LINEAR INDEPENDENCE OF LOGARITHMS OF ALGEBRAIC NUMBERS

by

Michel WALDSCHMIDT

The Institute of Mathematical Sciences, Madras, IMSc Report 116 (1992).

Let $a_1, \ldots, a_m$ be positive rational integers and $b_1, \ldots, b_m$ be rational integers; assume that the rational number $a_1^{b_1} \cdots a_m^{b_m}$ is not equal to 1; how close to 1 can it be ? Our goal is to give an estimate from below for this distance. The trivial estimate is

$$\left| a_1^{b_1} \cdots a_m^{b_m} - 1 \right| \geq A^{-nB}$$

where $A = \max\{2, a_1, \ldots, a_n\}$ and $B = \max\{2, |b_1|, \ldots, |b_n|\}$; this is a kind of Liouville estimate: the absolute value of a non-zero rational number is at least the inverse of a denominator. This estimate is sharp in terms of A and n, but not in terms of B; there are many cases where a better dependence in B is required. We give a short historical survey of this question in Chapter 1, and we quote the best known results to date in Chapter 12. In between, we give complete proofs of non-trivial estimates.

During a workshop which took place at Leiden in October 1990, E. Thomas and N. Tzanakis noticed that there is no introductory text for the non-expert on this domain; the non-trivial measures of linear independence for logarithms are used as a *black box* by several people, especially in connection with Diophantine equations. Therefore a *simple* introduction was needed. However, *simple* depends on the reader: for those who know a little bit of commutative algebra, Chapter 5 below will look unnecessary complicated, and they will prefer to replace it by Chapter 8, which yields a stronger result. On the opposite, those who dislike the words "algebraic geometry" will have better to skip Chapter 8 and just take for granted the "zero estimate" given in Proposition 8.1.

These notes grew out of lectures given at the Matscience Institute of Madras in January 1992. The initial goal was to give a proof of Baker transcendence theorem on linear independence of logarithms of algebraic numbers, which is supposed to be simpler than previously known proofs: no derivative is involved, and the auxiliary function is replaced by Laurent's interpolation determinants. Once this purpose was achieved (Chapters 2 to 6), we started looking at the effective aspect of the question, which is the most important one for applications. A first non-trivial estimate was proved, for linear combinations of logarithms

$$\beta_1 \log \alpha_1 + \cdots + \beta_m \log \alpha_m,$$

where α_i and β_i are algebraic numbers, under the assumption that the logarithms $\log \alpha_i$ are linearly independent over $\mathbb{Q}$, and also the coefficients β_i are linearly independent over $\mathbb{Q}$; the assumption on the $\log \alpha_i$ involves no loss of generality, while the condition on the β_i is really strong, since the most interesting case is when the β_i are all rational integers. However, the argument which is used to remove the assumption on linear independence of the $\log \alpha_i$ enables one to remove also the condition on the β_i, but at a rather heavy cost. Nevertheless this is sufficient to provide a non-trivial estimate, which is given in Chapter 7.

The three next chapters are devoted to a refinement of this first estimate. We do not give the sharpest known results (which require to introduce one more variable with derivatives, and also to use Fel'dman's polynomials), but nevertheless our estimate is not very far from the best known. A refined zero-estimate is required; this is a consequence of a general result due to P.Philippon; the corresponding chapter has been written by D. Roy and was the subject of three lectures at the University of Pondicherry.

Baker dealt also with non-homogeneous linear combinations of logarithms:

$$\beta_0 + \beta_1 \log \alpha_1 + \cdots + \beta_m \log \alpha_m.$$

The non-vanishing of such linear combinations (Chapter 11) has been the subject of lectures at Hyderabad (Central University) in February 1992. Finally, the sections devoted to the six exponential theorem (in Chapter 1) and its generalizations (Chapter 13) were developed at Bombay University and at the Tata Institute of Fundamental Research.

I have the pleasure to thank R. Balasubramanian who invited me to deliver these lectures at Matscience, and suggested that they would be published in the Matscience Publication Series; Venkataraman and Adhikari, who attended the Matscience lectures and made the first remarks. Later C. Jadot, M. Laurent, M. Mignotte, M. Huizing and A. Sert proposed some corrections. Then D. Roy sent me many pages of comments, corrected several inacurracies and improved some results.

My journey in India was supported by the National Board for Higher Mathematics. I am very thankful to S. Seshadri from the SPIC Foundation (Madras) and M.S. Raghunathan from Tata Institute Bombay who arranged this visit.

Paris, September 1992.

M. Waldschmidt.

1.– INTRODUCTION

We denote by $\overline{Q}$ the algebraic closure of the rational number field $\mathbb{Q}$ into $\mathbb{C}$; hence $\overline{Q}$ is the field of (complex) algebraic numbers. Further, let $\mathcal{L}$ be the set of logarithms of non-zero algebraic numbers, that is the inverse image of the multiplicative group $\overline{Q}^*$ by the exponential map:

$$\mathcal{L} = \{\ell \in \mathbb{C}\,;\, e^\ell \in \overline{Q}^*\}.$$

It is convenient to write $\ell = \log \alpha$ when $\alpha = e^\ell$, but of course for a given $\alpha \in \overline{Q}^*$ the set of ℓ with $\alpha = e^\ell$ is a whole class of $\mathbb{C}$ modulo $2i\pi\mathbb{Z}$.

It's plain that $\mathcal{L}$ is a $\mathbb{Q}$-vector subspace of $\mathbb{C}$; however it's not a $\overline{Q}$-vector space: the product of a logarithm of an algebraic number by an algebraic number is usually not a logarithm of an algebraic number. This remark, which goes back to Euler, is the root of our subject.

The main (if not the more general) statement of these lectures is the following:

Theorem 1.1 (Baker). — *If $\ell_1, \ldots, \ell_m$ are $\mathbb{Q}$-linearly independent elements of $\mathcal{L}$, then they are $\overline{Q}$-linearly independent.*

This result was proved by Alan Baker in 1966. The first part of these lectures is devoted to a complete and comparatively easy proof of this statement. However the present tex is by no means an introduction to Baker's method: the main new idea in Baker's transcendence proof is an ingenious, rather involved, extrapolation argument, which is performed on the derivatives of an auxiliary function. Here you will see no auxiliary function, no derivatives, no extrapolation. The proof of the first part is quite elementary; the only analytic argument which is used is Schwarz lemma for a function of a single variable. The most sophisticated tool is Bézout's theorem which is used in the following form (see lemma 5.6 in Chapter 5):

if $P_1, \ldots, P_h$ are polynomials in $\mathbb{C}[z_1, \ldots, z_n]$ of total degree $\leq D$, and if the set S of common zeroes in $\mathbb{C}^n$ of these polynomials is finite, then $\mathrm{Card} S \leq D^n$.

Apart from this result, everything is very easy: we use an argument of Michel Laurent to estimate a determinant; an analytic estimate (Chapter 4) provides an upper bound, an arithmetic estimate, namely Liouville's inequality (Chapter 3) implies that this determinant vanishes, and a zero estimate (which relies on Bézout's above mentioned theorem) provides the conclusion.

In the second part of these lectures we repeat the proof more carefully in order to prove explicit measures of linear independence of logarithms of algebraic numbers. The first estimate we produce (Chapter 7) is rather crude, but the proof follows closely the arguments in Part 1 and is rather transparent. The result we achieve is certainly far from the best known, but it is good enough to be useful for solving explicitly certain classes of Diophantine equations (we do not develop this aspect here).

We refine this rough estimate in Chapter 10; the refinement involves a better zero estimate, due to Philippon (Chapter 8, by Damien Roy), and improved results on interpolation determinants (Chapter 9, where an argument dual to Baker's one is developed, and also an idea of M. Laurent is used). The best known measures of linear independence of logarithms of algebraic numbers are stated in Chapter 12.

There is an extension, also due to Baker, of Theorem 1.1 to non-homogeneous linear combinations of logarithms: under the hypotheses of Theorem 1.1, the numbers $1, \log \alpha_1, \ldots, \log \alpha_m$ are linearly independent over $\bar{\mathbb{Q}}$ (Chapter 11). This statement does not include all that is known on the transcendence of the values of the usual complex exponential function. Specifically, it does not include the so-called *six exponentials theorem* (see §4 below). Chapter 13 is mainly devoted to a general result, the *linear subgroup theorem,* which generalizes at the same time the six exponentials theorem, Baker's theorem by Schneider's method and Baker's theorem by Gel'fond-Baker method. We do not give complete proofs (nor even do we state the result in the most general form) ; this will be postponed hopefully for another more advanced monograph. Chapter 14 deals with conjectures, including Schanuel's conjecture and the conjecture on the algebraic independence of logarithms of algebraic numbers, together with some consequences.

In this first chapter we give some historical background on Baker's theorem, both in the qualitative and in the quantitative form, and we describe the six exponentials theorem.

1Historical survey In his "Introductio in analysin infinitorum", L. Euler defined the exponential and logarithm functions, and said:

From what we have seen, it follows that the logarithm of a number will not be a rational number unless the given number is a power of the base a. That is, unless the number b is a power of the base a, the logarithm of b cannot be expressed as a rational number. In case b is a power of the base a, then the logarithm of b cannot be an irrational number. If, indeed, $\log b = \sqrt{n}$*, then* $a^{\sqrt{n}} = b$*, but this is impossible if both a and b are rational. It is especially desirable to know the logarithms of rational numbers, since from these it is possible to find the logarithms of fractions and also surds. Since the logarithms of numbers which are not the powers of the base are neither rational nor irrational, it is with justice that they are called transcendental quantities. For this reason, logarithms are said to be transcendental.*

(Reference: Euler, Introduction to Analysis of the Infinite, Book 1, Chap. VI, N° 105, Springer-Verlag 1988, p.80.)

Later in 1900, D. Hilbert proposed this question as the seventh of his problems:

The expression α^β *for an algebraic base* α *and an irrational algebraic exponent* β*, e.g. the number* $2^{\sqrt{2}}$ *or* $e^\pi = i^{-2i}$*, always represents a transcendental or at least an irrational number.*

This problem was solved in 1934 by A.O. Gel'fond and Th. Schneider, independently and simultaneously:

Theorem 1.2 (Gel'fond-Schneider). — *If* ℓ_1, ℓ_2 *are* $\mathbb{Q}$*-linearly independent elements of* $\mathcal{L}$*, then they are* $\overline{Q}$*-linearly independent.*

This means that the quotient ℓ_1/ℓ_2 of two non-zero elements of $\mathcal{L}$ is either a rational or a transcendental number; it cannot be an algebraic irrational number, like $\sqrt{2}$. The connection with Hilbert's problem is most easily seen by stating Theorem 1.2 as follows:

if ℓ *and* β *are two complex numbers with* $\ell \neq 0$ *and* $\beta \notin \mathbb{Q}$*, then one at least of the three numbers* e^ℓ*,* β *and* $e^{\beta\ell}$ *is transcendental.*

Hence, if α is a non zero algebraic number, $\log\alpha$ any non-zero logarithm of α, and β an irrational algebraic number, then $\alpha^\beta = \exp(\beta\log\alpha)$ is a transcendental number. The transcendence of e^π is obtained also by the choice of $\alpha = 1$, $\log\alpha = 2i\pi$ and $\beta = -i/2$.

In his book [G], Gel'fond emphasized the importance of getting a generalization of this statement to more than two logarithms (see below). This problem was solved in 1966 by A. Baker; the qualitative aspect of his result is Theorem 1.1. From Baker's theorem, one deduces that if a number of the form

$$\alpha_1^{\beta_1}\cdots\alpha_n^{\beta_n} = \exp\{\beta_1\log\alpha_1 + \cdots + \beta_n\log\alpha_n\}$$

(with algebraic α_i and β_i, $\alpha_i \neq 0$) is algebraic, then either the numbers $\log\alpha_1, \ldots, \log\alpha_n$ all vanish, or else the numbers $1, \beta_1, \ldots, \beta_n$ are linearly dependent over $\mathbb{Q}$.

1Equivalent statements Baker's result obviously generalizes the theorem of Gel'fond-Schneider (just take $n = 2$). As pointed out by J-P. Serre in his Bourbaki lecture on Baker's work (*), it means that the natural map from $\bar{\mathbb{Q}} \otimes_{\mathbb{Q}} \mathcal{L}$ in $\mathbb{C}$, which extends the injection from $\mathcal{L}$ to $\mathbb{C}$, is still injective (see exercise 3). We shall say that $\mathcal{L}$ *and* $\overline{Q}$ *are linearly disjoint over* $\mathbb{Q}$.

The only linear dependence relations, with algebraic coefficients, between logarithms of algebraic numbers, are the trivial ones, like

$$\log 24 = \sqrt{3}\log 9 + \left(1 - 2\sqrt{3}\right)\log 3 + \sqrt{2}\log 4 + (3 - 2\sqrt{2})\log 2.$$

Roughly speaking, if Baker's result were not true, then a vanishing non-trivial linear combination of elements ℓ of $\mathcal{L}$ with algebraic coefficients β and *minimal length* would have the property that the coefficients β's are linearly independent over $\mathbb{Q}$, and at the same time the ℓ's also are linearly independent over $\mathbb{Q}$. More precisely one can state Theorem 1.1 in several equivalent ways:

(*) Travaux de Baker, Sém. Bourbaki 1969/70, n° 368; Springer Lecture Notes **180** (1971), 73–86.

Lemma 1.3. — *Let $k \subset K$ be two fields, $\mathcal{E}$ be a K-vector space, and $\mathcal{M}$ be a k-vector subspace in $\mathcal{E}$. The three following statements are equivalent.*

(i) Let $m \geq 1$; let $\ell_1, \ldots, \ell_m$ be elements of $\mathcal{M}$ which are linearly independent over k; then these elements are also linearly independent over K in $\mathcal{E}$.

(ii) Let $m \geq 1$ be a positive integer. Let $\ell_1, \ldots, \ell_m$ be elements of $\mathcal{M}$, not all vanishing, and let $\beta_1, \ldots, \beta_m$ be k-linearly independent elements of K. Then

$$\beta_1\ell_1 + \ldots + \beta_m\ell_m \neq 0.$$

(iii) Let $m \geq 1$ be a positive integer. Let $\ell_1, \ldots, \ell_m$ be k-linearly independent elements of $\mathcal{M}$ and $\beta_1, \ldots, \beta_m$ be k-linearly independent elements of K. Then

$$\beta_1\ell_1 + \ldots + \beta_m\ell_m \neq 0.$$

When these properties are satified, $\mathcal{M}$ and K are said to be *linearly disjoint over k*.

Proof. We first remark that the implication *(i)* $\Rightarrow$ *(iii)* is trivial.

a) *Proof of (ii)* $\Rightarrow$ *(i).* Assume that for some $m \geq 1$ we have a relation $\beta_1\ell_1 + \ldots + \beta_m\ell_m = 0$ with $\beta_1, \ldots, \beta_m$ not all zero. Let $\beta'_1, \ldots, \beta'_s$ (with $0 < s \leq m$) be a basis of the k-vector space they span; we can write

$$\beta_i = \sum_{j=1}^{s} c_{ij}\beta'_j \qquad (1 \leq i \leq m),$$

with $c_{ij} \in k$, which do not all vanish. Then

$$\sum_{j=1}^{s} \beta'_j \left(\sum_{i=1}^{m} c_{ij}\ell_i \right) = 0.$$

Since $\beta'_1, \ldots, \beta'_s$ are k-linearly independent, we deduce from *(ii)*

$$\sum_{i=1}^{m} c_{ij}\ell_i = 0 \qquad \text{for } 1 \leq j \leq s.$$

Therefore $\ell_1, \ldots, \ell_m$ are k-linearly dependent.

b) *Proof of (iii)* $\Rightarrow$ *(ii).* Assume $\beta_1\ell_1 + \cdots + \beta_m\ell_m = 0$ with $\beta_1, \ldots, \beta_m$ linearly independent over k in K and $\ell_1, \ldots, \ell_m$ in $\mathcal{M}$. We shall argue by induction on m and conclude $\ell_1 = \cdots = \ell_m = 0$. Renumbering $\ell_1, \ldots, \ell_m$ if necessary, we may assume that $\ell_1, \ldots, \ell_r$ (for some r with $0 \leq r \leq m$) is a basis of the k-vector space spanned by $\ell_1, \ldots, \ell_m$:

$$\ell_i = \sum_{j=1}^{r} c_{ij}\ell_j, \qquad (r+1 \leq i \leq m),$$

where c_{ij} are in k. We deduce

$$\sum_{j=1}^{r} \gamma_j\ell_j = 0 \qquad \text{with} \qquad \gamma_j = \beta_j + \sum_{i=r+1}^{m} c_{ij}\beta_i, \quad (1 \leq j \leq r).$$

Using *(iii)* (with m replaced by r), we deduce from the linear independence of $\ell_1, \ldots, \ell_r$ over k that the r elements $\gamma_1, \ldots, \gamma_r$ are k-linearly dependent in K; however, since $\beta_1, \ldots, \beta_m$ are linearly independent over k, the only possibility is $r = 0$, which means $\ell_1 = \cdots = \ell_m = 0$. □

When $k = \mathbb{Q}$, $K = \overline{Q}$, $\mathcal{M} = \mathcal{L}$ and $\mathcal{E} = \mathbb{C}$, assertion *(i)* is nothing but Baker's Theorem 1.1 (see §11.1 for another application of this lemma 1.3). Other statements which are equivalent to Baker's Theorem 1.1 are given in exercise 5 (and will be used in Chapter 13).

1Lower bounds for the distance between 1 and a product of powers of rational integers Baker's theorem shows that numbers of the form

$$\beta_1 \log \alpha_1 + \cdots + \beta_m \log \alpha_m$$

(with algebraic β_i and α_i, $1 \le i \le m$) can vanish only in trivial cases. The most important aspect of the theory is that the proof provides explicit lower bounds for such non-zero numbers. We explain these results in the easiest case, namely $\beta_i \in \mathbb{Z}$, $\alpha_i \in \mathbb{Z}$, $\alpha_i \ge 2$.

Let $a_1, \ldots, a_m$ be rational integers which are ≥ 2 and $b_1, \ldots, b_m$ rational integers. We assume

$$a_1^{b_1} \cdots a_m^{b_m} \ne 1,$$

and we ask for a lower bound for the distance between these two numbers.

There is a trivial estimate: a non-zero rational number is at least as large as the inverse of a denominator:

$$\begin{aligned} \left|a_1^{b_1} \cdots a_m^{b_m} - 1\right| &\ge \prod_{b_i<0} a_i^{b_i} \\ &\ge \exp\left\{-\sum_{i=1}^{m} |b_i| \log a_i\right\} \\ &\ge \exp\bigl\{-mB \log A\bigr\}, \end{aligned}$$

where $B = \max\{|b_1|, \ldots, |b_m|\}$ and $A = \max\{a_1, \ldots, a_m\}$. This kind of estimate extends to algebraic α's; we shall call it *Liouville's inequality* (see Chapter 3 §5).

The dependence in m and A in Liouville's inequality is sharp, but the main interest for applications is with the dependence in B. In order to see what can be expected, it is convenient to give a connection with lower bounds for linear forms in logarithms. If

$$0 < \left|a_1^{b_1} \cdots a_m^{b_m} - 1\right| \le \frac{1}{2},$$

then

$$\frac{1}{2}\bigl|b_1 \log a_1 + \cdots + b_m \log a_m\bigr| \le \left|a_1^{b_1} \cdots a_m^{b_m} - 1\right| \le 2\bigl|b_1 \log a_1 + \cdots + b_m \log a_m\bigr|$$

(see exercise 1 at the end of this chapter). Therefore it is equivalent to give a lower bound for the distance between 1 and the product $a_1^{b_1} \cdots a_m^{b_m}$, or to give a lower bound for the non vanishing linear form $b_1 \log a_1 + \cdots + b_m \log a_m$.

An easy application of the Dirichlet box principle (see exercise 2) now yields:

Lemma 1.4. — *Let m, $a_1, \ldots, a_m$ be rational integers, all of which are ≥ 2. Define $A = \max\{a_1, \ldots, a_m\}$. Then for every integer $B \ge 2m \log A$, there exist rational integers $b_1, \ldots, b_m$ with*

$$0 < \max_{1 \le i \le m} |b_i| \le B$$

such that

$$\left|a_1^{b_1} \cdots a_m^{b_m} - 1\right| \le \frac{2m \log A}{B^{m-1}}.$$

In particular, if $a_1, \ldots, a_m$ are multiplicatively independent, then the left hand side does not vanish. The upper bound is polynomial in $1/B$, while Liouville's inequality is exponential in $-B$. We shall see that, as far as the dependence in B is concerned, lemma 1.4 is closer to the truth than Liouville's lower bound.

In 1935, one year after he had solved Hilbert's seventh problem, Gel'fond used his transcendence method in order to derive a lower bound for a linear combination of two logarithms of algebraic numbers with algebraic coefficients. Let us give a simple example of such an estimate: for a_1, a_2 multiplicatively independent positive rational integers, and for $\epsilon > 0$, there exists a constant $C_1 = C_1(a_1, a_2, \epsilon)$, which can be explicitly computed, such that, for all $(b_1, b_2) \in \mathbb{Z}^2$ with $(b_1, b_2) \ne 0$, if we set $B = \max\{|b_1|, |b_2|, 2\}$, then

$$\left|a_1^{b_1} a_2^{b_2} - 1\right| \ge C_1 \exp\bigl\{-(\log B)^{5+\epsilon}\bigr\}.$$

In 1939 Gel'fond refined the estimate and replaced the exponent $5+\epsilon$ by $3+\epsilon$, and in 1949 he reached $2+\epsilon$. At the same time he gave an estimate which is valid for any $m \ge 2$ (see [G] Th. 3):

Theorem 1.5 (Gel'fond's ineffective estimate). — *For every m-tuple $(a_1, \dots, a_m)$ of positive multiplicatively independent rational integers, and for every $\delta > 0$, there exists a positive constant $C_2 = C_2(a_1, \dots, a_m, \delta)$ such that, if $b_1, \dots, b_m$ are rational integers, not all of which are zero, and if we set $B = \max\{|b_1|, \dots, |b_m|, 2\}$, then*

$$\left|a_1^{b_1} \cdots a_m^{b_m} - 1\right| \geq C_2 \exp\{-\delta B\}.$$

For the proof of Theorem 1.5, the main tool is a result of Diophantine approximation, which we shall take for granted; Gel'fond used a result of his own, which was a refinement of earlier results due to Thue, Siegel and Dyson; here, for simplicity, we shall use the stronger result due to Roth (see [S], [L] or [B]):

Theorem 1.6 (Thue-Siegel-Roth). — *Let α be an algebraic number and let ϵ be a positive real number. There exists a number $C_0 = C_0(\alpha, \epsilon) > 0$ such that for any rational number p/q with $q > 0$ and $p/q \neq \alpha$,*

$$\left|\alpha - \frac{p}{q}\right| > C_0 q^{-2-\epsilon}.$$

Proof of Theorem 1.5.
We shall use Theorem 1.6 with $\epsilon = 1$:

$$\left|\alpha - \frac{p}{q}\right| > C_0(\alpha, 1)/q^3.$$

Let $\delta > 0$. Assume C_2 does not exist: for each real number $C > 0$ there exists $b = (b_1, \dots, b_m) \in \mathbb{Z}^m$ with

$$0 < \left|a_1^{b_1} \cdots a_m^{b_m} - 1\right| \leq C \exp\{-\delta B\}$$

(where, as usual, $B = \max\{2, |b_1|, \dots, |b_m|\}$). Hence the set E_1 of $b \in \mathbb{Z}^m$ for which

$$0 < \left|a_1^{b_1} \cdots a_m^{b_m} - 1\right| \leq \exp\{-\delta B\}$$

is infinite. Let N be a positive integer satisfying $N > (6m/\delta) \log A$, with $A = \max\{a_i\}$. Since the set $(\mathbb{Z}/N\mathbb{Z})^m$ is finite, there is an infinite subset E_2 of E_1 having all elements in the same class modulo N; this means that there exists $r \in \mathbb{N}^m$ with $0 \leq r_i < N$, $(1 \leq i \leq m)$ such that, for all $b \in E_2$,

$$b_i \equiv r_i \mod N \quad (1 \leq i \leq m).$$

Let E_3 be the set of $b \in E_2$ with $B \geq N$; once more this is an infinite set. For each $b \in E_3$, there is a $x \in \mathbb{Z}^m$ such that

$$b_i = r_i + N x_i \quad (1 \leq i \leq m).$$

We have $|x_i| \leq 1 + B/N \leq 2B/N$, $(1 \leq i \leq m)$. Let us define two rational numbers $s = a_1^{r_1} \cdots a_m^{r_m}$ and $t = a_1^{x_1} \cdots a_m^{x_m}$. Notice that s does not depend on $b \in E_3$, while t depends on $b \in E_3$. From the construction of E_3 we deduce

$$0 < \left|st^N - 1\right| \leq e^{-\delta B}.$$

We now use the estimate $|x - 1| \leq |x^N - 1|$ which is valid for all $x > 0$ (the number $1 + x + \cdots + x^{N-1}$ is at least 1):

$$0 < \left|s^{1/N} t - 1\right| \leq e^{-\delta B}.$$

This shows that the rational number t is close to the algebraic number $\alpha = s^{-1/N}$ which is the real N-th root of $1/s$:

$$0 < |t - \alpha| \leq \alpha e^{-\delta B}.$$

Since the denominator of t is at most $A^{2mB/N}$, Theorem 1.6 yields:

$$|t - \alpha| \geq C_0(\alpha, 1) A^{-6mB/N}.$$

Combining the upper and lower bound, we deduce the estimate

$$B\left(\delta - \frac{6m\log A}{N}\right) \le -\log C_0(\alpha,1) - \frac{1}{N}\log s,$$

which shows that the number B is bounded (the numbers δ, A, N, $C_0(\alpha,1)$ and s do not depend on $b \in E_3$), which is in contradiction with the fact that E_3 is an infinite set. □

This proof does not enable one to compute the constant C_2, because one uses the Thue-Siegel-Roth theorem which is not effective.

Gel'fond used his Theorem 1.5 in several Diophantine questions, in particular (with Linnik) for Gauss' problem of determining all imaginary quadratic number fields with class number one; he also applied his lower bound to the study of several types of Diophantine equations. In his book [G] published in 1952, he said (p.126 of the English edition):

> *... one can assume the fundamental problem in the analytic theory of transcendental numbers to be that of strengthening the analytic methods in the theory of transcendental numbers, so that it will be possible to apply them to the investigation of the behaviour of linear forms in n logarithms of algebraic numbers.*

Also, p.177:

> *Nontrivial lower bounds for linear forms, with integral coefficients, of an arbitrary number of logarithms of algebraic numbers, obtained effectively by methods of the theory of transcendental numbers, will be of extraordinarily great significance in the solution of very difficult problems of modern number theory. Therefore, one may assume, as was already mentioned above, that the most pressing problem in the theory of transcendental numbers is the investigation of the measures of transcendence of finite sets of logarithms of algebraic numbers.*

As we said earlier, this problem was solved in 1966 by A. Baker. A refinement due to N.I. Fel'dman two years later gives

$$\left|a_1^{b_1}\cdots a_m^{b_m} - 1\right| \ge \exp\big\{-C_3\log B\big\},$$

where $C_3 = C_3(a_1,\dots,a_m)$ is a positive effectively computable number. This number C_3 has been explicitly computed; one of the best known value today (see Chapter 12 where further information is given) is

$$C_3 = 2^{4m+16}m^{3m+5}\log a_1\cdots\log a_m.$$

This bound has been computed by means of the method which is described in the present lectures (however an auxiliary function was introduced, in place of Laurent's determinant). The second part of Lang's book [L] deals with lower bounds for linear combinations in logarithms (either for the usual exponential function, or else for elliptic functions). The introduction to chapters 10 and 11 (p.212–217) proposes far reaching conjectures; for instance, for any $\epsilon > 0$, there should exist a constant $C_4(\epsilon) > 0$ such that

$$\left|a_1^{b_1}\cdots a_m^{b_m} - 1\right| \ge \frac{C_4(\epsilon)^m}{B^{m-1+\epsilon}A^{m+\epsilon}}.$$

We come back to this question in Chapter 14.

1The six exponentials theorem Let us start with an easy question: *which are the real numbers t for which* 2^t *is a rational integer ?* Of course all $t \in \mathbb{N}$ satisfy this requirement; but there are others: for $a \in \mathbb{N}$, $a \ne 0$, if we set $t = \log a/\log 2$, then $2^t = \exp(t\log 2) = a \in \mathbb{N}$. Hence

$$\{t \in \mathbb{R}; 2^t \in \mathbb{N}\} = \left\{\frac{\log a}{\log 2}\,;\, a \in \mathbb{N},\, a > 0\right\}.$$

If we denote this set by E_1, then $E_1 \cap \mathbb{Q} = \mathbb{N}$.

We consider now the set

$$E_2 = \{t \in \mathbb{R}\,;\, 2^t \in \mathbb{N} \text{ and } 3^t \in \mathbb{N}\}.$$

This set contains $\mathbb{N}$ and is contained in E_1. In particular $E_2 \cap \mathbb{Q} = \mathbb{N}$. The following problem is still open: *is-it true that* $E_2 = \mathbb{N}$*?* This means:

Problem.– *Does there exist an irrational number which belongs to* E_2 *?*
This question amounts to ask whether there exist two positive integers a and b such that

$$\frac{\log a}{\log 2} = \frac{\log b}{\log 3}$$

and at the same time this quotient is irrational. Another equivalent formulation it to ask whether a 2×2 matrix

$$\begin{pmatrix} \log a & \log b \\ \log 2 & \log 3 \end{pmatrix}$$

(with positive integers a and b) can be singular without a being a power of 2. We shall soon see this question in a more general setting (the four exponentials conjecture).

Finally we introduce a third set

$$E_3 = \{t \in \mathbb{R}\,;\, 2^t \in \mathbb{N},\ 3^t \in \mathbb{N} \text{ and } 5^t \in \mathbb{N}\}.$$

Of course we have $\mathbb{N} \subset E_3 \subset E_2 \subset E_1$. We have the following transcendence result: $E_3 = \mathbb{N}$.

It's possible to replace the integers 2, 3 and 5 by any set of three multiplicatively independent (complex) algebraic numbers ; in this case there is no need to restrict the problem to real values of t.

The following result is due to Siegel (unpublished), Lang and Ramachandra (1967):

Theorem 1.7 (six exponentials theorem). — *Let* $x_1, \dots, x_d$ *be complex numbers which are linearly independent over* $\mathbb{Q}$ *and let* $y_1, \dots, y_\ell$ *be also complex numbers which are linearly independent over* $\mathbb{Q}$. *Assume* $\ell d > \ell + d$. *Then one at least of the* ℓd *numbers*

$$\exp(x_i y_j), \qquad (1 \le i \le d,\ 1 \le j \le \ell)$$

is transcendental.

It is clear that the interesting case is $\ell = 2$, $d = 3$ (or $\ell = 3$, $d = 2$, which gives the same result because of the symmetry), and this explains the name of the result.

One conjectures that the conclusion is still valid under the weaker hypothesis $\ell d \ge \ell + d$: this is the *four exponentials conjecture:*

Conjecture 1.8 (four exponentials). — *Let* x_1, x_2 *be two* $\mathbb{Q}$*-linearly independent complex numbers and* y_1, y_2 *also two* $\mathbb{Q}$*-linearly independent complex numbers. Then one at least of the* 4 *numbers*

$$\exp(x_i y_j), \qquad (i = 1, 2,\ j = 1, 2)$$

is transcendental.

The six exponentials theorem occurs for the first time in a paper by L. Alaoglu and P. Erdős : On highly composite and similar numbers, Trans. Amer. Math. Soc. **56** (1944), 448–469; when these authors try to prove Ramanujan's assertion that the quotient of two consecutive *superior highly composite numbers* (*) is a prime, they need to know that if x is a real number such that p_1^x and p_2^x are both rational numbers, with p_1 and p_2 distinct prime numbers, then x is an integer; however this statement (special case of the four exponentials conjecture) is yet unproved; they quote Siegel and claim that x indeed is an integer if one assumes p_i^x to be rational for *three* distinct primes p_i; this is just a special case of the six exponentials

(*) Ramanujan defines an integer n to be a *superior highly composite number* if there exists $\epsilon > 0$ such that the divisor function $d(n)$ (number of divisors of n) satisfies $d(m)m^{-\epsilon} < d(n)n^{-\epsilon}$ for $m \neq n$; for further references, see for instance M. Waldschmidt, Some transcendental aspects of Ramanujan's work, Proc. Ramanujan Cent. Intern. Conf., Annamalainagar Dec. 1987, Ramanujan Math. Soc., **1** (1988), 67–76.

theorem. They deduce that the quotient two consecutive superior highly composite numbers is either a prime, or else a product of two primes.

The six exponentials theorem can be deduced from a very general (and complicated) result of Schneider (Ein Satz über ganzwertige Funktionen als Prinzip für Transzendenzbeweise, Math. Ann. **121** (1949), 131–140). The four exponentials conjecture is equivalent to the first of the eight problems at the end of Schneider's book [S]. An explicit statement of the six exponentials conjecture, together with a proof, has been published independently and at about the same time by S. Lang and K. Ramachandra:

– S. Lang, Nombres transcendants, Sém. Bourbaki 18ème année (1965/66), N° 305; Algebraic values of meromorphic functions, 2, Topology **5** (1966), 363–370; see also [L] Chap.2.
– K. Ramachandra, Contributions to the theory of transcendental numbers, Acta Arith. **14** (1968), 65–88; see also [R] Chap.2.

They both formulated the four exponentials conjecture explicitly.

We shall come back on this subject in part 3 of these lectures (Chapters 13 and 14).

1Exercises **1.** Let z be a complex number. Write $\Re z$ for the real part of z.
a) For any $\delta > 0$, the condition $|\Re z| \le \delta$ implies

$$|e^z - 1| \le \frac{e^\delta - 1}{\delta}|z|,$$

hence

$$|e^z - 1| \le |z|e^\delta.$$

`Hint.` *For* $x = \Re z$,

$$\left|\int_0^1 e^{tz}dt\right| \le \int_0^1 e^{tx}dt.$$

b) For any $0 \le \theta < 1$, the condition $|e^z - 1| \le \theta$ implies, for the principal value of the complex logarithm,

$$|\log z| \le \frac{1}{1-\theta}\,|z-1|\,.$$

`Hint.` *Check that, for any* $t \in \mathbb{R}$ *satisfying* $t \ge -\theta$, *the following upper bound holds:*

$$|\log(1+t)| \le \frac{|t|}{1-\theta}.$$

c) Let $\vartheta \in \mathbb{R}$ and $v, w \in \mathbb{C}$ satisfy

$$|we^{-v} - 1| \le \vartheta \qquad \text{and} \qquad 0 \le \vartheta < 1.$$

Show that there exists $\ell \in \mathbb{C}$ with $e^\ell = w$ and

$$|\ell - v| \le \frac{1}{1-\vartheta}|we^{-v} - 1|.$$

`Hint.` *Define* $\ell = v + \log(we^{-v})$ *where* log *is the principal value of the logarithm.*

2. Complete the proof of lemma 1.4 by applying the pigeonhole principle to the points

$$b_1 \log a_1 + \cdots b_m \log a_m, \qquad (0 \le b_i \le B,\ 1 \le i \le m)$$

which all lie in the interval $[0, mB\log A]$.
`Hint.` *Check* $B^{m-1}\log 2 \ge m \log A$ *and use exercise* 1a *with* $\delta = \log 2$.

3. Write a shorter proof of lemma 1.3: show that the statements *(i)*, *(ii)* and *(iii)* are also equivalent to:
(iv) The natural map $\mathcal{M} \otimes_k K \to \mathcal{E}$, which extends the injection from $\mathcal{M}$ to $\mathcal{E}$, is still injective.

`Hint.` *Let $(\mu_i)_{i\in I}$ be a basis of the k-vector space $\mathcal{M}$, and let $(\gamma_j)_{j\in J}$ be a basis of the k-vector space K. Then $\mu_i\otimes\gamma_j$, $(i\in I,\ j\in J)$ is a basis of $\mathcal{M}\otimes_k K$ over k:*

$$\begin{aligned}\mathcal{M}\otimes_k K &= \left\{\sum_{i\in I}\mu_i\otimes\beta_i\,;\quad \beta_i\in K\quad \textit{with}\quad \operatorname{supp}(\beta_i)_{i\in I}\quad \textit{finite}\right\}\\ &= \left\{\sum_{j\in J}\lambda_j\otimes\gamma_j\,;\quad \lambda_j\in\mathcal{M}\quad \textit{with}\quad \operatorname{supp}(\lambda_j)_{j\in J}\quad \textit{finite}\right\}\\ &= \left\{\sum_{i\in I}\sum_{j\in J}c_{ij}\mu_i\otimes\gamma_j\,;\quad c_{ij}\in K\quad \textit{with}\quad \operatorname{supp}(c_{ij})_{i\in I,j\in J}\quad \textit{finite}\right\},\end{aligned}$$

where finite support *means that all but finitely many elements vanish.*

The map $\mathcal{M}\otimes_k K\to\mathcal{E}$ is nothing but

$$\sum_{i\in I}\mu_i\otimes\beta_i\longmapsto\sum_{i\in I}\mu_i\beta_i,\qquad \sum_{j\in J}\lambda_j\otimes\gamma_j\longmapsto\sum_{j\in J}\lambda_j\gamma_j$$

as well as

$$\sum_{i\in I}\sum_{j\in J}c_{ij}\mu_i\otimes\gamma_j\longmapsto\sum_{i\in I}\sum_{j\in J}c_{ij}\mu_i\gamma_j.$$

4. Let $k\subset K$ be two fields and $\mathcal{V}$ be a vector subspace of K^d. Show that the following conditions are equivalent:
(*i*) $\mathcal{V}$ is intersection of hyperplanes which are defined by linear forms with coefficients in k.
(*ii*) $\mathcal{V}$ has a basis whose elements belong to k^d.
(*iii*) There exists a surjective linear map $K^d\longrightarrow K^r$ with kernel $\mathcal{V}$ whose matrix (in the canonical bases) has coefficients in k.

Such a subspace $\mathcal{V}$ is called rational over k.

5. Show that Theorem 1.1 is also equivalent to:
(i) Let d be a positive integer; let $\mathcal{V}$ be a subspace of $\mathbb{C}^d$ which is rational over $\overline{Q}$ *(see exercise* 4*)* such that $\mathcal{V}\cap\mathbb{Q}^d=0$. Then $\mathcal{V}\cap\mathcal{L}^d=0$.
(ii) Let ℓ, d be positive integers and $\lambda_1,\dots,\lambda_\ell$ be $\mathbb{Q}$-linearly independent elements in $\mathcal{L}^d$. Then $\lambda_1,\dots,\lambda_\ell$ are $\overline{Q}$-linearly independent.

`Hint.` *The implication (ii)* $\Rightarrow$ Theorem 1.1 *is clear (take $d=1$).*

For the proof of Theorem 1.1 $\Rightarrow$ *(i), write $\mathcal{V}$ as intersection of $\overline{Q}$-rational hyperplanes; for $(\ell_1,\dots,\ell_d)\in\mathcal{V}\cap\mathcal{L}^d$, choose a basis of the $\mathbb{Q}$-vector subspace of $\mathbb{C}$ spanned by $\ell_1,\dots,\ell_d$.*

For the proof of (i) $\Rightarrow$ (ii), assume $\beta_1\lambda_1+\cdots+\beta_\ell\lambda_\ell=0$; choose a basis $\gamma_1,\dots,\gamma_r$ of the $\mathbb{Q}$-vector subspace of $\mathbb{C}$ spanned by $\beta_1,\dots,\beta_\ell$, and use (iv) with d replaced by dr.

6. (1972 Putnam Prize competition). Using the *calculus of finite differences*, show that, if $t\in\mathbb{R}$ is such that $n^t\in\mathbb{Z}$ for all $n\geq 1$, then $t\in\mathbb{N}$.
`Hint. First method` (cf. H. Halberstam. – Transcendental numbers; The Mathematical Gazette **58** (1976), 276–284.)
Let a be a non-negative integer; assume

$$n^t\in\mathbb{Z},(n+1)^t\in\mathbb{Z},\cdots,(n+a)^t\in\mathbb{Z}$$

for infinitely many $n\geq 1$, with $0\leq t<a$; we have to prove $t\in\{0,1,\dots,a-1\}$. For τ a positive integer, consider the Taylor series expansion of $(d/dx)^\tau(X-1)^a$ at the origin:

$$\sum_{i=0}^{a}(-1)^i\binom{a}{i}i^\tau=\begin{cases}0 & \textit{for } 0\leq\tau<a,\\ (-1)^a a! & \textit{for } \tau=a.\end{cases}$$

Deduce that, for infinitely many $n > 0$, the number

$$u_n = \sum_{i=0}^{a} (-1)^i \binom{a}{i} (n+i)^\tau$$

is an integer. Check also that

$$u_n = (-1)^a t(t-1)\cdots(t-a+1)n^{t-a} + O(n^{t-a-1})$$

and deduce the desired statement.

`Second method -- Balasubramanian.`
Let $N \geq 1$ be an integer; define $f(x) = (N+x)^t$. Show (by induction on k) that the k-th difference

$$\big(\Delta_k f\big)(x) = \big(\Delta_{k-1} f\big)(x+1) - \big(\Delta_{k-1} f\big)(x)$$

for $k \geq 1$, with $\big(\Delta_0 f\big)(x) = f(x)$, is

$$\big(\Delta_k f\big)(x) = \int_0^1 \cdots \int_0^1 f^{(k)}(x + t_1 + \cdots + t_k) dt_1 \cdots dt_k$$

(where $f^{(k)}$ is the k-th derivative of f). Choose $k = [t] + 3$; show that there exists a real number $u_0 = u_0(t, N) > 0$ such that

$$|f^{(k)}(u)| \leq u^{-2} \qquad \text{for} \quad u > u_0.$$

Deduce $\big(\Delta_k f\big)(n) = 0$ for $n \in \mathbb{N}$ sufficiently large. Since $f^{(k)}$ maintains the same sign on the real positive numbers, deduce that $f^{(k)} = 0$, hence f is a polynomial and $t \in \mathbb{N}$.

1References for Chapter 1 One of the first books on transcendental numbers is
[G] A.O. Gel'fond. – *Transcendental Number Theory;* Moscow, 1952; English transl. Dover Publ., N.Y., 1960.

Here is another reference of the same period of time:
[S] Th. Schneider. – *Einführung in die transzendenten Zahlen;* Springer Verlag 1957; trad. franç., *Introduction aux Nombres Transcendants*, Paris, Gauthier-Villars.

A further reference including a solution of Hilbert's seventh problem by boths methods of Schneider and Gel'fond is
[R] K. Ramachandra. – *Lectures on transcendental numbers;* The Ramanujan Institute, Vol. 1, Univ. of Madras, 1969.

A condensed exposition of the main results which were known ten years ago can be found in
[B] A. Baker. – *Transcendental Number Theory;* (Cambridge Univ. Press, 2nd ed. 1979)
The first chapter introduces rather old and very short proofs of classical results: Liouville, Hermite–Lindemann and Lindemann–Weierstrass. The second chapter contains a proof of Baker's theorem.

A review of classical proofs of the transcendence of the number e and π is given in the appendix of
[M] K. Mahler. – *Lectures on Transcendental Numbers;* Springer Lecture Notes in Math., **546** (1976).

The first book which introduced the subject in a general setting (starting with the usual exponential function, and going up to commutative algebraic groups) in a clear and understandable way is
[L] S. Lang. – *Introduction to Transcendental Numbers;* Addison-Wesley 1966.
It's still a good reference, in spite of many corrections which should be made.

The methods which we are going to use just started to grow ten years ago. See for instance:
[W1] M. Waldschmidt. – *Transcendence Methods;* Queen's Papers in Pure and Applied Math., **52** (1979).

Another introduction to Schneider's method (Chapter 2), Gel'fond's method (Chapter 3) and Baker's method (Chapter 8) is given in:
[W2] M. Waldschmidt. – *Nombres Transcendants;* Springer Lecture Notes in Math., **402** (1974).
Chapter 1 of this last reference contains a few prerequisites dealing with algebraic number theory and complex function theory. But we shall repeat all that we need in this lectures.

A detailed study of the history of irrational and transcendental numbers during the 18th and 19th centuries has been written recently:
M. Serfati. – *Quadrature du Cercle, Fractions Continues et autres Contes;* Fragments d'histoire des Mathématiques 4, Brochure A.P.M.E.P. N°86, 1992.

2.– SKETCH OF THE PROOF

The aim of the first part of these lectures (Chapters 2 to 6) is to give a complete proof of Baker's Theorem 1.1. In the present chapter we introduce the main ideas of the proof.

Throughout this chapter, the notations will be as follows: $\log\alpha_1,\dots,\log\alpha_{n+1}$ are $\mathbb{Q}$-linearly independent elements of $\mathcal{L}$ (which means that $\alpha_i=\exp(\log\alpha_i)$ is algebraic), and $\beta_1,\dots,\beta_n$ are algebraic numbers.

Assuming

$$\log\alpha_{n+1}=\beta_1\log\alpha_1+\cdots+\beta_n\log\alpha_n,$$

we want to deduce that $1,\beta_1,\dots,\beta_n$ are $\mathbb{Q}$-linearly dependent. As we saw in lemma 1.3, this will imply Baker's Theorem 1.1.

We first give a sketch of the proof, then we provide more details in the special case where $n=1$ (this is Gel'fond-Schneider's theorem) and $\log\alpha_1$, $\beta=\beta_1$ are both real numbers. Hence we prove that if $\beta\log\alpha_1=\log\alpha_2$ belongs to $\mathcal{L}$ (which means $\alpha_2\in\overline{Q}$), then β is rational. As an example one gets the transcendence of numbers like $2^{\sqrt{2}}$ and $\log 2/\log 3$. We shall use Liouville's estimate whose proof will be given only later in Chapter 3.

1Schneider's method with interpolation determinants We shall work with the following $n+1$ functions of n variables:

$$z_1,\dots,z_n,\alpha_1^{z_1}\cdots\alpha_n^{z_n},$$

where, of course, $\alpha_1^{z_1}\cdots\alpha_n^{z_n}$ stands for $\exp(z_1\log\alpha_1+\cdots+z_n\log\alpha_n)$. The main point is that these functions take algebraic values at all the points of the form

$$(s_1+s_{n+1}\beta_1,\dots,s_n+s_{n+1}\beta_n),\qquad (s_1,\dots,s_{n+1})\in\mathbb{Z}^{n+1}.$$

The set of these points is a finitely generated subgroup of $\mathbb{C}^n$, which we write

$$Y=\mathbb{Z}^n+\mathbb{Z}(\beta_1,\dots,\beta_n).$$

Another important property of our functions is that they are algebraically independent: if P is a non-zero polynomial in $n+1$ variables (with, say, complex coefficients), then the function

$$F(z_1,\dots,z_n)=P\big(z_1,\dots,z_n,\alpha_1^{z_1}\cdots\alpha_n^{z_n}\big)$$

does not vanish identically (exercise 3). The classical sketch of proof in transcendental number theory involves the construction of an auxiliary polynomial P (with algebraic coefficients) such that the associated function F has many zeroes (for several points y of Y). Here, following M. Laurent, we shall not construct such an auxiliary function, but we shall only consider the matrix which is associated to the system of equations $F(y)=0$.

For brevity, we write $\underline{s}$ for $(s_1,\dots,s_{n+1})\in\mathbb{Z}^{n+1}$. When S is a positive real number, we define $\mathbb{Z}^{n+1}(S)$ as the set of $\underline{s}$ in $\mathbb{Z}^{n+1}$ with $|s_i|<S$, $(1\le i\le n+1)$; this set has $\big(2[S]-1\big)^{n+1}$ elements.

We need to choose a large integer S; how large it should be can be explicitly specified, but it's sufficient here to say that it must be large compared with finitely many quantities arising from the data $\log\alpha_i$ and β_i (namely their degrees, and also the maximum absolute value of the coefficients of their minimal polynomials). Also we need two more parameters, say L_0 and L_1, which correspond to the degree in the n first variables, and in the last one, respectively, of the polynomial P above. The matrix which we are going to consider will be

$$\Big((s_1+s_{n+1}\beta_1)^{\lambda_1}\cdots(s_n+s_{n+1}\beta_n)^{\lambda_n}\big(\alpha_1^{s_1}\cdots\alpha_{n+1}^{s_{n+1}}\big)^{\lambda_{n+1}}\Big)_{\underline{\lambda},\underline{s}},$$

where the index of row is, say, $\underline{\lambda}$, and the index of columns is $\underline{s}$; (the ordering of the rows or columns will be irrelevant: we shall be interested only in the rank of this matrix); $\underline{\lambda}$ runs over the $(n+1)$-tuples $(\lambda_1,\dots,\lambda_{n+1})$ of elements in $\mathbb{N}^{n+1}$ satisfying $\lambda_1+\cdots+\lambda_n\le L_0$ and $\lambda_{n+1}\le L_1$; hence the number of rows is $\binom{L_0+n}{n}(L_1+1)$. On the other hand $\underline{s}$ runs over the $(n+1)$-tuples in $\mathbb{Z}^{n+1}(S)$, hence there are $(2S-1)^{n+1}$ columns. We shall choose our parameters in such a way that $(2S-1)^{n+1}\ge\binom{L_0+n}{n}(L_1+1)$.

The proof can be divided in two parts: in the first one, which is the purely transcendental part, we shall prove that our matrix has rank strictly less than the number $L:=\binom{L_0+n}{n}(L_1+1)$. In the second part, which is of a geometric nature (*zero estimate*), we show that this condition on the rank of the matrix implies the desired linear dependence condition on $1,\beta_1,\dots,\beta_n$.

Details on the second part of the proof are given in Chapter 5 for the general case; a simple example is worked out in §2 below.

Let us now consider more closely the first part. We consider any determinant Δ of a $L\times L$ matrix out of the above matrix. This means that we have a subset of $\underline{s}$'s, and we can write

$$\Delta=\det\left((s_1+s_{n+1}\beta_1)^{\lambda_1}\cdots(s_n+s_{n+1}\beta_n)^{\lambda_n}\left(\alpha_1^{s_1}\cdots\alpha_{n+1}^{s_{n+1}}\right)^{\lambda_{n+1}}\right)_{\underline{\lambda},\underline{s}}.$$

We want to prove that Δ vanishes. We first bound $|\Delta|$ from above: $|\Delta|\le\epsilon$ for some value of ϵ which we shall compute in terms of L_0, L_1 and S (and it is convenient to take these parameters sufficiently large to perform these computations). This upper bound for $|\Delta|$ arises from a lemma, due to Michel Laurent, which concerns all *interpolation matrices* (see Chapter 4; a simple case is explained below in lemma 2.2); indeed we can write

$$\Delta=\det\left(f_{\underline{\lambda}}(s_1+s_{n+1}\beta_1,\dots,s_n+s_{n+1}\beta_n)\right)_{\underline{\lambda},\underline{s}},$$

where, for $\underline{\lambda}=(\lambda_1,\dots,\lambda_{n+1})\in\mathbb{Z}^{n+1}$, we define

$$f_{\underline{\lambda}}=z_1^{\lambda_1}\cdots z_n^{\lambda_n}\left(\alpha_1^{z_1}\cdots\alpha_n^{z_n}\right)^{\lambda_{n+1}}.$$

As we shall see in Chapter 4, the upper bound for $|\Delta|$ follows from Schwarz lemma for functions of a single variable.

Next we deduce from the upper bound that Δ vanishes; this is a simple application of Liouville's inequality, which is explained in Chapter 3. This will complete the transcendental part of the proof.

1The zero estimate for the real case of Gel'fond-Schneider's theorem We consider here the second part of the proof, namely the zero estimate. In the case $n=1$, one can use analytic arguments and derive results on exponential polynomials in one variable. We only give one easy example of such a result, which involves real functions of one real variable. This will enable us to show that if β is an irrational real number and $\log\alpha$ a non-zero real number, then the matrix

$$\left((s_1+s_2\beta)^{\lambda_0}\left(\alpha^{s_1+s_2\beta}\right)^{\lambda_1}\right)_{(\lambda_0,\lambda_1),(s_1,s_2)}\qquad\text{with}\qquad\begin{cases}0\le\lambda_0\le L_0, & 0\le\lambda_1\le L_1,\\ |s_1|<S, & |s_2|<S\end{cases}$$

is of rank $(L_0+1)(L_1+1)$ as soon as $(L_0+1)(L_1+1)\le(2S-1)^2$. This plainly means that if $P\in\mathbb{C}[X,Y]$ is a non-zero polynomial of degree at most L_0 in X and L_1 in Y, then the function of a single variable $F(z)=P(z,\alpha_1^z)$ cannot vanish at all the points $s_1+s_2\beta$ for $(s_1,s_2)\in\mathbb{Z}^2(S)$. This is where we need the assumption that $\log\alpha$ and β are both real numbers; also the argument we are going to use does not seem to give anything in the case $n\ge2$.

The following result was already used in a similar context by A.O.Gel'fond and Yu.V.Linnik in Chapter 12 (*Transcendance de quelques classes de nombres* p.221–228) of [GL]. See also problem 75, Part V of Chapter 1 in [PS].

Lemma 2.1. — *Let $a_1,\dots,a_n$ be polynomials in $\mathbb{R}[t]$ of degrees $d_1,\dots,d_n$, and let $w_1,\dots,w_n$ be pairwise distinct real numbers. Then the real function of one real variable*

$$F(t)=\sum_{i=1}^n a_i(t)e^{w_it}$$

has at most $d_1 + \cdots + d_n + n - 1$ real zeroes.

In this result the zeroes are counted with multiplicities (this is important for the proof, which will be by induction); however, for our application, we need only an upper bound for the number of distinct real zeroes. It's also interesting to remark that simple arguments from linear algebra show that the upper bound in lemma 2.1 is best possible (see exercises 1 and 2 at the end of this Chapter). Further related exercises are given in Chapter 6 of [W] (in particular exercise 6.1.c of [W] where interpolation determinants are explicitly computed).

Proof. We prove this lemma by induction on the integer $k := d_1 + \cdots + d_n + n$. In the case $k = 1$, then $n = 1$ and the result is obvious. Assume $k \geq 2$. After multiplication of F by $e^{-w_n t}$, we may assume $w_n = 0$. Hence $w_i \neq 0$ for $1 \leq i < n$. If F has at least N real zeros, then (Rolle) its derivative F' has at least $N - 1$ real zeros. However, since $w_n = 0$, we have

$$F'(t) = \sum_{i=1}^{n-1} \tilde{a}_i(t) e^{w_i t} + (d/dt) a_n(t)$$

where

$$\tilde{a}_i = w_i a_i + (d/dt) a_i$$

is a polynomial of degree exactly d_i for $1 \leq i < n$, and $d_n - 1$ for $i = n$ (we consider here that the zero polynomial is of degree -1). One uses the induction hypothesis which yields $N - 1 \leq d_1 + \cdots + d_n + n - 2$, hence N is bounded as claimed. □

1The interpolation determinant in one variable We now come back to the proof of Gel'fond-Schneider theorem. The upper bound for $|\Delta|$ is slightly easier in the case $n = 1$.

We shall say that a complex function of one variable is *analytic in a closed disk $|z| \leq R$ of $\mathbb{C}$* if it is continuous on this disk and analytic inside.

Lemma 2.2. —*Let r and R be two real numbers with $0 < r \leq R$, $f_1, \ldots, f_L$ be functions of one complex variable, which are analytic in the disc $|z| \leq R$ of $\mathbb{C}$, and let $\zeta_1, \ldots, \zeta_L$ belong to the disk $|z| \leq r$. Then the determinant*

$$\Delta = \det \begin{pmatrix} f_1(\zeta_1) & \cdots & f_L(\zeta_1) \\ \vdots & \ddots & \vdots \\ f_1(\zeta_L) & \cdots & f_L(\zeta_L) \end{pmatrix}$$

is bounded from above by

$$|\Delta| \leq \left(\frac{R}{r}\right)^{-L(L-1)/2} L! \prod_{\lambda=1}^{L} |f_\lambda|_R.$$

As usual, we have denoted by $|f|_R$ the number $\sup\{|f(z)|\,;\, |z| \leq R\}$ when f is analytic in the disk $\{z \in \mathbb{C}\,;\, |z| \leq R\}$ of $\mathbb{C}$. Notice also that the conclusion is trivial in the case $R = r$.

Proof. The determinant $\Psi(z)$ of the matrix $\Big(f_\lambda(\zeta_\mu z)\Big)$ is a function of one complex variable which is analytic in the disk $|z| \leq R/r$. We shall prove that it has a zero of multiplicity at least $L(L-1)/2$ at the origin; then, using Schwarz lemma, one deduces

$$|\Delta| = |\Psi(1)| \leq \left(\frac{R}{r}\right)^{-L(L-1)/2} |\Psi|_{R/r}.$$

The trivial upper bound

$$|\Psi|_{R/r} \leq L! \prod_{\lambda=1}^{L} |f_\lambda|_R$$

gives the desired conclusion.

Let us come back to our claim on the order of vanishing of Ψ at the origin. Each f_λ can be written as the sum of its Taylor series; since the determinant is multilinear, one reduces the problem to the cases where $f_\lambda(z) = z^{n_\lambda}$; in this case

$$\Psi(z) = z^{n_1+\cdots+n_L} \det\Big(\zeta_\mu^{n_\lambda}\Big);$$

if $\Psi(z)$ does not vanish identically, then the n_μ are pairwise distinct, and we get a factor $z^{L(L-1)/2}$, which is what we wanted. □

1Proof of the real case of Gel'fond-Schneider theorem Let $\ell_1 \in \mathcal{L} \cap \mathbb{R}$ and $\beta \in \overline{Q} \cap \mathbb{R}$ be such that $\ell_2 = \beta\ell_1$ also belong to $\mathcal{L}$. Define $\alpha_i = e^{\ell_i}$, $(i = 1, 2)$, so that $\alpha_i \in \overline{Q}^*$ and $\alpha_1^\beta = \alpha_2$. We want to prove that β is rational.

We denote by c a sufficiently large real number. A suitable value for c can be easily computed once the proof is completed; it depends only on ℓ_1 and β (and involves also the algebraic number α_2). Next we choose three rational integers L_0, L_1 and S which are subject to the following conditions:

$$L_0 \geq 2, \qquad L_1 \geq 2, \qquad S \geq 2,$$

$$cL_0 \log S \leq L, \qquad cL_1 S \leq L, \qquad L \leq (2S-1)^2,$$

with $L = (L_0+1)(L_1+1)$. For instance one can take

$$L_1 = [\log S]^2 \qquad \text{and} \qquad L_0 = [S^2(\log S)^{-3}]$$

with S sufficiently large.

Let $\underline{s}^{(1)}, \ldots, \underline{s}^{(L)}$ be any elements in $\mathbb{Z}^2(S)$. We consider the $L \times L$ determinant

$$\Delta = \det\left((s_1^{(\mu)} + s_2^{(\mu)}\beta)^{\lambda_0} \left(\alpha_1^{s_1^{(\mu)}} \alpha_2^{s_2^{(\mu)}}\right)^{\lambda_1}\right)_{\underline{\lambda},\mu}$$

with $\underline{\lambda} = (\lambda_0, \lambda_1)$, $(0 \leq \lambda_0 \leq L_0, 0 \leq \lambda_1 \leq L_1)$, and with $1 \leq \mu \leq L$. We use lemma 2.2 with $r = S(1+|\beta|)$, $R = e^2 r$ and

$$f_\lambda(z) = z^{\lambda_0}\alpha_1^{\lambda_1 z}, \qquad \zeta_\mu = s_1^{(\mu)} + s_2^{(\mu)}\beta.$$

We bound $\log|f_\lambda|_R$ by $L_0 \log R + L_1 R|\ell_1|$; hence

$$\begin{aligned}\log|\Delta| &\leq -L(L-1) + \log(L!) + LL_0 \log R + LL_1 R|\ell_1| \\ &\leq -L^2 + c_1 L(L_0 \log S + L_1 S),\end{aligned}$$

where c_1 (like c_2 below) is a positive constant which can be easily computed in terms of ℓ_1 and β.

Our choice of the parameters L_0, L_1 and S shows that the dominating term in the right hand side is $-L^2$. More precisely, we get

$$\log|\Delta| \leq -L^2/2$$

provided that $c > 5c_1$, say, and that L is sufficiently large.

We shall show in the next Chapter (lemma 3.15) that if Δ does not vanish, then

$$\log|\Delta| \geq -c_2 L(L_0 \log S + L_1 S).$$

Again, assuming c sufficiently large with respect to c_2, we conclude $\Delta = 0$. This shows that the matrix

$$\left((s_1+s_2\beta)^{\lambda_0}\left(\alpha_1^{s_1+s_2\beta}\right)^{\lambda_1}\right)_{(\lambda_0,\lambda_1),(s_1,s_2)}, \qquad \text{with} \qquad \begin{cases} 0 \leq \lambda_0 \leq L_0, & 0 \leq \lambda_1 \leq L_1, \\ |s_1| < S, & |s_2| < S \end{cases}$$

is of rank $< L$. From lemma 2.1 we conclude that the points $s_1 + s_2\beta$, $(|s_1| < S, |s_2| < S)$ are not pairwise distinct, hence β is rational. □

1Exercises **1.**
a) Let $w_1, \dots, w_n$ distinct real numbers, $d_1, \dots, d_n$ non-negative rational integers, and $u_1, \dots, u_N$ distinct real numbers, with $N = d_1 + \cdots + d_n + n - 1$. Show that there exist polynomials $a_1, \dots, a_n$ in $\mathbb{R}[t]$, of degrees $d_1, \dots, d_n$ respectively, such that the function

$$F(t) = \sum_{i=1}^{n} a_i(t) e^{w_i t}$$

satisfies $F(u_1) = \cdots = F(u_N) = 0$.
`Hint.` *Use lemma* 2.1 *as well as linear algebra.*
b) Give also a generalization where the u_j are no more distinct, but multiplicities are required.
`Hint.` *See* [W] *Exercise* 6.1.a.

