INTRODUCTION TO RECENT RESULTS IN TRANSCENDENTAL NUMBER THEORY

by **Michel WALDSCHMIDT** (*)

The present text includes the notes of four lectures given at the *Workshop and conference in number theory* which took place in Hong Kong from June 29 to July 3, 1993. These notes were prepared during the author's visit at MSRI in May 1993, and distributed to the participants of the Hong Kong Workshop at the start of the conference. Thanks are due to Lisa Fastenberg, Jonathan Pila and Damien Roy for several comments on a preliminary version.

Lecture 1.– Historical survey and main tools

We start these lectures with a very brief historical survey of the subject in order to introduce recent results. Next we describe two of the main tools for the proofs: Liouville's inequality and zero estimates.

§1. History

The general title of these four lectures puts the emphasis on recent results. However we shall start by quoting some of the oldest results of the theory. The first Theorem on the subject goes back to 1844 [Lio 1844a,b; 1851]:

Liouville's Theorem. – *Let α be a complex number which is root of a non-zero polynomial in $\mathbf{Z}[X]$ of degree d. There exists a constant $c(\alpha)>0$, which can be easily computed, such that, for any rational number p/q with $p/q\neq\alpha$ and $q>0$,*

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

A complex number satisfying the assumption of Liouville's Theorem is called *algebraic*; a complex number which is not algebraic is called *transcendental*. The set of (complex) algebraic numbers is a subfield of $\mathbf{C}$ which we shall denote by $\bar{\mathbf{Q}}$. Liouville's Theorem is a result of diophantine approximation; it enabled Liouville to give the first example of transcendental numbers. It's a different matter to prove the transcendence of given numbers; the transcendence of e (natural basis of Napierian logarithms) was proved by Hermite [He 1873], the transcendence of π by Lindemann [Lin 1882a,b,c]:

(*) Research at MSRI supported in part by NSF grant # DMS 9022140

Theorem of Hermite-Lindemann. – *Let β be a non-zero complex number. Then one at least of the two numbers β and e^β is transcendental.*

Hence, if β is algebraic, then $\exp(\beta)$ is transcendental (for instance the number e itself is transcendental); also, if α is a non-zero algebraic number, and if $\log\alpha$ is any determination of its logarithm (which means any complex number such that $\exp(\log\alpha)=\alpha$), then $\log\alpha$ is a transcendental number. For instance, taking $\alpha=1$ and $\log 1=2i\pi$, one deduces the transcendence of the number π, which implies the impossibility of squaring the circle.

The set $\mathcal{L}$ of logarithms of non-zero algebraic numbers will play an important role in these lectures; this is a $\mathbf{Q}$-vector subspace of $\mathbf{C}$:

$$\mathcal{L}=\{\ell\in\mathbf{C}\,;\,e^\ell\in\bar{\mathbf{Q}}^*\}=\{\log\alpha;\alpha\in\bar{\mathbf{Q}}^*\}.$$

The proof of Liouville's Theorem is not difficult; on the opposite, there is no very simple proof for the Theorem of Hermite-Lindemann (see [M 1976]). In the second lecture we shall outline a proof of a special case of the Theorem of Hermite-Lindemann, by the method which is now used in the most recent papers in transcendental number theory.

The following result, which was stated by Lindemann, was proved by Weierstrass [We 1885]:

Theorem of Lindemann-Weierstrass. – *If $\alpha_1,\ldots,\alpha_n$ are algebraic numbers which are linearly independent over $\mathbf{Q}$, then the n numbers $e^{\alpha_1},\ldots,e^{\alpha_n}$ are algebraically independent.*

The conclusion means that if $P\in\mathbf{Z}[X_1,\ldots,X_n]$ is a non-zero polynomial, then the number $P\bigl(e^{\alpha_1},\ldots,e^{\alpha_n}\bigr)$ does not vanish. This is one of the very few results on algebraic independence of numbers connected with the exponential function.

After the contributions of Liouville, Hermite, Lindemann and Weierstrass, the next important step was provided by the work of Siegel [Si 1929], Gel'fond [G 1934] and Schneider [Sc 1934], which led to the solution of Hilbert's seventh problem [Hi 1900].

Theorem of Gel'fond-Schneider. – *Let $\log\alpha_1$ and $\log\alpha_2$ be two $\mathbf{Q}$-linearly independent logarithms of algebraic numbers. Then their quotient $\log\alpha_1/\log\alpha_2$ is transcendental.*

This shows that $\mathcal{L}$, which is a $\mathbf{Q}$-vector space, is not a $\bar{\mathbf{Q}}$-vector space, a fact which had been suggested already by Euler.

Let us check that this includes the transcendence of such numbers as $\log 2/\log 3$, $2^{\sqrt{2}}$, or e^π. This is plain for the first one; for the second (resp. the last) one, notice that $\log 2$ (resp. $2i\pi$) belongs to $\mathcal{L}$, while $\sqrt{2}$ (resp. $2i$) is an irrational algebraic number; hence $\sqrt{2}\log 2$ (resp. π) does not belong to $\mathcal{L}$.

Now let $\log\alpha_1,\ldots,\log\alpha_n$ be n logarithms of algebraic numbers which are linearly independent over $\mathbf{Q}$; the question arises to prove that they are also linearly independent over the field $\bar{\mathbf{Q}}$ of algebraic numbers; for $n=2$, this is the Theorem of Gel'fond-Schneider. This problem was solved in 1966 by A. Baker [Ba 1966], who extended one year later his result to a non-homogeneous situation as follows:

Baker's Theorem. – *If* $\log\alpha_1,\dots,\log\alpha_n$ *are* $\mathbf{Q}$*-linearly independent logarithms of algebraic numbers, then the* $n+1$ *numbers* $1,\log\alpha_1,\dots,\log\alpha_n$ *are linearly independent over* $\bar{\mathbf{Q}}$.

This statement also includes the Theorem of Hermite-Lindemann (take $n=1$). However it does not include all that is known on the transcendence of values of the exponential function, even if one does not mention results of algebraic independence (like the Theorem of Lindemann-Weierstrass). One such result, which is not included in Baker's Theorem, is the so-called *six exponentials Theorem*, due to Siegel (see [AE 1944]), Schneider (implicit in [Sc 1949]), Lang [La 1965, 1966a,b] and Ramachandra [Ra 1968, 1969]:

Six Exponentials Theorem. – *Let* $x_1,\dots,x_d$ *be complex numbers which are linearly independent over* $\mathbf{Q}$ *and let* $y_1,\dots,y_\ell$ *be also complex numbers which are linearly independent over* $\mathbf{Q}$*. Assume* $\ell d>\ell+d$*. Then one at least of the* ℓd *numbers*

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

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.

There are a few results of algebraic independence concerning the values of the exponential function which are not included in the Theorem of Lindemann-Weierstrass. For instance Gel'fond proved in 1949 that for a cubic number β and for $0\ne\log\alpha\in\mathcal{L}$, the two numbers α^β and α^{β^2} are algebraically independent (see [G 1952]). This result has been extended, especially by G.V. Chudnovsky and P. Philippon; the best result known in this direction is due to G. Diaz: if β is algebraic of degree $d\ge 3$, then for any $0\ne\log\alpha\in\mathcal{L}$, at least $\bigl[(d+1)/2\bigr]$ of the $d-1$ numbers $\alpha^\beta,\alpha^{\beta^2},\dots,\alpha^{\beta^{d-1}}$ are algebraically independent [Di 1989].

There is another method, due to Mahler, which yields results of algebraic independence, but not for the exponential function. A connection with finite automata was found by Cobham in 1968 and developed more recently by J.H. Loxton. This subject is also related to quasi-crystals (Bombieri-Taylor). Very recently, P.G. Becker used this method to solve a problem in complex dynamics and fractals which arose from the work by Douady and Hubbard in 1982, where they prove that *the Mandelbrot set* $\mathcal{M}$ *is connected*. This set is defined by iterating the polynomial $P_c(z)=z^2+c$, for $c\in\mathbf{C}$; if $P^{(k)}(z)=P^{(k-1)}\bigl(P(z)\bigr)$ denotes the k-th iterate of a polynomial P, then $\mathcal{M}$ is the set of $c\in\mathbf{C}$ for which $P_c^{(k)}(0)$ does not tend to infinity with k. Douady and Hubbard construct an analytic map φ from the complement (into the Riemann sphere) of $\mathcal{M}$ onto the complement of the unit disk; this map can be normalized to have an expansion of the form $\varphi(z)=z+c_0+c_1/z+\cdots$ at infinity. Then Becker shows that $\varphi(\alpha)$ is transcendental for any algebraic α which is not in $\mathcal{M}$.

Finally in this short historical survey, we did not speak of diophantine approximation, elliptic curves and commutative algebraic groups, or Drinfeld modules, since these topics will be considered in subsequent lectures.

§2. Conjectures

We start with the following open problem: *if* x *is a positive real number such that* 2^x *and* 3^x *are both rational integers, does it follow that* x *is an integer ?* This is a special case of the following: one conjectures that the conclusion of the six exponentials theorem is still valid under the weaker hypothesis $\ell d\ge\ell+d$ (see the first problem in [Sc 1957], as well as [La 1966b]).

Four Exponentials Conjecture. – *Let* x_1,x_2 *be two* $\mathbf{Q}$*-linearly independent complex numbers and* y_1,y_2 *also two* $\mathbf{Q}$*-linearly independent complex numbers. Then one at least of the 4 numbers*

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

is transcendental.

The most far reaching conjecture on the subject is due to Schanuel [La 1966b]:

Schanuel's Conjecture. – *If* $x_1,\dots,x_n$ *are* $\mathbf{Q}$*-linearly independent complex numbers, then, among the* $2n$ *numbers*

$$x_1,\dots,x_n,e^{x_1},\dots,e^{x_n},$$

at least n *are algebraically independent.*

The conclusion may also be phrased: the *transcendence degree* over $\mathbf{Q}$ of the field

$$\mathbf{Q}\bigl(x_1,\dots,x_n,e^{x_1},\dots,e^{x_n}\bigr)$$

is at least n.

This conjecture is supposed to include all known transcendence results as well as all reasonable transcendence conjectures on the values of the exponential function. The special case where $x_1,\dots,x_n$ are all algebraic is just the Theorem of Lindemann-Weierstrass; the other special case where $e^{x_1},\dots,e^{x_n}$ are algebraic would already have tremendous consequences:

Conjecture of algebraic independence of logarithms. – *Let* $\log\alpha_1,\dots,\log\alpha_n$ *be elements of* $\mathcal{L}$ *(which means that they are logarithms of algebraic numbers), which are linearly independent over* $\mathbf{Q}$*; then these numbers are algebraically independent over* $\mathbf{Q}$.

We are very far from this conjecture; indeed, it is not yet even known that there exist at least two algebraically independent logarithms of algebraic numbers! In spite of this terrible situation, interesting partial results are known, as we shall see.

We gave a small sample of well-known conjectures; many other problems will arise also in the next lectures.

§3. On the rank of matrices

The four exponentials Conjecture can be stated as follows: *consider a* 2×2 *matrix whose entries are logarithms of algebraic numbers:*

$$M = \begin{pmatrix} \log\alpha_{11} & \log\alpha_{12}\\ \log\alpha_{21} & \log\alpha_{22}\end{pmatrix};$$

assume that the two rows of this matrix are linearly independent over $\mathbf{Q}$ *(in* $\mathbf{C}^2$*), and also that the two columns are linearly independent over* $\mathbf{Q}$*; then the rank of this matrix is* 2.

