c'd)^{-n}.$$

It follows that $v_1 + \dots + v_n$ is bounded; let its maximal value be v . Then, as indicated above, this implies that $\alpha_1^{(v)}, \dots, \alpha_n^{(v)}$ satisfy the Kummer condition.

We put $c = c''n!$ and define $\alpha'_1, \dots, \alpha'_n$ as $\alpha_1'', \dots, \alpha_n''$ if $2^v > c$ and as $\alpha_1^{(v)}, \dots, \alpha_n^{(v)}$ if $2^v \leq c$. Then, in either case, $\alpha'_1, \dots, \alpha'_n$ satisfy the Kummer condition. Moreover we have

$$\log \alpha'_j = 2^{-v} L_j(\log \alpha_1, \dots, \log \alpha_n),$$

where $L_1, \dots, L_n$ are independent linear forms in $z_1, \dots, z_n$ with integer coefficients; indeed L_j is given by

$$\sum_{i=1}^n w_{ij} z_i \quad \text{or} \quad \sum_{i=1}^j m_{ij} z_i.$$

Now we have $h'(\alpha_j) \leq \sigma_j (1 \leq j \leq n)$, where σ_j is defined as $c' \mu_j$ if $2^v > c$ and as $\frac{1}{2} j h'(\alpha_j)$ for $j > 1$, $h'(\alpha_1)$ for $j = 1$ if $2^v \leq c$. Then $\sigma_1 \dots \sigma_n$ is at most

$$(n!/2^{n-1}) \min(c/2^v, 1) h'(\alpha_1) \dots h'(\alpha_n).$$

Further, since $F(w_j) = \mu_j$ and $h'(\alpha_1) \leq \dots \leq h'(\alpha_n)$, we see that, in either case,

$$\sum_{i=1}^n |\partial L_j / \partial z_i| h'(\alpha_i) \leq 2^v \sigma_j \quad (1 \leq j \leq n).$$

10. Multiplicity estimates

In this section we shall give a summary of the multiplicity estimates proved in [31]. Our aim is to state the main result established there in the form needed in our present work.

Let $\mathcal{L}$ be a linear form $B_1 Z_1 + \dots + B_r Z_r$ with rationals $B_1, \dots, B_r$ and assume that $B_r \neq 0$. For independent variables $Y_0, \dots, Y_r$ we consider the polynomial ring $\mathbb{C}[Y_0, \dots, Y_r]$ and we introduce the differential operators

$$\partial_0 = \frac{\partial}{\partial Y_0}, \quad \partial_j = B_r Y_j \frac{\partial}{\partial Y_j} - B_j Y_r \frac{\partial}{\partial Y_r} \quad (1 \leq j < r),$$

which are linearly independent derivations of the ring. Our proposition concerns a non-zero polynomial $\mathcal{P}(Y_0, \dots, Y_r)$ defined over $\mathbb{C}$ with degree at most $\mathcal{D}_j$ in Y_j for $j = 0, 1, \dots, r$.

Let $\mathcal{S}_0 \geq \dots \geq \mathcal{S}_r \geq 0$, let $\mathcal{T}_0 \geq \dots \geq \mathcal{T}_r \geq 0$ be integers and suppose that $\mathcal{S}_0 + \dots + \mathcal{S}_r$ and $\mathcal{T}_0 + \dots + \mathcal{T}_r$ are bounded above by $\mathcal{S}$ and $\mathcal{T}$, respectively. Suppose further that

$$(5) \quad \mathcal{S}_m \binom{\mathcal{T}_m + m + \delta_{m,r}}{m + \delta_{m,r}} \geq (m+1)! \mathcal{D}_0^{m_0} \dots \mathcal{D}_r^{m_r}$$

for $m = 0, \dots, r$ and for all $m_0, \dots, m_r$, 0 or 1, where $m_0 + \dots + m_r = m+1$ and $\delta_{m,r}$ is the reversed Kronecker delta, that is $\delta_{m,r} = 0$ for $m = r$, $\delta_{m,r} = 1$ otherwise. (Here, by convention, we have $x^0 = 1$ for all x including $x = 0$.)

Let now $\theta_1, \dots, \theta_r$ be algebraic numbers and assume that $\log \theta_1, \dots, \log \theta_r$ are linearly independent over the rationals with some fixed determinations of the logarithms. We put

$$A' = B_1 \log \theta_1 + \dots + B_r \log \theta_r$$

and assume that $|A'| < \pi/\mathcal{S}$. We further assume that $\mathcal{D}_j \leq \mathcal{T}_0$ for $j = 1, \dots, r$ and $\mathcal{T}_r < \mathcal{D}_0$. Then the following holds.

Proposition. *Suppose that for all non-negative integers $t_0, \dots, t_{r-1}$ with*

$$t_0 + \dots + t_{r-1} \leq \mathcal{T}$$

we have

$$\partial_0^{t_0} \dots \partial_{r-1}^{t_{r-1}} \mathcal{P}(s, \theta_1^s, \dots, \theta_r^s) = 0$$

for integers s with $0 \leq s \leq \mathcal{T}$. Then there exists an integer q with $1 \leq q < r$ having the following property. For any positive real numbers $a_1, \dots, a_r$ there is a set of primitive linear forms $\mathcal{L}_1, \dots, \mathcal{L}_q$ in $Z_1, \dots, Z_r$ with integer coefficients such that $\mathcal{L}$ is in the module generated by $\mathcal{L}_1, \dots, \mathcal{L}_q$ over the rationals and, on defining

$$\mathcal{R}_j = \sum_{i=1}^r (a_i |\partial \mathcal{L}_j / \partial Z_i|) \quad (1 \leq j \leq q)$$

and $\mathcal{C}(q) = 2^{1-q}(q!)^2(rq)^q$, we have

$$(6) \quad \mathcal{R}_1 \dots \mathcal{R}_q \mathcal{L}_{q-1} \left(\frac{\mathcal{T}_{q-1} + q - 1}{q - 1} \right) \leq \mathcal{C}(q) \max(\mathcal{D}_0^{m_0}(a_1 \mathcal{D}_1)^{m_1} \dots (a_r \mathcal{D}_r)^{m_r}),$$

where the maximum is over all $m_0, \dots, m_r$, 0 or 1, with $m_0 + \dots + m_r = q$.

Here, as usual, a set of linear forms $\mathcal{L}_1, \dots, \mathcal{L}_q$ in $Z_1, \dots, Z_r$ with integer coefficients is said to be primitive if the minors of order q of the matrix of coefficients are relatively prime. This implies in particular that the rank of the set is q . It is well known that a set $\mathcal{L}_1, \dots, \mathcal{L}_q$ of primitive linear forms can be extended to a basis $\mathcal{L}_1, \dots, \mathcal{L}_r$ of the module generated by $Z_1, \dots, Z_r$ over the integers. Thus, as in § 9, we see that if $\theta_1, \dots, \theta_r$ satisfy the Kummer condition with respect to K then so do the numbers $\theta'_1, \dots, \theta'_r$ defined by

$$\log \theta'_j = \mathcal{L}_j(\log \theta_1, \dots, \log \theta_r).$$

It follows a fortiori that $\theta'_1, \dots, \theta'_q$ also satisfy the Kummer condition with respect to K and this is the property we shall use later.

The basic Theorem 1.1 in [31], I, is a result on the commutative algebraic group $G = G_a \times G'_m$ where G_a denotes the additive and G'_m the multiplicative group variety. We shall now indicate briefly how to derive our proposition. Since $\mathcal{P}$ is a non-zero polynomial, Theorem 1.1 implies that there exists a connected algebraic subgroup H of G such that the property (i) or (ii) stated there holds. Further, H is non-trivial since it has rank at most n and it is also proper by construction. Now any algebraic subgroup of G can be written as a product of an algebraic subgroup of G_a and an algebraic subgroup of G'_m and so it must have the form $G_a \times H$ or $O \times H$ for some subgroup H of G'_m , where O is trivial. If $H = G_a \times H$ then H is plainly proper and if $H = O \times H$ then H is plainly non-trivial. In fact assuming, as we shall verify in a moment, that property (ii) can be excluded, we see that H is always non-trivial and proper. Indeed if $H = O \times H$ then the condition on the Lie algebra in (i) implies that H is proper. If $H = G_a \times H$ and H were trivial then it would have rank n and one of the partial degrees of H would be 1, the remainder 0; as a consequence we would have, by (i),

$$\mathcal{S}_{r-1} \binom{\mathcal{T}_{r-1} + r - 1}{r - 1} \leq r! \mathcal{D}_1 \dots \mathcal{D}_r$$

contrary to (5) with $m = r$, namely

$$\mathcal{S}_r \binom{\mathcal{T}_r + r}{r} \geq (r + 1)! \mathcal{D}_0 \dots \mathcal{D}_r,$$

by virtue of the hypotheses $\mathcal{S}_r \leq \mathcal{S}_{r-1}$, $\mathcal{T}_r \leq \mathcal{T}_{r-1}$ and $\mathcal{T}_r < \mathcal{D}_0$.

We note now that $\mathcal{H}$ can be defined in the Lie algebra of G_m^r by linear forms in $Z_1, \dots, Z_r$ with integer coefficients. The set of these forms defines a free module $\mathcal{Z}$ over the integers whose rank is equal to the codimension ϱ of $\mathcal{H}$ in G_m^r . Hence, since $\mathcal{H}$ is non-trivial and proper, we have $1 \leq \varrho < r$. We identify $\mathcal{Z}$ with a submodule $\mathcal{Z}'$ of $\mathbb{Z}^r$ by attaching to a linear form its vector of coefficients. In § 2 of [31], II, the volume $\mathcal{V}$ of $\mathcal{Z}'$ is defined in terms of $a_1, \dots, a_r$ and the minors of the matrix formed by a set of basis vectors; the absolute values of the minors are in fact the partial degrees of $\mathcal{H}$ and bounds for these can be calculated from the partial degrees of H given in Theorem 1.1. Thus we see that if (i) holds then

$$\mathcal{V} \mathcal{S}_{\varrho-1} \binom{\mathcal{T}_{\varrho-1} + \varrho - 1}{\varrho - 1} \leq \varrho! \max(\mathcal{D}_0^{m_0} (a_1 \mathcal{D}_1)^{m_1} \dots (a_r \mathcal{D}_r)^{m_r}),$$

where the maximum is over all $m_0, \dots, m_r$, 0 or 1, with $m_0 + \dots + m_r = \varrho$. Now by Lemma 2.1 of [31], II, there exists a set of linear forms $\mathcal{L}'_1, \dots, \mathcal{L}'_{\varrho}$ corresponding to a set of generators of $\mathcal{Z}'$ such that

$$\mathcal{R}'_1 \dots \mathcal{R}'_{\varrho} \leq (r\varrho)^{\varrho} \mathcal{V},$$

where $\mathcal{R}'$ is defined like $\mathcal{R}_j$ in the proposition but with $\mathcal{L}'_j$ instead of $\mathcal{L}_j$. In order to obtain primitive linear forms we need a basis rather than a set of generators. Accordingly we replace the application of Minkowski's theorem by an appeal to our Lemma 4. This gives linear forms $\mathcal{L}_1, \dots, \mathcal{L}_{\varrho}$ such that

$$\mathcal{R}_1 \dots \mathcal{R}_{\varrho} \leq 2^{1-\varrho} \varrho! (r\varrho)^{\varrho} \mathcal{V}$$

and the estimate (6) in our proposition follows at once. The assertion that $\mathcal{L}$ is in the module generated by $\mathcal{L}_1, \dots, \mathcal{L}_{\varrho}$ over $\mathbb{Z}$ is equivalent to the property of the Lie algebra in (i) by duality.