2. (Algebraic version of lemma 2.1: upper bound for the number of consecutive integral zeroes of an exponential polynomial.)

Let K be a field, $\alpha_1, \dots, \alpha_n$ non-zero elements of K which are pairwise distinct, and $a_1, \dots, a_n$ non-zero polynomials in $K[X]$, of degrees say $d_1, \dots, d_n$. Then the function $\mathbb{Z} \longrightarrow K$ which is defined by

$$F(m) = \sum_{i=1}^{n} a_i(m) \alpha_i^m$$

cannot vanish on a set of $d_1 + \cdots + d_n + n$ consecutive integers.

3. For $u = (u_1, \dots, u_n)$ and $z = (z_1, \dots, z_n)$ in $\mathbb{C}^n$, define $u \cdot z = u_1 z_1 + \cdots + u_n z_n$. Let $w_1, \dots, w_t$ be pairwise distinct elements of $\mathbb{C}^n$. Show that the t functions $e^{w_1 \cdot z}, \dots, e^{w_t \cdot z}$ are algebraically independent over the field $\mathbb{Q}(z_1, \dots, z_n)$: if $P \in \mathbb{C}[X_1, \dots, X_n, Y_1, \dots, Y_t]$ is a non-zero polynomial in $n + t$ variables, then the function

$$P\big(z_1, \dots, z_n, e^{w_1 \cdot z}, \dots, e^{w_t \cdot z}\big)$$

is not identically zero.
`Hint.` *Use induction on* t *like in the proof of lemma* 2.1.

4. The above proof of Gel'fond-Schneider's theorem requires the hypothesis that $\log \alpha$ and β are *real* algebraic numbers only because of lemma 2.1. Complete the proof in the complex cases by using the following result of Tijdeman (see for instance [W]):

Let $a_1, \dots, a_n$ be polynomials in $\mathbb{C}[t]$ of degrees $d_1, \dots, d_n$, and let $w_1, \dots, w_n$ pairwise distinct complex numbers. Define $\Omega = \max\{|w_1|, \dots, |w_n|\}$. Then the number of zeroes of the function

$$F(z) = \sum_{i=1}^{n} a_i(z) e^{w_i z}$$

in the disk $|z| \le R$ of $\mathbb{C}$ is at most $2(d_1 + \cdots + d_n + n - 1) + 5R\Omega$.

5. Compute explicitly a suitable value for c in the proof of §4.

1References
[GL] A.O.Gel'fond and Yu.V.Linnik. – *Analytic methods in analytic number theory;* trad. franç.: *"Méthodes élémentaires dans la théorie analytique des nombres";* Gauthier Villars 1965.
[L] M.Laurent. – Sur quelques résultats récents de transcendance; Journées arithmétiques Luminy 1989, Astérisque, **198**–**200** (1991), 209–230.
[PS] G.Pólya and G.Szegő. – *"Problems and theorems in analysis";* Volume 2, Springer Verlag (Grund. der Math. Wiss. **216**, 1976).
[W] M.Waldschmidt. – *Nombres transcendants;* Springer Lecture Notes **402** (1974).

3.– HEIGHTS – LIOUVILLE INEQUALITY

A non-zero rational integer has absolute value at least 1; a non-zero rational number has absolute value at least the inverse of a denominator. Liouville's inequality is an extension of these estimates and provides a lower bound for a non-zero algebraic number. More specifically, we are given finitely many (fixed) algebraic numbers $\gamma_1, \dots, \gamma_q$, and we have a polynomial $P \in \mathbb{Z}[X_1, \dots, X_q]$ which does not vanish at the point $(\gamma_1, \dots, \gamma_q)$; the algebraic number we want to estimate from below is $P(\gamma_1, \dots, \gamma_q)$. The lower bound must depend explicitly on the degrees of P, as well as on an upper bound for the absolute values of its coefficients.

In order to do so, we introduce a notion of height for an algebraic number. We study this height with somewhat more details than are strictly necessary, because it's an important tool in many situations.

1 p-adic valuation and p-adic absolute values over $\mathbb{Q}$ For $x \in \mathbb{Q}$, $x \neq 0$, we write the decomposition of x into a product of prime factors as follows

$$x = \pm \prod_p p^{v_p(x)}.$$

This defines, for each prime number p, a map v_p from $\mathbb{Q}^*$ to $\mathbb{Z}$, which we extend by $v_p(0) = \infty$. The map $v_p : \mathbb{Q} \longrightarrow \mathbb{Z} \cup \{\infty\}$ thus obtained is the *p-adic valuation* over $\mathbb{Q}$; it satisfies the following properties :

(i) for $x \in \mathbb{Q}$, $v_p(x) = \infty$ is equivalent to $x = 0$
(ii) for $(x, y) \in \mathbb{Q}^2$, $v_p(xy) = v_p(x) + v_p(y)$
(iii) for $(x, y) \in \mathbb{Q}^2$, $v_p(x + y) \geq \min\{v_p(x), v_p(y)\}$.

To v_p is associated an absolute value $|\ |_p$, which is the map from $\mathbb{Q}$ to $\mathbb{Q}$ defined

$$|x|_p = p^{-v_p(x)}.$$

The *p-adic absolute value* satisfies the following properties :

(i) for $x \in \mathbb{Q}$, $|x|_p = 0$ is equivalent to $x = 0$
(ii) for $(x, y) \in \mathbb{Q}^2$, $|xy|_p = |x|_p |y|_p$
(iii) for $(x, y) \in \mathbb{Q}^2$, $|x + y|_p \leq \max\{|x|_p, |y|_p\}$.

This p-adic absolute value defines a distance on $\mathbb{Q}$, hence a topology. The ball of center $a \in \mathbb{Q}$ and radius p^{-r} (with $r \in \mathbb{Z}$) :

$$\mathcal{D}(a, r) = \{x \in \mathbb{Q}\,;\, |x - a|_p \leq p^{-r}\} = \{x \in \mathbb{Q}\,;\, v_p(x - a) \geq r\}$$

is the set of rational numbers x such that the difference $x - a$ is divisible by p^r, i.e. such that $x - a$ is the product of p^r by a rational number with denominator not divisible by p; for $r \geq 1$, this means that the numerator of $x - a$ (written as a quotient of two coprime integers) is congruent to 0 modulo p^r. This is why p-adic numbers are useful for the study of congruences.

Writing, as usual, by $|\ |$ the usual absolute value on $\mathbb{Q}$, we have the *product formula*

$$|x| \prod_p |x|_p = 1 \qquad \text{for all } x \in \mathbb{Q}^*,$$

which can also be written additively :

$$\sum_p v_p(x) \log p = \log |x| \qquad \text{for all } x \in \mathbb{Q}^*.$$

1The absolute logarithmic height (Weil) We denote by $\bar{\mathbb{Q}}$ an algebraic closure of $\mathbb{Q}$. Here, we do not consider this field $\bar{\mathbb{Q}}$ as a subfield of $\mathbb{C}$, but we consider all the possible embeddings.

A *number field* is a subfield k of $\mathbb{C}$ which, considered as a vector space over $\mathbb{Q}$, is of finite dimension; this dimension is denoted by $[k:\mathbb{Q}]$ and is called the *degree* of k (over $\mathbb{Q}$).

Two absolute values on k are said to be *equivalent* if they define the same topology on k; a *place* of k is an equivalence class of non trivial absolute values. Let $|\ |$ be a non-trivial absolute value on k. The restriction of this absolute value to $\mathbb{Q}$ is equivalent either to the usual absolute value on $\mathbb{Q}$ (in this case the absolute value $|\ |$ is called *Archimedean*), or else to a p-adic absolute value (in this case the absolute value $|\ |$ is said to be *ultrametric*).

In each equivalence class v we choose the representative $|\ |_v$ which is normalized by

$$\begin{cases} |x|_v = x & \text{if } x \in \mathbb{Q},\ x > 0, \text{ and } v \text{ is Archimedean,} \\ |p|_v = 1/p & \text{if } v \text{ extends the } p\text{-adic valuation of } \mathbb{Q}. \end{cases}$$

We write $v \mid \infty$ if v is Archimedean, and $v \mid p$ if v extends the p-adic valuation. We denote by M_k (resp. M_k^∞) the set of normalized absolute values (resp. Archimedean normalized absolute values) of k. For $v \in M_k$, k_v will be the completion of k at the place v. The completion of $\mathbb{Q}$ for the p-adic valuation is the field $\mathbb{Q}_p$ of p-adic numbers.

According to the *theorem of the primitive element* (see exercise 1), a number field has a *generator* : there exists an algebraic number $\alpha \in k$ such that $k = \mathbb{Q}(\alpha)$. Denote by

$$f(X) = a_0 X^d + \cdots + a_d \in \mathbb{Z}[X]$$

the *minimal polynomial* of α : f is irreducible in $\mathbb{Z}[X]$ (this means that f is irreducible in $\mathbb{Q}[X]$ and the rational integers $a_0, \ldots, a_n$ are relatively prime), $f(\alpha) = 0$ and $a_0 > 0$.
a) Let $\alpha_1, \ldots, \alpha_d$ be the roots of f in $\mathbb{C}$. There are d embeddings of k into $\mathbb{C}$, which are given by

$$\begin{array}{ccc} k & \longrightarrow & \mathbb{C} \\ \alpha & \longmapsto & \alpha_i \end{array}$$

$(1 \le i \le d)$. To each embedding $\sigma : k \longrightarrow \mathbb{C}$ we associate an absolute value $|\ |_\sigma$ by $|\gamma|_\sigma = |\sigma(\gamma)|$. We obtain by this way all the Archimedean places of k. If $\sigma(\alpha) \in \mathbb{R}$, then $\sigma(k) \subset \mathbb{R}$ and $k_v = \mathbb{R}$; the embedding σ and the place v are called *real*. To a real place v corresponds one and only one real embedding of k; in this case we define $d_v = 1$. If $\sigma(\alpha) \notin \mathbb{R}$, then $k_v = \mathbb{C}$; the embedding σ and the place v are called *complex*; to such a place v correspond two (complex conjugate) embeddings of k into $\mathbb{C}$, and we set $d_v = 2$. Let r_1 be the number of real roots of f and r_2 the number of pairs of conjugate complex roots of f, with $d = r_1 + 2r_2$; then the number of Archimedean places of k is $r_1 + r_2$, and

$$\sum_{v \in M_k^\infty} d_v = d.$$

The numbers $\big(|\alpha_1|, \ldots, |\alpha_d|\big)$ are the same as $\big(|\alpha|_v\,;\, v \in M_k^\infty\big)$ where each $|\alpha|_v$ is repeated d_v times; this can also be written

$$\prod_{i=1}^{d} (X - |\alpha_i|) = \prod_{v \in M_k^\infty} (X - |\alpha|_v)^{d_v}.$$

b) Let p be a prime number. We denote by $\mathbb{C}_p$ the completion of an algebraic closure of $\mathbb{Q}_p$. The absolute value of $x \in \mathbb{C}_p$ is denoted by $|x|_p$. Let $\alpha_1^{(p)}, \ldots, \alpha_d^{(p)}$ be the roots of f in $\mathbb{C}_p$. The embeddings of k into $\mathbb{C}_p$ are given by

$$\begin{array}{ccc} k & \longrightarrow & \mathbb{C}_p \\ \alpha & \longmapsto & \alpha_i^{(p)} \end{array}$$

$(1 \le i \le d)$. To each embedding $\sigma : k \longrightarrow \mathbb{C}_p$ we associate an absolute value $|\ |_\sigma$, which is defined by $|\gamma|_\sigma = |\sigma(\gamma)|_p$. This gives all the places of k above p. Given a place v of k which extends the p-adic absolute

value, there are usually several embeddings σ of k into $\mathbb{C}_p$ to which this place is associated; their number d_v is the *local degree at* v; this is the degree of the extension $k_v/\mathbb{Q}_p$. Hence

$$d = \sum_{v|p} d_v.$$

The numbers $\big(|\alpha_1^{(p)}|_p, \dots, |\alpha_d^{(p)}|_p\big)$ are the same as the numbers $\big(|\alpha|_v\,;\, v \mid p\big)$ where each $|\alpha|_v$ is repeated d_v times; this can be written

$$\prod_{i=1}^{d}(X - |\alpha_i^{(p)}|_p) = \prod_{v|p}(X - |\alpha|_v)^{d_v}.$$

Let again k be a number field of degree d. For each place v of k we have defined a local degree d_v which satisfies

$$\begin{cases} d_v = [k_v : \mathbb{Q}_p] & \text{if } v \mid p, \\ d_v = [k_v : \mathbb{R}] & \text{if } v \in M_k^\infty. \end{cases}$$

The *product formula* reads

$$\prod_{v \in M_k} |x|_v^{d_v} = 1 \qquad \text{for} \quad x \in k,\ x \neq 0.$$

The relations $d = \sum_{v \in M_k^\infty} d_v = \sum_{v|p} d_v$ can be generalized as follows : if k' is a finite extension of k, one defines a map from $M_{k'}$ onto M_k by mapping w onto the restriction v of w on k; one writes : $w \mid v$; then

$$\sum_{w|v} [k'_w : k_v] = [k' : k] \tag{3.1}$$

(cf. for instance [L1] Chap. 2 §1 p.39 cor.1).

Let α be an algebraic number; when k is a number field which contains α, we define

$$\mathrm{h}(\alpha) = \frac{1}{d} \sum_{v \in M_k} d_v \log \max\{1, |\alpha|_v\}.$$

This is the (Weil) *absolute logarithmic height* of the number α. Using (3.1), one checks that it does not depend on the choice of the number field k containing α, but only on α.
Example. For two rational integers a, b which are relatively prime,

$$\mathrm{h}(a/b) = \log \max\{|a|, |b|\}.$$

Property 3.2. — *For algebraic numbers α_1 and α_2,*

$$\mathrm{h}(\alpha_1\alpha_2) \leq \mathrm{h}(\alpha_1) + \mathrm{h}(\alpha_2) \tag{3.3}$$

and

$$\mathrm{h}(\alpha_1 + \alpha_2) \leq \log 2 + \mathrm{h}(\alpha_1) + \mathrm{h}(\alpha_2). \tag{3.4}$$

Moreover, for any algebraic number $\alpha \neq 0$ and for any $n \in \mathbb{Z}$,

$$\mathrm{h}(\alpha^n) = |n|\mathrm{h}(\alpha). \tag{3.5}$$

Proof. The upper bound (3.3) is a consequence of the upper bound

$$\max\{1, xy\} \leq \max\{1, x\} \max\{1, y\} \qquad \text{for all} \ \ x \geq 0,\ y \geq 0,$$

while (3.4) follows from the inequality

$$\max\{1, x+y\} \le 2\max\{1,x\}\max\{1,y\} \qquad \text{for all } \ x \ge 0,\ y \ge 0.$$

Property (3.5) reduces to $\mathrm{h}(\alpha) = \mathrm{h}(1/\alpha)$ for $\alpha \neq 0$, which follows from the product formula, since $\max\{1,x\} = x\max\{1,1/x\}$ for $x > 0$. □

Remark. The term $\log 2$ in the right hand side of the estimate (3.4) cannot be replaced by a smaller absolute constant, as shown by the following example : $\alpha_1 = q/(q-1)$, $\alpha_2 = q/(q+1)$ with q an even integer. Another example is $\alpha_1 = \alpha_2 = 1$.

The next lemma provides an upper bound for the absolute logarithmic height of an algebraic number which is given as the value of a polynomial in algebraic numbers $\gamma_1, \dots, \gamma_q$.

When $f \in \mathbb{C}[X_1, \dots, X_t]$ is a polynomial in t variables, with complex coefficients, we denote by $L(f)$ its *length*, which is the sum of the modulus of its complex coefficients. We shall prove (as a consequence of lemma 3.7 below) the following estimate :

Lemma 3.6. — *Let $f \in \mathbb{Z}[X_1, \dots, X_t]$ be a non-zero polynomial in t variables with rational integer coefficients. Write $\deg_{X_i}$ $(1 \le i \le t)$ for the partial degrees of f. Let $\gamma_1, \dots, \gamma_t$ be algebraic numbers. Then*

$$\mathrm{h}\big(f(\gamma_1, \dots, \gamma_t)\big) \le \log L(f) + \sum_{i=1}^{t} \big(\deg_{X_i} f\big)\mathrm{h}(\gamma_i).$$

For instance, when p_1/q_1 and p_2/q_2 are two rational numbers with $(p_1, q_1) = (p_2, q_2) = 1$ and $q_i > 0$, then lemma 3.6 yields

$$\mathrm{h}\left(\frac{p_1}{q_1} + \frac{p_2}{q_2}\right) \le \log 2 + \log\max\{|p_1|, q_1\} + \log\max\{|p_2|, q_2\}.$$

However, it's more efficient to write $p_1/q_1 = a/c$ and $p_2/q_2 = b/c$ with $\gcd(a,b,c) = 1$ and $c > 0$:

$$\begin{aligned}\mathrm{h}\left(\frac{a}{c} + \frac{b}{c}\right) &\le \log\max\{|a+b|, c\} \\ &\le \log 2 + \log\max\{|a|, |b|, c\}.\end{aligned}$$

This example suggests a refinement of lemma 3.6, using a notion of simultaneous height for several numbers. Let k be a number field of degree d; let $\vartheta_0, \dots, \vartheta_s$ and λ be elements of k with $(\vartheta_0, \dots, \vartheta_s) \neq (0, \dots, 0)$ and $\lambda \neq 0$; from the product formula it follows that the number

$$\frac{1}{d}\sum_{v \in M_k} d_v \log\max\{|\vartheta_0|_v, \dots, |\vartheta_s|_v\},$$

which is attached to the $(s+1)$-tuple $(\vartheta_0, \dots, \vartheta_s) \in k^{s+1}$, is the same as the number

$$\frac{1}{d}\sum_{v \in M_k} d_v \log\max\{|\lambda\vartheta_0|_v, \dots, |\lambda\vartheta_s|_v\},$$

which is attached to the $(s+1)$-tuple $(\lambda\vartheta_0, \dots, \lambda\vartheta_s) \in k^{s+1}$; therefore this number depends only on the class $(\vartheta_0 : \cdots : \vartheta_s)$ of $(\vartheta_0, \dots, \vartheta_s)$ in the projective space $\mathbb{P}_n(k)$; we denote it by $\mathrm{h}(\vartheta_0 : \cdots : \vartheta_s)$. For instance $\mathrm{h}(\alpha) = \mathrm{h}(1 : \alpha)$.

Lemma 3.7. — *Let k be a number field and $s_1, \dots, s_t$ be positive integers; for $1 \leq i \leq t$, let $\gamma_{i1}, \dots, \gamma_{is_i}$ be elements of k; denote by $\underline{\gamma}$ the point $\big(\gamma_{ij}\big)_{1\leq j\leq s_i, 1\leq i\leq t}$ in $k^{s_1+\cdots+s_t}$. Further, let f be a non-zero polynomial in $s_1+\cdots+s_t$ variables, with coefficients in $\mathbb{Z}$, of total degree at most N_i with respect to the s_i variables corresponding to $\gamma_{i1}, \dots, \gamma_{is_i}$. Finally, denote by $L(f)$ the length of f (sum of the absolute values of the coefficients). Then*

$$\mathrm{h}\big(f(\underline{\gamma})\big) \leq \log L(f) + \sum_{i=1}^{t} N_i \mathrm{h}(1 : \gamma_{i1} : \cdots \gamma_{is_i}).$$

We deduce lemma 3.6 by taking $s_i = 1$ for $1 \leq i \leq t$.

Proof. Write

$$f = \sum_{\lambda} p_\lambda \prod_{i=1}^{t} \prod_{j=1}^{s_i} X_{ij}^{\lambda_{ij}},$$

where p_λ are rational integers and $\lambda = (\lambda_{ij})$ runs over a finite subset of $\mathbb{N}^{s_1+\cdots+s_t}$. Let v be a place of k. If v is ultrametric, then

$$\begin{aligned}\log \max\{1, |f(\underline{\gamma})|_v\} &\leq \log \max\left\{1, \max_{\lambda} \prod_{i=1}^{t}\prod_{j=1}^{s_i} |\gamma_{ij}|_v^{\lambda_{ij}}\right\} \\ &\leq \sum_{i=1}^{t} N_i \log \max\{1, |\gamma_{i1}|_v, \dots, |\gamma_{is_i}|_v\}.\end{aligned}$$

If v is Archimedean, then

$$\begin{aligned}\log \max\{1, |f(\underline{\gamma})|_v\} &\leq \log L(f) + \log \max\left\{1, \max_{\lambda} \prod_{i=1}^{t}\prod_{j=1}^{s_i} |\gamma_{ij}|_v^{\lambda_{ij}}\right\} \\ &\leq \log L(f) + \sum_{i=1}^{t} N_i \log \max\{1, |\gamma_{i1}|_v, \dots, |\gamma_{is_i}|_v\}.\end{aligned}$$

Using the relation $\sum_{v\in M_k^\infty} d_v = d$, we easily deduce the conclusion. □

1Mahler's measure Let $f \in \mathbb{C}[X]$ be a non-zero polynomial of degree d with leading coefficient $a_0 > 0$:

$$f(X) = a_0 X^d + a_1 X^{d-1} + \cdots + a_{d-1} X + a_d = a_0 \prod_{i=1}^{d} (X - \alpha_i).$$

The *Mahler's measure* of f is the number

$$\mathrm{M}(f) = a_0 \prod_{i=1}^{d} \max\{1, |\alpha_i|\}.$$

This defines a multiplicative function :

$$\mathrm{M}(f_1 f_2) = \mathrm{M}(f_1)\mathrm{M}(f_2)$$

for f_1 and f_2 in $\mathbb{C}[X]$. Let us check

$$\mathrm{M}(f) = \exp\left(\int_0^1 \log |f(e^{2i\pi t})| dt\right). \tag{3.8}$$

For this, we consider the analytic function

$$g(z) = z^d f(1/z) = a_0 \prod_{i=1}^{d} (1 - \alpha_i z);$$

its zeroes in the unit disk $|z| < 1$ are the $1/\alpha_i$, with $|\alpha_i| > 1$; Jensen's formula (which is easier in the case of polynomials; see for instance [M]) yields

$$\int_0^1 \log|g(e^{2i\pi t})| dt = \log|g(0)| + \sum_{|\alpha_i|>1} \log|\alpha_i|;$$

this proves (3.8).

When α be an algebraic number with minimal polynomial $f \in \mathbb{Z}[X]$, we define its *Mahler's measure* by $\mathrm{M}(\alpha) = \mathrm{M}(f)$.

Lemma 3.9. — *Let α be an algebraic complex number of degree d. Then*

$$\mathrm{h}(\alpha) = \frac{1}{d} \log \mathrm{M}(\alpha).$$

Proof. Denote, as before, by $a_0 > 0$ the leading coefficient of the minimal polynomial of α, by k the number field $\mathbb{Q}(\alpha)$, and, for $v \in M_k$, by d_v the local degree of k at v. Since

$$\mathrm{M}(\alpha) = a_0 \prod_{v \in M_k^\infty} \max\{1, |\alpha|_v\}^{d_v},$$

the desired relation reduces to

$$a_0 = \prod_{v \notin M_k^\infty} \max\{1, |\alpha|_v\}^{d_v}.$$

The product formula

$$a_0 = \prod_p |a_0|_p^{-1}$$

shows that it's sufficient to check

$$|a_0|_p^{-1} = \prod_{v|p} \max\{1, |\alpha|_v\}^{d_v}.$$

Therefore the result reduces to the following lemma:

Lemma 3.10. — *Let p be a prime number; let*

$$f(X) = a_0 X^d + a_1 X^{d-1} + \cdots + a_d$$

be a polynomial of $\mathbb{Z}[X]$ with degree d and $\gcd(a_0, \ldots, a_d) = 1$. Denote by $\alpha_1, \ldots, \alpha_d$ the roots of f in $\mathbb{C}_p$:

$$f(X) = a_0 \prod_{i=1}^{d} (X - \alpha_i).$$

Then

$$|a_0|_p \prod_{i=1}^{d} \max\{1, |\alpha_i|_p\} = 1.$$

Proof. We may assume $|\alpha_1|_p \le \cdots \le |\alpha_d|_p$. Since the a_i are relatively prime, $\max\{|a_0|_p, \dots, |a_d|_p\} = 1$. Let us write a_i/a_0 as a symmetric function of the α_i :

$$\frac{a_i}{a_0} = (-1)^i \sum_{s_1,\dots,s_i} \alpha_{s_1} \cdots \alpha_{s_i} \qquad (1 \le i \le d).$$

If $|\alpha_i|_p \le 1$ for all $i = 1, \dots, d$, then $|a_i|_p \le |a_0|_p$ and $\max\{|a_0|_p, \dots, |a_d|_p\} = |a_0|_p = 1$, which gives the desired result. Otherwise let j, $(1 \le j \le d)$, be such that

$$|\alpha_1|_p \le \cdots \le |\alpha_{j-1}|_p \le 1 < |\alpha_j|_p \le \cdots \le |\alpha_d|_p.$$

Then

$$\max\left\{\left|\frac{a_i}{a_0}\right|_p ; 1 \le i \le d\right\} = \left|\frac{a_{d-j+1}}{a_0}\right|_p = |\alpha_j \cdots \alpha_d|_p = \prod_{i=1}^{d} \max\{1, |\alpha_i|_p\},$$

hence

$$\max\{|a_1|_p, \dots, |a_d|_p\} = |a_0|_p \prod_{i=1}^{d} \max\{1, |\alpha_i|_p\}.$$

Since this number is $\ge |a_0|_p$, we deduce

$$\max\{|a_0|_p, \dots, |a_d|_p\} = |a_0|_p \prod_{i=1}^{d} \max\{1, |\alpha_i|_p\},$$

hence the result. □

Remark 1. When α is an algebraic number, lemma 3.10 shows that α is an algebraic integer if and only if $|\alpha|_v \le 1$ for all ultrametric absolute values of $\mathbb{Q}(\alpha)$.

Remark 2. Let α be an algebraic number with conjugates $\alpha_1, \dots, \alpha_d$. If $D \in \mathbb{Z}$ is such that

$$\left|D \prod_{i \in I} \alpha_i\right|_v \le 1$$

for all subsets I of $\{1, \dots, d\}$ and all ultrametric places v, then

$$|D|_p \prod_{i=1}^{d} \max\{1, |\alpha_i|_p\} \le 1$$

for each prime number p and each embedding of $\mathbb{Q}(\alpha_1, \dots, \alpha_d)$ into $\mathbb{C}_p$; hence $|D|_p \le |a_0|_p$ for each p, which means that a_0 divides D. This shows that a_0 is the positive generator of the ideal of $D \in \mathbb{Z}$ for which, for any subset $\{i_1, \dots, i_t\}$ of $\{1, \dots, d\}$, the number $D\alpha_{i_1} \cdots \alpha_{i_t}$ is an algebraic integer.

Remark 3 (M. Laurent). Let α be a non-zero algebraic number. The ring of integers $\mathbb{Z}_k$ of the number field $k = \mathbb{Q}(\alpha)$ is a Dedekind domain ; the principal fractional ideal (α) can be written $\mathcal{B}/\mathcal{C}$, where $\mathcal{B}$ and $\mathcal{C}$ are non-zero relatively prime integral ideals of k. Let us show that

$$\mathcal{C} = \{\gamma \in \mathbb{Z}_k ; \gamma\alpha \in \mathbb{Z}_k\} \qquad \text{and} \qquad \mathrm{N}\,\mathcal{C} = a_0,$$

where $\mathrm{N}\,\mathcal{C}$ is the absolute norm of the ideal $\mathcal{C}$.

We write

$$(\alpha) = \prod_{\mathcal{P}} \mathcal{P}^{m_{\mathcal{P}}(\alpha)},$$

where $\mathcal{P}$ runs over the set of prime ideals of $\mathbb{Z}_k$. Hence

$$\mathcal{B} = \prod_{\mathcal{P}} \mathcal{P}^{\max\{0, m_{\mathcal{P}}(\alpha)\}}, \qquad \mathcal{C} = \prod_{\mathcal{P}} \mathcal{P}^{\max\{0, -m_{\mathcal{P}}(\alpha)\}}.$$

Recall that the absolute norm $\mathrm{N}\,\mathcal{P}$ of $\mathcal{P}$ is $\mathrm{N}\,\mathcal{P} = \mathrm{Card}(\mathbb{Z}_k/\mathcal{P})$. If $v \in M_k$ is the ultrametric place associated to $\mathcal{P}$ and d_v the local degree, then

$$|\alpha|_v^{d_v} = \mathrm{N}\,\mathcal{P}^{-m_{\mathcal{P}}(\alpha)}$$

(the product of the left hand side for all ultrametric v, as well as the product of the left hand side for all prime ideals $\mathcal{P}$, is $1/|\mathrm{N}\,(\alpha)|$, where $\mathrm{N}\,(\alpha)$ is the norm of α) ; indeed, for $\gamma \in \mathbb{Z}_k$ and $m \geq 1$, we have

$$\gamma \in \mathcal{P}^m \iff |\gamma|_v^{d_v} \leq \mathrm{N}\,\mathcal{P}^{-m}.$$

Using remark 1, we conclude

$$\mathcal{C} = \big\{\gamma \in \mathbb{Z}_k\,;\, |\gamma|_v \leq |\alpha|_v^{-1} \text{ for all ultrametric } v \in M_k\big\} = \big\{\gamma \in \mathbb{Z}_k\,;\, \gamma\alpha \in \mathbb{Z}_k\big\}$$

and

$$\mathcal{B} = \big\{\gamma\alpha\,;\, \gamma \in \mathcal{C}\big\}.$$

Further, by the multiplicativity property of N, we deduce from lemma 3.10:

$$\mathrm{N}\,\mathcal{C} = \prod_{\mathcal{P}} \mathrm{N}\,\mathcal{P}^{\max\{0, -m_{\mathcal{P}}(\alpha)\}} = \prod_{v \text{ ultrametric}} \max\big\{1, |\alpha|_v^{-d_v}\big\} = a_0.$$

1Usual height and size There are several other notions of heights or size (in French : "taille") for algebraic numbers. Here are a few examples, with comparisons. Usually, a good notion of height includes the property that the set of algebraic numbers of bounded height and degree is finite. To give estimates for the number of elements of such sets is also an interesting question (see the reference to Schanuel in [L4]).

The *usual height* $H(f)$ of a polynomial $f(X) = a_0X^d + a_1X^{d-1} + \cdots + a_d \in \mathbb{C}[X]$ is the maximum of the complex modulus of its coefficients :

$$H(f) = \max\{|a_0|, \ldots, |a_d|\}.$$

The *usual height* $H(\alpha)$ of an algebraic number α is the usual height of its minimal polynomial over $\mathbb{Z}$.

The *house* of an algebraic number is the maximum of the modulus of its conjugates in $\mathbb{C}$:

$$\overline{|\alpha|} = \max\{|\alpha_1|, \ldots, |\alpha_d|\}$$

when the minimal polynomial of α is written in $\mathbb{C}[X]$ as

$$f(X) = a_0X^d + \cdots + a_d = a_0 \prod_{i=1}^{d} (X - \alpha_i).$$

The *denominator* $\mathrm{den}(\alpha)$ of α is the positive generator of the ideal of $D \in \mathbb{Z}$ for which $D\alpha$ is an algebraic integer; it is a divisor of a_0.

Among several notions of *size*, the most frequently used is

$$s(\alpha) = \log \max\{\mathrm{den}(\alpha)\,;\, \overline{|\alpha|}\}.$$

Lemma 3.11. — *For $\alpha \in \bar{\mathbb{Q}}$ of degree d, we have*

$$\frac{1}{d}\log H(\alpha) - \log 2 \leq \mathrm{h}(\alpha) \leq \frac{1}{d}\log H(\alpha) + \frac{1}{2d}\log(d+1) \tag{3.12}$$

and

$$\frac{1}{d}s(\alpha) \le \mathrm{h}(\alpha) \le \log \mathrm{den}(\alpha) + \log \max\{1, |\overline{\alpha}|\} \le 2s(\alpha).$$

Proof. Let us write (3.12) in the equivalent form

$$2^{-d}H(\alpha) \le \mathrm{M}(\alpha) \le H(\alpha)\sqrt{d+1};$$

the first of these inequalities is trivial. The second follows from the arithmetico-geometric inequality :

$$\exp\left(\int_0^1 \log|f(e^{2i\pi t})|dt\right) \le \int_0^1 |f(e^{2i\pi t})|dt.$$

Using this bound for f^p, with p positive real, we deduce

$$\mathrm{M}(f) \le \left(\int_0^1 |f(e^{2i\pi t})|^p dt\right)^{1/p}.$$

For $p = 2$ we obtain the desired estimate :

$$\mathrm{M}(f)^2 \le (d+1)H(f)^2.$$

The proof of the second series of inequalities does not involve any difficulty and is left as an exercise. □

1Liouville inequalities The simplest such inequality, from which all other are derived, is

$$|n| \ge 1 \qquad \text{for all } \ n \in \mathbb{Z},\ n \ne 0.$$

We used it already in Chapter 1. One of the most useful is

$$\log|\alpha|_v \ge -[\mathbb{Q}(\alpha) : \mathbb{Q}]\mathrm{h}(\alpha) \tag{3.13}$$

for all $\alpha \in \bar{\mathbb{Q}}$, $\alpha \ne 0$, and all places v of $\mathbb{Q}(\alpha)$. For the proof, we first remark that for all $\alpha \in \bar{\mathbb{Q}}$ (including $\alpha = 0$), we have

$$\log|\alpha|_v \le [\mathbb{Q}(\alpha) : \mathbb{Q}]\mathrm{h}(\alpha);$$

further, if $\alpha \ne 0$, then $\mathrm{h}(\alpha) = \mathrm{h}(\alpha^{-1})$ (see (3.5)).

From lemma 3.7 we now deduce the following statement: *under the hypotheses of lemma 3.7, if the number $f(\underline{\gamma})$ does not vanish, then for all places v of the field k, we have*

$$\log|f(\underline{\gamma})|_v \ge -d\log L(f) - d\sum_{i=1}^{t} N_i \mathrm{h}(1 : \gamma_{i1} : \cdots : \gamma_{is_i}).$$

where $d = [k : \mathbb{Q}]$.

We give a slight refinement, where $d\log L(f)$ is replaced by $(d-1)\log L(f)$ when v is an Archimedean place.

Lemma 3.14 (Liouville inequality). — *Let k be a number field of degree d, v be an Archimedean place of k and $s_1, \dots, s_t$ be positive integers; for $1 \le i \le t$, let $\gamma_{i1}, \dots, \gamma_{is_i}$ be elements of k. Further, let f be a polynomial in $s_1 + \cdots + s_t$ variables, with coefficients in $\mathbb{Z}$, which does not vanish at the point $\underline{\gamma} = (\gamma_{ij})_{1\le j\le s_i, 1\le i\le t}$. Assume f is of total degree at most N_i with respect to the s_i variables corresponding to $\gamma_{i1}, \dots, \gamma_{is_i}$. Finally, denote by $L(f)$ the length of f (sum of the absolute values of the coefficients). Then*

$$\log|f(\underline{\gamma})|_v \ge -(d-1)\log L(f) - d\sum_{i=1}^{t} N_i \mathrm{h}(1 : \gamma_{i1} : \cdots : \gamma_{is_i}).$$

The simplest case $t = 1$, $s_1 = 1$ can be written as follows: *for a polynomial $f \in \mathbb{Z}[X]$ of degree $\leq N$ and an algebraic number $\alpha \in \mathbb{C}$ of degree d which is not a root of f, we have*

$$|f(\alpha)| \geq L(f)^{1-d} e^{-dN\mathrm{h}(\alpha)}$$

(We take for v the Archimedean place associated with the given embedding of $\mathbb{Q}(\alpha)$ in $\mathbb{C}$).

Proof. We write the product formula for $f(\underline{\gamma}) \neq 0$:

$$d_v \log |f(\underline{\gamma})|_v = -\sum_{w \neq v} d_w \log |f(\underline{\gamma})|_w,$$

where w runs over the places of k distinct from v. If w is Archimedean we have

$$\log |f(\gamma)|_w \leq \sum_{i=1}^{t} N_i \log \max\{1, |\gamma_{i1}|_w, \ldots, |\gamma_{is_i}|_w\} + \log L(f);$$

the sum of d_w for w Archimedean and $w \neq v$ is $d - d_v \leq d - 1$. If w is ultrametric, the same estimate holds without the term $\log L(f)$. We conclude the proof by using the bound

$$\sum_{w \neq v} d_w \sum_{i=1}^{t} N_i \log \max\{1, |\gamma_{i1}|_w, \ldots, |\gamma_{is_i}|_w\} \leq d \sum_{i=1}^{t} N_i \mathrm{h}(1 : \gamma_{i1} : \cdots : \gamma_{is_i}).$$

□

Using inequality (3.13) for $\alpha = \beta - (p/q)$ (or, if v is Archimedean, using lemma 3.14 for the polynomial in a single variable $f(X) = qX - p$), we deduce that for each algebraic number β, there exists a constant $c(\beta) > 0$ such that for all $p/q \in \mathbb{Q}$ with $q > 0$ and $p/q \neq \beta$, and for any place v of $\mathbb{Q}(\beta)$, we have

$$\left|\beta - \frac{p}{q}\right|_v \geq \frac{c(\beta)}{\max\{|p|\,;\, q\}^d}$$

with $d = [\mathbb{Q}(\beta) : \mathbb{Q}]$ (and $|p|$ is the usual absolute value of p).

Finally, the *size inequality*

$$\begin{cases} \log |\alpha|_v \geq -(d-1)\log\lceil\alpha\rceil - d\log \mathrm{den}\alpha & \text{if } v \text{ is Archimedean} \\ \log |\alpha|_v \geq -d\log\lceil\alpha\rceil - d\log \mathrm{den}\alpha & \text{if } v \text{ is ultrametric} \end{cases}$$

for all $\alpha \in \bar{\mathbb{Q}}$, $\alpha \neq 0$ is proved by writing

- that the norm over $\mathbb{Q}$ of $\alpha\mathrm{den}(\alpha)$ is a non-zero rational integer if v is Archimedean,
- the product formula for $\alpha\mathrm{den}(\alpha)$ if v is ultrametric.

1Lower bound for a determinant Recall (see §2.1) that for S a positive real number, $\mathbb{Z}^{n+1}(S)$ denotes the set of $n+1$ tuples $\underline{s} = (s_1, \ldots, s_{n+1}) \in \mathbb{Z}^{n+1}$ with $|s_j| < S$ for $1 \leq j \leq n+1$. Now let $S_1, \ldots, S_{n+1}$ be positive real numbers; we write $\underline{S}$ for $(S_1, \ldots, S_{n+1})$ and we denote by $\mathbb{Z}^{n+1}(\underline{S})$ the set of $\underline{s} = (s_1, \ldots, s_{n+1}) \in \mathbb{Z}^{n+1}$ which satisfy $|s_i| < S_i$, $(1 \leq i \leq n+1)$.

Here is a consequence of lemma 3.14:

Proposition 3.15. — *Let $\alpha_1, \ldots, \alpha_{n+1}$ be non-zero algebraic numbers and $\beta_1, \ldots, \beta_n$ be algebraic numbers. Denote by D the degree of the number field $\mathbb{Q}(\alpha_1, \ldots, \alpha_{n+1}, \beta_1, \ldots, \beta_n)$. Let L_0, L_1 and $S_1, \ldots, S_{n+1}$ be positive rational integers; define $L = \binom{L_0+n}{n}(L_1+1)$ and $S = \max\{S_1, \ldots, S_{n+1}\}$. Further let $s^{(1)}, \ldots, s^{(L)}$ be any elements in $\mathbb{Z}^{n+1}(\underline{S})$. Consider the $L \times L$ determinant*

$$\Delta = \det\left((s_1^{(\mu)} + s_{n+1}^{(\mu)}\beta_1)^{\lambda_1} \cdots (s_n^{(\mu)} + s_{n+1}^{(\mu)}\beta_n)^{\lambda_n} \left(\alpha_1^{s_1^{(\mu)}} \cdots \alpha_{n+1}^{s_{n+1}^{(\mu)}}\right)^{\lambda_{n+1}} \right)_{\underline{\lambda},\mu}$$

with $\underline{\lambda} = (\lambda_1, \dots, \lambda_{n+1}) \in \mathbb{N}^{n+1}$, $\lambda_1 + \cdots + \lambda_n \le L_0$ *and* $\lambda_{n+1} \le L_1$ *and with* $1 \le \mu \le L$. *Then either* $\Delta = 0$ *or else*

$$\frac{1}{L}\log|\Delta| \ge -(D-1)\big(L_0\log(2S) + \log L\big) - DL_1\sum_{i=1}^{n+1} S_i \mathrm{h}(\alpha_i) - DL_0\mathrm{h}(1:\beta_1:\cdots:\beta_n).$$

Proof. The number Δ is the value, at the point $(\alpha_1, \dots, \alpha_{n+1}, \alpha_1^{-1}, \dots, \alpha_{n+1}^{-1}, \beta_1, \dots, \beta_n)$, of the polynomial $Q(X_1, \dots, X_{n+1}, Y_1, \dots, Y_{n+1}, Z_1, \dots, Z_n)$, which is defined by

$$Q(\underline{X}, \underline{Y}, \underline{Z}) = \det\Big(Q_{\underline{\lambda},\mu}(\underline{X}, \underline{Y}, \underline{Z})\Big)_{\underline{\lambda},\mu},$$

where

$$Q_{\underline{\lambda},\mu}(\underline{X}, \underline{Y}, \underline{Z}) = \prod_{j=1}^{n}(s_j^{(\mu)} + s_{n+1}^{(\mu)}Z_j)^{\lambda_j}\prod_{i=1}^{n+1}\left(X_i^{\max\{s_i^{(\mu)},0\}}Y_i^{\max\{-s_i^{(\mu)},0\}}\right)^{\lambda_{n+1}}$$

For each $i, \underline{\lambda}, \mu$, the polynomial $Q_{\underline{\lambda},\mu}$ is of degree $\le \lambda_{n+1}\max\{s_i^{(\mu)}, 0\}$ in X_i and of degree $\le \lambda_{n+1}\max\{-s_i^{(\mu)}, 0\}$ in Y_i; moreover each $Q_{\underline{\lambda},\mu}$ is of total degree at most L_0 with respect to the variables $Z_1, \dots, Z_n$; the coefficients are rational integers ; the sum of their absolute values is bounded by

$$L(Q_{\underline{\lambda},\mu}) \le \prod_{j=1}^{n}(|s_j^{(\mu)}| + |s_{n+1}^{(\mu)}|)^{\lambda_j} \le (2S)^{L_0}.$$

It follows easily that the polynomial

$$Q = \sum_{\{\sigma\}}\epsilon(\sigma)\prod_{\mu=1}^{L} Q_{\sigma(\mu),\mu},$$

(where σ runs over the set of bijective maps from $\{1, \dots, L\}$ onto the set of $(\lambda_1, \dots, \lambda_{n+1})$, and $\epsilon(\sigma)$ is $+1$ or -1, and depends on the ordering of the $\underline{\lambda}$'s) is a polynomial of degree in X_i as well as in Y_i at most

$$S_i\sum_{\underline{\lambda}}\lambda_{n+1} \le \frac{1}{2}LL_1S_i,$$

of total degree at most LL_0 with respect to $Z_1, \dots, Z_n$, while its length satisfies

$$L(Q) \le L!(2S)^{LL_0}.$$

We use lemma 3.14 with $t = 2n+3$, $s_1 = \cdots = s_{2n+2} = 1$, $s_{2n+3} = n$, $\gamma_{i1} = \alpha_i$ for $1 \le i \le n+1$, $\gamma_{i1} = \alpha_{i-n-1}^{-1}$ for $n+2 \le i \le 2n+2$ and $\gamma_{2n+3,j} = \beta_j$ for $1 \le j \le n$, $N_i = N_{n+i+1} \le LL_1S_i/2$, $(1 \le i \le n+1)$, $N_{2n+3} = LL_0$, and we use the fact that α_j and α_j^{-1} have the same height. □

1Lower bound for the height An algebraic integer whose complex conjugates are all of modulus ≤ 1 is a root of unity. Indeed, for such an α, the set of α^ℓ, $(\ell \ge 1)$, is finite (each α^ℓ is a root of a polynomial with rational integer coefficients of degree d and whose coefficients have usual absolute values at most 2^d, where d is the degree of α). This gives the following statement, due to Kronecker : *if a non-zero algebraic number* $\alpha \in k$ *satisfies* $|\alpha|_v \le 1$ *for all* $v \in M_k$, *then* α *is a root of unity.*

Therefore the only algebraic numbers α which satisfy $\mathrm{h}(\alpha) = 0$ are 0 and the roots of unity; the other ones satisfy $\mathrm{h}(\alpha) > 0$. To give a sharp lower bound for $\mathrm{h}(\alpha)$ (when it is not zero) in terms of the degree of α is an interesting and difficult problem (see [L4] Chap.9 §7).

If a non-zero algebraic number α satisfies $\mathrm{M}(\alpha) < 2$, then α is an integer, and α^{-1} also; hence α is an algebraic unit. The problem is now to derive a lower bound for the height of algebraic units which are not roots of unity.

It is easy to see (exercise 7) that for each positive integer d there exists a positive number $c(d)$ such that, for any non-zero algebraic number α which is not a root of unity and is of degree $\leq d$, the inequality $\mathrm{h}(\alpha) \geq c(d)$ is valid. The example $\alpha = 2^{1/d}$ shows that such a function $c(d)$ must satisfy $c(d) \leq (\log 2)/d$. Lehmer's problem is : *is-it possible to choose $c(d) = c_0/d$ for some positive absolute constant c_0 ?* The smallest known value for $d\mathrm{h}(\alpha)$ is $\log \alpha_0 = 0.1623576\ldots$ where $\alpha_0 = 1.1762808\ldots$ is the root of the reciprocal polynomial of degree 10 :

$$X^5 Q\big(X + (1/X)\big) \qquad \text{for} \qquad Q(Y) = (Y+1)^2(Y-1)(Y+2)(Y-2) - 1.$$

The first result in the direction of Lehmer's problem is due to Schinzel and Zassenhaus (1965) : when $\alpha \neq 0$ is an algebraic number of degree $d \geq 2$ which is not a root of unity, then $\mathrm{h}(\alpha) > c/2^d$ for some absolute constant $c > 0$. In 1971, Blanksby and Montgomery [B-M] refined this result and proved $\mathrm{h}(\alpha) > 1/\big(52d^2 \log(6d)\big)$. In 1978, C.L. Stewart [St] introduced a method from transcendental number theory to prove $\mathrm{h}(\alpha) > 1/\big(10^4 d^2 \log d\big)$; this is marginally weaker than the previous result, but the interest lies in the method. Indeed, in 1979, Dobrowolski [Do] extended Stewart's argument and obtained the following statement: for each $\epsilon > 0$, there exists an integer $d_0(\epsilon)$ such that, for $d > d_0(\epsilon)$,

$$\mathrm{h}(\alpha) > \frac{1-\epsilon}{d}\left(\frac{\log\log d}{\log d}\right)^3;$$

this result is effective: according to [Do], for all $d \geq 3$, $\mathrm{h}(\alpha) > (1/1200d)\big(\log\log d/\log d\big)^3$. Later Cantor-Straus [C-S] introduced an interpolation determinant and replaced $1-\epsilon$ by $2-\epsilon$. Finally R. Louboutin [Lo] reached $(9/4)-\epsilon$ by a modification of the determinant introduced by Cantor and Straus; the same result with $(9/4)-\epsilon$ has been also obtained by M. Meyer using a construction of an auxiliary function (like Dobrowolski), but with Siegel's lemma replaced by a lemma due to Bombieri and Vaaler.

Our aim in this section is to give a further example of a transcendence proof using an interpolation determinant.

Theorem 3.16. — *Let α be a non-zero algebraic number of degree $d \geq 2$; assume*

$$\mathrm{h}(\alpha) \leq \frac{1}{2200 d^2 \log d}.$$

Then α is a root of unity.

Our proof will follow the method of Stewart in [St], apart from the fact that we replace the auxiliary function by an interpolation determinant. A variant of this proof is given in [MW]. In Chapter 7 (proof of lemma 7.2), we shall use the following consequence of theorem 3.16: if $\alpha \neq 0$ is not a root of unity, then

$$\mathrm{h}(\alpha) > \frac{1}{10^3 d^3}.$$

We split the proof in two parts: the first one is a transcendence argument, the second is the choice of parameters. Here is the first part:

Proposition 3.17. — *Let $L \geq 2$ be an even integer, $A \geq 2$ an integer and $C > 0$ a real number. Let α be an algebraic number of degree d satisfying $|\alpha| \geq 1$. Assume*

$$\left(\frac{\pi}{A}\right)^2 + \big(AL \log|\alpha|\big)^2 \leq \frac{1}{C^2} \tag{3.18}$$

and

$$\left(1 - \frac{1}{L}\right)\log C > 1 + \frac{2d}{L}\log L + \frac{d}{2}AL\mathrm{h}(\alpha). \tag{3.19}$$

Then α is a root of unity.

Proof. We denote by log the principal value of the logarithm with imaginary part in $]-\pi,\pi]$. We consider the AL numbers (not necessarily distinct)

$$\Im \log \alpha^s, \qquad (0 \le s < AL),$$

which all sit in an interval of length 2π. We write this interval $]-\pi,\pi]$ as a union of A intervals $I_j =]-\pi+(2\pi j/A), -\pi+\big(2\pi(j+1)/A\big)]$, $0 \le j \le A-1$. Using Dirichlet box principle, we deduce that there exists j with $0 \le j \le A-1$ such that I_j contains at least L of our AL numbers. Consider the center $\vartheta = -\pi + \big(\pi(2j+1)/A\big)$ of the interval I_j. Then there exist rational integers s_λ, $(1 \le \lambda \le L)$ with $0 \le s_1 < s_2 < \cdots < s_L < AL$, such that

$$\big|\Im \log\big(\alpha^{s_\lambda}\big) - \vartheta\big| \le \frac{\pi}{A}, \qquad (1 \le \lambda \le L).$$

From (3.18), using the estimate

$$0 \le \log|\alpha^{s_\lambda}| < AL \log|\alpha|$$

we deduce

$$\big|\log\big(\alpha^{s_\lambda}\big) - i\vartheta\big| \le \frac{1}{C}, \qquad (1 \le \lambda \le L). \tag{3.20}$$

Consider the $L \times L$ determinant

$$\Delta = \det\Big(\alpha^{s_\lambda \ell}\Big)_{1\le\lambda\le L, -L/2<\ell\le L/2}$$

This determinant is closely related to a Vandermonde determinant:

$$\Delta \prod_{\lambda=1}^{L} \alpha^{s_\lambda (L-2)/2} = \prod_{1\le\lambda<\mu\le L} \big(\alpha^{s_\mu} - \alpha^{s_\lambda}\big).$$

If α is not a root of unity, then $\Delta \ne 0$. On the other hand we can write $\Delta = f(\alpha, \alpha^{-1})$, where $f \in \mathbb{Z}[X,Y]$ is defined by

$$f(X,Y) = \sum_\sigma \epsilon(\sigma) \prod_{-L/2<\ell\le L/2} X^{\sigma(\ell)\max\{\ell,0\}} Y^{\sigma(\ell)\max\{-\ell,0\}};$$

in the sum, σ runs over the bijective maps from $\{(-L/2)+1,\dots,L/2\}$ onto $\{s_1,\dots,s_L\}$, and $\epsilon(\sigma)$ is the signature of the corresponding permutation. The length of f is at most $\sum_\sigma 1 = L!$. The degree of f with respect to X is bounded by

$$\sum_\ell \sigma(\ell)\max\{\ell,0\} < AL \sum_{\ell=0}^{L/2} \ell = \frac{1}{8} AL^2(L+2),$$

while the degree in Y is at most

$$\sum_\ell \sigma(\ell)\max\{-\ell,0\} < AL \sum_{\ell=0}^{(L/2)-1} \ell = \frac{1}{8} AL^2(L-2).$$

From Liouville's estimate we deduce, when α is not a root of unity,

$$\frac{1}{L}\log|\Delta| > -(d-1)\log L - \frac{d}{4} AL^2 \mathrm{h}(\alpha).$$

In order to derive an upper bound for $|\Delta|$, we define

$$f_\lambda(z) = \exp\big\{z\big(\log \alpha^{s_\lambda} - i\vartheta\big)\big\}, \quad (1 \le \lambda \le L),$$

$$\zeta_\ell = \ell, \quad (-L/2 < \ell \le L/2), \qquad r = L/2, \qquad R = CL/2.$$

Since $|e^{\ell i\vartheta}| = 1$, we have

$$|\Delta| = \left|\det\Big(f_\lambda(\zeta_\ell)\Big)_{1\le\lambda\le L, -L/2<\ell\le L/2}\right|.$$

Using (3.20), we obtain

$$\log|f_\lambda|_R < R/C = L/2.$$

We apply lemma 2.2:

$$\frac{1}{L}\log|\Delta| \le -\frac{L-1}{2}\log C + \log L + \frac{L}{2}.$$

Combining with the lower bound for $|\Delta|$, we conclude

$$\frac{d}{4}AL^2\mathrm{h}(\alpha) + d\log L + \frac{L}{2} > \frac{L-1}{2}\log C.$$

This is clearly contradictory with (3.19). Therefore α is a root of unity. □

Proof of Theorem 3.16. Let α be a non-zero algebraic number of degree d satisfying

$$\mathrm{h}(\alpha) < \frac{1}{Bd^2\log d}$$

for some positive number B. We want to prove that if B is sufficiently large, then α is a root of unity. The case $d = 2$ is easy (see exercise 7) ; therefore we assume $d \ge 3$.

As noticed before, as soon as $\mathrm{h}(\alpha) < (\log 2)/d$, α is an algebraic integer. We may replace α by a conjugate of α; therefore there is no loss of generality to assume $|\alpha| \ge 1$. From the upper bound $\log|\alpha| \le d\mathrm{h}(\alpha)$ we deduce

$$\log|\alpha| < \frac{1}{Bd\log d}.$$

If we find two integers $L \ge 2$ and $A \ge 2$, with L even, such that the number C which is defined by

$$\frac{1}{C^2} = \Big(\frac{\pi}{A}\Big)^2 + \left(\frac{AL}{Bd\log d}\right)^2$$

satisfies

$$\left(1 - \frac{1}{L}\right)\log C > 1 + \frac{2d}{L}\log L + \frac{AL}{2Bd\log d}, \tag{3.21}$$

then Proposition 3.17 yields the conclusion. We put $A = 30$. Here is our choice of L for various values of d, together with the corresponding value for B:

$d =$	3	4	5	6	7	8	9
$L =$	24	32	46	58	78	80	90
$B =$	2200	1900	1700	1600	1500	1500	1500

Finally for $d \ge 8$ we check (3.21) with $B = 1500$ by chosing $L = 2\big[2d\log(2d)\big]$ and $A = 30$. This completes the proof of Theorem 3.16. □

1Open problems **1.** (Lehmer's problem — see §7). Does there exist an absolute constant $c > 0$ such that, for any non-zero algebraic number which is not a root of unity, $d\mathrm{h}(\alpha) \ge c$?

2. In the case $f(X) = qX - p$ with p and q rational integers, Liouville's inequality gives an estimate for the approximation of algebraic numbers by rational numbers; in this special case this estimate is not the best

known (theorem of Thue, Siegel, Roth, Schmidt). Is-it possible to improve the estimate in the general case of lemma 3.14 ? Even an ineffective result would be useful.

1Exercises **1.** Let $\alpha_1, \dots, \alpha_s$ be algebraic numbers; define $k = \mathbb{Q}(\alpha_1, \dots, \alpha_s)$ and $d = [k : \mathbb{Q}]$. Show that there exist rational integers $a_2, \dots, a_s$ with $0 \le a_i \le d(d-1)/2$ such that the number $\alpha = \alpha_1 + a_2\alpha_2 + \cdots + a_s\alpha_s$ satisfies $k = \mathbb{Q}(\alpha)$.

2. For $f \in \mathbb{C}[X_1, \dots, X_t]$, we denote by $|f|_1$ the upper bound of $f(z)$ on the unit polydisk:

$$|f|_1 = \sup\bigl\{|f(z_1, \dots, z_t)|\,;\, |z_i| = 1,\, 1 \le i \le t\bigr\}.$$

Hence $|f|_1 \le L(f)$. Show that in lemmas 3.6, 3.7 and 3.14, one can replace $\log L(f)$ by $\log|f|_1$.
`Hint.` *Start by proving the following statement: if $a_0, \dots, a_N$, y are complex numbers, then*

$$\left|\sum_{i=0}^{N} a_i y^i\right| \le \sup_{|z|=1}\left|\sum_{i=0}^{N} a_i z^i\right| \cdot \max\bigl(1, |y|\bigr)^N.$$

When $|y| \le 1$, this inequality follows from the maximum modulus principle, for the polynomial $a_0 + a_1 z + \cdots + a_N z^N$; when $|y| > 1$, perform the change of variables $z' = 1/z$.

Deduce by induction: for a polynomial $f \in \mathbb{C}[z_1, \dots, z_t]$, when $y_1, \dots, y_t$ are complex numbers,

$$\bigl|f(y_1, \dots, y_t)\bigr| \le |f|_1 \prod_{i=1}^{t} \max\bigl(1, |y_i|\bigr)^{\deg_{z_i} f}.$$

3. For algebraic numbers $\vartheta_0, \dots, \vartheta_s$, not all of which are zero, check

$$\mathrm{h}(\vartheta_0 : \cdots : \vartheta_s) \le \sum_{i=0}^{s} \mathrm{h}(\vartheta_i).$$

4. Show that in lemma 3.14, if the Archimedean place v is not real, then the conclusion can be replaced by

$$\log|f(\underline{\gamma})|_v \ge -\left(\frac{d}{2} - 1\right)\log L(f) - \frac{d}{2}\sum_{i=1}^{t} N_i \mathrm{h}(1 : \gamma_{i1} : \cdots : \gamma_{is_i}).$$

Show also that if v is an ultrametric place of k, then

$$\log|f(\underline{\gamma})|_v \ge -\frac{d}{d_v}\left(\log L(f) + \sum_{i=1}^{t} N_i \mathrm{h}(1 : \gamma_{i1} : \cdots : \gamma_{is_i})\right).$$

where d_v is, as usual, the local degree at the place v.

5. Let $f \in \mathbb{Z}[X]$ be a non-zero polynomial of degree d with leading coefficient $a_0 > 0$ and let $\alpha \in \mathbb{C}$ be a zero of f.
a) Let p/q be a rational number with $q > 0$ such that $f(p/q) \ne 0$. Show that

$$\left|\alpha - \frac{p}{q}\right| \ge \frac{\max\{1, |\alpha|\}}{q(|p| + q)^{d-1}\mathrm{M}(f)}.$$

b) Deduce that for an algebraic number α of degree d, if we set

$$c(\alpha) = \frac{\max\{1, |\alpha|\}}{(2 + |\alpha|)^{d-1}\mathrm{M}(\alpha)},$$

then for all $p/q \in \mathbb{Q}$ with $p/q \neq \alpha$ we have

$$\left|\alpha - \frac{p}{q}\right| \geq \frac{c(\alpha)}{q^d}.$$

c) Show that, for each $\kappa > |f'(\alpha)|$, there are only finitely many $p/q \in \mathbb{Q}$ with

$$\left|\alpha - \frac{p}{q}\right| \leq \frac{1}{\kappa q^d}.$$

Example: for α a real quadratic number, which is root of a polynomial $aX^2 + bX + c$ of discriminant $\Delta = b^2 - 4ac > 0$, for each $\kappa > \sqrt{\Delta}$ there exist $q_0 > 0$ such that, for $p/q \in \mathbb{Q}$ with $q > q_0$,

$$\left|\alpha - \frac{p}{q}\right| > \frac{1}{\kappa q^2}.$$

6. a) Let β be a non-zero algebraic number and ℓ a non-zero logarithm of an algebraic number. Define $\alpha = e^\ell$ and $D = [\mathbb{Q}(\alpha, \beta) : \mathbb{Q}]$. Then

$$|\beta\ell| > \Big(2e^{\mathrm{h}(\alpha)+\mathrm{h}(\beta)}\Big)^{-D}.$$

`Hint.` *Using* (3.13)*, deduce* $|\beta| \geq e^{-D\mathrm{h}(\beta)}$*. Using lemma* 3.14*, show that* $|\alpha - 1| \geq 2\Big(2e^{\mathrm{h}(\alpha)}\Big)^{-D}$ *if* $\alpha \neq 1$*. From exercise* 1 *of Chapter* 1*, deduce* $\min\{|\alpha - 1|, 1\} < 2|\ell|\}$.

b) Let $\ell_1, \ldots, \ell_m$ be logarithms of algebraic numbers and $b_1, \ldots, b_m$ rational integers. Let D be the degree of a number field containing the m algebraic numbers $\alpha_j = \exp(\ell_j)$, $(1 \leq j \leq m)$. If the number

$$\Lambda = b_1\ell_1 + \cdots + b_m\ell_m$$

does not vanish, then

$$|\Lambda| \geq 2^{-D} \exp\left\{-D \sum_{j=1}^{m} |b_j| \mathrm{h}(\alpha_j)\right\}.$$

7.

a) Check that for a non-zero algebraic number α of degree $d \leq 4$ which is not a root of unity, the number $d\mathrm{h}(\alpha) = \log \mathrm{M}(\alpha)$ is bounded from below by the value given in the following table (the last column provides a polynomial which yields the minimum):

$d =$	$d\mathrm{h}(\alpha) \geq$	minimum for
1	$\log 2 = 0.6931\ldots$	$X - 2$
2	$\log\big((1+\sqrt{5})/2\big) = 0.4812\ldots$	$X^2 - X - 1$
3	$0.2811\ldots$	$X^3 - X - 1$
4	$0.3223\ldots$	$X^4 - X - 1$

b) Show that the proof of Kronecker's result (see §7) is effective: if d is a positive integer, there exists a positive number $c(d)$ such that, for any non-zero algebraic numbers α which is not a root of unity and is of degree $\leq d$, the inequality $\mathrm{h}(\alpha) \geq c(d)$ is valid.