It is not difficult to check that the four exponentials Conjecture is a consequence of Schanuel's Conjecture, and more precisely of the Conjecture on algebraic independence of logarithms.

The six exponentials Theorem yields a partial result: consider a $d\times\ell$ matrix whose entries are logarithms of algebraic numbers:

$$M = \begin{pmatrix} \log\alpha_{11} & \cdots & \log\alpha_{1\ell}\\ \vdots & \ddots & \vdots\\ \log\alpha_{d1} & \cdots & \log\alpha_{d\ell}\end{pmatrix};$$

assume that the d rows of this matrix are $\mathbf{Q}$-linearly independent (in $\mathbf{C}^\ell$), and also that the ℓ columns are $\mathbf{Q}$-linearly independent (in $\mathbf{C}^d$). If $\ell d > \ell + d$, then the rank of this matrix is ≥ 2. We obtain the equivalence with the initial formulation of the six exponentials Theorem by noticing that a $d\times\ell$ matrix is of rank ≤ 1 if and only if it can be written $\bigl(x_iy_j\bigr)_{1\leq i\leq d, 1\leq j\leq \ell}$, for some complex numbers $x_1,\ldots,x_d$, $y_1,\ldots,y_\ell$.

Assume now that $\ell d/(\ell+d)$ is "large"; *is-it possible to get a better lower bound for the rank of the matrix?* We notice first that conditions on linear independence of rows and columns are no more sufficient, as shown by matrices like the following, which is of rank 2:

$$\begin{pmatrix} \log 2 & \log 3 & \cdots & \log p_m\\ \log 3 & & & \\ \vdots & & 0 & \\ \log p_m & & & \end{pmatrix}$$

where $\ell = d = m$, and p_m is the m-th prime number.

To start with, assume that the Conjecture on algebraic independence of logarithms is true; *how can one describe the rank of a matrix*

$$\Bigl(\log\alpha_{ij}\Bigr)_{1\leq i\leq d, 1\leq j\leq \ell}?$$

This problem has been solved by D. Roy [R 1989] as follows: let $\lambda_1,\ldots,\lambda_r$ be a basis of the $\mathbf{Q}$-vector space generated by the $d\ell$ entries of M: there exist rational integers a_{ijk} such that

$$\log\alpha_{ij} = \sum_{k=1}^r a_{ijk}\lambda_k, \qquad (1\leq i\leq d, 1\leq j\leq \ell);$$

consider the matrix

$$\tilde M = \left(\sum_{k=1}^r a_{ijk}X_k\right)_{1\leq i\leq d, 1\leq j\leq \ell} = \sum_{k=1}^r X_k\Bigl(a_{ijk}\Bigr)_{1\leq i\leq d, 1\leq j\leq \ell},$$

with coefficients which are linear forms in unknowns $X_1,\ldots,X_r$; define the *conjectural rank of* M as the rank of $\tilde M$ in the field $\mathbf{Q}(X_1,\ldots,X_r)$ of rational functions in r variables:

$$r_{\mathrm{conj}}(M) = \mathrm{rank}(\tilde M);$$

then this number does not depend on the choice of $\lambda_1,\ldots,\lambda_r$, and the Conjecture on algebraic independence of logarithms plainly implies that the equality $\mathrm{rank}(M) = r_{\mathrm{conj}}(M)$ holds. One does not need the full force of the Conjecture on algebraic independence: one needs only the homogeneous special case of it: *if* $\log\alpha_1,\ldots,\log\alpha_n$ *are elements of* $\mathcal{L}$ *which are linearly independent over* $\mathbf{Q}$, *and if* $P\in\mathbf{Q}[X_1,\ldots,X_n]$ *is a non-zero* homogeneous *polynomial, then the number* $P(\log\alpha_1,\ldots,\log\alpha_n)$ *does not vanish.*

A quite remarkable fact, proved by D. Roy [R 1989], is that the converse holds, namely: *if* $\mathrm{rank}\, M = r_{\mathrm{conj}}(M)$ *holds for all matrices* M *with entries in* $\mathcal{L}$*, then the Conjecture on homogeneous algebraic independence of logarithms is true.*

If one wishes to consider non-homogeneous polynomials in logarithms of algebraic numbers, then it's sufficient to deal with matrices whose entries lie in the $\mathbf{Q}$-vector subspace of $\mathbf{C}$ generated by 1 and $\mathcal{L}$.

More generally, denote by $\mathcal{L}_{\bar{\mathbf{Q}}}$ the $\bar{\mathbf{Q}}$-vector space generated in $\mathbf{C}$ by 1 and $\mathcal{L}$:

$$\mathcal{L}_{\bar{\mathbf{Q}}} = \{\beta_0+\beta_1\log\alpha_1+\cdots+\beta_n\log\alpha_n;\ n\geq 0,\ \beta_i\in\bar{\mathbf{Q}},\ \log\alpha_i\in\mathcal{L}\}.$$

The conjectural rank of a matrix with coefficients in $\mathcal{L}_{\bar{\mathbf{Q}}}$ is defined as before, taking a basis of the $\bar{\mathbf{Q}}$-vector spanned by the coefficients and considering matrices whose entries are linear forms; again the Conjecture on algebraic independence of logarithms is equivalent to the fact that the rank equals the conjectural rank for matrices with coefficients in $\mathcal{L}_{\bar{\mathbf{Q}}}$.

Theorem (Roy [R 1990a]**).** – *Let* M *be a matrix whose entries are in* $\mathcal{L}_{\bar{\mathbf{Q}}}$*. Then* $\mathrm{rank}\, M\geq (1/2)r_{\mathrm{conj}}(M)$.

Therefore, from this point of view, half of Schanuel's Conjecture is now proved!

The proof of this result rests on the so-called *Theorem of the linear subgroup* [W 1986, 1987]; further related results are given in Roy's papers, especially [R 1992b] where he answers a question of J-J. Sansuc on the density of finitely generated subgroups in the multiplicative group k^* of a number field k for the canonical embedding into $(k\otimes_{\mathbf{Q}}\mathbf{R})^*$.

§4. Liouville's inequality; height

One characteristic of transcendence proofs, and more generally of results of diophantine approximation, is that the following fact is needed at some place: *if a rational integer does not vanish, then its absolute value is at least* 1. There are many variants of this fact; for instance: *if an irrational number* p/q (where p and q are relatively prime rational integers and $q>0$) *does not vanish, then* $|p/q|\geq 1/q$. Now the bound depends on the number considered; we shall define the *logarithmic height* of a rational number p/q as $\mathrm{h}(p/q) = \log\max\{|p|, q\}$; therefore the previous inequality reads:

$$\log|x| \geq -\mathrm{h}(x) \qquad \text{for all } x \in \mathbf{Q}^*.$$

Liouville's inequality, which we are going to discuss now, is a generic name for similar lower bounds for non-zero algebraic numbers α. When one wants to prove that a number is transcendental, one assumes it is not, and the proof requires some properties of algebraic numbers; most often Liouville's inequality is all that is needed.

Let α be an algebraic number; consider the *minimal polynomial of α over* $\mathbf{Z}$: this is an irreducible polynomial in the factorial ring $\mathbf{Z}[X]$:

$$f(X) = a_0X^d + a_1X^{d-1} + \cdots + a_{d-1}X + a_d,$$

with leading coefficient $a_0 > 0$, which vanishes at α; such a polynomial is uniquely determined; the associated monic polynomial $(1/a_0)f$ is the *irreducible polynomial of α over* $\mathbf{Q}$. The positive integer d is the *degree* of α. One measures the *height* of α by taking into account the size of the coefficients of f; there are several ways of doing so (there are several norms on the space $\mathbf{Z}[X]$); to each choice of a norm, there is a corresponding Liouville's inequality.

It used to be that the results of diophantine approximation were stated in terms of the so-called "usual" (or "naive") height of α, which is

$$H(\alpha) = \max\{|a_0|, \ldots, |a_d|\};$$

for instance, when α is of degree 1 (i.e. rational), then $\mathrm{h}(\alpha) = \log H(\alpha)$. We now prove the following Liouville's inequality for the usual height:

$$\text{for any non-zero algebraic number } \alpha, \qquad |\alpha| \geq \frac{1}{H(\alpha)+1}.$$

We first prove (without the asssumption $\alpha \neq 0$) an *upper bound* for $|\alpha|$, namely $|\alpha| \leq H(\alpha) + 1$. This is trivial if $|\alpha| \leq 1$, while, if $|\alpha| > 1$, we write

$$-a_0\alpha = a_1 + a_2\alpha^{-1} + \cdots + a_d\alpha^{-d+1},$$

hence $|\alpha| \leq |a_0\alpha| \leq H(\alpha)/(1 - |\alpha|^{-1})$. Now if $\alpha \neq 0$, then $H(\alpha^{-1}) = H(\alpha)$, which completes the proof of Liouville's inequality.

The trouble with the usual height is that it is not obvious how to compute the height of a product, or of a sum, of algebraic numbers. The solution which is used nowadays is to work out the transcendence argument using a more efficient height; if one wishes to state some corollaries in terms of another height (like the usual one), one invokes some inequalities relating the different heights.

Before we introduce the *absolute logarithmic height*, we state a consequence of Jensen's formula (cf. M 1976]):

Lemma (Mahler). – *Let $f \in \mathbf{C}[X]$ be a non-zero polynomial of degree d with leading coefficient $a_0 > 0$:*

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

Then

$$a_0\prod_{i=1}^{d}\max\{1, |\alpha_i|\} = \exp\left(\int_0^1 \log|f(e^{2i\pi t})|dt\right).$$

Under the notation of lemma 3.9, we define *Mahler's measure* of f by

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

This is a multiplicative function:

$$\mathrm{M}(f_1f_2) = \mathrm{M}(f_1)\,\mathrm{M}(f_2)$$

for f_1 and f_2 in $\mathbf{C}[X]$.

When α is an algebraic number with minimal polynomial $f \in \mathbf{Z}[X]$, we define its *Mahler's measure* by $\mathrm{M}(\alpha) = \mathrm{M}(f)$; further, if α is of degree d, one defines its *logarithmic height* as

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

There are, for $\alpha \in \bar{\mathbf{Q}}$ of degree d, inequalities between the naive and the logarithmic heights:

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

The following Liouville's inequality is one of the most efficient for transcendence purposes: *for a non-zero algebraic number α of degree d,*

$$\log|\alpha| \geq -d\,\mathrm{h}(\alpha).$$

One can bound the height of sums or products of algebraic numbers as follows.