It remains to exclude the possibility (ii) in Theorem 1.1. We proceed as above to obtain a free module $\mathcal{Z}$ which defines the Lie algebra of $\mathcal{H}$. Then (ii) implies that the point $(s, \theta_1^s, \dots, \theta_r^s)$ is in $G_a \times \mathcal{H}$ for some positive integer $s \leq \mathcal{S}$. (Note that the statement of (ii) in Theorem 1.1 erroneously refers only to the case $s = 1$; our corrected version is clear from the proof.) Hence $(\theta_1^s, \dots, \theta_r^s)$ is in $\mathcal{H}$ and so the value of any linear form in $\mathcal{Z}$ at $Z_j = s \log \theta_j$ ($1 \leq j \leq r$) is an integer multiple of $2\pi i$. If we had $\varrho \geq 2$ then elimination of πi would give a linear dependence relation for $\log \theta_1, \dots, \log \theta_r$ contrary to hypothesis. Thus we must have $\varrho = 1$. Now if $\mathcal{L}$ were in $\mathcal{Z}$ then sA' would be a non-zero integer multiple of πi whence $\mathcal{S}|A'| \geq \pi$ again contrary to hypothesis. Hence $\mathcal{L}$ is not in $\mathcal{Z}$. In this case the partial degrees

of $\mathcal{H}$ are respectively bounded above by $(\mathcal{T}_0 + 1)^{-1} \mathcal{D}_j$ for $j = 1, \dots, r$; the assertion is obvious from the proof of (5.8) of [31], I. We obtain accordingly $\mathcal{T}_0 + 1 \leq \max \mathcal{D}_j$ which contradicts another hypothesis.

We remark that the assumptions on $\mathcal{A}'$ and $\mathcal{T}_0$ would not be needed if $\theta_1, \dots, \theta_r$ were multiplicatively independent. This will correspond to the multiplicative independence of $\alpha_1, \dots, \alpha_n$, a condition that can in fact be attained in the same way as the logarithmic independence was established in § 6; but there would be some loss in the expression for $C(n, d)$. The assumptions will be trivially satisfied in the subsequent work.

We remark also that, since (6) is homogeneous with respect to $a_1, \dots, a_r$, there would be no loss of generality in assuming that $a_1, \dots, a_r$ are all ≥ 1 . This is in fact in the general hypothesis of [31] but it was used there only to obtain (ii) in Lemma 3.1 of [31], II, which is not needed here.

The proposition will be applied to a polynomial $\mathcal{P}(Y_0, \dots, Y_r)$ as above but with the differential operators $\partial_1, \dots, \partial_{r-1}$ replaced by a new set as follows. Let L be the linear form $b_1 z_1 + \dots + b_n z_n$ indicated in § 1 and assume that $b_n \neq 0$. In the next section we shall introduce linear forms $L_1, \dots, L_r$ in $z_1, \dots, z_n$ with integer coefficients such that $L_1, \dots, L_r$ are linearly independent over the rationals and satisfy

$$L = B_1 L_1 + \dots + B_r L_r$$

for some rationals $B_1, \dots, B_r$ with $B_r \neq 0$. We write

$$\partial_j^* = (1/B_r) \sum_{i=1}^{r-1} (b_n \partial L_i / \partial z_j - b_j \partial L_i / \partial z_n) \partial_i \quad (1 \leq j < n).$$

Here the matrix of coefficients of the ∂_i has rank $r - 1$; for if the expressions on the right vanish when rationals B'_i are substituted for ∂_i ($1 \leq i < r$) then

$$b_n (B'_1 L_1 + \dots + B'_{r-1} L_{r-1}) = b'_n L,$$

where

$$b'_n = \sum_{i=1}^{r-1} B'_i \partial L_i / \partial z_n,$$

whence the linear independence of $L_1, \dots, L_r$ implies that all the B'_i are 0. It follows that the set $\partial_1^*, \dots, \partial_{n-1}^*$ contains a subset of $r - 1$ linearly independent differential operators and we shall suppose, as we may without loss of generality, that it is given by $\partial_1^*, \dots, \partial_{r-1}^*$. Then the proposition holds with these in place of $\partial_1, \dots, \partial_{r-1}$. Note that the asterisked operators can be written in the form

$$\partial_j^* = \sum_{i=1}^r (b_n \partial L_i / \partial z_j - b_j \partial L_i / \partial z_n) Y_i \partial / \partial Y_i.$$

11. Inductive hypothesis

Let L be the linear form $b_1 z_1 + \dots + b_n z_n$ indicated in § 1. We shall assume, as we may without loss of generality, that $b_1, \dots, b_n$ are relatively prime, that $b_n \neq 0$ and that $h'(\alpha_j) \leq h'(\alpha_n)$ for all j . Our basic hypothesis is that there exists a set of linear forms $L_1, \dots, L_r$ in $z_1, \dots, z_n$ with integer coefficients having the following properties. First, $L_1, \dots, L_r$ are linearly independent and L is in the module generated by $L_1, \dots, L_r$ over the rationals. Secondly, on defining v as in § 9, the algebraic numbers $\alpha'_1, \dots, \alpha'_r$ given by

$$\log \alpha'_j = 2^{-v} L_j(\log \alpha_1, \dots, \log \alpha_n) \quad (1 \leq j \leq r)$$

are in K and satisfy the Kummer condition with respect to K . Thirdly we have $h'(\alpha'_j) \leq \sigma_j$ ($1 \leq j \leq r$) and

$$\sum_{i=1}^n |\partial L_j / \partial z_i| h'(\alpha_i) \leq 2^v \sigma_j \quad (1 \leq j \leq r)$$

for some positive real numbers $\sigma_1, \dots, \sigma_r$ satisfying

$$(7) \quad \sigma_1 \dots \sigma_r \leq \kappa(r) h'(\alpha_1) \dots h'(\alpha_n),$$

where

$$\kappa(r) = (64nd)^{n-r} (n!/2^{n-1}) \min(c/2^v, 1).$$

The construction of § 9 establishes the existence of linear forms as above for $r = n$. We now take r as the least integer for which such a set exists. Then we can assume that $r \geq 2$. For if $r = 1$ then $qL = L_1$ for some positive integer q whence A , as defined in our Theorem, is given by $(2^v/q) \log \alpha'_1$; but by Lemma 3 we see that

$$\log |\log \alpha'_1| \geq -d\sigma_1 - d \log 2$$

and, on noting that q divides the coefficients of L_1 and that $h'(\alpha_i) \geq 1/d$, we obtain $q \leq 2^v d\sigma_1$, whence $\log |A| \geq -3d^2\sigma_1$ and our Theorem follows in this case since we have

$$\sigma_1 \leq \kappa(1) h'(\alpha_1) \dots h'(\alpha_n), \quad 3d^2\kappa(1) \leq C(n, d).$$

Assuming now the basic hypothesis stated above and supposing further that our Theorem is not valid, we proceed to establish the existence of a polynomial $\mathscr{P}$ as in the proposition of § 10 with $\theta_j = \alpha'_j$. Thus we shall conclude that there exists an integer q with $1 \leq q < r$ and linear forms $\mathscr{L}_1, \dots, \mathscr{L}_q$ as described there. Then, taking $\theta'_1, \dots, \theta'_q$ instead of $\alpha'_1, \dots, \alpha'_r$, this will imply that the hypothesis is satisfied with r replaced by q whence the minimal choice of r will give the required contradiction. We note that on writing

$$\kappa'(r) = (9/4)(n+1)r^{r+1}(64d)^{r+2} \log(2rd) \max(2^v/c, 1)$$

we have, by (7),

$$\kappa'(r) \sigma_1 \dots \sigma_r \leq C(n, d) h'(\alpha_1) \dots h'(\alpha_n),$$

and therefore the supposition gives

$$(8) \quad \log |A| \leq -\kappa'(r) \sigma_1 \dots \sigma_r h'(L).$$

12. The delta functions

A delta function was first introduced into the theory of logarithmic forms by Feldman in order to obtain a best possible estimate with respect to the height of L . The topic was subsequently developed by Baker in two directions leading to the refined delta functions Π and Θ defined below.

Let k be any positive integer and z be a complex variable. Our basic function is defined by

$$\Delta(z; k) = (z + 1) \dots (z + k)/k!.$$

We write $\Delta(z; 0) = 1$. Plainly $\Delta(z; k)$ is an integer when z is an integer. For non-negative integers $t_1, \dots, t_{r-1}$ and complex variables $z_1, \dots, z_{r-1}$ we define

$$\Pi(z_1, \dots, z_{r-1}; t_1, \dots, t_{r-1}) = \prod_{j=1}^{r-1} \Delta(z_j; t_j).$$

Then the functions Π with $t_1 + \dots + t_{r-1} \leq T$ form a basis for the vector space of polynomials in $z_1, \dots, z_{r-1}$ of total degree at most T . Further we have, for $T > 0$,

$$|\Pi| \leq e^T (1 + (|z_1| + \dots + |z_{r-1}|)/T)^T.$$

This is readily verified for $r = 2$, on noting that $k! \geq k^k e^{-k+1}$, and the general result follows by virtue of the inequality of the arithmetic and geometric means.

Suppose now that l and m are non-negative integers. We put

$$\Theta(z; k, l, m) = \frac{1}{m!} \left(\frac{d}{dz} \right)^m (\Delta(z; k))^l.$$

From Lemma 1.6 of Yu [33] we have

$$|\Theta| \leq (e(1 + |z|/k))^{kl}.$$

Further, for any positive integer q and any x for which qx is an integer the expression $q^{2kl} (u(k))^m \Theta(x; k, l, m)$ is an integer, where $u(k)$ denote the lowest common multiple of $1, \dots, k$; see Tijdeman [24] or Baker [3] (the lemma refers there to the case $x > 0$ but clearly remains valid for all x). Furthermore, by Yu [33], we have $u(k) \leq 3^k$. Note here that the prime-number theorem implies that $\log u(k) \sim k$ as $k \rightarrow \infty$ and so the constant 3 cannot be reduced below e , the best possible value.

Finally we recall that, by Lemma 2 of Chapter 3 of Baker [4], the polynomials $(\Delta(z + j; k))^l$ with $0 \leq j \leq k - 1$ and $l = 1, 2, \dots$ are linearly independent.

13. The auxiliary polynomials

Let $\mathcal{O}_K$ be the ring of integers of the field K generated by $\alpha_1, \dots, \alpha_n$ over $\mathcal{Q}$. Further let $Y_0, \dots, Y_r$ be independent variables. We shall construct a polynomial $P = P(Y_0, \dots, Y_r)$ of the form

$$P = \sum_{\lambda_{-1}=0}^{D_{-1}} \dots \sum_{\lambda_r=0}^{D_r} p(\lambda) (\Delta(Y_0 + \lambda_{-1}; h))^{\lambda_0+1} Y_1^{\lambda_1} \dots Y_r^{\lambda_r}$$

with coefficients $p(\lambda) = p(\lambda_{-1}, \dots, \lambda_r)$ in $\mathcal{O}_K$.

Let now L and $L_1, \dots, L_r$ be the linear forms indicated in § 11. Further denote by $\partial_1^*, \dots, \partial_{n-1}^*$ the differential operators specified in § 10 and put $\partial_0^* = \partial/\partial Y_0$. Then we have

$$\partial_j^* Y_1^{\lambda_1} \dots Y_r^{\lambda_r} = \gamma_j Y_1^{\lambda_1} \dots Y_r^{\lambda_r} \quad (1 \leq j \leq n),$$

where

$$\gamma_j = \sum_{i=1}^r (b_n \partial L_i / \partial z_j - b_j \partial L_i / \partial z_n) \lambda_i.$$

For any set t of non-negative integers $t_0, \dots, t_{r-1}$ we put

$$\begin{aligned} \Pi(t) &= \Pi(\gamma_1, \dots, \gamma_{r-1}; t_1, \dots, t_{r-1}), \\ \Theta(Y_0; t) &= (u(h))^{t_0} \Theta(Y_0 + \lambda_{-1}; h, \lambda_0 + 1, t_0). \end{aligned}$$

We now introduce further polynomials $Q(t) = Q(Y_0, \dots, Y_r; t)$ by

$$Q(t) = \sum_{\lambda_{-1}=0}^{D_{-1}} \dots \sum_{\lambda_r=0}^{D_r} p(\lambda) \Pi(t) \Theta(Y_0; t) Y_1^{\lambda_1} \dots Y_r^{\lambda_r}.$$

Then the vector space generated over K by the $Q(t)$ is the same as that generated by the polynomials $\partial^t P$ where $\partial^t = \partial_0^{t_0} \dots \partial_{r-1}^{t_{r-1}}$.