`Hint.` *Let* α *be an algebraic unit of degree* d*. Assume that there exists a positive integer* ℓ *such that*

$$\mathrm{M}(\alpha)^\ell < 1 + 2^{-d} \qquad \textit{and} \qquad \ell \geq 2d\big(2^{d+1} + 1\big)^{d-1}.$$

Check $H(\alpha^j) \le 2^d$ *for* $1 \le j \le \ell$ *and deduce that the numbers* $1, \alpha, \dots, \alpha^\ell$ *are not pairwise distinct.*
c) Let A and d be two positive integers, H and C two positive real numbers, and α a non-zero algebraic number of degree d. Assume

$$d\mathrm{h}(\alpha) \le 1/H, \qquad \frac{1}{C^2} = \left(\frac{\pi}{A}\right)^2 + \left(\frac{2A-1}{H}\right)^2$$

and

$$C > 2^d e^{(2A-1)/H}.$$

Show that α is a root of unity of order $< 2A$.
`Hint.` *Show that there exists an integer* r *in the range* $1 \le r \le 2A-1$ *such that* $|\log(\alpha^r)| \le 1/C$ *; deduce* $|\alpha^r - 1| < 2/C$. *Use Liouville's inequality* (3.14) *for* $f(X) = X^r - 1$ *and conclude.*
d) Deduce from c) that a suitable value for $c(d)$ in question b) above is 2^{-2d-4}.
`Hint.` *Choose* $A = 2^{d+2}$, $H = A^2$.

8.
a) Let $L \ge 2$ be an even integer and α a **real** algebraic number of degree d satisfying $\alpha > 1$. Define $C = 2/(L \log|\alpha|)$. Prove

$$\log C \le \frac{2d}{L-1}\log L + \frac{d}{3}(L+1)\mathrm{h}(\alpha) + \frac{L}{L-1}.$$

`Hint.` *Repeat the proof of Proposition* 3.17 *with* $\{s_1, \dots, s_L\}$ *replaced by* $\{(-L/2)+1, \dots, L/2\}$.
b) Under the assumptions of Proposition 3.17, assume that α is not real; show that (3.19) can be replaced by

$$\left(1 - \frac{1}{L}\right)\log C > 1 + \frac{d}{L}\log L + \frac{d}{4}AL\mathrm{h}(\alpha).$$

`Hint.` *Use exercise* 4.
c) Deduce an improvement of the constant 2200 in theorem 3.16.
`Remark.` *Further improvements are possible; see* [MW].

9. (Dobrowolski). Let α be a non-zero algebraic integer of degree d satisfying

$$|\overline{\alpha}| \le 1 + \frac{1}{4ed^2}.$$

Let p be a prime number in the range $2ed < p < 4ed$. For each positive integer k, define

$$S_k = \sum_{i=1}^{d} \alpha_i^k.$$

Check the estimates, for $k \le d$,

$$|S_k| \le d\left(1 + \frac{1}{4ed^2}\right)^d < de$$

and

$$|S_{kp}| \le d\left(1 + \frac{1}{4ed^2}\right)^{4ed^2} < de.$$

Deduce $|S_k - S_{kp}| < p$. On the other hand, check the congruences $S_k \equiv S_k^p \equiv S_{kp} \pmod p$; deduce $S_k = S_{kp}$ for $1 \le k \le d$. Show that α and α^p are conjugate. Conclude that α is a root of unity.

1References

[A] E. Artin. – *Algebraic Numbers and Algebraic Functions;* Gordon Breach, New-York 1967.
[B] N. Bourbaki. – *Algèbre Commutative;* Masson (1985), Chap. 6: Valuations.
[B-M] P.E. Blanksby and H.L. Montgomery. – Algebraic integers near the unit circle; Acta Arith., **18** (1971), 355–369.

[C-S] D.C. Cantor and E.G. Straus. – On a conjecture of D.H. Lehmer; Acta Arith., **42** (1982), 97–100.
[Do] E. Dobrowolski. – On a question of Lehmer and the number of irreducible factors of a polynomial; Acta Arith., **34** (1979), 391–401.
[Du] A. Durand. – Quelques aspects de la théorie analytique des polynômes; dans *Cinquante Ans de Polynômes*, Proceedings, Paris 1988, Springer Lecture Notes **1415** (1990), p.1–85.
[F-T] A. Fröhlich and M.J. Taylor. – *Algebraic number theory;* Cambridge studies in advanced mathematics, **27**, Cambridge Univ. Press 1991, Chap. 1, 2, 3.
[L1] S. Lang. – *Algebraic Number Theory;* Addison-Wesley 1970.
[L2] S. Lang. – *Elliptic Curves Diophantine Analysis;* Springer Verlag, Grund. der Math. Wiss., **231** (1978), Chap. 4 §1, p.77–84, et Chap 7 §1 p.159–162.
[L3] S. Lang. – *Fundamentals of Diophantine Geometry;* Springer Verlag (1983), Chap. 3 §1, p. 50–54.
[L4] S. Lang. – *Number theory* 3; Encycl. of Math. Sciences, **60**, Springer Verlag 1991.
[La] M. Langevin. – Mesures des polynômes et des nombres algébriques; Journée de Théorie élémentaire et analytique des nombres de Limoges (1980); Thèse Paris 6 (1987), p.197–215.
[Lo] R. Louboutin. – Sur la mesure de Mahler d'un nombre algébrique; C. r. Acad. Sci. Paris, sér. A **296** (1983), 707–708.
[M] K. Mahler. – *Lectures on transcendental numbers ;* Springer Lecture Notes in Math., **546** (1976).
[MW] M. Mignotte and M. Waldschmidt. – On algebraic numbers of small height: linear forms in one logarithm; manuscript.
[S] J.-P. Serre. – *Lectures on the Mordell-Weil theorem;* Vieweg, Aspects of Math. **E15**, (1989), Chap. 2 §1-3, p.7–16.
[St] C.L. Stewart. – Algebraic integers whose conjugates lie near the unit circle; Bull. Soc. Math. France, **106** (1978), 169–176.

ANNEX TO CHAPTER III.– INEQUALITIES BETWEEN DIFFERENT HEIGHTS OF A POLYNOMIAL

From a manuscript by Alain DURAND

Let $f \in \mathbb{C}[X]$ be a non-zero polynomial with complex coefficients of degree d:

$$f = a_0X^d + a_1X^{d-1} + \cdots + a_d = a_0\prod_{i=1}^{d}(X - \alpha_i).$$

There are several notions of *height* for f; for instance we have the usual height of f (see §4):

$$H(f) = \max\{|a_0|, |a_1|, \ldots, |a_d|\},$$

Mahler's measure of f (see §3):

$$M(f) = |a_0|\prod_{i=1}^{d}\max\{1, |\alpha_i|\},$$

the length of f (see §2):

$$L(f) = |a_0| + |a_1| + \cdots + |a_d|,$$

the Euclidean norm of f:

$$L_2(f) = \big(|a_0|^2 + |a_1|^2 + \cdots + |a_d|^2\big)^{1/2} = \left(\int_0^1 \big|f\big(e^{2i\pi t}\big)\big|^2 dt\right)^{1/2},$$

and finally the sup norm on the unit disk (or on the unit circle, which is the same by the maximum modulus principle):

$$\|f\| = \sup_{|z|\le 1}|f(z)| = \sup_{|z|=1}|f(z)|.$$

The figure below (due to the late Alain Durand) provides an upper bound for the quotient of one of the norms (left column) by another one (first row); in each case but two, below the upper bound is displayed one polynomial for which the estimate is optimal (where f_d denotes the polynomial $1 + X + \cdots + X^d$). There are two exceptions where the optimal result is not known:
(1) the upper bound for $M(f)/H(f)$ reads

$$M(f) \le \sqrt{d+1}H(f);$$

there exists $A > 0$ such that for each $d \ge 1$ there is such a polynomial f of degree d with

$$M(f) \ge A\sqrt{d+1}H(f).$$

(2) the upper bound for $L(f)/\|f\|$ reads

$$L(f) \le \sqrt{d+1}\|f\|;$$

there exists $A > 0$ such that for each $d \ge 1$ there is such a polynomial f of degree d with

$$L(f) \ge A\sqrt{d+1}\|f\|.$$

	$H(f)$	$L_2(f)$	$L(f)$	$\|f\|$	$M(f)$
$H(f) \leq$	1	1 X^d	1 X^d	1 X^d	$\binom{d}{[d/2]}$ $(X+1)^d$
$L_2(f) \leq$	$\sqrt{d+1}$ f_d	1	1 X^d	1 X^d	$\binom{2d}{d}^{1/2}$ $(X+1)^d$
$L(f) \leq$	$d+1$ f_d	$\sqrt{d+1}$ f_d	1	$\sqrt{d+1}$ (2)	2^d $(X+1)^d$
$\|f\| \leq$	$d+1$ f_d	$\sqrt{d+1}$ f_d	1 X^d	1	2^d $(X+1)^d$
$M(f) \leq$	$\sqrt{d+1}$ (1)	1 X^d	1 X^d	1 X^d	1

4.– INTERPOLATION DETERMINANTS

In this Chapter we denote by $f_1, \ldots, f_L$ analytic functions in $\mathbb{C}^n$, and by $\zeta_1, \ldots, \zeta_L$ elements of $\mathbb{C}^n$. Our aim is to give an upper bound for the determinant

$$\Delta = \det\Big(f_\lambda(\zeta_\mu)\Big)_{1\le\lambda,\mu\le L},$$

following an idea due to Michel Laurent [L1], [L2], [L3]. We show that the function of a single complex variable z

$$\Psi(z) = \det\Big(f_\lambda(z\zeta_\mu)\Big)_{1\le\lambda,\mu\le L}$$

has a zero of high multiplicity at the origin. Then Schwarz lemma provides the desired upper bound. At the end of this Chapter, we remark that the proofs can be considered as "elementary" so far as no complex analysis is required.

For $x = (x_1, \ldots, x_n) \in \mathbb{C}^n$ we denote by $|x|$ the number $\max\{|x_1|, \ldots, |x_n|\}$. When f is an analytic function in$\mathbb{C}^n$, we denote by $|f|_R$ the maximum of $|f(x)|$ for $|x| \le R$.

For $\kappa = (\kappa_1, \ldots, \kappa_n) \in \mathbb{N}^n$ we denote by $\|\kappa\|$ the number $\kappa_1 + \cdots + \kappa_n$.

1Schwarz lemma The only tool from complex analysis which occurs in these lectures is the following result:

Lemma 4.1. — *Let $r > 0$ and $R > 0$ be positive real numbers such that*

$$\max_{1\le\mu\le L} |\zeta_\mu| \le r \qquad \text{and} \qquad R \ge r.$$

Let T be the multiplicity of the zero $z = 0$ of the function Ψ at the origin. Then

$$|\Delta| \le \left(\frac{R}{r}\right)^{-T} L! \prod_{\lambda=1}^{L} |f_\lambda|_R.$$

Proof. Define $E = R/r$. From Schwarz lemma in one variable we deduce

$$|\Psi(1)| \le \left(\frac{R}{r}\right)^{-T} |\Psi|_E.$$

However $\Psi(1) = \Delta$, and

$$|\Psi|_E \le L! \prod_{\lambda=1}^{L} |f_\lambda|_R.$$

□

1Estimate for the multiplicity of Ψ at the origin Here is a generalization in several variables of lemma 2.2.

The proof in the one dimensional case involved the number

$$\Theta_1(L) = \min\{\kappa_1 + \cdots + \kappa_L\} = \frac{L(L-1)}{2},$$

where the minimum runs over the L-tuples $(\kappa_1, \ldots, \kappa_L)$ of non-negative integers which are pairwise distinct. In the general case $n \ge 1$, we define

$$\Theta_n(L) = \min\{\|\kappa_1\| + \cdots + \|\kappa_L\|\}$$

where the minimum runs over the L-tuples $(\kappa_1, \ldots, \kappa_L)$ of elements in $\mathbb{N}^n$ which are pairwise distinct.

Lemma 4.2. — *The function Ψ has a zero at $z = 0$ of multiplicity $\geq \Theta_n(L)$.*

Proof. Since the determinant is multilinear, by expanding each f_λ in Taylor series at the origin, we may assume that each f_λ is a monomial $f_\lambda(\zeta) = \zeta^{\kappa_\lambda}$, with $\kappa_\lambda \in \mathbb{N}^n$. In this case $f_\lambda(z\zeta) = \zeta^{\kappa_\lambda} z^{\|\kappa_\lambda\|}$.

In the row indexed by λ, we have a common factor $z^{\|\kappa_\lambda\|}$:

$$\Psi(z) = \det\left(\zeta_\mu^{\kappa_\lambda}\right)_{1\leq\lambda,\mu\leq L} \cdot z^{\|\kappa_1\|+\cdots+\|\kappa_L\|}.$$

If the elements $\kappa_1, \ldots, \kappa_L$ in $\mathbb{N}^n$ are not pairwise distinct, then this determinant vanishes and $\Psi = 0$. If they are pairwise distinct, then Ψ has a zero at 0 of multiplicity at least $\|\kappa_1\| + \cdots + \|\kappa_L\|$, which proves our claim. □

1Lower bound for Θ_n Here is a lower bound for the coefficient $\Theta_n(L)$:

Lemma 4.3. — *For $L > 2^n e^{n+1}$ we have*

$$\Theta_n(L) \geq \frac{n}{6e} L^{(n+1)/n}.$$

Proof. To begin with we assume only $L \geq 2$. The smallest value for the sum $\|\kappa_1\| + \cdots + \|\kappa_L\|$ is reached by chosing for κ_μ successively:

$(0, \ldots, 0)$;

the n elements of $\mathbb{N}^n$ of length 1:

$$(1, 0, \ldots, 0), \ldots, (0, \ldots, 0, 1);$$

the $\binom{n+1}{2} = \binom{n+1}{n-1}$ elements of length 2:

$$(2, 0, \ldots, 0),\ (1, 1, 0, \ldots, 0), \ldots,\ (0, \ldots, 0, 1, 1),\ (0, \ldots, 0, 2);$$

and so on.

In general, for a a non-negative integer, the number of elements $\kappa \in \mathbb{N}^n$ of length $\|\kappa\| = a$ is the coefficient of z^a in the series

$$\sum_{\kappa\in\mathbb{N}^n} z^{\|\kappa\|} = \left(\sum_{k=0}^{\infty} z^k\right)^n = \frac{1}{(1-z)^n} = \sum_{a\geq 0} \binom{n+a-1}{a} z^a,$$

hence this number is

$$\binom{n+a-1}{a} = \binom{n+a-1}{n-1}.$$

For any positive integer A we have

$$\sum_{k=0}^{A-1} \binom{n+k}{n} = \binom{n+A}{n+1};$$

this is an easy consequence (by induction) of the formula

$$\binom{n+k-1}{n+1} + \binom{n+k-1}{n} = \binom{n+k}{n+1}.$$

Let A be the positive integer such that

$$\sum_{a=0}^{A} \binom{n+a-1}{n-1} = \binom{n+A}{n} \leq L < \binom{n+A+1}{n}.$$

This integer A is the integral part of the real number α which is defined by

$$(\alpha+n)\cdots(\alpha+1)/n! = L.$$

We have

$$\begin{aligned}\|\kappa_1\|+\cdots+\|\kappa_L\| &\geq \sum_{a=0}^{A} a\binom{n+a-1}{n-1} = n\sum_{a=1}^{A}\binom{n+a-1}{n}\\ &= n\sum_{a=0}^{A-1}\binom{n+a}{n} = n\binom{n+A}{n+1},\end{aligned}$$

hence

$$\Theta_n(L) \geq n\binom{n+A}{n+1}.$$

We bound A from below by $\alpha-1$; we deduce

$$(n+A)(n+A-1)\cdots(1+A)A \geq (\alpha+n-1)\cdots\alpha A = \frac{\alpha}{\alpha+n}(\alpha+n)\cdots(\alpha+1)A = \frac{\alpha}{\alpha+n}n!AL;$$

therefore

$$\Theta_n(L) \geq \frac{n}{n+1}\cdot\frac{\alpha}{\alpha+n}\cdot AL.$$

Now we bound α from below by $B-n$ and A by $B-n-1$ with

$$B \geq (n!L)^{1/n} > \frac{n}{e}L^{1/n}.$$

and we obtain

$$\Theta_n(L) \geq \frac{n}{n+1}BL\left(1-\frac{n}{B}\right)\left(1-\frac{n+1}{B}\right).$$

This inequality holds for all $L\geq 1$ and $n\geq 1$. Assume now $L\geq 2^n e^{n+1}$; then $B\geq 2(n+1)$,

$$1-\frac{n+1}{B}\geq\frac{1}{2}\quad\text{and consequently}\quad 1-\frac{n}{B}\geq\frac{1}{2};$$

since $n/4e(n+1)\geq 1/6e$ for $n\geq 2$ (lemma 4.3 is true for $n=1$), the desired result follows. □

1Conclusion We now combine the three preceding lemmas as follows:

Proposition 4.4. — *Let $\ell_1,\ldots,\ell_n$, $\beta_1,\ldots,\beta_n$ be complex numbers. For $1\leq i\leq n$ define $\alpha_i=\exp(\ell_i)$. There exists a constant $c=c(\ell_1,\ldots,\ell_n,\beta_1,\ldots,\beta_n)>0$, which can be easily computed, and satisfies the following property: let L_0, L_1 and S be rational integers ≥ 2, define $L=\binom{L_0+n}{n}(L_1+1)$, and let $s^{(1)},\ldots,s^{(L)}$ be any elements in $\mathbb{Z}^{n+1}(S)$. Consider the $L\times L$ determinant*

$$\Delta=\det\left((s_1^{(\mu)}+s_{n+1}^{(\mu)}\beta_1)^{\lambda_1}\cdots(s_n^{(\mu)}+s_{n+1}^{(\mu)}\beta_n)^{\lambda_n}\left(\alpha_1^{s_1^{(\mu)}+s_{n+1}^{(\mu)}\beta_1}\cdots\alpha_n^{s_n^{(\mu)}+s_{n+1}^{(\mu)}\beta_n}\right)^{\lambda_{n+1}}\right)_{\underline{\lambda},\mu}$$

with $\underline{\lambda}=(\lambda_1,\ldots,\lambda_{n+1})\in\mathbb{N}^{n+1}$, $\lambda_1+\cdots+\lambda_n\leq L_0$ and $\lambda_{n+1}\leq L_1$, and with $1\leq\mu\leq L$. Then

$$\frac{1}{L}\log|\Delta| \leq -L^{1/n}+c(L_0\log S+L_1 S).$$

Proof. We consider the functions

$$f_{\underline{\lambda}}(z)=z_1^{\lambda_1}\cdots z_n^{\lambda_n}\left(\alpha_1^{z_1}\cdots\alpha_n^{z_n}\right)^{\lambda_{n+1}}$$

and the points

$$\zeta_\mu = \left(s_1^{(\mu)} + s_{n+1}^{(\mu)}\beta_1, \dots, s_n^{(\mu)} + s_{n+1}^{(\mu)}\beta_n\right) \in \mathbb{C}^n.$$

For any $R > 0$ we plainly have

$$\log |f_\lambda|_R \le L_0 \log R + L_1 R \sum_{i=1}^{n} |\ell_i|.$$

We choose

$$r = S\left(1 + \max_{1\le j\le n} |\beta_j|\right), \qquad R = re^{6e/n}.$$

From lemmas 4.1 and 4.2 one deduces

$$\log |\Delta| \le -\frac{6e}{n}\Theta_n(L) + \log L! + LL_0 \log R + LL_1 R \sum_{i=1}^{n} |\ell_i|. \tag{4.5}$$

Assuming $L \ge 2^n e^{n+1}$, we can apply lemma 4.3 and conclude $\frac{6e}{n}\Theta_n(L) \ge L^{1+1/n}$; the desired result readily follows.

If $L \le 2^n e^{n+1}$, then the result is an easy consequence of (4.5). □

1Avoiding the use of complex analysis We conclude this Chapter with a remark that the proofs we give in these lectures do not require any complex analysis : from this point of view they are "elementary". The only point where analysis played any role so far was in the use of Schwarz lemma, in the proof of lemma 4.1. But we use it only for exponential polynomials in one variable, and in this case the estimate is quite easy:

Lemma 4.5. – *Let a_{ij} (for $1 \le i \le s$, $1 \le j \le t$) and w_j (for $1 \le j \le t$) be complex numbers. Assume that the exponential polynomial*

$$F(z) = \sum_{i=1}^{s}\sum_{j=1}^{t} a_{ij} z^i e^{w_j z}$$

has a zero of multiplicity $\ge T$ at the origin. Then for $z_0 \in \mathbb{C}$ and $R \ge |z_0|$ we have

$$|F(z_0)| \le \left(\frac{R}{|z_0|}\right)^{-T} \sum_{i=1}^{s}\sum_{j=1}^{t} |a_{ij}| R^i e^{|w_j|R}.$$

Proof. We consider the Taylor expansion of F at the origin:

$$F(z) = \sum_{n\ge 0} \alpha_n z^n \qquad \text{where} \qquad \alpha_n = \sum_{i=1}^{\min\{s,n\}} \sum_{j=1}^{t} a_{ij} \frac{w_j^{n-i}}{(n-i)!}.$$

By assumption $\alpha_0 = \cdots = \alpha_{T-1} = 0$. For $n \ge T$ we have $(R/|z_0|)^T \le (R/|z_0|)^n$ (because $R \ge |z_0|$), hence

$$\begin{aligned} |F(z_0)| &= \left|\sum_{n\ge T} \alpha_n z_0^n\right| \\ &\le \sum_{n\ge T} |\alpha_n|\ |z_0|^n \\ &\le \left(\frac{R}{|z_0|}\right)^{-T} \sum_{n\ge T} |\alpha_n|\ R^n. \end{aligned}$$

We now use the trivial bound

$$\sum_{n\ge T} |\alpha_n|\ R^n \le \sum_{i=1}^{\min\{s,n\}} \sum_{j=1}^{t} |a_{ij}| \sum_{n\ge i} \frac{|w_j|^{n-i}}{(n-i)!} R^n,$$

where the right hand side is nothing else than

$$\sum_{i=1}^{s}\sum_{j=1}^{t}|a_{ij}|R^i e^{|w_j|R}.$$

□

1Exercises **1.** With the notations of lemma 4.3, show that for all $n \geq 1$ and $\epsilon > 0$, there exists $L_0 = L_0(n,\epsilon)$ such that, for $L \geq L_0$, we have

$$\Theta_n(L) \geq \left(\frac{n(n!)^{1/n}}{n+1} - \epsilon\right) L^{(n+1)/n}.$$

In particular, for $n \geq 2$ and for L sufficiently large,

$$\Theta_n(L) \geq \frac{1}{2} L^{(n+1)/n}.$$

2. Give an explicit value for the constant c in Proposition 4.4.
`Hint.` *See Chapter* 7 §4, *Step* 2.

1References

[L1] M.Laurent. – Sur quelques résultats récents de transcendance; Journées arithmétiques Luminy 1989, Astérisque, **198**–**200** (1991), 209–230.
[L2] M.Laurent. – Hauteurs de matrices d'interpolation; in *Approximations Diophantiennes et Nombres Transcendants*, Luminy 1990, éd. P. Philippon, de Gruyter 1992, 215–238.
[L3] M. Laurent. – Linear forms in two logarithms and interpolation determinants; this volume, Appendix.

5.– ZERO ESTIMATE

The first zero estimate in connection with transcendental number theory was given by Gel'fond [G] in his work around 1948 on algebraic independence of transcendental numbers; the proof was of an analytic nature. Such arguments have been developed later, but turned out not to be sufficient. Algebraic arguments have been introduced by Brownawell and Masser [BM], then refined by Masser [Ma]. The proof we are going to give in section 2 has its source in a letter of D.W. Masser which is quoted in [MW]; in §3 we use Moreau's version [Mo] of Masser's paper [Ma], as well as Philippon's approach [P] to this question.

In all this Chapter we denote by K any field of zero characteristic.

1 The main result The aim of this Chapter is to prove the following result:

Proposition 5.1. — *Let $\alpha_1, \dots, \alpha_{n+1}$ be non-zero elements of K which generate a multiplicative subgroup of K^* of rank $\geq n$. Let $\beta_1, \dots, \beta_n$ be elements of K. Assume that there exist three positive rational integers L_0, L_1 and S satisfying*

$$(S/2n)^{n+1} \geq (L_0 L_1)^n, \qquad S \geq 2n(n+1) \qquad \text{and} \qquad S^n > L_1,$$

such that the rank of the matrix

$$\left((s_1 + s_{n+1}\beta_1)^{\lambda_1} \cdots (s_n + s_{n+1}\beta_n)^{\lambda_n} \left(\alpha_1^{s_1} \cdots \alpha_{n+1}^{s_{n+1}}\right)^{\lambda_{n+1}} \right)_{\underline{\lambda}, \underline{s}},$$

is strictly less than $\binom{L_0+n}{n}(L_1+1)$. Then the numbers $1, \beta_1, \dots, \beta_n$ are linearly dependent over $\mathbb{Q}$.

In the matrix above the index of row is, as usual,

$$\underline{\lambda} = (\lambda_1, \dots, \lambda_{n+1}) \in \mathbb{N}^{n+1}, \qquad \lambda_1 + \cdots + \lambda_n \leq L_0, \qquad \lambda_{n+1} \leq L_1,$$

while the index of columns is $\underline{s} \in \mathbb{Z}^{n+1}(S)$. Recall that when S is a non-negative integer, $\mathbb{Z}^{n+1}(S)$ is the set of $\underline{s} = (s_1, \dots, s_{n+1}) \in \mathbb{Z}^{n+1}$ with $|s_i| < S$, $(1 \leq i \leq n+1)$.

Our assumption on the rank of the matrix means that there exists a non-zero polynomial $P \in K[X_1, \dots, X_n, Y]$, of total degree $\leq L_0$ in the variables $X_1, \dots, X_n$ and of degree $\leq L_1$ in Y, which vanishes at all the points

$$\left(s_1 + s_{n+1}\beta_1, \dots, s_n + s_{n+1}\beta_n, \alpha_1^{s_1} \cdots \alpha_{n+1}^{s_{n+1}}\right) \in K^n \times K^*, \qquad \underline{s} \in \mathbb{Z}^{n+1}(S)$$

(we emphasize the fact that the last coordinate does not vanish: we are working in fact with the product of the additive group of K^n with the multiplicative group K^*). In this Chapter, we shall use two sorts of elimination: firstly we eliminate the variable Y thanks to a resultant; next we use Bézout's theorem to deal with the variables $(X_1, \dots, X_n)$, which we denote for simplicity by $\underline{X}$.

The assumption $S^n > L_1$ does not matter in our application ; in fact, as soon as $n > 1$, it is a consequence of the hypothesis $(S/2n)^{n+1} \geq (L_0 L_1)^n$. Here, the constant $2^n n^{n+1}$, which appears implicitly in this hypothesis, does not play an important role either. What is important to know is that a stronger estimate is true, with the condition $(S/2n)^{n+1} \geq (L_0 L_1)^n$ replaced by $2^n S^{n+1} \geq (n+1)^{n+2} L_0^n L_1$ (this is a consequence of the main result in [P]; see exercise 7). However we found it useful to give here this simpler proof of a weaker result. It may be also considered as an introduction to the slightly more sophisticated arguments of Chapter 8.

The basic idea of the proof of Proposition 5.1 is to remark that if P satisfies the above vanishing property, and if S' and S'' are two positive integers satisfying $S \geq S' + S'' - 1$, then all the polynomials

$$P\left(X_1 + s_1' + s_{n+1}'\beta_1, \dots, X_n + s_n' + s_{n+1}'\beta_n, \alpha_1^{s_1'} \cdots \alpha_{n+1}^{s_{n+1}'} Y\right),$$

for $\underline{s}' \in \mathbb{Z}^{n+1}(S')$, vanish at all points

$$\big(s_1'' + s_{n+1}''\beta_1, \dots, s_n'' + s_{n+1}''\beta_n, \alpha_1^{s_1''} \cdots \alpha_{n+1}^{s_{n+1}''}\big) \in K^n \times K^*,$$

for $\underline{s}'' \in \mathbb{Z}^{n+1}(S'')$.

1Elimination of Y In this section, we eliminate the last variable Y between the polynomials

$$P\big(X_1 + s_1' + s_{n+1}'\beta_1, \dots, X_n + s_n' + s_{n+1}'\beta_n, \alpha_1^{s_1'} \cdots \alpha_{n+1}^{s_{n+1}'} Y\big), \qquad \underline{s}' \in \mathbb{Z}^{n+1}(S').$$

a) *Statement of the result*

Denote K^*_{tors} the torsion subgroup of K^* (viz. the group of roots of unity) and by σ be the canonical surjective map of K^* onto the quotient K^*/K^*_{tors}.

Lemma 5.2. — *Let $\alpha_1, \dots, \alpha_{n+1}$ be non-zero elements of K, $\beta_1, \dots, \beta_n$ be elements of K and L_0, L_1, S', S'' be positive rational integers. Define $S = S' + S'' - 1$, and assume*

$$\mathrm{Card}\Big\{\sigma\big(\alpha_1^{s_1'} \cdots \alpha_{n+1}^{s_{n+1}'}\big)\,;\, \underline{s}' \in \mathbb{Z}^{n+1}(S')\Big\} > L_1.$$

Assume further that there exists a non-zero polynomial $P \in K[\underline{X}, Y]$ of total degree $\le L_0$ in $X_0, \dots, X_n$ and of degree $\le L_1$ in Y for which

$$P\big(s_1 + s_{n+1}\beta_1, \dots, s_n + s_{n+1}\beta_n, \alpha_1^{s_1} \cdots \alpha_{n+1}^{s_{n+1}}\big) = 0 \qquad \text{for all} \quad \underline{s} \in \mathbb{Z}^{n+1}(S).$$

Then there exists a non-zero polynomial $Q \in K[\underline{X}]$ of total degree $\le 2L_0L_1$ for which

$$Q\big(s_1'' + s_{n+1}''\beta_1, \dots, s_n'' + s_{n+1}''\beta_n\big) = 0 \qquad \text{for all} \quad \underline{s}'' \in \mathbb{Z}^{n+1}(S'').$$

The proof of lemma 5.2 will use an argument of D.W. Masser (cf. [MW], §4). It's interesting to notice that lemma 5.2 completes the proof of Proposition 5.1 in the case $n = 1$; this means that for the proof of Gel'fond-Schneider theorem a single elimination is sufficient.

b) *The Kronecker u-resultant*

Here is an extension of lemma 4.2 in [MW]:

Lemma 5.3. — *Let $F_1, \dots, F_r$ be polynomials in $K[X_1, \dots, X_n, Y]$, of total degree at most L_0 in $X_1, \dots, X_n$ and of degree at most L_1 in Y; we assume that they have no common irreducible factor, in the factorial ring $K[X_1, \dots, X_n, Y]$, of degree ≥ 1 with respect to Y. Let (ξ_j, η_j), $(j \in J)$ be common zeroes to $F_1, \dots, F_r$ in $K^n \times K$. Then there exists a non-zero polynomial in $K[X_1, \dots, X_n]$, of total degree $\le 2L_0L_1$, which vanishes at all the points ξ_j, $(j \in J)$.*

Proof. Introduce $2r$ new variables $U_1, \dots, U_r, V_1, \dots, V_r$. Then define the two polynomials G and H in the ring $A = K[U_1, \dots, U_r, V_1, \dots, V_r, X_1, \dots, X_n, Y]$ by

$$G = \sum_{i=1}^{r} U_i F_i(X_1, \dots, X_n, Y), \qquad H = \sum_{i=1}^{r} V_i F_i(X_1, \dots, X_n, Y).$$

Let $R \in K[U_1, \dots, U_r, V_1, \dots, V_r, X_1, \dots, X_n]$ be the resultant of the polynomials G and H with respect to the variable Y (see for instance [W1] Chap.5, or [V], for a definition of the resultant). Then the following is true:

(*i*) $R \neq 0$. Indeed, suppose R vanishes; then G and H have a common irreducible factor Q in the factorial ring A, with Q of degree ≥ 1 in Y. Then Q is one of the irreducible factors of G, hence does not depend on $V_1, \dots, V_r$; in the same way Q does not depend on $U_1, \dots, U_r$, hence is a common factor of $F_1, \dots, F_r$ in the ring $K[X_1, \dots, X_n, Y]$; this is a contradiction.

(*ii*) The polynomial R is of total degree $\le 2L_0L_1$ in $X_1, \dots, X_n$.

(*iii*) For $j \in J$, we have $R(U_1, \dots, U_r, V_1, \dots, V_r, \xi_j) = 0$, because R is a linear combination of G and H with coefficients in the ring A.

We obtain the desired polynomial in $K[X_1, \dots, X_n]$ vanishing at all the points $\xi_1, \dots, \xi_N$ by taking any non-zero coefficient of a monomial in $U_1, \dots, U_r, V_1, \dots, V_r$ in the expansion of R in $K[X_1, \dots, X_n][U_1, \dots, U_r, V_1, \dots, V_r]$. □

c) *Another lemma*

Here we solve a very simple functional equation.

Lemma 5.4. — *Let $Q \in K[X_1, \dots, X_n, Y]$ be irreducible and of degree ≥ 1 in Y. Let $u_1, \dots, u_n, v, \lambda$ be elements of K with $\lambda \neq 0$ and v not a root of unity. Assume*

$$Q(X_1 + u_1, \dots, X_n + u_n, vY) = \lambda Q(X_1, \dots, X_n, Y).$$

Then Y divides Q.

Proof. We expand Q in $K[\underline{X}][Y]$:

$$Q(\underline{X}, Y) = \sum_{i=0}^{d} a_i(\underline{X}) Y^j,$$

and we write our assumption:

$$a_i(\underline{X} + \underline{u}) v^i = \lambda a_i(\underline{X}), \qquad (0 \leq i \leq d).$$

Looking at the homogeneous term of higher degree in $a_i(\underline{X})$, we deduce $v^i = \lambda$ for all i such that $a_i(\underline{X}) \neq 0$. Since v is not a root of unity, there is only one index i for which $a_i(\underline{X}) \neq 0$; further we have $i \neq 0$ because Q depends on Y. This shows that Q reduces to a single term $a_i(X)Y^i$ with $i \neq 0$ and $a_i(X) \in K[X]$; our assumption that Q is irreducible implies that it is of the form cY with $c \in K$, $c \neq 0$. □

d) *Proof of lemma* 5.2

Obviously we may suppose that Y does not divide P and that $P \notin K[X_1, \dots, X_n]$. For $\underline{s} = (s_1, \dots, s_{n+1}) \in \mathbb{Z}^{n+1}$, we define a map $T_{\underline{s}}$ from the ring $K[X_1, \dots, X_n, Y]$ into itself by

$$T_{\underline{s}} Q(X_1, \dots, X_n, Y) = Q\big(X_1 + s_1 + s_{n+1}\beta_1, \dots, X_n + s_n + s_{n+1}\beta_n, \alpha_1^{s_1} \cdots \alpha_{n+1}^{s_{n+1}} Y\big).$$

The image of an irreducible polynomial is still an irreducible polynomial, and the degree in each variable of Q and $T_{\underline{s}}Q$ is the same.

1) We prove that the polynomials $T_{\underline{s}}P$ for $\underline{s} \in \mathbb{Z}^{n+1}(S')$ have no common irreducible factor of degree ≥ 1 in Y.

Let

$$P = Q_0 \prod_{i=1}^{k} Q_i^{r_i}$$

be a decomposition of P into a product, where $Q_0 \in K[\underline{X}]$ does not depend on Y, while for $1 \leq i \leq k$, Q_i is an irreducible polynomial in $K[\underline{X}, Y]$ of degree ≥ 1 in Y (such a decomposition is unique up to constant factors). We notice that $k \leq L_1$. Then

$$T_{\underline{s}} P = (T_{\underline{s}} Q_0) \prod_{i=1}^{k} (T_{\underline{s}} Q_i)^{r_i}$$

and $T_{\underline{s}}Q_0 \in K[\underline{X}]$ does not depend on Y, while for $1 \leq i \leq k$, $T_{\underline{s}}Q_i$ is an irreducible polynomial in $K[\underline{X}, Y]$ of degree ≥ 1 in Y. We proceed by contradiction: assume that there is an irreducible polynomial Q of degree ≥ 1 in Y which divides all $T_{\underline{s}}P$. Then for each such $\underline{s}$ there is an index $i(\underline{s})$ with $1 \leq i(\underline{s}) \leq k$ and a non-zero element $c_{\underline{s}}$ of K such that

$$Q = c_{\underline{s}} T_{\underline{s}} Q_{i(\underline{s})}.$$

Consider the map

$$\underline{s} \longmapsto \Big(i(\underline{s}), \sigma\big(\alpha_1^{s_1} \cdots \alpha_{n+1}^{s_{n+1}}\big) \Big)$$

from $\mathbb{Z}^{n+1}(S')$ into $\{1, \dots, k\} \times K^*/K^*_{\mathrm{tors}}$. Using our assumption on L_1 together with Dirichlet box principle, we see that there exist two different $\underline{s}$ in $\mathbb{Z}^{n+1}(S')$, say $\underline{s}'$ and $\underline{s}''$, for which the two following properties hold:

– the two indices $i(\underline{s}')$ and $i(\underline{s}'')$ are the same; let i_0 be this common value;

– the two elements $\sigma\big(\alpha_1^{s'_1} \cdots \alpha_{n+1}^{s'_{n+1}}\big)$ and $\sigma\big(\alpha_1^{s''_1} \cdots \alpha_{n+1}^{s''_{n+1}}\big)$ are distinct.

The difference $\underline{s} = \underline{s}' - \underline{s}''$ is a non-zero element of $\mathbb{Z}^{n+1}$ which has the property

$$T_{\underline{s}} Q_{i_0} = \lambda Q_{i_0}$$

for some $\lambda \in K^*$ and

$$\alpha_1^{s_1} \cdots \alpha_{n+1}^{s_{n+1}} \qquad \text{is not a root of unity.}$$

Since Y does not divide P, lemma 5.4 with

$$u_i = s_i + s_{n+1}\beta_i, \qquad (1 \le i \le n), \qquad v = \alpha_1^{s_1} \cdots \alpha_{n+1}^{s_{n+1}}$$

gives the desired contradiction.
2) The application of lemma 5.3 to the set of polynomials

$$\{F_1, \dots, F_r\} = \left\{T_{\underline{s}'} P\,;\, \underline{s}' \in \mathbb{Z}^{n+1}(S')\right\}$$

and to the following set $\{(\xi_i, \eta_i)\,;\, 1 \le i \le N\} \subset K^n \times K^*$:

$$\left\{(s_1'' + s_{n+1}''\beta_1, \dots, s_n'' + s_{n+1}''\beta_n, \alpha_1^{s_1''} \cdots \alpha_{n+1}^{s_{n+1}''})\,;\, \underline{s}'' \in \mathbb{Z}^{n+1}(S'')\right\}$$

gives the conclusion. □

1 An homogeneous zero estimate for the additive group K^n As we said earlier, the proof of this section relies on Moreau's version [Mo] of Masser's paper OPEP [Ma] as well as on Philippon's paper [P]. I am thankful to Daniel Bertrand, Laurent Denis, Patrice Philippon and Damien Roy for useful discussions on this matter.

a) *Statement of the result*

The aim of this §3 is to prove the following result:

Lemma 5.5. — *Let $\beta_1, \dots, \beta_n$ be elements of K. Assume that there exist two integers D and S satisfying*

$$\left(\frac{2S}{n} - 1\right)^{n+1} > D^n,$$

and also that there exists a non-zero polynomial $P \in K[X_1, \dots, X_n]$, of total degree $\le D$ which vanishes on the set

$$\left\{(s_1 + s_{n+1}\beta_1, \dots, s_n + s_{n+1}\beta_n)\,;\, (s_1, \dots, s_{n+1}) \in \mathbb{Z}^{n+1}(S)\right\}.$$

Then $1, \beta_1, \dots, \beta_n$ are linearly dependent over $\mathbb{Q}$.

In the case $n = 2$ one can prove such a result by using the same argument as in §2 (see exercise 3); hence for a proof of Baker's theorem with only three logarithms the resultant is sufficient. The general case will be dealt with by means of Bézout's theorem.

b) *Bézout's theorem*

Here is the geometric tool of this Chapter.

Lemma 5.6. — *Assume K is algebraically closed. Let $(P_i)_{i \in I}$ be a family of polynomials in $K[X_1, \dots, X_n]$, each of which is of total degree $\le D$. Assume that the set F of common zeroes to all P_i in K^n is finite. Then*

$$\mathrm{Card} F \le D^n.$$

Proof. We shall use some properties of the degree of affine varieties; we refer to exercise 4 in Chapter 8 for another proof.

We may assume $I = \{1, \dots, n\}$ by replacing, if necessary, the family $(P_i)_{i \in I}$ by a *regular sequence* of n polynomials in the ideal they generate (cf. [Ma], "inductive lemma"; the argument is similar to Kronecker u-resultant in lemma 5.3), which means that, for $1 \le i \le n$, the algebraic set

$$Y_i = Z(P_1) \cap \cdots \cap Z(P_i)$$

is of codimension i. In this case, if we denote by D_i the total degree of P_i, $(1 \leq i \leq n)$, we show that

$$\mathrm{Card} F \leq D_1 \cdots D_n.$$

For $1 \leq i \leq n-1$, Y_i is not contained in the hypersurface $H_i = Z(P_{i+1})$, hence

$$\deg(Y_i \cap H_i) \leq (\deg Y_i)(\deg H_i).$$

However $Y_i \cap H_i = Y_{i+1}$ and $\deg H_i = D_{i+1}$. By induction we deduce

$$\deg Y_i \leq D_1 \cdots D_i, \qquad (1 \leq i \leq n).$$

For $i = n$, the degree of $F = Y_n$ is nothing else than $\mathrm{Card} F$. □

Remark. Much deeper results are given in [V].

c) *A further lemma*

When $\mathcal{V}$ is a vector subspace of K^n and F any finite subset of K^n, we denote by $(F+\mathcal{V})/\mathcal{V}$ the image of F under the canonical map of K^n onto $K^n/\mathcal{V}$.

Lemma 5.7. *Let $\mathcal{V}$ be a vector subspace of K^n of codimension r, F a finite subset of K^n, and $(P_i)_{i\in I}$ a set of polynomials in $K[X_1, \ldots, X_n]$, each of which is of total degree $\leq D$. Assume that the set of common zeroes in K^n of all P_i is*

$$F + \mathcal{V} = \{y + v\,;\, y \in F, v \in \mathcal{V}\}.$$

Then

$$\mathrm{Card}\big((F+\mathcal{V})/\mathcal{V}\big) \leq D^r.$$

Proof. The case $\mathcal{V} = 0$, $r = n$ follows from lemma 5.6. In the general case, after a change of basis of K^n, we may assume $\mathcal{V} = K^{n-r} \times \{0\}^r$; hence we identify $K^n/\mathcal{V}$ with $\{0\}^{n-r} \times K^r$. We apply lemma 5.6 to the following polynomials in r variables

$$P_i(v, X_{n-r+1}, \ldots, X_n), \qquad (i \in I, v \in \mathcal{V});$$

indeed the set of common zeroes of these polynomials is exactly $(F+\mathcal{V})/\mathcal{V}$. □

d) *The main zero estimate*

We now prove a general zero estimate from which we shall later deduce lemma 5.5.

When E is a subset of K^n containing 0 and d a non-negative integer, we define

$$E[d] = \big\{x_1 + \cdots + x_d\,;\, x_i \in E,\, (1 \leq i \leq d)\big\};$$

for instance $E[0] = \{0\}$, $E[1] = E$ and $E[0] \subset E[1] \subset E[2] \cdots$

Proposition 5.8. *Let n and D two positive integers and E a subset of K^n containing 0. Assume that there exists a non-zero polynomial $P \in K[X_1, \ldots, X_n]$, of total degree $\leq D$, which vanishes on $E[n]$; then there exists a vector subspace $\mathcal{V}$ of K^n of codimension $r \geq 1$ in K^n such that*

$$\mathrm{Card}\big((E+\mathcal{V})/\mathcal{V}\big) \leq D^r.$$

Proof. There is no loss of generality to assume that the field K is algebraically closed. Denote by $Z = Z(P)$ the hypersurface which is defined by P in K^n. We introduce a collection of algebraic subsets of K^n:

$$Z_0 = Z, \qquad Z_1 = \bigcap_{\gamma \in E} (Z_0 - \gamma),$$

$$Z_s = \bigcap_{\gamma\in E} (Z_{s-1} - \gamma), \qquad (1 \le s \le n),$$

so that

$$Z_n = \bigcap_{\gamma\in E[n]} (Z - \gamma).$$

Our hypothesis that Z contains $E[n]$ implies that for $1 \le s \le n$, Z_s contains $E[n-s]$, and in particular Z_n contains 0. Moreover we have

$$Z_0 \supset Z_1 \supset \cdots \supset Z_n$$

because $0 \in E$. Notice that Z_0 is of dimension $n-1$ while Z_n is of dimension ≥ 0; let t be the largest integer in the range $1 \le t \le n$ for which $\dim Z_{t-1} \le n - t$. Therefore $n - t - 1 < \dim Z_t \le \dim Z_{t-1} \le n - t$. The two algebraic sets Z_t and Z_{t-1} have the same dimension, hence have a common component Y of dimension $n - t$. Define

$$\mathcal{S} = \big\{x \in K^n\,;\, x + Y \subset Z_{t-1}\big\}.$$

For each $\gamma \in E$ we have $\gamma + Z_t \subset Z_{t-1}$; this shows that $\mathcal{S}$ contains E. Now let

$$\mathcal{V} = \big\{x \in K^n\,;\, x + Y = Y\big\}.$$

Then $\mathcal{V}$ is at the same time an additive subgroup of K^n, and an algebraic subset of K^n:

$$\mathcal{V} = \bigcap_{y\in Y} (Y - y);$$

hence $\mathcal{V}$ is a vector subspace of K^n (cf. exercise 6). Moreover

$$\mathcal{S} = \bigcap_{y\in Y} (Z_{t-1} - y) = \bigcap_{y\in Y} \bigcap_{\gamma_1\in E} \cdots \bigcap_{\gamma_{t-1}\in E} \big(Z - y - \gamma_1 - \cdots - \gamma_{t-1}\big);$$

this shows that $\mathcal{S}$ is an algebraic set of dimension $\le \dim Z_t$, which is intersection of hypersurfaces of degrees $\le D$. Next $\mathcal{S}$ contains $\mathcal{V}$; further, for $x \in \mathcal{S}$, we have $x + \mathcal{V} \subset \mathcal{S}$. Furthermore, for x' and x'' in K^n, the condition $x' + Y = x'' + Y$ implies $x' + \mathcal{V} = x'' + \mathcal{V}$. However, since Z_{t-1} has only finitely many connected components (for the Zariski topology), the set of $x + Y$ with $x \in \mathcal{S}$ is finite, and therefore the set of classes $x + \mathcal{V}$ also; we choose a finite subset $F = \{x_1, \ldots, x_m\}$ in K^n so that $\mathcal{S}/\mathcal{V} = (F + \mathcal{V})/\mathcal{V}$; we see that $\mathcal{S}$ and $\mathcal{V}$ have the same dimension, say $n - r$, the irreducible components of $\mathcal{S}$ being the $x_i + \mathcal{V}$, $1 \le i \le m$. We also have $r \ge 1$; in fact, since

$$n - r = \dim \mathcal{S} \le \dim Z_{t-1} = n - t,$$

we have $1 \le t \le r$. We conclude by using lemma 5.7:

$$\mathrm{Card}\big((E + \mathcal{V})/\mathcal{V}\big) \le \mathrm{Card}(\mathcal{S}/\mathcal{V}) \le D^r.$$

□

e) *A lemma on the subgroup $\mathbb{Z}^n + \mathbb{Z}(\beta_1, \ldots, \beta_n)$ of K^n*

For the proof of lemma 5.5 we need one more lemma which explains how the conclusion on the linear dependence of $1, \beta_1, \ldots, \beta_n$ will appear: it comes from the conclusion of Proposition 5.8.

Lemma 5.9. — *Let $\beta_1, \ldots, \beta_n$ be elements of K. Define*

$$\begin{aligned} Y &= \mathbb{Z}^n + \mathbb{Z}(\beta_1, \ldots, \beta_n) \subset K^n \\ &= \big\{(s_1 + s_{n+1}\beta_1, \ldots, s_n + s_{n+1}\beta_n)\,;\, (s_1, \ldots, s_{n+1}) \in \mathbb{Z}^{n+1}\big\} \end{aligned}$$

and, for $S \ge 1$, $S \in \mathbb{Z}$,

$$Y(S) = \big\{(s_1 + s_{n+1}\beta_1, \ldots, s_n + s_{n+1}\beta_n)\,;\, (s_1, \ldots, s_{n+1}) \in \mathbb{Z}^{n+1}(S)\big\}.$$

Then the following conditions are equivalent.
(*i*) *The numbers* $1, \beta_1, \dots, \beta_n$ *are linearly independent over* $\mathbb{Q}$.
(*ii*) *For any vector subspace* $\mathcal{V} \subset K^n$ *of codimension* $r \geq 1$, *we have*

$$\mathrm{rk}_{\mathbb{Z}}\Big((Y+\mathcal{V})/\mathcal{V}\Big) \geq r+1.$$

(*iii*) *For all* $S \geq 1$ *and any vector subspace* $\mathcal{V} \subset K^n$ *of codimension* $r \geq 1$, *we have*

$$\mathrm{Card}\Big(\big(Y(S)+\mathcal{V}\big)/\mathcal{V}\Big) \geq (2S-1)^{r+1}.$$

(*ii*)$'$ *For any vector subspace* $\mathcal{W} \subset K^{n+1}$ *of codimension* $r \geq 1$, *containing* $(\beta_1, \dots, \beta_n, -1)$, *we have*

$$\mathrm{rk}_{\mathbb{Z}}\Big((\mathbb{Z}^{n+1}+\mathcal{W})/\mathcal{W}\Big) \geq r+1.$$

(*iii*)$'$ *For all* $S \geq 1$ *and any vector subspace* $\mathcal{W} \subset K^{n+1}$ *of codimension* $r \geq 1$ *containing* $(\beta_1, \dots, \beta_n, -1)$, *we have*

$$\mathrm{Card}\Big(\big(\mathbb{Z}^{n+1}(S)+\mathcal{W}\big)/\mathcal{W}\Big) \geq (2S-1)^{r+1}.$$

Proof.
The proofs of (*ii*) $\Leftrightarrow$ (*ii*)$'$ and of (*iii*) $\Leftrightarrow$ (*iii*)$'$ are easily obtained by considering the linear surjective map

$$\begin{array}{ccc} K^{n+1} & \longrightarrow & K^n \\ (z_1, \dots, z_{n+1}) & \longmapsto & (z_1 + z_{n+1}\beta_1, \dots, z_n + z_{n+1}\beta_n) \end{array}$$

whose kernel is the line $K(\beta_1, \dots, \beta_n, -1)$.

The fact that (*iii*) $\Rightarrow$ (*ii*) is trivial. Also the implication (*ii*)$' \Rightarrow$ (*i*) is clear: (*ii*)$'$ implies that the point $(\beta_1, \dots, \beta_n, -1)$ is not contained in a hyperplane which is rational over $\mathbb{Q}$.

The useful part of the statement is (*i*) $\Rightarrow$ (*iii*)$'$. Assume $\mathrm{Card}\Big(\big(\mathbb{Z}^{n+1}(S)+\mathcal{W}\big)/\mathcal{W}\Big) < (2S-1)^{r+1}$. Let $\sigma_{\mathcal{W}} : K^{n+1} \to K^{n+1}/\mathcal{W}$ denote the canonical surjective map and $(e_1, \dots, e_{n+1})$ denote the canonical basis of K^{n+1}. There exists a subset $\{i_1, \dots, i_r\}$ of $\{1, \dots, n+1\}$ such that $\big(\sigma_{\mathcal{W}}(e_{i_1}), \dots, \sigma_{\mathcal{W}}(e_{i_r})\big)$ is a basis of $K^{n+1}/\mathcal{W}$. For ease of notation we assume that $\{i_1, \dots, i_r\} = \{1, \dots, r\}$.

Let j be an index in the range $r+1 \leq j \leq n+1$. We consider the elements $\underline{s}$ of $\mathbb{Z}^{n+1}$ for which $s_i = 0$ for $r+1 \leq i \leq n+1$ and $i \neq j$; the elements

$$\sigma_{\mathcal{W}}(s_1e_1 + \cdots + s_re_r + s_je_j)\,;\, (s_1, \dots, s_r, s_j) \in \mathbb{Z}^{r+1}(S)$$

belong to $\big(\mathbb{Z}^{n+1}(S)+\mathcal{W}\big)/\mathcal{W}$; since $\mathrm{Card}\big(\mathbb{Z}^{r+1}(S)\big) > \mathrm{Card}\Big(\big(\mathbb{Z}^{n+1}(S)+\mathcal{W}\big)/\mathcal{W}\Big)$, these elements are not pairwise distinct (this is once more a consequence of the pigeon hole principle). Hence there is a relation

$$a_1^{(j)}e_1 + \cdots + a_r^{(j)}e_r + e_j \in \mathcal{W}$$

with rational numbers $a_i^{(j)}$. This means that $\mathcal{W}$ is generated by the $n+1-r$ elements

$$\big(a_1^{(j)}, \dots, a_r^{(j)}, 0, \dots, 0, 1, 0, \dots, 0\big) \in \mathbb{Q}^{n+1} \qquad (r+1 \leq j \leq n+1).$$

Since $n+1-r = \dim \mathcal{W} < n+1$, the $(n+1-r) \times (n+1)$ matrix

$$\begin{pmatrix} a_1^{(r+1)} & \cdots & a_r^{(r+1)} & 1 & 0 & \cdots & 0 \\ a_1^{(r+2)} & \cdots & a_r^{(r+2)} & 0 & 1 & \cdots & 0 \\ \vdots & \ddots & \cdots & \vdots & \vdots & \ddots & \vdots \\ a_1^{(n+1)} & \cdots & a_r^{(n+1)} & 0 & 0 & \cdots & 1 \end{pmatrix}$$

is of rank $n+1-r < n+1$; therefore there exists $(b_1,\dots,b_{n+1}) \in \mathbb{Z}^{n+1}$, $(b_1,\dots,b_{n+1}) \neq 0$, such that

$$b_1 z_1 + \cdots + b_{n+1} z_{n+1} = 0 \qquad \text{for all} \quad z \in \mathcal{W};$$

in other terms $\mathcal{W}$ is a subspace of K^{n+1} which is generated by elements of $\mathbb{Q}^{n+1}$; this means that it is *rational over* $\mathbb{Q}$; since it is of codimension ≥ 1, it follows that it is contained in a hyperplane which is rational over $\mathbb{Q}$ (cf. Chapter 1 exercise 4). Now the point $(\beta_1,\dots,\beta_n,-1)$ belongs to $\mathcal{W}$, hence we get the desired non-trivial linear dependence relation between $\beta_1,\dots,\beta_n$ and 1. □

f) *Proof of lemma* 5.5

For $x \in \mathbb{R}$ we denote by $\lfloor x \rfloor$ the smallest integer $\geq x$: in other words $x \leq \lfloor x \rfloor < x+1$. Put $S_1 = \lfloor S/n \rfloor$; this means that S_1 is the integer defined by $S \leq nS_1 \leq S+n-1$. If $a_1,\dots,a_n$ are rational integers with $a_i < S_1$, then $a_1 + \cdots + a_n < S$. Therefore, if we set

$$E = \big\{(s_1 + s_n\beta_1,\dots,s_n + s_{n+1}\beta_n)\,;\, |s_j| < S_1, (1 \leq j \leq n+1)\big\},$$

then $E[n] \subset Y(S)$. Under the assumptions of lemma 5.5, the polynomial P vanishes on $Y(S)$, hence on $E[n]$. From Proposition 5.8 we deduce that there exists a vector subspace $\mathcal{V}$ of K^n of codimension $r \geq 1$ in K^n such that

$$\mathrm{Card}\big((E+\mathcal{V})/\mathcal{V}\big) \leq D^r.$$

Our hypothesis

$$D^n < \left(\frac{2S}{n} - 1\right)^{n+1},$$

implies

$$D^r < (2S_1 - 1)^{r+1},$$

hence

$$\mathrm{Card}\big((E+\mathcal{V})/\mathcal{V}\big) < (2S_1-1)^{r+1}.$$

Finally lemma 5.9 (with S replaced by S_1) implies that $1, \beta_1 \dots, \beta_n$ are linearly dependent over the rationals. □

1 Proof of Proposition 5.1 We start with the assumptions of Proposition 5.1. Define $S'' = \lfloor S/2 \rfloor$ and $S' = S - S'' + 1$. Our assumption the $\alpha_1,\dots,\alpha_{n+1}$ generate a multiplicative group of rank $\geq n$ means that there exists n distinct elements $\{i_1,\dots,i_n\}$ among $\{1,\dots,n+1\}$ such that $\alpha_{i_1},\dots,\alpha_{i_n}$ are multiplicatively independent. Since $S+1 \leq 2S' \leq S+2$, our hypothesis $S^n > L_1$ implies $(2S'-1)^n > L_1$. This shows that the assumptions of lemma 5.2 are satisfied.

Our assumption $S \geq 2n(n+1)$ enables us to deduce from the main condition $(S/2n)^{n+1} \geq (L_0L_1)^n$ the inequality $\big((S/n)-1\big)^{n+1} > (2L_0L_1)^n$; from the inequality $S'' \geq S/2$ we deduce $(2L_0L_1)^n < \big((2S''/n) - 1\big)^{n+1}$; this shows that the hypotheses of lemma 5.5 are satisfied with $D = 2L_0L_1$ and S replaced by S''. This completes the proof of Proposition 5.1. □

1Open problems **1.** The conclusion of lemma 5.2 in the case $n=1$ is that the set of $s_1 + s_2\beta_1$, for $\underline{s} \in \mathbb{Z}^2(S'')$, has at most $2L_0L_1$ elements. Is-it possible to improve the constant 2 in this upper bound ? This would enable one to improve the lower bounds for linear forms in two logarithms (see [MW]). One cannot replace 2 by a constant < 1.

2. Can one improve the constant $(n/2)^{n+1}$ (when $n \geq 2$) in the hypothesis of Lemma 5.5 ?

1Exercises **1.** Using lemma 5.2, complete the proof of Gel'fond-Schneider theorem in the complex cases (going back to the proof of the real case in Chapter 2 §4, replace lemma 2.1 by lemma 5.2).

2. Prove the following refinement of Proposition 5.1 (compare with [MW] Proposition 4.1) : one can replace the hypotheses

$$(S/2n)^{n+1} \geq (L_0L_1)^n, \qquad S \geq 2n(n+1) \qquad \text{and} \qquad S^n > L_1,$$

by

$$\left(\frac{S''}{n}-1\right)^{n+1} \geq (L_0L_1)^n$$

and

$$\mathrm{Card}\Big\{\sigma\big(\alpha_1^{s_1}\cdots\alpha_{n+1}^{s_{n+1}}\big)\,;\,\underline{s}\in\mathbb{Z}^{n+1}(S')\Big\} > L_1$$

(with the same notations as in lemma 5.2) when S' and S'' are positive integers with $S = S' + S'' - 1$.

3. Using a resultant in the same way as in §2, prove the following variant of the case $n = 2$ of lemma 5.5: Let β_1, β_2 be two elements of K. Assume that there exist integers D, S', S'' and S satisfying

$$S = S' + S'' - 1, \qquad (2S'-1)^2 > D \qquad \text{and} \qquad (2S''-1)^3 > 2D^2,$$

and also that there exists a non-zero polynomial $P \in K[X_1, X_2]$, of total degree $\leq D$ which vanishes on the set

$$\big\{(s_1 + s_3\beta_1, s_2 + s_3\beta_2)\,;\,(s_1,s_2,s_3)\in\mathbb{Z}^3(S)\big\} \subset K^2.$$

Then $1, \beta_1, \beta_2$ are linearly dependent over $\mathbb{Q}$.

`Hint.` *Define* $\Gamma(S) = \big\{(s_1 + s_3\beta_1, s_2 + s_3\beta_2)\,;\,(s_1,s_2,s_3)\in\mathbb{Z}^3(S)\big\}$, *and similarly* $\Gamma(S')$ *and* $\Gamma(S'')$. *For* $\gamma = (\gamma_1,\gamma_2) \in K^2$, *define* $T_\gamma P(X,Y) = P(\gamma_1 + X, \gamma_2 + Y)$.
a) *Assume that the polynomials* $T_\gamma P$, $\gamma \in \Gamma(S')$ *have a common irreducible factor* Q. *Show that there exist* $c \in K^*$ *and* $\gamma^0 = (\gamma_1^0,\gamma_2^0) \in \Gamma(2S'-1)$ *with* $\gamma^0 \neq 0$ *and* $T_{\gamma^0}Q = cQ$. *Show that there exists* $R \in K[T]$ *such that* $Q(X,Y) = R(\gamma_2^0X - \gamma_1^0Y)$. *Check that the set of* $\vartheta \in K$ *such that* $R(\gamma_2^0X - \gamma_1^0Y + \vartheta)$ *divides* P *has at most* D *elements. Deduce that there are at most* D *elements in the image of* $\Gamma(S')$ *under the mapping* $K^2 \longrightarrow K$ *which maps* (z_1,z_2) *to* $\gamma_2^0z_1 - \gamma_1^0z_2$. *Derive the desired conclusion from lemma* 5.9.
b) *Assume that the polynomials* $T_\gamma P$, $\gamma \in \Gamma(S')$ *have no common irreducible factor. The goal is to show* $\mathrm{Card}\Gamma(S'') < (2S''-1)^3$, *which implies that* β_1 *and* β_2 *are both rational numbers. Show that, if* $\mathrm{Card}\Gamma(S'') = (2S''-1)^3$, *then there exists* $\lambda \in K^*$ *such that the* $(2S''-1)^3$ *numbers* $\gamma_1 + \lambda\gamma_2 \in K$, $(\gamma_1,\gamma_2) \in \Gamma(S'')$, *are pairwise distinct. Eliminate* Y *by means of Kronecker* u*-resultant between the polynomials* $T_\gamma P(X - \lambda Y, Y)$.