For algebraic numbers α_1 and α_2,

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

and

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

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

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

The main point of the proof of these estimates is that the logarithmic height of an element α in a number field k is also given by

$$\mathrm{h}(\alpha) = \frac{1}{[k:\mathbf{Q}]} \sum_{v \in M_k} d_v \log \max\{1, |\alpha|_v\},$$

where M_k is the set of "normalized" absolute values of k, d_v is the local degree of v, and the normalization of the absolute values is done in such a way that the product formula can be written

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

Using these properties of the height, one deduces the following lower bound: *let $P \in \mathbf{Z}[X_1, \ldots, X_q]$ be a polynomial of degree $\leq L_i$ in X_i, $(1 \leq i \leq q)$; denote by $L(P)$ the sum of the absolute values of the coefficients of P (*length of P*); let $\gamma_1, \ldots, \gamma_q$ be algebraic numbers, in a number field of degree D, such that P does not vanish at the point $(\gamma_1, \ldots, \gamma_q)$. Then*

$$\bigl|P(\gamma_1, \ldots, \gamma_q)\bigr| \geq L(P)^{-D} \prod_{i=1}^{q} e^{-DL_i \mathrm{h}(\gamma_i)}.$$

We conclude this section with a well-known open problem, due to Lehmer.

Let α be a non-zero algebraic number; a result due to Kronecker (which follows from what has been said above) is that $\mathrm{h}(\alpha) = 0$ *if and only if α is a root of unity.*

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 :

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

Lehmer's problem is : *does there exist a positive absolute constant c_0 such that $d\,\mathrm{h}(\alpha) \geq c_0$ for any non-zero algebraic number α which is not a root of unity and is of degree $\leq d$?*

The best partial result known in this direction is due to Dobrowolski [Do 1979]: *for each $\epsilon > 0$, there exists an integer $d_0(\epsilon)$ such that, for $d > d_0(\epsilon)$,*

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

§5. Zero estimates; Nullstellensatz

One important tool in transcendence proofs is the zero estimate. This is always a crucial step. In Liouville's Theorem, it's essential to check first $\alpha \neq p/q$; looking at the works of Hermite, Lindemann, Thue, Siegel, Dyson, Gel'fond, Schneider, Roth, Schmidt, Feldman ..., one realizes that many different types of arguments have been used in order to produce the non-zero algebraic number which will be estimated (from below

by arithmetic arguments, namely Liouville's inequality, and from above using analytic arguments). Masser was one of the first to investigate this problem in a systematic way. Among the tools which he introduced in this subject, an important one (which occurred in a joint work with Brownawell) is elimination with a resultant; Bézout's Theorem is also efficient in this context. More powerful methods from commutative algebra (connected with Chow forms) were then introduced by Yu. V. Nesterenko, and developped by Masser and Wüstholz, as well as Philippon. In another context (connected with the Thue-Siegel-Roth Theorem which will be considered in the third lecture), one of the most famous arguments which is used to prove that some number does not vanish is the so-called Dyson's lemma. There are several variants of this lemma, including a result of Esnault and Viehweg using algebraic geometry. After the work of Vojta which relates diophantine approximation (and diophantine geometry) to Nevanlinna's theory, Faltings proved a zero estimate which he called the "Product Theorem". Very recently (spring 1993), Faltings and Wüstholz announced a generalization of this result in connection with W.M.Schmidt's subspace Theorem (a generalization of the Thue-Siegel-Roth Theorem to higher dimension). Finally, we mention a recent paper due to Nakamaye [Na 1993] which contains new results (e.g. generalizations to algebraic groups which are not always commutative), and which includes also all necessary references.

Another related subject is *Hilbert Nullstellensatz*; in 1893, Hilbert proved: *let $\mathcal{A}$ be an ideal in the ring $R = \mathbf{C}[X_1, \ldots, X_n]$; assume $Q \in R$ vanishes on the zeroes of $\mathcal{A}$ in $\mathbf{C}$; then there exists a positive integer k such that $Q^k \in \mathcal{A}$.*

In particular (Bézout) if $\mathcal{A}$ has no zeroes, then $1 \in \mathcal{A}$; in 1929 Rabinowitsch proved that the Bézout case implies the general case. In Bézout case, if $\mathcal{A} = (P_1, \ldots, P_m)$, then one would like to know upper bounds for the degree of polynomials $A_1, \ldots, A_m$ satisfying a relation

$$A_1 P_1 + \cdots + A_m P_m = 1;$$

such estimates have been provided already in 1926 by G. Hermann, but the bounds were double exponential in terms of the number n of variables. Masser and Philippon gave examples which show that the bound must involve at least one exponential, while an example due to Mayr and Meyer showed that a double exponential is unavoidable to express elements of an ideal in terms of the generators. In 1987, W.D. Brownawell [Br 1987] obtained:

$$\max_{1 \leq i \leq m} \deg(A_i) \leq n^2 D^n + nD,$$

where D is the maximum of the degrees of $P_1, \ldots, P_m$. His proof involved analytic estimates due to Berenstein and Yger. Brownawell's result has been improved and extended by several authors, in particular Amoroso, Berenstein, Kollàr, Philippon, Shiffman, Yger. The best estimate known is valid in any characteristic: $\max_{1 \leq i \leq m} \deg(A_i) \leq D^n$ for $D \geq 3$. Also estimates for the coefficients of A_i (when one deals with polynomials with, say, integer coefficients) are available.

Lecture 2.– A proof of irrationality by a transcendence method

The original method of Hermite for the transcendence of e, which was generalized by Lindemann for the transcendence of π, involved a construction of an explicit "auxiliary function". One important step in the theory was provided by the work of Thue and Siegel [Si 1929] at the beginning of this century, when they introduced in this context the so-called Dirichlet Pigeonhole principle (principe des tiroirs, Schubfachprinzip). This means that the auxiliary function which they built was no more explicit; only the existence of it was asserted, using a counting principle. A few years ago, a new type of auxiliary function arose, introduced by M. Laurent [Lau 1989, 1990, 1992], where the pigeonhole principle is no more used; this is the path we shall follow. The same idea occurs also independently in a work by J. Pila [Pi 1993], in connection with the study of lattice points on curves [Pi 1991].

The proof we are going to give is not supposed to be the easiest one; what is important is that the scheme of proof enables one to prove more general results; some of these results (not their proofs) have been discussed in the first lecture; further ones will be considered in the following lectures.

We start with a complex number β and we define $\alpha = e^{\beta}$. Assume that both numbers α and β are algebraic; then the Theorem of Hermite-Lindemann asserts that $\beta = 0$ (and hence $\alpha = 1$).

For simplicity, we shall assume that α and β are rational numbers; the general case, where α and β are complex algebraic numbers, involves the same ideas (see §3); only a new zero estimate is needed.

We proceed in two stages; in the first one we assume that α and β are rational integers (which we denote respectively by a and b); we give a complete proof of the fact that $\beta = b$ vanishes. Next we assume only that these two numbers are rational; there is just one simple change to make in order to complete the proof.

§1. If b and $a = e^b$ are both integers, then $b = 0$

Assume $b \in \mathbf{Z}$ is such that $a = e^b$ also lies in $\mathbf{Z}$ (hence they are both in $\mathbf{N}$, that is non-negative). We want to prove $b = 0$. This is not a trivial result, and moreover it gives rise to an open problem, as follows (see the references in [Wa 1978]). Given two positive rational integers a and b, since $a \neq e^b$, one may ask for a lower bound for the difference $|a - e^b|$; K. Mahler was the first to consider this question, and he proved in 1953

$$|a - e^b| > \exp\{-40 \log a \log b\}$$

(provided that $a \geq 2$); 14 years later, he replaced 40 by 33; in 1973, M. Mignotte improved the constant down to 17.7. Mahler conjectured that *there exists an absolute constant $c > 0$ such that for $a \in \mathbf{Z}$ and $b \in \mathbf{Z}$ with $a \geq 2$,*

$$|a - e^b| > a^{-c};$$

the solution of this problem would probably involve new ideas which, as one might expect, should have other interesting applications. For instance the same method of proof enabled Mahler and Mignotte to derive irrationality measures for the number π, namely

$$\left|\pi - \frac{p}{q}\right| \geq q^{-21}, \qquad \text{for} \quad q \geq 2.$$

For sufficiently large q, the exponent 21 has been replaced recently by 13.398 (M. Hata). We now come to the proof that if b and $a = e^b$ are both rational integers, then $b = 0$.

Since $b \in \mathbf{Z}$ and $e^b \in \mathbf{Z}$, the two functions z and e^z take simultaneously their values in $\mathbf{Z}$ for $z = b$; from the addition Theorem which is satisfied by the exponential function, namely $e^{z_1+z_2} = e^{z_1}e^{z_2}$, one deduces that the values are also in $\mathbf{Z}$ for all $z \in \{0, b, 2b, \ldots\}$. Further, the differential equation $(d/dz)e^z = e^z$ shows that the derivatives of these two functions also take their values in $\mathbf{Z}$ for the same values of the variable z. Furthermore, for each $\tau \in \mathbf{N}$ and $t \in \mathbf{N}$, the function $f_{\tau t}(z) = z^{\tau}e^{tz}$ has the same property, namely

$$\left(\frac{d}{dz}\right)^{\sigma} f_{\tau t}(sb) \in \mathbf{Z} \qquad \text{for all } \sigma \in \mathbf{N} \text{ and } s \in \mathbf{N}.$$

The first idea is to put all these numbers into a matrix; we shall consider only finite matrices, and, to begin with, only square matrices. For this reason we choose four (large) positive integers T_0, T_1, S_0, S_1, with $T_0T_1 = S_0S_1$, we put $L = T_0T_1 = S_0S_1$, and we consider the L^2 numbers

$$\left(\frac{d}{dz}\right)^{\sigma} f_{\tau t}(sb) = \sum_{\kappa=0}^{\min\{\tau,\sigma\}} \kappa! \binom{\tau}{\kappa}\binom{\sigma}{\kappa} t^{\sigma-\kappa}(sb)^{\tau-\kappa}a^{ts}$$

for $0 \leq \tau < T_0$, $0 \leq t < T_1$, $0 \leq \sigma < S_0$ and $0 \leq s < S_1$. In order to put them into a matrix, we choose any ordering for the pairs (τ, t), and also for the pairs (σ, s); a change of these orderings will multiply the determinant of the matrix by a factor ± 1, but we are interested only in the absolute value of this determinant.

Now define

$$\Delta = \det\Big((d/dz)^{\sigma}\big(z^{\tau}e^{tz}\big)(sb)\Big)_{(\tau,t);(\sigma,s)},$$

where (τ, t) is the index of rows, $(0 \leq \tau < T_0,\ 0 \leq t < T_1)$, while (σ, s) is the index of columns, $(0 \leq \sigma < S_0,\ 0 \leq s < S_1)$. Since the entries of the matrix are in $\mathbf{Z}$, we plainly have $\Delta \in \mathbf{Z}$. The goal is to show $|\Delta| < 1$, which implies (a special case of Liouville's inequality !) $\Delta = 0$, and from this fact we shall conclude $b = 0$ (using a *zero estimate*).

a) Upper bound for $|\Delta|$

The idea, as we said, is due to Michel Laurent [La 1989]. We start with a simple case, where derivatives are not involved.