In order to define the quantities $D_{-1}, \dots, D_r$ we first put

$$D = 2r'(32d)^{r+1} \log(2rd) \sigma_1 \dots \sigma_r.$$

Then we write

$$D_0 = [rD/2 \log(2rd)], \quad D_j = [D/rd\sigma_j] \quad (1 \leq j \leq r).$$

Further we write $D_{-1} = h - 1$, where

$$h = [h'(L) + v \log 2].$$

We proceed to determine the $p(\lambda)$, not all 0, by Lemma 1 such that

$$(9) \quad Q(s, \alpha_1^s, \dots, \alpha_r^s; t) = 0$$

for all integers s with $|s| \leq S$ and all sets t of non-negative integers $t_0, \dots, t_{r-1}$ with $t_0 + \dots + t_{r-1} \leq T$. Here S and T are defined by

$$S = 16rdh, \quad T = [11 \cdot 75rD].$$

Then by (8) we have

$$(10) \quad \log |A| \leq -9.2' SD.$$

This follows from the estimate

$$h \leq (n+1)h'(L) \max(2^v/c, 1).$$

To verify the latter we recall that $c = c''n!$, where c' is defined in Lemma 5, whence, by the assumption at the end of § 5, we obtain $\log c < nh'(L)$; the desired inequality is now a consequence of the fact that

$$v \log 2 \leq (\log c) \max(2^v/c, 1).$$

We shall need height estimates for $\Pi(t)$, $\Theta(s; t)$ and $\alpha_1^{s\lambda_1} \dots \alpha_r^{s\lambda_r}$. To deal with $\Pi(t)$, we note that γ_j is an integer and, since $h'(\alpha_j) \geq 1/d$, we deduce from § 11 that

$$|\gamma_j| \leq e^{h'(L)2^v} \sum_{i=1}^r d\sigma_i \lambda_i \leq e^{h+1} D.$$

Thus we have $\Pi(t)$ an integer such that

$$|\Pi(t)| \leq e^{T'} (1 + (r-1)e^{h+1}D/T')^{T'}$$

for $T' > 0$, where $T' = t_1 + \dots + t_{r-1}$. The expression on the right is at most

$$e^{hT'} (1 + e^2 r D/T')^{T'}$$

and the latter factor can be replaced by $(1 + e^2 r D/T)^T$ by monotonicity. Thus the definition of T shows that

$$|\Pi(t)| \leq e^{hT'} (1 + e^2/11 \cdot 7)^T \leq e^{hT'} (1 \cdot 7)^T.$$

By § 11 we see that $\Theta(s; t)$ is an integer with absolute value at most

$$3^{ht_0} (e(2 + S/h))^{h(D_0+1)}.$$

Further, using the fact that $1 + \log(2 + 8x)$ does not exceed $3 \cdot 27 \log x$ for $x \geq 4$, we obtain

$$(1 + \log(2 + S/h))(D_0 + 1) \leq 1 \cdot 64 r D \leq 0 \cdot 14 T$$

whence

$$\log |\Theta(s; t)| \leq ht_0 \log 3 + (0 \cdot 14) h T.$$

Furthermore from § 5 we have

$$h'(L) \geq \log C(2, 1) - \log 3 > 19$$

and thus $h \geq 19$. We conclude therefore that

$$\log |\Pi(t) \Theta(s; t)| \leq (0 \cdot 14 + \log 3) h T + T \log(1 \cdot 7) \leq 1 \cdot 27 h T.$$

For the factor involving the α'_j we note that by §11 we have $h'(\alpha'_j) \leq \sigma_j$ whence $h(\alpha'_j) \leq d\sigma_j$. Now by the basic properties of heights we see that

$$h(\alpha_1^{\lambda_1 s} \dots \alpha_r^{\lambda_r s}) \leq |s| \lambda_1 h(\alpha_1) + \dots + |s| \lambda_r h(\alpha_r)$$

and the expression on the right is at most

$$|s| d \sum_{j=1}^r D_j \sigma_j \leq |s| D.$$

We now apply Lemma 1 with K replaced by $K' = \mathbb{Q}(\alpha'_1, \dots, \alpha'_r)$ and with L_i given by the left hand side of (9). Let d' and $\mathscr{D}'$ be the degree and discriminant of K' , respectively. Then the lemma gives a non-trivial solution in $\mathcal{O}_{K'}$ with

$$h_0(x) \leq \frac{1}{2d'} \log |\mathscr{D}'| + \frac{1}{N-M} \sum_{i=1}^M \left(\frac{1}{2} \log N + h_0(L_i) \right).$$

By Lemma 2 we see that

$$\log |\mathscr{D}'| \leq 2d'(d' - 1)(h_0(\alpha'_1) + \dots + h_0(\alpha'_r) + \frac{1}{2} r \log 2).$$

Now $h_0(\alpha'_j) \leq \sigma_j/d$ and, since $\sigma_j \geq 1/d$, we have

$$r/d \leq \sigma_1 + \dots + \sigma_r \leq rd^{r-1} \sigma_1 \dots \sigma_r.$$

Hence we obtain

$$\frac{1}{2d'} \log |\mathscr{D}'| \leq \sigma_1 + \dots + \sigma_r + \frac{1}{2} rd \log 2 \leq \frac{D}{32^{r+1}}.$$

We turn next to the contribution of the sum. Our estimates above give

$$h_0(L_i) \leq 1 \cdot 27hT + (1/d)|s|D.$$

Further we have

$$N = (D_{-1} + 1)(D_0 + 1) \dots (D_r + 1) \leq 2^{r+1} h D_0 \dots D_r.$$

The right hand side is at most $4S(64D)^r$ whence

$$\log N \leq \log(4S) + r \log(64D)$$

and since clearly $\log(4S) \leq S$ and $\log(64D) \leq 10^{-4}D$ we get

$$(11) \quad \log N \leq 0.001hT.$$

The summation is with respect to $i = 1, \dots, M$, that is over all s with $|s| \leq S$ and all $t_0, \dots, t_{r-1}$ with $t_0 + \dots + t_{r-1} \leq T$. Thus the number of terms in the sum is

$$M = (2S + 1) \binom{T+r}{r}$$

and its value is at most

$$\binom{T+r}{r} \{1 \cdot 271hT(2S+1) + (1/d)DS(S+1)\}.$$

Since $S \geq 608$, this does not exceed

$$M \{1 \cdot 271hT + 0 \cdot 501(1/d)SD\}.$$

Finally we estimate $N - M$. We have

$$N = h(D_0 + 1) \dots (D_r + 1)$$

and, by choice of parameters, this is at least

$$32rdh(32D)^r \geq 2S(T/r)^r e^r.$$

Since $T \geq 10^6 r^2$ and

$$\binom{T+r}{r} \leq \frac{(T+r)^r}{r!} \leq e^{r-1} \left(1 + \frac{T}{r}\right)^r$$

it follows that $N \geq 0 \cdot 99eM$. Hence we have

$$M/(N - M) \leq 0 \cdot 592$$

and the solution to the system (9) gives a point p with projective co-ordinates $p(\lambda)$ such that

$$h_0(p) \leq 0 \cdot 592 \{1 \cdot 271hT + 0 \cdot 501(1/d)SD\}.$$

Thus, noting that $dhT \leq 0 \cdot 735SD$, we obtain

$$(12) \quad h(p) \leq 0 \cdot 85SD.$$

Here we recall from § 2 that

$$h(p) = \sum \log \max |p(\lambda_{-1}, \dots, \lambda_r)|_v,$$

where the maximum is over all $\lambda_{-1}, \dots, \lambda_r$ and the summation is over all places v of K .

14. The auxiliary functions

Let $L, L_1, \dots, L_r$ be the linear forms in $z_1, \dots, z_n$ specified in § 11 and let

$$Q(t) = Q(Y_0, \dots, Y_r; t)$$

be the polynomials constructed in §13. We now define linear forms

$$M_j = L_j - \frac{1}{b_n} \frac{\partial L_j}{\partial z_n} L \quad (1 \leq j \leq r).$$

Then clearly

$$b_n M_j = \sum_{i=1}^{n-1} (b_n \partial L_j / \partial z_i - b_i \partial L_j / \partial z_n) z_i$$

so that $M_1, \dots, M_r$ involve only $z_1, \dots, z_{n-1}$. We shall consider in the sequel the functions given by

$$f(z_0, \dots, z_{n-1}; t) = Q(z_0, e^{M_1}, \dots, e^{M_r}; t).$$

We put

$$f(z) = f(z, 2^{-v} z \log \alpha_1, \dots, 2^{-v} z \log \alpha_{n-1}; t)$$

and proceed to estimate $|f(z)|$ for arbitrary complex z and all sets t with

$$t_0 + \dots + t_{r-1} \leq T^*,$$

where $T^* \leq T$.

We note first that

$$|\lambda_1 \partial L_1 / \partial z_n + \dots + \lambda_r \partial L_r / \partial z_n| \leq 2^v D;$$

this follows from the estimate

$$|\partial L_j / \partial z_n| h'(\alpha_n) \leq 2^v \sigma_j \quad (1 \leq j \leq r),$$

given by §11, combined with $h'(\alpha_n) \geq 1/d$ and $\lambda_j \leq D/(rd\sigma_j)$. Thus we see that

$$|(\lambda_1 L_1 + \dots + \lambda_r L_r) - (\lambda_1 M_1 + \dots + \lambda_r M_r)| \leq 2^v D |L|.$$

On substituting $z_j = 2^{-v} z \log \alpha_j$ for $j = 1, 2, \dots, n$, the right hand side becomes $|Az|D$ and by (10) this is less than $0 \cdot 001|z|D$. The first sum on the left becomes

$$(\lambda_1 \log \alpha'_1 + \dots + \lambda_r \log \alpha'_r) z$$

and this has absolute value at most $|z|D$ since by §11 and the definition of h' we have

$$|\log \alpha'_j| \leq dh'(\alpha'_j) \leq d\sigma_j.$$

It follows that the expression

$$|\lambda_1 M_1 + \dots + \lambda_r M_r|$$

evaluated as above is at most $1 \cdot 001|z|D$.

Now as in § 13 we have

$$\log |\Pi(t)| \leq h(T^* - t_0) + T \log(1 \cdot 7)$$

and we observe that $\log(1 \cdot 7) < 0 \cdot 028h$. Further, by § 11, we obtain

$$|\Theta(z; t)| \leq (u(h))^{t_0} (e(2 + |z|/h))^{h(D_0 + 1)}.$$

On noting that, for any $\mu > 0$, the maximum of the function $(2 + x/h)^h e^{-x/\mu}$ occurs at $x = (\mu - 2)h$, we get

$$(e(2 + |z|/h))^h \leq (\mu e^{2/\mu})^h e^{|z|/\mu}$$

and hence

$$\log |\Theta(z; t)/(u(h))^{t_0}| \leq \{(\log \mu + (2/\mu))h + |z|/\mu\} (D_0 + 1).$$

Taking $\mu = 57rd$, it follows from

$$\log(57rd)/\log(2rd) \leq \log 114/\log 4$$

that the expression in braces on the right does not exceed

$$\{(\log 114 + (1/57))(S/16) + (|z|/57)\} \log(2rd)/(rd \log 4)$$

and the product with $D_0 + 1$ is at most

$$(0 \cdot 108S + 0 \cdot 007|z|)D/d.$$

On combining our results, noting that

$$(\log u(h) - h)t_0 \leq 0 \cdot 1hT,$$

and recalling that $dhT \leq 0 \cdot 735SD$ we obtain

$$\log |\Pi(t) \Theta(z; t)| \leq hT^* + (0 \cdot 203 + 0 \cdot 007|z|/S)SD/d.$$

Hence, since the number N of summands in the expression for Q satisfies (11), this gives

$$(13) \quad \log |f(z)| \leq \ln(p) + hT^* + 0 \cdot 204(1/d)SD + 1 \cdot 008|z|D,$$

where, for brevity, we have written $\ln(p) = \log \max |p(\lambda)|$.