4. Prove the following variant of Proposition 5.8 (cf. [W2]) : let n and D two positive integers and $E_1,\dots,E_n$ subsets of K^n containing 0. Assume that there exists a non-zero polynomial $P \in K[X_1,\dots,X_n]$, of total degree $\leq D$, which vanishes on

$$E_1 + \cdots + E_n := \big\{x_1 + \cdots + x_n\,;\,x_i \in E_i,\,1 \leq i \leq n\big\}.$$

then there exists an integer t and a vector subspace $\mathcal{V}$ of K^n, of codimension r in K^n, such that

$$\mathrm{Card}\big((E_t + \mathcal{V})/\mathcal{V}\big) \leq D^r$$

and

$$1 \leq t \leq r \leq n.$$

5. Let n and D two positive integers and E a subset of K^n. Assume that there exists a vector subspace $\mathcal{V}$ of K^n of codimension $r \geq 1$ in K^n such that

$$\mathrm{Card}\big((E + \mathcal{V})/\mathcal{V}\big) < \binom{D+r}{r}.$$

Show that there exists a non-zero polynomial $P \in K[X_1,\dots,X_n]$, of total degree $\leq D$, which vanishes on E.

6. A subset $\mathcal{V}$ of K^n which is at the same time an additive subgroup of K^n and an algebraic subset of K^n is a vector subspace of K^n.
`Hint.` *See lemma* 8.6.

7. With the notations of lemma 5.9, prove that the conditions *(i)* to *(iii)'* are also equivalent to the following ones :

(iv) For any hyperplane $\mathcal{V}$ of K^n which is rational over $\mathbb{Q}$,

$$\mathrm{rk}_{\mathbb{Z}}\Big((Y+\mathcal{V})/\mathcal{V}\Big) \geq 2.$$

(v) For all $S \geq 1$ and any hyperplane $\mathcal{V} \subset K^n$ which is rational over $\mathbb{Q}$, we have

$$\mathrm{Card}\Big(\big(Y(S)+\mathcal{V}\big)/\mathcal{V}\Big) \geq (2S-1)^2.$$

8. Using Theorem 8.1, prove the following variant of Proposition 5.1: *Let $\alpha_1, \ldots, \alpha_{n+1}$ be non-zero elements of K which generate a multiplicative subgroup of K^* of rank $\geq n$. Let $\beta_1, \ldots, \beta_n$ be elements of K. Assume that there exist three positive rational integers L_0, L_1 and S satisfying*

$$2^n S^{n+1} \geq (n+1)^{n+2} L_0^n L_1, \qquad S \geq n(n+1) \qquad \text{and} \qquad L_0 \geq 4,$$

such that the rank of the matrix

$$\left((s_1 + s_{n+1}\beta_1)^{\lambda_1} \cdots (s_n + s_{n+1}\beta_n)^{\lambda_n} \big(\alpha_1^{s_1} \cdots \alpha_{n+1}^{s_{n+1}}\big)^{\lambda_{n+1}}\right)_{\underline{\lambda},\underline{s}},$$

is strictly less than $\binom{L_0+n}{n}(L_1+1)$. Then the numbers $1, \beta_1, \ldots, \beta_n$ are linearly dependent over $\mathbb{Q}$.

1References

[BM] W.D. Brownawell and D.W. Masser. – Multiplicity estimates for analytic functions; 2; Duke Math. J., **47** (1980), 273–295.

[G] A.O. Gel'fond. – *Transcendental Number Theory;* Moscow, 1952; English transl. Dover Publ., N.Y., 1960.

[Ma] D.W. Masser. – On polynomials and exponential polynomials in several variables; Invent. Math., **63** (1981), 81–95.

[MW] M. Mignotte and M. Waldschmidt. – Linear forms in two logarithms and Schneider's method, 2; Acta Arith., **53** (1989), 251–287.

[Mo] J-C. Moreau. – Démonstrations géométriques de lemmes de zéros; (1), Sém. Th. Nombres, Paris 1981–82, Birkhäuser P.M. **38** (1983), 201–205; (2), in *Approximations diophantiennes et nombres transcendants*, Birkhäuser P.M. **31** (1983), 191–197.

[P] P. Philippon. – Lemme de zéros dans les groupes algébriques commutatifs; Bull. Soc. Math. France, **114** (1986), 355–383, et **115** (1987), 397–398.

[V] W. Vogel. – *Lectures on Results on Bezout's theorem;* Tata Institute of Fundamental Research, Lectures on Mathematics and Physics, **74** (1984); Narosa Publ. House, New Delhi.

[W1] M. Waldschmidt. – *Nombres Transcendants;* Springer Lecture Notes in Math., **402** (1974).

[W2] M. Waldschmidt. – Nouvelles méthodes pour minorer des combinaisons linéaires de logarithmes de nombres algébriques; Sém. Th. Nombres Bordeaux, **3** (1991), 129–185.

[W3] M. Waldschmidt. – Minorations de combinaisons linéaires de logarithmes de nombres algébriques; Canadian J. Math., to appear.

6.– PROOF OF THE MAIN THEOREM

In this Chapter we complete the proof of Theorem 1.1

Step 0. Assumptions.

Let $\ell_1, \dots, \ell_{n+1}$ be $\mathbb{Q}$-linearly independent logarithms of algebraic numbers and $\beta_1, \dots, \beta_n$ be algebraic numbers. We assume

$$\ell_{n+1} = \beta_1 \ell_1 + \cdots + \beta_n \ell_n. \tag{6.1}$$

For $1 \le i \le n+1$, define $\alpha_i = e^{\ell_i}$.

The sentence "there exists a constant $c_1 > 0$ such that ..." means that one can compute explicitly (and easily: exercise 1) a number $c_1 > 0$ in terms of n, $\ell_1, \dots, \ell_{n+1}$ and $\beta_1, \dots, \beta_n$ which satisfies the desired property.

Step 1. Choice of the parameters.

We denote by c a sufficiently large real number depending only on n, $\ell_1, \dots, \ell_{n+1}$ as well as on $\beta_1, \dots, \beta_n$.

Next we choose three rational integers L_0, L_1 and S which are required to satisfy

$$L_0 \ge 2, \qquad L_1 \ge 2, \qquad S \ge 2,$$

$$cL_0 \log S \le L^{1/n}, \qquad cL_1 S \le L^{1/n}, \qquad c(L_0 L_1)^n \le S^{n+1},$$

with $L = \binom{L_0+n}{n}(L_1+1)$. For instance one can take

$$L_1 = [\log S]^{2n} \qquad \text{and} \qquad L_0 = [S^{1+1/n}(\log S)^{-3n}]$$

with S sufficiently large.

Step 2. Definition of Δ.

Consider the $L \times (2S-1)^{n+1}$ matrix

$$\mathcal{M} = \left((s_1 + s_{n+1}\beta_1)^{\lambda_1} \cdots (s_n + s_{n+1}\beta_n)^{\lambda_n} \left(\alpha_1^{s_1} \cdots \alpha_{n+1}^{s_{n+1}}\right)^{\lambda_{n+1}} \right)_{\underline{\lambda}, \underline{s}},$$

where the index of row is $\underline{\lambda}$ and the index of column is $\underline{s}$; as usual, $\underline{\lambda}$ runs over the $(n+1)$-tuples $(\lambda_1, \dots, \lambda_{n+1})$ of elements in $\mathbb{N}^{n+1}$ satisfying $\lambda_1 + \cdots + \lambda_n \le L_0$ and $\lambda_{n+1} \le L_1$, while $\underline{s}$ runs over the $(n+1)$-tuples in $\mathbb{Z}^{n+1}(S)$.

Let $s^{(1)}, \dots, s^{(L)}$ be any elements in $\mathbb{Z}^{n+1}(S)$. We consider the following determinant of a $L \times L$ matrix

$$\Delta = \det\left((s_1^{(\mu)} + s_{n+1}^{(\mu)}\beta_1)^{\lambda_1} \cdots (s_n^{(\mu)} + s_{n+1}^{(\mu)}\beta_n)^{\lambda_n} \left(\alpha_1^{s_1^{(\mu)}} \cdots \alpha_{n+1}^{s_{n+1}^{(\mu)}}\right)^{\lambda_{n+1}} \right)_{\underline{\lambda}, \mu}.$$

Step 3. Upper bound for $|\Delta|$.

Our assumption (6.1) enables us to write, for $(s_1, \dots, s_{n+1}) \in \mathbb{Z}^{n+1}$,

$$\alpha_1^{s_1 + s_{n+1}\beta_1} \cdots \alpha_n^{s_n + s_{n+1}\beta_n} = \alpha_1^{s_1} \cdots \alpha_{n+1}^{s_{n+1}}.$$

Therefore we can use Proposition 4.4: there exists a constant $c_1 > 0$ such that

$$\frac{1}{L} \log |\Delta| \le -L^{1/n} + c_1(L_0 \log S + L_1 S).$$

Step 4. Liouville inequality.

We use our assumption that the numbers $\alpha_1, \ldots, \alpha_{n+1}, \beta_1, \ldots, \beta_n$ are algebraic: from Proposition 3.15 we deduce that there exists a constant $c_2 > 0$ such that either $\Delta = 0$ or else

$$\frac{1}{L} \log |\Delta| \geq -c_2(L_0 \log S + L_1 S).$$

However in step 1 we chose c sufficiently large with respect to c_1 and c_2, and therefore we deduce from step 3 that $\Delta = 0$.

Step 5. Consequence of the zero estimate.

From Step 4 we deduce that the rank of the matrix $\mathcal{M}$ is strictly less than L.

Our hypothesis that $\log \alpha_1, \ldots, \log \alpha_{n+1}$ are linearly independent over $\mathbb{Q}$ implies that the rank of the multiplicative subgroup of $\mathbb{C}^*$ generated by $\alpha_1, \ldots, \alpha_{n+1}$ is at least n.

Our conditions on the parameters imply $L_1^{n-1} S^n < L_0^n$ and $L_0^n L_1^n < S^{n+1}$, hence $L_1^{2n-1} < S$. This allows us to use Proposition 5.1, and we deduce that $1, \beta_1, \ldots, \beta_n$ are linearly dependent over $\mathbb{Q}$. Thanks to lemma 1.3, this completes the proof of Theorem 1.1. □

1Exercise **1.** Compute the constants c_1 and c_2 above, and deduce a suitable value for c.

7.– A FIRST MEASURE WITH SIMPLE PROOF

In the second part of these lectures, which starts with the present Chapter, we produce explicit measures of linear independence of logarithms of algebraic numbers. In this Chapter we prove such an estimate by using the method of the first part. Our aim is to present a proof as transparent as possible, not to give a sharp estimate. The result we reach is far from the best known, but is non trivial, and is quite sufficient for many Diophantine problems. Refinements of this estimate will be discussed in Chapter 10.

1 Statement of the result

Theorem 7.1. — *Let $\ell_1, \dots, \ell_m$ be logarithms of algebraic numbers, $\alpha_i = \exp(\ell_i)$, $(1 \le i \le m)$ and $\beta_1, \dots, \beta_m$ be algebraic numbers. We assume that the number*

$$\Lambda = \beta_1\ell_1 + \cdots + \beta_m\ell_m$$

does not vanish. Let D be the degree of the number field $\mathbb{Q}(\alpha_1, \dots, \alpha_m, \beta_1, \dots, \beta_m)$ over $\mathbb{Q}$ and let $\log H$ be an upper bound for the absolute logarithmic height of the $2m$ numbers $\alpha_1, \dots, \alpha_m, \beta_1, \dots, \beta_m$, with $H \ge \max\{e, D\}$. Assume also $e|\ell_i| \le D \log H$ for $1 \le i \le m$. Then

$$|\Lambda| \ge \exp\bigl\{-(10^3 m^3 D \log H)^{\kappa(m)}\bigr\}$$

with $\kappa(m) = 2^m(m!)^2$.

Here is the plan of this Chapter. We show in section 2 that there is no loss of generality, for the proof of Theorem 7.1, to assume that the numbers $\ell_1, \dots, \ell_m$ are linearly independent over $\mathbb{Q}$. Next (§3) we consider the coefficients β_i; it would be a loss of generality to assume that they are independent over $\mathbb{Q}$; indeed, the most interesting case is when they are all rational integers; but we show that the general case can be reduced to the special case where the β_i satisfy some condition of linear independence; it turns out that, in the special case, we will be able to prove a stronger result (see Proposition 7.10). The purely transcendental part of the proof is given in section 4. We complete the proof of theorem 7.1 in section 5.

1 On the linear independence of the logarithms In this section we show that for the proof of Theorem 7.1, we may assume that the numbers $\ell_1, \dots, \ell_m$ are linearly independent over $\mathbb{Q}$.

We need the following lemma:

Lemma 7.2. — *Let $\ell_1, \dots, \ell_m$ be $\mathbb{Q}$-linearly dependent logarithms of algebraic numbers; define $\alpha_j = e^{\ell_j}$, $(1 \le j \le m)$. Let $\log H \ge 1$ be an upper bound for $\max_{1\le j\le m} \mathrm{h}(\alpha_j)$ and also for $\max_{1\le j\le m} |\ell_j|/D$, where D is the degree of the number field $K = \mathbb{Q}(\alpha_1, \dots, \alpha_m)$ over $\mathbb{Q}$. Then there exist rational integers $t_1, \dots, t_m$, not all of which are zero, such that*

$$t_1\ell_1 + \cdots + t_m\ell_m = 0$$

and

$$\max\{|t_1|, \dots, |t_m|\} \le \bigl(10^3 m D^3 \log H\bigr)^{m-1}.$$

Proof. (cf. [W] lemma 4.1, [L] Chap. 9 §7; see also [M]). We assume, as we may without loss of generality, that $m \ge 2$, and that any $m-1$ of $\ell_1, \dots, \ell_m$ are linearly independent. Thus there exists a unique (up to a factor ± 1) set of relatively prime integers $t_1, \dots, t_m$ such that

$$t_1\ell_1 + \cdots + t_m\ell_m = 0.$$

Hence

$$\alpha_1^{t_1} \cdots \alpha_m^{t_m} = 1.$$

Let k be an integer, $1 \le k \le m$. We define

$$c = (10^3 m D^3 \log H)^{-1}.$$

Using Minkowski's linear form theorem (e.g. [S1] p.33 Th. 2C) we see that there exist integers $s_1, \dots, s_m$, not all zero, such that

$$|s_j - s_k t_j/t_k| < c, \qquad (1 \le j \le m,\ j \ne k), \qquad \text{and} \qquad |s_k| \le 1/c^{m-1}.$$

We now prove the relation $s_1\ell_1 + \cdots + s_m\ell_m = 0$, from which the desired upper bound $|t_k| \le c^{-m+1}$ readily follows. We first show that the number $\alpha = \alpha_1^{s_1} \cdots \alpha_m^{s_m}$ is a root of unity. Using (3.3) and (3.5) for the number

$$\alpha^{t_k} = \prod_{j=1}^{m} \alpha_j^{s_j t_k} = \prod_{1 \le j \le m} \alpha_j^{s_j t_k - s_k t_j},$$

we get

$$|t_k| \mathrm{h}(\alpha) \le \sum_{1 \le j \le m, j \ne k} |s_j t_k - s_k t_j| \mathrm{h}(\alpha_j),$$

hence

$$\mathrm{h}(\alpha) \le cm \log H \le (10D)^{-3}.$$

So by Theorem 3.16 it follows that α is a root of unity. Let N be the order of α; then $\varphi(N) \le D$ (where φ is Euler function), therefore $N \le 2D^2 \le 2\pi/(cm|\ell_j|)$ and

$$N \sum_{j=1}^{m} s_j \ell_j \in 2i\pi\mathbb{Z}.$$

We observe that

$$\left| N \sum_{j=1}^{m} s_j \ell_j \right| = \left| N \sum_{j=1}^{m} \left(s_j - \frac{s_k t_j}{t_k} \right) \ell_j \right| < cN \sum_{1 \le j \le m, j \ne k} |\ell_j| \le 2\pi,$$

and we conclude

$$\sum_{i=1}^{m} s_j \ell_j = 0.$$

□

We deduce from lemma 7.2 the following result:

Lemma 7.3. – *Let m_0 be a positive integer and $U(x, y)$ be a positive function of two variables $x \in \mathbb{N}$, $x \ge 1$ and $y \in \mathbb{R}$, $y \ge 1$. For $1 \le m \le m_0$, denote by (P_m) the following property:*
(P_m) for each non-vanishing linear combination

$$\Lambda = \beta_1\ell_1 + \cdots + \beta_m\ell_m$$

of logarithms of algebraic numbers with algebraic coefficients, if the field

$$\mathbb{Q}(e^{\ell_1}, \dots, e^{\ell_m}, \beta_1, \dots, \beta_m)$$

has degree $\le D$ over $\mathbb{Q}$, and if $H \ge \max\{e, D\}$ satisfies, for $1 \le j \le m$,

$$\log H \ge \mathrm{h}(\alpha_j), \qquad \log H \ge e|\ell_j|/D \qquad \textit{and} \qquad \log H \ge \mathrm{h}(\beta_j),$$

then

$$|\Lambda| \ge \exp\bigl\{-U(m, D \log H)\bigr\}.$$

Assume, for $1 \le m \le m_0$, that (P_m) holds whenever $\ell_1, \dots, \ell_m$ are linearly independent over $\mathbb{Q}$. Assume further that, for $2 \le m \le m_0$ and $T = (10^3 m D^3 \log H)^{m-1}$, the following inequality holds:

$$U\big(m-1, D\log(2TH^2)\big) + \log T \le U(m, D\log H).$$

Then, for $1 \le m \le m_0$, (P_m) holds also when $\ell_1, \dots, \ell_m$ are linearly dependent over $\mathbb{Q}$.

Proof. The proof is by induction on m_0; for $m_0 = 1$ the result is obvious: since Λ does not vanish, the number ℓ_1 is not zero, hence is independent over $\mathbb{Q}$. Assume $m_0 \ge 2$; consider a non-vanishing linear combination in m logarithms (with $m \le m_0$) such that there is a linear dependence relation between $\ell_1, \dots, \ell_m$; from lemma 7.2 we deduce that there exist rational integers $t_1, \dots, t_m$ such that

$$t_1\ell_1 + \cdots + t_m\ell_m = 0$$

and

$$0 < \max\{|t_1|, \dots, |t_m|\} \le T \qquad \text{with} \qquad T = \big(10^3 m D^3 \log H\big)^{m-1}.$$

One of the t_i, say t_m, is not zero. We eliminate ℓ_m:

$$t_m\Lambda = \tilde\beta_1\ell_1 + \cdots + \tilde\beta_{m-1}\ell_{m-1}$$

with $\tilde\beta_j = t_m\beta_j - \beta_m t_j$, $(1 \le j \le m-1)$. Lemma 3.6 with $f(X_1, X_2) = t_m X_1 - t_j X_2$ shows that, for $1 \le j \le m-1$, the height of $\tilde\beta_j$ is bounded by

$$\mathrm{h}(\tilde\beta_j) \le \log(2T) + \mathrm{h}(\beta_j) + \mathrm{h}(\beta_m) \le \log H' \qquad \text{with} \qquad H' = 2TH^2.$$

We deduce, either from the induction hypothesis (if $\ell_1, \dots, \ell_{m-1}$ are linearly dependent) or from hypothesis (P_{m-1}) (otherwise):

$$|t_m\Lambda| \ge \exp\big\{-U\big(m-1, D\log H'\big)\big\}.$$

Hence

$$\begin{aligned} |\Lambda| &\ge \exp\big\{-U\big(m-1, D\log H'\big) - \log T\big\} \\ &\ge \exp\big\{-U\big(m, D\log H\big)\big\}. \end{aligned}$$

□

Using lemma 7.3 with the function

$$U\big(m, D\log H\big) = (10^3 m^3 D\log H)^{\kappa(m)},$$

where $\kappa(m) = 2^m(m!)^2$, we see that there is no loss of generality, for the proof of Theorem 7.1, to assume that $\ell_1, \dots, \ell_m$ are linearly independent over $\mathbb{Q}$. Notice that the assumption of lemma 7.3 (namely that property (P_m) is satisfied when the ℓ_i are linearly independent) is true for $m = 1$ thanks to Liouville's inequality (see exercise 6 a in Chapter 3).

1On the linear independence of the coefficients The transcendence argument requires that some determinant does not vanish; an easy way of ensuring this condition is to assume that the coefficients $\beta_1, \dots, \beta_m$ satisfy some linear independence condition. We show here how the general case will follow.

Lemma 7.4. – *Let m_0 be a positive integer, $U(x, y)$ and $T_0(x, y)$ be two positive functions of two variables $x \in \mathbb{N}$, $x \ge 1$ and $y \in \mathbb{R}$, $y \ge 1$. Denote by (P_m) the same property as in lemma 7.3. Assume, for $1 \le m \le m_0$, that (P_m) holds provided that $\beta_1, \dots, \beta_m$ satisfy the following linear independence condition: for $(b_1, \dots, b_m) \in \mathbb{Z}^m$ with $0 < \max\{|b_1|, \dots, |b_m|\} < T_0(m, D\log H)$, we have*

$$b_1\beta_1 + \cdots + b_m\beta_m \ne 0.$$

Assume further that, for $2 \le m \le m_0$, the following inequality holds:

$$U\big(m-1, 2D(\log H)T_0(m, D\log H)\big) + \log T_0(m, D\log H) \le U(m, D\log H).$$

Then, for $1 \le m \le m_0$, (P_m) holds also when $\beta_1, \dots, \beta_m$ do not satisfy the linear independence condition.

Proof. Once more the proof is by induction on m_0, once more the result is obvious if $m_0 = 1$. Take m with $2 \le m \le m_0$. Assume that there exists $(b_1, \dots, b_m) \in \mathbb{Z}^m$ with $0 < \max\{|b_1|, \dots, |b_m|\} < T_0(m, D\log H)$ such that

$$b_1\beta_1 + \cdots + b_m\beta_m = 0.$$

One of the coefficients, say b_m, does not vanish; we eliminate β_m:

$$b_m\Lambda = \sum_{i=1}^{m-1} \beta_i\tilde{\ell}_i$$

with

$$\tilde{\ell}_i = b_m\ell_i - b_i\ell_m, \qquad (1 \le i \le m-1).$$

Notice that, when $\ell_1, \dots, \ell_m$ are linearly independent, then $\tilde{\ell_1}, \dots, \tilde{\ell_{m-1}}$ are also linearly independent. If we set $\alpha_i = \exp(\ell_i)$ and $\tilde{\alpha}_i = \exp(\tilde{\ell}_i)$, we have $\tilde{\alpha}_i = \alpha_i^{b_m}/\alpha_m^{b_i}$ and

$$\mathrm{h}(\tilde{\alpha}_i) \le |b_m|\mathrm{h}(\alpha_i) + |b_i|\mathrm{h}(\alpha_m) \le \log H' \qquad \text{with} \qquad \log H' = 2(\log H)T_0(m, D\log H).$$

From the induction hypothesis or from hypothesis (P_{m-1}) we deduce

$$|b_m\Lambda| \ge \exp\bigl\{-U(m-1, D\log H')\bigr\},$$

hence

$$\begin{aligned}|\Lambda| &\ge \exp\bigl\{-U(m-1, D\log H') - \log T_0(m, D\log H)\bigr\}\\ &\ge \exp\bigl\{-U(m, D\log H)\bigr\}.\end{aligned}$$

□

We shall use lemma 7.4 with

$$U(m, D\log H) = \bigl(10^3m^3D\log H\bigr)^{\kappa(m)}$$

and

$$T_0(m, D\log H) = 2\bigl[10^3m^3D\log H\bigr]^{2(m-1)^2}.$$

The following inequalities (where T_0 stands for $T_0(m, D\log H)$)

$$U\bigl(m-1, 2D(\log H)T_0\bigr) \le \Bigl(4\bigl(10^3m^3D\log H\bigr)^{2(m-1)^2+1}\Bigr)^{\kappa(m-1)}$$

and

$$\bigl(2(m-1)^2+1\bigr)\kappa(m-1) \le (2m^2-m)\kappa(m-1) \le \kappa(m) - m\kappa(m-1)$$

imply

$$U\bigl(m-1, 2D(\log H)T_0\bigr) + \log T_0 \le U(m, D\log H);$$

this enables us to check the hypothesis of lemma 7.4 for $m \ge 2$. Hence, for the proof of Theorem 7.1, we may assume $b_1\beta_1 + \cdots + b_m\beta_m \ne 0$ for all $0 \ne (b_1, \dots, b_m) \in \mathbb{Z}^m(T_0)$. Incidentally, we shall prove a stronger result than Theorem 7.1 in this special case, namely with $\kappa(m) = 2^m(m!)^2$ replaced by $2m^3$.

Here is how this independence condition on the coefficients β_i will take place in the proof.

Lemma 7.5. – *Let K be a field of characteristic zero, S_1 be a positive integer and $\mathcal{V}$ be a subspace of K^m of codimension $r \geq 1$, such that*

$$\mathrm{Card}\Big(\big(\mathbb{Z}^m(S_1)+\mathcal{V}\big)/\mathcal{V}\Big) < (2S_1-1)^{r+1}.$$

Then
1) there exists a basis $(v_1,\dots,v_{m-r})$ of $\mathcal{V}$ with $v_j \in \mathbb{Z}^m(2S_1-1)$ for $1 \leq j \leq m-r$.
2) the vector space $\mathcal{V}$ is intersection of r hyperplanes of equations

$$b_{i1}z_1 + \cdots + b_{im}z_m = 0, \qquad (1 \leq i \leq r),$$

where, for $1 \leq i \leq r$, $b_i = (b_{i1},\dots,b_{im})$ is in $\mathbb{Z}^m(2S_1-1)$.

Proof. This is an effective version of the implication $(i) \Rightarrow (iii)'$ in lemma 5.9. The proof of the first assertion is the same : we use Dirichlet box principle together with the assumption on $\mathrm{Card}\Big(\big(\mathbb{Z}^m(S_1)+\mathcal{V}\big)/\mathcal{V}\Big)$ (see also exercise 3a). Notice that this assumption also implies $V \neq 0$, thus $m > r$.

In an earlier version of this lemma, a weaker form of the second assertion was proved: *the vector space $\mathcal{V}$ is contained in a hyperplane of equation $b_1z_1 + \cdots + b_mz_m = 0$, where $b = (b_1,\dots,b_m) \neq 0$ is in $\mathbb{Z}^m(S_2)$, with $S_2 = (m-1)!2^{m-1}(S_1-1)^{m-1}+1$* (see exercise 2); this yielded a larger value for $\kappa(m)$ in Theorem 7.1, namely $\kappa(m) = 2^m(m!)^3$. The refinement which follows is due to D. Roy ; I reproduce his argument here.
a) Assume first $r = 1$. In this case $\mathcal{V}$ is the kernel of a linear form $\varphi : K^m \longrightarrow K$, given by

$$\varphi(x_1,\dots,x_m) = b_1x_1 + \cdots + b_mx_m,$$

where $b_1,\dots,b_m$ are relatively prime rational integers. After permutation of the coordinates and replacement of φ by $-\varphi$ if necessary, we may assume $b_1 = \max\{|b_1|,\dots,|b_m|\}$. From the hypothesis $\mathrm{Card}\varphi\big(\mathbb{Z}^m(S_1)\big) < (2S_1-1)^2$, we shall deduce $b_1 < 2S_1-1$. For this purpose we define

$$d_i = \gcd(b_1,\dots,b_i), \qquad (1 \leq i \leq m),$$

and we consider the set

$$E = \Big\{(x_1,\dots,x_m) \in \mathbb{Z}^m\,;\, -S_1 < x_i \leq -S_1 + \frac{d_{i-1}}{d_i},\ 2 \leq i \leq m\Big\}.$$

Notice first that the restriction of φ to E is injective: indeed, if two distinct elements of E give the same image by φ, their difference $(y_1,\dots,y_m)$ belongs to $\ker\varphi$ and satisfies

$$|y_i| < d_{i-1}/d_i, \qquad (2 \leq i \leq m);$$

let $i \geq 2$ be the largest integer such that $y_i \neq 0$:

$$b_iy_i = -b_1y_1 - \cdots - b_{i-1}y_{i-1};$$

hence d_{i-1} divides b_iy_i; since $\gcd(b_i,d_{i-1}) = d_i$, the quotient d_{i-1}/d_i divides $|y_i|$, which contradicts the inequality $|y_i| < d_{i-1}/d_i$. Therefore φ is injective on $E \cap \mathbb{Z}^m(S_1)$; this implies

$$(2S_1-1)\prod_{i=2}^{m}\min\big\{2S_1-1, d_{i-1}/d_i\big\} < (2S_1-1)^2.$$

From this estimate follows $d_{i-1}/d_i < 2S_1-1$ for $2 \leq i \leq m$, and then

$$2S_1-1 > \prod_{i=2}^{m} d_{i-1}/d_i = d_1/d_m = b_1.$$

b) Assume now $r \geq 1$. Choose r linear forms $L_1, \ldots, L_r$ such that $\mathcal{V}$ is the intersection of their kernels. After permutation of the coordinates if necessary, we may assume that the m linear forms $L_1, \ldots, L_m$ are still linearly independent, where $L_{r+i}(z) = z_i$ for $1 \leq i \leq m-r$. This means that the kernel of the projection on the first $m-r$ coordinates is injective on $\mathcal{V}$; therefore, for $m-r < i \leq m$, the projection

$$\begin{array}{rccc} \pi_i : & K^m & \longrightarrow & K^{m-r+1} \\ & (x_1, \ldots, x_m) & \longmapsto & (x_1, \ldots, x_{m-r}, x_i) \end{array}$$

is injective on $\mathcal{V}$. Fix i with $m-r < i \leq m$. Now $\pi_i(\mathcal{V})$ is a hyperplane in K^{m-r+1} and π_i maps $\mathbb{Z}^m(S_1)$ onto $\mathbb{Z}^{m-r+1}(S_1)$; further, since $\mathcal{V} \cap \ker \pi_i = 0$, for each $x \in \mathbb{Z}^m(S_1)$, the classes modulo $\mathcal{V}$ of the $(2S_1-1)^{r-1}$ elements $x+y$, $(y \in \mathbb{Z}^m(S_1) \cap \ker \pi_i)$ are pairwise distinct; therefore (see lemma 10.3)

$$\mathrm{Card}\Big(\big(\mathbb{Z}^m(S_1) + \mathcal{V}\big)/\mathcal{V}\Big) \geq (2S_1-1)^{r-1}\mathrm{Card}\Big(\big(\mathbb{Z}^{m-r+1}(S_1) + \pi_i(\mathcal{V})\big)/\pi_i(\mathcal{V})\Big).$$

From the assumption $\mathrm{Card}\Big(\big(\mathbb{Z}^m(S_1) + \mathcal{V}\big)/\mathcal{V}\Big) < (2S_1-1)^{r+1}$ we deduce

$$\mathrm{Card}\Big(\big(\mathbb{Z}^{m-r+1}(S_1) + \pi_i(\mathcal{V})\big)/\pi_i(\mathcal{V})\Big) < (2S_1-1)^2;$$

from a) it follows that $\pi_i(\mathcal{V})$ is the kernel of a linear form $K^{m-r+1} \longrightarrow K$ with integer coefficients of absolute value $< 2S_1 - 1$; we compose this form with π_i and get a linear form on K^m whose kernel contains $\mathcal{V}$ and whose coefficients satisfy the required property. □

We now use lemma 7.5 and refine the zero estimate (Proposition 5.1) as follows:

Lemma 7.6. — *Let $\alpha_1, \ldots, \alpha_{n+1}$ be non-zero elements of K which generate a multiplicative subgroup of K^* of rank $\geq n$. Let $\beta_1, \ldots, \beta_n$ be elements of K. Assume that there exist three positive rational integers L_0, L_1 and S satisfying*

$$S^{n+1} \geq (2n)^{n+1}(L_0L_1)^n, \qquad S \geq 2n(n+1) \quad \text{and} \quad S^n > L_1,$$

such that the rank of the matrix

$$\left((s_1 + s_{n+1}\beta_1)^{\lambda_1} \cdots (s_n + s_{n+1}\beta_n)^{\lambda_n}\big(\alpha_1^{s_1} \cdots \alpha_{n+1}^{s_{n+1}}\big)^{\lambda_{n+1}}\right)_{\underline{\lambda},\underline{s}},$$

is strictly less than $\binom{L_0+n}{n}(L_1+1)$. As before, in the above matrix, the index of rows is $\underline{\lambda} = (\lambda_1, \ldots, \lambda_{n+1}) \in \mathbb{N}^{n+1}$ with $\lambda_1 + \cdots + \lambda_n \leq L_0$ and $0 \leq \lambda_{n+1} \leq L_1$, while the index of columns is $\underline{s} \in \mathbb{Z}^{n+1}(S)$. Then there exists a linear dependence relation

$$b_1\beta_1 + \cdots + b_n\beta_n = b_{n+1}$$

with $(b_1, \ldots, b_{n+1}) \in \mathbb{Z}^{n+1}$ and

$$0 < \max_{1 \leq i \leq n+1} |b_i| < \frac{S}{n}.$$

Proof. From the assumption $S \geq 2n(n+1)$ we deduce

$$\left(\frac{S}{n}\right)^{n+1} < 2\left(\frac{S}{n} - 1\right)^{n+1},$$

because

$$\left(1 + \frac{1}{2n+1}\right)^{n+1} < 2 \qquad \text{for} \qquad n \geq 1.$$

We repeat the proof of Proposition 5.1: we set $S'' = \lfloor S/2 \rfloor$, $S' = S - S'' + 1$. Therefore we have

$$\begin{cases} S' = S'' = (S+1)/2 & \text{if } S \text{ is odd,} \\ S' = (S/2) + 1,\ S'' = S/2 & \text{if } S \text{ is even.} \end{cases}$$

The assumption $S^n > L_1$ implies $(2S'-1)^n > L_1$ and enables us to use lemma 5.2. We deduce from the inequalities $S'' \geq S/2$ and $\big((S/n)-1\big)^{n+1} > (2L_0L_1)^n$ that the hypotheses of lemma 5.5 are satisfied with $D = 2L_0L_1$ and S replaced by S''. We now repeat the proof of lemma 5.5: we define $S_1 = \lfloor S''/n \rfloor$; from Proposition 5.8 and lemma 5.9 we deduce that there exists a vector subspace $\mathcal{V}$ of K^{n+1} containing $(\beta_1, \ldots, \beta_n, -1)$ such that

$$\mathrm{Card}\Big(\big(\mathbb{Z}^{n+1}(S_1) + \mathcal{V}\big)/\mathcal{V}\Big) < (2S_1 - 1)^{r+1}$$

where $r \geq 1$ is the codimension of $\mathcal{V}$ in K^{n+1}. Notice that $S_1 = \lfloor S/2n \rfloor < (S/2n) + 1$, hence $2S_1 - 2 \leq (S-1)/n$. Finally we use lemma 7.5: the vector space $\mathcal{V}$ is contained in a hyperplane $b_1z_1 + \cdots + b_{n+1}z_{n+1} = 0$ with $|b_i| \leq 2S_1 - 2$, and the point $(\beta_1, \ldots, \beta_n, -1)$ belongs to $\mathcal{V}$. □

1The transcendence proof We prove the following result:

Proposition 7.7. — *Let $\ell_1, \ldots, \ell_{n+1}$ be logarithms of algebraic numbers, $\alpha_i = \exp(\ell_i)$, $(1 \leq i \leq n+1)$ and $\beta_1, \ldots, \beta_n$ be algebraic numbers with $\max\{|\beta_1|, \ldots, |\beta_n|\} \leq 1$. Let D be the degree of the number field $\mathbb{Q}(\alpha_1, \ldots, \alpha_{n+1}, \beta_1, \ldots, \beta_n)$ over $\mathbb{Q}$ and let A, B and E be real numbers, which are $\geq e$, and satisfy*

$$\max_{1 \leq i \leq n+1} \mathrm{h}(\alpha_i) \leq \log A, \qquad E \max_{1 \leq i \leq n+1} |\ell_i| \leq D \log A$$

and

$$\mathrm{h}(1 : \beta_1 : \cdots : \beta_n) \leq \log B.$$

Assume that there exist three positive rational integers S, L_0, L_1, all ≥ 2, satisfying the following condition, where $L := \binom{L_0+n}{n}(L_1+1)$ and $\Theta_n(L)$ was defined in Chapter 4 §2:

$$\frac{1}{L}\Theta_n(L) \log E \geq D \log(2L) + DL_0 \log(2BS) + L_0 \log E + (3n+1)DL_1S \log A. \tag{7.8}$$

Assume further that the following matrix is of rank L:

$$\Big((s_1 + s_{n+1}\beta_1)^{\lambda_1} \cdots (s_n + s_{n+1}\beta_n)^{\lambda_n} \big(\alpha_1^{s_1} \cdots \alpha_{n+1}^{s_{n+1}}\big)^{\lambda_{n+1}}\Big)_{\underline{\lambda}, \underline{s}},$$

where the index of rows is $\underline{\lambda} = (\lambda_1, \ldots, \lambda_{n+1}) \in \mathbb{N}^{n+1}$ with $\lambda_1 + \cdots + \lambda_n \leq L_0$ and $0 \leq \lambda_{n+1} \leq L_1$, while the index of columns is $\underline{s} \in \mathbb{Z}^{n+1}(S)$. Then the number

$$\Lambda = \beta_1\ell_1 + \cdots + \beta_n\ell_n - \ell_{n+1}$$

does not vanish, and if we write $|\Lambda| = e^{-U}$, we have

$$\frac{U}{L} \leq D \log L + DL_0 \log(2BS) + 2(n+1)DL_1S \log A. \tag{7.9}$$

The assumption on the rank of the matrix implies in particular $L \leq (2S-1)^{n+1}$.

Proof. We introduce two determinants, one with algebraic entries which is called Δ_r, while the second Δ_n is an interpolation determinant. The determinant Δ_r will be different from zero because of our assumption on the rank of the matrix; from Liouville's estimate we get a lower bound for $|\Delta_r|$. Further $|\Delta_n|$ is small, because it is an interpolation determinant. Furthermore the difference $|\Delta_r - \Delta_n|$ is bounded from above by a small multiple of $|\Lambda|$; this gives the desired lower bound for $|\Lambda|$.

Step one: Lower bound for $|\Delta_r|$

Our hypothesis on the rank of the matrix shows that there exist L elements $\underline{s}^{(1)}, \ldots, \underline{s}^{(L)}$ in $\mathbb{Z}^{n+1}(S)$, such that the determinant

$$\Delta_r = \det\Big((s_1^{(\mu)} + s_{n+1}^{(\mu)}\beta_1)^{\lambda_1} \cdots (s_n^{(\mu)} + s_{n+1}^{(\mu)}\beta_n)^{\lambda_n} \big(\alpha_1^{s_1^{(\mu)}} \cdots \alpha_{n+1}^{s_{n+1}^{(\mu)}}\big)^{\lambda_{n+1}}\Big)_{\underline{\lambda}, \mu}$$

does not vanish. From Proposition 3.15 we deduce

$$\frac{1}{L} \log |\Delta_r| \geq -U_1$$

with

$$U_1 = (D-1)\big(L_0 \log(2S) + \log L\big) + DL_0 \log B + (n+1)DL_1S \log A.$$

Step two: Upper bound for $|\Delta_n|$

Let us define

$$\Delta_n = \det\left(\prod_{i=1}^{n}(s_i^{(\mu)} + s_{n+1}^{(\mu)}\beta_i)^{\lambda_i}\alpha_i^{(s_i^{(\mu)}+s_{n+1}^{(\mu)}\beta_i)\lambda_{n+1}}\right)_{\underline{\lambda},\mu}.$$

We apply the results of Chapter 4 to the functions

$$f_{\underline{\lambda}}(z_1,\dots,z_n) = z_1^{\lambda_1}\cdots z_n^{\lambda_n}e^{(\ell_1 z_1+\cdots+\ell_n z_n)\lambda_{n+1}}$$

and to the points

$$\zeta_\mu = \left(s_1^{(\mu)} + s_{n+1}^{(\mu)}\beta_1,\dots,s_n^{(\mu)} + s_{n+1}^{(\mu)}\beta_n\right) \in \mathbb{C}^n, \qquad (1 \le \mu \le L)$$

with $r = 2S$ and $R = Er$ (we use our assumption $|\beta_j| \le 1$). From our hypothesis $E|\ell_i| \le D\log A$ we deduce

$$\begin{aligned}\log|f_{\underline{\lambda}}|_R &\le L_0\log R + L_1 R\sum_{i=1}^{n}|\ell_i| \\ &\le L_0\log(2ES) + 2nDL_1S\log A.\end{aligned}$$

Therefore lemmas 4.1 and 4.2 give

$$\frac{1}{L}\log|\Delta_n| \le -U_2$$

with

$$U_2 = \frac{1}{L}\Theta_n(L)\log E - \log L - L_0\log(2ES) - 2nDL_1S\log A.$$

Step three: Upper bound for $|\Delta_r - \Delta_n|$

We write Δ_r as a polynomial in $\alpha_1,\dots,\alpha_{n+1}$ and $\alpha_1^{-1},\dots,\alpha_{n+1}^{-1}$ with coefficients in $\mathbb{Q}(\beta_1,\dots,\beta_n)$:

$$\Delta_r = \sum_t q_t\alpha_1^{t_1}\cdots\alpha_{n+1}^{t_{n+1}},$$

where $t = (t_1,\dots,t_{n+1})$ with $|t_i| \le LL_1S$. Thanks to our hypothesis $|\beta_i| \le 1$ we have

$$\sum_t |q_t| \le L!(2S)^{LL_0}.$$

The number Δ_n is obtained by replacing α_{n+1} by $\alpha_1^{\beta_1}\cdots\alpha_n^{\beta_n}$. We set $x = \alpha_{n+1}$ and $y = \alpha_1^{\beta_1}\cdots\alpha_n^{\beta_n}$:

$$\Delta_r - \Delta_n = \sum_t q_t e^{\ell_1 t_1+\cdots\ell_n t_n}\left(x^{t_{n+1}} - y^{t_{n+1}}\right).$$

Since $|\ell_i| \le (D/E)\log A$, we have

$$\log|\Delta_r - \Delta_n| \le L\log L + LL_0\log(2S) + \frac{nD}{E}LL_1S\log A + \log\max_{|t|\le LL_1S}|x^t - y^t|.$$

For any integer t in the range $-LL_1S \le t \le LL_1S$, we have (compare with exercise 1 of Chapter 1; notice also that there is no loss of generality to assume $|\Lambda|LL_1S \le 1$)

$$\begin{aligned}|x^t - y^t| \le |\alpha_{n+1}^t|\ |1 - e^{t\Lambda}| &\le e^{|t\ell_{n+1}|}|t\Lambda|e^{|t\Lambda|} \\ &\le eLL_1S|\Lambda|e^{LL_1S|\ell_{n+1}|}.\end{aligned}$$

Therefore

$$\log|x^t - y^t| \le \frac{D}{E}LL_1S\log A + \log(LL_1S) + 1 - U.$$

We shall bound

$$1 + \log(2LL_1S) + \frac{D}{E}(n+1)LL_1S\log A$$

by $(n+1)DLL_1S\log A$. This is allowed by the inequalities $A \ge e$, $E \ge e$, $D \ge 1$, $n \ge 1$, $S \ge 2$, $L_1 \ge 2$ and $L \ge 9$, and the fact that the number $x = 2eLL_1S$ is greater than $72e$, hence satisfies $\log x \le (1/e^2)(e-1)x$. We deduce

$$|\Delta_r - \Delta_n| \le e^{-LU_3}$$

with

$$U_3 = \frac{U}{L} - L_0\log(2S) - (n+1)DL_1S\log A - \log L + \frac{\log 2}{L}.$$

Step four: Conclusion

We write the triangular inequality:

$$|\Delta_r| \le |\Delta_n| + |\Delta_r - \Delta_n|$$

from which we deduce, using steps 1, 2 and 3,

$$e^{-LU_1} \le e^{-LU_2} + e^{-LU_3}.$$

Our assumption (7.8) implies $U_1 + (1/L)\log 2 \le U_2$, from which we deduce $U_3 \le U_1 + (1/L)\log 2$. This concludes the proof of Proposition 7.7. □

1Proof of Theorem 7.1 We first deduce from Proposition 7.7 the following result:

Proposition 7.10. – *With the same assumptions as in Theorem 7.1, assume that there is no linear relation* $b_1\beta_1 + \cdots + b_m\beta_m = 0$ *between* $\beta_1, \ldots, \beta_m$ *with rational integers* b_i *satisfying*

$$0 < \max_{1\le i\le m} |b_i| < 2T^{2(m-1)^2} \qquad \text{where} \qquad T = \big[10^3 m^3 D \log H\big].$$

Assume also that $\ell_1, \ldots, \ell_m$ *are linearly independent over* $\mathbb{Q}$*. Then the conclusion of Theorem 7.1 holds with* $\kappa(m)$ *replaced by* $2m^3$*, namely*

$$|\Lambda| \ge \exp\big\{-(10^3 m^3 D \log H)^{2m^3}\big\}.$$

Proof.

a) *We divide by the largest* $|\beta_i|$.

We shall assume $\beta_m = -1$ and $|\beta_i| \le 1$ for $1 \le i \le m-1$, and in this case we shall prove the lower bound

$$|\Lambda| \ge \exp\big\{-(10^3 m^3 D \log H)^{2m^3-1}\big\}.$$

The general case will follow from Liouville's inequality (3.13):

$$\max_{1\le j\le m} |\beta_j| \ge H^{-D}$$

thanks to the trivial upper bound

$$(10^3 m^3 D \log H)^{2m^3-1} + D\log H \le (10^3 m^3 D \log H)^{2m^3}.$$

We shall use Proposition 7.7 with $n = m-1$, $E = e$, $A = H$, $B = H^m$ (cf. exercise 3 of Chapter 3). We shall check later $L > 2^n e^{n+1}$; lemma 4.3 shows that one has $\Theta_n(L) \ge nL^{1+(1/n)}/6e$.

b) *Preliminary comments.*

Let us explain how we shall choose our other parameters; we shall make the real choice only later.

We want to choose L_0, L_1 and S positive integers so that the right hand side of (7.9) is as small as possible, while condition (7.8) is satisfied, and also the matrix is of maximal rank. Thanks to lemma 7.6 and to our assumption on the linear independence of the β's, this last condition will be satisfied as soon as

$$(2n)^{n+1}(L_0L_1)^n \le S^{n+1} \tag{7.11}$$

(the conditions $S \ge 2n(n+1)$ and $S^n > L_1$ will be checked later). Let us come back to condition (7.8); we shall check below that

$$D\log(2L) + DL_0\log\big(2H^{n+1}S\big) + L_0 < 25n^3 DL_0 \log H \tag{7.12}$$

This reduces (7.8) to the condition

$$L^{1/n} \ge 150en^2 DL_0 \log H + \frac{6e}{n}(3n+1)DL_1 S \log H.$$

Since we do not try to get the best possible constant, we shall impose

$$L^{1/n} \geq 10^3 n^2 D L_0 \log H \qquad \text{and} \qquad L^{1/n} \geq 500 n D L_1 S \log H.$$

The simplest choice is

$$L_0 = L^{1/n}\big(10^3 n^2 D \log H\big)^{-1}$$

and

$$L_1 = L^{1/n}\big(500 n D S \log H\big)^{-1}.$$

We now replace L by $L_0^n L_1/n^n$, which is a good approximation; this gives

$$L^{1/n} = \frac{S}{2n^2}\big(10^3 n^3 D \log H\big)^{n+1}.$$

Now we have

$$L_0 = \frac{S}{2n}\big(10^3 n^3 D \log H\big)^{n}$$

and

$$L_1 = \big(10^3 n^3 D \log H\big)^{n}.$$

From (7.11), we deduce that a good choice for S is

$$S = 2n\big(10^3 n^3 D \log H\big)^{2n^2},$$

which implies

$$L^{1/n} = \frac{1}{n}\big(10^3 n^3 D \log H\big)^{2n^2+n+1}.$$

This is the way these parameters are chosen, the only substantial difference being that in Proposition 7.7 these parameters are supposed to be integers, while the preceding computations provide real numbers.

c) *Choice of the parameters.*

Here is now the real choice we make. Recall that $n = m - 1$, hence

$$T = \big[10^3 (n+1)^3 D \log H\big].$$

We put

$$S = 2nT^{2n^2}, \qquad L_0 = T^{2n^2+n} \qquad \text{and} \qquad L_1 = T^n.$$

The following estimates for $L := \binom{L_0+n}{n}(L_1+1)$ will be useful:

$$n^{-n} T^{2n^3+n^2+n} < L < 2T^{2n^3+n^2+n}. \tag{7.13}$$

The inequality on the left is a consequence of the bound $n! \leq n^n$, while the inequality on the right hand side comes from the estimate

$$\frac{1}{n!}\left(1+\frac{n}{L_0}\right)\left(1+\frac{1}{L_1}\right) < 2.$$

In particular the inequality $L > 2^n e^{n+1}$ is obvious.

d) *Verification of (7.11).*

We have $L_0 L_1 = T^{2n(n+1)}$ and $S^{n+1} = (2n)^{n+1} T^{2n^2(n+1)}$. The other conditions $S \geq 2n(n+1)$ and $S^n > L_1$ of lemma 7.6 are trivial. Our assumption that $\beta_1, \ldots, \beta_n, -1$ do not satisfy a linear dependence relation with coefficients $< 2T^{2n^2}$ shows that the conclusion of lemma 7.6 is not true. Hence the assumption on the rank of the matrix in Proposition 7.7 is satisfied.

e) *Verification of (7.8).*

We use the following estimates:

$$\log(2L) < L_0 \log(3/2), \qquad \log(3S) \le \log(6n) + 2n^2 \log T < (25n^3 - n - 2)\log H$$

(this is where the assumption $H \ge D$ is used); therefore

$$D\log(2L) + DL_0 \log\bigl(2H^{n+1}S\bigr) + L_0 < (n+2)DL_0 \log H + DL_0 \log(3S)$$
$$< 25n^3 DL_0 \log H < \frac{1}{12e} T^{2n^2+n+1}$$

because $T > 10^3 n^3 D \log H$; this proves (7.12). We also have

$$(3n+1)DL_1 S \log H \le 4nDL_1 S \log H < \frac{8}{10^3 n} T^{2n^2+n+1} < \frac{1}{12e} T^{2n^2+n+1}.$$

From (7.13) we deduce

$$\frac{1}{L}\Theta_n(L)\log E \ge \frac{1}{6e} T^{2n^2+n+1};$$

hence (7.8) follows.

f) *Conclusion.*

We can now bound U from (7.9). Using the estimates in e) above, we obviously have

$$D\log L + DL_0 \log(2BS) + 2(n+1)DL_1 S \log A < \frac{1}{6e} T^{2n^2+n+1}.$$

Hence (7.9) and (7.13) yield

$$U < \frac{L}{6e} T^{2n^2+n+1} < T^{(n+1)^3+n^3-n}.$$

We bound $(n+1)^3 + n^3 - n$ by $2(n+1)^3 - 1$ (we are a bit sloppy at this point, but it does not really matter).

This completes the proof of Proposition 7.10. □

Finally, we deduce Theorem 7.1 from Proposition 7.10 as explained in sections 2 and 3: assume first that $\ell_1, \dots, \ell_m$ are linearly independent over $\mathbb{Q}$; the conclusion is true if $\beta_1, \dots, \beta_m$ satisfy the linear independence condition stated in Proposition 7.10. Otherwise, we use lemma 7.4 and get the desired conclusion thanks to Proposition 7.10 (in property (P_m), we restrict our attention to linear independent logarithms). Finally, if $\ell_1, \dots, \ell_m$ are not $\mathbb{Q}$-linearly independent, we deduce the conclusion from lemma 7.3.

1Open problem Is theorem 7.1 true without the condition $e|\ell_i| \le D \log H$?

1Exercises **1.** Prove the following refinement of lemma 7.2: let $\ell_1, \dots, \ell_m$ be $\mathbb{Q}$-linearly dependent logarithms of algebraic numbers; define $\alpha_j = e^{\ell_j}$, $(1 \le j \le m)$. For $1 \le j \le m$, let $\log H_j \ge 1$ be an upper bound for $\max\{\mathrm{h}(\alpha_j), |\ell_j|/D\}$. Further D be the degree of the number field $K = \mathbb{Q}(\alpha_1, \dots, \alpha_m)$ over $\mathbb{Q}$. Then there exist rational integers $t_1, \dots, t_m$, not all of which are zero, such that

$$t_1\ell_1 + \cdots + t_m\ell_m = 0$$

and

$$|t_k| \le \bigl(4e(m-1)D^3\bigr)^{m-1} \log H_1 \cdots \log H_m / \log H_k$$

for $1 \le k \le m$.

`Hint.` *First use exercise* 9 *of Chapter* 3*; next see* [W] *lemmas* 2.6 *and* 4.1.

2. Let S be a positive integer and $v_1, \dots, v_{m-r}$ be $m-r$ linearly independent elements in $\mathbb{Z}^m(S)$. Show that the vector space $\mathcal{V}$ they span in $\mathbb{C}^m$ is contained in a hyperplane of equation $b_1 z_1 + \cdots + b_m z_m = 0$ with $0 \ne (b_1, \dots, b_m) \in \mathbb{Z}^m(S')$ and

$$S' = (m-r)!(S-1)^{m-r} + 1.$$

`Hint.` *Since $m-r<m$, the $m-r$ elements of this basis satisfy a linear dependence condition with rational integral coefficients: this amounts to write that a $m\times(m-r)$ matrix has rank $\le m-1$; expanding determinants with entries of absolute values $\le S-1$, yields a linear relation with coefficients $\le (m-r)!(S-1)^{m-r}$.*

3. (`With D. Roy and W.M. Schmidt`). Let $S\ge 2$ be a positive integer and $\mathcal{V}$ a subspace of $\mathbb{R}^m$ of codimension $r\ge 1$ satisfying the following condition (the same as in lemma 7.5)

$$\mathrm{Card}\Big(\big(\mathbb{Z}^m(S)+\mathcal{V}\big)/\mathcal{V}\Big)<(2S-1)^{r+1}.$$

a) Show that the intersection $\mathcal{V}\cap\mathbb{Z}^m(2S-1)$ contains more than $(2S-1)^{m-r-1}$ points and contains a basis of $\mathcal{V}$; hence $\Lambda=\mathcal{V}\cap\mathbb{Z}^m$ is a lattice in $\mathcal{V}$ of dimension $m-r$.
`Hint.` *See Exercise* 2 *in Chapter* 10.
b) The *determinant* $\det\Lambda$ of the lattice Λ in $\mathcal{V}$ is the volume of $\mathcal{V}/\Lambda$, i.e. the volume of a fundamental domain of Λ in $\mathcal{V}$ (see [S2]). Check

$$\det\Lambda<m^{3(m-r)/2}(2S-1).$$

`Hint.` *Choose a basis of $\mathcal{V}$ belonging to $\mathbb{Z}^m(2S-1)$, and denote by P the corresponding parallelepiped. Check that P contains a fundamental domain of $\mathcal{V}/\Lambda$.*

Define $K=\mathcal{V}\cap\mathbb{R}^m(2S-1)$. Check

$$\mathrm{Card}(K\cap\Lambda)\det\Lambda\le\mathrm{vol}(K+P),$$

where $\mathrm{vol}(K+P)$ *is the volume of $K+P$ in $\mathcal{V}$ (for the metric induced by the metric of $\mathbb{R}^m$). Check also* $\mathrm{vol}(K+P)\le m^{m-r}(2S-2)^{m-r}$.
c) Denote by $\|\cdot\|_2$ the Euclidean norm in $\mathbb{R}^m$. Deduce from Minkowski's theorem that there is a basis $v_1,\dots,v_{m-r}$ of $\mathcal{V}$, where $v_i\in\Lambda$ satisfy

$$\|v_1\|_2\cdots\|v_{m-r}\|_2\le m^{2(m-r)}(2S-1).$$

d) Let $\mathcal{V}^\perp$ be the orthogonal complement of $\mathcal{V}$ in $\mathbb{R}^m$:

$$\mathcal{V}^\perp=\{x\in\mathbb{R}^m\,;\,\langle x,y\rangle=0\text{ for all }y\in\mathcal{V}\},$$

where $\langle\ ,\ \rangle$ denotes the usual scalar product in $\mathbb{R}^m$. Then $\Lambda^\perp=\mathbb{Z}^m\cap\mathcal{V}^\perp$ is a lattice in $\mathcal{V}^\perp$ of dimension r, with $\det\Lambda^\perp=\det\Lambda$ (see [S2] Chap. 1). Deduce that $\mathcal{V}$ is intersection of r hyperplanes in $\mathbb{R}^m$ of equations

$$\langle b_i,z\rangle=0,\qquad(1\le i\le r),$$

where $b_i=(b_{i1},\dots,b_{im})$ are in $\mathbb{Z}^m$ and satisfy

$$\|b_1\|_2\cdots\|b_r\|_2\le m^{2(m-r)}(2S-1).$$

4. Refine Theorem 7.10 by replacing the single parameter H by two parameters A and B satisfying

$$\mathrm{h}(\beta_j)\le\log B,\qquad(1\le j\le m),$$
$$\max\{\mathrm{h}(\alpha_j),|\ell_j|/D\}\le\log A,\qquad(1\le j\le m),$$
$$\log B\ge\log(D\log A);$$

then in the conclusion the factor $(D\log H)^{2m^3}$ can be replaced by

$$\big(D^m(\log B)^{2m-1}\log A\big)^{m^2}.$$

1References

[L] S. Lang. – *Number theory* 3; Encycl. of Math. Sciences, Vol. 60, Springer Verlag 1991.
[M] D.W. Masser. – Linear relations on algebraic groups; in *New Advances in transcendence theory*, ed. A. Baker, Cambridge Univ. Press (1988), 248–262.
[S1] W.M. Schmidt. – *Diophantine approximation*; Springer Lecture Notes in Math., **785** (1980).
[S2] W.M. Schmidt. – *Diophantine approximations and Diophantine equations*; Springer Lecture Notes in Math., **1467**, 1991.
[W] M. Waldschmidt. – A lower bound for linear forms in logarithms; Acta Arith. **37** (1980), 257–283.

8.– ZERO ESTIMATE (CONTINUED) by Damien ROY

The present chapter is devoted to a refinement of Proposition 5.1.

Let K be a field of zero characteristic and let d_0, d_1 be two non-negative integers with $d = d_0 + d_1 > 0$. We denote by G the group $K^{d_0} \times (K^*)^{d_1}$; the group law on G will be written additively ; hence its neutral element is denoted by 0. When Σ is a finite subset of G and n a positive integer, we define

$$\Sigma[n] = \big\{\sigma_1 + \cdots + \sigma_n \,;\, (\sigma_1, \ldots, \sigma_n) \in \Sigma^n\big\}.$$

For each subgroup Φ of $\mathbb{Z}^{d_1}$, we denote by T_Φ the following subgroup of $(K^*)^{d_1}$:

$$T_\Phi = \big\{(y_1, \ldots, y_{d_1}) \in (K^*)^{d_1} \,;\, y_1^{\varphi_1} \cdots y_{d_1}^{\varphi_{d_1}} = 1 \text{ for all } \varphi = (\varphi_1, \ldots, \varphi_{d_1}) \in \Phi\big\}.$$

Our aim is to show:

Proposition 8.1. – *Let Σ be a finite subset of G containing 0. Assume that there exists a non-zero polynomial in $K[X_1, \ldots, X_{d_0}, Y_1, \ldots, Y_{d_1}]$, of total degree $\leq D_0$ in $X_1, \ldots, X_{d_0}$ and of total degree $\leq D_1$ in $Y_1, \ldots, Y_{d_1}$, which vanishes on $\Sigma[d]$. Then there exist a vector subspace V of K^{d_0} of dimension $\delta_0 \geq 0$ and a subgroup Φ of $\mathbb{Z}^{d_1}$ of rank $d_1 - \delta_1$ with $\delta = \delta_0 + \delta_1 < d$ such that*

$$\frac{\delta!}{\delta_0!\delta_1!}\mathrm{Card}\Big(\big(\Sigma + (V \times T_\Phi)\big)/(V \times T_\Phi)\Big) \leq \frac{d!}{d_0!d_1!} D_0^{d_0-\delta_0} D_1^{d_1-\delta_1}.$$

In fact, we will establish this result in the case where K is algebraically closed. The general case will be left to the reader (see exercise 1).

1 Some algebraic geometry In this section and in the following ones, K denotes an algebraically closed field of characteristic zero. In the applications, one can take K equal either to $\mathbb{C}$ or to the algebraic closure of $\mathbb{Q}$ in $\mathbb{C}$. We also fix a positive integer d.

(a) Algebraic subsets of K^d

An *algebraic subset of K^d* is a subset of K^d which is the set of common zeroes of a family of polynomials in $K[X_1, \ldots, X_d]$.