Lemma 2.1. – *Let r and R be two real numbers with $0 < r \le R$, $f_1, \ldots, f_L$ be functions of one complex variable, which are analytic in the disk $|z| \le R$ of $\mathbf{C}$, and let $\zeta_1, \ldots, \zeta_L$ belong to the disk $|z| \le r$. Then the determinant*

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

is bounded from above by

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

As usual, we have denoted by $|f|_R$ the number $\sup\{|f(z)|\,;\,|z| \le R\}$ when f is analytic in the disk $\{z \in \mathbf{C}\,;\,|z| \le R\}$ of $\mathbf{C}$. 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 $|z| \le R/r$.
a) We first prove that Ψ has a zero of multiplicity at least $L(L-1)/2$ 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 $f_\lambda(z) = z^{n_\lambda}$, for some non-negative integer n_λ, $(1 \le \lambda \le L)$; 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_λ are pairwise distinct, and the sum $n_1 + \cdots + n_L$ is at least $0 + 1 + \cdots + (L-1) = L(L-1)/2$; hence we find the factor $z^{L(L-1)/2}$ which we wanted.

The fact that $\Psi(z)$ vanishes at 0 with multiplicity $\ge L(L-1)/2$ can also be checked by taking derivatives of Ψ:

$$\left(\frac{d}{dz}\right)^s \Psi(z) = \sum_{\sigma_1+\cdots+\sigma_L=s} \frac{s!}{\sigma_1!\cdots\sigma_L!} \det\Big((d/dz)^{\sigma_\mu} f_\lambda(z\zeta_\mu)\Big)_{1\le\lambda,\mu\le L}.$$

At the point $z = 0$, if one at least of the determinants at the right hand side does not vanish, then the numbers σ_μ are pairwise distinct, hence $s = \sigma_1 + \cdots + \sigma_L$ is at least $L(L-1)/2$.
b) We now use Schwarz lemma: *for an analytic function Ψ of one complex variable having a zero of multiplicity $\ge T$ at 0, and for $0 < r_1 \le R_1$, we have*

$$|\Psi|_{r_1} \le (R_1/r_1)^{-T} |\Psi|_{R_1}.$$

With $T = L(L-1)/2$, $r_1 = 1$ and $R_1 = R/r$ we get

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

The upper bound

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

which we obtain by expanding the determinant and by using a trivial upper bound for each of the $L!$ terms, yields the desired conclusion. □

Now we include derivatives.

Lemma 2.2. – *Let $f_1, \ldots, f_L$ be entire functions in $\mathbf{C}$, $\zeta_1, \ldots, \zeta_L$ be elements of $\mathbf{C}$, $\sigma_1, \ldots, \sigma_L$ non-negative integers, and $0 < r \le R$ be real numbers. Assume $|\zeta_\mu| \le r$ for $1 \le \mu \le L$. Then the determinant*

$$\Delta = \det\Big((d/dz)^{\sigma_\mu} f_\lambda(\zeta_\mu)\Big)_{1\le\lambda,\mu\le L}$$

is bounded from above by

$$|\Delta| \le \left(\frac{R}{r}\right)^{-L(L-1)/2+\sigma_1+\cdots+\sigma_L} L! \prod_{\lambda=1}^{L} \max_{1\le\mu\le L} \sup_{|z|=R} \big|(d/dz)^{\sigma_\mu} f_\lambda(z)\big|.$$

Proof. We claim that the function of one variable

$$\Psi(\zeta) = \det\Big((d/dz)^{\sigma_\mu}\big(f_\lambda(\zeta\zeta_\mu)\big)\Big)_{1\le\lambda,\mu\le L}$$

has a zero at the origin of multiplicity

$$\ge L(L-1)/2 - \sigma_1 - \cdots - \sigma_L.$$

By multilinearity we reduce the proof of this claim to the case $f_\lambda(z) = z^{n_\lambda}$ for some $n_\lambda \in \mathbf{N}$, $(1 \le \lambda \le L)$. In this case we have

$$\Psi(\zeta)\zeta^{\sigma_1+\cdots+\sigma_L} = \sigma_1!\cdots\sigma_L!\zeta^{n_1+\cdots+n_L} \det\left(\binom{n_\lambda}{\sigma_\mu}\zeta_\mu^{n_\lambda-\sigma_\mu}\right)_{1\le\lambda,\mu\le L}$$

where the binomial coefficient $\binom{n_\lambda}{\sigma_\mu}$ means 0 if $\sigma_\mu > n_\lambda$. If the right hand side is not identically zero, then the numbers $n_1, \ldots, n_L$ are pairwise distinct, and then the right hand side has a zero at the origin of multiplicity $n_1 + \cdots + n_L$. Our claim on the order of vanishing of Ψ at the origin easily follows.

Here again, like in the proof of lemma 2.1, one could check directly that the first $L(L-1)/2 - \sigma_1 - \cdots - \sigma_L$ derivatives of Ψ vanish at 0.

We conclude the proof of lemma 2.2 by means of the Schwarz lemma, just as in lemma 2.1. □

From lemma 2.2 we shall derive the following estimate:

Lemma 2.3. – *Let b be any complex number. Let T_0, T_1, S_0, S_1 and L be positive integers with $L = T_0T_1 = S_0S_1$. Let Δ be the determinant of the matrix*

$$\Bigl((d/dz)^\sigma\bigl(z^\tau e^{tz}\bigr)(sb)\Bigr)_{(\tau,t);(\sigma,s)}.$$

Then

$$\frac{1}{L}\log|\Delta| \le -L + S_0 + \log L + S_0\log(T_0+T_1) + T_0\log R + T_1R,$$

where $R = \max\{1, e^2|b|S_1\}$.

Proof. We use Lemma 2.2 with $r = S_1|b|$, and f_λ replaced by $f_{\tau t}$, while the points ζ_μ are $\{0, b, 2b, \ldots, (S_1-1)b\}$, each of these being repeated S_0 times. We need an upper bound for $\sup_{|z|=R}\bigl|(d/dz)^\sigma f_{\tau t}(z)\bigr|$; we develop

$$(d/dz)^\sigma f_{\tau t}(z) = \sum_{\kappa=0}^{\min\{\tau,\sigma\}}\kappa!\binom{\tau}{\kappa}\binom{\sigma}{\kappa}t^{\sigma-\kappa}z^{\tau-\kappa}e^{tz},$$

and bound $\kappa!\binom{\tau}{\kappa}$ by τ^κ:

$$\sum_{\kappa=0}^{\min\{\tau,\sigma\}}\kappa!\binom{\tau}{\kappa}\binom{\sigma}{\kappa}t^{\sigma-\kappa} \le (\tau+t)^\sigma \le (T_0+T_1)^{S_0},$$

hence

$$\max_{0\le\sigma<S_0}\sup_{|z|=R}\bigl|(d/dz)^\sigma\log|f_{\tau t}(z)|\bigr| \le (T_0+T_1)^{S_0}R^{T_0}e^{T_1R}.$$

The conclusion of lemma 2.3 easily follows. □

One important step in all transcendence proofs comes now: we need to choose our parameters. Here, we would like that the dominating term in the right hand side of the conclusion of lemma 2.3 be $-L$, in such a way that one could conclude $\log|\Delta| < 0$, which means $|\Delta| < 1$. Hence our requirement is

$$L > S_0 + \log L + S_0\log(T_0+T_1) + T_0\log R + T_1R. \tag{2.4}$$

A rather natural idea is to assume that the four parameters T_0, T_1, S_0 and S_1 are relatively large with respect to b, and to consider only the asymptotic behaviour. There are plenty of reasonable choices; we just provide one example. Choose a large integer N (a new parameter), and define

$$T_0 = S_0 = N^2, \qquad T_1 = S_1 = N,$$

so that $L = N^3$, while the right hand side of (2.4) is only $O(N^2\log N)$ for $N \to \infty$. Therefore, for N sufficiently large (a condition which can easily be explicitly written), we deduce the desired upper bound $|\Delta| < 1$.

b) The zero estimate

Assume that a determinant of the form

$$\det\Bigl((d/dz)^{\sigma_\mu}f_\lambda(\zeta_\mu)\Bigr)_{1\le\lambda,\mu\le L}$$

vanishes. This means that there exist complex numbers $c_1, \ldots, c_L$, which do not all vanish, such that the function

$$F = \sum_{\lambda=1}^{L}c_\lambda f_\lambda$$

satisfies

$$(d/dz)^{\sigma_\mu}F(\zeta_\mu) = 0 \qquad \text{for } 1 \le \mu \le L.$$

Generally speaking, a *zero estimate* states that this can happend only in "trivial" circumstances. Here, the f_λ are exponential polynomials with **real** frequencies, and the points ζ_μ are **real**. We shall use the following result, which was introduced in a similar context by A.O. Gel'fond and Yu.V. Linnik [GL 1962].

Lemma 2.5. – *Let $a_1, \ldots, a_n$ be non-zero polynomials in $\mathbf{R}[t]$ of degrees $d_1, \ldots, d_n$, and let $w_1, \ldots, w_n$ be pairwise distinct real numbers. Then the real function of one real variable*

$$F(x) = \sum_{i=1}^{n}a_i(x)e^{w_ix}$$

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

In this result the zeroes are counted with multiplicities. Simple arguments from linear algebra show that the upper bound in lemma 2.5 is best possible.

Proof. We first prove the following result: *let N be a positive integer; if a N-times continuously differentiable real function F of one real variable has at least N real zeroes (counting multiplicities), then its derivative F' has at least $N-1$ real zeroes.*

Indeed, let $x_1, \ldots, x_k$ (with $k \ge 1$) be pairwise distinct real zeroes of F, in increasing order: $x_1 < x_2 < \cdots < x_k$; let $n_1, \ldots, n_k$ be positive integers, with $n_1 + \cdots + n_k \ge N$; assume x_i is a zero of F with multiplicity $\ge n_i$, $(1 \le i \le k)$. Then x_i is a zero of F' with multiplicity $\ge n_i - 1$, $(1 \le i \le k)$; moreover, since $F(x_i) = F(x_{i+1})$ for $1 \le i \le k-1$, it follows from Rolle's Theorem that F' has at least one zero in the open interval (x_i, x_{i+1}). Therefore F' has at least

$$(n_1 - 1) + \cdots + (n_k - 1) + (k-1) \ge N - 1$$

real zeroes. This proves the preliminary statement.

We now prove lemma 2.5 by induction on the integer $k = d_1 + \cdots + d_n + n$. In the case $k = 1$, we have $n = 1$ and the result is obvious. Assume $k \ge 2$. After multiplication of F by e^{-w_nx}, we may assume $w_n = 0$. Hence $w_i \ne 0$ for $1 \le i < n$. Let N be a positive integer such that F has at least N real zeros; then, as we have seen, its derivative F' has at least $N-1$ real zeros. However, since $w_n = 0$, we have

$$F'(x) = \sum_{i=1}^{n-1} \tilde{a}_i(x) e^{w_i x} + (d/dx) a_n(x)$$

where

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

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

c) Conclusion of the proof

We just put together all previous information. Again, let a and b in $\mathbf{Z}$ satisfy $a = e^b$. Let N be a sufficiently large integer; define, as above,

$$T_0 = S_0 = N^2, \qquad T_1 = S_1 = N, \qquad L = N^3,$$

and

$$\Delta = \det\Big((d/dz)^\sigma \big(z^\tau e^{tz}\big)(sb) \Big)_{(\tau,t);(\sigma,s)}.$$

From part a) of the proof, we know that $|\Delta| < 1$ (provided that N has been chosen large enough). Hence there exist (rational) numbers $c_{\tau t}$, not all of which are zero, such that the exponential polynomial

$$F = \sum_{\tau=0}^{T_0-1} \sum_{t=0}^{T_1-1} c_{\tau t} z^\tau e^{tz}$$

vanishes at each point sb, $(0 \le s < S_1)$, with multiplicity $\ge S_0$. According to lemma 2.3, the total number of zeroes of F is strictly less than $T_0 T_1 = L = S_0 S_1$. Hence the numbers sb, $(0 \le s < S_1)$ are not pairwise distinct, which means $b = 0$.