In analogy with $f(z)$ we define

$$g(z) = Q(z, \alpha'_1 z, \dots, \alpha'_r z; t).$$

Then our discussion shows that the function $\log |f(z) - g(z)|$ does not exceed the right hand side of (13) with the additional sum

$$|Az|D + \log(|Az|D).$$

Indeed $f(z) - g(z)$ is given by $f(z)$ with a further factor $1 - e^{\delta(z;\lambda)}$ inside the summation where $\delta(z; \lambda)$ is the expression

$$(\lambda_1 L_1 + \dots + \lambda_r L_r) - (\lambda_1 M_1 + \dots + \lambda_r M_r)$$

evaluated at $z_j = 2^{-v} z \log \alpha_j$; we have

$$\log |1 - e^{\delta(z;\lambda)}| \leq |\delta(z; \lambda)| + \log |\delta(z; \lambda)|$$

and $|\delta(z; \lambda)| \leq |Az|D$, whence our assertion. Now noting that $x \leq \mu e^{(x/\mu)-1}$ for all $x \geq 0$ and any $\mu > 0$, we obtain

$$\log |zD| \leq 0 \cdot 001 ((1/d)SD + |z|D).$$

Thus, by (10), we see that our upper bound for $\log |f(z) - g(z)|$ does not exceed

$$(14) \quad \ln(p) + hT^* + \{0 \cdot 205(1/d) + 1 \cdot 01(|z|/S) - 9 \cdot 2^r\}SD.$$

15. Algebraic estimates

We now observe that, when s is an integer, $g(s)$ is an element of the algebraic number field K . Our main objective here is to estimate $|g(s)|$ from below, assuming that $g(s) \neq 0$.

In view of the preceding discussion, we can readily estimate $|g(s)|_v$ from above, where v is any valuation of K . In fact, on writing

$$\Omega_v = \sum_{j=1}^r D_j \log \max(1, |\alpha'_j|_v),$$

we see that if v is non-Archimedean then

$$\log |g(s)|_v \leq \log \max |p(\lambda)|_v + |s| \Omega_v,$$

and, by §14, the same estimate holds if v is Archimedean with the extra quantity

$$hT^* + (0 \cdot 204 + 0 \cdot 007|s|/S)SD/d$$

multiplied by $d_v = 1$ or 2 . Now, if $g(s) \neq 0$, then by the product formula for algebraic number fields we have

$$\sum \log |g(s)|_v = 0,$$

where the summation is over all valuations v of K . Hence, noting that $|g(s)| = |g(s)|_{v_0}$ or $|g(s)|_{v_0}^{1/2}$ for some v_0 , we obtain either

$$\log |g(s)| = - \sum_{v \neq v_0} \log |g(s)|_v$$

or the same with a factor $\frac{1}{2}$; in fact it will suffice to deal with the first case, that is $d_{v_0} = 1$, since the conclusion for $d_{v_0} = 2$ holds similarly and indeed in stronger form. Then we have

$$\sum_{v \neq v_0} \log \max |p(\lambda)|_v = h(p) - \ln(p).$$

Furthermore, since $\Omega_v \geq 0$ for all v , we see that

$$\sum_{v \neq v_0} \Omega_v \leq \sum_{j=1}^r D_j h(\alpha'_j),$$

and, by virtue of the definition of σ_j in § 11, we have $h(\alpha'_j) \leq d\sigma_j$ whence the latter sum does not exceed D . It follows, since there are $d-1$ Archimedean valuations $v \neq v_0$ counting v twice if $d_v = 2$, that $\log |g(s)| - \ln(p)$ is at least

$$(15) \quad -\{h(p) + (1 - 1/d)(dhT^* + 0 \cdot 204SD) + 1 \cdot 007|s|D\}.$$

We now observe that, if $|s| \leq 2^r S$, then

$$|f(s) - g(s)| < \frac{1}{2} |g(s)|;$$

indeed, on taking $z = s$, we see that (14) does not exceed $\ln(p) - 7 \cdot 2^r SD$ whereas, from (12), it is clear that (15) is at least $-2 \cdot 2^r SD$. Thus we obtain $|f(s)| > \frac{1}{2} |g(s)|$. On combining (12), (13) and (15), we conclude that for any integer s such that $g(s) \neq 0$ and $|s| \leq 2^r S$ we have $\log |f(z)/f(s)|$ at most

$$(16) \quad dhT^* + 1 \cdot 055SD + 1 \cdot 008(|z| + |s|)D.$$

Finally we establish an estimate analogous to (16) with the integer s replaced by $s/2$. In this case $g(s/2)$ is an element of the field $K' = K(\alpha_1^{1/2}, \dots, \alpha_r^{1/2})$ and we assume that it is not 0. The field K' plainly has degree at most $2^r d$ and in fact this is the precise value in view of our Kummer condition. On taking v to run through all valuations of K' rather than those of K , we obtain

$$\sum_{v \neq v_0} \log \max |p(\lambda)|_v = 2^r h(p) - \ln(p),$$

and, moreover, we get

$$\sum_{v \neq v_0} \Omega_v \leq 2^r \sum_{j=1}^r D_j h(\alpha'_j);$$

here the heights $h(p)$ and $h(\alpha'_j)$ are still those with respect to K and $d_{v_0} = 1$. Now the estimates given earlier for $|g(s)|_v$ remain valid for $|g(s/2)|_v$ if $v \nmid 2$. In the case $v \mid 2$ we have to take into account the fact that $\Theta(s/2; t)$ may not be a 2-adic integer. However, by our remarks in § 12, we see that $2^{2h(D_0+1)}\Theta(s/2; t)$ is an integer. Hence, if $v \mid 2$, then it suffices to include an additional term

$$2h(D_0 + 1) \log |2|_v$$

in the estimate for $\log |g(s/2)|_v$. On using

$$\sum_{v|2} \log |2|_v = 2^r d \log 2$$

together with

$$2h(D_0 + 1) \log 2 \leq 0.032SD/d$$

and noting that there are now $2^r d - 1$ Archimedean valuations $v \neq v_0$ counting as earlier, we deduce that the expression

$$(17) \quad 2^{-r} \{ \log |g(s/2)| - \ln(p) \}$$

is at least (15) with $1/d$ replaced by $1/(2^r d)$, with s replaced by $s/2$ and with an extra $-0.032SD$. Furthermore, if $|s| \leq 4S$ then we have $|f(s/2)| > \frac{1}{2} |g(s/2)|$; this follows as before since (17) is at least $-4SD$ whereas, when $z = s/2$, we see that (14) remains at most $\ln(p) - 7.2^r SD$. We conclude from (12) and (13) that for any integer s with $g(s/2) \neq 0$ and $|s| \leq 4S$ we have $\log |f(z)/f(s/2)|$ at most

$$(18) \quad 2^r \{ dhT^* + 1.087SD + 1.008(|z/2^r| + |s/2|)D \}.$$

We remark that the small additional contribution to the estimate for $|g(s/2)|$ arising from the valuations v dividing 2 increases inductively in a procedure that we use later referred to as the Kummer descent. It is this feature that is the basis of the second order logarithmic factor that occurs in the work of Baker [3] mentioned in §1. The introduction of multiplicity estimates enables one to limit the descent to a relatively small number of steps depending only on rd ; as in Wüstholz [32], this eliminates the factor and it turns out to be one of the most critical aspects of the exposition.

16. A differential lemma

We recall that in §13 we constructed polynomials $Q(Y_0, \dots, Y_r; t)$ for any set t of non-negative integers $t_0, \dots, t_{r-1}$, and we specified differential operators $\partial_0^*, \dots, \partial_{n-1}^*$ on the ring $C[Y_0, \dots, Y_r]$. Let now T', T'' be any real numbers and let t', t'' be any sets of non-negative integers $t'_0, \dots, t'_{n-1}$ and $t''_0, \dots, t''_{r-1}$ respectively such that

$$t'_0 + \dots + t'_{n-1} \leq T', \quad t''_0 + \dots + t''_{r-1} \leq T''.$$

We shall prove the following lemma.

Lemma 6. *The polynomial*

$$(19) \quad \partial_0^{*t'_0} \dots \partial_{n-1}^{*t'_{n-1}} Q(Y_0, \dots, Y_r; t'')$$

is in the vector space generated over C by the polynomials $Q(Y_0, \dots, Y_r; t)$ where t runs through all sets of non-negative integers $t_0, \dots, t_{r-1}$ with $t_0 + \dots + t_{r-1} \leq T' + T''$.

Proof. We begin by recalling that $\partial_1^*, \dots, \partial_{r-1}^*$ is a maximal set of linearly independent differential operators among $\partial_1^*, \dots, \partial_n^*$. Hence we see that $\partial_0^{*\tau_0} \dots \partial_{n-1}^{*\tau_{n-1}}$ is a linear combination of operators of the form $\partial_0^{*\tau_0} \dots \partial_{r-1}^{*\tau_{r-1}}$ with sets τ of non-negative integers $\tau_0, \dots, \tau_{r-1}$ satisfying $\tau_0 + \dots + \tau_{r-1} \leq T'$. It suffices therefore to prove the lemma with (19) replaced by

$$(20) \quad \partial_0^{*\tau_0} \dots \partial_{r-1}^{*\tau_{r-1}} Q(Y_0, \dots, Y_r; t'').$$

By the property of ∂_j^* recorded in §13 we have

$$\partial_1^{*\tau_1} \dots \partial_{r-1}^{*\tau_{r-1}} Y_1^{\lambda_1} \dots Y_r^{\lambda_r} = \gamma_1^{\tau_1} \dots \gamma_{r-1}^{\tau_{r-1}} Y_1^{\lambda_1} \dots Y_r^{\lambda_r}.$$

Further, from our remark in §12 on the functions Π , we see that the polynomial

$$z_1^{\tau_1} \dots z_{r-1}^{\tau_{r-1}} \Pi(z_1, \dots, z_{r-1}; t_1'', \dots, t_{r-1}'')$$

is in the vector space generated by

$$\Pi(z_1, \dots, z_{r-1}; t_1, \dots, t_{r-1})$$

as $t_1, \dots, t_{r-1}$ run through non-negative integers with

$$t_1 + \dots + t_{r-1} \leq (\tau_1 + \dots + \tau_{r-1}) + (t_1'' + \dots + t_{r-1}'').$$

On substituting $z_j = \gamma_j$, it follows that $\gamma_1^{\tau_1} \dots \gamma_{r-1}^{\tau_{r-1}} \Pi(t'')$ is a linear combination of the $\Pi(t)$ with coefficients independent of $\lambda_1, \dots, \lambda_r$, where the elements of the sets τ, t'' and t satisfy the above inequality. Now since

$$\partial_0^{*\tau_0} \Theta(Y_0; t'') = (u(h))^{-\tau_0} ((\tau_0 + t_0'')! / t_0'') \Theta(Y_0; \tau + t''),$$

it is clear that the expressions

$$\partial_0^{*\tau_0} \dots \partial_{r-1}^{*\tau_{r-1}} \Pi(t'') \Theta(Y_0; t'') Y_1^{\lambda_1} \dots Y_r^{\lambda_r}$$

which occur in the polynomial (20) are linear combinations of

$$\Pi(t) \Theta(Y_0; t) Y_1^{\lambda_1} \dots Y_r^{\lambda_r}, \quad t_0 + \dots + t_{r-1} \leq T' + T'',$$

with coefficients independent of the λ 's. The lemma follows from the definition of $Q(Y_0, \dots, Y_r; t)$.

17. Differential estimates

Let $T' \geq 0$ and $T'' \geq 0$ be real numbers with $T' + T'' \leq T^*$. We denote by $f(z)$ the function defined in §14 corresponding to a set t'' of non-negative integers $t_0'', \dots, t_{r-1}''$ satisfying $t_0'' + \dots + t_{r-1}'' \leq T''$. We signify by m any integer with $0 \leq m \leq T'$ and we write for brevity

$$f_m(z) = \frac{1}{m!} \left(\frac{d}{dz} \right)^m f(z).$$

By $g(z; t)$ we designate the function $g(z)$ defined in § 12 and we shall assume in this section that $g(l; t) = 0$ for some complex number l and for all sets t of non-negative integers $t_0, \dots, t_{r-1}$ with $t_0 + \dots + t_{r-1} \leq T' + T''$. We proceed to derive an estimate for $f_m(l)$.