From this definition, it follows that the intersection of any family of algebraic subsets of K^d is again an algebraic subset of K^d. In particular each subset E of K^d is contained in a smallest algebraic subset of K^d, which will be denoted by $\overline{E}$: this is the set of common zeroes of the polynomials which vanish on E. A finite union of algebraic subsets of K^d is also an algebraic subset of K^d. In particular, if E is a finite union of sets $E_1, \ldots, E_r$, then $\overline{E}$ is the union of $\overline{E}_1, \ldots, \overline{E}_r$.

An algebraic subset of K^d is called *irreducible* if it cannot be written as the union of two algebraic subsets of K^d properly contained in it. An irreducible algebraic subset of K^d is also called an *algebraic subvariety* of K^d. Thus, if an algebraic subvariety of K^d is contained in a finite union of algebraic subsets of K^d, then it is contained in one of them. The empty set, the space K^d and the points of K^d are examples of algebraic subvarieties of K^d. One can show that each algebraic subset V of K^d is a finite union of algebraic subvarieties $V_1, \ldots, V_s$ of K^d:

$$V = V_1 \cup \cdots \cup V_s.$$

In this decomposition of V, one can require the condition $V_i \not\subset V_j$ for $i \neq j$. In this case the subvarieties V_i are uniquely determined: they are the maximal irreducible algebraic subsets of K^d contained in V, and they are called the *irreducible components of V*.

To each non-empty algebraic subvariety of K^d is attached a *dimension* which is a non-negative integer $\leq d$. This dimension satisfies the following properties:

(i) for a point it is 0, for K^d it is d ;
(ii) if V_1, V_2 are two distinct algebraic subvarieties of K^d and if $V_1 \subset V_2$, then $\dim(V_1) < \dim(V_2)$.
The *dimension* of a non-empty algebraic subset of K^d is defined as the maximum of the dimensions of its irreducible components. We observe:

If V, V' are two algebraic subsets of K^d with $V' \subset V$, then we have $\dim(V') \leq \dim(V)$, *with equality if and only if* V *and* V' *have a common irreducible component of dimension* $\dim(V)$. This follows from the property (ii) and from the fact that each irreducible component of V' is contained in one of V. *In particular, an algebraic subset* V *of* K^d *of dimension* n *contains only finitely many subvarieties of* K^d *of dimension* n.

(b) Hilbert–Samuel polynomial

Let d_0, d_1 be two non-negative integers with sum d. We now write K^d as a product $K^{d_0} \times K^{d_1}$, and use the letters $Y_1, \ldots, Y_{d_1}$ to denote the variables $X_{d_0+1}, \ldots, X_d$. A polynomial $P(\underline{X}, \underline{Y}) \in K[X_1, \ldots, X_{d_0}, Y_1, \ldots, Y_{d_1}]$ is said to be *of bidegree* $\leq (D_0, D_1)$ if its total degree with respect to the variables $X_1, \ldots, X_{d_0}$ is $\leq D_0$ and its total degree in the variables $Y_1, \ldots, Y_{d_1}$ is $\leq D_1$. We denote by $K[\underline{X}, \underline{Y}]_{\leq (D_0, D_1)}$ the set of elements in $K[\underline{X}, \underline{Y}]$ which are of bidegree $\leq (D_0, D_1)$.

Let E be a non-empty subset of $K^{d_0} \times K^{d_1}$. We denote by K^E the set of mappings from E into K, and we consider the K-linear map

$$\mathrm{res}_E : K[\underline{X}, \underline{Y}] \longrightarrow K^E$$

which maps each polynomial $P \in K[\underline{X}, \underline{Y}]$ to the restriction to E of the polynomial map from K^d in K induced by P. For each $(D_0, D_1) \in \mathbb{N}^2$, we set

$$H(E; D_0, D_1) = \dim_K \Big(\mathrm{res}_E \big(K[\underline{X}, \underline{Y}]_{\leq (D_0, D_1)} \big) \Big).$$

Since the kernels of res_E and $\mathrm{res}_{\overline{E}}$ are the same, we have

$$H(E; D_0, D_1) = H(\overline{E}; D_0, D_1).$$

The main point is that *for all* $(D_0, D_1) \in \mathbb{N}^2$ *with* D_0 *and* D_1 *sufficiently large,* $H(E; D_0, D_1)$ *coincides with the value at the point* (D_0, D_1) *of a polynomial whose degree is the dimension of* $\overline{E}$*:*

$$H(E; D_0, D_1) = \sum_{i+j \leq n} a_{ij} D_0^i D_1^j \qquad \textit{with} \quad n = \dim(\overline{E}).$$

This polynomial which gives the value of $H(E; D_0, D_1)$ for sufficiently large D_0 and D_1 is called the *Hilbert–Samuel bi-homogeneous polynomial of* E. In fact, each decomposition of K^d into a product $K^{d_0} \times \cdots \times K^{d_s}$ with $s \geq 0$ gives rise, as above, to a multi-homogeneous Hilbert–Samuel polynomial of E. For $s = 0$, this is the usual Hilbert–Samuel polynomial of E.

Let us come back to our special case and denote by

$$\mathcal{H}(E; D_0, D_1) = n! \sum_{i+j=n} a_{ij} D_0^i D_1^j$$

the product by $n!$ of the homogeneous part of degree $n = \dim(\overline{E})$ of the polynomial which coincides with $H(E; D_0, D_1)$ for sufficiently large D_0 and D_1. It can be proven that the coefficients of $\mathcal{H}(E; D_0, D_1)$ are rational and non-negative. In the sequel we will need the important fact that if V is an algebraic subset of K^d of dimension n and if $V_1, \ldots, V_r$ are its irreducible components of dimension n, then

$$\mathcal{H}(V; D_0, D_1) = \sum_{i=1}^{r} \mathcal{H}(V_i; D_0, D_1).$$

Example. For $V = K^d$, we have

$$\begin{aligned} H(K^d; D_0, D_1) &= \dim_K \Big(K[\underline{X}, \underline{Y}]_{\leq (D_0, D_1)} \Big) \\ &= \binom{D_0 + d_0}{d_0} \binom{D_1 + d_1}{d_1} \\ &= \frac{1}{d_0!} \frac{1}{d_1!} D_0^{d_0} D_1^{d_1} + \cdots, \end{aligned}$$

hence

$$\mathcal{H}(K^d; D_0, D_1) = \frac{d!}{d_0! d_1!} D_0^{d_0} D_1^{d_1}.$$

If we choose $d_0 = d$ and $d_1 = 0$, the function $H(E; D, D_1)$ defined previously does not depend on D_1, and neither does $\mathcal{H}(E; D, D_1)$. In that case, we denote them respectively by $H(E; D)$ and $\mathcal{H}(E; D)$. For any $D \in \mathbb{N}$, $H(E; D)$ is simply the dimension over K of the space of mappings from E to K induced by polynomials of degree $\leq D$. We also have $H(E; D_0, D) = H(E; D)$ and $\mathcal{H}(E; D_0, D) = \mathcal{H}(E; D)$ independently of D_0 if $d_0 = 0$ and $d_1 = d$. We conclude this section with a proof of the following result.

Lemma 8.2. — *Assume $d_0, d_1 > 0$. Let E_0 and E_1 be respectively non-empty subsets of K^{d_0} and K^{d_1}, and let δ_0 and δ_1 be the respective dimensions of $\overline{E}_0$ and $\overline{E}_1$. Then, the dimension of $\overline{E_0 \times E_1}$ is $\delta_0 + \delta_1$ and we have*

$$\mathcal{H}(E_0 \times E_1; D_0, D_1) = \frac{(\delta_0 + \delta_1)!}{\delta_0! \delta_1!} \mathcal{H}(E_0; D_0) \mathcal{H}(E_1; D_1).$$

Proof. Let $E = E_0 \times E_1$. We first observe that we have

$$H(E; D_0, D_1) = H(E_0; D_0) H(E_1; D_1)$$

for all $(D_0, D_1) \in \mathbb{N}^2$. In fact, if S_0 is a maximal subset of $K[\underline{X}]_{\leq D_0}$ whose image under res_{E_0} is linearly independent in K^{E_0} and if S_1 is a maximal subset of $K[\underline{Y}]_{\leq D_1}$ whose image under res_{E_1} is linearly independent in K^{E_1}, then the set S consisting of all products $P(\underline{X})Q(\underline{Y})$ with $P(\underline{X}) \in S_0$ and $Q(\underline{Y}) \in S_1$ is a maximal subset of $K[\underline{X}, \underline{Y}]_{\leq (D_0, D_1)}$ whose image under res_E is linearly independent in K^E. Since the cardinality of S_0 and S_1 are respectively $H(E_0; D_0)$ and $H(E_1; D_1)$, this gives the above equality. Therefore, for large integers D_0, D_1, the value of $H(E; D_0, D_1)$ is given by the product of a polynomial in D_0 of degree δ_0 with a polynomial in D_1 of degree δ_1. This shows that the dimension of $\overline{E_0 \times E_1}$ is $\delta_0 + \delta_1$ and the equality of the lemma follows. □

1 Algebraic subgroups of G We denote by K^* the multiplicative group of non-zero elements in K, and by G the product $K^{d_0} \times (K^*)^{d_1}$ of d_0 copies of the additive group of K with d_1 copies of the multiplicative group K^*. A subset E of G is called an *algebraic subset of G* if E is the set of common zeroes in G of a family of polynomials in $K[\underline{X}, \underline{Y}]$, a condition which is equivalent to $E = \overline{E} \cap G$; the dimension of E is then defined as the dimension of $\overline{E}$ or equivalently as the degree of the polynomial $\mathcal{H}(E; D_0, D_1)$. Further, a subset H of G is called an *algebraic subgroup of G* if H is at the same time a subgroup of G and an algebraic subset of G. When $d_0 > 0$ (resp. when $d_1 > 0$), we have the corresponding notions of algebraic subsets and algebraic subgroups of K^{d_0} (resp. of $(K^*)^{d_1}$).

If $d_0 > 0$, each vector subspace V of K^{d_0} is an algebraic subgroup of K^{d_0}, since it is defined by linear equations. On the other hand, if $d_1 > 0$, then for each subgroup Φ of $\mathbb{Z}^{d_1}$, the set

$$T_\Phi = \left\{ (y_1, \ldots, y_{d_1}) \in (K^*)^{d_1} \,;\, y_1^{\varphi_1} \cdots y_{d_1}^{\varphi_{d_1}} = 1 \ \text{ for all } \ (\varphi_1, \ldots, \varphi_{d_1}) \in \Phi \right\}$$

is an algebraic subgroup of $(K^*)^{d_1}$, because, after multiplication of both sides of each equation $y_1^{\varphi_1} \cdots y_{d_1}^{\varphi_{d_1}} = 1$ by a product of powers of the y_i with sufficiently large positive exponents, we get a set of polynomial equations which define T_Φ. As a consequence, the products $V \times T_\Phi$ are algebraic subgroups of G, being understood that such a product is V if $d_1 = 0$, and that it is T_Φ if $d_0 = 0$. We will show that the converse holds and moreover that we have:

Proposition 8.3. — *The algebraic subgroups of G are the products $V \times T_\Phi$, where V is a vector subspace of K^{d_0} and Φ a subgroup of $\mathbb{Z}^{d_1}$. For such a product, we have*

$$\mathcal{H}(V \times T_\Phi; D_0, D_1) \geq \frac{\delta!}{\delta_0! \delta_1!} D_0^{\delta_0} D_1^{\delta_1},$$

where $\delta_0 = \dim_K(V)$, $\delta_1 = d_1 - \mathrm{rk}_{\mathbb{Z}}(\Phi)$ and $\delta = \delta_0 + \delta_1$.

The proof of this inequality will follow immediately from the next three lemmas. Before going into these lemmas, let us observe that, since no non-zero polynomial vanishes identically on G, we have $\overline{G} = K^d$. Therefore the dimension of G is d and, from the example given before Lemma 8.2, we get

$$\mathcal{H}(G; D_0, D_1) = \frac{d!}{d_0! d_1!} D_0^{d_0} D_1^{d_1}. \tag{8.4}$$

Lemma 8.5. — *Assume $d_0 > 0$ and $d_1 > 0$. Then, the algebraic subgroups of G are the products $H_0 \times H_1$ where H_0 is an algebraic subgroup of K^{d_0} and H_1 an algebraic subgroup of $(K^*)^{d_1}$. Moreover, if the dimensions of H_0 and H_1 are respectively δ_0 and δ_1, then the dimension of $H_0 \times H_1$ is $\delta_0 + \delta_1$, and for all $(D_0, D_1) \in \mathbb{N}^2$ we have*

$$\mathcal{H}(H_0 \times H_1; D_0, D_1) = \frac{(\delta_0 + \delta_1)!}{\delta_0!\delta_1!}\mathcal{H}(H_0; D_0)\mathcal{H}(H_1; D_1).$$

Proof. It is clear that the product of an algebraic subgroup of K^{d_0} by an algebraic subgroup of $(K^*)^{d_1}$ is an algebraic subgroup of G. It remains to show the converse. The rest of the lemma follows from Lemma 8.2.

Let H be an algebraic subgroup of G. Define

$$H_0 = \{x \in K^{d_0}\,;\, (x, 1) \in H\} \quad \text{and} \quad H_1 = \{y \in (K^*)^{d_1}\,;\, (0, y) \in H\}$$

where 0 and 1 denote respectively the neutral elements of K^{d_0} and $(K^*)^{d_1}$. Then, H_0 and H_1 are algebraic subgroups of K^{d_0} and $(K^*)^{d_1}$ respectively, and their product $H_0 \times H_1$ is contained in H. To prove that H is precisely $H_0 \times H_1$, we choose an element (x, y) of H and a polynomial $P(\underline{X}, \underline{Y}) \in K[\underline{X}, \underline{Y}]$ which vanishes identically on H, and we show that P vanishes at $(x, 1)$ and $(0, y)$: since P is arbitrary, this will imply that $(x, 1)$ and $(0, y)$ belong to H, and therefore $(x, y) \in H_0 \times H_1$. Let us write $x = (x_1, \ldots, x_{d_0})$ and $y = (y_1, \ldots, y_{d_1})$, and consider the function $f\colon \mathbb{Z}^2 \to K$ given by

$$f(m, n) = P(mx_1, \ldots, mx_{d_0}, y_1^n, \ldots, y_{d_1}^n)$$

for all $(m, n) \in \mathbb{Z}^2$. After simplifications, it can be written in the form

$$f(m, n) = \sum_{i=1}^{s} Q_i(m)a_i^n$$

where $Q_1(X), \ldots, Q_s(X)$ are elements of $K[X]$ and $a_1, \ldots, a_s$ are distinct elements of K^*. Since P vanishes on $n(x, y)$ for all $n \in \mathbb{Z}$, we have $f(n, n) = 0$ for the same values of n. By a property of exponential polynomials (see Chapter 2, Ex. 2), this implies that $Q_1(X), \ldots, Q_s(X)$ are all equal to 0, and so the function f vanishes identically on $\mathbb{Z}^2$. In particular we have $f(1, 0) = 0$ and $f(0, 1) = 0$ which mean that P vanishes at $(x, 1)$ and at $(0, y)$. □

Lemma 8.6. — *Assume $d_0 > 0$. Then, the algebraic subgroups of K^{d_0} are its vector subspaces over K. If V is a vector subspace of K^{d_0} over K and if δ_0 is its dimension over K, then δ_0 is also the dimension of V as an algebraic subgroup of K^{d_0}, and for all $D \in \mathbb{N}$ we have*

$$\mathcal{H}(V; D) = D^{\delta_0}.$$

Proof. Let H be an algebraic subgroup of K^{d_0}. It is closed under addition; so, to prove that it is a vector subspace of K^{d_0}, it suffices to show that it is also closed under scalar multiplication by the elements of K. Let $x = (x_1, \ldots, x_{d_0})$ be an element of H and let $P(\underline{X}) \in K[\underline{X}]$ be a polynomial which vanishes identically on H. The function $f\colon K \to K$ given by $f(t) = P(tx_1, \ldots, tx_{d_0})$ for all $t \in K$ is a polynomial map. Since $P(nx) = 0$ for all $n \in \mathbb{Z}$, it vanishes on $\mathbb{Z}$ and so it vanishes identically on K. The choice of P being arbitrary, this shows that tx belongs to H for all $t \in K$, thereby proving that H is closed under scalar multiplication.

Conversely, let V be a vector subspace of K^{d_0} over K. We already noticed that V is an algebraic subgroup of K^{d_0}. If $V = 0$, we have $H(V; D) = 1$ for all $D \in \mathbb{N}$. Assume $V \neq 0$. Put $\delta_0 = \dim_K(V)$ and choose a K-isomorphism $\theta\colon K^{\delta_0} \to V$. The vector space of mappings from V to K is isomorphic to the vector space of mappings from K^{δ_0} to K via the map that sends a function $f\colon V \to K$ to the composite $f \circ \theta\colon K^{\delta_0} \to K$. If f is induced by a polynomial of $K[X_1, \ldots, X_{d_0}]$ of degree $\leq D$ then $f \circ \theta$ is induced by a polynomial of $K[X_1, \ldots, X_{\delta_0}]$ of degree $\leq D$, and conversely. This shows that for all $D \in \mathbb{N}$, we have

$$H(V; D) = \binom{D + \delta_0}{\delta_0} = \frac{1}{\delta_0!}D^{\delta_0} + \cdots\ .$$

The formula for $\mathcal{H}(V; D)$ follows. □

Lemma 8.7. — *Assume $d_1 > 0$. Then, the map which sends a subgroup Φ of $\mathbb{Z}^{d_1}$ to the subgroup T_Φ of $(K^*)^{d_1}$ establishes a bijection between the subgroups of $\mathbb{Z}^{d_1}$ and the algebraic subgroups of $(K^*)^{d_1}$. Moreover, if Φ is subgroup of $\mathbb{Z}^{d_1}$ of rank $d_1 - \delta_1$, then the dimension of T_Φ is δ_1 and for all $D \in \mathbb{N}$ we have*

$$\mathcal{H}(T_\Phi; D) \geq D^{\delta_1}.$$

Proof. For each $\varphi = (\varphi_1, \dots, \varphi_{d_1}) \in \mathbb{Z}^{d_1}$ we define a character $\chi_\varphi \colon (K^*)^{d_1} \to K^*$ by

$$\chi_\varphi(y_1, \dots, y_{d_1}) = y_1^{\varphi_1} \cdots y_{d_1}^{\varphi_{d_1}} \quad \text{for all } (y_1, \dots, y_{d_1}) \in (K^*)^{d_1}.$$

We also associate to each algebraic subgroup H of $(K^*)^{d_1}$ a subgroup $\Phi(H)$ of $\mathbb{Z}^{d_1}$:

$$\Phi(H) = \{\varphi \in \mathbb{Z}^{d_1} \, ; \, H \subset \ker(\chi_\varphi)\}.$$

Our aim is to show that the map which sends a subgroup Φ of $\mathbb{Z}^{d_1}$ to the algebraic subgroup T_Φ of $(K^*)^{d_1}$, and the map which sends an algebraic subgroup H of $(K^*)^{d_1}$ to the subgroup $\Phi(H)$ of $\mathbb{Z}^{d_1}$ are inverse one to the other. This will prove the first half of the proposition. We readily note the inclusions $H \subset T_{\Phi(H)}$ and $\Phi \subset \Phi(T_\Phi)$. It remains to show that in both cases we in fact have an equality.

Consider first an algebraic subgroup H of $(K^*)^{d_1}$ and put $H' = T_{\Phi(H)}$. By construction, if φ and ψ are elements of $\mathbb{Z}^{d_1}$, then χ_φ and χ_ψ restrict to the same character of H in K^* if and only if φ and ψ belong to the same translate of $\Phi(H)$ in $\mathbb{Z}^{d_1}$, in which case they also restrict to the same character of H'. We will show the equality $H = H'$ by proving that any polynomial $P(\underline{Y}) \in K[\underline{Y}]$ which vanishes on H also vanishes on H'. In fact, the function $f \colon (K^*)^{d_1} \to K$ induced by a polynomial can be written as a linear combination

$$f = \sum_{\varphi \in R} p_\varphi \chi_\varphi$$

where R is a finite subset of $\mathbb{N}^{d_1}$ and $(p_\varphi)_{\varphi \in R}$ is a family of elements of K. Let $\overline{R}$ be the image of R under the canonical map from $\mathbb{Z}^{d_1}$ to $\mathbb{Z}^{d_1}/\Phi(H)$. For each $\overline{\varphi} \in \overline{R}$, we denote by $R_{\overline{\varphi}}$ the inverse image of $\overline{\varphi}$ in R and by $\chi_{\overline{\varphi}}$ and $\chi'_{\overline{\varphi}}$ the respective characters of H and H' in K^* induced by restriction by χ_φ for any $\varphi \in \overline{\varphi}$: these characters do not depend on the choice of φ. Then, the restriction of f to H and H' are respectively

$$\sum_{\overline{\varphi} \in \overline{R}} \Big(\sum_{\varphi \in R_{\overline{\varphi}}} p_\varphi \Big) \chi_{\overline{\varphi}} \quad \text{and} \quad \sum_{\overline{\varphi} \in \overline{R}} \Big(\sum_{\varphi \in R_{\overline{\varphi}}} p_\varphi \Big) \chi'_{\overline{\varphi}}.$$

If f vanishes on H, then the left sum is zero, and since the mappings $\chi_{\overline{\varphi}}$ with $\overline{\varphi} \in \overline{R}$ are distinct characters of H in K^*, Artin's theorem on the independence of characters (*) implies that they are linearly independent over K. We then have

$$\sum_{\varphi \in R_{\overline{\varphi}}} p_\varphi = 0 \quad \text{for all } \overline{\varphi} \in \overline{R},$$

and this shows that the restriction of f to H' is also zero.

Now, let Φ be a subgroup of $\mathbb{Z}^{d_1}$ and let $\Phi' = \Phi(T_\Phi)$. We have $\Phi \subset \Phi'$ and $T_\Phi = T_{\Phi'}$. If $\Phi \neq \Phi'$, then, since K is algebraically closed, there exists a non-trivial character of Φ' in K^* which is trivial on Φ. This character extends to a character $c \colon \mathbb{Z}^{d_1} \to K^*$ given by

$$c(\varphi_1, \dots, \varphi_{d_1}) = y_1^{\varphi_1} \cdots y_{d_1}^{\varphi_{d_1}}$$

for an element $y = (y_1, \dots, y_{d_1})$ of $(K^*)^{d_1}$. By construction, we have $y \in T_\Phi$ and $y \notin T_{\Phi'}$. This contradiction shows that we must have $\Phi = \Phi'$.

(*) See for instance S. Lang, Algebra, Second Ed. (1984), Addison Wesley, Chap.8, Theorem 4.1.

Finally, let Φ be a subgroup of $\mathbb{Z}^{d_1}$ and let $\delta_1 = d_1 - \mathrm{rk}_{\mathbb{Z}}(\Phi)$. We choose among the canonical basis of $\mathbb{Z}^{d_1}$ over $\mathbb{Z}$ a maximal subset $\{u_1, \dots, u_{\delta_1}\}$ whose image in $\mathbb{Z}^{d_1}/\Phi$ is linearly independent over $\mathbb{Z}$. For each $D \in \mathbb{N}$, we form the sets

$$A(D) = \{(a_1, \dots, a_{d_1}) + \Phi\,;\, (a_1, \dots, a_{d_1}) \in \mathbb{N}^{d_1}, \sum_{i=1}^{d_1} a_i \le D\},$$

$$B(D) = \{a_1u_1 + \cdots + a_{\delta_1}u_{\delta_1} + \Phi\,;\, (a_1, \dots, a_{\delta_1}) \in \mathbb{N}^{\delta_1}, \sum_{i=1}^{\delta_1} a_i \le D\},$$

$$B'(D) = \{a_1u_1 + \cdots + a_{\delta_1}u_{\delta_1} + \Phi\,;\, (a_1, \dots, a_{\delta_1}) \in \mathbb{Z}^{\delta_1}, \sum_{i=1}^{\delta_1} |a_i| \le D\}.$$

Then, $H(T_\Phi; D)$ is the cardinality of $A(D)$ and, since $B(D) \subset A(D)$, we get:

$$H(T_\Phi; D) \ge \mathrm{Card}(B(D)) = \binom{D + \delta_1}{\delta_1}.$$

On the other hand, since $\Phi + \mathbb{Z}u_1 + \cdots + \mathbb{Z}u_{\delta_1}$ is of finite index in $\mathbb{Z}^{d_1}$, it contains $m\mathbb{Z}^{d_1}$ for an integer $m \ge 1$, and there exists an integer $c \ge 1$ such that $B'(c)$ contains $mA(1)$. This implies $mA(D) \subset B'(cD)$, and since $A(D)$ is contained in the union of at most m^{d_1} translates of $mA(D)$, we obtain:

$$H(T_\Phi; D) = \mathrm{Card}(A(D)) \le m^{d_1}(1 + 2cD)^{\delta_1}.$$

This inequality and the preceding one show that the degree of the Hilbert–Samuel polynomial of T_Φ is δ_1 and that we have $\mathcal{H}(T_\Phi; D) \ge D^{\delta_1}$. In particular, T_Φ has dimension δ_1. □

1 Algebraic subvarieties of G Most definitions and results about algebraic subsets of K^d also extend to algebraic subsets of G. First, we see that the family of algebraic subsets of G is closed under union and intersection. Let us say that an algebraic subset V of G is *irreducible* or that it is *an algebraic subvariety* of G if it cannot be written as the union of two algebraic subsets of G, none of which is V. It follows from this that whenever an algebraic subvariety of G is contained in a finite union of algebraic subsets of G, then it is contained in one of them. The empty set is an example of algebraic subvariety of G. In analogy with the case of the algebraic subsets of K^d, let us define the *irreducible components* of an algebraic subset V of G as the maximal algebraic subvarieties of G contained in V. Then, we have the following result which shows in particular that each algebraic subset of G is a finite union of irreducible ones:

Lemma 8.8. — *Each algebraic subset of G has a finite number of irreducible components. If $V_1, \dots, V_s$ are the distinct irreducible components of an algebraic subset V of G, then V is their union, and $\overline{V}_1, \dots, \overline{V}_s$ are the distinct irreducible components of the algebraic subset $\overline{V}$ of K^d. Finally, if V' is an algebraic subset of K^d, and if $V'_1, \dots, V'_s$ are the distinct irreducible components of V' which meet G, then $V'_1 \cap G, \dots, V'_s \cap G$ are the distinct irreducible components of the algebraic subset $V' \cap G$ of G.*

Proof. We begin by establishing the following fact: *if V' is an algebraic subvariety of K^d, then $V' \cap G$ is an algebraic subvariety of G, and if moreover $V' \cap G \ne \emptyset$, then $V' = \overline{V' \cap G}$.* In fact, let V' be an algebraic subvariety of K^d. If $V' \cap G$ is empty, it is certainly irreducible. Assume $V' \cap G \ne \emptyset$. We observe that the complement of G in K^d is an algebraic subset U of K^d:

$$U = \{(x_1, \dots, x_{d_0}, y_1, \dots, y_{d_1}) \in K^{d_0} \times K^{d_1}\,;\, y_1 \cdots y_{d_1} = 0\},$$

and that we have $V' \subset (\overline{V' \cap G}) \cup U$. Since V' is irreducible and not contained in U, this implies $V' \subset \overline{V' \cap G}$, hence $V' = \overline{V' \cap G}$. Moreover, let V_1, V_2 be algebraic subsets of G whose union is $V' \cap G$. From the equality $V' = \overline{V' \cap G}$, we deduce $V' = \overline{V}_1 \cup \overline{V}_2$. Since V' is irreducible this implies $V' = \overline{V}_i$ for $i = 1$ or 2, and therefore $V' \cap G = V_i$ for the same value of i. This shows that $V' \cap G$ is irreducible and proves our assertion.

Let V' be an algebraic subset of K^d and let $V'_1, \dots, V'_s$ be the distinct irreducible components of V' which meet G. Define $V = V' \cap G$ and $V_i = V'_i \cap G$ for $i = 1, \dots, s$. Since any algebraic subset V of G arises

in this way, we only have to show that $V_1, \ldots, V_s$ are the distinct irreducible components of V, that their union is V, and that $\overline{V}_1, \ldots, \overline{V}_s$ are the distinct irreducible components of $\overline{V}$. We first observe that V is the union of $V_1, \ldots, V_s$ since V' is the union of its irreducible components. By the fact proven at the beginning, $V_1, \ldots, V_s$ are irreducible and we have $V_i' = \overline{V}_i$ for $i = 1, \ldots, s$. Since $V_i' \not\subset V_j'$ for $i \neq j$, this implies $V_i \not\subset V_j$ for $i \neq j$. Therefore $V_1, \ldots, V_s$ are the distinct irreducible components of V. Finally, since V is the union of $V_1, \ldots, V_s$, the set $\overline{V}$ is the union of $\overline{V}_1, \ldots, \overline{V}_s$. Since $\overline{V}_1, \ldots, \overline{V}_s$ are distinct irreducible components of V', they are all the distinct irreducible components of $\overline{V}$. □

Remark. The proof of this lemma rests on the fact that G is the complement of an algebraic subset U of K^d. A similar result holds in general for the algebraic subsets of any *quasi-affine algebraic subvariety* of K^d (see Chapter 1, §1 of [H]).

Lemma 8.9. — *If W, V are non-empty algebraic subsets of G with $W \subset V$, then their dimensions satisfy* $\dim(W) \leq \dim(V)$ *with equality if and only if W and V have a common irreducible component of dimension* $\dim(V)$*; in particular, V contains only finitely many algebraic subvarieties of G of dimension* $\dim(V)$.

Proof. Since $W \subset V$, we have $\overline{W} \subset \overline{V}$, and the conclusion follows from the corresponding fact about algebraic subsets of K^d, using Lemma 8.8. □

Lemma 8.10. — *Let V be a non-empty algebraic subset of G and let $V_1, \ldots, V_r$ be its irreducible components of dimension* $\dim(V)$*. Then, for all $(D_0, D_1) \in \mathbb{N}^2$, we have*

$$\mathcal{H}(V; D_0, D_1) = \sum_{i=1}^{r} \mathcal{H}(V_i; D_0, D_1).$$

Proof. By Lemma 8.8, $\overline{V}_1, \ldots, \overline{V}_r$ are the irreducible components of $\overline{V}$ of dimension $\dim(\overline{V})$. Therefore, the polynomial $\mathcal{H}(\overline{V}; D_0, D_1)$ associated to $\overline{V}$ is the sum of the corresponding polynomials associated to $\overline{V}_1, \ldots, \overline{V}_r$. The equality of the lemma then follows from the fact that, for each subset E of K^d, the polynomial $\mathcal{H}(E; D_0, D_1)$ associated to E is the same as the corresponding polynomial associated to $\overline{E}$. □

For each $g \in G$, we denote by $\tau_g \colon G \to G$, the operator of translation by g in G:

$$\tau_g(x) = g + x \qquad \text{for all } x \in G.$$

Looking at the addition law in G, we see that each τ_g is given in coordinates by polynomials of degree 1. We will need these operators in the proofs of the next three lemmas.

Lemma 8.11. — *Let V be a non-empty algebraic subset of G and let $g \in G$. Then, $g + V$ is an algebraic subset of G with the same dimension as V and we have*

$$\mathcal{H}(g + V; D_0, D_1) = \mathcal{H}(V; D_0, D_1)$$

for all $(D_0, D_1) \in \mathbb{N}^2$; moreover, $g + V$ is irreducible if V is irreducible.

Proof. By hypothesis, V is the set of common zeroes in G of a family of polynomials $\{P_\alpha\}_{\alpha \in I}$. Therefore, $g + V = \tau_g(V)$ is the set of common zeroes in G of the polynomials $P_\alpha \circ \tau_{-g}$ with $\alpha \in I$. This proves that $g + V$ is an algebraic subset of G.

The vector space of mappings from $g + V$ to K is isomorphic to the vector space of mappings from V to K under the map which sends a function $f \colon g + V \to K$ to the composite $f \circ \tau_g \colon V \to K$. If f is induced by a polynomial of bidegree $\leq (D_0, D_1)$, then $f \circ \tau_g$ is also induced by a polynomial of bidegree $\leq (D_0, D_1)$, and conversely. We therefore have

$$H(g + V; D_0, D_1) = H(V; D_0, D_1)$$

for all $(D_0, D_1) \in \mathbb{N}^2$. This shows that V and $g+V$ have the same Hilbert-Samuel polynomial. Consequently, they have the same dimension, and the polynomials $\mathcal{H}(g + V; D_0, D_1)$ and $\mathcal{H}(V; D_0, D_1)$ coincide for all $(D_0, D_1) \in \mathbb{N}^2$.

Finally, assume that V is irreducible. If $g + V$ were not irreducible, it could be written as the union of two algebraic subsets V_1, V_2 of G both distinct from $g+V$; then V would be the union of $-g+V_1$ and $-g+V_2$, and this is a contradiction since both are algebraic subsets of G which are distinct from V. Therefore $g + V$ is irreducible. □

Lemma 8.12. — *Let H be an algebraic subgroup of G, and let E be a finite and non-empty union of translates of H in G. Then, E is an algebraic subset of G and, for all $(D_0, D_1) \in \mathbb{N}^2$, we have*

$$\mathcal{H}(E; D_0, D_1) = \mathrm{Card}(E/H)\mathcal{H}(H; D_0, D_1).$$

Proof. Let n be the dimension of H. Lemma 8.11 shows that each translate $g + H$ of H is an algebraic subset of G of dimension n and that the polynomials $\mathcal{H}(g + H; D_0, D_1)$ and $\mathcal{H}(H; D_0, D_1)$ are the same. Since E is a disjoint union of translates of H, E is therefore an algebraic subset of G of dimension n, and the conclusion follows by applying Lemma 8.10. □

Lemma 8.13. — *Let V and X be algebraic subsets of G. Define*

$$E = \{g \in G\,;\, g + V \subset X\}.$$

Then E is an algebraic subset of G. Moreover, if X is defined by polynomials of bidegree $\leq (D_0, D_1)$, then E is also defined by polynomials of bidegree $\leq (D_0, D_1)$.

Proof. Let $\{P_\alpha\}_{\alpha \in I}$ be a family of polynomials whose set of common zeroes in G is X. We have

$$\begin{aligned} E &= \{g \in G\,;\, g + v \in X \quad \text{for all} \quad v \in V\} \\ &= \{g \in G\,;\, P_\alpha(g + v) = 0 \quad \text{for all} \quad \alpha \in I, \quad v \in V\}. \end{aligned}$$

This shows that E is the set of common zeroes in G of the polynomials $P_\alpha \circ \tau_v$ with $\alpha \in I$ and $v \in V$. Therefore E is an algebraic subset of G. Furthermore, if the polynomials P_α are of bidegree $\leq (D_0, D_1)$, then the same holds for the polynomials $P_\alpha \circ \tau_v$. This proves the second part of the lemma. □

We conclude this section with a proof of the following fundamental result due to P. Philippon (see Proposition 3.3 of [P]):

Proposition 8.14. — *Let D_0, D_1 be non-negative integers, and let V be a non-empty algebraic subset of G which is defined by polynomials of bidegree $\leq (D_0, D_1)$. Then we have*

$$\mathcal{H}(V; D_0, D_1) \leq \mathcal{H}(G; D_0, D_1).$$

For the proof of this proposition we shall say that an algebraic subset of G or of K^d is *equidimensional* if all its irreducible components have the same dimension. We will need the following lemma:

Lemma 8.15. — *Let W be an algebraic subvariety of G of dimension $n \geq 1$ and let Z be the set of zeroes in G of a polynomial P of bidegree $\leq (D_0, D_1)$. Assume that $W \cap Z$ is not empty and distinct from W. Then, $W \cap Z$ is an equidimensional algebraic subset of G of dimension $n - 1$, and we have*

$$\mathcal{H}(W \cap Z; D_0, D_1) \leq \mathcal{H}(W; D_0, D_1).$$

Proof. Let $W' = \overline{W}$. By Lemma 8.8, this is an algebraic subvariety of K^d, and its dimension is n. Let Z' be the set of zeroes of P in K^d. Since $W \not\subset Z'$, the polynomial P does not vanish identically on W'; it then follows from Theorem 1.11A and exercise 1.8 in chapter 1 of [H] that $W' \cap Z'$ is an equidimensional algebraic subset of K^d of dimension $n - 1$. Moreover, Lemma 3.1 of [P] gives

$$\mathcal{H}(W' \cap Z'; D_0, D_1) \leq \mathcal{H}(W'; D_0, D_1).$$

Since $W \cap Z$ is the intersection of $W' \cap Z'$ with G, this implies, by virtue of Lemmas 8.8 and 8.10, that $W \cap Z$ is an equidimensional algebraic subset of G of dimension $n - 1$ and that we have

$$\mathcal{H}(W \cap Z; D_0, D_1) \leq \mathcal{H}(W' \cap Z'; D_0, D_1).$$

Since $W' = \overline{W}$, we also have $\mathcal{H}(W'; D_0, D_1) = \mathcal{H}(W; D_0, D_1)$. The inequality of the lemma follows. □

Remark. In particular, if we choose $W = G$, the preceding lemma shows that the set of zeroes in G of a non-zero polynomial which vanishes at least at one point of G is equidimensional of dimension $d-1$.

Proof of Proposition 8.14. Define $r = d - \dim(V)$, and let S be a family of polynomials with bidegree $\leq (D_0, D_1)$ whose set of common zeroes in G is V. By induction on the integer $i = 0, \ldots, r$, we shall construct an equidimensional algebraic subset V_i of G of dimension $d-i$ which contains V and satisfies

$$\mathcal{H}(V_i; D_0, D_1) \leq \mathcal{H}(G; D_0, D_1). \tag{8.16}$$

For $i = 0$, we set $V_0 = G$. Assume that V_i is constructed for an integer $i \geq 0$ with $i < r$, and let $W_1, \ldots, W_s$ be the irreducible components of V_i. We have

$$V \subset W_1 \cup \cdots \cup W_s.$$

Since $\dim(W_j) = d - i > \dim(V)$, there exists for each j a polynomial P_j in S which does not vanish everywhere on W_j; let Z_j be the set of zeroes of P_j in G. We define

$$V_{i+1} = (W_1 \cap Z_1) \cup \cdots \cup (W_s \cap Z_s).$$

By construction, V_{i+1} contains V, therefore $V_{i+1} \neq \emptyset$. Without loss of generality, we may assume that there exists an integer $t \geq 1$ such that $W_j \cap Z_j \neq \emptyset$ for $j = 1, \ldots, t$, and $W_j \cap Z_j = \emptyset$ for $j > t$. Then, Lemma 8.15 shows that $W_j \cap Z_j$ is an equidimensional algebraic subset of G of dimension $d-i-1$ for $j = 1, \ldots, t$. Therefore, V_{i+1} is also an equidimensional algebraic subset of G of dimension $d-i-1$ and its irreducible components are the union of those of $W_j \cap Z_j$ for $j = 1, \ldots, t$. By virtue of Lemma 8.10, this gives

$$\mathcal{H}(V_{i+1}; D_0, D_1) \leq \sum_{j=1}^{t} \mathcal{H}(W_j \cap Z_j; D_0, D_1).$$

Since each P_j is of bidegree $\leq (D_0, D_1)$, we also have, by Lemma 8.15,

$$\sum_{j=1}^{t} \mathcal{H}(W_j \cap Z_j; D_0, D_1) \leq \sum_{j=1}^{t} \mathcal{H}(W_j; D_0, D_1).$$

Since $W_1, \ldots, W_t$ are among the irreducible components of V_i of dimension $d-i$, Lemma 8.10 gives

$$\sum_{j=1}^{t} \mathcal{H}(W_j; D_0, D_1) \leq \mathcal{H}(V_i; D_0, D_1).$$

Combining these inequalities with (8.16), we get $\mathcal{H}(V_{i+1}; D_0, D_1) \leq \mathcal{H}(G; D_0, D_1)$ as required. This shows the existence of $V_0, \ldots, V_r$. Since V and V_r have the same dimension $d-r$, the inclusion $V \subset V_r$ implies that the irreducible components of V of dimension $d-r$ are among those of V_r; therefore applying Lemma 8.10 and using the relation (8.16) with $i = r$, we get

$$\mathcal{H}(V; D_0, D_1) \leq \mathcal{H}(V_r; D_0, D_1) \leq \mathcal{H}(G; D_0, D_1).$$

The proof is complete. □

1 The zero estimate The main result of Philippon in [P] has the following consequence:

Theorem 8.17. — *Let Σ be a finite subset of G which contains 0 (the identity of G). Assume that there exists a non-zero polynomial P of bidegree $\leq (D_0, D_1)$, which vanishes at each point of $\Sigma[d]$. Then there exists an algebraic subgroup H of G, with $H \neq G$, such that*

$$\mathrm{Card}\big((\Sigma + H)/H\big)\mathcal{H}(H; D_0, D_1) \leq \mathcal{H}(G; D_0, D_1).$$

Using Proposition 8.3 and the value of $\mathcal{H}(G; D_0, D_1)$ given by (8.4), we readily deduce Proposition 8.1 for an algebraically closed field K.

If we set $D_0 = D_1 = D$, we get a lower bound for the degree of polynomials which vanish on $\Sigma[d]$. The zero estimate above is more general since it yields a constraint for the bidegree of such polynomials. In the applications, it turns out to be essentially optimal (see exercise 3).

Proof of Theorem 8.17. Let us denote by X_1 the set of zeroes of P in G. For each integer $r \geq 2$, we define

$$X_r = \bigcap_{(\sigma_1,\dots,\sigma_{r-1})\in\Sigma^{r-1}} \big(-\sigma_1 - \cdots - \sigma_{r-1} + X_1\big).$$

We can also view X_r as the set of common zeroes in G of the polynomials $P\circ\tau_{\sigma_1+\cdots+\sigma_{r-1}}$ with $(\sigma_1, \dots, \sigma_{r-1}) \in \Sigma^{r-1}$. Therefore, for each integer $r \geq 1$, X_r is an algebraic subset of G which is defined by polynomials of bidegree $\leq (D_0, D_1)$.

The sets $X_1, X_2, \dots$ are related by the formulas

$$X_{r+1} = \bigcap_{\sigma\in\Sigma} \big(-\sigma + X_r\big), \qquad (r \geq 1). \tag{8.18}$$

Since $0 \in \Sigma$, this implies

$$X_1 \supset X_2 \supset \cdots \supset X_{d+1} \supset \cdots$$

Since P vanishes on $\Sigma[d]$, X_{d+1} contains 0 ; therefore this set is not empty. On the other hand, since $P \neq 0$, we have $\dim(X_1) = d - 1$. Consequently, there exists a positive integer $r \leq d$ such that

$$\dim(X_r) = \dim(X_{r+1}).$$

Let n be the common dimension of X_r and X_{r+1}, and let V be an irreducible component of dimension n of X_{r+1}. Using (8.18), we get

$$V \subset \bigcap_{\sigma\in\Sigma} \big(-\sigma + X_r\big);$$

hence for all $\sigma \in \Sigma$, $\sigma + V$ is contained in X_r. We set

$$E = \{g \in G\,;\, g + V \subset X_r\}.$$

We just showed $\Sigma \subset E$. We also set

$$H = \{g \in G\,;\, g + V = V\}$$

and

$$R = \{g + V\,;\, g \in E\}.$$

From lemma 8.11 we deduce that the elements in the set R are, like V, algebraic subvarieties of G of dimension n. Since they are contained in X_r, and since X_r has dimension n, R is a finite set. We notice also that H is a subgroup of G, that E is stable under translation by the elements of H, and that there is a bijection

$$E/H \longrightarrow R.$$

Therefore E is a finite union of translates of H. Lemma 8.13, with $X = V$, shows that H is an algebraic subset of G. Hence H is an algebraic subgroup of G. It is distinct from G because V is non-empty and strictly contained in G. Applying again lemma 8.13, but with $X = X_r$, shows that E is an algebraic subset of G, which is defined, like X_r, by polynomials of bidegree $\leq (D_0, D_1)$. Since E is a finite union of translates of H, lemma 8.12 gives

$$\mathcal{H}(E; D_0, D_1) = \mathrm{Card}(E/H)\mathcal{H}(H; D_0, D_1).$$

Since E is defined by polynomials of bidegree $\leq (D_0, D_1)$, Proposition 8.14 provides an upper bound for the left hand side of the previous equality:

$$\mathcal{H}(E; D_0, D_1) \leq \mathcal{H}(G; D_0, D_1).$$

Finally, since $\Sigma \subset E$, we have

$$\mathrm{Card}(E/H) \geq \mathrm{Card}\big((\Sigma + H)/H\big).$$

□

1Exercises **1.** Prove Proposition 8.1 for any field K of characteristic zero on the basis that it is true when K is algebraically closed.

`Hint.` *For all fields K and all subgroups Φ of $\mathbb{Z}^{d_1}$, define $G(K) = K^{d_0} \times (K^*)^{d_1}$ and*

$$T_\Phi(K) = \big\{(y_1, \ldots, y_{d_1}) \in (K^*)^{d_1}\,;\, y_1^{\varphi_1} \cdots y_{d_1}^{\varphi_{d_1}} = 1 \text{ for all } \varphi = (\varphi_1, \ldots, \varphi_{d_1}) \in \Phi\big\}.$$

Now, fix a field K of characteristic zero and denote by $\bar{K}$ its algebraic closure. Assume that there exists a non-zero polynomial $P \in K[\underline{X}, \underline{Y}]$ of bidegree $\leq (D_0, D_1)$ which vanishes at each point of $\Sigma[d]$ where Σ is a finite subset of $G(K)$ containing 0. Since P belongs to $\bar{K}[\underline{X}, \underline{Y}]$ and since Σ is contained in $G(\bar{K})$, we know that there exist a vector subspace V of $\bar{K}^{d_0}$ of dimension $\delta_0 \geq 0$ and a subgroup Φ of $\mathbb{Z}^{d_1}$ of rank $d_1 - \delta_1$ with $\delta = \delta_0 + \delta_1 < d$ such that the subgroup $H = V \times T_\Phi(\bar{K})$ of $G(\bar{K})$ satisfies

$$\frac{\delta!}{\delta_0!\delta_1!}\mathrm{Card}\big((\Sigma + H)/H\big) \leq \frac{d!}{d_0!d_1!} D_0^{d_0-\delta_0} D_1^{d_1-\delta_1}.$$

Show that

$$\mathrm{Card}\big((\Sigma + H)/H\big) = \mathrm{Card}\big((\Sigma + H')/H'\big)$$

where H' is the subgroup $(V \cap K^{d_0}) \times T_\Phi(K)$ of $G(K)$.

2. Let H be an algebraic subgroup of G. Show that exactly one of the irreducible components of H is an algebraic subgroup H' of G and that the others are translates of H'. Deduce from this that H is equidimensional.

`Hint.` *Let n be the dimension of H, and let V be an irreducible component of H of dimension n. Define*

$$H' = \{g \in G\,;\, g + V = V\} \quad \text{and} \quad R = \{g + V\,;\, g \in H\}.$$

Show that H' is an algebraic subgroup of H, that R is the set of all irreducible components of H and that the quotient H/H' is in bijection with R. Deduce from this that the dimension of H' is n. Moreover, choose $g \in V$ and show that H' is contained in $-g + V$. Since $-g + V$ is irreducible and has dimension n, conclude that H' coincides with it.

3. (A converse to Theorem 8.17) Let Σ be a finite subset of G and let G' be an algebraic subgroup of G with $G' \neq G$. Show that for any $(D_0, D_1) \in \mathbb{N}^2$ satisfying

$$\mathrm{Card}\big((\Sigma + G')/G'\big) H(G'; D_0, D_1) < H(G; D_0, D_1) \tag{8.19}$$

there exists a non-zero polynomial P of bidegree $\leq (D_0, D_1)$, which vanishes at each point of Σ.

`Hint.` *Let $E = \cup_{\sigma \in \Sigma}(\sigma + G')$. Show that the left hand side of* (8.19) *is $\geq H(E; D_0, D_1)$. Therefore, if* (8.19) *holds, there exists a non-zero polynomial P of bidegree $\leq (D_0, D_1)$ which vanishes identically on E.*

4. Use Proposition 8.14 with $d_0 = n$ and $d_1 = 0$ to prove Lemma 5.6, namely that if F is a finite algebraic subset of K^n defined by polynomials of $K[X_1, \ldots, X_n]$ of degree $\leq D$, then the cardinality of F is $\leq D^n$.

`Hint.` *Show that for a finite algebraic subset F of K^n, the polynomial $\mathcal{H}(F; T) \in K[T]$ is constant, equal to the cardinality of F.*

1References

[H] R. Hartshorne. – *Algebraic Geometry*, Springer-Verlag, New-York (1977).

[M] D.W. Masser. – On polynomials and exponential polynomials in several variables ; *Invent. Math.*, **63** (1981), 81–95.

[P] P. Philippon. – Lemme de zéros dans les groupes algébriques commutatifs ; *Bull. Soc. Math. France*, **114** (1986), 355–383 and **115** (1987), 397–398.

9.– INTERPOLATION DETERMINANTS (CONTINUED)

Our purpose in this Chapter is to introduce two refinements in the estimates of Chapter 7: in the upper bound for $|\Delta_n|$, we replace the function $\Phi_n(L)$ by a larger function $\tilde{\Phi}_n(L_0, L)$, which takes into account the fact that the interpolation determinant $\Big(f_\lambda(\zeta_\mu)\Big)$ involves functions f_λ of the form

$$z_1^{\lambda_1} \cdots z_n^{\lambda_n} \varphi_{\lambda_{n+1}}(\ell_1 z_1 + \cdots + \ell_n z_n)$$

where $0 \le \lambda_i \le L_0$ for $1 \le i \le n$, and φ_j are analytic functions of a single variable (see section 1). The point is that, apart from monomials in $z_1, \ldots, z_n$, the functions f_λ depend only of one variable. There is a connection (which is explained in [W]; see also Chapter 12) with the main idea of Baker's extrapolation argument, where derivatives are taken (in an n-dimensional space) of an auxiliary function, at several points which all lie on a complex line (of dimension 1).

The second refinement is due to M. Laurent [L]: in the transcendence proof we gave in Chapter 7, the upper bound for $|\Delta_r|$ came from the triangular inequality $|\Delta_r| \le |\Delta_n - \Delta_r| + |\Delta_n|$. The last term is quite small, but the difference $|\Delta_n - \Delta_r|$ was estimated very crudely: we said that it is at most the product of Λ by some number which is not too large. Michel Laurent wrote the expansion of this difference in powers of Λ and found that the first coefficients are pretty small, essentially as small as $|\Delta_n|$ (they are almost interpolation polynomials, again). As a consequence, in the upper bound for $|\Delta_r|$, it is possible to replace the main term U/L by U (see section 2).

1 Improving the analytic upper bound for the interpolation determinant

Let n, L_0 and L be positive integers, $\varphi_1, \ldots, \varphi_L$ be analytic functions in $\mathbb{C}$, $\ell_1, \ldots, \ell_n$ be complex numbers, and $a_{\lambda i}$ (for $1 \le i \le n$, $1 \le \lambda \le L$) be non-negative rational integers with $a_{\lambda 1} + \cdots + a_{\lambda n} \le L_0$, $(1 \le \lambda \le L)$. We define, for $1 \le \lambda \le L$,

$$f_\lambda(z_1, \ldots, z_n) = z_1^{a_{\lambda 1}} \cdots z_n^{a_{\lambda n}} \varphi_\lambda(\ell_1 z_1 + \cdots + \ell_n z_n).$$

Further let $\zeta_1, \ldots, \zeta_L$ be elements of $\mathbb{C}^n$. We consider the determinant

$$\Delta = \det\Big(f_\lambda(\zeta_\mu)\Big)_{1 \le \lambda, \mu \le L},$$

The upper bound we shall produce depends on the following quantity:

$$\tilde{\Theta}_n(L_0, L) = \min\{\|\kappa_1\| + \cdots + \|\kappa_L\|\}$$

where the minimum runs over the L-tuples $(\kappa_1, \ldots, \kappa_L)$ of elements of $\mathbb{N}^n$ which are pairwise distinct and satisfy $\kappa_{\lambda 2} + \cdots + \kappa_{\lambda n} \le L_0$ for $1 \le \lambda \le L$.

Lemma 9.1. — *The function of one complex variable z*

$$\Psi(z) = \det\Big(f_\lambda(z\zeta_\mu)\Big)_{1 \le \lambda, \mu \le L}$$

has a zero at $z = 0$ of multiplicity $\ge \tilde{\Theta}_n(L_0, L)$.

Proof. The multiplicity of the zero of Ψ at the origin is not affected by a change of variables in $\mathbb{C}^n$; also such a change of variables will not modify the degree of the monomials in $z_1, \ldots, z_n$; therefore we may assume $\ell_2 = \cdots = \ell_n = 0$.

Since the determinant is multilinear, by expanding each φ_λ in Taylor series at the origin, we may assume that each f_λ is a monomial $f_\lambda(\zeta) = \zeta^{\kappa_\lambda}$, with $\kappa_\lambda = (\kappa_{\lambda 1}, \ldots, \kappa_{\lambda n}) \in \mathbb{N}^n$ and $\kappa_{\lambda 2} + \cdots + \kappa_{\lambda n} \le L_0$. In this case $f_\lambda(z\zeta) = \zeta^{\kappa_\lambda} z^{\|\kappa_\lambda\|}$. If the elements $\kappa_1, \ldots, \kappa_L$ in $\mathbb{N}^n$ are not pairwise distinct, then $\Psi = 0$. If they are pairwise distinct, then Ψ has a zero at 0 of multiplicity at least $\|\kappa_1\| + \cdots + \|\kappa_L\|$, which proves our claim. □

Here is a lower bound for the coefficient $\tilde{\Theta}_n(L_0, L)$:

Lemma 9.2. — *For $L \geq 2n\binom{L_0+n}{n}$ and $L_0 \geq 2$ we have*

$$\tilde{\Theta}_n(L_0, L) > \frac{L^2}{4\binom{L_0+n-1}{n-1}}.$$

Notice that this estimate yields a stronger result than lemma 4.2 only if L_0 is small compared with $L^{1/n}$; in our case we shall have $L = \binom{L_0+n}{n}(L_1+1)$, and the main term in the final estimate involves

$$\frac{L}{\binom{L_0+n-1}{n-1}} = \frac{(L_0+n)(L_1+1)}{n} \qquad \text{in place of} \quad L^{1/n} \leq (L_0+n)(L_1+1)^{1/n}.$$

Proof. To begin with we assume only $L \geq 2$ and $L_0 \geq 1$. The lower bound is true for $n = 1$ (see lemma 2.2); hence we may assume $n \geq 2$. The smallest value for the sum $\|\kappa_1\| + \cdots + \|\kappa_L\|$ is reached when we choose successively, for each integers $a = 0, 1, \ldots$, all points in the domain

$$\mathcal{D}_a = \big\{(x_1, \ldots, x_n) \in \mathbb{N}^n\,;\, x_2 + \cdots + x_n \leq L_0,\, x_1 + \cdots + x_n = a\big\},$$

and we stop when the total number of points is L. For $a \geq L_0$ the number of points in $\mathcal{D}_a$ is exactly $\binom{L_0+n-1}{n-1}$ (once $(x_2, \ldots, x_n)$ is chosen, there is exactly one value for x_1); for $a < L_0$ the number of points in $\mathcal{D}_a$ is at most $\binom{a+n-1}{n-1}$ (we just forget the condition involving L_0), hence the number of points we get by varying a between 0 and, say, $A-1$ (with $A \geq L_0$), is at most

$$(A-L_0)\binom{L_0+n-1}{n-1} + \sum_{a=0}^{L_0-1}\binom{a+n-1}{n-1} = (A-L_0+1)\binom{L_0+n-1}{n-1}.$$

Therefore, it A is such that the above quantity is at most L, then

$$\tilde{\Theta}_n(L_0, L) \geq \sum_{a=L_0}^{A-1}\binom{L_0+n-1}{n-1}a = \frac{1}{2}\binom{L_0+n-1}{n-1}(A-L_0)(A+L_0-1).$$

We now assume $L \geq 2n\binom{L_0+n}{n}$ and $L_0 \geq 2$, and we choose

$$A = \left[\frac{L}{\binom{L_0+n-1}{n-1}}\right] + 1.$$

From the inequality $L_0 \geq 2$ we deduce that the required condition

$$(A-L_0+1)\binom{L_0+n-1}{n-1} \leq L$$

is satisfied. Since $A + L_0 - 1 \geq A + 1 > L/\binom{L_0+n-1}{n-1}$ we get

$$\tilde{\Theta}_n(L_0, L) \geq \frac{L}{2}(A-L_0).$$

Our assumption $L \geq 2n\binom{L_0+n}{n}$ implies $L \geq 2(L_0+1)\binom{L_0+n-1}{n-1}$, hence

$$A - L_0 \geq \frac{L}{2\binom{L_0+n-1}{n-1}}.$$

This completes the proof of lemma 9.2. □

1 Improving the upper bound for the distance between the two determinants The refinements which we give here rest on an idea due to M. Laurent [L].

Lemma 9.3. – *Let*

$$A = \Big(a_{\lambda\mu}\Big)_{1\le\lambda,\mu\le L} \qquad \text{and} \qquad B = \Big(b_{\lambda\mu}\Big)_{1\le\lambda,\mu\le L}$$

be two $L \times L$ matrices with complex coefficients, and let ϵ be a complex number. Then

$$\det(A + \epsilon B) = \sum_{I\subset\{1,\dots,L\}} \epsilon^{L-|I|}\Delta_I,$$

where I runs over the subsets of $\{1,\dots,L\}$, $|I|$ is the number of elements in I, and

$$\Delta_I = \det\Big(c_{\lambda\mu}^{(I)}\Big)_{1\le\lambda,\mu\le L},$$

with

$$c_{\lambda\mu}^{(I)} = \begin{cases} a_{\lambda\mu} & \text{if } \lambda \in I \\ b_{\lambda\mu} & \text{if } \lambda \notin I. \end{cases}$$

Proof. This follows from the multilinearity of the determinant. □

We shall apply this result when A in an interpolation matrix, with $a_{\lambda\mu} = f_\lambda(\zeta_\mu)$, and ϵ has a small absolute value (less than 1). When $|I|$ is small, say $\le L/2$, then the coefficient $\epsilon^{L-|I|}$ is small, namely $\le \epsilon^{L/2}$. For these terms a trivial upper bound for $|\Delta_I|$ will be sufficient. On the other hand, if $|I|$ is large, $|I| > L/2$, then Δ_I is almost an interpolation determinant, hence has a small absolute value. We give a more precise result which takes into account the estimate of section 1 (corresponding to $\epsilon = 0$).

Lemma 9.4. – *Let n, L_0, L and L' be positive integers with $L' \le L$, $\varphi_1,\dots,\varphi_{L'}$ be analytic functions in $\mathbb{C}$, $\ell_1,\dots,\ell_n$ be complex numbers, and $a_{\lambda i}$ (for $1 \le i \le n$, $1 \le \lambda \le L'$) be non-negative rational integers with $a_{\lambda 1} + \cdots + a_{\lambda n} \le L_0$. We define, for $1 \le \lambda \le L'$,*

$$f_\lambda(z_1,\dots,z_n) = z_1^{a_{\lambda 1}} \cdots z_n^{a_{\lambda n}} \varphi_\lambda(\ell_1 z_1 + \cdots + \ell_n z_n).$$

Further let $\zeta_1,\dots,\zeta_L$ be elements of $\mathbb{C}^n$. Furthermore, for $L'+1 \le \lambda \le L$ and $1 \le \mu \le L$ let $\delta_{\lambda\mu}$ be a complex number. For $1 \le \lambda \le L'$ and $1 \le \mu \le L$ we define $\delta_{\lambda\mu} = f_\lambda(\zeta_\mu)$. Finally, let $E > 1$ and $M_1,\dots,M_L$ be positive real numbers satisfying

$$M_\lambda \ge \log \sup_{|z|=E} \max_{1\le\mu\le L} |f_\lambda(z\zeta_\mu)|, \qquad 1 \le \lambda \le L',$$

$$M_\lambda \ge \log \max_{1\le\mu\le L} |\delta_{\lambda,\mu}| \qquad L'+1 \le \lambda \le L.$$

We consider the determinant

$$\Delta = \det\Big(\delta_{\lambda\mu}\Big)_{1\le\lambda,\mu\le L}.$$

Then we have

$$\log|\Delta| \le -\tilde{\Theta}_n(L_0, L')\log E + \log(L!) + M_1 + \cdots + M_L.$$

Proof. In the case $L' = L$, the result follows from lemmas 4.1 and 9.1. The general case involves the same arguments. For $1 \le \mu \le L$, we define functions $d_{1\mu}(z),\dots,d_{L\mu}(z)$ of a single variable $z \in \mathbb{C}$ by

$$d_{\lambda\mu}(z) = \begin{cases} f_\lambda(\zeta_\mu z) & \text{for } 1 \le \lambda \le L', \\ \delta_{\lambda\mu} & \text{for } L' < \lambda \le L. \end{cases}$$

This means that for $\lambda > L'$ the function $d_{\lambda\mu}$ is constant. We claim that the function

$$D(z) = \det\Big(d_{\lambda\mu}(z)\Big)_{1\le\lambda,\mu\le L}.$$

has a zero at the origin of multiplicity $\geq \Theta_n(L_0, L')$. To prove this claim, we may assume $\ell_2 = \cdots = \ell_n = 0$ and $\varphi_\lambda(z_1) = z_1^{b_\lambda}$ for some $b_\lambda \in \mathbb{N}$. In this case $f_\lambda(z_1, \ldots, z_n)$ is of the form $z_1^{\kappa_1} \cdots z_n^{\kappa_n}$ with $\kappa_{\lambda i} \in \mathbb{N}$ and $\kappa_{\lambda 2} + \cdots + \kappa_{\lambda n} \leq L_0$, $(1 \leq \lambda \leq L')$. Therefore either two of the functions f_λ are the same, and then $D(z) = 0$, or else D has a zero of multiplicity $\|\kappa_1\| + \cdots + \|\kappa_{L'}\|$ at the origin, where $\kappa_\lambda = (\kappa_{\lambda 1}, \ldots, \kappa_{\lambda n})$. This proves our claim.