§2. If b and $a = e^b$ are both rational numbers, then $b = 0$

We now prove an irrationality result: if b and $a = e^b$ are both rational numbers, then $b = 0$. There are easy proofs for the irrationality of e or of e^2, involving either the Taylor expansion of the exponential function, or the algorithm of continued fractions (Euler, Fourier, Liouville); but these arguments, as far as I know, do not yield the irrationality of e^b for all non-zero $b \in \mathbf{Q}$.

Again, there is an open problem of diophantine approximation, which is to give a quantitative refinement to the qualitative result: does there exist an absolute constant $c > 0$ such that, for m, n, p and q positive integers,

$$\left| e^{m/n} - \frac{p}{q} \right| > \max\{m, n, p, q\}^{-c}?$$

Of course the case $n = q = 1$ is just Mahler's Conjecture above. In this direction, only a partial result is known:

$$\left| e^{m/n} - \frac{p}{q} \right| > \exp\{-2^{42}(\log p)(\log m + \log n + \log\log p)\} \qquad \text{for} \quad p \ge 3;$$

it should not be difficult to improve the numerical constant 2^{42}, but it does not seem easy to sharpen significantly this estimate.

A related open problem is to prove that e^π is not a Liouville number: *does there exist a constant $C > 0$ such that $|e^\pi - p/q| > q^{-C}$ for all $p/q \in \mathbf{Q}$?* The best estimate known is

$$\left| e^{\pi} - \frac{p}{q} \right| > \exp\{-2^{60}(\log q)(\log\log q)\} \qquad \text{for} \quad q \ge 3.$$

We now come to the proof of the claimed irrationality result. We repeat the above arguments; obviously, the only point where the proof has to be modified is the fact that $|\Delta| < 1$ implies $\Delta = 0$. Here, Δ is merely a rational number; what we need is an upper bound for its denominator, and also a better upper bound for its absolute value.

We start with the last point; if we replace the condition (2.4) by

$$L/2 > S_0 + \log L + S_0 \log(T_0 + T_1) + T_0 \log R + T_1 R, \tag{2.6}$$

then we improve the upper bound from $|\Delta| < 1$ down to

$$\log |\Delta| < -L^2/2,$$

which is much stronger. Of course the choice of parameters $T_0 = S_0 = N^2$, $T_1 = S_1 = N$ is sufficient to guarantee (2.6).

The upper bound for the denominator of Δ is not hard. For each τ, t, σ and s in the usual ranges, the number

$$(d/dz)^\sigma \big(z^\tau e^{tz}\big)(sb)$$

is the value, at the point (a, b), of a polynomial with rational integer coefficients; the degree in a is at most $T_1 S_1$, and the degree in b is at most T_0. Hence a denominator is

$$(\text{den } a)^{T_1 S_1} (\text{den } b)^{T_0}$$

and a denominator for Δ is

$$(\text{den } a)^{L T_1 S_1} (\text{den } b)^{L T_0}.$$

Since $T_1 S_1$ and T_0 are, for our choice of parameters, $O(N^2 \log N)$, while $L = N^3$, one deduces that the integer $\Delta \cdot \text{den } \Delta$ has absolute value < 1, hence vanishes, which is what we wanted.

§3. A Proof of the Theorem of Hermite-Lindemann

Let $\beta \in \mathcal{L} \cap \bar{\mathbf{Q}}$. We want to prove $\beta = 0$. Define $\alpha = e^{\beta}$. We choose a sufficiently large constant c, and integers T_0, T_1, S_0 and S_1, all of which are ≥ 2, such that, if we set $L = T_0 T_1$, then

$$cT_0 \log S_1 \leq L, \qquad cS_0 \log(T_0 + T_1) \leq L, \qquad cT_1 S_1 \leq L,$$

and

$$cL \leq S_0 S_1.$$

The difference with the situation in the previous sections is only in the last inequality, which replaces the equality between L and $S_0 S_1$ which took place above. For instance one can take

$$T_1 = S_1 = N \qquad T_0 = N^2, \qquad \text{and} \qquad S_0 = N^2 \log N,$$

where N is a sufficiently large integer. We select L elements $(\sigma^{(\mu)}, s^{(\mu)})$ in $\mathbf{Z}^2$ with $0 \leq \sigma^{(\mu)} < S_0$ and $|s^{(\mu)}| < S_1$, and we consider the $L \times L$ determinant

$$\Delta = \det\Bigl((d/dz)^{\sigma^{(\mu)}} \bigl(z^{\tau} e^{tz}\bigr)(s^{(\mu)}\beta) \Bigr)_{(\tau,t);\mu},$$

where (τ, t) is the index of rows, $(0 \leq \tau < T_0,\ 0 \leq t < T_1)$, while μ is the index of columns, $(1 \leq \mu \leq L)$. We get, using Schwarz lemma as before,

$$\log |\Delta| \leq -L^2 + c_1 L (S_0 \log(T_0 + T_1) + T_0 \log S_1 + T_1 S_1),$$

where c_1 is a positive constant (like c_2 below) which depends only on β. From Liouville's inequality we deduce that if Δ does not vanish, then

$$\log |\Delta| \geq -c_2 L (S_0 \log(T_0 + T_1) + T_0 \log S_1 + T_1 S_1).$$

Again we conclude $\Delta = 0$. This shows that the matrix

$$\Bigl((d/dz)^{\sigma} \bigl(z^{\tau} e^{tz}\bigr)(s\beta) \Bigr)_{(\tau,t);(\sigma,s)} \qquad \text{with} \qquad \begin{cases} 0 \leq \tau < T_0, & 0 \leq t < T_1, \\ 0 \leq \sigma < S_0, & |s| < S_1 \end{cases}$$

is of rank $< L$. From a zero estimate due to Philippon [P 1986] (see also [W 1992] Proposition 11.2) we conclude $\beta = 0$. $\square$

Lecture 3.– Diophantine approximation and linear forms in logarithms

We first discuss a problem involving only rational integers, which is closely related to Baker's Theorem on linear independence of logarithms of algebraic numbers. Next we consider other related problems of diophantine approximation.

§1. Lower bounds for the distance between 1 and a product of powers of rational integers

Baker's theorem shows that numbers of the form

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

(with algebraic β_i, $0 \leq i \leq m$, and algebraic α_j, $1 \leq j \leq m$) 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 when $\beta_0 = 0$, $\beta_i \in \mathbf{Z}$, and $\alpha_i \in \mathbf{Z}$, $\alpha_i \geq 2$.

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

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

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:

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

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 (*Liouville's inequality*).

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

$$0 < \Bigl| a_1^{b_1} \cdots a_m^{b_m} - 1 \Bigr| \leq \frac{1}{2},$$

then

$$\frac{1}{2} \bigl| b_1 \log a_1 + \cdots + b_m \log a_m \bigr| \leq \Bigl| a_1^{b_1} \cdots a_m^{b_m} - 1 \Bigr| \leq 2 \bigl| b_1 \log a_1 + \cdots + b_m \log a_m \bigr|.$$

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 now yields:

Lemma 3.1. – *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 $B \geq 2m \log A$, there exist rational integers $b_1, \ldots, b_m$ with*

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

such that

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

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 3.1 is closer to the truth than Liouville's lower bound.

In 1935, one year after he had solved Hilbert's seventh problem, Gel'fond (see the references in [G 1952] and [Ba 1976]) 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 $(b_1, b_2) \in \mathbf{Z}^2$ with $(b_1, b_2) \neq 0$, if we set $B = \max\{|b_1|, |b_2|, 2\}$, then

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

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 $m \geq 2$ (see [G 1952] Th. III):

Theorem 3.2 (Gel'fond's ineffective estimate). – *For every m-tuple $(a_1, \ldots, a_m)$ of positive multiplicatively independent rational integers, and for every $\delta > 0$, there exists a positive constant $C_2 = C_2(a_1, \ldots, a_m, \delta)$ such that, if $b_1, \ldots, b_m$ are rational integers, not all of which are zero, and if we set $B = \max\{|b_1|, \ldots, |b_m|, 2\}$, then*

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

For the proof of Theorem 3.2, 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 [Ro 1955]:

Theorem 3.3 (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 3.2.

We shall use Theorem 3.3 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 $b = (b_1, \ldots, b_m) \in \mathbf{Z}^m$ with

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

(where, as usual, $B = \max\{2, |b_1|, \ldots, |b_m|\}$). Hence the set E_1 of $b \in \mathbf{Z}^m$ 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 $(\mathbf{Z}/N\mathbf{Z})^m$ 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 $r \in \mathbf{N}^m$ 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 $x \in \mathbf{Z}^m$ 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

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

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 3.3 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 3.2 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 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 saw in the first lecture, this problem was solved in 1966 by A. Baker. A refinement due to N.I. Fel'dman [F 1968] two years later gives

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

where $C_3=C_3(a_1,\ldots,a_m)$ is a positive effectively computable number. An important consequence of Feldman's result is an effective improvement on Liouville's Theorem: for each algebraic number α of degree $d\ge 3$, there exists two positive constants $c(\alpha)$ and $\eta(\alpha)$ such that, for $p/q\in\mathbf{Q}$,

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

Recent related results are due to Bombieri [Bo 1993].

§2. Recent results and Conjectures

The number C_3 has been explicitly computed; in [PW 1986], it is shown that one can take

$$C_4(m)\log a_1\cdots\log a_m$$

with $C_4(m)=2^{8m+53}m^{3m}$ (this constant has been computed only under the assumption $B\ge\log a_j$, because a more general situation was considered, where the b_j are replaced

by algebraic numbers; when they are rational integers, this assumption is unnecessary). The same result (but with an unspecified value for $C_4(m)$) appears in [Wü 1985]. Another method [W 1992] gives $C_4(m)=2^{4m+16}m^{3m+5}$. Baker [Ba 1991] anounces a forthcoming joint paper with Wüstholz including the estimate with $C_4(m)=(16m)^{2(m+2)}$.

The case $m=2$ is specially important for applications; the first explicit estimates (with arithmetic applications) go back to 1967 (A. Schinzel). Very recently [LauMiNe 1993], Laurent, Mignotte and Nesterenko obtained the following result:
Let b_1 and b_2 be two positive integers and α_1 and α_2 be two multiplicatively independent algebraic numbers in a number field of degree D; let A_1 and A_2 be positive real numbers satisfying $\log A_i\ge\max\{1,\mathrm{h}(\alpha_i)\}$ for $i=1,2$. Define

$$b'=\frac{b_1}{\log A_2}+\frac{b_2}{\log A_1};$$

then

$$|b_2\log\alpha_2-b_1\log\alpha_1|\ge\exp\{-25D^4(0.6+\log b')^2\log A_1\log A_2\}.$$

The dependence in $B=\max\{b_1,b_2\}$ is not as good as before: there is essentially $(\log B)^2$ in place of $\log B$, but the constant is very small, and this is important for applications (see section 3 below).