We begin by noting that if $f^{(r)}(z; t'')$ is the function

$$\left(\frac{\partial}{\partial z_0}\right)^{t_0} \left(b_n \frac{\partial}{\partial z_1}\right)^{t_1} \dots \left(b_n \frac{\partial}{\partial z_{n-1}}\right)^{t_{n-1}} f(z_0, \dots, z_{n-1}; t'')$$

evaluated at $z_0 = z$ and $z_j = 2^{-v} z \log \alpha_j$ for $j = 1, \dots, n-1$, then we have

$$f_m(z) = \sum (2^v b_n)^{-(m-t_0)} (1/t_0!) a(t') f^{(r)}(z; t''),$$

where

$$a(t') = (\log \alpha_1)^{t'_1} \dots (\log \alpha_{n-1})^{t'_{n-1}} / (t'_1! \dots t'_{n-1}!)$$

and the summation is over all non-negative integers $t'_0, \dots, t'_{n-1}$ with $t'_0 + \dots + t'_{n-1} = m$. We shall compare $f^{(r)}(z; t'')$ with the corresponding expression $g^{(r)}(z; t'')$ defined by (19) with $Y_0 = z$ and $Y_i = \alpha_i^{z_i}$ for $i = 1, \dots, r$. Since

$$(b_n \partial / \partial z_j) e^{\lambda_1 M_1 + \dots + \lambda_r M_r} = \gamma_j e^{\lambda_1 M_1 + \dots + \lambda_r M_r}$$

and the right hand side is just $\partial_j^* Y_1^{\lambda_1} \dots Y_r^{\lambda_r}$ with $Y_i = e^{M_i}$, we see that the difference

$$f^{(r)}(z; t'') - g^{(r)}(z; t'')$$

is given by the sum over $\lambda_{-1}, \dots, \lambda_r$ of the terms

$$p(\lambda) \Pi(t'') \Theta'(z; t'') \alpha_1'^{\lambda_1 z} \dots \alpha_r'^{\lambda_r z} \gamma_1^{t'_1} \dots \gamma_{n-1}^{t'_{n-1}} (e^{-\delta(z; \lambda)} - 1),$$

where

$$\Theta'(z; t'') = (\partial / \partial z_0)^{t_0} \Theta(z; t'')$$

and $\delta(z; \lambda)$ is the expression indicated in § 14. By our discussion there we have

$$\log |1 - e^{-\delta(z; \lambda)}| \leq \{0 \cdot 001(1/d) + 0 \cdot 002(|z|/S) - 9 \cdot 2r\} SD.$$

Further, as in § 14, we see that

$$\log |\alpha_1'^{\lambda_1 z} \dots \alpha_r'^{\lambda_r z}| \leq |z| D.$$

Moreover, by § 13, we have

$$\log |\Pi(t'')| \leq h(T'' - t_0'') + T \log(1 \cdot 7).$$

Now since $h'(\alpha_j) \geq |\log \alpha_j|/d$ and furthermore, in view of § 11, the inequality $h'(\alpha_j) \leq h'(\alpha_n)$ holds for all j , we obtain

$$|\gamma_j \log \alpha_j| \leq e^{h'(L)} d \sum_{i=1}^r \{|\partial L_i / \partial z_j| h'(\alpha_j) + |\partial L_i / \partial z_n| h'(\alpha_n)\} \lambda_i.$$

It follows from our inductive hypothesis that the summand on the right is at most $2^r \alpha_i \lambda_i$, whence the same bound that we gave in § 13 for $|\gamma_j|$, namely $e^{h+1}D$, is valid also for $|\gamma_j \log \alpha_j|$. Thus the absolute value of the expression

$$\Gamma(t') = a(t') \gamma_1^{t'_1} \dots \gamma_{n-1}^{t'_{n-1}}$$

can be estimated by

$$(e^{h+1}D)^{t'_1 + \dots + t'_{n-1}} / (t'_1! \dots t'_{n-1}!)$$

and the logarithm of this quantity is at most $h(T' - t'_0) + (n-1)eD$. Now, as already noted, the assumption at the end of § 5 implies that $h \geq 19$; moreover, since $k! \geq k^k e^{-k+1}$, it implies further that $h \geq (2n+1)(1 + \log n)$ so that $h \geq 5n$ for all n . Since $T \geq 11 \cdot 75rD - 1$ and $r \geq 2$, this gives

$$(n-1)eD + T \log(1 \cdot 7) \leq 0 \cdot 06 hT.$$

Hence we obtain

$$\log |\Gamma(t') \Pi(t'')| \leq h(T^* + 0 \cdot 06 T) - h(t'_0 + t''_0).$$

It follows as in § 13 that

$$\log |\Gamma(t') \Pi(t'') \Theta(z; t' + t'')| \leq hT^* + (0 \cdot 226 + 0 \cdot 007 |z|/S) SD/d.$$

Now as noted in § 16 we have

$$\frac{\Theta'(z; t'')}{t'_0!} = \binom{t'_0 + t''_0}{t'_0} \frac{\Theta(z; t' + t'')}{(u(h))^{t_0}}$$

and the binomial factor is at most 2^T . Hence on combining our estimates we see that the logarithm of the absolute value of

$$(1/t'_0!) a(t') (f^{(r)}(z; t') - g^{(r)}(z; t''))$$

is at most (14) with $0 \cdot 205$ increased slightly to $0 \cdot 255$; here we are again using (11) for the number of terms in the sum over $\lambda_{-1}, \dots, \lambda_r$ and the fact that $T \log 2$ is less than $0 \cdot 027 SD/d$.

The desired estimate for $f_m(l)$ now follows readily. By virtue of Lemma 6 we see that $g^{(r)}(l; t'')$ is a linear combination of terms $g(l; t)$ for sets t of non-negative integers $t_0, \dots, t_{r-1}$ with $t_0 + \dots + t_{r-1} \leq T' + T''$. Hence by our hypothesis at the beginning we have $g^{(r)}(l; t'') = 0$. On noting that the number of sets t' is given by

$$\binom{m+n}{n} \leq 2^{T+n}$$

and recalling that $h \geq \max(19, 5n)$, we conclude that $\log |f_m(l)|$ does not exceed (14) with z replaced by l and with $0 \cdot 205$ increased to $0 \cdot 282$.

For later application we actually need an estimate for the quotient of $f_m(l)$ by $f(s)$ rather than for $f_m(l)$ itself; here s is any integer such that $g(s) \neq 0$ and $|s| \leq 2^r S$. Then from (12) and (15) we see that $\log |f_m(l)/f(s)|$ is at most

$$(21) \quad dhT^* + (1 \cdot 133 - 9 \cdot 2^r)SD + 1 \cdot 01(|l| + |s|)D.$$

Similarly if s is any integer such that $g(s/2) \neq 0$ and $|s| \leq 4S$ then, on noting that the terms involving $1/d$ cancel up to a residue $0 \cdot 02$, we deduce from (12) and our estimate for (17) that $\log |f_m(l)/f(s/2)|$ is at most

$$(22) \quad 2^r \{dhT^* - 7 \cdot 893SD + 1 \cdot 01(|l/2^r| + |s/2|)D\}.$$

18. Finite Blaschke products

We shall turn in the next section to the question of extrapolation and we shall use there finite Blaschke products of the kind well known in conformal mapping theory; as regards previous application in the context of transcendence studies we refer to M. Mignotte and M. Waldschmidt [19]. Here we record some simple properties.

Suppose that $R > 0$ and let k be an integer with $|k| < R$. We consider the Blaschke factor

$$\beta(z; k) = \frac{R(z - k)}{R^2 - kz}.$$

This fractional linear transformation maps the Riemann sphere conformally onto itself. Moreover the image of the complex disc $|z| \leq R$ is given by $|z| \leq 1$ and it takes the circle $|z| = R$ to $|z| = 1$; this can be verified briefly by observing that the images of the points $\pm R$ and iR each have absolute value 1. Thus we have $|\beta(z; k)| = 1$ for $|z| = R$. Since clearly $\beta(\bar{z}; k)$ is the complex conjugate of $\beta(z; k)$ where $\bar{z}$ denotes the conjugate of z , we see that the image of any region symmetric with respect to the real axis is again symmetric. It follows that any disc with centre on the real axis is again mapped onto a disc with real centre. We note also, by computing the derivative, that the function $\beta(x; k)$ for real x with $|x| \leq R$ is increasing.

We shall be concerned in the sequel with integration over the circle C_l given by $|z - l| = \eta$ where $0 < \eta < \frac{1}{2}$ and l is an integer with $|l| \leq R - \eta$. From our discussion above it is readily verified that for z on C_l we have $|\beta(z; k)| \geq \beta(l - \eta; k)$ if $l > k$ and $|\beta(z; k)| \geq -\beta(l + \eta; k)$ if $l < k$. For $l = k$ the situation is different since then the image of the disc with boundary C_l contains the origin; in this case we have $|\beta(z; l)|$ at least $-\beta(l - \eta; l)$ if $l \geq 0$ and $\beta(l + \eta; l)$ if $l < 0$. We now observe that for $k > 0$ we have

$$|\beta(z; k) \beta(z; -k)| \geq (k + l' - \eta)|k - l' - \eta|/R^2,$$

where for simplicity we have written l' for $|l|$. This follows in the case $l \geq k$ from

$$\beta(l - \eta; k) \beta(l - \eta; -k) = R^2((l - \eta)^2 - k^2)/(R^4 - k^2(l - \eta)^2);$$

it follows similarly with η replaced by $-\eta$ in the case $l \leq -k$, and for the remaining range, that is $-k < l < k$, we use

$$\beta(l + \eta; k) \beta(l - \eta; -k) = R^2(l^2 - (k - \eta)^2) / ((R^2 - k\eta)^2 - k^2 l^2).$$

We note also that $|\beta(z; 0)| \geq |l' - \eta|/R$ for all l .

Now let X be any integer with $0 < X \leq R - \eta$. We define the Blaschke product by

$$B(z; X) = \prod_{|k| \leq X} \beta(z; k)$$

and we proceed to derive a lower bound for its absolute value on the circle C_l where $|l| \leq X$. On writing

$$B(z; X) = \beta(z; 0) \prod_{k=1}^X \beta(z; k) \beta(z; -k),$$

we see that the results just obtained give the lower bound

$$R^{-(2X+1)} \left(\prod_{k=1}^X (k + l' - \eta) \right) \left(\prod_{k=0}^X ||k - l'| - \eta| \right).$$

We estimate the first product from below by

$$\prod_{k=1}^X (k + l' - 1) = (X + l' - 1)! / (l' - 1)!.$$

For the second product we use the bound $\eta(1 - \eta)^2$ for the terms given by $k = l' - 1$, l' and $l' + 1$ that occur in our range, and we then estimate the complementary factor from below by $(X - l' - 1)!(l' - 1)!$; here the first factorial is interpreted as 1 when l' is X and $X - 1$, and similarly for the second factorial when l' is 0 or 1. We conclude that

$$|B(z; X)| \geq \eta(1 - \eta)^2 R^{-(2X+1)} (X + l' - 1)! (X - l' - 1)!.$$

On replacing $X + l' - j$ by $X - j$ for $j = 1, 2, \dots, l'$, we get

$$(X + l' - 1)! (X - l' - 1)! \geq ((X - 1)!)^2.$$

Now from Stirling's formula we have $X! \geq (X/e)^X \sqrt{(2\pi X)}$; this gives

$$((X - 1)!)^2 \geq 2\pi X^{2X-1} e^{-2X}$$

and therefore our bound for $|B(z; X)|$ becomes

$$2\pi\eta(1 - \eta)^2 X^{-2} e^{-2X} (X/R)^{2X+1}.$$

Finally we compare $B(z; X)$ with $B(x; X)$ where x is any real number with $|x| \leq R$. Suppose first that $|x| \geq X$. Then for $k = 1, 2, \dots, X$ we have

$$|\beta(x; k) \beta(x; -k)| = R^2(x^2 - k^2)/(R^4 - k^2x^2) \leq x^2/R^2.$$

Clearly this remains valid for x in the range $k \leq |x| \leq X$; if $|x| < k$ then, on interchanging x and k on the right, the estimate here becomes k^2/R^2 . Thus, since $|\beta(x; 0)| = |x|/R$, we obtain, for all x ,

$$(23) \quad |B(x; X)| \leq (\max(|x|, X)/R)^{2X+1}.$$

Now on combining with our previous result we see that, for z on C_l ,

$$(24) \quad |B(x; X)/B(z; X)| \leq (2\pi\eta)^{-1}(1-\eta)^{-2}X^2e^{2X}(\max(1, |x|/X))^{2X+1}.$$

Note also that, in view of our earlier remarks, we have $|B(z; X)| = 1$ on the circle C given by $|z| = R$.