We conclude the proof of lemma 9.4 by using Schwarz lemma like in the proof of lemma 4.1:

$$\log|\Delta| = \log|D(1)| \leq -\tilde{\Theta}_n(L_0, L')\log E + \log \sup_{|z|=E} |D(z)|;$$

for $|z| = E$, we plainly have

$$\log|D(z)| \leq \log(L!) + M_1 + \cdots + M_L.$$

□

Here is a consequence of lemmas 9.3 and 9.4, which will give a much better upper bound for the determinant Δ_r in the transcendence proof.

Proposition 9.5. — *Let $L_0 \geq 2$, $L_1 \geq 4n$ be integers and $E > 1$ be a real number. Define $L = \binom{L_0+n}{n}(L_1+1)$. Let $\varphi_1, \ldots, \varphi_{L_1}$ be analytic functions of one variable, let $\ell_1, \ldots, \ell_n$ be complex numbers, and, for $\underline{\lambda} = (\lambda_1, \ldots, \lambda_{n+1}) \in \mathbb{N}^{n+1}$ with $\lambda_1 + \cdots + \lambda_n \leq L_0$, $\lambda_{n+1} \leq L_1$, define*

$$f_{\underline{\lambda}}(z_1, \ldots, z_n) = z_1^{\lambda_1} \cdots z_n^{\lambda_n} \varphi_{\lambda_{n+1}}(\ell_1 z_1 + \cdots + \ell_n z_n).$$

For the same $\underline{\lambda}$, let $b_{\underline{\lambda}1}, \ldots, b_{\underline{\lambda}L}$ be complex numbers. Further, let $\zeta_1, \ldots, \zeta_L$ be elements in $\mathbb{C}^n$. Define

$$V = \frac{1}{48n}(L_0+1)(L_1+1)\log E.$$

Assume that, for each $\underline{\lambda}$ as above, we have a positive real number $M_{\underline{\lambda}}$ for which

$$M_{\underline{\lambda}} \geq \log \sup_{|z|=E} \max_{1\leq\mu\leq L} |f_{\underline{\lambda}}(z\zeta_\mu)|, \qquad M_{\underline{\lambda}} \geq \log \max_{1\leq\mu\leq L} |b_{\lambda,\mu}|$$

and

$$\log L + M_{\underline{\lambda}} \leq V$$

Finally, let ϵ be a complex number with

$$|\epsilon| \leq e^{-4V}.$$

Then the determinant

$$\Delta = \det\Big(f_{\underline{\lambda}}(\zeta_\mu) + \epsilon b_{\underline{\lambda}\mu}\Big)_{\underline{\lambda},\mu}$$

has absolute value bounded by

$$|\Delta| \leq 2^L e^{-LV}.$$

Proof. Consider the set of $\underline{\lambda} = (\lambda_1, \ldots, \lambda_{n+1}) \in \mathbb{N}^{n+1}$ satisfying $\lambda_1 + \cdots + \lambda_n \leq L_0$, $\lambda_{n+1} \leq L_1$. This set has L elements. For each subset I, we define $\Delta_I = \det\big(c^{(I)}_{\underline{\lambda}\mu}\big)_{\underline{\lambda},\mu}$ where

$$c^{(I)}_{\underline{\lambda}\mu} = \begin{cases} f_{\underline{\lambda}}(\zeta_\mu) & \text{for } \underline{\lambda} \in I, \\ b_{\underline{\lambda}\mu} & \text{for } \underline{\lambda} \notin I. \end{cases}$$

Define $L' = \lfloor L/2 \rfloor$. When $|I| \geq L'$, we use lemma 9.4:

$$\log|\Delta_I| \leq -\tilde{\Theta}_n(L_0, |I|)\log E + \log L! + \sum_{\underline{\lambda}} M_{\underline{\lambda}}.$$

The assumption $L_1 \geq 4n$ implies $|I| \geq L' \geq L/2 \geq 2n\binom{L_0+n}{n}$, hence by lemma 9.2 we have

$$\tilde{\Theta}_n(L_0, |I|) \geq \frac{|I|^2}{4\binom{L_0+n-1}{n-1}} \geq \frac{|I|}{8n}(L_0+1)(L_1+1),$$

because

$$|I| \geq \frac{1}{2}L \geq \frac{1}{2}\binom{L_0+n}{n}(L_1+1) \geq \frac{1}{2n}\binom{L_0+n-1}{n-1}(L_0+1)(L_1+1).$$

Therefore

$$\tilde{\Theta}_n(L_0, |I|)\log E \geq \frac{|I|}{8n}(L_0+1)(L_1+1)\log E \geq 6V|I|.$$

Hence, for $|I| \geq L'$, we have

$$\log|\Delta_I| \leq -4V|I|;$$

from the hypothesis $|\epsilon| \leq e^{-4V}$ we deduce

$$|\epsilon|^{L-|I|}|\Delta_I| \leq e^{-4(L-|I|)V}e^{-4|I|V} \leq e^{-4LV} \leq e^{-LV}.$$

For $|I| < L'$ we use the trivial estimate

$$\log|\Delta_I| \leq \log L! + \sum_{\underline{\lambda}} M_{\underline{\lambda}} \leq LV;$$

from the inequalities $L - |I| \geq L - L' + 1 \geq (L+1)/2$ we get

$$|\epsilon|^{L-|I|}|\Delta_I| \leq e^{-2LV}e^{LV} \leq e^{-LV}.$$

The number of subsets I is 2^L; the desired result follows now from lemma 9.3. □

1Exercise

1. With the notations of lemma 9.2, show that for each $\epsilon > 0$ there exists a number $c = c(n, \epsilon)$, which depends only on n and ϵ, such that, for $L \geq cL_0^n$ and $L_0 \geq c$,

$$\tilde{\Theta}_n(L_0, L) \geq \frac{\left(\frac{1}{2} - \epsilon\right)L^2}{\binom{L_0+n-1}{n-1}}.$$

1References

[L] M. Laurent. – Linear forms in two logarithms and interpolation determinants; this volume, Appendix.
[W] M. Waldschmidt. – Fonctions auxiliaires et fonctionnelles analytiques; J. Analyse Math., **56** (1991), 231–279.

10.– A REFINED MEASURE

In this Chapter, we prove the following result, which improves Theorem 7.1.

Theorem 10.1. — *Let $\ell_1, \dots, \ell_m$ be logarithms of algebraic numbers, $\alpha_i = \exp(\ell_i)$, $(1 \le i \le m)$, $\beta_1, \dots, \beta_m$ be algebraic numbers, D be the degree of the number field $\mathbb{Q}(\alpha_1, \dots, \alpha_m, \beta_1, \dots, \beta_m)$ over $\mathbb{Q}$ and let $A_1, \dots, A_m$ and B be real numbers, which are $\ge e$, and satisfy*

$$\log A_i \ge \mathrm{h}(\alpha_i), \quad D \log A_i \ge e|\ell_i|, \qquad (1 \le i \le m)$$

and

$$\log B \ge \mathrm{h}(1 : \beta_1 : \cdots : \beta_m), \qquad B \ge (50mD \log A)^{3m}$$

with $A = \max\{A_1, \dots, A_m\}$. If the number

$$\Lambda = \beta_1\ell_1 + \cdots + \beta_m\ell_m$$

does not vanish, then

$$|\Lambda| > \exp\{-(50m)^{3m} D^{m+2} (\log B)^2 \log A_1 \cdots \log A_m\}.$$

The main new point in the proof is an argument which enables us to avoid any assumption of linear dependence between the coefficients $\beta_1, \dots, \beta_m$. The proof given in Chapter 7 shows that if a linear form $\beta_1\ell_1 + \cdots + \beta_n\ell_n - \ell_{n+1}$ assumes a sufficiently small absolute value, then a certain matrix is not of maximal rank; we deduce from the zero estimate that there exists a vector subspace $\mathcal{V}$ of $\mathbb{C}^{n+1}$, of codimension $r \ge 1$, which contains the point $(\beta_1, \dots, \beta_n, -1)$, such that for some positive integer S the number of elements in $\big(\mathbb{Z}^{n+1}(S) + \mathcal{V}\big)/\mathcal{V}$ is relatively small; in particular we can make it smaller than $(2S-1)^{r+1}$. As we know from lemma 7.5, this implies that $1, \beta_1, \dots, \beta_n$ satisfy a linear dependence condition over $\mathbb{Q}$ with some explicit bound for the coefficients.

However this is not very efficient. It is much better to use directly the information on the upper bound for $\mathrm{Card}\big(\mathbb{Z}^{n+1}(S) + \mathcal{V}\big)/\mathcal{V}$. Instead of constructing a determinant with analytic functions in $\mathbb{C}^n$ (which we view as $\mathbb{C}^{n+1}/\mathbb{C}(\beta_1, \dots, \beta_n, -1)$), we take analytic functions in $\mathcal{V}/\mathbb{C}(\beta_1, \dots, \beta_n, -1)$, which involve only $d = n - r$ complex variables. This is explained in section 1.

The transcendence argument is given in section 2, where a more precise result than Theorem 10.1 is established. Finally in section 3 we deduce Theorem 10.1.

1 Construction of a non-zero determinant Let K be a field of zero characteristic, $\alpha_1, \dots, \alpha_{n+1}$ be non-zero elements of K, $\beta_1, \dots, \beta_n$ be elements of K, and L_0, L_1, $S_1, \dots, S_{n+1}$ be positive integers. Like in Chapter 3 (§6), we denote by $\mathbb{Z}^{n+1}(\underline{S})$ the set of $\underline{s} = (s_1, \dots, s_{n+1}) \in \mathbb{Z}^{n+1}$ which satisfy $|s_i| < S_i$, $(1 \le i \le n+1)$.

Let $\mathcal{V}$ be a vector subspace of K^{n+1} which contains the point $(\beta_1, \dots, \beta_n, -1)$. We denote by $d+1$ the dimension of $\mathcal{V}$, by $\sigma_{\mathcal{V}}$ the canonical map from K^{n+1} onto $K^{n+1}/\mathcal{V}$, by $(e_1, \dots, e_{n+1})$ the canonical basis of K^{n+1}, and we assume that $\sigma_{\mathcal{V}}(e_1), \dots, \sigma_{\mathcal{V}}(e_{n-d})$ is a basis of $K^{n+1}/\mathcal{V}$. This means that if $z = (z_1, \dots, z_{n+1}) \in \mathcal{V}$ satisfies $z_{n-d+1} = \cdots = z_{n+1} = 0$, then $z = 0$.

We consider the following matrix

$$\mathcal{M}_{\dashv_\nabla} = \Bigg(\prod_{j=n-d+1}^{n} \big(s_j + s_{n+1}\beta_j\big)^{\lambda_j} \prod_{i=1}^{n+1} \alpha_i^{s_i\lambda_{n+1}} \Bigg)_{\underline{\lambda}, \underline{s}},$$

where the index of rows is $\underline{\lambda} = (\lambda_{n-d+1}, \dots, \lambda_{n+1}) \in \mathbb{N}^{d+1}$ with $\lambda_{n-d+1} + \cdots + \lambda_n \le L_0$ and $\lambda_{n+1} \le L_1$, while the index of columns is $\underline{s} \in \mathcal{V} \cap \mathbb{Z}^{n+1}(\underline{S})$. The number of rows is $L^{(d)} = \binom{L_0+d}{d}(L_1+1)$.

We show that the zero estimate of Chapter 8 gives the following result:

Proposition 10.2. – *Assume that each S_i is a multiple of $2(n+1)$, and define $S_i' = S_i/2(n+1)$. Assume also that the parameters L_0, L_1 and $S_1', \dots, S_{n+1}'$ satisfy*

$$2^n S_1' \cdots S_{n+1}' \geq (n+1) L_0^n L_1 \qquad \text{and} \qquad S_i' \geq n+1, \qquad L_0 \geq 4S_i', \qquad (1 \leq i \leq n+1).$$

Assume further that for all $s \in \mathbb{Z}$ with $0 < s < 4S_{n+1}' - 3$, we have $(s\beta_1, \dots, s\beta_n, -s) \notin \mathbb{Z}^{n+1}(4\underline{S}' - 3)$. Finally, assume that

$$\mathrm{Card}\Big(\big(\mathbb{Z}^{n+1}(\underline{S}') + \mathcal{V}\big)/\mathcal{V}\Big) \leq \frac{n+1}{d+1} L_0^{n-d},$$

and that there is no subspace of smaller dimension satisfying this inequality. Then the matrix $\mathcal{M}_{\dashv\nabla}$ is of rank $L^{(d)}$.

The proof of this Proposition requires some preparation.

Lemma 10.3. – *Let $\mathcal{C}$ be a finite set and $f : \mathcal{C} \longrightarrow \mathcal{C}'$ be a mapping. Then*

$$\mathrm{Card}\mathcal{C} = \sum_{u \in f(\mathcal{C})} \mathrm{Card} f^{-1}(u).$$

Proof. The map f induces on $\mathcal{C}$ an equivalence relation with Card $f(\mathcal{C})$ classes, namely

$$\big\{ f^{-1}(u)\,;\, u \in f(\mathcal{C}) \big\}.$$

□

From lemma 10.3 one deduces

$$\mathrm{Card} f(\mathcal{C}) \min_{u \in f(\mathcal{C})} \mathrm{Card} f^{-1}(u) \leq \mathrm{Card}\mathcal{C} \leq \mathrm{Card} f(\mathcal{C}) \max_{u \in f(\mathcal{C})} \mathrm{Card} f^{-1}(u).$$

The lower bound was already used in the proof of lemma 7.5. We consider here the upper bound. When $\psi : G_1 \longrightarrow G_2$ is a homomorphism of $\mathbb{Z}$-modules and $\mathcal{C}$ a finite subset of G_1, if we define $\underline{\mathcal{C}} = \big\{ \underline{\lambda} - \underline{\lambda}'\,;\, \lambda \in \mathcal{C},\, \lambda' \in \mathcal{C} \big\}$, then

$$\mathrm{Card}\ \psi(\mathcal{C}) \cdot \mathrm{Card}\big(\underline{\mathcal{C}} \cap \ker \psi\big) \geq \mathrm{Card}\ \mathcal{C}.$$

Indeed, one applies lemma 10.3 to the restriction $f : \mathcal{C} \longrightarrow \psi(\mathcal{C})$ of ψ to $\mathcal{C}$; if $\lambda^{(1)}, \dots, \lambda^{(t)}$ are distinct elements in the same class $f^{-1}(u)$, then $0, \lambda^{(2)} - \lambda^{(1)}, \dots, \lambda^{(t)} - \lambda^{(1)}$ are distinct elements in $\underline{\mathcal{C}} \cap \ker \psi$.

For instance take $G_1 = \mathbb{Z}^{n+1}$, $\mathcal{C} = \mathbb{Z}^{n+1}(\underline{S}')$, and ψ is the restriction to $\mathbb{Z}^{n+1}$ of the canonical map $\mathbb{C}^{n+1} \longrightarrow \mathbb{C}^{n+1}/\mathcal{V}$; since $\underline{\mathcal{C}}$ is contained in $\mathbb{Z}^{n+1}(2\underline{S}' - 1)$, we deduce

$$\mathrm{Card}\Big(\big(\mathbb{Z}^{n+1}(\underline{S}') + \mathcal{V}\big)/\mathcal{V}\Big)\mathrm{Card}\big(\mathcal{V} \cap \mathbb{Z}^{n+1}(2\underline{S}' - 1)\big) \geq (2S_1' - 1) \cdots (2S_{n+1}' - 1).$$

Here is another simple consequence of lemma 10.3.

Lemma 10.4. – *Let G be a subgroup of $\mathbb{Z}^{n+1}$; for positive integers $S_1, \dots, S_{n+1}$, define*

$$G(\underline{S}) = G \cap \mathbb{Z}^{n+1}(\underline{S}).$$

Let $\alpha_1, \dots, \alpha_{n+1}$ be elements in K^* which generate a multiplicative subgroup of rank $\geq n$. Then the number of elements in the image in K^*/K^*_{tors} of the set

$$\big\{ \alpha_1^{s_1} \cdots \alpha_{n+1}^{s_{n+1}}\,;\, \underline{s} \in G(\underline{S}) \big\}$$

is at least

$$\frac{\big(\mathrm{Card}\ G(\underline{S})\big)}{2 \max_{1 \leq i \leq n+1} S_i}.$$

Proof. If $\alpha_1,\dots,\alpha_{n+1}$ are multiplicatively independent, then the number of elements in this image is just Card $G(\underline{S})$. Otherwise the map

$$\begin{array}{rccc}\psi: & \mathbb{Z}^{n+1} & \longrightarrow & K^*/K^*_{\rm tors}\\ & (s_1,\dots,s_{n+1}) & \longmapsto & \alpha_1^{s_1}\cdots\alpha_{n+1}^{s_{n+1}}\end{array}$$

has a kernel which is a subgroup of $\mathbb{Z}^{n+1}$ of rank 1; this kernel is of the form $\mathbb{Z}\underline{a}$ with $\underline{a}=(a_1,\dots,a_{n+1})\in\mathbb{Z}^{n+1}$; we apply lemma 10.3 with $\mathcal{C}=G(\underline{S})$, $\mathcal{C}'=K^*/K^*_{\rm tors}$, and f is the restriction of ψ to $\mathcal{C}$. Let $u=f(\underline{s}^0)\in f(\mathcal{C})$ be such that Card$f^{-1}(u)$ is maximal :

$$\text{Card}\mathcal{C}\le\text{Card}f(\mathcal{C})\text{Card}f^{-1}(u).$$

For each $\underline{s}\in f^{-1}(u)$, there exists $\lambda_{\underline{s}}\in\mathbb{Z}$ with $\underline{s}-\underline{s}^0=\lambda_{\underline{s}}\underline{a}$. Let $i\in\{1,\dots,n+1\}$ be such that $a_i\neq 0$; then all the $\lambda_{\underline{s}}=(s_i-s_i^0)/a_i$ belong to an interval of length $\le(2S_i-2)/|a_i|\le 2S_i-2$, and therefore Card$f^{-1}(u)\le 2S_i-1<2S_i$. □

Proof of Proposition 10.2. Assume that the rank of $\mathcal{M}_{\dashv\nabla}$ is less than $L^{(d)}$: there exists a non-zero polynomial in $K[X_{n-d+1},\dots,X_n,Y]$, of total degree $\le L_0$ in $X_{n-d+1},\dots,X_n$ and of degree $\le L_1$ in Y which vanishes on the set $\Sigma[d+1]$, where

$$\Sigma=\big\{(s_{n-d+1}+s_{n+1}\beta_{n-d+1},\dots,s_n+s_{n+1}\beta_n,\alpha_1^{s_1}\cdots\alpha_{n+1}^{s_{n+1}})\,;\,\underline{s}\in\mathcal{V}\cap\mathbb{Z}^{n+1}(2\underline{S}'-1)\big\}.$$

We use Proposition 8.1 with d_0 replaced by d, $d_1=1$ and $D_0=L_0$, $D_1=L_1$. We deduce the existence of a vector subspace $\mathcal{W}_1$ of K^d, of dimension δ and of a subgroup Φ of $\mathbb{Z}$ such that $\mathcal{W}_1\times T_\Phi\neq K^d\times K^*$ and either

$$(\delta+1)\text{Card}\Big(\big(\Sigma+(\mathcal{W}_1\times K^*)\big)/(\mathcal{W}_1\times K^*)\Big)\le(d+1)L_0^{d-\delta}\qquad\text{and}\qquad\Phi=0$$

or

$$\text{Card}\Big(\big(\Sigma+(\mathcal{W}_1\times T_\Phi)\big)/(\mathcal{W}_1\times T_\Phi)\Big)\le(d+1)L_0^{d-\delta}L_1\qquad\text{and}\qquad\Phi\neq 0.$$

We are going to prove firstly $\mathcal{W}_1\neq 0$, secondly $\Phi=0$.

We claim that the elements

$$\big\{(s_{n-d+1}+s_{n+1}\beta_{n-d+1},\dots,s_n+s_{n+1}\beta_n)\,;\,\underline{s}\in\mathcal{V}\cap\mathbb{Z}^{n+1}(2\underline{S}'-1)\big\}$$

are pairwise distinct. Indeed, if this is not true, then there exists $\underline{s}\in\mathcal{V}\cap\mathbb{Z}^{n+1}(4\underline{S}'-3)$ with $\underline{s}\neq 0$, $s_{n+1}\ge 0$ and

$$s_i+s_{n+1}\beta_i=0\qquad\text{for}\qquad n-d+1\le i\le n.$$

Therefore the point

$$(s_1,\dots,s_{n+1})+(s_{n+1}\beta_1,\dots,s_{n+1}\beta_n,-s_{n+1})$$

belongs to $\mathcal{V}$ and has its $d+1$ last components which vanish; hence the first $n-d$ components also vanish, and $(s_{n+1}\beta_1,\dots,s_{n+1}\beta_n,-s_{n+1})\in\mathcal{V}\cap\mathbb{Z}^{n+1}(4\underline{S}'-3)$, contrary to our assumption. This proves our claim.

From this claim we deduce, for any subgroup Φ of $\mathbb{Z}$ (including $\Phi=0$)

$$\text{Card}\Big(\big(\Sigma+(0\times T_\Phi)\big)/(0\times T_\Phi)\Big)=\text{Card}\big(\mathcal{V}\cap\mathbb{Z}^{n+1}(2\underline{S}'-1)\big).$$

The assumption $S_i'\ge n+1$ is used for the bound

$$\Big(1-\frac{1}{2S_1'}\Big)\cdots\Big(1-\frac{1}{2S_{n+1}'}\Big)\ge\Big(1-\frac{1}{2(n+1)}\Big)^{n+1}>\frac{1}{2},$$

which enables us to deduce from lemma 10.3

$$\text{Card}\Big(\big(\mathbb{Z}^{n+1}(\underline{S}')+\mathcal{V}\big)/\mathcal{V}\Big)\text{Card}\big(\mathcal{V}\cap\mathbb{Z}^{n+1}(2\underline{S}'-1)\big)>2^nS_1'\cdots S_{n+1}'.$$

From our choice of $\mathcal{V}$ and our hypothesis on $S'_1 \cdots S'_{n+1}$, we deduce

$$\frac{n+1}{d+1} L_0^{n-d} \mathrm{Card}\big(\mathcal{V} \cap \mathbb{Z}^{n+1}(2\underline{S}' - 1)\big) > 2^n S'_1 \cdots S'_{n+1} \geq (n+1) L_0^n L_1,$$

hence

$$\mathrm{Card}\big(\mathcal{V} \cap \mathbb{Z}^{n+1}(2\underline{S}' - 1)\big) > (d+1) L_0^d L_1.$$

Combining this with the previous inequality, we deduce

$$\mathrm{Card}\Big(\big(\Sigma + (0 \times T_\Phi)\big)/(0 \times T_\Phi)\Big) > (d+1) L_0^d L_1$$

which implies $\mathcal{W}_1 \neq 0$.

Assume now $\Phi \neq 0$; then T_Φ is a finite group, hence is contained in K^*_{tors}, and, according to lemma 10.4, the number of distinct points in

$$\big\{\alpha_1^{s_1} \cdots \alpha_{n+1}^{s_{n+1}} \, ; \, \underline{s} \in \mathcal{V} \cap \mathbb{Z}^{n+1}(2\underline{S}' - 1)\big\}$$

modulo torsion is at least $(4 \max\{S'_i\})^{-1} \mathrm{Card}\big(\mathcal{V} \cap \mathbb{Z}^{n+1}(2\underline{S}' - 1)\big)$. The hypothesis $L_0 \geq 4S'_i$ together with the previous lower bound, shows that this number is greater than

$$(d+1) L_0^{d-1} L_1.$$

We deduce that the number of elements in $\big(\Sigma + (\mathcal{W}_1 \times T_\Phi)\big)/(\mathcal{W}_1 \times T_\Phi)$ is greater than $(d+1)L_0^{d-1}L_1$; since we already know that δ is at least 1, we get a contradiction. From the condition $\mathcal{W}_1 \times T_\Phi \neq K^d \times K^*$ we conclude $\Phi = 0$ and $\delta < d$.

Let $\theta : \mathcal{V} \to K^d$ be the linear map which sends $(z_1, \ldots, z_{n+1})$ onto the point $(z_{n-d+1} + z_{n+1}\beta_{n-d+1}, \ldots, z_n + z_{n+1}\beta_n)$. Using once more the assumption that $e_1, \ldots, e_{n-d}$ are linearly independent modulo $\mathcal{V}$, we deduce that θ is surjective with kernel $K(\beta_1, \ldots, \beta_n, -1)$. We define $\mathcal{W} = \theta^{-1}(\mathcal{W}_1)$. Hence $\mathcal{W}$ is a vector subspace of $\mathcal{V}$, of dimension $\delta + 1 < d + 1$, containing $(\beta_1, \ldots, \beta_n, -1)$, such that

$$\mathrm{Card}\Big(\Big(\big(\mathcal{V} \cap \mathbb{Z}^{n+1}(2\underline{S}' - 1)\big) + \mathcal{W}\Big)/\mathcal{W}\Big) \leq \frac{d+1}{\delta+1} L_0^{d-\delta}.$$

We apply lemma 10.3 to the canonical map

$$\psi : K^{n+1}/\mathcal{W} \longrightarrow K^{n+1}/\mathcal{V}$$

with

$$\mathcal{C} = \sigma_{\mathcal{W}}\big(\mathbb{Z}^{n+1}(\underline{S}')\big) = \big(\mathbb{Z}^{n+1}(\underline{S}') + \mathcal{W}\big)/\mathcal{W},$$
$$\psi(\mathcal{C}) = \sigma_{\mathcal{V}}\big(\mathbb{Z}^{n+1}(\underline{S}')\big) = \big(\mathbb{Z}^{n+1}(\underline{S}') + \mathcal{V}\big)/\mathcal{V}$$

and

$$\underline{\mathcal{C}} \cap \ker\psi = \sigma_{\mathcal{W}}\big(\mathbb{Z}^{n+1}(2\underline{S}' - 1)\big) \cap \ker\psi = \big(\mathcal{V} \cap \mathbb{Z}^{n+1}(2\underline{S}' - 1) + \mathcal{W}\big)/\mathcal{W}$$

We get

$$\begin{aligned}
&\mathrm{Card}\Big(\big(\mathbb{Z}^{n+1}(\underline{S}') + \mathcal{W}\big)/\mathcal{W}\Big) \\
&\qquad \leq \mathrm{Card}\Big(\big(\mathbb{Z}^{n+1}(\underline{S}') + \mathcal{V}\big)/\mathcal{V}\Big) \cdot \mathrm{Card}\Big(\big(\mathcal{V} \cap \mathbb{Z}^{n+1}(2\underline{S}' - 1) + \mathcal{W}\big)/\mathcal{W}\Big) \\
&\qquad \leq \frac{d+1}{\delta+1} L_0^{d-\delta} \cdot \frac{n+1}{d+1} L_0^{n-d} \\
&\qquad \leq \frac{n+1}{\delta+1} L_0^{n-\delta}.
\end{aligned}$$

Since $\dim \mathcal{W} = \delta + 1 < d + 1$, this contradicts the minimality of $\dim \mathcal{V}$. □

1 The main proof In this section we prove the following result.

Theorem 10.5. — *Let $\ell_1, \dots, \ell_{n+1}$ be logarithms of algebraic numbers $\alpha_i = \exp(\ell_i)$, $(1 \le i \le n+1)$ and $\beta_1, \dots, \beta_n$ be algebraic numbers with $\max\{|\beta_1|, \dots, |\beta_n|\} \le 1$. Assume that the numbers $\ell_1, \dots, \ell_{n+1}$ are $\mathbb{Q}$-linearly independent. Let D be the degree of the number field $\mathbb{Q}(\alpha_1, \dots, \alpha_{n+1}, \beta_1, \dots, \beta_n)$ over $\mathbb{Q}$ and let $A_1, \dots, A_{n+1}$, B and E be real numbers, which are $\ge e$, and satisfy*

$$\mathrm{h}(\alpha_i) \le \log A_i, \qquad E|\ell_i| \le D \log A_i, \qquad (1 \le i \le n+1)$$

and

$$\mathrm{h}(\beta_1 : \cdots : \beta_n : 1) \le \log B, \qquad E \le B^D.$$

Assume that there exist $n+3$ positive rational integers L_0, L_1 and $S'_1, \dots, S'_{n+1}$ satisfying the following conditions:

$$L_0 \ge 4S'_i, \qquad S'_i \ge n+1$$

and

$$2^n S'_1 \cdots S'_{n+1} \ge (n+1) L_0^n L_1. \tag{10.6}$$

Define

$$V = \frac{1}{48n}(L_0+1)(L_1+1)\log E,$$

and assume

$$V \ge DL_0 \log(2BS) + DL_1 \sum_{i=1}^{n+1} S_i \log A_i + D \log L + \log\bigl(2L_1 S_{n+1}\bigr), \tag{10.7}$$

where $L := \binom{L_0+n}{n}(L_1+1)$, $S_i = 2(n+1)S'_i$ and $S = \max_{1 \le i \le n+1} S_i$. If

$$\Lambda = \beta_1\ell_1 + \cdots + \beta_n\ell_n - \ell_{n+1}$$

does not vanish, then we have $|\Lambda| > e^{-4nV}$.

Proof.

Step one: Liouville inequality

We begin with an easy case, when there exists a rational integer $s \in \mathbb{Z}$ with $0 < s < 4S'_{n+1} - 3$ such that

$$(s\beta_1, \dots, s\beta_n, -s) \in \mathbb{Z}^{n+1}(4\underline{S}' - 3).$$

In this case we write $b_i = s\beta_i$, $(1 \le i \le n)$ and $b_{n+1} = -s$; hence $s\Lambda = b_1\ell_1 + \cdots + b_{n+1}\ell_{n+1}$ and $b_i \in \mathbb{Z}$ with $|b_i| \le 4S'_i - 4$. We use Liouville's estimate (exercise 6b of Chapter 3):

$$s|\Lambda| \ge 2^{-D} \exp\left\{-2D \sum_{i=1}^{n+1} (2S'_i - 2)\mathrm{h}(\alpha_i)\right\}.$$

This gives the desired bound:

$$\begin{aligned} \log|\Lambda| &\ge -D\log 2 - 4D \sum_{i=1}^{n+1} S'_i \log A_i - \log(4S'_{n+1}) \\ &\ge -4nV. \end{aligned}$$

Therefore we shall now assume

$$(s\beta_1, \dots, s\beta_n, -s) \notin \mathbb{Z}^{n+1}(4\underline{S}' - 3)$$

for $0 < s < 4S'_{n+1} - 3$.

Step two: Choice of $\mathcal{V}$

We remark that there exist vector subspaces $\mathcal{V}$ of $\mathbb{C}^{n+1}$, containing $(\beta_1,\dots,\beta_n,-1)$, such that

$$\mathrm{Card}\Big(\big(\mathbb{Z}^{n+1}(\underline{S}')+\mathcal{V}\big)/\mathcal{V}\Big) \le \frac{n+1}{d+1}L_0^{n-d}$$

with $d=\dim\mathcal{V}-1$; indeed $\mathcal{V}=\mathbb{C}^{n+1}$ is such a space. Among them, we choose one (which we call $\mathcal{V}$) which is of minimal dimension $d+1$.

Let $\sigma_{\mathcal{V}}$ be the canonical map from $\mathbb{C}^{n+1}$ onto $\mathbb{C}^{n+1}/\mathcal{V}$. Since $\mathcal{V}\ni(\beta_1,\dots,\beta_n,-1)$, we have

$$\sigma_{\mathcal{V}}(e_{n+1}) = \beta_1\sigma_{\mathcal{V}}(e_1)+\cdots+\beta_n\sigma_{\mathcal{V}}(e_n),$$

hence there exists a basis of $\mathbb{C}^{n+1}/\mathcal{V}$ of the form $\big(\sigma_{\mathcal{V}}(e_{i_1}),\dots,\sigma_{\mathcal{V}}(e_{i_{n-d}})\big)$, with $1\le i_1<\cdots<i_{n-d}\le n$. For ease of notation we shall assume that $\{i_1,\dots,i_{n-d}\}=\{1,\dots,n-d\}$. Writing $\sigma_{\mathcal{V}}(e_i)$ in terms of $\sigma_{\mathcal{V}}(e_1),\dots,\sigma_{\mathcal{V}}(e_{n-d})$, we see that there exist $(n-d)(d+1)$ complex numbers $u_i^{(j)}$ such that

$$e_i+\sum_{j=1}^{n-d}u_i^{(j)}e_j\in\mathcal{V},\qquad (n-d+1\le i\le n+1);$$

these $d+1$ elements, which can be written

$$\big(u_i^{(1)},\dots,u_i^{(n-d)},0,\dots,0,1,0,\dots,0\big),\qquad (n-d+1\le i\le n+1)$$

form a basis of $\mathcal{V}$; from this one deduces that $\mathcal{V}$ is intersection of $n-d$ hyperplanes

$$z_j=\sum_{i=n-d+1}^{n+1}u_i^{(j)}z_i\qquad (1\le j\le n-d).$$

We define

$$\vartheta_i=\ell_i+\sum_{j=1}^{n-d}u_i^{(j)}\ell_j,\qquad (n-d+1\le i\le n+1).$$

Then, for $z\in\mathcal{V}$, we have

$$\sum_{i=n-d+1}^{n+1}z_i\vartheta_i=\sum_{j=1}^{n+1}z_j\ell_j.$$

In particular, since $(\beta_1,\dots,\beta_n,-1)$ is in $\mathcal{V}$,

$$\sum_{i=n-d+1}^{n}\beta_i\vartheta_i=\vartheta_{n+1}+\Lambda.$$

Step three: Lower bound for $|\Delta_r|$

Thanks to Proposition 10.2, we know that the matrix $\mathcal{M}_{\dashv\nabla}$ is of rank $L^{(d)}=\binom{L_0+d}{d}(L_1+1)$. Therefore there exist $L^{(d)}$ elements $\underline{s}^{(1)},\dots,\underline{s}^{(L^{(d)})}$ in $\mathcal{V}\cap\mathbb{Z}^{n+1}(\underline{S})$ such that, if we define

$$a_{\underline{\lambda}}^{(\mu)}=\prod_{j=n-d+1}^{n}\big(s_j^{(\mu)}+s_{n+1}^{(\mu)}\beta_j\big)^{\lambda_j}\prod_{i=1}^{n+1}\alpha_i^{s_i^{(\mu)}\lambda_{n+1}},\qquad \big((1\le\mu\le L^{(d)}\big),$$

then the $L^{(d)}\times L^{(d)}$ determinant

$$\Delta_r=\det\Big(a_{\underline{\lambda}}^{(\mu)}\Big)_{\underline{\lambda},\mu}$$

does not vanish. Of course, $\underline{\lambda}$ runs over the elements $(\lambda_{n-d+1},\dots,\lambda_{n+1})$ as in §1 above, while μ runs over $\{1,\dots,L^{(d)}\}$.

We use again Liouville's inequality, like in step one of the proof of Proposition 7.7 : we deduce from Proposition 3.15

$$\frac{1}{L^{(d)}}\log|\Delta_r|\ge -U_1$$

with

$$U_1=(D-1)\big(L_0\log(2S)+\log L^{(d)}\big)+DL_0\log B+DL_1\sum_{i=1}^{n+1}S_i\log A_i.$$

Step four: Conclusion of the proof

For each $\underline{\lambda}$ as before, we define a function $f_{\underline{\lambda}}$ of d complex variables:

$$f_{\underline{\lambda}}(z_{n-d+1},\dots,z_n)=\prod_{i=n-d+1}^{n}\left(z_i^{\lambda_i}e^{\lambda_{n+1}\vartheta_i z_i}\right).$$

For $\underline{s}\in\mathcal{V}\cap\mathbb{Z}^{n+1}$, if we set

$$(z_{n-d+1},\dots,z_n)=\big(s^{(\mu)}_{n-d+1}+s^{(\mu)}_{n+1}\beta_{n-d+1},\dots,s^{(\mu)}_{n}+s^{(\mu)}_{n+1}\beta_n\big),$$

we have

$$\sum_{i=n-d+1}^{n}\vartheta_i z_i=\sum_{j=1}^{n+1}s^{(\mu)}_j\ell_j+s^{(\mu)}_{n+1}\Lambda.$$

Therefore the corresponding value of $f_{\underline{\lambda}}$ is

$$f_{\underline{\lambda}}(z_{n-d+1},\dots,z_n)=a^{(\mu)}_{\underline{\lambda}}e^{\lambda_{n+1}s^{(\mu)}_{n+1}\Lambda}.$$

We define $\zeta_1,\dots,\zeta_{L^{(d)}}$ in $\mathbb{C}^d$ by

$$\zeta_\mu=\big(s^{(\mu)}_{n-d+1}+s^{(\mu)}_{n+1}\beta_{n-d+1},\dots,s^{(\mu)}_{n}+s^{(\mu)}_{n+1}\beta_n\big),\qquad(1\le\mu\le L^{(d)}),$$

and we consider the interpolation determinant in d variables:

$$\mathcal{M}_{\dashv\backslash}=\Big(f_{\underline{\lambda}}(\zeta_\mu)\Big)_{\underline{\lambda},\mu}$$

(with the same indices as Δ_r for rows and columns). We shall use Proposition 9.5 with $\epsilon=\Lambda$ and

$$b_{\underline{\lambda},\mu}=a^{(\mu)}_{\underline{\lambda}}\Big(1-e^{\lambda_{n+1}\Lambda s^{(\mu)}_{n+1}}\Big)\Lambda^{-1}.$$

Let us check that the hypotheses of Proposition 9.5 hold with

$$M_{\underline{\lambda}}=L_0\log(2ES)+DL_1\sum_{i=1}^{n+1}S_i\log A_i+\log\big(2L_1S_{n+1}\big).$$

We first remark that there is no loss of generality to assume $|\Lambda|L_1S_{n+1}E<1$. Now on one hand, for $z\in\mathbb{C}$ with $|z|\le E$, we have

$$\log|f_{\underline{\lambda}}(z\zeta_\mu)|\le L_0\log(2ES)+L_1E\left(\sum_{i=1}^{n+1}S_i|\ell_i|+S_{n+1}|\Lambda|\right).$$

On the other hand, we have (using the estimate in exercise 1a of Chapter 1, with $\delta=1$)

$$|b_{\underline{\lambda},\mu}|\le 2\big|a^{(\mu)}_{\underline{\lambda}}\lambda_{n+1}s^{(\mu)}_{n+1}\big|;$$

since $\big|\log|\alpha_i|\big|\le D\log A_i$, we obtain

$$\log|b_{\underline{\lambda},\mu}|\le L_0\log(2S)+DL_1\sum_{i=1}^{n+1}S_i\log A_i+\log(2L_1S_{n+1}).$$

Define $V_d = (1/48d)(L_0+1)(L_1+1)\log E$; we obviously have, thanks to (10.7),

$$\log L^{(d)} + M_{\underline{\lambda}} \le V_d$$

(because $V_d \ge V = V_n$); using again (10.7), we obtain $U_1 + \log 2 < V_d$, which shows that the conclusion of Proposition 9.5 is not satisfied; therefore

$$|\Lambda| \ge e^{-4V_d} \ge e^{-4nV}.$$

This completes the proof of Theorem 10.5. □

1Proof of Theorem 10.1 There is no loss of generality to assume that the m numbers $\ell_1, \dots, \ell_m$ are $\mathbb{Q}$-linearly independent (see exercise 1).

Under the assumptions of Theorem 10.1, we shall prove the estimate

$$|\Lambda| > \exp\{-\big(50(m-1)\big)^{3m} D^{m+2} (\log B)^2 \log A_1 \cdots \log A_m\}$$

in the special case where $\beta_m = -1$ and $|\beta_i| \le 1$ for $1 \le i \le m-1$; the general case follows easily from Liouville's inequality (cf. part a in the proof of Proposition 7.10).

We write $n = m-1$ and

$$\Lambda = \beta_1\ell_1 + \cdots + \beta_n\ell_n - \ell_{n+1}.$$

We define a real number U by

$$U = (1/5n)(50n)^{3n+3} D^{n+3} (\log B)^2 \log A_1 \cdots \log A_{n+1}$$

and rational integers L_0, L_1, $S'_1, \dots, S'_{n+1}$ by

$$L_0 = \left[\frac{U}{5D\log B}\right], \qquad L_1 = \big[240nD\log B\big],$$

$$S'_i = \left[\frac{U}{4(n+1)^2 D L_1 \log A_i}\right] \qquad (1 \le i \le n+1).$$

Next we define a real number V and rational integers $S_1, \dots, S_{n+1}$ by

$$V = \frac{1}{48n}(L_0+1)(L_1+1), \qquad S_i = 2(n+1)S'_i, \quad (1 \le i \le n+1).$$

It is easy to check that $V > U$. We shall use Theorem 10.5 with $E = e$.

Our assumption $B \ge (50mD\log A)^{3m}$ enables us to check:

$$B \ge \frac{2}{n+1}(50n)^{3n+1} D^{n+1} (\log A)^n \log B,$$

which implies $B > 2S$, where $S = \max\{S_1, \dots, S_{n+1}\}$. We now use the bounds

$$DL_0 \log(2BS) \le \frac{2}{5}U, \qquad DL_1 \sum_{i=1}^{n+1} S_i \log A_i \le \frac{1}{2}U, \qquad D\log L + \log\big(2L_1 S_{n+1}\big) < \frac{1}{10}U,$$

from which we deduce (10.7). The main condition is (10.6); we use the lower bound (where the coefficient $1/2$ takes care of the integral parts)

$$2^n S'_1 \cdots S'_{n+1} > \frac{U^{n+1}}{2^{n+3}(n+1)^{2n+2} D^{n+1} L_1^{n+1} \log A_1 \cdots \log A_{n+1}}$$

and the upper bound

$$(n+1)L_0^n L_1 \le \frac{(n+1)U^n L_1}{5^n D^n (\log B)^n}.$$

Therefore it is sufficient to check

$$U \ge 2^{n+3}5^{-n}(n+1)^{2n+3}DL_1^{n+2}(\log B)^{-n}\log A_1 \cdots \log A_{n+1}.$$

The constant 50 in the final estimate has been chosen because for $n \ge 1$,

$$5n2^{n+3}5^{-n}(n+1)^{2n+3}(240n)^{n+2} < (50n)^{3n+3}.$$

This proves (10.6). Theorem 10.1 is then a consequence of the estimate

$$4nV < (50n)^{3n+3}D^{n+3}(\log B)^2 \log A_1 \cdots \log A_{n+1}.$$

□

1Exercises **1.** Let K be a field, m a positive integer, and $\mathcal{V}$ a vector subspace of K^m of dimension d. The following properties are equivalent:
(*i*) If $\sigma_{\mathcal{V}} : K^m \longrightarrow K^m/\mathcal{V}$ is the canonical projection, then $\big(\sigma_{\mathcal{V}}(e_1), \dots, \sigma_{\mathcal{V}}(e_{m-d})\big)$ is a basis of $K^m/\mathcal{V}$;
(*ii*) for $z = (z_1, \dots, z_m) \in \mathcal{V}$, the conditions $z_{m-d+1} = \cdots = z_m = 0$ imply $z = 0$;
(*iii*) the restriction to $\mathcal{V}$ of the projection $K^m \longrightarrow K^d$ on the last d coordinates is injective;
(*iv*) $\mathcal{V}$ is intersection of $m-d$ hyperplanes of equations

$$z_j = \sum_{i=m-d+1}^{m} a_{ij} z_i, \qquad (1 \le j \le m-d).$$

`Hint.` *Compare with part* b *in the proof of lemma* 5.7 *and with step* 2 *in the proof of Theorem* 10.5.

2. Let K be a field of characteristic zero, m and S positive integers, and $\mathcal{V}$ a vector subspace of K^m.
a) Show that there exists $x \in \mathbb{Z}^m(S)$ such that

$$\mathrm{Card}\Big(\big(\mathbb{Z}^m(S)+\mathcal{V}\big)/\mathcal{V}\Big)\mathrm{Card}\big((x+\mathcal{V})\cap\mathbb{Z}^m(S)\big) \ge (2S-1)^m.$$

`Hint.` *Use lemma* 10.3.
b) Let $\mathcal{W}$ be a vector subspace of K^m of dimension d. Check the inequality

$$\mathrm{Card}\big((x+\mathcal{W})\cap\mathbb{Z}^m(S)\big) \le (2S-1)^d$$

for each $x \in K^m$.
`Hint.` *Show first that there is no loss of generality to assume* $x \in \mathbb{Z}^m$. *After a permutation of coordinates, one may also assume that the projection* $K^m \longrightarrow K^d$ *on the first* d *coordinates maps* $\mathcal{W}$ *isomorphically onto* K^d. *Then the image of* $(x+\mathcal{W})\cap\mathbb{Z}^m(S)$ *under this projection has at most* $(2S-1)^d$ *elements.*
c) Assume

$$\mathrm{Card}\Big(\big(\mathbb{Z}^m(S)+\mathcal{V}\big)/\mathcal{V}\Big) < (2S-1)^{r+1}$$

where $r \ge 1$ is the codimension of $\mathcal{V}$. Show that $\mathcal{V}\cap\mathbb{Z}^m(2S-1)$ contains more than $(2S-1)^{m-r-1}$ points, and that these points span $\mathcal{V}$ as a vector space.

3. Show that for the proof of Theorem 10.1, there is no loss of generality to assume that the m numbers $\ell_1, \dots, \ell_m$ are $\mathbb{Q}$-linearly independent.
`Hint.` *Use either lemma* 7.2 *or lemma* 7.3.

4. Reduce the constant 50 which occurs in the lower bound for $|\Lambda|$ in Theorem 10.1.

11.– NON HOMOGENEOUS LINEAR RELATIONS

A generalization of Theorem 1.1, once more due to A. Baker, is the following:

Theorem 11.1. – *Let $\ell_1, \dots, \ell_m$ be $\mathbb{Q}$-linearly independent logarithms of algebraic numbers. Then the numbers $1, \ell_1, \dots, \ell_m$ are linearly independent over $\overline{Q}$.*

For $m = 1$ this gives Hermite-Lindemann theorem: is ℓ is a non-zero complex number, then one at least of the two numbers ℓ, e^ℓ is transcendental. For instance

$$e,\ \pi,\ \log 2,\ e^{\sqrt{2}},$$

are all transcendental numbers.

Another consequence of Theorem 11.1 is the transcendence of numbers like

$$\int_0^1 \frac{dt}{1+t^3} = \frac{1}{3}\left(\log 2 + \frac{\pi}{\sqrt{3}}\right).$$

The measures of linear independence over $\overline{Q}$ of the m numbers $\ell_1, \dots, \ell_m$ which we discussed earlier have been extended to the $m+1$ numbers $1, \ell_1, \dots, \ell_m$; however the consequences of such estimates concern only transcendental number theory (so far) and have not the same importance as the homogeneous case (see Chapter 12). This is why, in this Chapter, we speak only on the qualitative result.

We do not give here Baker's proof of Theorem 11.1, but we show how the method of the previous chapters extends to the non-homogeneous case.

1Sketch of proof According to lemma 1.3 (with $k = \mathbb{Q}$, $K = \overline{Q}$, $\mathcal{E} = \mathbb{C}$, while $\mathcal{M}$ is the $\mathbb{Q}$-vector space spanned by 1 and $\mathcal{L}$), Theorem 11.1 means that if we have

$$\beta_0 + \beta_1\ell_1 + \cdots + \beta_n\ell_n - \ell_{n+1} = 0$$

with $\ell_1, \dots, \ell_{n+1}$ in $\mathcal{L}$ linearly independent over $\mathbb{Q}$ and with algebraic β's, then the $n+1$ numbers $1, \beta_1, \dots, \beta_n$ are $\mathbb{Q}$-linearly dependent. From Theorem 1.1 (homogeneous case of Theorem 11.1) we get at once $\beta_0 \neq 0$.

To take care of the new constant coefficient β_0, we introduce one more variable z_0, and we consider $n+2$ functions of $n+1$ variables

$$z_0, z_1, \dots, z_n, \exp\{z_0 + \ell_1 z_1 + \cdots + \ell_n z_n\};$$

we shall consider the values of these functions (and of monomials in these functions) at the $n+1$ points

$$(0,1,0,\dots,0), (0,0,1,\dots,0), \dots, (0,0,\dots,1) \quad \text{and} \quad (\beta_0, \beta_1, \dots, \beta_n).$$

We shall also take linear combinations of these points: for $\underline{s} = (s_1, \dots, s_{n+1}) \in \mathbb{Z}^{n+1}$ we denote by $\xi_{\underline{s}}$ the point in $\mathbb{C}^{n+1}$ of coordinates

$$(s_{n+1}\beta_0, s_1 + s_{n+1}\beta_1, \dots, s_n + s_{n+1}\beta_n).$$

It is necessary to use somewhere the fact that each function satisfies a partial differential equation with algebraic coefficients by taking the derivative with respect to z_0; if this information were not used, one could multiply the variable z_0 by a transcendental constant, and the assumption that β_0 is algebraic would not be used !

For $\underline{\lambda} = (\lambda_0, \dots, \lambda_{n+1}) \in \mathbb{N}^{n+2}$ and $z = (z_0, \dots, z_n) \in \mathbb{C}^{n+1}$, define

$$f_{\underline{\lambda}}(z) = z_0^{\lambda_0} \cdots z_n^{\lambda_n} \exp\big\{\lambda_{n+1}(z_0 + \ell_1 z_1 + \cdots + \ell_n z_n)\big\};$$

then

$$\left(\frac{\partial}{\partial z_0}\right)^t f_{\underline{\lambda}}(z) = \sum_{\tau=0}^{\min\{t,\lambda_0\}} \frac{t!}{\tau!(t-\tau)!}\frac{\lambda_0!}{(\lambda_0-\tau)!}\lambda_{n+1}^{t-\tau} z_0^{\lambda_0-\tau} z_1^{\lambda_1}\cdots z_n^{\lambda_n}\exp\bigl\{\lambda_{n+1}(z_0+\ell_1 z_1+\cdots+\ell_n z_n)\bigr\}.$$

Hence, for $\underline{s}\in\mathbb{Z}^{n+1}$, $t\in\mathbb{N}$ and $\underline{\lambda}\in\mathbb{N}^{n+2}$, we have

$$\left(\frac{\partial}{\partial z_0}\right)^t f_{\underline{\lambda}}(\xi_{\underline{s}}) = \sum_{\tau=0}^{\min\{t,\lambda_0\}} \frac{t!}{\tau!(t-\tau)!}\frac{\lambda_0!}{(\lambda_0-\tau)!}\lambda_{n+1}^{t-\tau}(s_{n+1}\beta_0)^{\lambda_0-\tau}\prod_{i=1}^{n}(s_i+s_{n+1}\beta_i)^{\lambda_i}\prod_{i=1}^{n+1}\alpha_i^{\lambda_{n+1}s_i}.$$

These numbers are algebraic, by our assumptions (we have written α_i for $\exp(\ell_i)$, as usual). The sketch of proof is now clear: we write a matrix whose entries are these algebraic numbers, we select any determinant of maximal size, we estimate from above the absolute value of this interpolation determinant, and thanks to Liouville's inequality, we deduce that this determinant vanishes. This provides a non-trivial upper bound for the rank of the matrix; a zero estimate implies the desired linear dependence condition on $1,\beta_1,\ldots,\beta_n$.

The new points in the proof are the following: first of all a new zero estimate is needed, involving derivatives. We explain this result in section 2. We shall work on a field of zero characteristic; we need to give an algebraic expression for the derivatives; this is done as follows: for $P\in\mathbb{C}[X_0,\ldots,X_n,Y]$, the function

$$F(z_0,\ldots,z_n)=P\bigl(z_0,\ldots,z_n,\exp\{z_0+\ell_1 z_1+\cdots+\ell_n z_n\}\bigr)$$

has a partial derivative $(\partial/\partial z_0)F$ which is again a polynomial in the $n+2$ functions $z_0,\ldots,z_n$ and $\exp\{z_0+\ell_1 z_1+\cdots+\ell_n z_n\}$. This means that there exists a polynomial DP such that

$$\left(\frac{\partial}{\partial z_0}\right)F(z_0,\ldots,z_n)=(DP)\bigl(z_0,\ldots,z_n,\exp\{z_0+\ell_1 z_1+\cdots+\ell_n z_n\}\bigr).$$

For $P=X_0$ we have $DP=1$, for $P=X_i$, $(1\le i\le n)$ we have $DP=0$, and for $P=Y$ we have $DP=Y$. From this it follows easily that D is the derivative operator

$$\frac{\partial}{\partial X_0}+Y\frac{\partial}{\partial Y}.$$

The only other minor point which has to be explained is the upper bound for the interpolation determinant: we do not consider only values of functions, but also derivatives. The relevant estimate is explained in section 3. The proof of Theorem 11.1 is given in section 4.

1 The zero estimate Let K be a field of characteristic zero and $n\ge 0$ a non-negative integer. We denote by D the derivative operator $(\partial/\partial X_0)+Y(\partial/\partial Y)$ on the ring $K[X_0,\ldots,X_n,Y]$.

Proposition 11.2. – *Let $\alpha_1,\ldots,\alpha_{n+1}$ be non-zero elements of K which generate a multiplicative subgroup of K^* of rank $\ge n$, and let $\beta_0,\ldots,\beta_n$ be elements of K. Assume that L_0, L_1, S and T are positive integers satisfying the following conditions:*

$$T\ge 4(n+1),\qquad S\ge 4n(n+1),\qquad TS^n\ge 2L_1,\qquad T\le 2(n+1)L_0L_1,$$

and

$$TS^{n+1}>2^{n+3}(n+1)^{n+2}(L_0L_1)^{n+1}.$$

For $t\in\mathbb{N}$, $\underline{\lambda}\in\mathbb{N}^{n+2}$ and $\underline{s}\in\mathbb{Z}^{n+1}$, define $a_{\underline{\lambda}}^{(t,\underline{s})}$ as the value, at the point

$$\zeta_{\underline{s}}=\bigl(s_{n+1}\beta_0,s_1+s_{n+1}\beta_1,\ldots,s_n+s_{n+1}\beta_n,\alpha_1^{s_1}\cdots\alpha_{n+1}^{s_{n+1}}\bigr)\in K^{n+1}\times K^*,$$

of the polynomial

$$D^t\big(X_0^{\lambda_0}\cdots X_n^{\lambda_n}Y^{\lambda_{n+1}}\big).$$

Consider the following matrix:

$$\mathcal{M}=\Big(a_{\underline{\lambda}}^{(t,\underline{s})}\Big)_{\underline{\lambda},(t,\underline{s})}$$

where the index of rows $\underline{\lambda}$ runs over the elements of $\mathbb{N}^{n+2}$ with $\lambda_0+\cdots+\lambda_n\le L_0$ and $\lambda_{n+1}\le L_1$, while the index of columns $(t,\underline{s})$ runs over the elements of $\mathbb{N}\times\mathbb{Z}^{n+1}(S)$ with $t<T$. If $\beta_0\neq 0$ and if $1,\beta_1,\dots,\beta_n$ are linearly independent over $\mathbb{Q}$, then the matrix $\mathcal{M}$ is of rank $\binom{L_0+n+1}{n+1}(L_1+1)$.

If the rank of $\mathcal{M}$ is not equal to the number of rows, then there is a non-zero polynomial $P\in K[X_0,\dots,X_n,Y]$, of total degree at most L_0 in $X_0,\dots,X_n$ and of degree at most L_1 in Y, which vanishes, together with its T first derivatives D^t, $(0\le t<T)$, at the points $\zeta_{\underline{s}}$. This enables one to check the hypotheses of Philippon's zero estimate [P] (see exercise 1). However we shall explain here how to deduce Proposition 11.2 from a special case of [P] (Proposition 11.6 below): we shall eliminate the variable Y and produce a non-zero polynomial $Q\in K[X_0,\dots,X_n]$ which vanishes, together with its $T/2$ first derivatives $(\partial/\partial X_0)^t$, $(0\le t<T/2)$, at the points

$$\xi_{\underline{s}}=(s_{n+1}\beta_0,s_1+s_{n+1}\beta_1,\dots,s_n+s_{n+1}\beta_n)\in K^{n+1}$$

for all $\underline{s}\in\mathbb{Z}^{n+1}(S/2)$.

As in Chapter 5 we denote by σ the canonical surjection from K^* onto the quotient group K^*/K^*_{tors}.

Lemma 11.3. – *Let $\alpha_1,\dots,\alpha_{n+1}$ be non-zero elements of K and let $\beta_0,\dots,\beta_n$ be elements of K. Let L_0, L_1, S', S'', T' and T'' be positive integers; we set $S=S'+S''-1$ and $T=T'+T''-1$. Assume*

$$\mathrm{Card}\big\{\sigma\big(\alpha_1^{s_1}\cdots\alpha_{n+1}^{s_{n+1}}\big)\,;\,\underline{s}\in\mathbb{Z}^{n+1}(S')\big\}>L_1/T'.$$

Assume further that there exists a non-zero polynomial $P\in K[X_0,\dots,X_n,Y]$, of total degree $\le L_0$ in $X_0,\dots,X_n$ and of degree $\le L_1$ in Y which satisfies

$$D^tP(\zeta_{\underline{s}})=0\qquad\text{for all }(t,\underline{s})\in\mathbb{N}\times\mathbb{Z}^{n+1}(S)\quad\text{with }t<T.$$

Then there exists a non-zero polynomial $Q\in K[X_0,\dots,X_n]$ of total degree $\le 2L_0L_1$ for which

$$\left(\frac{\partial}{\partial X_0}\right)^t Q(\xi_{\underline{s}})=0\qquad\text{for all}\quad(t,\underline{s})\in\mathbb{N}\times\mathbb{Z}^{n+1}(S'')\quad\text{with}\quad t<T''.$$

The proof of lemma 11.3 is essentially the same as the proof of lemma 5.2. We need some variants of lemmas 5.3 and 5.4.

Lemma 11.4. — *Let $F_1,\dots,F_r$ be polynomials in $K[X_0,\dots,X_n,Y]$, of total degree at most L_0 in $X_0,\dots,X_n$ and of degree at most L_1 in Y; we assume that they have no common irreducible factor, in the factorial ring $K[X_0,\dots,X_n,Y]$, of degree ≥ 1 with respect to Y. Let T be a positive integer and (ξ_j,η_j), $(j\in J)$ be elements of $K^{n+1}\times K$ such that*

$$D^tF_i(\xi_j,\eta_j)=0\qquad\text{for}\qquad 1\le i\le r,\quad j\in J\quad\text{and}\quad 0\le t<T.$$

Then there exists a non-zero polynomial in $K[X_0,\dots,X_n]$, of total degree $\le 2L_0L_1$, such that

$$\left(\frac{\partial}{\partial X_0}\right)^t Q(\xi_j)=0\qquad\text{for}\qquad j\in J\quad\text{and}\quad 0\le t<T.$$

Proof. We just repeat the proof of lemma 5.3: the u-resultant R in the ring

$$K[U_1,\dots,U_r,V_1,\dots,V_r,X_0,\dots,X_n]$$

is a linear combination of G and H; it follows that $D^tR=(\partial/\partial X_0)^tR$ is a linear combination of the $D^\tau G$ and $D^\tau H$ with $0\le\tau\le t$. The desired result easily follows. □

Lemma 11.5. – *Let P be a polynomial in the ring $K[X_0,\dots,X_n,Y]$. We decompose P into a product $P = Q_0 Q_1^{r_1}\cdots Q_k^{r_k}$, where Q_0 is a polynomial in $K[X_0,\dots,X_n]$ (independent of Y), $Q_1,\dots,Q_k$ are distinct irreducible polynomials in the ring $K[X_0,\dots,X_n,Y]$, of degree at least 1 in Y, and $r_1,\dots,r_k$ are positive integers. If Q_1 divides $D^{r_1}P$, then Y divides P.*

Proof. Clearly, Q_1 divides $D^t P$ for $0 \le t \le r_1 - 1$, and $D^{r_1}P$ is congruent to $r_1!(D^{r_1}Q_1)Q_0 Q_2^{r_2}\cdots Q_k^{r_k}$ modulo Q_1. If Q_1 also divides $D^{r_1}P$, then Q_1 divides $D^{r_1}Q_1$. Considering the degrees, we deduce that there exists a constant $\lambda \neq 0$ in K such that $Q_1 = \lambda D^{r_1}Q_1$. We write

$$Q_1 = \sum_{i\ge 0} a_i(X_0)Y^i$$

where a_i is a polynomial in X_0 with coefficients in the ring $K[X_1,\dots,X_n]$. We obtain

$$a_i = \lambda \sum_{j=0}^{r_1} \binom{r_1}{j} i^j a_i^{(r_1-j)}$$

where $a_i^{(r_1-j)} = (d/dX_0)^{r_1-j} a_i$. If $a_i(X_0)$ does not vanish, then, considering the term of highest degree (in X_0), we obtain $\lambda i^{r_1} = 1$. This shows that there is a unique i with $a_i(X_0) \neq 0$, hence Y divides Q_1. □

Proof of lemma 11.3. We assume, as we may without loss of generality, that Y does not divide the given polynomial P, and also that P has degree ≥ 1 with respect to Y. For $\underline{s} \in \mathbb{Z}^{n+1}$ we define a linear map $\tau_{\underline{s}}$ from the ring $K[X_0,\dots,X_n,Y]$ into itself by

$$\begin{aligned} \tau_{\underline{s}}(X_0) &= X_0 + s_{n+1}\beta_0, \\ \tau_{\underline{s}}(X_i) &= X_i + s_i + s_{n+1}\beta_i, \quad (1 \le i \le n), \end{aligned}$$

and

$$\tau_{\underline{s}} Y = \alpha_1^{s_1}\cdots\alpha_{n+1}^{s_{n+1}} Y.$$

These operators, which represent a translation by $\zeta_{\underline{s}}$, commute with D:

$$D \circ \tau_{\underline{s}} = \tau_{\underline{s}} \circ D, \qquad (\underline{s} \in \mathbb{Z}^{n+1}).$$

1) We prove that the polynomials $D^t \circ \tau_{\underline{s}} P$ for $0 \le t < T'$ and $\underline{s} \in \mathbb{Z}^{n+1}(S')$ have no common irreducible factor of degree ≥ 1 in Y.