Another case where very sharp numerical constants are known arises in the work of Rhin, Dubois and Toffin, using very different techniques, related with Padé approximation and Siegel's G-functions [Rh 1986]: *for rational integers b_0, b_1 and b_2 with $B=\max\{|b_1|,|b_2|\}\ge 2$,*

$$|b_0+b_1\log 2+b_2\log 3|\ge B^{-13.3}.$$

A related method (initiated by F. Beukers) has been developed by M. Bennett in order to produce sharp lower bound for $\|\left(1+(1/N)\right)^k\|$ (distance to the nearest integer), which are much better than the estimates which can be deduced from lower bounds for linear forms in logarithms. The case $N=2$ is specially important in view of Waring's problem.

The method of Padé approximations for diophantine problems has been developed recently by Yu.V. Nesterenko. There is also a recent work by P. Bundschuh, which yields strong measures of linear independence, but nor for logarithms of algebraic numbers.

Finally, p-adic estimates for linear forms in logarithms have been considered by several authors: Mahler, Schinzel, Brumer, van der Poorten, Loxton, and, more recently, by Yu Kunrui [Yu 1989], and by Dong Pingping [Dpp 1992]; Yu found an efficient way of avoiding the assumption that the α_i are closed to 1 modulo p, and Dong reached improved estimates when one considers *simultaneous* linear forms).

The second part of Lang's book [La 1978] 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 $C_5(\epsilon)>0$ such that

$$\left|a_1^{b_1}\cdots a_m^{b_m}-1\right|\ge\frac{C_5(\epsilon)^m}{B^{m-1+\epsilon}A^{m+\epsilon}}.$$

This is related to a conjecture of Hall: if x and y are positive integers with $y^2 \neq x^3$, then
$$|y^2 - x^3| \geq C \max\{y^2, x^3\}^{1/6},$$
and also to the *abc* conjecture (see below).

The results we mentioned (as well as the conjectures) are valid more generally when the integers $a_1, \ldots, a_m$ are replaced by algebraic numbers; they can be also (partially) extended to the case where $b_1, \ldots, b_m$ also are replaced by algebraic numbers; in this case it is more convenient to state the result as a lower bound for a linear combination of logarithms of algebraic numbers, and the more general estimates deal with lower bounds for numbers like (cf [PW 1986])
$$\beta_0 + \beta_1 \log \alpha_1 + \cdots + \beta_m \log \alpha_m.$$
Estimates from below for such numbers are called (by Gel'fond, and later by Baker) *lower bounds for linear forms in logarithms*; in the next section we quote a few consequences of them.

Methods of proof. We say a few words on the ideas which are involved in proving lower bounds for linear forms in logarithms. Assume a number
$$\left|\log \alpha_{k+1} - \sum_{i=1}^{k} \beta_i \log \alpha_i\right|$$
is *small*. Consider the determinant Δ of the matrix
$$\left(\prod_{i=1}^{k} (s_i + s_{k+1}\beta_i)^{\tau_i} \prod_{i=1}^{k+1} \alpha_i^{s_i t}\right)_{(\tau,t);s}.$$
The general scheme of the proof is roughly as follows: a zero estimate (Philippon) gives $\Delta \neq 0$; Liouville's inequality provides a lower bound for $|\Delta|$; an upper bound for this number is obtained by introducing an interpolation determinant (*alternant*). Comparing the upper bound with the lower bound provides the desired estimate.

For the zero estimate as well as for the analytic upper bound, there are essentially two methods (corresponding to the solutions by Gel'fond and Schneider of Hilbert's seventh problem).

To start with, assume first $k = 1$; Gel'fond's proof involves the functions
$$f_s(z) = e^{(s_1 + s_2\beta_1)z},$$
which satisfy
$$\left(\frac{d}{dz}\right)^{\tau} f_s(t \log \alpha_1) = (s_1 + s_2\beta_1)^{\tau} \alpha_1^{s_1 t} \bigl(\alpha_1^{\beta_1}\bigr)^{s_2 t}.$$
On the other hand Schneider's proof introduces the functions
$$g_{\tau t}(z) = z^{\tau} \alpha_1^{tz},$$

where
$$g_{\tau t}(s_1 + s_2\beta_1) = (s_1 + s_2\beta_1)^{\tau} \alpha_1^{s_1 t} \bigl(\alpha_1^{\beta_1}\bigr)^{s_2 t}.$$
We now extend to the case $k \geq 2$.

We define $\gamma_i = \alpha_i$ for $1 \leq i \leq k$ and
$$\gamma_{k+1} = \alpha_1^{\beta_1} \cdots \alpha_k^{\beta_k}.$$
The generalization of Gel'fond's method by Baker uses the functions of k variables:
$$f_s(z) = \exp\{(s_1 + s_{k+1}\beta_1)z_1 + \cdots + (s_k + s_{k+1}\beta_k)z_k\},$$
which satisfy
$$D^{\tau} f_s(t \log \alpha_1, \ldots, t \log \alpha_k) = \prod_{i=1}^{k} (s_i + s_{k+1}\beta_i)^{\tau_i} \prod_{i=1}^{k+1} \gamma_i^{s_i t},$$
while the generalization of Schneider's method uses the functions
$$g_{\tau t}(z) = z_1^{\tau_1} \cdots z_k^{\tau_k} \bigl(\alpha_1^{z_1} \cdots \alpha_k^{z_k}\bigr)^t,$$
with
$$g_{\tau t}(s_1 + s_{k+1}\beta_1, \ldots, s_k + s_{k+1}\beta_k) = \prod_{i=1}^{k} (s_i + s_{k+1}\beta_i)^{\tau_i} \prod_{i=1}^{k+1} \gamma_i^{s_i t}.$$

§3. Applications

In [Ba 1991], applications of lower bounds for linear forms in logarithms to the following questions are quoted: class number problems (Baker-Stark), p-adic L-functions (Ax-Brumer), Knot theory (Riley), modular forms (Odoni), Ramanujan τ function (Murty), primitive divisors (Schinzel, Stewart), diophantine equations (Gel'fond and many others, including Baker).

Recent estimates have been produced recently by Glass et al. in Bowling Green, and by M. Mignotte, concerning Catalan's equation:
$$x^p - y^q = 1.$$
It had been proved by R. Tijdeman [T 1976] that this equation has only finitely many solutions in integers x, y, p, q, all of which are ≥ 2 (the only known solution is $(x, y, p, q) = (3, 2, 2, 3)$); using the above mentioned improved estimate for linear forms in logarithms, Mignotte is now able to prove, for each solution x, y, p, q, the upper bound $\max\{p, q\} \leq 2.15 \cdot 10^{24}$. Also there are no solutions with $\min\{p, q\} \leq 59$.

Another application of lower bounds for linear forms in logarithms deals with the *abc* conjecture of Masser and Oesterlé, which reads as follows: *for each* $\epsilon > 0$ *there exists* *a positive number* $\kappa(\epsilon)$ *which has the following property: if* a, b *and* c *are three positive rational integers which are relatively prime, with* $a+b=c$, *and if*

$$G = \prod_{p|abc} p$$

denotes the squarefree part of the product abc, *then*

$$c < \kappa(\epsilon) G^{1+\epsilon}.$$

The example $a=1$, $c=3^{2^n}$, $b=c-a$ (where 2^n divides b) shows that the exponent $1+\epsilon$ cannot be replaced by 1. This conjecture is related to a conjecture of Szpiro on the conductor of elliptic curves; an analog of the *abc* conjecture for function fields is a Theorem of Mason (see [La 1993]). Using (p-adic) lower bounds for linear forms in logarithms, Tijdeman, Stewart and Yu Kunrui (see [SY 1993]) reached the first estimate in the direction of the *abc* conjecture:

$$\log c \le \kappa(\epsilon) G^{(2/3)+\epsilon}.$$

The *abc* conjecture obviously implies the following statement: *there exist only finitely many quadruples* (x,y,z,n) *of positive integers with* $\gcd(x,y,z)=1$ *and* $n \ge 3$ *satisfying* $x^n+y^n=z^n$; more generally, N. Elkies [E 1991] has shown that the *abc* conjecture implies Mordell's Conjecture (which is now Falting's Theorem).

Improvement on the constants for linear forms in logarithms are relevant when one tries to solve explicitly some diophantine equations; there have been many papers on solving such equations recently. Here is a sample of results.

R. Steiner proved that the largest solution to the diophantine equation

$$y^2 + 999 = x^3$$

is $(x,y) = (22480, 3370501)$.

Tzanakis and de Weger proved that the Thue-Mahler equation

$$x^3 - 23x^2y + 5xy^2 + 24y^3 = \pm 2^{z_1} 3^{z_2} 5^{z_3} 7^{z_4}$$

has precisely 72 solutions with $(x,y)=1$, $x>0$.

It is now possible to give complete sets of solutions for families of diophantine equations (E. Thomas, Mignotte, Tzanakis, Pethő, Roth); for instance the diophantine equation

$$x^3 - (n-1)x^2y - (n+2)xy^2 - y^3 = 1$$

has only the trivial solutions $(1,0)$, $(0,-1)$ and $(-1,1)$ for all $n \ge 4$.

The following question raised by R. Graham (concerning Radon transforms) has been solved by Stroeker and de Weger: the diophantine equation

$$6x^2(x^2-1) + 9 = y^2$$

has only the integer solutions $(x,y) = (0,3)$, $(1,3)$, $(2,9)$, $(3,21)$, $(6,87)$, $(91,20283)$. It has been noticed by H.W. Lenstra that these solutions correspond for $t=2x-1$ to the solutions $(t,k) = (1,3)$, $(3,4)$, $(5,5)$, $(11,7)$ and $(181,15)$ of the Ramanujan-Nagell equation

$$t^2 + 7 = 2^k.$$

Another recent progress is a *sieving argument* due to R. Pinch, using linear recurrence sequences, to show that there are no "small" solutions to certain diophantine equations; he reduces the so-called Shimura-Taniyama-Weil conjecture to checking that some diophantine equations (a typical one being $y^2 = x^3 + 1728k$) have exactly the set of complete integer solutions which are conjectured; sieving uses only single precision for verifying solution sets.

Study of diophantine equations by means of lower bounds for linear forms in logarithms introduces *Siegel's equation*

$$a_1\epsilon_1 + a_2\epsilon_2 = 1;$$

when K is a given number field, and a_1, a_2 two non-zero elements in K, this equation has only finitely many solutions in units (ϵ_1, ϵ_2) of K; moreover all these solutions can be effectively determined.

The work of W.M. Schmidt on simultaneous diophantine approximation makes it possible, as shown by Evertse, van der Poorten and Schlickewei, to prove that the more general equation

$$a_1\epsilon_1 + \cdots + a_n\epsilon_n = 1.$$

also has only finitely many solutions where no subsum vanishes; but the result is still not effective: upper bounds for the number of solutions are being worked out nowadays, but the proof does not allow one to bound the size of the solutions themselves.

Several people recently achieved strong estimates for the number of solutions of certain diophantine equations, including E. Bombieri, W.M. Schmidt, J. Silverman, J.H. Evertse, M. Bean, P. Voutier. A closely related problem is to estimate the number of rational points of bounded height on algebraic varieties (S. Schanuel, J. Silverman, P. Vojta, Yu.I. Manin, W.M. Schmidt, J. Thunder, Y. Tschinkel, V. Batyrev, N.A. Nikishine and M.M. Skriganov; see [Ts 1991]).