Analogous estimates hold for the function $B'(z; X)$ defined like $B(z; X)$ but with k restricted to run through odd integers and X is assumed to be even. In fact the number of k is then X and (23) is clearly valid for B' with the exponent $2X+1$ replaced by X . Moreover, for z on C_l with l odd, (24) holds for B' with a slightly modified expression on the right, namely

$$(25) \quad (4\pi\eta)^{-1}(1-\eta/2)^{-2}X^2e^X(\max(1, |x|/X))^X.$$

To prove this, we write $k = 2k' - 1$ so that, for $k > 0$, we have $k' = 1, 2, \dots, X/2$, and we put $l'' = (l' - 1)/2$. Then

$$k + l' - \eta = 2(k' + l'' - \eta/2)$$

and the product of the quantity on the right over k' is at least

$$2^{X/2}((X/2) + l'' - 1)!/(l'' - 1)!$$

assuming that $l'' > 0$; if $l'' = 0$ then the estimate holds with a further factor $1 - \eta/2$. Similarly we have

$$||k - l'| - \eta| = 2||k' - l'' - 1| - \eta/2|$$

and the product over k' is at least

$$(\eta/2)(1 - \eta/2)^2 2^{X/2}((X/2) - l'' - 2)!(l'' - 1)!;$$

in the case $l'' = 0$ we can omit one of the factors $1 - \eta/2$. Hence a lower bound for $|B'(z; X)|$ on C_l is given by

$$(\eta/2)(1 - \eta/2)^2(2/R)^X((X/2) + l'' - 1)!((X/2) - l'' - 2)!.$$

Now the product of the factorials is at least $2\pi(X/2)^{X-2}e^{-X}$ and (25) follows.

19. Extrapolation

We proceed first to show that for $j = 0, 1, \dots, r-1$ we have $g(s; t) = 0$ for all integers s with $|s| \leq 2^j S$ and all sets t of non-negative integers $t_0, \dots, t_{r-1}$ with

$$(26) \quad t_0 + \dots + t_{r-1} \leq \xi^j T,$$

where $\xi = 1 - (0 \cdot 536)/r$. The proposition is valid for $j = 0$ by virtue of our construction of the polynomial Q . We assume that it holds for $j = J$, where J is an integer with $0 \leq J \leq r-2$, and we shall prove the assertion for $j = J+1$. Accordingly we shall verify that $g(s; t) = 0$ for any integer s with $S' < |s| \leq 2S'$, where $S' = 2^J S$, and any set t satisfying (26) with $j = J+1$.

Let now $f(z)$ be the function defined in §14 corresponding to our set t . Further let

$$F(z) = (B(z; S'))^{T'+1}$$

where $T' = [(1 - \xi) \xi^J T]$ and $B(z; X)$ is the Blaschke product with R given by $7 \cdot 2S'$. We consider the integral

$$\mathcal{J} = \mathcal{J}(F, f, s) = \frac{1}{2\pi i} \int_C \frac{f(z) dz}{(z-s)F(z)},$$

where C is the circle $|z| = R$. By Cauchy's theorem we have

$$(27) \quad \mathcal{J} - \mathcal{J} = f(s)/F(s),$$

where

$$\mathcal{J} = \frac{1}{2\pi i} \sum_{l=-S'}^{S'} \sum_{m=0}^{T'} f_m(l) \int_{C_l} \frac{(z-l)^m dz}{(z-s)F(z)}$$

and C_l is the circle defined in §18. We now assume that there exist s, t as above such that $g(s; t) \neq 0$; then (16) holds with $T^* = \xi^J T$ and moreover (21) is valid similarly since the hypothesis at the beginning of §17 holds with $T'' = \xi^{J+1} T$. We shall show that the estimates imply that $|\mathcal{J}|$ and $|\mathcal{J}|$ are both less than $\frac{1}{2} |f(s)/F(s)|$; this contradicts (27) and we conclude that $g(s; t) = 0$ as asserted.

First we note that, on the circle C , we have $|F(z)| = 1$ and also $|z-s| \geq 5 \cdot 2S'$. This gives at once

$$|\mathcal{J}| \leq 2 \sup |f(z)|,$$

where the supremum is taken on C . By (23) with $R = 7 \cdot 2S'$ we have

$$\log |F(s)| \leq -(2S' + 1)(T' + 1) \log(3 \cdot 6)$$

and, since $(1 - \xi) T \geq 6 \cdot 297D$, the bound is at most $-16 \cdot 13 \xi^J S' D$. Further, from (16), on using $dhT^* \leq 0 \cdot 735SD$ and $|z| + |s| \leq 9 \cdot 2S'$, we get

$$\log |f(z)/f(s)| \leq ((1 \cdot 79/2^J) + 9 \cdot 274) S' D.$$

Hence we see that the expression

$$\log |(F(s)/f(s))\mathscr{J}|$$

is at most

$$\{(1 \cdot 79/2^J) + 9 \cdot 275 - (16 \cdot 13)\xi^J\}S'D.$$

Now we have $J \leq r - 2$ whence $\xi^J \geq e^{-0.536}$. Thus, for $J \geq 4$, our estimate does not exceed $-0.05S'D$. This holds also in the cases $J = 0, 1, 2$ and 3 as one verifies readily on using the fact that $\xi \geq 1 - (0.536)/(J + 2)$. The desired result for $|\mathscr{J}|$ follows.

To deal with $\mathscr{J}$ we begin by noting that, for z on C_l , we have $|z - l| = \eta$ and $|z - s| \geq 1 - \eta$. Hence the integral over C_l has absolute value at most

$$2\pi\eta^{m+1}(1 - \eta)^{-1} \sup (|F(z)|^{-1}).$$

By (24) with $X = S'$ we see that the product with $|F(s)|$ does not exceed

$$(2\pi)^{-T'}\eta^{m-T'}(1 - \eta)^{-2T'-3}(S'^2 e^{2S'} 2^{2S'+1})^{T'+1}.$$

It follows that we can estimate $|F(s)\mathscr{J}|$ from above by

$$(2S' + 1)(S'(2e)^{S'})^{2(T'+1)} \max |f_m(l)|,$$

together with a factor

$$\pi^{-(T'+1)}\eta^{-T'}(1 - \eta)^{-2(T'+2)},$$

where the maximum is over all l and m . On choosing $\eta = \frac{1}{3}$, the factor is just

$$\frac{3}{4}(4\pi/27)^{-(T'+1)}$$

and, since $S' \geq 608$, its logarithm is then at most $0.002S'(T' + 1)$. Further, the logarithm of the quantity involving S' is at most $3.41S'(T' + 1)$. Furthermore, from (21), on noting that $|l| + |s| \leq 3S'$, we obtain

$$\log |f_m(l)/f(s)| \leq 4.9S'D - 9.2'SD.$$

Hence we see that the expression

$$\log |(F(s)/f(s))\mathscr{J}|$$

does not exceed

$$3 \cdot 5S'(T' + 1) + 4 \cdot 9S'D - 9.2'SD.$$

Since $T' \leq (1 - \xi)T \leq 6 \cdot 3D$ and $S' \leq 2^{r-2}S$, we get the upper bound $-2 \cdot 2.2'SD$, whence $|\mathscr{J}| \leq \frac{1}{2}|f(s)/F(s)|$ and our proposition is established.

Now let s be any integer with $|s| \leq 4S$ and let t be any set of non-negative integers $t_0, \dots, t_{r-1}$ satisfying (26) with $j = r$. Our object is to prove that $g(s/2; t) = 0$. This certainly holds if s is even in view of the above result with $j = r - 1$. Hence we shall assume that s is odd. Taking S' and T' as before with $J = r - 1$ and the same definitions of R, F and f , we consider the integral $\mathcal{J} = \mathcal{J}(F, f, s/2)$. Then (27) holds with s replaced by $s/2$ and with $\mathcal{J}$ modified similarly. We assume that $g(s/2; t) \neq 0$; then on defining T^* and T'' as above with $J = r - 1$ we see that (18) and (22) hold. We proceed to obtain a contradiction as before.

Clearly our basic estimate for $\mathcal{J}$ remains valid and (23) now gives

$$\log |F(s/2)| \leq -(2S' + 1)(T' + 1) \log(7 \cdot 2);$$

here the bound is at most $-24 \cdot 86 \xi^{r-1} S' D$. Further, from (18), since $T^* = \xi^{r-1} T$ and

$$|z/2'| + |s/2| \leq 5 \cdot 6S,$$

we deduce that $\log |f(z)/f(s/2)|$ is at most

$$2^r \{0 \cdot 735 \xi^{r-1} + 6 \cdot 732\} S D.$$

Hence we see that the expression

$$\log |(F(s/2)/f(s/2)) \mathcal{J}|$$

does not exceed

$$2 \{0 \cdot 735 \xi^{r-1} + 6 \cdot 733 - 12 \cdot 43 \xi^{r-1}\} S' D.$$

Now using the fact that $\xi^{r-1} \geq e^{-0.536}$ we get the bound $-0 \cdot 21 S' D$ and the desired result for $|\mathcal{J}|$ follows.

As regards $\mathcal{J}$, we note that s is odd, whence on C_i we have $|z - (s/2)| \geq \frac{1}{2} - \eta$ and the same basic estimate holds for the integral over C_i with $1 - \eta$ replaced by $\frac{1}{2} - \eta$. Further, by (24), the product with $|F(s/2)|$ does not exceed

$$(2\pi)^{-T'} \eta^{m-T'} (1 - \eta)^{-2T'-2} \left(\frac{1}{2} - \eta\right)^{-1} (S' e^{S'})^{2(T'+1)}.$$

It follows that we can estimate $|F(s/2) \mathcal{J}|$ from above by the same expression as before with $2e$ replaced by e and with a new factor

$$(2\pi)^{-(T'+1)} \eta^{-T'} (1 - \eta)^{-2T'-3} \left(\frac{1}{2} - \eta\right)^{-1}.$$

Again choosing $\eta = \frac{1}{3}$, we see that the logarithm of the factor is at most $0 \cdot 001 S' (T' + 1)$.

Further, the logarithm of the quantity involving S' is at most $2 \cdot 03 S' (T' + 1)$. Furthermore, from (23), on noting that

$$|l/2'| + |s/2| \leq 2 \cdot 5S,$$

we obtain

$$\log |f_m(l)/f(s/2)| \leq 2\{0.735\xi^{r-1} - 5.368\}S'D.$$

On combining our estimates we see that the expression

$$\log |(F(s/2)/f(s/2))\mathscr{J}|$$

does not exceed

$$2\{1.02S'(T' + 1) + 0.735\xi^{r-1}S'D - 5.368S'D\}.$$

Now for any $x \geq 0$ we have $(1 - (x/r))^{r-1} \leq 1 - (x/2)$ whence $\xi^{r-1} \leq 0.732$. Since also $T' \leq 6 \cdot 3 \xi^{r-1}D$ we get the upper bound $-0.25S'D$ and the result follows.

20. Kummer descent

We have now proved that the polynomials $Q(Y_0, \dots, Y_r; t)$ defined in §13 have the property that

$$Q(s/2, \alpha_1'^{s/2}, \dots, \alpha_r'^{s/2}; t) = 0$$

for all integers s with $|s| \leq 4S$ and all sets t of non-negative integers $t_0, \dots, t_{r-1}$ satisfying (26) with $j = r$. Here $\alpha_1'^{1/2}, \dots, \alpha_r'^{1/2}$ are the square-roots determined by the definition of the logarithms in §11. In fact, by the hypothesis there, we know that $\alpha_1', \dots, \alpha_r'$ satisfy the Kummer condition with respect to K and hence the equations hold for any determinations of the square-roots.