For this we consider, as in lemma 11.5, a decomposition of P into a product

$$P = Q_0 \prod_{i=1}^{k} Q_i^{r_i}$$

where $Q_0 \in K[\underline{X}]$ does not depend on Y, while for $1 \le i \le k$, Q_i is an irreducible polynomial in $K[\underline{X},Y]$ of degree ≥ 1 in Y. Here, $\underline{X}$ stands for $(X_0,\dots,X_n)$. Assume that there is an irreducible polynomial Q depending on Y which divides all $D^t \circ \tau_{\underline{s}} P$. For each $\underline{s} \in \mathbb{Z}^{n+1}(S')$, Q is an irreducible factor of $\tau_{\underline{s}} P$; hence there exists $i = i(\underline{s})$ with $1 \le i(\underline{s}) \le k$ and a non-zero element $c_{\underline{s}}$ of K such that

$$Q = c_{\underline{s}} \tau_{\underline{s}} Q_{i(\underline{s})}.$$

Now Q divides also $D^t \tau_{\underline{s}} P$ for $0 \le t < T'$; from lemma 11.5 we deduce $T' \le r_{i(\underline{s})}$. Let I be the subset of $\{1,\dots,k\}$ which is constituted of the $i(\underline{s})$, $s \in \mathbb{Z}^{n+1}(S')$. Consider the map

$$\underline{s} \longmapsto \left(i(\underline{s}), \sigma\big(\alpha_1^{s_1}\cdots\alpha_{n+1}^{s_{n+1}}\big) \right)$$

from $\mathbb{Z}^{n+1}(S')$ into $I \times \left(K^*/K^*_{\rm tors}\right)$. For each $i \in I$ we have $r_i \geq T'$, hence $\sum_{i\in I} r_i \geq T'\mathrm{Card}(I)$. On the other hand $\sum_{i\in I} r_i \leq \sum_{i=1}^{k} r_i \leq L_1$. Hence $\mathrm{Card}(I) \leq L_1/T'$. Using our assumption on L_1/T' together with Dirichlet box principle, we see that there exists a non-zero element $\underline{s}$ in $\mathbb{Z}^{n+1}$ which has the property

$$\tau_{\underline{s}} Q_{i_0} = \lambda Q_{i_0}$$

for some $\lambda \in K^*$ and

$$\alpha_1^{s_1} \cdots \alpha_{n+1}^{s_{n+1}} \qquad \text{is not a root of unity.}$$

Since Y does not divide P, lemma 5.4 with

$$u_0 = s_{n+1}\beta_0, \qquad u_i = s_i + s_{n+1}\beta_i, \qquad (1 \leq i \leq n), \qquad v = \alpha_1^{s_1} \cdots \alpha_{n+1}^{s_{n+1}}$$

and an obvious change of notations (with n replaced by $n+1$) gives the desired contradiction.
2) We now take into account our assumptions $S = S' + S'' - 1$ and $T = T' + T'' - 1$. We apply lemma 11.4 to the set of polynomials

$$\{F_1, \ldots, F_r\} = \left\{D^t \circ \tau_{\underline{s}'} P\,;\, 0 \leq t < T',\, \underline{s}' \in \mathbb{Z}^{n+1}(S')\right\}$$

and to the set $\{(\xi_i, \eta_i)\,;\, 1 \leq i \leq N\} \subset K^{n+1} \times K^*$ defined by

$$\left\{\left(s''_{n+1}\beta_0, s''_1 + s''_{n+1}\beta_1, \ldots, s''_n + s''_{n+1}\beta_n, \alpha_1^{s''_1} \cdots \alpha_{n+1}^{s''_{n+1}}\right)\,;\, \underline{s}'' \in \mathbb{Z}^{n+1}(S'')\right\};$$

this gives the conclusion. □

Thanks to lemma 11.3, to complete the proof of Proposition 11.2, it is now sufficient to deal with polynomials in $X_0, \ldots, X_n$. Here is the corresponding zero estimate.

Proposition 11.6. – *Let $\beta_0, \ldots, \beta_n$ be elements of K with $\beta_0 \neq 0$. Let D, S and T be three positive integers. Assume either $n = 0$ and $T(2S-1) > D$, or else $n \geq 1$ and*

$$S \geq 2n(n+1), \qquad 2 \leq T/(n+1) \leq D, \qquad TS^{n+1} > 2^{-n}(n+1)^{n+2}D^{n+1}.$$

Assume that there is a non-zero polynomial $Q \in K[X_0, \ldots, X_n]$ of total degree $\leq D$ for which

$$\left(\frac{\partial}{\partial X_0}\right)^t Q(\xi_{\underline{s}}) = 0 \qquad \text{for all } (t, \underline{s}) \in \mathbb{N} \times \mathbb{Z}^{n+1}(S) \quad \text{with } t < T.$$

Then the numbers $1, \beta_1, \ldots, \beta_n$ are linearly dependent over $\mathbb{Q}$.

Proof. When $n = 0$, the result is straightforward. Assume $n \geq 1$ and define $S_1 = \lfloor S/(n+1) \rfloor$. We claim that our hypotheses imply

$$(2S_1 - 1)^{\delta+1} > D^\delta \qquad \text{for} \qquad 1 \leq \delta \leq n$$

and

$$T(2S_1 - 1)^\delta > (n+1)D^\delta \qquad \text{for} \qquad 1 \leq \delta \leq n+1.$$

Indeed our assumption $S \geq 2n(n+1)$ gives

$$(2S_1 - 1)^\nu > \frac{1}{2}\left(\frac{2S}{n+1}\right)^\nu \qquad \text{for} \qquad 1 \leq \nu \leq n+1,$$

because

$$\left(1 - \frac{1}{4n}\right)^{n+1} > \frac{1}{2} \qquad \text{for} \qquad n \geq 1.$$

Since $2(n+1) \le T \le (n+1)D$, we have

$$D^{n+1} \le \frac{D}{2}\left(\frac{2S}{n+1}\right)^{n+1}, \qquad \text{hence} \qquad \left(\frac{D}{2}\right)^{n} \le \left(\frac{S}{n+1}\right)^{n+1}.$$

It follows that, for $1 \le \delta \le n$,

$$\left(\frac{D}{2}\right)^{\delta} \le \left(\frac{S}{n+1}\right)^{(n+1)\delta/n} \le \left(\frac{S}{n+1}\right)^{\delta+1},$$

hence

$$(2S_1-1)^{\delta+1} > 2^{\delta}\left(\frac{S}{n+1}\right)^{\delta+1} \ge D^{\delta}.$$

Similarly, for $1 \le \delta \le n+1$,

$$D^{\delta} \le \left(\frac{T}{2(n+1)}\right)^{\delta/(n+1)}\left(\frac{2S}{n+1}\right)^{\delta} < \frac{T}{n+1}(2S_1-1)^{\delta}$$

(this is the only place in the proof where the assumption $T \ge 2(n+1)$ is needed; see exercise 2). This proves our initial claim.

Define

$$E = \{\xi_{\underline{s}}\,;\, \underline{s} \in \mathbb{Z}^{n+1}(S_1)\}.$$

We are going to use the main result in [P]; more precisely, we apply Proposition 5.1 of [W] with $d_0 = d = n+1$, $d_1 = 0$, $E_1 = \cdots = E_d = E$ and $W = K \times 0^n$. We deduce that there exists a vector subspace $\mathcal{V}$ of K^{n+1}, of codimension $\delta \ge 1$, such that either

$$\big(T/(n+1)\big)\mathrm{Card}\big((E+\mathcal{V})/\mathcal{V}\big) \le D^{\delta} \qquad \text{and} \qquad (1,0,\dots,0) \notin \mathcal{V},$$

or

$$\mathrm{Card}\big((E+\mathcal{V})/\mathcal{V}\big) \le D^{\delta} \qquad \text{and} \qquad (1,0,\dots,0) \in \mathcal{V}.$$

We consider two cases.

a) If $(1,0,\dots,0) \in \mathcal{V}$, we take the quotient of $\mathcal{V}$ by $K \times 0^n$: let $\pi : K^{n+1} \longrightarrow K^n$ be the projection on the last n components; the kernel of π is $K \times 0^n$, the image $\mathcal{V}_1 = \pi(\mathcal{V})$ of $\mathcal{V}$ is of codimension δ in K^n, and $\pi(E) = Y(S_1)$ where

$$Y(S_1) = \big\{s_1 + s_{n+1}\beta_1, \dots, s_n + s_{n+1}\beta_n)\,;\, \underline{s} = (s_1,\dots,s_{n+1}) \in \mathbb{Z}^{n+1}(S_1)\big\} \subset K^n.$$

The restriction to E of the diagram

$$\begin{array}{ccc} K^{n+1} & \xrightarrow{\ \pi\ } & K^n \\ \downarrow & & \downarrow \\ K^{n+1}/\mathcal{V} & \xrightarrow{\ \sim\ } & K^n/\mathcal{V}_1 \end{array} \qquad \text{gives} \qquad \begin{array}{ccc} E & \longrightarrow & Y(S_1) \\ \downarrow & & \downarrow \\ (E+\mathcal{V})/\mathcal{V} & \longrightarrow & \big(Y(S_1)+\mathcal{V}_1\big)/\mathcal{V}_1. \end{array}$$

The estimates

$$\mathrm{Card}\Big(\big(Y(S_1)+\mathcal{V}_1\big)/\mathcal{V}_1\Big) = \mathrm{Card}\big((E+\mathcal{V})/\mathcal{V}\big) \le D^{\delta} < (2S_1-1)^{\delta+1}$$

together with lemma 5.9 provide the desired linear dependence relation between the numbers $1, \beta_1, \dots, \beta_n$.

b) Assume $(1,0,\dots,0)\notin\mathcal{V}$. From our assumption $\beta_0\neq 0$, we deduce $\mathrm{Card}\big((E+\mathcal{V})/\mathcal{V}\big)\geq 2S_1-1$. Therefore

$$D^\delta\geq\big(T/(n+1)\big)\mathrm{Card}\big((E+\mathcal{V})/\mathcal{V}\big)\geq T(2S_1-1)/(n+1)>D,$$

which shows that $\delta\geq 2$. Consequently the quotient $\mathcal{V}_1$ of $\mathcal{V}$ by $\mathcal{V}\cap K\times 0^n$ is of codimension $\delta-1\geq 1$ in K^n, and again we can apply lemma 5.9 and conclude that $1,\beta_1,\dots,\beta_n$ are linearly dependent over $\mathbb{Q}$. □

Proof of Proposition 11.2. Define $S''=\lfloor S/2\rfloor$, $T''=\lfloor T/2\rfloor$, $S'=S-S''+1$, $T'=T-T''+1$. Since $2S'-1\geq S$ and $T'>T/2$, we have $(2S'-1)^n>L_1/T'$. This shows that the assumptions of lemma 11.3 are satisfied. We deduce that the assumptions of Proposition 11.6 are also satisfied with $D=2L_0L_1$ and (S,T) replaced by (S'',T''). Indeed, assuming $n\geq 1$ (the case $n=0$ is trivial), we have $S''>S/2$, $T''>T/2$, hence $S''>2n(n+1)$, $T''>2(n+1)$; also $T''<(T/2)+1<T\leq(n+1)D$ and

$$(2L_0L_1)^{n+1}\leq\frac{T}{4(n+1)}\left(\frac{S}{n+1}\right)^{n+1}<\frac{T''}{2(n+1)}\left(\frac{2S''}{n+1}\right)^{n+1}.$$

□

1 Interpolation determinants with derivatives Here is a generalization of lemma 4.2.

Lemma 11.7. – *Let $f_1,\dots,f_L$ be entire functions in $\mathbb{C}^{n+1}$, $\zeta_1,\dots,\zeta_L$ be elements of $\mathbb{C}^{n+1}$ and $\tau_1,\dots,\tau_L$ non-negative integers. The function of one variable*

$$\Psi(z)=\det\Big((\partial/\partial z_0)^{\tau_\mu}f_\lambda(z\zeta_\mu)\Big)_{1\leq\lambda,\mu\leq L}$$

has a zero at the origin of multiplicity

$$\geq\Theta_{n+1}(L)-\tau_1-\cdots-\tau_L.$$

Proof. By multilinearity we reduce the proof to the case $f_\lambda(\zeta)=\zeta^{\kappa_\lambda}$ for some $\kappa_\lambda=(\kappa_{\lambda0},\dots,\kappa_{\lambda n})\in\mathbb{N}^{n+1}$, $(1\leq\lambda\leq L)$. In this case we have

$$\psi(z)z^{\tau_1+\cdots+\tau_L}=z^{\|\kappa_1\|+\cdots+\|\kappa_L\|}\det\left(\binom{\kappa_{\lambda0}}{\tau_\mu}\zeta_\mu^{\kappa_\lambda-\tau_\mu}\right)_{1\leq\lambda,\mu\leq L}$$

where the binomial coefficient $\binom{\kappa_{\lambda0}}{\tau_\mu}$ means 0 if $\tau_\mu>\kappa_{\lambda0}$. Lemma 11.7 easily follows. □

1 Proof of Theorem 11.1 We use the notations of section 1: assume

$$\beta_0+\beta_1\ell_1+\cdots+\beta_n\ell_n-\ell_{n+1}=0,$$

with $\beta_0\neq0$ and with $\ell_1,\dots,\ell_{n+1}$ linearly independent over $\mathbb{Q}$. Define $\alpha_i=\exp(\ell_i)$, $(1\leq i\leq n+1)$. The field $\mathbb{Q}(\alpha_1,\dots,\alpha_{n+1},\beta_1,\dots,\beta_n)$ is a finite extension of $\mathbb{Q}$, of degree say D.

We denote by c a positive constant which depends only on $\ell_1,\dots,\ell_{n+1}$, $\beta_1,\dots,\beta_n$. Next we introduce parameters L_0, L_1, T and S, which are positive integers ≥ 2 satisfying

$$cL_0\log S\leq L^{1/(n+1)},\quad cT\log(L_0L_1)\leq L^{1/(n+1)},\quad cL_1S\leq L^{1/(n+1)},\quad cT\leq L_0L_1$$

and

$$c(L_0L_1)^{n+1}\leq TS^{n+1},$$

with $L:=\binom{L_0+n+1}{n+1}(L_1+1)$. For instance we can take

$$\begin{aligned}T&=\big[(\log S)^{2(n+1)(n+2)}\big],\\ L_1&=\big[(\log S)^{n+2}\big],\\ L_0&=\big[S(\log S)^{n+1}\big],\end{aligned}$$

with S a sufficiently large positive integer. In any case the above conditions, for sufficiently large c, imply that each of the four parameters L_0, L_1, T and S is sufficiently large (for instance $> 8n^2$; also $L > 2^n e^{n+1}$) and moreover imply that

$$TS^n \geq 2L_1 \qquad \text{and} \qquad T \leq 2(n+1)L_0L_1.$$

Let $\bigl(t_\mu, \underline{s}^{(\mu)}\bigr)$ be any elements in $\mathbb{N} \times \mathbb{Z}^{n+1}(S)$ with $t_\mu \leq T$, $(1 \leq \mu \leq L)$. Denote by Δ the determinant of the matrix

$$\left(\left(\frac{\partial}{\partial z_0}\right)^{t_\mu} f_{\underline{\lambda}}(\xi_{\underline{s}^{(\mu)}})\right)_{\underline{\lambda},\mu}$$

Each entry of this matrix is the value of a polynomial in $\alpha_1, \ldots, \alpha_{n+1}$, $\alpha_1^{-1}, \ldots, \alpha_{n+1}^{-1}$ and $\beta_0, \beta_1, \ldots, \beta_n$; this polynomial has degree at most L_1S in each of the first $2n+2$ variables and total degree at most L_0 in the last $n+1$ ones, its coefficients are rational integers, and the length is at most

$$2^T(2S)^{L_0}L_1^TL_0^T \leq (2L_0L_1)^T(2S)^{L_0}.$$

Liouville's inequality (lemma 3.14) gives: either $\Delta = 0$ or else

$$\frac{1}{DL}\log|\Delta| \geq -L_0\log(2S) - T\log(2L_0L_1) - \log L - L_0\sum_{i=1}^{n}\mathrm{h}(\beta_i) - 2L_1S\sum_{i=1}^{n+1}\mathrm{h}(\alpha_i).$$

According to lemmas 11.7 and 4.3, the function of a single variable z

$$\Psi(z) = \det\left((\partial/\partial z_0)^{\tau_\mu} f_{\underline{\lambda}}(z\xi_{\underline{s}^{(\mu)}})\right)_{\underline{\lambda},\mu}$$

has a zero at the origin of multiplicity at least

$$\Theta_{n+1}(L) - LT \geq L\left(\frac{1}{17}L^{1/(n+1)} - T\right).$$

We set

$$r = S\max\bigl\{|\beta_0|, 1+|\beta_1|, \ldots, 1+|\beta_n|, |\ell_1| + \cdots + |\ell_{n+1}|\bigr\}$$

and $R = e^{18}r$, and we use Schwarz lemma (lemma 4.1):

$$\frac{1}{L}\log|\Delta| = \frac{1}{L}\log|\Psi(1)| \leq -\frac{18}{17}L^{1/(n+1)} + 18T + \frac{1}{L}\log|\Psi|_{e^{18}}.$$

From the relation

$$\left(\frac{\partial}{\partial z_0}\right)^t f_{\underline{\lambda}}(z\xi_{\underline{s}}) = \sum_{\tau=0}^{\min\{t,\lambda_0\}} \frac{t!}{\tau!(t-\tau)!}\frac{\lambda_0!}{(\lambda_0-\tau)!}\lambda_{n+1}^{t-\tau}(s_{n+1}\beta_0)^{\lambda_0-\tau}$$
$$z^{\lambda_0+\cdots+\lambda_n-\tau}\prod_{i=1}^{n}(s_i + s_{n+1}\beta_i)^{\lambda_i}\prod_{i=1}^{n+1}e^{\lambda_{n+1}\ell_i s_i z}$$

we deduce, for $|z| \leq e^{18}$ and all $\underline{\lambda}$, μ,

$$\left|\left(\frac{\partial}{\partial z_0}\right)^t f_{\underline{\lambda}}(z\xi_{\underline{s}^{(\mu)}})\right| \leq (2L_0L_1)^T R^{L_0}e^{L_1R}.$$

It plainly follows

$$\frac{1}{L}\log|\Psi|_{e^{18}} \leq L_0\log R + L_1R + T\log(2L_0L_1) + \log L.$$

From our choice of the parameters we deduce

$$\frac{1}{L}\log|\Delta| \le -L^{1/(n+1)}.$$

A simple comparison with Liouville's lower bound, using again our conditions on the parameters, gives $\Delta = 0$. From Proposition 11.2 we obtain the desired conclusion: the numbers $1, \beta_1, \dots, \beta_n$ are linearly dependent over $\mathbb{Q}$. □

1Exercises

1.

a) Deduce from the main result of [P] the following statement: with the notations of section 2, define $S_1 = \lfloor S/(n+2)\rfloor$,

$$\Sigma = \{\zeta_{\underline{s}}\,;\, \underline{s} \in \mathbb{Z}^{n+1}(S_1)\} \subset K^{n+1} \times K^*$$

and

$$E = \{\xi_{\underline{s}}\,;\, \underline{s} \in \mathbb{Z}^{n+1}(S_1)\} \subset K^{n+1}.$$

If the rank of the matrix $\mathcal{M}$ of Proposition 11.2 is not $\binom{L_0+n+1}{n+1}(L_1+1)$, then there exists a vector subspace $\mathcal{V}$ of K^{n+1}, of dimension ν, satisfying one at least of the following three conditions:
(i) one has

$$T\mathrm{Card}\Big((\Sigma + \mathcal{V}\times 0)/\mathcal{V}\times 0\Big) \le (n+2)^2 L_0^{n+1-\nu} L_1;$$

(ii) the space $\mathcal{V}$ does not contain $(1,0,\dots,0)$, its dimension ν satisfies $0 \le \nu \le n$, and

$$T\mathrm{Card}\Big((E+\mathcal{V})/\mathcal{V}\Big) \le \frac{(n+2)^2}{\nu+1} L_0^{n+1-\nu};$$

(iii) the space $\mathcal{V}$ contains $(1,0,\dots,0)$, its dimension ν satisfies $1 \le \nu \le n$, and

$$\mathrm{Card}\Big((E+\mathcal{V})/\mathcal{V}\Big) \le \frac{n+2}{\nu+1} L_0^{n+1-\nu}.$$

`Hint.` *Use corollary* 5.3 *from* [W] *with* $W = K(1,0,\dots,0,1)$, $d_0 = n+1$, $a_\nu = (S_1-1)/(S-1)$, *(*$0 \le \nu \le n+1$*), with* S *replaced by* L_0, H *replaced by* L_1, *and* $L_1,\dots,L_n$ *replaced by* $S-1$.

b) Deduce that the conditions on L_0, L_1, S and T in Proposition 11.2 can be replaced by the following ones:

$$S > \max\{6n(n+2), 3\}, \qquad (n+2)L_0 \ge 2S, \qquad (2S)^{n+1} \ge (n+2)^{n+2} L_0^n$$

and

$$TS^{n+1} \ge 2^{-n}(n+2)^{n+3} L_0^{n+1} L_1.$$

`Hint.` *Check, for* $S_1 = \lfloor S/(n+2)\rfloor$, *the following estimates*

$$(n+2)^2 L_0^{n+1} L_1 < T(2S_1-1)^{n+1},$$

$$(n+2)^2 L_0^{n} L_1 < T(2S_1-1)^{n},$$

$$\frac{(n+2)^2}{\nu+1} L_0^{n+1-\nu} < T(2S_1-1)^{n+1-\nu}, \qquad (0 \le \nu \le n),$$

and

$$\frac{n+2}{\nu+1} L_0^{n+1-\nu} < (2S_1-1)^{n+2-\nu}, \qquad (1 \le \nu \le n).$$

2. Show that the conclusion of Proposition 11.6 still holds when the conditions on S, T and D are replaced by

$$T < 2(n+1) \qquad \text{and} \qquad S \ge (n+1)^2 D.$$

3. For each $k = (k_1, \dots, k_d)$ in $\mathbb{N}^d$, we write $\|k\|$ for $k_1 + \cdots + k_d$. We introduce derivative operators: for $x = (x_1, \dots, x_d) \in \mathbb{C}^d$, we set $D_x = x_1(\partial/\partial z_1) + \cdots + x_d(\partial/\partial z_d)$. If f is an analytic function in $\mathbb{C}^d$ and ζ a new variable in $\mathbb{C}$, we have

$$D_x F(z) = \frac{\partial}{\partial \zeta} F(x\zeta + z)_{\zeta=0}.$$

When $w_1, \dots, w_t$ are in $\mathbb{C}^d$ and τ in $\mathbb{N}^t$, we write $\mathbf{w} = (w_1, \dots, w_t)$ and we set $D^\tau_{\mathbf{w}} = D^{\tau_1}_{w_1} \cdots D^{\tau_t}_{w_t}$. Therefore, if $\zeta_1, \dots, \zeta_t$ are t new complex variables, then

$$D^\tau_{\mathbf{w}} F(z) = \prod_{j=1}^{t} \left(\frac{\partial}{\partial \zeta_j} \right)^{\tau_j} \big(F(\zeta_1 w_1 + \cdots + \zeta_t w_t + z) \big)_{\zeta=0}.$$

Prove the following extension of lemma 11.7:

Let $f_1, \dots, f_L$ be entire functions in $\mathbb{C}^n$, $\zeta_1, \dots, \zeta_L$ be elements of $\mathbb{C}^n$, $\tau_1, \dots, \tau_L$ be elements of $\mathbb{N}^t$ and $\mathbf{w} = (w_1, \dots, w_t)$ be an element in $(\mathbb{C}^n)^t$. The function of one variable

$$\Psi(z) = \det\Big(D^{\tau_\mu}_{\mathbf{w}} f_\lambda(z\zeta_\mu) \Big)_{1 \le \lambda, \mu \le L}$$

has a zero at the origin of multiplicity

$$\ge \Theta_n(L) - \sum_{\mu=1}^{L} \|\tau_\mu\|.$$

4. Compute a suitable value for the constant c in §4.

1References

[P] P. Philippon. – Lemme de zéros dans les groupes algébriques commutatifs; Bull. Soc. Math. France, **114** (1986), 355–383, et **115** (1987), 397–398.

[W] M. Waldschmidt. – Minorations de combinaisons linéaires de logarithmes de nombres algébriques; Canadian J. Math., to appear.

12.– FURTHER ESTIMATES (WITHOUT PROOF)

In this Chapter we first give some indications on possible refinements for the estimates from the preceding Chapters, next we explain the connection between the method which has been developed in these lectures and Baker's method, finally we give a survey of the best known results so far.

1Refinements and variants It's possible to improve the term $(\log B)^2$. By introducing (like in Chapter 11) one more variable z_0, and by taking derivatives with respect to this new variable, we can replace $(\log B)^2$ by $(\log B)(\log\log B)$; if, moreover, we use the so-called *Fel'dman polynomials* (cf [F]), then we get only $\log B$.

Further improvements are possible in the case where the coefficients β_j are all rational integers (this is the most important case for applications). Firstly the assumption $\log B \geq \log A$ is no more needed; secondly the assumption $B \geq |\beta_j|$ can be replaced by

$$B \geq \max_{1\leq j\leq n} \left\{ \frac{|\beta_n|}{\log A_j} + \frac{|\beta_j|}{\log A_n} \right\}$$

if $\beta_n \neq 0$. Once more these refinements use Feldman's polynomials.

It's useful in certain applications to keep the dependence on E (see Proposition 7.7 and Theorem 10.5) in the final estimate: when the numbers $|\ell_j|$ are small, then E can be chosen comparatively large, and the final estimate is stronger. This improvement originates in a work by T.N. Shorey [S].

Better results can be achieved for simultaneous linear forms [R], [Lo], [Dpp4], [H3].

Better constants are known for $n = 2$ ([Mi-W1,2,3], [La], and, for the p-adic case, [Dpp1]; see also [D], where a special attention is paid to the dependence on the degree D). The first estimate for measures of linear independence of two logarithms which did not involve the construction of an auxiliary function is the one of Laurent given in Appendix to these notes.

The proof yields a result like lemma 7.2: if $|\Lambda|$ is small, then not only do we have $\Lambda = 0$ and the $\log \alpha_i$ are $\mathbb{Q}$-linearly independent, but also we produce a vanishing linear combination of the $\log \alpha_i$ with rather small coefficients in $\mathbb{Z}$. This is specially interesting for the analog of Baker's theorem on algebraic groups (see [Ma-W] and [L] pp.121–122 and 238–239; by the way, speaking of algebraic groups, see [H1,2,3]).

The method extends to non-homogeneous linear combinations of logarithms:

$$\Lambda = \beta_0 + \beta_1\ell_1 + \cdots + \beta_m\ell_m.$$

If $\beta_0 \neq 0$, then $\Lambda \neq 0$, and we can give an explicit lower bound. The main interest of such a result lies in corollaries for measures of transcendence of various numbers [W2], [H2].

1Duality: connection with Baker's method Our starting point, to estimate the difference between $\beta_1\ell_1 + \cdots + \beta_n\ell_n$ and ℓ_{n+1} was to consider (generalizing Schneider's idea) the values of the $n+1$ functions $z_1, \ldots, z_n$ and $\exp\{\ell_1 z_1 + \cdots + \ell_n z_n\}$, as well as the values of monomials in these functions, at the points

$$(1, 0, \ldots, 0), \ldots, (0, \ldots, 0, 1) \quad \text{and} \quad (\beta_1, \ldots, \beta_n),$$

as well as at linear combinations of these points (with rational integer coefficients). Baker's starting point is quite different: he considers the $n+1$ functions $\exp(z_1), \ldots, \exp(z_n)$ and $\exp\{\beta_1 z_1 + \cdots + \beta_n z_n\}$, as well as their derivatives, at the point $(\ell_1, \ldots, \ell_n)$; once more one takes monomials in the functions, and multiples of the considered point.

One can work out a proof along Baker's approach without constructing an auxiliary function, but only using Laurent's interpolation determinants. The fact that derivatives are there means that the corresponding zero estimate needs to involve multiplicities. The scheme of proof is just the same: using the *multiplicity estimate* one constructs a non-zero determinant; Liouville's inequality provides a lower bound; estimates of interpolation determinants (involving derivatives) yield the conclusion. So far no complete proof has been written along these lines, but there is no difficulty to do so.

There is a very interesting connection between the two approaches: *one shifts from one method to the other just by transposing matrices.* This is a consequence of the *duality formula*:

$$\left(\frac{d}{dz}\right)^s \left(z^t e^{uz}\right)_{z=v} = \left(\frac{d}{dz}\right)^t \left(z^s e^{vz}\right)_{z=u}$$

for s and t non-negative integers and u and v complex numbers. This formula extends to exponentials in several variables (exercise 3).

In Chapters 6 and 7, the proofs used a generalization of Schneider's method in several variables; the improved estimate in Chapter 10 involved the refinement of section 1 in Chapter 9, where the main point is that we are working with a product of monomials by a function of a *single* variable. The method which is *dual* (namely looking at a transposed matrix; see exercise 2) to the method in Chapters 6 and 7 is just a generalization in several variables of Gel'fond's solution to Hilbert's seventh problem; the main new fact in Baker's method (compared with Gel'fond's one) is that the values of the functions of several variables are taken on a one dimensional complex vector space; this is just the dual of the argument in §9.1. Explicitly, we have the dual correspondence:

- monomials $z_1^{\lambda_1} \cdots z_n^{\lambda_n}$ in the previous chapters correspond (in the methods of Gel'fond and Baker) to derivatives $(\partial/\partial z_1)^{\lambda_1} \cdots (\partial/\partial z_n)^{\lambda_n}$;
- an exponential of a linear form in several variables (in the previous chapters) corresponds (in Baker's method) to a product of exponential functions in one variable (which happends to be also an exponential function in one variable).

This explains why it's possible to give a proof of theorem 11.1 along Baker's method by using only functions of a single variable, while this is not possible with Schneider's approach.

In Baker's original proof, the fact that all points are on a complex line was used in an essential way for an extrapolation formula (which is not available in higher dimension); with interpolation determinants, extrapolation is no more needed.

There are now several ways for proving measures of linear independence of logarithms: one can construct a non-zero determinant either by using Baker's approach (with the multiplicity estimate) or by using the generalization of Schneider's approach (with a zero estimate without multiplicities). Once the determinant is constructed, the lower bound is clear (Liouville). The analytic argument involving interpolation determinants can be performed either by looking at the determinant or at its transpose; it would be interesting to compare the estimates which can be obtained using these different approaches.

As far as the dependence in the number m of logarithms is concerned, the most precise known estimate involves only m^m, under the extra assumption that, for a given prime q, the q-th roots $\alpha_1^{1/q}, \ldots, \alpha_m^{1/q}$ generate an extension of the field $\mathbb{Q}(\alpha_1, \ldots, \alpha_m)$ of maximal degree q^m (see [BGMMS], [P-W1], [W1]). This estimate has been reached so far only via Baker's method, thanks to a double induction procedure involving extrapolations with small steps. It seems that the simpler proof (allued to above) along Baker's method involving a determinant will yield a rather bad dependence in m, unless one knows better multiplicity estimates (essentially, best possible estimates seem to be needed).

1The state of the art The reference [B] contains a historical survey of known estimates up to 1977. At that time the best known lower bounds were the two main results of [B]. We describe here briefly more recent results.

We first fix the notations (compare with Theorem 10.1: we only add a coefficient β_0, like in Chapter 11).

Let $\ell_1, \ldots, \ell_m$ be logarithms of algebraic numbers, $\alpha_i = \exp(\ell_i)$, $(1 \le i \le m)$ and $\beta_0, \ldots, \beta_m$ be algebraic numbers, such that the number

$$\Lambda = \beta_0 + \beta_1\ell_1 + \cdots + \beta_m\ell_m$$

does not vanish.

We denote by D be the degree over $\mathbb{Q}$ of the number field $\mathbb{Q}(\alpha_1, \ldots, \alpha_m, \beta_0, \ldots, \beta_m)$ and by $A, A_1, \ldots, A_m$ and B real numbers, which are $\ge e$, and satisfy

$$A \ge A_i, \quad \log A_i \ge \mathrm{h}(\alpha_i), \quad D\log A_i \ge e|\ell_i|, \qquad (1 \le i \le m)$$

and

$$\log B \ge \mathrm{h}(1 : \beta_0 : \beta_1 : \cdots : \beta_m).$$

The best known estimates (see [P-W1], [Wü] and [W5]) state that there exist two positive numbers $C_1(m)$ and $C_2(m)$, which depend only on the number m of logarithms, and which satisfy the following property:

– *General case:* $|\Lambda| \geq e^{-U_1}$ with

$$U_1 = C_1(m)D^{m+2}(\log B + \log\log A)\log A_1 \cdots \log A_m.$$

– *Rational case:* assume $\beta_0 = 0$ and $(\beta_1, \ldots, \beta_m) \in \mathbb{Q}^m$. Then $|\Lambda| \geq e^{-U_2}$ with

$$U_2 = C_2(m)D^{m+2}\log B \log A_1 \cdots \log A_m.$$

One essential feature of these estimates is that the numbers $C_1(m)$ and $C_2(m)$ can be explicitly computed. For instance it follows from [P-W1] that one can take

$$C_1(m) = 2^{8m+53}m^{2m}$$

provided that one assumes $A_i \geq e^m$, $\log A_i \geq |\log \alpha_i|$ $(1 \leq i \leq m)$ and $A \geq e^e$.

In [Wü], the dependence in m and D is not given explicitly, but Wüstholz announces that in a subsequent note he will *determine an explicit value for the constant which is much better than Baker's constant* $(16mD)^{200m}$. According to [Ri] (Chap. C, §1.1 p.236), there is a forthcoming joint paper by Baker and Wüstholz on this subject.

Some authors state their results in terms of the usual height of the algebraic numbers, in place of Weil's height; the exponent of D then looks smaller ($m+1$ in place of m), but in fact the result is weaker (see (3.12)).

The proofs in [P-W] as well as [Wü] use Baker's method (see also [Ma]). The proof in [W5] involves the generalization of Schneider's method to several variables which has been discussed in these lectures. It's not clear which one should give the best estimates; in view of the duality between both approaches, one might expect that the same result will arise in each case; but some minor differences seem to occur in the estimates, and a combination of both arguments could be the best solution.

Here is an explicit result concerning the value of $C_2(m)$ (see [W5] Cor. 10.4). For simplicity we state it in the form of a lower bound for $\left|\alpha_1^{b_1} \cdots \alpha_m^{b_m} - 1\right|$.

Let $\alpha_1, \ldots, \alpha_m$ be non-zero algebraic numbers and $b_1, \ldots, b_m$ be rational integers; assume

$$\alpha_1^{b_1} \cdots \alpha_m^{b_m} \neq 1.$$

We denote by D be the degree of the number field $\mathbb{Q}(\alpha_1, \ldots, \alpha_m)$ over $\mathbb{Q}$ and by $A_1, \ldots, A_m$ real numbers, which are $\geq e$, and satisfy

$$\log A_i \geq \mathrm{h}(\alpha_i), \qquad (1 \leq i \leq m).$$

Further, let

$$B = \max\{2, |b_1|, \ldots, |b_m|\}.$$

Then

$$\left|\alpha_1^{b_1} \cdots \alpha_m^{b_m} - 1\right| \geq e^{-U}$$

with

$$U = 2^{6m+32}m^{3m+6}D^{m+2}(1+\log D)(\log B + \log D)\log A_1 \cdots \log A_m.$$

The results in [P-W1] and [W5] include another parameter E (compare with Proposition 7.7 and Theorem 10.5) which makes the result slightly more complicated, but which is important in many applications. In the case $m = 2$, better constants have already been derived from Schneider's method in [Mi-W1,2,3]. By the way, A.W. Glass told me that Tahei Okada went through all details in [Mi-W2]; he pointed out a few minor corrections which should be made in the arguments, but do not invalidate the final result. This result is now superseded by [Mi-W3], and more seriously by [La].

There is an extensive literature on the so-called p-adic case; we refer to van der Poorten's survey [vdP], as well as Yu Kunrui's papers [Yu]; these works deal with Baker's method. Schneider's method in the p-adic

case has been worked out by Dong Pingping [Dpp1,2,3,4], who derives also estimates for simultaneous linear relations. As suggested in §1 above, in the complex case also it is possible to derive stronger estimates for several independent linear combinations of logarithms (see [P-W2] for Baker's method).

Another quite different direction which leads very sharp estimates from below for linear combinations of logarithms is related with Padé approximation and with Siegel's G-functions. We quote only one such example due to G. Rhin, involving numerical computations by E. Dubois and Ph. Toffin [Rh]: for rational integers b_0, b_1, b_2 with $B = \max\{|b_1|, |b_2|\} \geq 2$,

$$|b_0 + b_1 \log 2 + b_2 \log 3| \geq B^{-13.3}.$$

The exponent 13.3 can be replaced by 7.616 for sufficiently large B.

1Open problems.

1. So far, only Baker's method gives a sharp estimate in terms of the number m of logarithms, namely m^{2m} in the general case, and m^m when, for instance, the numbers $\alpha_i^{1/2}$ generate a number field of maximal degree 2^m; it's an interesting question to achieve such an estimate using the method which is described in the present notes.

2. Does there exist an absolute constant $C > 0$ such that, for all rational p/q, $|e^\pi - p/q| > q^{-C}$?

1Exercises **1.** Improve the estimate of Theorem 10.1: replace $(\log B)^2$ by $\log B$.

`Hint.` *See* [W5]*, but replace the auxiliary function of* [W5] *by an interpolation determinant, like in Chapters* 10 *and* 11*.*

2. Let $\ell_1, \ldots, \ell_{n+1}$, $\beta_1, \ldots, \beta_n$ be complex numbers satisfying $\beta_1\ell_1 + \cdots + \beta_n\ell_n = \ell_{n+1}$. Define $\alpha_i = e^{\ell_i}$, $(1 \leq i \leq n+1)$. For $\underline{s} = (s_1, \ldots, s_{n+1}) \in \mathbb{Z}^{n+1}$, define

$$\begin{aligned} f_{\underline{s}}(z_1, \ldots, z_n) &= e^{s_1 z_1} \cdots e^{s_n z_n} e^{(\beta_1 z_1 + \cdots + \beta_n z_n) s_{n+1}} \\ &= \exp\left\{ \sum_{i=1}^{n} (s_i + s_{n+1}\beta_i) z_i \right\}. \end{aligned}$$

Define also $\ell = (\ell_1, \ldots, \ell_n) \in \mathbb{C}^n$.

a) Compare the numbers

$$\left(\frac{\partial}{\partial z_1}\right)^{\lambda_1} \cdots \left(\frac{\partial}{\partial z_n}\right)^{\lambda_n} f_{\underline{s}}(\lambda_{n+1}\ell),$$

for $\underline{\lambda} = (\lambda_1, \ldots, \lambda_{n+1}) \in \mathbb{N}^{n+1}$, with the entries of the matrix in Proposition 7.7.

b) Use exercise 2 of Chapter 11 to produce another upper bound for the determinant $|\Delta_r|$ in the proof of Proposition 7.7 and also of Theorem 10.5.

3. Let n, s and t be positive integers; further let x, y, $w_1, \ldots, w_t$, $u_1, \ldots, u_s$ be elements of $\mathbb{C}^n$; furthermore let $\tau \in \mathbb{N}^t$ and $\sigma \in \mathbb{N}^s$. Define

$$\mathbf{w} = (w_1, \ldots, w_t) \in \big(\mathbb{C}^n\big)^t \quad \text{and} \quad \mathbf{u} = (u_1, \ldots, u_s) \in \big(\mathbb{C}^n\big)^s.$$

For $z \in \mathbb{C}^n$, define

$$(z \cdot u)^\sigma = \prod_{i=1}^{s} (z \cdot u_i)^{\sigma_i},$$

where $z \cdot u_i$ is the usual scalar product in $\mathbb{C}^n$ (see Chapter 2 exercise 3). Define also $D^\tau_{\mathbf{w}}$ in the same way as in exercise 2 of Chapter 11. Check

$$D^\tau_{\mathbf{w}}\big((z \cdot \mathbf{u})^\sigma e^{xz}\big)_{z=y} = D^\sigma_{\mathbf{u}}\big((z \cdot \mathbf{w})^\tau e^{yz}\big)_{z=x}$$

`Hint.` *See* [W3].

1References

[B] A. Baker. – The theory of linear forms in logarithms; Chap.1 of: *Transcendence Theory: Advances and Applications*; ed. A.Baker and D.W.Masser, Academic Press (1977), 1–27.

[BGMMS] J. Blass, A.M. Glass, D.K. Manski, D.B. Meronk and R.P. Steiner. – Constants for lower bounds for linear forms in the logarithms of algebraic numbers; Acta Arith., **55** (1990), 1–22; *Problèmes Diophantiens 1987-1988*, Publ. Univ. P. et M. Curie (Paris 6) **88**, N°2, 31p.

[D] G. Diaz. – Minoration de $|\alpha_1^\beta - \alpha_2|$ lorsque β est de degré 2; *Approximations Diophantiennes et Nombres Transcendants, Luminy 1990,* éd. P. Philippon, W. de Gruyter (1992), 105–121.

[Dpp1] Dong Ping Ping. – Minorations de combinaisons linéaires de deux logarithmes p-adiques; Annales Fac. Sci. Toulouse **12** (1991), 195–250.

[Dpp2] Dong Ping Ping. – Minoration de la distance p-adique entre deux produits de puissances de nombres algébriques; *Problèmes Diophantiens 1989-1990*, Publ. Univ. P. et M. Curie (Paris 6) **93**, N°3, 9p.

[Dpp3] Dong Ping Ping. – Minorations de combinaisons linéaires de logarithmes de nombres algébriques p-adiques; C. R. Acad. Sci. Paris, Sér. 1, **315** (1992), 103–106.

[Dpp4] Dong Ping Ping. – Minorations de combinaisons linéaires de logarithmes de nombres algébriques p-adiques; manuscript, 1992.

[F] N.I. Feldman. – Improved estimates for a linear form of the logarithms of algebraic numbers; Mat. Sb. **77** (1968), 423-436; English transl., p. 393–406.

[H1] N. Hirata-Kohno. – Formes linéaires de logarithmes de points algébriques sur les groupes algébriques; Invent. Math. **104** (1991), 401–433.

[H2] N. Hirata-Kohno. – Nouvelles mesures de transcendance liées aux groupes algébriques commutatifs; *Approximations Diophantiennes et Nombres Transcendants, Luminy 1990,* éd. P. Philippon, W. de Gruyter (1992), 165–172.

[H3] N. Hirata-Kohno. – Approximations simultanées sur les groupes algébriques commutatifs; Compositio Math., to appear.

[L] S. Lang. – *Number theory* 3; Encycl. of Math. Sciences, Vol. 60, Springer Verlag 1991.

[La] M. Laurent. – Linear forms in two logarithms and interpolation determinants; this volume, Appendix.

[Lo] J.H. Loxton. – Some problems involving powers of integers; Acta Arith., **46** (1986), 113–123.

[Ma] D.W. Masser. – A note on Baker's theorem; in *Recent progress in analytic number theory,* Proc. Durham 1979, Vol. 2, Academic Press (1981), 153–158.

[Ma-W] D.W. Masser and G. Wüstholz. – Estimating isogenies on elliptic curves; Invent. Math., **100** (1990), 1–24.

[Mi-W1] M. Mignotte and M. Waldschmidt. – Linear forms in two logarithms and Schneider's method; Math. Ann., **231** (1978), 241–267.

[Mi-W2] M. Mignotte and M. Waldschmidt. – Linear forms in two logarithms and Schneider's method, 2; Acta Arith., **53** (1989), 251–287.

[Mi-W3] M. Mignotte and M. Waldschmidt. – Linear forms in two logarithms and Schneider's method, 3; Ann. Fac. Sci. Toulouse, **97** (1989), 43–75.

[P-W1] P. Philippon and M. Waldschmidt. – Lower bounds for linear forms in logarithms; in: Chap. 18 of *New Advances in Transcendence Theory*, ed. A.Baker, Cambridge Univ. Press (1988), 280–312.

[P-W2] P. Philippon and M. Waldschmidt. – Formes linéaires de logarithmes simultanées sur les groupes algébriques commutatifs; Sém. Th. Nombres Paris 1986-87, Birkhäuser Verlag, Progress in Math. **75** (1989), 313–347.

[vdP] A.J. van der Poorten. – Linear forms in logarithms in the p-adic case; Chap.2 of: *Transcendence Theory: Advances and Applications*; ed. A.Baker and D.W.Masser, Academic Press (1977), 29–57.

[R] K. Ramachandra. – A note on Baker's method; J. Austral. Math. Soc., **10** (1969), 197–203.

[Rh] G. Rhin. – Approximants de Padé et mesures effectives d'irrationalité; Sém. Théor. Nombres, Paris 1986–86, Birkhäuser, Prog. in Math. **71** (1987), 155–164.

[Ri] P. Ribenboim. – *Consecutive powers*; to appear.

[S] T.N. Shorey. – On gaps between numbers with a large prime factor, 2; Acta Arith. **25** (1974), 365–373.

[W1] M. Waldschmidt. – A lower bound for linear forms in logarithms; Acta Arith., **37** (1980), 257–283.

[W2] M. Waldschmidt. – Transcendence measures for numbers connected with the exponential function J. Austral. Math. Soc., **25** (1978), 445–465.

[W3] M. Waldschmidt. – Fonctions auxiliaires et fonctionnelles analytiques; J. Analyse Math., **56** (1991), 231–279.
[W4] M. Waldschmidt. – Nouvelles méthodes pour minorer des combinaisons linéaires de logarithmes de nombres algébriques; Sém. Th. Nombres Bordeaux, **3** (1991), 129–185; (2); *Problèmes Diophantiens 1989-1990*, Publ. Univ. P. et M. Curie (Paris 6) **93**, (1991), N°8, 36p.
[W5] M. Waldschmidt. – Minorations de combinaisons linéaires de logarithmes de nombres algébriques; Canadian J. Math., to appear.
[Wü] G. Wüstholz. – A new approach to Baker's theorem on linear forms in logarithms (1); in *Diophantine approximations and transcendence theory*, Sem. Bonn 1985, Springer Lecture Notes **1290** (1987), 189–202. (2); id., 203–211. (3); in: Chap. 25 of *New Advances in Transcendence Theory*, ed. A.Baker, Cambridge Univ. Press (1988), 399–410.
[Yu] Yu Kunrui. – Linear forms in p-adic logarithms; Acta Arith., **53** (1989), 107–186; (2), Compositio Math. **74** (1990), 15–113.

13.– GENERALIZATIONS OF THE SIX EXPONENTIALS THEOREM

Baker's theorem on linear independence of logarithms over $\overline{Q}$ (Theorem 11.1) does not contain all known informations concerning the transcendence of the values of the exponential function (not mentioning results of algebraic independence); specifically, it does not contain the six exponentials theorem (Theorem 1.6). An obvious way of giving a result containing both statements (Baker's theorem and the six exponentials) would be to prove the algebraic independence of logarithms of algebraic numbers (Conjecture 14.1); this would imply the four exponentials conjecture (Conjecture 1.7). But this does look like a difficult problem, and our goal will be more modest.

The six exponentials theorem can be stated in an equivalent way as follows ; like in Chapter 1, denote by $\mathcal{L}$ the $\mathbb{Q}$-vector space of logarithms of algebraic numbers; *for $1 \le i \le d$ and $1 \le j \le \ell$, let λ_{ij} be an element of $\mathcal{L}$; assume that the ℓ columns of the matrix*

$$\big(\lambda_{ij}\big)_{1\le i\le d, 1\le j\le \ell} = \begin{pmatrix} \lambda_{11} & \dots & \lambda_{1\ell} \\ \vdots & \ddots & \vdots \\ \lambda_{d1} & \dots & \lambda_{d\ell} \end{pmatrix}$$

are linearly independent in $\mathbb{C}^d$, that the d rows of the same matrix are linearly independent in $\mathbb{C}^\ell$ and that $\ell d > \ell + d$; then the rank of the matrix is at least 2.

To check that this proposition is equivalent to the six exponentials theorem, it is sufficient to consider the case $d = 2$ and $\ell = 3$; the statement concerning the rank of the matrix implies the six exponentials theorem: indeed, if the six numbers $e^{x_i y_j}$, $(i = 1, 2,\ j = 1, 2, 3)$ are algebraic, then the matrix

$$\begin{pmatrix} x_1y_1 & x_1y_2 & x_1y_3 \\ x_2y_1 & x_2y_2 & x_2y_3 \end{pmatrix}$$

has entries in $\mathcal{L}$, the two rows are linearly independent (since x_1 and x_2 are linearly independent), the three columns also (since y_1, y_2 and y_3 are linearly independent), and the rank is 1. Conversely, if the matrix

$$\begin{pmatrix} \lambda_{11} & \lambda_{12} & \lambda_{13} \\ \lambda_{21} & \lambda_{22} & \lambda_{23} \end{pmatrix}$$

is of rank 1, if we set

$$y_j = \lambda_{1j}, \quad (j = 1, 2, 3), \qquad \text{and} \qquad x_1 = 1, \quad x_2 = \lambda_{21}/\lambda_{11},$$

then $\exp(x_i y_j) = \lambda_{ij}$ for $i = 1, 2$ and $j = 1, 2, 3$; moreover, since the matrix is of rank 1, the assumption on the linear independence of the rows (resp. of the columns) is sufficient to ensure that x_1, x_2 (resp. y_1, y_2, y_3) are linearly independent. This shows the equivalence between the six exponentials theorem and the statement on the rank of the matrix.

When the rank of the 2×3 matrix is < 2, then the three column vectors

$$\begin{pmatrix} \lambda_{11} \\ \lambda_{21} \end{pmatrix}, \quad \begin{pmatrix} \lambda_{12} \\ \lambda_{22} \end{pmatrix}, \quad \begin{pmatrix} \lambda_{13} \\ \lambda_{23} \end{pmatrix}$$

belong to a vector subspace of $\mathbb{C}^2$ of dimension 1; the six exponentials theorem says that this can happen only when the quotients $\lambda_{1j}/\lambda_{2j}$ are rational numbers, which means that the subspace containing the three vectors is spanned by a rational vector $(b_1, b_2) \in \mathbb{Q}^2$.

Michel Emsalem has noticed that this result can be extended to higher dimension thanks to the so-called *theorem of the linear subgroup*; we do not state this theorem in full generality (see [R1-4], [W1-2], [R-W]), but only the simplest consequences. Let $\mathcal{V}$ be a hyperplane of $\mathbb{C}^d$; the intersection $\mathcal{V} \cap \mathcal{L}^d$ is a vector space

over $\mathbb{Q}$; if $\mathcal{V}$ contains a non-zero rational point $(b_1, \dots, b_d) \in \mathbb{Q}^d$, then this $\mathbb{Q}$-vector space $\mathcal{V} \cap \mathcal{L}^d$ contains all the points $(b_1\lambda, \dots, b_d\lambda)$, for $\lambda \in \mathcal{L}$; therefore it is of infinite dimension. The result of M. Emsalem [E] is that the converse is true: *if $\mathcal{V}$ is a hyperplane of $\mathbb{C}^d$ for which $\mathcal{V} \cap \mathbb{Q}^d = 0$, then $\mathcal{V} \cap \mathcal{L}^d$ is a $\mathbb{Q}$-vector space of finite dimension, and this dimension is $\leq d(d-1)$.* For $d = 2$ this is just the six exponentials theorem.

A connection with Baker's theorem arises in two different ways, corresponding to the point of view of either Gel'fond-Baker or Schneider. Let us start with Schneider's approach: instead of working with points whose coordinates are logarithms of algebraic numbers, we take points whose coordinates are either algebraic numbers, or logarithms of algebraic numbers. When d_0 and d_1 are two non-negative integers with $d = d_0 + d_1 > 0$, we denote by Λ_{d_0,d_1} the product $\overline{Q}^{d_0} \times \mathcal{L}^{d_1}$. Emsalem's result (which corresponds to $d_0 = 0$, $d = d_1$) can be extended as follows: *let $\mathcal{V}$ be a vector subspace of the product $\mathbb{C}^d = \mathbb{C}^{d_0} \times \mathbb{C}^{d_1}$, satisfying*

$$\mathcal{V} \cap \left(\overline{Q}^{d_0} \times 0\right) = 0 \quad \textit{and} \quad \mathcal{V} \cap \left(0 \times \mathbb{Q}^{d_1}\right) = 0.$$

Then the $\mathbb{Q}$-vector space $\mathcal{V} \cap \Lambda_{d_0,d_1}$ is of finite dimension $\leq d_1(d-1)$.

Here is how one deduces Baker's Theorem 1.1: we consider a linear dependence relation

$$\beta_1\ell_1 + \cdots + \beta_n\ell_n = \ell_{n+1},$$

with $\beta_1, \dots, \beta_n$ algebraic and $\ell_1, \dots, \ell_{n+1}$ in $\mathcal{L}$; we assume that $\ell_1, \dots, \ell_n$ are $\overline{Q}$-linearly independent; we need only to prove that $\beta_1, \dots, \beta_n$ are all rational numbers (see exercise 1). We choose $d_0 = n$, $d_1 = 1$ and we take for $\mathcal{V}$ the hyperplane of equation $z_{n+1} = \ell_1 z_1 + \cdots + \ell_n z_n$ in $\mathbb{C}^{n+1}$; the assumption that $\ell_1, \dots, \ell_n$ linearly independent over $\overline{Q}$ implies $\mathcal{V} \cap \left(\overline{Q}^n \times 0\right) = 0$; moreover $\mathcal{V}$ contains the following points $\lambda_1, \dots, \lambda_{n+1}$ of $\overline{Q}^n \times \mathcal{L}$:

$$\lambda_i = (\delta_{i,1}, \dots, \delta_{in}, \ell_i), \quad (1 \leq i \leq n),$$

where δ_{ij} is Kronecker's symbol, and

$$\lambda_{n+1} = (\beta_1, \dots, \beta_n, \ell_{n+1}).$$

According to our result above, the vector space $\mathcal{V} \cap \left(\overline{Q}^n \times \mathcal{L}\right)$ is of dimension $\leq d_1(d-1) < n+1$, hence the points $\lambda_1, \dots, \lambda_{n+1}$ are linearly dependent over $\mathbb{Q}$, which implies that $\beta_1, \dots, \beta_n$ are all rational numbers.

Let us now take Gel'fond-Baker's point of view: the second connection with Theorem 1.1 arises by considering a hyperplane $\mathcal{V}$ which is *rational* over the field $\overline{Q}$ of algebraic numbers (see exercise 4 of Chapter 1). Theorem 1.1 can be stated in the following equivalent way:

If $\mathcal{V}$ is a hyperplane of $\mathbb{C}^d$, which is rational over $\overline{Q}$, and if $\mathcal{V} \cap \mathbb{Q}^d = 0$, then $\mathcal{V} \cap \mathcal{L}^d = 0$ (see exercise 5 of Chapter 1).

Here is another statement which contains at the same time the six exponentials theorem and Baker's Theorem 1.1:

If $\mathcal{V}$ is a hyperplane of $\mathbb{C}^d$ for which $\mathcal{V} \cap \mathbb{Q}^d = 0$, if $\mathcal{V}$ contains a vector subspace $\mathcal{W}$ of $\mathbb{C}^d$, of dimension $t \geq 0$, which is rational over $\overline{Q}$, then $\dim_{\mathbb{Q}}\left(\mathcal{V} \cap \mathcal{L}^d\right) \leq d(d-t-1)$.

Emsalem's result corresponds to $\mathcal{W} = 0$, $t = 0$, Baker's Theorem 1.1 to $\mathcal{W} = \mathcal{V}$, $t = d-1$.

We have just seen two generalizations of Emsalem's result, which both contain Baker's Theorem 1.1. We now combine them into a general result.

Theorem 13.1. – *Let d_0 and d_1 be to non-negative integers with $d = d_0 + d_1 > 0$; let $\mathcal{V}$ be a vector subspace of the product $\mathbb{C}^d = \mathbb{C}^{d_0} \times \mathbb{C}^{d_1}$, satisfying*

$$\mathcal{V} \cap \left(\overline{Q}^{d_0} \times 0\right) = 0 \quad \textit{and} \quad \mathcal{V} \cap \left(0 \times \mathbb{Q}^{d_1}\right) = 0.$$

Let $\mathcal{W}$ be a subspace of of $\mathbb{C}^d$, of dimension $t \geq 0$, which is rational over $\overline{Q}$ and contained in $\mathcal{V}$. Then the $\mathbb{Q}$-vector space $\mathcal{V} \cap \Lambda_{d_0,d_1}$ is of finite dimension $\leq d_1(d-t-1)$.

As we have seen, this result obviously contains Baker's homogeneous Theorem 1.1 in two different ways, with either $d_1 = 1$ and $t = 0$ (method of Schneider), or else $d_0 = 0$ and $t = d-1$ (method of Gel'fond-Baker). It also contains the non-homogeneous result 11.1 in two different ways: if we have a relation

$$\beta_0 + \beta_1\ell_1 + \cdots + \beta_n\ell_n = \ell_{n+1},$$

with algebraic β's and with ℓ_i in $\mathcal{L}$, then we can either
a) (Schneider's method) choose $d_0 = n+1$, $d_1 = 1$, $d = n+2$, $t = 1$, $\mathcal{V}$ is the hyperplane of equation

$$z_0 + z_1\ell_1 + \cdots + z_n\ell_n = z_{n+1}$$

and $\mathcal{W} = \mathbb{C}(1, 0, \ldots, 1)$. The intersection $\mathcal{V} \cap \Lambda_{n+1,1} = \mathcal{V} \cap \left(\overline{Q}^{n+1} \times \mathcal{L}\right)$ contains $n+1$ points $\lambda_1, \ldots, \lambda_{n+1}$:

$$\lambda_i = (0, \delta_{i,1}, \ldots, \delta_{in}, \ell_i), \quad (1 \le i \le n),$$

and

$$\lambda_{n+1} = (\beta_0, \beta_1, \ldots, \beta_n, \ell_{n+1}).$$

Since $\mathcal{V} \cap (0 \times \mathbb{Q}) = 0$, Theorem 13.1 implies either $\mathcal{V} \cap (\overline{Q}^{n+1} \times 0) \neq 0$ (which means that $1, \ell_1, \ldots, \ell_n$ are $\overline{Q}$-linearly dependent), or else $\lambda_1, \ldots, \lambda_{n+1}$ are $\mathbb{Q}$-linearly dependent (which means that $\ell_1, \ldots, \ell_{n+1}$ are $\mathbb{Q}$-linearly dependent). Thanks to exercise 1, this completes the proof of Proposition 11.1.
b) (Gel'fond-Baker method) or else take $d_0 = 1$, $d_1 = t = n+1$, $d = n+2$ and choose for $\mathcal{V} = \mathcal{W}$ the hyperplane

$$z_0 + \beta_1 z_1 + \cdots + \beta_n z_n = z_{n+1}.$$

We have

$$(\beta_0, \ell_1, \ldots, \ell_{n+1}) \in \mathcal{V} \cap \Lambda_{1,n+1} = \mathcal{V} \cap \left(\overline{Q} \times \mathcal{L}^{n+1}\right);$$

we deduce from Theorem 13.1 that either $(\beta_0, \ell_1, \ldots, \ell_{n+1}) = 0$, or $\mathcal{V} \cap (0 \times \mathbb{Q}^{n+1}) = 0$. In the later case we get a non-trivial dependence relation between $\beta_1, \ldots, \beta_n$ over $\mathbb{Q}$. From lemma 1.3, we deduce Theorem 11.1.

The next step has been achieved by D. Roy: instead of taking some coordinates in $\overline{Q}$, and some in $\mathcal{L}$, he takes coordinates in the $\overline{Q}$-vector space spanned by 1 and $\mathcal{L}$; let us denote by $\mathcal{L}_{\overline{Q}}$ this vector space:

$$\mathcal{L}_{\overline{Q}} = \{\beta_0 + \beta_1\ell_1 + \cdots + \beta_n\ell_n \,;\, n \ge 0,\, \beta_i \in \overline{Q}, \ell_i \in \mathcal{L}\}.$$

We can ask the same questions on $\mathcal{V} \cap \mathcal{L}_{\overline{Q}}$ as we asked before concerning $\mathcal{V} \cap \mathcal{L}$: when is the dimension of this $\overline{Q}$-vector space finite ? An obvious necessary condition is $\mathcal{V} \cap \overline{Q}^d = 0$; as shown by D. Roy, this condition is sufficient.

Theorem 13.2. – *If $\mathcal{V}$ is vector subspace of the product $\mathbb{C}^d = \mathbb{C}^{d_0} \times \mathbb{C}^{d_1}$, satisfying*

$$\mathcal{V} \cap \left(\overline{Q}^{d_0} \times 0\right) = 0 \quad \textit{and} \quad \mathcal{V} \cap \left(0 \times \overline{Q}^{d_1}\right) = 0,$$

then the $\overline{Q}$-vector space $\mathcal{V} \cap \left(\overline{Q}^{d_0} \times \mathcal{L}_{\overline{Q}}^{d_1}\right)$ is of finite dimension $\le d_1(d-t-1)$, where t is the dimension of the maximal vector subspace of $\mathcal{V}$ which is rational over $\overline{Q}$.