Lecture 4.– Algebraic groups

In the previous three lectures, we were dealing only with the usual exponential function; a couple of times, we used the words "linear algebraic group", because we were working in fact with the product ${\mathbf{G}_\mathrm{a}}^{d_0} \times {\mathbf{G}_\mathrm{m}}^{d_1}$ of d_0 copies of the additive group by d_1 copies of the multiplicative group. The results can be extended to any commutative algebraic group over the field of algebraic numbers. We first consider elliptic curves, then we quote briefly the general case.

§1. Elliptic curves

It was already noted by Bachet de Méziriac that, given a polynomial f of degree 3 in two variables with rational coefficients, the chord and tangent process enables one to construct, from a given rational solution to the diophantine equation $f(x,y)=0$, other rational solutions. The group structure which is underlying is the Mordell-Weil group of the elliptic curve, which was already studied by Poincaré.

Let g_2 and g_3 be two complex algebraic numbers such that $g_2^3 \neq 27g_3^2$; we consider the elliptic curve

$$E = \{(t:x:y) \in \mathbf{P}_2\,;\, y^2t = 4x^3 - g_2xt^2 - g_3t^3\}.$$

The complex points $E(\mathbf{C})$ on E form a group (the intersection of this cubic with a line has three points, whose sum vanishes); the neutral element is $(0:0:1)$. The points of $E(\mathbf{C})$ are parametrized by

$$\exp_E = (1:\wp:\wp') : \mathbf{C} \longrightarrow E(\mathbf{C}),$$

where $\wp$ is Weierstrass elliptic function, which satisfies the differential equation

$${\wp'}^2 = 4\wp^3 - g_2\wp - g_3.$$

This function will play a role similar to the role of the exponential function in the preceding lectures. While $\exp(z) = e^z$ is an entire function with periods $2i\pi\mathbf{Z}$ (a rank one $\mathbf{Z}$-module in $\mathbf{C}$), which establishes an isomorphism between $\mathbf{C}/(2i\pi\mathbf{Z})$ and $\mathbf{C}^*$, $\wp$ is a meromorphic function with periods a lattice $\Omega = \mathbf{Z}\omega_1 + \mathbf{Z}\omega_2$ in $\mathbf{C}$ (i.e. a discrete submodule of $\mathbf{C}$ of rank two over $\mathbf{Z}$), and $\exp_E$ induces an isomorphism (for the analytic structure as well as for the group structure) between the torus $\mathbf{C}/\Omega$ and $E(\mathbf{C})$. Finally, the poles of $\wp$ are the points of Ω.

Notice that $\mathbf{C}/\Omega \simeq E(\mathbf{C})$ is compact, which sometimes makes life easier in the elliptic case than in the exponential case, whereas $\mathbf{C}^*/(2i\pi\mathbf{Z})$ is not compact.

The addition Theorem for the exponential function $e^{z_1+z_2} = e^{z_1}e^{z_2}$ has a counterpart in the elliptic case, namely $\wp(z_1+z_2)$ is a rational function of $\wp(z_1), \wp(z_2), \wp'(z_1), \wp'(z_2)$, which just means that the graph of the group law on $E(\mathbf{C})$ is an algebraic variety.

In order to proceed to arithmetic investigations, we shall always assume that g_2 and g_3 are algebraic numbers; then

$$E(\bar{\mathbf{Q}}) = \{(t:x:y) \in \mathbf{P}_2(\bar{\mathbf{Q}})\,;\, y^2t = 4x^3 - g_2xt^2 - g_3t^3\}$$

is a subgroup of $E(\mathbf{C})$.

The first transcendence results are due to Siegel and Schneider; in particular the analog of the Theorem of Hermite-Lindemann holds:

Theorem (Schneider). – *If α is a non-zero algebraic number, then α is not a pole of $\wp$, and $\wp(\alpha)$ is a transcendental number.*

Also the analog of the Theorem of Gel'fond-Schneider is true; to state it, we need to define the *field of endomorphisms of E*; here, it will be convenient to choose the following definition:

$$k = \begin{cases} \mathbf{Q} & \text{if } \omega_2/\omega_1 \text{ is not quadratic,} \\ \mathbf{Q}(\omega_2/\omega_1) & \text{if } \omega_2/\omega_1 \text{ is quadratic.} \end{cases}$$

In the case where ω_2/ω_1 is quadratic, the curve E is said to be of C.M. type (*complex multiplication*); this means that the lattice Ω has non trivial endomorphisms.

The role played by the $\mathbf{Q}$-vector space $\mathcal{L}$ in the previous lectures, namely

$$\mathcal{L} = \{\ell \in \mathbf{C}; e^\ell \in \bar{\mathbf{Q}}^*\} = \exp^{-1}(\bar{\mathbf{Q}}^*) = \{\log\alpha; \alpha \in \bar{\mathbf{Q}}^*\}$$

(space of logarithms of algebraic numbers) is now played by the complex numbers u whose images under the map $(1:\wp:\wp')$ belong to the group $E(\bar{\mathbf{Q}})$ of algebraic points on E:

$$\mathcal{L}_E = \{u \in \mathbf{C}; u \in \Omega \text{ or } \wp(u) \in \bar{\mathbf{Q}}\} = \exp_E^{-1} E(\bar{\mathbf{Q}}).$$

This set is not only a $\mathbf{Q}$-vector space, but also a k-vector space. Schneider's Theorem above states that any non-zero element in $\mathcal{L}_E$ is transcendental; the analog of the Theorem of Gel'fond-Schneider is as follows:

Theorem (Schneider). – *If u_1 and u_2 are two elements in $\mathcal{L}_E$ which are linearly independent over k, then they are also linearly independent over $\bar{\mathbf{Q}}$.*

An important corollary of this result is: *if τ is an algebraic point in the upper half plane $\Im m\,\tau > 0$, then the modular function j maps τ to an algebraic number if and only if τ is quadratic.*

The "if" part is known from the theory of complex multiplication; the "only if" part is a transcendence result, which is deduced from Schneider's Theorem by using

$$\tau = \omega_2/\omega_1, \qquad j(\tau) = \frac{1728g_2^3}{g_2^3 - 27g_3^2}, \qquad u_1 = \omega_1, \qquad u_2 = \omega_2.$$

Measures of simultaneous approximations for τ and $j(\tau)$ by algebraic numbers α and β (where α is not quadratic) have been derived by A. Faisant and G. Philibert.

There are very recent results on transcendence properties of values of automorphic functions (Shiga, Cohen, Wolfart) which extend this result on the modular function to higher dimension (generalizing a previous work by Y. Morita).

An *open problem* (which is the second of Schneider's eight problems in [Sc 1957]) is to prove the transcendence of $j(\tau)$ (for an algebraic τ with $\Im m\,\tau > 0$ which is not quadratic) without using the $\wp$-functions, but using the properties of the modular function j. One should investigate the arithmetic properties of analytic functions in the unit disk (work of Wakabayashi [Wa 1988]).

The analog for elliptic curves of Baker's linear independence result on logarithms has been proved by Masser [Ma 1975] in the C.M. case, and later, by Bertrand and Masser [BeMa 1980] in the non-C.M. case. Effective lower bounds for non-vanishing linear forms

$$\beta_0+\beta_1u_1+\cdots+\beta_mu_m$$

(with algebraic $\beta_0,\ldots,\beta_m$, and with $u_1,\ldots,u_m$ in $\mathcal{L}_E$) have been given by Masser [Ma 1978], and then by Coates and Lang [CLa 1976] in the C.M. case; in the general case, the first estimates have been given in [PW 1988]; the dependence on the maximal height $\log B$ of the coefficients β_i was of the shape $(\log B)^{m+1}$; this estimate has been refined by N. Hirata in [HK 1991], who obtained a dependence of the form $(\log B)(\log\log B)^{m+1}$. Finally, very recently, S. David proved a completely explicit version of Hirata's estimate, which we now quote (in a somewhat simplified version: the result in [Da 1993] deals with a product of several elliptic curves; also the result of David is sharper when the numbers $|u_i|$ are small).

Before we state David's result, we need to introduce Weil's absolute logarithmic height, which is defined over the algebraic points of a projective space as follows: for K a number field of degree D, and for $P=(x_0:\cdots:x_N)\in\mathbf{P}_N(K)$,

$$\mathrm{h}(P)=\frac{1}{D}\sum_v d_v\log\max\{|x_0|_v,\ldots,|x_N|_v\},$$

where v runs over the set of normalized absolute values of K, and d_v is the local degree; the normalization is done in such a way that the product formula is:

$$\prod_v|\alpha|_v^{d_v}=1\qquad\text{for } \alpha\in K^*.$$

For an algebraic number α, we put $\mathrm{h}(\alpha)=\mathrm{h}(1:\alpha)$.

Let K be a number field of degree D over $\mathbf{Q}$, let g_2 and g_3 be two elements of K with $g_2^3\neq 27g_3^2$, and E be the corresponding elliptic curve; define $\tau=\omega_2/\omega_1$, $j=j(\tau)$, and $\mathrm{h}_E=\max\{1,\mathrm{h}(j),\mathrm{h}(1:g_2:g_3)\}$; assume that τ belongs to the usual fundamental domain of the upper half plane modulo the action of $\mathrm{SL}_2(\mathbf{Z})$.

For $\gamma=E(\bar{\mathbf{Q}})$, we consider the Neron-Tate height of γ, which is defined as follows:

$$\hat{\mathrm{h}}(\gamma)=\lim_{n\to\infty}\frac{1}{n^2}\mathrm{h}(n\gamma).$$

Let $L(z)=\beta_0z_0+\beta_1z_1+\cdots+\beta_mz_m$ be a non-zero linear form on $\mathbf{C}^{m+1}$ with coefficients in K; let $u_1,\ldots,u_m$ be complex numbers such that $\gamma_i=\exp_E(u_i)$ belongs to $E(K)$. Define $v=(1,u_1,\ldots,u_m)$. Let B and $A_1,\ldots,A_m$ be positive real numbers satisfying

$$B\geq(1/D)\log A_i,\qquad \log A_i\geq\max\left\{\hat{\mathrm{h}}(\gamma_i),\mathrm{h}_E,\frac{3\pi|u_i|^2}{|\omega_1|^2D\,\Im m\,\tau}\right\},\qquad(1\leq i\leq m)$$

and

$$\log B\geq\max\{e\,\mathrm{h}_E,\mathrm{h}(\beta_0),\ldots,\mathrm{h}(\beta_m)\}.$$

Theorem (David). – *If $L(v)$ does not vanish, we have*

$$\log|L(v)|\geq -CD^{2m+2}(\log B+\log D+1)(\mathrm{h}_E+\log\log B+\log D+1)^{m+1}\log A_1\cdots\log A_m,$$

with

$$C=2\cdot10^{7m+8}(2/e)^{2m^2}(m+1)^{4m^2+10m}.$$

The dependence in B is not far from the best possible one; an open problem is to prove that there exists a constant C, which does not depend on B (but which depends on E, D and A) such that

$$|L(v)|>B^{-C}.$$

As a consequence of David's estimate, N. Tzanakis is able to give the complete list of integer points on the elliptic curve

$$y^2=(x+p)(x^2+p^2)\qquad\text{for}\quad p=337.$$

David deduces from his proof an explicit version of the result of Masser and Wüstholz on isogenies of elliptic curves [MaWü 1990].