We can express Q in the form

$$(28) \quad Q(Y_0, \dots, Y_r; t) = \sum Q_\varepsilon(Y_0, Y_1^2, \dots, Y_r^2; t) Y_1^{\varepsilon_1} \dots Y_r^{\varepsilon_r},$$

where the summation is over the 2^r vectors $\varepsilon = (\varepsilon_1, \dots, \varepsilon_r)$ with $\varepsilon_j = 0$ or 1 and

$$Q_\varepsilon(X_0, \dots, X_r; t)$$

denotes a polynomial in $X_0, \dots, X_r$ with coefficients given by a subset of those of Q ; moreover this decomposition is unique. It holds in particular in the case $t = 0$, that is $t_0 = \dots = t_{r-1} = 0$, and then Q coincides with the polynomial P defined in §13. Now, by construction, P does not vanish identically and thus there is an ε such that $Q_\varepsilon(X_0, \dots, X_r; 0)$ is not 0. Let $Q^{(1)}(Y_0^{(1)}, \dots, Y_r^{(1)}; t)$ denote Q_ε with $X_0 = \frac{1}{2} Y_0^{(1)}$ and $X_j = Y_j^{(1)}$ for $j = 1, 2, \dots, r$. Then by the Kummer property of $\alpha_1', \dots, \alpha_r'$ we see that

$$(29) \quad Q^{(1)}(s, \alpha_1'^s, \dots, \alpha_r'^s; t) = 0$$

for all s and t as above and with s restricted to be odd. Furthermore we have

Lemma 7. *The analogue of Lemma 6 holds for $Q^{(1)}$ with the differential operators $\partial_0^*, \dots, \partial_{n-1}^*$ defined in terms of the new variables $Y_0^{(1)}, \dots, Y_r^{(1)}$.*

Proof. We have $Y_0^{(1)} = 2Y_0$ and $Y_j^{(1)} = Y_j^2$ for $j = 1, 2, \dots, r$ whence the new operators are precisely twice the original operators. On applying ∂_j^* to (28) we get a similar decomposition for $\partial_j^* Q$ with coefficients $\partial_j^* Q_\varepsilon + \gamma_j' Q_\varepsilon$, where $\gamma_j' = 0$ for $j = 0$ and γ_j' is γ_j for $j > 0$ evaluated at $\lambda_i = \varepsilon_i$ ($1 \leq i \leq r$). Now, by Lemma 6, we see that $\partial_j^* Q(Y_0, \dots, Y_r; t'')$ is a linear combination of polynomials $Q(Y_0, \dots, Y_r; t)$, where t runs through all sets as in the assertion with $T' = 1$, whence the same combination of the $Q_\varepsilon(Y_0, Y_1^2, \dots, Y_r^2; t)$ gives the coefficients in the decomposition of $\partial_j^* Q$. The analogue of Lemma 6 for Q_ε and for a single differential operator follows from the uniqueness of the latter on noting that $\gamma_j' Q_\varepsilon$ can be included in the combination. The corresponding conclusion for $Q^{(1)}$ is evident on substituting the new variables $Y_0^{(1)}, \dots, Y_r^{(1)}$ for $Y_0, \dots, Y_r$ and the general result is then obtained by induction.

We now prove that (29) holds not only for odd integers but also for even integers s with $|s| \leq 4S$ provided that we restrict t to sets satisfying (26) with $j = r + 1$. We shall extrapolate as in § 19 and accordingly we define $f^{(1)}$ and $g^{(1)}$ as the functions f and g in § 14 with $Q = Q^{(1)}$. It is clear that if s is an even integer as above and $g^{(1)}(s) \neq 0$ then $\log |f^{(1)}(z)/f^{(1)}(s)|$ can be estimated by (16) with $(|z| + |s|)$ replaced by $\frac{1}{2}(|z| + |s|)$. Indeed the degree of $Q^{(1)}$ in $Y_j^{(1)}$ for $j \geq 1$ is at most $\frac{1}{2} D_j$ and we have now $\Theta^{(1)}(z; t) = \Theta\left(\frac{1}{2}z; t\right)$ in place of Θ in f ; thus (13) holds with $f = f^{(1)}$ and with $|z|$ replaced by $\frac{1}{2}|z|$, and similarly, since s is even, the lower bound deduced from (15) for $|f^{(1)}(s)|$ holds with $|s|$ replaced by $\frac{1}{2}|s|$. Further, for l and m as in § 17, we see that $\log |f_m^{(1)}(l)/f^{(1)}(s)|$ is at most (21) with $(|l| + |s|)$ replaced by $\frac{1}{2}(|l| + |s|)$.

We consider the integral $\mathcal{J} = \mathcal{J}(F', f^{(1)}, s)$ with

$$F'(z) = (B'(z; 2S'))^{T'+1},$$

where $B'(z, X)$ is the lacunary Blaschke product defined in § 18 and $S' = 2S$, $T' = [(1 - \xi)\xi^r T]$ and $R = 7 \cdot 2S'$ as before. Then (27) holds with F' and $f^{(1)}$ in place of F and f in $\mathcal{J}$ and where l runs through the odd integers with $|l| \leq 2S'$. By the analogues of (23) and (16) we see that

$$\log |F'(s)| \leq -16 \cdot 13 \xi^r S' D$$

and

$$\log |f^{(1)}(z)/f^{(1)}(s)| \leq \frac{1}{2}(1 \cdot 79 + 9 \cdot 274)S'D.$$

Now for any $x \geq 0$ we have $(1 - (x/r))^r \geq (1 - (x/2))^2$ whence $\xi^r \geq 0 \cdot 535$ and the desired conclusion that $|\mathcal{J}|$ is at most $\frac{1}{2} |f^{(1)}(s)/F'(s)|$ follows. To obtain the same conclusion for $\mathcal{J}$ we note that, by (25), the product of $|F'(s)|$ with the absolute value of the integral over C_1 does not exceed

$$2\pi^{-T'} \eta^{m-T'} (1 - \eta/2)^{-2(T'+1)} (1 - \eta)^{-1} (S'^2 e^{2S'})^{T'+1}.$$

Thus we can estimate $|F'(s)\mathscr{J}|$ from above by

$$2S'(S'e^{S'})^{2(T'+1)} \max |f_m^{(1)}(I)|$$

together with a factor which, on choosing $\eta = \frac{1}{3}$, has logarithm less than $0 \cdot 001 S'(T' + 1)$.

Moreover the logarithm of the quantity involving S' is at most $2 \cdot 03 S'(T' + 1)$. Now we have $|I| + |s| \leq 4S'$ whence the analogue of (21) gives

$$\log |f_m^{(1)}(I)/f^{(1)}(s)| \leq 1 \cdot 9SD + 2 \cdot 02S'D - 9 \cdot 2'SD.$$

Since $T' \leq 6 \cdot 3D$ and $S' = 2S$, it follows easily that $|\mathscr{J}|$ is bounded above by

$$\frac{1}{2} |f^{(1)}(s)/F'(s)|.$$

This contradicts (27) and hence (29) holds for even s as asserted.

We can now proceed with the Kummer descent. For $I = 0, 1, 2, \dots$ we define

$$S^{(I)} = \xi^{-rI} S \quad \text{and} \quad T^{(I)} = \xi^{rI} T.$$

Then for every set t of non-negative integers $t_0, \dots, t_{r-1}$ with

$$t_0 + \dots + t_{r-1} \leq \xi T^{(I)}$$

there exists a polynomial $Q^{(I)}(Y_0^{(I)}, \dots, Y_r^{(I)}; t)$ in the variables $Y_0^{(I)}, \dots, Y_r^{(I)}$ with the following properties. The polynomial $Q^{(I+1)}(Y_0^{(I+1)}, \dots, Y_r^{(I+1)}; t)$ is given, for some ε , by the coefficient $Q_\varepsilon^{(I)}(Y_0^{(I)}, Y_1^{(I)2}, \dots, Y_r^{(I)2}; t)$ occurring in the decomposition (28) with $Q = Q^{(I)}$, on substituting $Y_0^{(I+1)} = 2Y_0^{(I)}$ and $Y_j^{(I+1)} = Y_j^{(I)2}$; here ε is chosen so that $Q^{(I+1)}$ does not vanish identically for $t = 0$. Further we have (29) with $Q^{(I)}$ in place of $Q^{(1)}$ for all integers s with $|s| \leq 2S^{(I)}$ and all sets t as above. The hypothesis for $I = 0$ corresponds to the case $j = 1$ in the proposition at the beginning of § 19 with $Q^{(0)} = Q$. We have just shown that this implies the result for $I = 1$; for clearly $\xi^{-r} \leq 1 \cdot 87$ whence $2S^{(1)} \leq 4S$.

The general result can be deduced similarly for all I up to a certain bound I^* . In fact let $f^{(I)}$ and $g^{(I)}$ be the functions f and g with $Q^{(I)}$ in place of Q . Then the lower bound for $f^{(I)}(s)$ implied by (15) remains valid with $|s|$ replaced by $2^{-I}|s|$ and with an extra Kummer contribution $2hI(D_0 + 1) \log 2$ arising from the 2-adic valuation of $\Theta^{(I)}(s; t) = \Theta(2^{-I}s; t)$ occurring in $g^{(I)}$. Hence (16) and (21) hold for $f^{(I)}$ with $|I|$, $|s|$ and $|z|$ each multiplied by 2^{-I} and with the same additional contribution. Further, the estimates (18) and (22) remain valid for $f^{(I)}$ with the analogous modifications inside the braces. It is now clear that the extrapolation procedure in § 19 goes through without essential change taking $S^{(I)}$ and $T^{(I)}$ in place of S and T so that, in particular, the value of $S^{(I)}T^{(I)}$ remains fixed. The modifications just mentioned do not affect the basic estimates provided that $I \leq I^*$ with $I^* = 50 \log(2rd)$. It will suffice to verify this in the case based on (22); we have then

$$|I/2^r| + |s/2| \leq 2 \cdot 5S^{(I)}$$

whereas the Kummer contribution is

$$2hI(D_0 + 1) \log 2 \leq \{0.044I/\log(2rd)\} SD.$$

Thus we need to show that $aI + b^{-I} \leq 1$, where

$$a = 0.044/(2.5 \log(2rd)), \quad b = 2\xi^r.$$

Now the function $ax + b^{-x}$ with $a > 0$ and $b > 1$ is continuous for real x and it has a single stationary point, namely a minimum at $x = (\log \log b - \log a)/\log b$. Here we have $a \leq 0.02$ and $b \geq 1.07$ whence the minimum occurs for $x > 0$. The function takes the value 1 at $x = 0$ and, for $x = I^*$, it is less than 1. The desired inequality for $I \leq I^*$ follows; a similar observation applies in the cases based on (16), (18) and (21) where 9.2 , 5.6 and 3 respectively are present in place of 2.5 . This establishes the existence of polynomials as asserted.

21. Group variety reduction

We shall now complete the proof of our theorem by referring to the proposition in §10. Accordingly we take $\mathcal{P} = Q^{(I)}$ with $Y_j = Y_j^{(I)}$ and with $I = [I^*]$ and $t = 0$. Then $\mathcal{P}$ does not vanish identically and bounds for the degrees are given by $\mathcal{D}_0 = h(D_0 + 1)$ and $\mathcal{D}_j = 2^{-I}D_j$ for $j \geq 1$. We define $\mathcal{S} = 2S^{(I)}$ and $\mathcal{T} = \xi T^{(I)}$ and we then put $\mathcal{S}_i = \mathcal{S}/(r+1)$ and $\mathcal{T}_i = [\mathcal{T}/(r+1)]$ for $i = 0, 1, \dots, r$. Let now $L_1, \dots, L_r$ be the linear forms in §11 and let $B_1, \dots, B_r$ be the rationals indicated in §10. Then with the differential operators $\partial_1, \dots, \partial_{r-1}$ given there we see that the vanishing hypothesis in the proposition holds with $\theta_j = \alpha'_j$ for $j = 1, 2, \dots, r$. Taking the determinations of the logarithms as in §11 we obtain $A' = 2^{-v}A$; now clearly $\log \mathcal{S} \leq SD$ whence, from (10), we have $|A'| \leq \pi/\mathcal{S}$. Further, since $\xi^r \geq \frac{1}{2}$, we plainly have $\mathcal{D}_j \leq \mathcal{T}_0$ for $j \geq 1$ and furthermore, using $\xi^r \leq e^{-0.536}$ and $I \geq 49 \log(2rd)$, we get $\mathcal{T}_r < \mathcal{D}_0$.