Theorems 13.1 and 13.2 are both special cases ot the above mentioned *theorem of the linear subgroup.*

1Exercises

1. Show that the statements *(i)*, *(ii)* and *(iii)* in lemma 1.3, as well as *(iv)* in exercise 3 of Chapter 1, are also equivalent to:
(v) Let n be a non-negative integer, $\ell_1, \ldots, \ell_{n+1}$ be elements of $\mathcal{M}$, and $\beta_1, \ldots, \beta_n$ elements of K. Assume $\ell_1, \ldots, \ell_n$ are K-linearly independent and

$$\beta_1\ell_1 + \cdots + \beta_n\ell_n = \ell_{n+1}.$$

Then $\beta_1, \ldots, \beta_n$ are all in k.

2. Deduce from Theorem 13.1 the *five exponentials theorem*: *if x_1, x_2 (resp. y_1, y_2) are $\mathbb{Q}$-linearly independent complex numbers, then one at least of the five numbers*

$$e^{x_1y_1},\ e^{x_1y_2},\ e^{x_2y_1},\ e^{x_2y_2},\ e^{x_1/x_2},$$

is transcendental.

3. Deduce from Theorem 13.2 the *strong six exponentials theorem*: *if x_1, x_2 (resp. y_1, y_2, y_3) are $\overline{Q}$-linearly independent complex numbers, then one at least of the six numbers*

$$x_1y_1,\ x_1y_2,\ x_1y_3,\ x_2y_1,\ x_2y_2, x_2y_3,$$

does not belong to $\mathcal{L}_{\overline{Q}}$.

Deduce also the five exponentials theorem from this statement.

4.

a) Let G be a subgroup of $\mathbb{R}^d$. Show that the following properties are equivalent.

(i) There exists a finitely generated subgroup of G which is dense in $\mathbb{R}^d$.

(ii) For each hyperplane $\mathcal{V}$ of $\mathbb{R}^d$, the lower bound $\mathrm{rk}_{\mathbb{Z}}\big((G+\mathcal{V})/\mathcal{V}\big) \geq 2$ holds.

(iii) For each vector subspace $\mathcal{V}$ of $\mathbb{R}^d$ with $\mathcal{V} \neq \mathbb{R}^d$, the lower bound $\mathrm{rk}_{\mathbb{Z}}\big((G+\mathcal{V})/\mathcal{V}\big) > \dim_{\mathbb{R}}\big(\mathbb{R}^d/\mathcal{V}\big)$ holds.

b) Let ℓ and d be positive integers with $\ell > d^2 - d + 1$. Let α_{ij}, $(1 \leq i \leq d,\ 1 \leq j \leq \ell)$ be multiplicatively independent positive real algebraic numbers. Denote by $\mathbb{R}_+^*$ the multiplicative group of positive real numbers, and by A the multiplicative subgroup of $(\mathbb{R}_+^*)^d$ which is spanned by $\alpha_1, \ldots, \alpha_\ell$, with $\alpha_j = (\alpha_{1j}, \ldots, \alpha_{dj})$:

$$A = \left\{ \left(\prod_{j=1}^{\ell} \alpha_{1j}^{s_j}, \ldots, \prod_{j=1}^{\ell} \alpha_{dj}^{s_j} \right) ;\ \underline{s} = (s_1, \ldots, s_\ell) \in \mathbb{Z}^\ell \right\}.$$

Prove that A is dense in $(\mathbb{R}_+^*)^d$.

`Hint.` *Let G be the subgroup of $\mathbb{R}^d$ which is spanned by $\lambda_1, \ldots, \lambda_\ell$, with*

$$\lambda_j = (\log \alpha_{1j}, \ldots, \log \alpha_{dj}), \quad (1 \leq j \leq \ell).$$

Using Theorem 13.1*, show that for each hyperplane $\mathcal{V}$ of $\mathbb{R}^d$, $\mathrm{rk}_{\mathbb{Z}}\big((G+\mathcal{V})/\mathcal{V}\big) \geq \ell - d(d-1)$; deduce from* a) *that G is dense in $\mathbb{R}^d$, and conclude.*

1 References

[E] M. Emsalem. – Sur les idéaux dont l'image par l'application d'Artin dans une $\mathbb{Z}_p$-extension est triviale; J. reine angew. Math., **382** (1987), 181–198.

[R1] D. Roy. – Sur la conjecture de Schanuel pour les logarithmes de nombres algébriques; *Groupe d'Etudes sur les Problèmes Diophantiens* 1988-1989, Publ. Math. Univ. P. et M. Curie (Paris 6), **90**, N° 6, 12 p.

[R2] D. Roy. – Matrices dont les coefficients sont des formes linéaires de logarithmes; Sém. Théorie Nombres Paris (1987-88), Birkhäuser Verlag, Progress in Math. **81** (1990), 273–281.

[R3] D. Roy. – Matrices whose coefficients are linear forms in logarithms, J. Number Theory, **41** (1992), 22–47.

[R4] D. Roy. – Transcendance et questions de répartition dans les groupes algébriques, *Approximations Diophantiennes et Nombres Transcendants, Luminy 1990*, éd. P. Philippon, W. de Gruyter (1992), 249–274.

[R-W] D. Roy et M. Waldschmidt. – Autour du théorème du sous-groupe algébrique; Canadian Bull. Math., to appear.

[W1] M. Waldschmidt. – On the transcendence methods of Gel'fond and Schneider in several variables; in *New Advances in transcendence theory*, ed. A. Baker, Cambridge Univ. Press (1988), 375–398.

[W2] M. Waldschmidt. – Dependence of logarithms of algebraic points; Coll. Math. Soc. János Bolyai, **51** (1987), 1013-1035.

14.– CONJECTURES

The main conjecture for this subject is:

Conjecture 14.1. – *Let $\ell_1, \dots, \ell_m$ be $\mathbb{Q}$-linearly independent logarithms of algebraic numbers. Then $\ell_1, \dots, \ell_m$ are algebraically independent.*

This means that a non-zero polynomial with rational (or even algebraic) coefficients in m unknowns cannot vanish at the point $(\ell_1, \dots, \ell_m)$. This conjecture has been stated explicitly by A.O. Gel'fond [G]. So far, it is not yet known whether there exist two algebraically independent logarithms of algebraic numbers. Only the case of linear polynomials (with algebraic coefficients) is solved, by Baker. For polynomials of degree 2, very partial results are known (strong six exponentials theorem).

There are two extensions of Conjecture 14.1: the first one in the direction of transcendental number theory [L1], the other for Diophantine approximations [L2]. Here is the first one, which is known for containing any *reasonable* transcendence conjecture dealing with values of the exponential function.

Conjecture 14.2 (Schanuel). – *Let $x_1, \dots, x_m$ be $\mathbb{Q}$-linearly independent complex numbers. Then m at least of the $2m$ numbers $x_1, \dots, x_m, e^{x_1}, \dots, e^{x_m}$ are algebraically independent.*

This means that the transcendence degree over $\mathbb{Q}$ of the field

$$\mathbb{Q}\big(x_1, \dots, x_m, e^{x_1}, \dots, e^{x_m}\big)$$

should be at least m. Conjecture 14.1 is a special case of Schanuel's conjecture (when the m numbers $\exp(x_i)$ are algebraic); another special case is Lindemann-Weierstrass theorem (which corresponds to the case where $x_1, \dots, x_m$ are algebraic).

Another kind of open problems deals with measures of linear independence; the strongest conjectures are stated in [L2]. Here is one example (Conjecture 2 p.213 of [L2]).

Conjecture 14.3. – *Let ϵ be a positive real number. There exists a constant $C(\epsilon) > 0$ satisfying the following property. Let $a_1, \dots, a_m$ be positive integers and $b_1, \dots, b_m$ be non-zero rational integers. Define*

$$B = \max\{|b_1|, \dots, |b_m|\}.$$

Assume that the number $\Lambda = b_1 \log a_1 + \cdots + b_m \log a_m$ does not vanish. Then

$$|\Lambda| \geq \frac{C(\epsilon)^m B}{(|b_1| \cdots |b_m|\ a_1 \cdots a_m)^{1+\epsilon}}.$$

One can formulate an explicit version of Schanuel's conjecture; it has been pointed out to me that the suggestion in [W] is not the right one, in view of Bijlsma's counterexamples [B]. The following might be more reasonable: we add a hypothesis which is a measure of linear independence of the x_i; it's interesting to notice that the known results of algebraic independence for *large transcendence degrees* involve so far such a *technical hypothesis*.

Conjecture 14.4. – *Let $x_1, \dots, x_m$ be $\mathbb{Q}$-linearly independent complex numbers. Assume that there exists a constant $\kappa > 0$ such that, for all $S \geq 2$ and all $\underline{s} = (s_1, \dots, s_m) \in \mathbb{Z}^m(S)$,*

$$|s_1 x_1 + \cdots + s_m x_m| > S^{-\kappa}.$$

Let d be a positive integer. Then there exists a constant $C > 0$, depending on $x_1, \dots, x_m$ and d (and also on κ) such that, for all $P_1, \dots, P_{m+1}$ polynomials in $\mathbb{Z}[X_1, \dots, X_m, Y_1, \dots, Y_m]$ of degree $\leq d$ generating an

ideal of rank $m+1$, if $H_j \geq e$ is an upper bound for the absolute values of the coefficients of P_j, $(1 \leq j \leq m)$, then

$$\sum_{j=1}^{m+1} \left|P_j\big(x_1, \ldots, x_m, e^{x_1}, \ldots, e^{x_m}\big)\right| \cdot H_j^C \geq 1/C.$$

Finally, in connection with Chapter 13, we mention some very interesting results by D. Roy [R1], [R2]; he shows in particular that Schanuel's conjecture is equivalent to a conjecture on the rank of matrices whose entries are logarithms of algebraic numbers.

1Exercises **1.** Deduce the following consequences from Conjecture 14.1. Let $\mathcal{V}$ be a vector subspace of $\mathbb{C}^d$.
a) Assume $\mathcal{V} \cap \mathbb{Q}^d = 0$; then $\dim_{\mathbb{Q}} \mathcal{V} \cap \mathcal{L}^d \leq d(d-1)/2$.
b) Assume $\mathcal{V} \cap \overline{Q}^d = 0$; then $\dim_{\overline{Q}} \mathcal{V} \cap \mathcal{L}^d_{\overline{Q}} \leq d(d-1)/2$.
c) *Strong four exponentials conjecture.* Let x_1, x_2 be $\overline{Q}$-linearly independent complex numbers, and let y_1, y_2 be also $\overline{Q}$-linearly independent complex numbers. Then one at least of the four numbers

$$x_1y_1, \quad x_1y_2, \quad x_2y_1, \quad x_2y_2$$

does not belong to $\mathcal{L}_{\overline{Q}}$.
`Hint.` *See* [R2].

2. Deduce from Conjecture 14.3 an effective version of *Pillai's conjecture* : For each $\epsilon > 0$ there exists a positive number $C(\epsilon) > 0$ with the following property; let x, y, p and q be integers, all of which are ≥ 2, such that $x^p \neq y^q$; then

$$|x^p - y^q| \geq C(\epsilon) \max\big\{x^p, y^q\big\}^{1-(1/p)-(1/q)-\epsilon}.$$

`Hint.` *See* [L2] *Introduction to Chapters* 10 and 11.

3. Deduce from Conjecture 14.4 the following *measure of algebraic independence for logarithms of algebraic numbers*. Let $\ell_1, \ldots, \ell_m$ be $\mathbb{Q}$-linearly independent elements of $\mathcal{L}$ and let d be a positive integer. There exists a positive number c such that for any non-zero polynomial $P \in \mathbb{Z}[X_1, \ldots, X_m]$ of degree at most d, the lower bound

$$|P(\ell_1, \ldots, \ell_m)| \geq H^{-c}$$

holds with $H = \max\{H(P), 2\}$.

1References

[B] A. Bijlsma. – On the simultaneous approximations of a, b and a^b; Compos. Math., **35** (1977), 99–111.
[G] A.O. Gel'fond. – *Transcendental Number Theory;* Moscow, 1952; English transl. Dover Publ., N.Y., 1960.
[L1] S. Lang. – *Introduction to Transcendental Numbers;* Addison-Wesley 1966.
[L2] S. Lang. – *Elliptic curves Diophantine analysis;* Springer-Verlag, Grund. der Math. Wiss., **231** (1978).
[R1] D. Roy. – Matrices dont les coefficients sont des formes linéaires; Sém. Théorie des Nombres Paris (1987/88), Birkhäuser Progress in Math. **81** (1990), 273–281.
[R2] D. Roy. – Sur la conjecture de Schanuel pour les logarithmes de nombres algébriques; *Groupe d'Etudes sur les Problèmes Diophantiens* 1988-1989, Publ. Math. Univ. P. et M. Curie (Paris 6), **90**, N° 6, 12 p.
[W] M. Waldschmidt. – Algebraic independence of transcendental numbers – Gel'fond's method and its developments; in *Perspective in Mathematics,* (Anniversary Oberwolfach), Birkhäuser Verlag 1984, 551–571.

LINEAR FORMS IN TWO LOGARITHMS AND INTERPOLATION DETERMINANTS

by Michel Laurent

1 Introduction This appendix is an expanded version of the manuscript quoted in the preceding chapters. Our aim is to test numerically the new method of interpolation determinants in the context of linear forms in two logarithms. In the recent past years, M. Mignotte and M. Waldschmidt have used Schneider's construction, in a serie of papers [2],[3],[4], to get lower bounds for such a linear form with rational integer coefficients. They got relatively precise results with a numerical constant around a few hundreds. Here we shall take again Schneider's method in the frame of interpolation determinants. We shall decrease this constant to less than one hundred, when the logarithms involved are real numbers. Theorems 1 and 2 are simple corollaries of our main result which is Theorem 3. At first glance, the statement of Theorem 3 seems to be a bit complicated, but it is much more precise than the above mentioned corollaries, which are only examples of applications. Let us also mention that we have been lead in §3 to some technical lemmas which can reveal useful in some other situations from transcendence number theory. I would like to thank Dong Ping Ping to have detected some inaccuracies in a first writing of this text.

1 Statement of the results Let α_1 and α_2 be two real algebraic numbers which are supposed to be ≥ 1 and multiplicatively independent. We shall give lower bounds for the linear form

$$\Lambda = b_2 \log \alpha_2 - b_1 \log \alpha_1,$$

where b_1 and b_2 are rational integers which can be supposed to be ≥ 1 without loss of generality. Denote by D the degree over $\mathbf{Q}$ of the number field $\mathbf{Q}(\alpha_1, \alpha_2)$, and let a_1, a_2 be two real numbers > 1 such that

$$\mathrm{h}(\alpha_i) \leq \log a_i, \qquad (i = 1, 2),$$

where $\mathrm{h}(\alpha)$ means the logarithmic absolute height of the algebraic number α, as defined in Chapter 3.

For each couple of integers $b_1 \geq 1$, $b_2 \geq 1$, denote

$$b' = \frac{b_1}{D \log a_2} + \frac{b_2}{D \log a_1}.$$

Our first result gives the asymptotical value of the constant when b' tends to infinity.

Theorem 1. *For each number $c > 48$, there exists a number $b'(c)$ such that*

$$\log |\Lambda| \geq -cD^4 \big(\log b'\big)^2 \log a_1 \log a_2$$

for each couple of integers $b_1 \geq 1$, $b_2 \geq 1$ with $b' \geq b'(c)$.

We can of course compute effectively such a constant $b'(c)$ in term of c. Here is a concrete example.

Theorem 2. *Suppose that $\log a_1 \geq 1$, $\log a_2 \geq 1$ and $\log b' \geq 25$. Then*

$$\log |\Lambda| \geq -87D^4 \big(0.5 + \log b'\big)^2 \log a_1 \log a_2.$$

Our main result is the following

Theorem 3. *Let K be an integer ≥ 2, let L, R_1, R_2, S_1, S_2 be integers ≥ 1 and let ρ be a real number ≥ 1. Suppose that*

$$R_1S_1 \geq \max(K, L), \qquad R_2S_2 \geq 2KL. \tag{1}$$

Denote

$$R = R_1 + R_2 - 1, \quad S = S_1 + S_2 - 1, \quad \gamma = RS/KL,$$
$$g = \frac{1}{4} - \frac{1}{12\gamma} + \max\left(\frac{1}{4\gamma L^2}, \frac{\gamma}{4LR^2}, \frac{\gamma}{4LS^2}\right).$$

For integers $b_1 \geq 1$, $b_2 \geq 1$, call

$$b = \big((R-1)b_2 + (S-1)b_1\big)\left(\prod_{k=1}^{K-1} k!\right)^{-2/(K^2-K)}.$$

Suppose now that α_1 and α_2 are multiplicatively independent, that the numbers $rb_2 + sb_1$, $(0 \leq r \leq R-1$, $0 \leq s \leq S-1)$, are pairwise distinct, and that we have

$$\begin{aligned} K(L-1)\log\rho + (K-3)\log 2 > {} & 2D\log(KL) + D(K-1)\log b \\ & + gL\Big((\rho-1)\big(R\log\alpha_1 + S\log\alpha_2\big) + 2D\big(R\log a_1 + S\log a_2\big)\Big). \end{aligned} \tag{2}$$

Then we have the lower bound

$$|\Lambda'| \geq \rho^{-KL + (1/2)},$$

where

$$\Lambda' = \Lambda \max\left(\frac{LSe^{LS|\Lambda|/(2b_2)}}{2b_2}, \frac{LRe^{LR|\Lambda|/(2b_1)}}{2b_1}\right).$$

Theorems 1 and 2 will be deduced from Theorem 3 by plugging the inequalities:

$$\alpha_i \leq a_i^D, \qquad (i = 1, 2),$$

in condition (2) for specific values of the parameters K, L, R_1, R_2, S_1, S_2 and ρ.

1 Technical lemmas We shall have to investigate the determinant of a matrix whose entries are monomials in α_1 and α_2. It is crucial to know what sort of monomials appears in the expansion of this determinant. To that purpose, we shall use some combinatorial results which have been gathered in this part because their statements are independent from the original problem.

Lemma 1. *Let K, S and N be integers ≥ 1. We have*

$$\sum_{\nu=1}^{N}\left(\left[\frac{\nu-1}{K}\right]+1\right)\left(\left[\frac{N-\nu}{S}\right]+1\right) \geq \frac{N(2N^2+3KN+3SN+3KS+1)}{12KS}.$$

Proof. Denote by E the sum appearing on the left hand side of the inequality. We shall decompose E into subsums corresponding to the congruence classes for the summation index ν modulo K and S successively.

If ν is congruent to k modulo K, where $1 \leq k \leq K$, then $\big[(\nu-1)/K\big] = (\nu-k)/K$, so that we can write

$$E = \frac{1}{K}\left(\sum_{\nu=1}^{N}\nu a_\nu\right) + \frac{1}{K}\left(\sum_{k=1}^{K}(K-k)S_k\right),$$

where we have denoted

$$a_\nu = \left[\frac{N-\nu}{S}\right] + 1, \qquad S_k = \sum_\nu a_\nu,$$

and where the summation index ν is congruent to k modulo K in the sum S_k.
Let us now remark that the sequence $\big(a_\nu\big)_{1\le\nu\le N}$ is non-increasing, so that the sequence $\big(S_k\big)_{1\le k\le K}$ of the partial sums is also non-increasing. By Abel's summation, we get

$$\sum_{k=1}^{K}(K-k)S_k = \sum_{k=1}^{K-1}\sum_{j=1}^{k} S_j \ge \sum_{k=1}^{K-1} kS_k,$$

from which it follows that

$$\sum_{k=1}^{K}(K-k)S_k \ge \frac{K}{2}\sum_{k=1}^{K-1} S_k \ge \frac{K-1}{2}\sum_{k=1}^{K} S_k$$

the last term being equal to $\big((K-1)/2\big)\left(\sum_{\nu=1}^{N} a_\nu\right)$. In this first step, we have got the lower bound

$$E \ge \frac{1}{K}\sum_{\nu=1}^{N}\left(\nu+\frac{K-1}{2}\right)\left(\left[\frac{N-\nu}{S}\right]+1\right) = \frac{1}{K}\sum_{\nu=1}^{N}\left(\left[\frac{\nu-1}{S}\right]+1\right)b_\nu,$$

where we have denoted $b_\nu = N-\nu+\big((K+1)/2\big)$, $(1\le\nu\le N)$. The sequence $\big(b_\nu\big)_{1\le\nu\le N}$ is also non-increasing. The same argument, with K replaced by S and the sequence $\big(a_\nu\big)$ replaced by the sequence $\big(b_\nu\big)$, provides us the lower bound

$$\sum_{\nu=1}^{N}\left(\left[\frac{\nu-1}{S}\right]+1\right)b_\nu \ge \frac{1}{S}\sum_{\nu=1}^{N}\left(\nu+\frac{S-1}{2}\right)b_\nu,$$

from which it follows that

$$E \ge \frac{1}{KS}\sum_{\nu=1}^{N}\left(\nu+\frac{S-1}{2}\right)\left(N-\nu+1+\frac{K-1}{2}\right).$$

But the last sum is elementarily seen to be equal to

$$\frac{N\left(2N^2+3KN+3SN+3KS+1\right)}{12},$$

and the lemma is proven.

The next lemma is also computational.

Lemma 2. *Let N and S be natural integers. Then we have*

$$\sum_{\nu=1}^{N}\left[\frac{\nu-1}{S}\right] \le \frac{(2N-S)^2}{8S}.$$

Proof. Denote by F the sum on the left hand side. If $N\le S$, the sum F is equal to zero while the right hand side of the inequality is ≥ 0. Suppose now that $N>S$. By Euclidean division, we can write $N=(a+1)S+b$, $(1\le b\le S,\ a\ge 0)$. Then we have

$$\begin{aligned} F &= \sum_{\nu=1}^{(a+1)S}\left[\frac{\nu-1}{S}\right] + \sum_{\nu=(a+1)S+1}^{N}(a+1) \\ &= \frac{S(a^2+a)}{2} + (a+1)b = \frac{N^2-SN+b(S-b)}{2S} \\ &\le \frac{N^2}{2S} - \frac{N}{2} + \frac{S}{8}, \end{aligned}$$

because b is located between 1 and S.

Let K and L be integers ≥ 1, and let $N = KL$. Denote

$$\ell_\nu = \left[\frac{\nu - 1}{K}\right], \qquad (1 \leq \nu \leq N),$$

so that the sequence $(\ell)_{1\leq\nu\leq N}$ is nothing else that the sequence of integers $(0, \ldots, L-1)$, repeated K times and classified by increasing order. The next lemma will be directly used to estimate our determinants.

Lemma 3. *Furthermore let R and S be integers ≥ 1. For each sequence $(r_1, \ldots, r_N)$ of integers between 0 and $R-1$, and such that any given integer is repeated at most S times in the sequence, we have the estimate*

$$M - G \leq \sum_{\nu=1}^{N} \ell_\nu r_\nu \leq M + G,$$

where

$$M = \frac{(L-1)(r_1 + \cdots + r_N)}{2},$$
$$G = \frac{NLR}{2}\left(\frac{1}{4} - \frac{1}{12\gamma} + \epsilon\right),$$
$$\gamma = \frac{RS}{KL}, \quad \epsilon = \max\left(\frac{1}{4\gamma L^2}, \quad \frac{\gamma}{4LR^2}\right).$$

Proof. In other words, the problem is to estimate the oscillation of the sum

$$\sigma = \sum_{\nu=1}^{N} \left(\ell_\nu - \frac{L-1}{2}\right) r_\nu,$$

when $(r_1, \ldots, r_N)$ runs over the set of sequences of N integers, with value between 0 and $R-1$, such that a given integer appears at most S times. Let us first remark that in the sum σ the terms whose index ν lies between 1 and $(N+1)/2$ are ≤ 0, while those with index $(N+1)/2 \leq \nu \leq N$ are ≥ 0. The symmetry

$$\ell_{N-\nu+1} + \ell_\nu = L - 1, \qquad (1 \leq \nu \leq N),$$

allows us to write σ in the form:

$$\sigma = -\sum_{(N+1)/2\leq\nu\leq N} \left(\ell_\nu - \frac{L-1}{2}\right) r_{N-\nu+1} + \sum_{(N+1)/2\leq\nu\leq N} \left(\ell_\nu - \frac{L-1}{2}\right) r_\nu.$$

To precise the values of the above sums, we have to distinguish two cases, according to the parity of L.
i) Suppose that L is odd.
Denote $N' = K(L-1)/2$. In this case we have

$$\sum_{(N+1)/2\leq\nu\leq N} \left(\ell_\nu - \frac{L-1}{2}\right) r_\nu = \sum_{\nu=1}^{N'} \left(\left[\frac{\nu-1}{K}\right] + 1\right) r_{N'+K+\nu},$$

and σ is the difference of two numbers of the shape

$$\beta = \sum_{\nu=1}^{N'} \left(\left[\frac{\nu-1}{K}\right] + 1\right) b_\nu,$$

where $(b_1, \ldots, b_{N'})$ denotes a sequence of N' integers between 0 and $R-1$ such that each value appears at most S times. It follows that

$$-\max(\beta) + \min(\beta) \leq \sigma \leq \max(\beta) - \min(\beta).$$

The substitution $b_\nu \mapsto R - 1 - b_\nu$ shows that

$$\begin{aligned}\max(\beta) + \min(\beta) &= (R-1)\sum_{\nu=1}^{N'} \left(\left[\frac{\nu-1}{K} \right] + 1 \right) \\ &= \frac{1}{8}(R-1)K(L^2-1),\end{aligned}$$

from which follows the upper bound

$$|\sigma| \leq \frac{(R-1)K(L^2-1)}{8} - 2\min(\beta).$$

We have to find the value $\min(\beta)$. Let us show that

$$\min(\beta) = \sum_{\nu=1}^{N'} \left(\left[\frac{\nu-1}{K} \right] + 1 \right) \left[\frac{N'-\nu}{S} \right],$$

that is to say that the minimal value is reached for the sequence $b_\nu = \big[(N'-\nu)/S\big]$, $(1 \leq \nu \leq N')$. Let us first remark that for each minimal sequence $\big(b_\nu\big)$, we have $b_i \geq b_j$ whenever $\big[(i-1)/K\big] < \big[(j-1)/K\big]$. Indeed, if we denote by (b'_ν) the sequence deduced from $\big(b_\nu\big)$ by permuting b_i and b_j, we have

$$\sum_{\nu=1}^{N'} \left(\left[\frac{\nu-1}{K} \right] + 1 \right) (b'_\nu - b_\nu) = \left(\left[\frac{j-1}{K} \right] - \left[\frac{i-1}{K} \right] \right) (b_i - b_j)$$

which must be ≥ 0 by the minimal property of (b_ν). As the value of the sum

$$\sum_{\nu=1}^{N'} \left(\left[\frac{\nu-1}{K} \right] + 1 \right) b_\nu$$

is invariant by substitution in each block $(b_1, \ldots, b_K)$, $(b_{K+1}, \ldots, b_{2K}), \ldots$, we may suppose without restriction that the sequence $\big(b_\nu\big)$ is non-increasing. By minimality, it is then clear that the S last values $b_{N'}, \ldots, b_{N'-S+1}$ are necessarily equal to zero, the S preceding ones are equal to one, and so on. In other terms, we have $b_\nu = \big[(N'-\nu)/S\big]$ for $1 \leq \nu \leq N'$. We have proven the upper bound:

$$\begin{aligned}|\sigma| \leq \frac{(R-1)K(L^2-1)}{8} \\ -2\sum_{\nu=1}^{N'} \left(\left[\frac{\nu-1}{K} \right] + 1 \right) \left(\left[\frac{N'-\nu}{S} \right] + 1 \right) + 2\sum_{\nu=1}^{N'} \left(\left[\frac{\nu-1}{K} \right] + 1 \right).\end{aligned}$$

The second sum in the right hand side of the above inequality is equal to $K(L^2-1)/8$, while lemma 1, with N replaced by N', gives us the lower bound

$$\begin{aligned}\frac{K(L-1)}{24KS} \left(\frac{K^2(L-1)^2}{2} + \frac{3K^2(L-1)}{2} + \frac{3KS(L+1)}{2} + 1 \right) \geq \\ \frac{1}{48S} \big(K^2(L^3 - 3L + 2) + 3KS(L^2-1) \big)\end{aligned}$$

for the sum in the mid term. Putting altogether and using the trivial estimate

$$\frac{(R-1)K(L^2-1)}{8} \leq \frac{RKL^2}{8} - \frac{K(L^2-1)}{8},$$

we finally get

$$|\sigma| \leq \frac{RKL^2}{8} - \frac{K^2L^3}{24S} + \frac{K^2L}{8S} - \frac{K^2}{12S}.$$

Neglecting the last term, we can write

$$|\sigma| \leq \frac{NLR}{2}\left(\frac{1}{4} - \frac{1}{12\gamma} + \frac{1}{4\gamma L^2}\right) \leq G.$$

ii) Suppose now that L is even.

Then we denote $N' = KL/2 = N/2$. In this case, we have

$$\sum_{(N+1)/2 \leq \nu \leq N} \left(\ell_\nu - \frac{L-1}{2}\right) r_\nu = \sum_{\nu=1}^{N'} \left(\left[\frac{\nu-1}{K}\right] + \frac{1}{2}\right) r_{\nu+N'}.$$

The proof runs along the same line, with sums of the shape

$$\beta = \sum_{\nu=1}^{N'} \left(\left[\frac{\nu-1}{K}\right] + \frac{1}{2}\right) b_\nu,$$

for which, with corresponding notations, we obtain the upper bound

$$|\sigma| \leq (R-1)\left(\sum_{\nu=1}^{N'} \left(\left[\frac{\nu-1}{K}\right] + \frac{1}{2}\right)\right) - 2\sum_{\nu=1}^{N'} \left(\left[\frac{\nu-1}{K}\right] + \frac{1}{2}\right)\left[\frac{N'-\nu}{S}\right].$$

The right term of this inequality is better written as equal to

$$\frac{(R+1)KL^2}{8} - 2\sum_{\nu=1}^{N'} \left(\left[\frac{\nu-1}{K}\right] + 1\right)\left(\left[\frac{N'-\nu}{S}\right] + 1\right) + \sum_{\nu=1}^{N'} \left(\left[\frac{\nu-1}{S}\right] + 1\right).$$

In the same way, using lemma 1 and 2, we get finally

$$|\sigma| \leq \frac{RKL^2}{8} - \frac{K^2L^3}{24S} - \frac{L}{12S} + \frac{S}{8} = \frac{NLR}{2}\left(\frac{1}{4} - \frac{1}{12\gamma} - \frac{1}{6\gamma K^2L^2} + \frac{\gamma}{4LR^2}\right).$$

Neglecting the third term, we obtain $|\sigma| \leq G$.

Remark. The upper bound $|\sigma| \leq NLR/8$ can be proven very easily in the following way. We write

$$\sigma = \sum_{\nu=1}^{N} \left(\ell_\nu - \frac{L-1}{2}\right) r_\nu = \sum_{\nu=1}^{N} \left(\ell_\nu - \frac{L-1}{2}\right)(r_\nu - \eta)$$

for each complex number η, because the average value of the sequence $\left(\ell_\nu\right)_{1\leq\nu\leq N}$ is $(L-1)/2$. Choosing the center $\eta = (R-1)/2$ and bounding $|r_\nu - \eta| \leq (R-1)/2$, we get

$$|\sigma| \leq \frac{R-1}{2} \sum_{\nu=1}^{N} \left|\ell_\nu - \frac{L-1}{2}\right|.$$

If we suppose for instance L odd, the last sum is easily seen to be $K(L^2-1)/4$. We get

$$|\sigma| \le \frac{K(R-1)(L^2-1)}{8} \le \frac{NLR}{8}.$$

Idem for L even. The lemmas 1 and 2 have the effect to substract $1/(24\gamma)$ to $1/8$.

1 Zero estimate Let K, L, R_1, R_2, S_1, S_2 be integers ≥ 1. As in Theorem 3, put

$$R = R_1 + R_2 - 1, \qquad S = S_1 + S_2 - 1.$$

Let b_1 and b_2 be two complex numbers. For positive integers n and p, denote as usual $\binom{n}{p} = n\cdots(n-p+1)/p!$ the binomial coefficient, and denote by A the $KL \times RS$ matrix whose entries are the numbers

$$\binom{rb_2 + sb_1}{k} \alpha_1^{\ell r} \alpha_2^{\ell s},$$

where (k,ℓ), $(0 \le k \le K-1,\ 0 \le \ell \le L-1)$ is the index of row, while (r,s), $(0 \le r \le R-1,\ 0 \le s \le S-1)$ is the index of column. It will be convenient to number the lines by setting

$$k_i = \left[\frac{i-1}{L}\right], \quad \ell_i = \left[\frac{i-1}{K}\right], \qquad (1 \le i \le KL).$$

The order of the columns is irrelevant. Various zero estimates can show us that under suitables conditions, the matrix A is of maximal rank. Here is an example.

Lemma 4. *Suppose that conditions*

$$R_1 S_1 \ge \max(K, L), \qquad R_2 S_2 \ge 2KL, \tag{1}$$

hold. Suppose also that the numbers α_1 and α_2 are multiplicatively independent and that the RS numbers $rb_2 + sb_1$, $(0 \le r \le R-1,\ 0 \le s \le S-1)$, are all distinct. Then the rank of the matrix A is equal to KL.

Proof. We have to show that the KL lines of A are linearly independent. If not, there would exist a non-zero polynomial $P[X,Y]$, with degree in X bounded by $K-1$ and degree in Y bounded by $L-1$, vanishing at the points

$$(rb_2 + sb_1, \alpha_1^r \alpha_2^s), \qquad (0 \le r \le R-1,\ 0 \le s \le S-1).$$

Now proposition 4.1 from [3] tells us that the assumptions of the lemma cannot be fulfilled. Notice that our hypotheses are stronger than those of proposition 4.1, and that the strict inequalities $(a),(b),(c)$ in this proposition become the large inequalities (1), because of a shift by one for the degrees. Of course, a suspicious reader could object that the set of points we consider, is not the same as in proposition 4.1. One can answer that, first when R_1, R_2, S_1, S_2 are odd, the two sets of points differ by a translation in $\mathbf{G}_a \times \mathbf{G}_m$, and secondly that if one of the parameters is even, the proof runs along the same lines!

1 Arithmetical lower bounds for minors from A

From now on, we begin the proof of Theorem 3. So we have five parameters K, L, R_1, R_2, S_1, S_2 satisfying (1) and integers $b_1 \ge 1, b_2 \ge 1$ which are almost linearly independent in the sense that the numbers $rb_2 + sb_1$, $(0 \le r \le R-1,\ 0 \le s \le S-1)$ are pairwise distinct. By lemma 4, the matrix A associated to this set of data, is of maximal rank $N := KL$. Let Δ be a non-zero minor of order $N \times N$ from the matrix A. For a suitable ordering on the set of columns contained in Δ, we can write

$$\Delta = \det\left(\binom{r_j b_2 + s_j b_1}{k_i} \alpha_1^{\ell_i r_j} \alpha_2^{\ell_i s_j}\right)_{1 \le i,j \le N}.$$

The aim of this section is to prove the following lower bound for $|\Delta|$.

Lemma 5. *Denote*

$$\begin{aligned} g &= \frac{1}{4} - \frac{1}{12\gamma} + \max\left(\frac{1}{4\gamma L^2},\ \frac{\gamma}{4LR^2},\ \frac{\gamma}{4LS^2}\right), \\ G_1 &= gLRN/2, \qquad G_2 = gLSN/2, \\ M_1 &= (L-1)(r_1+\cdots+r_N)/2, \qquad M_2 = (L-1)(s_1+\cdots+s_N)/2. \end{aligned}$$

Then we have

$$\log|\Delta| \geq -(D-1)\log(N!) + (M_1+G_1)\log\alpha_1 + (M_2+G_2)\log\alpha_2 \\ -2DG_1\log a_1 - 2DG_2\log a_2 - \frac{1}{2}(D-1)(K-1)N\log b.$$

(Recall that we have defined

$$b = \left((R-1)b_2 + (S-1)b_1\right)\left(\prod_{k=1}^{K-1} k!\right)^{-2/(K^2-K)}).$$

Proof. Let us consider the polynomial

$$P(X,Y) = \sum_{\sigma} \mathrm{sg}(\sigma) \prod_{i=1}^{N} \binom{r_{\sigma(i)}b_2 + s_{\sigma(i)}b_1}{k_i} X^{\sum_{i=1}^N \ell_i r_{\sigma(i)}} Y^{\sum_{i=1}^N \ell_i s_{\sigma(i)}},$$

where σ runs over the symmetric group $\mathcal{S}_N$, and $\mathrm{sg}(\sigma)$ means the signature of the substitution σ. By expanding the determinant Δ, we get $\Delta = P(\alpha_1, \alpha_2)$. As

$$\binom{r_j b_2 + s_j b_1}{k_i} \leq \frac{\left((R-1)b_2 + (S-1)b_1\right)^{k_i}}{k_i!}, \qquad (1 \leq i \leq N), \\ \sum_{i=1}^{N} k_i = (K-1)N/2,$$

we easily see that the *length* $L(P)$ of the polynomial P is bounded by

$$\frac{N!\left((R-1)b_2 + (S-1)b_1\right)^{(K-1)N/2}}{\prod_{i=1}^N k_i!} = N! b^{(K-1)N/2}.$$

To get a good lower bound for $|\Delta|$, we have to notice that P is divisible by a large power of X and Y. In a precise way, lemma 3 gives us the estimates

$$M_1 - G_1 \leq \sum \ell_i r_{\sigma(i)} \leq M_1 + G_1,$$

$$M_2 - G_2 \leq \sum \ell_i s_{\sigma(i)} \leq M_2 + G_2.$$

Let us denote by V_1 (resp. V_2) the integer part of $M_1 + G_1$ (resp. $M_2 + G_2$), and by U_1 (resp. U_2) the least integer $\geq M_1 - G_1$ (resp. $M_2 - G_2$). Then we can write

$$\Delta = P(\alpha_1, \alpha_2) = \alpha_1^{V_1}\alpha_2^{V_2}\tilde{P}\left(\frac{1}{\alpha_1}, \frac{1}{\alpha_2}\right),$$

where $\tilde{P}(X,Y)$ is a polynomial with integers coefficients, with the same length as P, and whose degree in X (resp. Y) is bounded by $V_1 - U_1$ (resp. $V_2 - U_2$). As $\mathrm{h}(1/\alpha_1) = \mathrm{h}(\alpha_1)$ and $\mathrm{h}(1/\alpha_2) = \mathrm{h}(\alpha_2)$, Liouville's inequality, in the shape of lemma 3.14 from the preceding Chapter 3, gives us the lower bound

$$\log \left| \tilde{P}\left(\frac{1}{\alpha_1}, \frac{1}{\alpha_2}\right) \right| \geq -(D-1)\log L(\tilde{P}) - D(V_1 - U_1)\log a_1 - D(V_2 - U_2)\log a_2.$$

Taking into account the above upper bound for $L(P) = L(\tilde{P})$, we get

$$\log|\Delta| \geq -(D-1)\log(N!) + V_1 \log \alpha_1 + V_2 \log \alpha_2 \\ -D(V_1 - U_1)\log a_1 - D(V_2 - U_2)\log a_2 - \frac{1}{2}(D-1)(K-1)N \log b.$$

Now, from the inequalities $D \log a_i \geq \log \alpha_i \geq 0$, we get

$$V_i \log \alpha_i - D(V_i - U_i)\log a_i \geq (M_i + G_i)\log \alpha_i - 2DG_i \log a_i$$

for $i = 1, 2$, inequalities which imply lemma 5.

1 Analytic upper bound for $|\Delta|$ Here is the crucial point where the smallness of $|\Lambda|$ is to be used essentially.

Lemma 6. *Let ρ be a real number ≥ 1. Suppose that*

$$|\Lambda'| \leq \rho^{-N+(1/2)}.$$

Then, we have the upper bound

$$|\Delta| \leq \rho^{-(N^2-N)/2} 2^N (N!) \left(\frac{\rho b}{2}\right)^{(K-1)N/2} \alpha_1^{M_1 + \rho G_1} \alpha_2^{M_2 + \rho G_2}.$$

Proof. Without loss of generality, we may assume that

$$b_1 \log \alpha_1 \leq b_2 \log \alpha_2,$$

so that Λ is ≥ 0. Denote $\beta = b_1/b_2$. Then we have

$$\log \alpha_2 = \beta \log \alpha_1 + \frac{\Lambda}{b_2}.$$

Let us first modify slightly the matrix whose Δ is the determinant. For any complex number η, as

$$\binom{r_j b_2 + s_j b_1}{k_i} = \frac{b_2^{k_i}}{k_i!}(r_j + s_j\beta - \eta)^{k_i} + (\text{ terms of degree } < k_i)$$

we have by multilinearity

$$\Delta = \det\left(\frac{b_2^{k_i}}{k_i!}(r_j + s_j\beta - \eta)^{k_i} \alpha_1^{\ell_i r_j} \alpha_2^{\ell_i s_j}\right).$$

Then it is convenient to center the exponents ℓ_i around their average value $(L-1)/2$. We get in this way:

$$\Delta = \alpha_1^{M_1}\alpha_2^{M_2} \det\left(\frac{b_2^{k_i}}{k_i!}(r_j + s_j\beta - \eta)^{k_i} \alpha_1^{\lambda_i r_j} \alpha_2^{\lambda_i s_j}\right),$$

where $\lambda_i = \ell_i - \frac{L-1}{2}$, $(1 \leq i \leq N)$. We write now

$$\begin{aligned}\alpha_1^{\lambda_i r_j}\alpha_2^{\lambda_i s_j} &= \alpha_1^{\lambda_i(r_j+s_j\beta)}e^{\lambda_i s_j \Lambda/b_2}\\ &= \alpha_1^{\lambda_i(r_j+s_j\beta)}\left(1+\Lambda'\theta_{i,j}\right),\end{aligned}$$

with

$$\theta_{i,j} = \frac{e^{\lambda_i s_j \Lambda/b_2}-1}{\Lambda'}$$

so that

$$|\theta_{i,j}| \leq \frac{2b_2\left(e^{|\lambda_i| s_j\Lambda/b_2}-1\right)}{LS\Lambda e^{LS\Lambda/2b_2}} \leq 1$$

(here is the unique reason for which it is better to work with Λ' instead of Λ). Plugging this expression in the determinant Δ, we get the formula

$$(*) \qquad \Delta = \alpha_1^{M_1}\alpha_2^{M_2}\left(\sum_{I\subseteq\{1,\dots,N\}}(\Lambda')^{N-\mathrm{Card}I}\Delta_I\right),$$

where

$$\Delta_I = \det\begin{pmatrix} c_{i,1} & \cdots & c_{i,N}\end{pmatrix} \begin{matrix}\}\\ \\ \}\end{matrix} \begin{matrix} i\in I\\ \\ i\notin I\end{matrix}$$
$$\begin{pmatrix}\theta_{i,1}c_{i,1} & \cdots & \theta_{i,N}c_{i,N}\end{pmatrix}$$

and

$$c_{i,j} = \frac{b_2^{k_i}}{k_i!}\left(r_j+s_j\beta-\eta\right)^{k_i}\alpha_1^{\lambda_i(r_j+s_j\beta)}.$$

As $\sum_{i=1}^N \lambda_i = 0$, it is licit to replace in Δ_I the quantity $c_{i,j}$ by $c_{i,j}\alpha_1^{-\lambda_i\eta}$, in such a way that our determinant Δ_I takes now the form

$$\Delta_I = \det\begin{pmatrix} \varphi_i(z_1) & \cdots & \varphi_i(z_N)\end{pmatrix} \begin{matrix}\}\\ \\ \}\end{matrix} \begin{matrix} i\in I\\ \\ i\notin I\end{matrix}$$
$$\begin{pmatrix}\theta_{i,1}\varphi_i(z_1) & \cdots & \theta_{i,N}\varphi_i(z_N)\end{pmatrix}$$

where we have set

$$\begin{aligned}\varphi_i(z) &= \frac{b_2^{k_i}}{k_i!}z^{k_i}\alpha_1^{\lambda_i z}, \qquad (1\leq i\leq N),\\ z_j &= r_j+s_j\beta-\eta, \qquad (1\leq j\leq N).\end{aligned}$$

Let us now choose $\eta = \frac{(R-1)+\beta(S-1)}{2}$, in such a way that

$$|z_j| \leq \frac{(R-1)+\beta(S-1)}{2}, \qquad (1\leq j\leq N).$$

We shall next give an upper bound for $|\Delta_I|$. Let us consider the entire function Φ_I of the complex variable x defined by

$$\Phi_I(x) = \det\begin{pmatrix} \varphi_i(xz_1) & \cdots & \varphi_i(xz_N)\end{pmatrix} \begin{matrix}\}\\ \\ \}\end{matrix} \begin{matrix} i\in I\\ \\ i\notin I\end{matrix}$$
$$\begin{pmatrix}\theta_{i,1}\varphi_i(xz_1) & \cdots & \theta_{i,N}\varphi_i(xz_N)\end{pmatrix}$$

so that $\Delta_I = \Phi_I(1)$. Expanding in Taylor series the functions φ_i for index of lines $i\in I$, we see as usual in the previous lectures, that the function Φ_I has a zero of multiplicity $\geq(\nu^2-\nu)/2$ for $x=0$, where we have set $\nu = \mathrm{Card}(I)$. The usual Schwarz lemma then implies

$$|\Delta_I| = |\Phi_I(1)| \leq \rho^{-(\nu^2-\nu)/2}\max_{|x|=\rho}|\Phi_I(x)|$$

for any real number $\rho \geq 1$. Using these inequalities for all subsets $I \subseteq \{1, \dots, N\}$, together with

$$|\Lambda'| \leq \rho^{-N+(1/2)}$$

and reporting in $(*)$, we get

$$|\Delta| \leq \alpha_1^{M_1} \alpha_2^{M_2} 2^N \max_{0 \leq \nu \leq N} \left(\rho^{-(N-\frac{1}{2})(N-\nu)-\frac{1}{2}(\nu^2-\nu)} \right) \max_I \max_{|x|=\rho} |\Phi_I(x)| .$$

As

$$\min_{0 \leq \nu \leq N} \left((N-\frac{1}{2})(N-\nu) + \frac{\nu^2-\nu}{2} \right) = \frac{N^2-N}{2},$$

we get

$$|\Delta| \leq \alpha_1^{M_1} \alpha_2^{M_2} 2^N \rho^{-(N^2-N)/2)} \max_I \max_{|x|=\rho} |\Phi_I(x)| .$$

Then lemma 6 is an immediate consequence of the following upper bound

Lemma 7. *For each subset $I \subseteq \{1, \dots, N\}$ and each complex number x, we have*

$$|\Phi_I(x)| \leq N! \left(\frac{|x|b}{2} \right)^{(K-1)N/2} {\alpha_1}^{|x|G_1} {\alpha_2}^{|x|G_2}.$$

Proof. Since $|\theta_{i,j}| \leq 1$, expanding the determinant $\Phi_I(x)$ shows that

$$|\Phi_I(x)| \leq N! \max_\sigma \left| \prod_{i=1}^N \varphi_i(x z_{\sigma(i)}) \right|,$$

where σ runs over all substitutions $\sigma \in \mathcal{S}_N$. We have:

$$\prod_{i=1}^N \varphi_i\big(x z_{\sigma(i)}\big) = \prod_{i=1}^N \frac{\big(b_2 x z_{\sigma(i)}\big)^{k_i}}{k_i!} \alpha_1^{\left(\sum \lambda_i z_{\sigma(i)}\right) x},$$

$$\begin{aligned} \sum \lambda_i z_{\sigma(i)} &= \sum \lambda_i \big(r_{\sigma(i)} + \beta s_{\sigma(i)} - \eta \big) \\ &= \sum \lambda_i \big(r_{\sigma(i)} + \beta s_{\sigma(i)} \big) \\ &= \big(\sum \lambda_i r_{\sigma(i)} \big) + \beta \big(\sum \lambda_i s_{\sigma(i)} \big). \end{aligned}$$

Now lemma 3 gives us respectively the upper bound G_1 and G_2 for the absolute value of the two last sums. We get

$$\left| \sum \lambda_i z_{\sigma(i)} \right| \leq G_1 + \beta G_2.$$

By assumption $\alpha_1^\beta \leq \alpha_2$. Finally, the exponential term in the product $\prod_{i=1}^N \varphi_i\big(x z_{\sigma(i)}\big)$ is bounded by $\alpha_1^{|x|G_1} \alpha_2^{|x|G_2}$, as was to be shown. For the monomial term, it is enough to use the simple bound

$$|z_j| \leq \frac{(R-1)+\beta(S-1)}{2}, \qquad (1 \leq j \leq N),$$

so that

$$\prod_{i=1}^N \frac{\big|b_2 x z_{\sigma(i)}\big|^{k_i}}{k_i!} \leq \left(\frac{b_2|x|\big((R-1)+\beta(S-1)\big)}{2} \right)^{(K-1)N/2} \left(\prod_{k=1}^{K-1} k! \right)^{-L}$$

$$= \left(\frac{|x|b}{2} \right)^{(K-1)N/2}.$$

Remark. The determinant Δ is nothing else that the interpolation determinant of the N functions in two variables x, y

$$\varphi_i(x,y) = \frac{b_2^{k_i}}{k_i!} x^{k_i} \alpha_1^{\ell_i x} e^{\ell_i y}, \qquad (1 \le i \le N),$$

evaluated at the N points

$$(r_j + \beta s_j, s_j \Lambda / b_2)\,, \qquad (1 \le j \le N).$$

For bounding such a determinant, the general pattern consists to expand it in Taylor series (around the origin or any other point) of the $2N$ variables $x_j, y_j, (1 \le j \le N)$, determined by the coordinates of the given N points.

In our special case, the second coordinate y is small, so it has been sufficient to expand the functions $\varphi_i(x,y)$ at the order 1 in y.

1 End of the proof of Theorem 3 On the opposite, suppose that the conditions of Theorem 3 are satisfied and that

$$|\Lambda'| \le \rho^{-KL+(1/2)}.$$

Lemmas 5 and 6 allow us to precise the value of $\log|\Delta|$:

$$-(D-1)\log(N!) + (M_1+G_1)\log\alpha_1 + (M_2+G_2)\log\alpha_2 - 2D(G_1\log a_1 + G_2\log a_2)$$
$$-\frac{1}{2}(D-1)(K-1)N\log b \le \log|\Delta| \le N\log(2N!) + \frac{1}{2}(K-1)N\log\big(\rho b/2\big)$$
$$+(M_1+\rho G_1)\log\alpha_1 + (M_2+\rho G_2)\log\alpha_2 - \frac{1}{2}(N^2-N)\log\rho.$$

The quantities involving M_1 and M_2 cancel on both sides of the above inequalities. We finally get the opposite of (2) by bounding $\log(N!) \le N\log N$ and replacing N, G_1, G_2 by their values. This contradiction proves the Theorem 3.

1 Proof of Theorems 1 and 2 As $\alpha_1 \le a_1^D$ and $\alpha_2 \le a_2^D$, it is sufficient to check instead of (2) the stronger, but simpler, inequality

$$(3) \qquad K(L-1)\log\rho + (K-3)\log 2 > 2D\log(KL) + D(K-1)\log b + g(\rho+1)DL\,(R\log a_1 + S\log a_2)\,.$$

Now, we have to compare b and b'. This will be provided by

Lemma 8. *For any integers $R \ge 1$, $S \ge 1$ and $K \ge 2$, we have*

$$b \le \frac{5\big((R-1)b_2 + (S-1)b_1\big)}{K-1}.$$

Proof. We are lead to give an uniform lower bound for

$$\left(\prod_{k=1}^{K-1} k!\right)^{2/(K^2-K)}.$$

Let us show that this quantity is $\ge (K-1)/5$ for any $K \ge 2$, which is the meaning of lemma 8. This is a problem of standard calculus. One can proceed as follows. First notice that

$$\prod_{k=1}^{K-1} k! = \prod_{k=1}^{K-1} (K-k)^k = \prod_{k=1}^{K-1} k^{K-k}$$
$$= \frac{((K-1)!)^K}{\prod_{k=1}^{K-1} k^k}.$$

Now we are reduced to give an upper bound for $\prod_{k=1}^{K-1} k^k$. Let us show that

$$\sum_{k=1}^{K-1} k \log k \leq \frac{K^2-K}{2} \log(K-1) - \frac{K^2-K}{4} + \frac{K}{3},$$

for $K \geq 2$. We use Euler-Maclaurin's summation formula, in the notations of formula (7.2.4.) p. 303 in [1]:

$$f(1) + \cdots + f(n) = \int_1^n f(x)dx + \frac{f(1)+f(n)}{2} + \frac{f'(n)-f'(1)}{12} + R_1$$

with $r = 1$ and

$$R_1 \leq \frac{1}{2\pi^2} \int_1^n |f^{(3)}(x)|dx.$$

We take $f(x) = x \log x$ and $n = K-1$, and we get

$$\sum_{k=1}^{K-1} k \log k \leq \frac{(K-1)^2}{2} \log(K-1) - \frac{(K-1)^2}{4} + \frac{1}{4} + \frac{(K-1)\log(K-1)}{2} + \frac{\log(K-1)}{12} + \frac{1}{2\pi^2},$$

in which formula, it is enough to bound $\log(K-1) \leq K-2$ for any $K \geq 2$. Now, we use the standard lower bound

$$(K-1)! \geq (K-1)^{K-1} e^{-(K-1)}.$$

Putting altogether, we get

$$\left(\prod_{k=1}^{K-1} k! \right)^{2/(K^2-K)} \geq (K-1) e^{-(3/2)-(2/3(K-1))} \geq \frac{K-1}{5},$$

for $K \geq 8$. If $K = 2, \ldots, 7$, the inequality between the left hand side and the right hand side is obvious to check.

The principle of the proofs of Theorems 1 and 2 is as follows. In each case, we shall define a system of parameters $K, L, R_1, R_2, S_1, S_2, \rho$ satisfying the conditions (1) and (3). Theorem 3 provides us a lower bound for $|\Lambda'|$, and consequently for $|\Lambda|$, if we assume that the numbers $rb_1 + sb_2$, $(0 \leq r \leq R-1,\ 0 \leq s \leq S-1)$ are pairwise distinct. If this last condition is unsatisfied, Liouville's inequality furnishes a much better lower bound for $|\Lambda|$ than the one which is required.

Let $c_1 > 0$, $c_2 > 0$, $c_3 > 0$, $c_4 > 0$ and f be constants (that is to say, numbers independent of b', a_1, and a_2) which shall be defined in each case. For simplicity, denote $B = f + \log b'$. We set

$$\begin{aligned}
K &= \left[c_1 D^3 B \log a_1 \log a_2 \right], \\
L &= \left[c_2 DB \right], \\
R_1 &= \left[c_3 D^{3/2} B^{1/2} \log a_2 \right] + 1, \\
S_1 &= \left[c_3 D^{3/2} B^{1/2} \log a_1 \right] + 1, \\
R_2 &= \left[c_4 D^2 B \log a_2 \right], \\
S_2 &= \left[c_4 D^2 B \log a_1 \right].
\end{aligned}$$

Let us begin by Theorem 1 for which the computations are simpler because it suffices to compare the leading terms for large B in the inequalities involved. First, thanks to lemma 8, we bound

$$b \leq \frac{5\left((R-1)b_2 + (S-1)b_1\right)}{K-1} \leq e^f b' = e^B,$$

if we have chosen $f > \log 5 + \log c_4 - \log c_1$. To satisfy (1) and (3) for large B, it is enough to choose positive constants $c_1, \ldots, c_4$ so that:

$$\begin{aligned} c_4 &> \sqrt{2c_1c_2}, \\ c_1c_2 \log \rho &> c_1 + 2g(\rho+1)c_2c_4, \\ c_3 &= \max\left(\sqrt{c_1}, \sqrt{c_2}\right). \end{aligned} \tag{4}$$

Remark that the ratio $\gamma = RS/KL$ is > 2 and then the quantity g is $> (1/4) - (1/24) = 5/24$. We easily check that there exist positive solutions of the system (4) which are as close as we wish from the limit values:

$$c_1 = \frac{64g^2(\rho+1)^2}{(\log \rho)^3}, \quad c_2 = \frac{2}{\log \rho}, \quad c_3 = \max\left(\sqrt{c_1}, \sqrt{c_2}\right), \quad c_4 = \sqrt{2c_1c_2},$$

with $g = 5/24$. Strictly speaking, these values are not convenient because they lead to equalities in the first two relations of (4). Now choose $\rho = 5.8$, so that

$$c_1 = 23.64\cdots, \quad c_2 = 1.13\cdots, \quad c_3 = 4.86\cdots, \quad c_4 = 7.33\cdots.$$

From Theorem 3 follows the alternative: either

$$\log|\Lambda'| \geq -KL \log \rho \geq -c_1c_2 \log \rho D^4 B^2 \log a_1 \log a_2,$$

or there exist two integers r and s, with $|r| \leq R-1, |s| \leq S-1$ such that $rb_2 + sb_1 = 0$. Obviously we may suppose that r and s are relatively prime. Then from exercise 6.a in Chapter 3, we get

$$|\Lambda| \geq |r \log \alpha_1 + s \log \alpha_2| \geq \exp\big\{-D \log 2 - D\big(|r| \log a_1 + |s| \log a_2\big)\big\},$$

which implies

$$\log|\Lambda| \geq -D \log 2 - 2c_3 D^{5/2} B^{1/2} \log a_1 \log a_2 - 2c_4 D^3 B \log a_1 \log a_2.$$

Here above, the main term is the third, which is better than required. To conclude, one has only to remark that for the above limit values, we have $c_1c_2 \log \rho < 48$ and that $\log|\Lambda'/\Lambda| = \mathcal{O}(\log B)$.

For Theorem 2, the preceding arguments have to be made effective. We choose our constants slightly larger than the above limit values. Let us set

$$c_1 = 36, \quad c_2 = 1.5, \quad c_3 = 6, \quad c_4 = 6\sqrt{3} + 0.04 = 10.43\cdots, \quad f = 0.49, \quad \rho = 4.9.$$

Using systematically estimates of the type

$$(x - 0.04)y < [xy] \leq xy,$$

which are true for any real numbers $x \geq 0$ and $y \geq 25$, we easily check that for $B \geq 25$, we have

$$\begin{aligned} R &\leq 11.633 D^2 B \log a_2 \\ S &\leq 11.633 D^2 B \log a_1 \\ \gamma &\leq 2.578 \\ g &\leq 0.218 \end{aligned}$$

(note that the third term from the definition of g in Theorem 3, is bounded by 10^{-4}). The lemma 8 gives us the upper bounds

$$b \leq \frac{5\big((R-1)b_2 + (S-1)b_1\big)}{K-1} \leq \frac{5\big(Rb_2 + Sb_1\big)}{K} \leq 1.62b'$$

from which follows $\log b \le B$. Inequalities (1) are consequences of the lower bounds:

$$R_1 \ge 6D^{3/2}B^{1/2}\log a_2,$$
$$S_1 \ge 6D^{3/2}B^{1/2}\log a_1,$$
$$R_2 \ge 6\sqrt{3}D^2B\log a_2,$$
$$S_2 \ge 6\sqrt{3}D^2B\log a_1.$$

To check the main inequality (3), it is convenient to break it into two parts

$$K(L-1)\log\rho > D(K-1)B + g(\rho+1)DL\,(R\log a_1 + S\log a_2) \tag{3.1}$$

$$(K-3)\log 2 > 2D\log(KL). \tag{3.2}$$

The reader will easily check that the left hand side of (3.1) is $\ge 81.15D^4B^2\log a_1\log a_2$, while the right hand side is $\le 80.89D^4B^2\log a_1\log a_2$, for $B \ge 25$. The condition (3.2) is quite largely fulfilled for $B \ge 25$. By Theorem 3, we know that either

$$\log|\Lambda'| \ge -KL\log\rho \ge -86D^4B^2\log a_1\log a_2,$$

or

$$\log|\Lambda| \ge -D\log 2 - DR\log a_1 - DS\log a_2 \ge -24D^3B\log a_1\log a_2.$$

Finally, the bound (quite weak for $B \ge 25$)

$$1 + \log L + \log S + \log R \le D^4B^2\log a_1\log a_2,$$

provides us the required lower bound

$$\log|\Lambda| \ge -87D^4B^2\log a_1\log a_2.$$

References

[1] J. Dieudonné. – Calcul infinitésimal ; Collection méthodes Paris, (1968).
[2] M. Mignotte and M. Waldschmidt. – Linear forms in two logarithms and Schneider's method; Math. Annalen, **231** (1978), 231-237.
[3] M. Mignotte and M. Waldschmidt. – Linear forms in two logarithms and Schneider's method II; Acta Arithmetica, **53** (1989), 250-287.
[4] M. Mignotte and M. Waldschmidt. – Linear forms in two logarithms and Schneider's method III; Ann. Fac. Sc. Toulouse, **97** (1989), 43-75.

Notations

$\mathbb{N}$ (set of non-negative rational integers)

$\mathbb{Z}$ (ring of rational integers)

$\mathbb{Q}$ (field of rational numbers)

$\mathbb{R}$ (field of real numbers)

$\overline{Q}$ (field of algebraic numbers)

$\mathbb{C}$ (field of complex numbers)

$\mathbb{Q}_p$ (field of p-adic numbers; §3.2)

$\mathbb{C}_p$ (completion of an algebraic closure of $\mathbb{Q}_p$; §3.3)

K^* (multiplicative group of non-zero elements of a field K)

$\dim_K$ (dimension of a K-vector space)

$\mathrm{rk}_{\mathbb{Z}}$ (rank of finitely generated $\mathbb{Z}$-module)

Card (number of elements of a set)

$\bar{E}$ (Zariski closure of a subset E in K^d; §8.1.a)

gcd (greatest common divisor)

$\binom{n}{k}$ (binomial coefficient)

$[x]$ (integral part of a real number x)

$\lfloor x \rfloor$ (smallest integer $\geq x$; §5.3.f).

Index