We shall verify below that (5) is satisfied. Thus we conclude that there exists an integer ϱ with $1 \leq \varrho < r$ as in the proposition. Let $\mathcal{L}_1, \dots, \mathcal{L}_\varrho$ be the linear forms indicated there corresponding to $a_j = \sigma_j$. Further let $\mathcal{L}'_1, \dots, \mathcal{L}'_\varrho$ and $\mathcal{L}'$ be the linear forms in $z_1, \dots, z_n$ given by substituting $Z_j = L_j$ in $\mathcal{L}_1, \dots, \mathcal{L}_\varrho$ and $\mathcal{L}$, respectively. Then $L = \mathcal{L}'$ and so L is in the module of rank ϱ generated by $\mathcal{L}'_1, \dots, \mathcal{L}'_\varrho$ over the rationals. Moreover the algebraic numbers $\theta'_1, \dots, \theta'_\varrho$ given by

$$\log \theta'_j = 2^{-v} \mathcal{L}'_j(\log \alpha_1, \dots, \log \alpha_n) \quad (1 \leq j \leq \varrho)$$

are the same as those defined in §10 whence, as noted there, they satisfy the Kummer condition with respect to K . Since $h'(\alpha'_i) \leq \sigma_i$ we see that $h'(\theta'_j) \leq \mathcal{D}_j$ for $j = 1, \dots, \varrho$, and from the differential identity

$$\partial \mathcal{L}'_j / \partial z_i = \sum_{k=1}^r (\partial \mathcal{L}'_j / \partial Z_k) (\partial L_k / \partial z_i)$$

together with the estimate for the sum with $j = k$ in the inductive hypothesis, we obtain

$$\sum_{i=1}^n |\partial \mathcal{L}'_j / \partial z_i| h'(\alpha_i) \leq 2^v \mathcal{R}_j \quad (1 \leq j \leq \varrho).$$

We shall prove shortly that (6) gives

$$(30) \quad \mathcal{R}_1 \dots \mathcal{R}_\varrho \leq \kappa(\varrho) h'(\alpha_1) \dots h'(\alpha_n);$$

thus all the assumptions in § 11 hold with ϱ in place of r . By the minimal choice of r , we have a contradiction and this establishes our Theorem.

In order to verify (5) and (30) we observe first that, by our choice of parameters, we have

$$S(T+1)^r \geq \frac{1}{2} (r/\zeta)^r h D_0 D_1 \dots D_r,$$

where $\zeta = 32/11 \cdot 75 \leq 1 \cdot 002e$. Now, in the case $m = r$, the inequality (5) becomes

$$\mathcal{S}_r \binom{\mathcal{T}_r + r}{r} \geq (r+1)! \mathcal{D}_0 \mathcal{D}_1 \dots \mathcal{D}_r.$$

Here the left hand side is at least $\mathcal{S}_r (\mathcal{T}_r + 1)^r / r!$ and the right hand side is at most

$$(r+1)! 2^{-rI+1} h D_0 D_1 \dots D_r.$$

Thus, since

$$\mathcal{S}_r = 2 \xi^{-rI} S / (r+1), \quad \mathcal{T}_r + 1 \geq \xi^{rI+1} T / (r+1)$$

and $(1 + 1/T)^r \leq 2$, it suffices to verify that

$$(2 \xi^{r-1})^{rI} \geq 4 \xi^{-r} (\zeta/r)^r (r!) ((r+1)!) (r+1)^{r+1}.$$

We have $\xi^{r-1} \geq e^{-0.536} = 0.585 \dots$ and $I \geq 49 \log(2rd)$ whence $(2 \xi^{r-1})^I \geq (2r)^7$ and the desired result follows easily. To deal with the case $m < r$ it is enough to show that

$$\mathcal{S}_m (\mathcal{T}_m + 1)^{m+1} \geq ((m+1)!)^2 \mathcal{D}_0^{m_0} \dots \mathcal{D}_r^{m_r}$$

where $m_0 + \dots + m_r = m+1$; this is in fact readily checked on noting that

$$\mathcal{S}_m (\mathcal{T}_m + 1) \geq \max((1/r) \mathcal{D}_0, r \mathcal{D}_j)$$

for $j \geq 1$ and $\mathcal{T}_m + 1 \geq b^I \mathcal{D}_j$ where, as in § 20, $b = 2 \xi^r \geq 1.07$ so that $b^I \geq (2rd)^3$.

It remains to prove (30). Now clearly $\mathcal{D}_0 \geq \sigma_j \mathcal{D}_j$ for all $j \geq 1$. Thus the maximum in (6) is at most

$$h(D_0 + 1)(2^{-I} D / rd)^{e-1}.$$

Further we see that

$$\mathcal{L}_{q-1}(\mathcal{T}_{q-1} + 1)^{q-1} \geq (r+1)^{-q} \xi^{(rI+1)(q-2)+1} S(T+1)^{q-1}$$

and moreover our choice of parameters gives as above

$$S(T+1)^r \geq \frac{1}{4} (r/\zeta)^r h(D_0 + 1)(D/rd)^r (\sigma_1 \dots \sigma_r)^{-1}.$$

Hence, by (6), we have

$$\mathcal{R}_1 \dots \mathcal{R}_q \leq b^{-I(q-1)} \xi^{rI} \kappa^*(q) \sigma_1 \dots \sigma_r,$$

where

$$\kappa^*(q) = 4(q-1)! \mathcal{C}(q) (r+1)^q \xi^{-(q-1)} (\zeta/r)^r ((T+1)rd/D)^{r-q+1}.$$

We conclude from (7) that, to obtain (30), it suffices to show that the coefficient of $\sigma_1 \dots \sigma_r$ is at most $(64rd)^{r-q}$. On substituting for T , we see that κ^* does not exceed

$$4(q-1)! \mathcal{C}(q) (r+1)^q (\zeta/r\xi)^{q-1} (33rd)^{r-q+1}.$$

Thus it is enough to verify that

$$b^{I(q-1)} \xi^{-rI} \geq 8(q-1)! (33r^2d) (3\xi)^{q-1} \mathcal{C}(q).$$

But the definition of $\mathcal{C}(q)$ in the proposition gives $\mathcal{C}(q) \leq r^{4q}$ and, since $(q-1)! \leq r^{q-1}$, the right hand side is at most $(3\xi r^5)^{q-1} (264r^6d)$. Now $\xi^{-r} \geq 1 \cdot 7$ and, if $r \geq 3$, we have $b \geq 1 \cdot 108$. Hence $\xi^{-rI} \geq (2rd)^{26}$ and $b^I \geq (2rd)^5$ and the result follows.

References

- [1] *A. Baker*, Linear forms in the logarithms of algebraic numbers IV, *Mathematika* **15** (1968), 204–216.
- [2] *A. Baker*, A sharpening of the bounds for linear forms in logarithms II, *Acta Arith.* **24** (1973), 33–36.
- [3] *A. Baker*, The theory of linear forms in logarithms, *Transcendence Theory: Advances and Applications*, London 1977.
- [4] *A. Baker*, *Transcendental Number Theory*, Cambridge 1990.
- [5] *A. Baker* and *H. M. Stark*, On a fundamental inequality in number theory, *Ann. Math.* **94** (1971), 190–199.
- [6] *A. Baker* and *C. L. Stewart*, On effective approximations to cubic irrationals, *New Advances in Transcendence Theory*, Cambridge 1988.
- [7] *P. E. Blanksby* and *H. L. Montgomery*, Algebraic integers near the unit circle, *Acta Arith.* **18** (1971), 355–369.
- [8] *J. Blass*, *A. M. W. Glass*, *D. K. Manski*, *D. B. Merson* and *R. P. Steiner*, Constants for lower bounds for linear forms in the logarithms of algebraic numbers I, II, *Acta Arith.* **55** (1990), 1–22.
- [9] *E. Bombieri* and *J. Vaaler*, On Siegel's lemma, *Invent. Math.* **73** (1983), 11–32, Addendum, *ibid.* **75** (1984), 377.
- [10] *W. D. Brownawell* and *D. W. Masser*, Multiplicity estimates for analytic functions I, II, *J. reine angew. Math.* **314** (1980), 200–216; *Duke Math. J.* **47** (1980), 273–295.
- [11] *E. Dobrowolski*, On the maximal modulus of conjugates of an algebraic integer, *Bull. Acad. Polon. Sci.* **26** (1978), 291–292.
- [12] *E. Dobrowolski*, On a question of Lehmer and the number of irreducible factors of a polynomial, *Acta Arith.* **34** (1979), 391–401.
- [13] *P. M. Gruber* and *C. G. Lekkerkerker*, *Geometry of Numbers*, Amsterdam 1987.

- [14] *E. Landau*, Sur quelques théorèmes de M. Petrovich relatifs aux zéros des fonctions analytiques, *Bull. Soc. Math. France* **33** (1905), 251–261.
- [15] *K. Mahler*, A theorem on inhomogeneous diophantine inequalities, *Proc. Kon. Ned. Akad. Wet. Amsterdam* **41** (1938), 634–637.
- [16] *K. Mahler*, An application of Jensen's formula to polynomials, *Mathematika* **7** (1960), 98–100.
- [17] *K. Mahler*, On some inequalities for polynomials in several variables, *J. London Math. Soc.* **37** (1962), 341–344.
- [18] *D. W. Masser* and *G. Wüstholz*, Zero estimates on group varieties I, II, *Invent. Math.* **64** (1981), 489–516; **80** (1985), 233–267.
- [19] *M. Mignotte* and *M. Waldschmidt*, Linear forms in two logarithms and Schneider's method II, *Acta Arith.* **53** (1989), 251–287.
- [20] *Yu. V. Nesterenko*, Bounds on the orders of zeros of a class of functions and their application to the theory of transcendental numbers, *Math. USSR Izvest.* **11** (1977), 253–284.
- [21] *P. Philippon* and *M. Waldschmidt*, Lower bounds for linear forms in logarithms, *New Advances in Transcendence Theory*, Cambridge 1988.
- [22] *C. J. Smyth*, On the product of the conjugates outside the unit circle of an algebraic integer, *Bull. London Math. Soc.* **3** (1971), 169–175.
- [23] *H. M. Stark*, Some effective cases of the Brauer-Siegel theorem, *Invent. Math.* **23** (1974), 135–152.
- [24] *R. Tijdeman*, On the equation of Catalan, *Acta Arith.* **29** (1976), 197–209.
- [25] *M. Waldschmidt*, A lower bound for linear forms in logarithms, *Acta Arith.* **37** (1980), 257–283.
- [26] *G. Wüstholz*, Über das abelsche Analogon des Lindemannschen Satzes I, *Invent. Math.* **72** (1983), 363–388.
- [27] *G. Wüstholz*, Zum Periodenproblem, *Invent. Math.* **78** (1984), 381–391.
- [28] *G. Wüstholz*, Transzendenzeigenschaften von Perioden elliptischer Integrale, *J. reine angew. Math.* **354** (1984), 164–174.
- [29] *G. Wüstholz*, Multiplicity estimates on group varieties, *Ann. Math.* **129** (1989), 471–500.
- [30] *G. Wüstholz*, Algebraische Punkte auf analytischen Untergruppen algebraischer Gruppen, *Ann. Math.* **129** (1989), 501–517.
- [31] *G. Wüstholz*, A new approach to Baker's theorem on linear forms in logarithms I, II, *Diophantine Problems and Transcendence Theory*, *Lect. Notes Math.* **1290** (1987), 189–211.
- [32] *G. Wüstholz*, A new approach to Baker's theorem on linear forms in logarithms III, *New Advances in Transcendence Theory*, Cambridge 1988.
- [33] *Kunrui Yu*, Linear forms in p -adic logarithms II, *Comp. Math.* **74** (1990), 15–113.

Trinity College, Cambridge, England
ETH-Zentrum, Zürich, Switzerland

Eingegangen 20. Mai 1992, in revidierter Fassung 16. Oktober 1992