Corollary. – *Let d be a positive integer, K a number field of degree $\leq d$, E an elliptic curve which is defined over K, and $y^2=4x^3-g_2x-g_3$ a Weierstrass model of E over K. Define $\mathrm{h}_E=\max\{1,\mathrm{h}(j),\mathrm{h}(1:g_2:g_3)\}$. If E^* is another elliptic curve over K which is isogeneous to E, then there exists an isogeny between E and E^* of degree at most*

$$10^{91}d^{12}\,\mathrm{h}_E^6.$$

A closely related problem is the elliptic analog of Lehmer's problem; since the Néron-Tate height $\hat{\mathrm{h}}$ vanishes only on torsion points, the question arises to provide a lower bound for a non-torsion point, in terms of the degree of the number field on which the point is defined. More precisely, let E be an elliptic curve over a number field K; *does there exist a constant $c(E,K)$ such that, for each extension L/K of degree say D, and each non-torsion point $P\in E(L)$,*

$$\hat{\mathrm{h}}(P)\geq c(E,K)D^{-1}?$$

The best estimate known is in the case of complex multiplication, where M. Laurent proved an analog of Dobrowolski's estimate:

$$\hat{\mathrm{h}}(P)\geq\frac{c(E,K)}{D}\left(\frac{\log\log D}{\log D}\right)^3.$$

In the case where there is no complex multiplication, the following estimate is due to D.W. Masser:

$$\hat{\mathrm{h}}(P)\geq\frac{C(E,K,\epsilon)}{D^{3+\epsilon}}\qquad\text{for all}\quad\epsilon>0.$$

The next question is to compute the above "constants" in terms of E. A conjecture due to S. Lang states: *for each number field K, there exists a constant $c(K) > 0$ such that, for each elliptic curve E over K and each non-torsion point $P \in E(K)$,*

$$\hat{\mathrm{h}}(P) \geq c(K)\,\mathrm{h}_E\,.$$

(Lang's conjecture is stated with Falting's height, and in fact more generally for abelian varieties). Partial results are known; for instance D.W. Masser computed his constant $C(E, K, \epsilon)$ above as follows:

$$C(E, K, \epsilon) = c'(K, \epsilon)/\,\mathrm{h}_E^3\,.$$

Also S. David proved: if $P_1, \ldots, P_5$ are 5 points on $E(K)$ which are linearly independent over $\mathbf{Z}$, then

$$\max_{1\leq i\leq 5} \hat{\mathrm{h}}(P_i) \geq c(K, \epsilon)\,\mathrm{h}(j)^{(1/120)-\epsilon}.$$

§2. Abelian varieties and algebraic groups

Many things which we said for elliptic curves can be extended to higher dimensional abelian varieties, and even to commutative algebraic groups.

When G is a commutative algebraic group over the field $\bar{\mathbf{Q}}$, there is a maximal linear subgroup L of G such that G/L is an abelian variety:

$$0 \longrightarrow L \longrightarrow G \longrightarrow A \longrightarrow 0;$$

the linear group G can be written

$$L = \mathbf{G}_{\mathrm{a}}{}^{d_0} \times \mathbf{G}_{\mathrm{m}}{}^{d_1}, \qquad \text{so that} \qquad L(\bar{\mathbf{Q}}) = \bar{\mathbf{Q}}^{d_0} \times (\bar{\mathbf{Q}}^*)^{d_1},$$

and if g is the dimension of A, then the dimension d of G is $d_0 + d_1 + g$, and $A \simeq \mathbf{C}^g/\Omega$, where $\Omega = \mathbf{Z}\omega_1 + \cdots + \mathbf{Z}\omega_{2g}$ is a lattice (discrete subgroup of rank $2g$) in $T_A(\mathbf{C}) \simeq \mathbf{C}^g$. The tangent space at the origin $T_G(\mathbf{C})$ of G is a $\mathbf{C}$-vector space, which has a natural $\bar{\mathbf{Q}}$-structure. We define

$$\mathcal{L}_G = \exp^{-1} G(\bar{\mathbf{Q}}) \subset T_G(\mathbf{C}).$$

<u>`Example`</u>: if $E_1, \ldots, E_g$ are elliptic curves over $\bar{\mathbf{Q}}$, the product

$$G = \mathbf{G}_{\mathrm{a}}{}^{d_0} \times \mathbf{G}_{\mathrm{m}}{}^{d_1} \times E_1 \times \cdots \times E_g,$$

is an algebraic group of dimension $d = d_0 + d_1 + g$, and the exponential map of $G(\mathbf{C}) \subset \mathbf{C}^{d_0+d_1}\mathbf{P}_2(\mathbf{C})^g$ is given by

$$\exp_G(z_1, \ldots, z_d) = \big(z_1, \ldots, z_{d_0}, e^{z_{d_0+1}}, \ldots, e^{z_{d_0+d_1}},$$
$$\exp_{E_1}(z_{d_0+d_1+1}), \ldots, \exp_{E_g}(z_{d_0+d_1+g})\big);$$

in this case we have

$$\mathcal{L}_G = \bar{\mathbf{Q}}^{d_0} \times \mathcal{L}^{d_1} \times \mathcal{L}_{E_1} \times \cdots \times \mathcal{L}_{E_g}.$$

The first transcendence result involving Abelian varieties is again due to Schneider: the Beta function $B(a, b)$ takes transcendental values for each pair (a, b) of rational numbers (not in $\mathbf{Z}$, and $a+b \notin \mathbf{Z}$, in order to avoid the poles). These special values occur as periods of Jacobian of Fermat curves. By the way, if $n \geq 3$ is an integer, the transcendence of $\Gamma(1/n)$ is known only if $n = 3$ or $n = 4$; this result, due to Chudnovsky, involves elliptic functions; for $n \geq 5$ the Jacobian which is involved is of dimension $g \geq 2$, and because of that only weaker assertions are known so far.

The analogs of the Theorems of Hermite-Lindemann and Gel'fond-Schneider for algebraic groups have been proved by Lang [La 1966b], following a question by P. Cartier; the analog of Baker's qualitative result on linear independence of logarithms is due to Wüstholz [Wü 1989], lower bounds for non-vanishing linear combinations of logarithms on algebraic groups were given in [PW 1988] and refined by Hirata in [HK 1991]. Here they are.

Theorem. *Let G be a commutative algebraic group which is defined over $\bar{\mathbf{Q}}$, of dimension d; let $u \in \mathcal{L}_G$. There exists a constant $c = c(G, u)$ such that, if L is a linear form on $T_G(\mathbf{C})$ with algebraic coefficients of logarithmic height $\mathrm{h}(L)$ such that $L(u) \neq 0$, then*

$$|L(u)| > \exp\{-c\,\mathrm{h}(L)^{d+1}\}.$$

The dependence of c in terms of the height of $\exp u$ and the degree of the number field is explicitely given in [PW 1988].

The refinement by N. Hirata [HK 1991] is:

$$|L(u)| > \exp\{-c\,\mathrm{h}(L)\big(\log \mathrm{h}(L)\big)^{d+1}\}.$$

<u>Example</u>: these estimates apply to linear forms like

$$\beta_0 + \beta_1 \log \alpha_1 + \cdots + \beta_n \log \alpha_n + \gamma_1 u_1 + \cdots + \gamma_k u_k,$$

when $\beta_i, \gamma_j \in \bar{\mathbf{Q}}$, $\log \alpha_i \in \mathcal{L}$ and $u_j \in \mathcal{L}_{E_j}$.

The work of Masser-Wüstholz on isogenies of elliptic curves has been extended by the same authors to abelian varieties [MaWü 1993a, b]. One result of [MaWü 1993b] is as follows.

Let A be an abelian variety of dimension n over a number field K, with a given ample divisor; denote by $\mathrm{h}(A)$ the Faltings' height of A, by $T_A(\mathbf{C}) \simeq \mathbf{C}^n$ the tangent space of $A(\mathbf{C})$ at the origin, and by $\Omega_A \subset T_A(\mathbf{C})$ the kernel of the exponential map $\exp_A : T_A(\mathbf{C}) \longrightarrow A(\mathbf{C})$; this set Ω_A is a lattice (discrete subgroup of rank $2n$) in $T_A(\mathbf{C})$.

The *Néron-Severi group* $\mathrm{NS}(A)$ of A is the group of sesquilinear forms r on $T_A(\mathbf{C}) \times T_A(\mathbf{C})$, such that $r(z, w) = \overline{r(w, z)}$ and $\Im m\, r(\Omega_A \times \Omega_A) \subset \mathbf{Z}$ (these are called the *Riemann forms* on $T_A(\mathbf{C}) \times T_A(\mathbf{C})$).

A *polarization* is a positive definite element in $\mathrm{NS}(A)$, i.e. a Riemann form which satisfies $r(z, z) > 0$ for $z \neq 0$. For instance when $n = 1$, A is an elliptic curve, and if $\Omega = \mathbf{Z} + \mathbf{Z}\tau$ with $\Im m\,\tau > 0$, then $r(z, w) = (\Im m\,\tau)^{-1} z\bar{w}$ is a polarization.

The degree of the polarization r is the determinant of the imaginary part of r on $\Omega(A)$; this is the square of an integer.

Theorem (Masser-Wüstholz). – *There exist two positive constants $c(n,K) > 0$ and $\kappa(n)$, such that if A and A^* are two isogeneous abelian varieties over K, then there is an isogeny of degree*

$$\leq c(n,K)\max\{\deg r, \deg r^*, \mathrm{h}(A)\}^{\kappa(n)}$$

The end of this section is devoted to the **Theorem of the algebraic subgroup** [W 1986], [RW 1993], which contains all the transcendence results which have been mentionned in these four lectures (with a single exception, namely the Theorem of Lindemann-Weierstrass). We shall not give the most general statement, but only explain some special cases.

Let G be a commutative algebraic group which is defined over $\bar{\mathbf{Q}}$; consider the intersection $V \cap \mathcal{L}_G$; this is a $\mathbf{Q}$-vector space; *is-it of finite dimension*? The answer is as follows: if V contains a subspace of $T_G(\mathbf{C})$ of the form $T_H(\mathbf{C})$ where H is an algebraic subgroup of positive dimension, then $V \cap \mathcal{L}_G \supset \mathcal{L}_H$, hence is of infinite dimension over $\mathbf{Q}$. The converse holds:

Theorem. *Let V be a subspace of $T_G(\mathbf{C})$ which does not contain any subspace of the form $T_H(\mathbf{C})$, when H is an algebraic subgroup of G of positive dimension; then*

$$\dim_{\mathbf{Q}} V \cap \mathcal{L}_G \leq 2d \dim_{\mathbf{C}} V.$$

The conclusion can be refined in several ways. First of all when G is a linear algebraic group, the upper bound can be replaced by $d\dim_{\mathbf{C}} V$; in order to produce an estimate which includes this one and is valid in all cases, we write G as a product ${\mathbf{G}_{\mathrm{a}}}^{d_0} \times {\mathbf{G}_{\mathrm{m}}}^{d_1} \times G'$, where G' is of dimension $d_2 = d - d_0 - d_1$ (there is no condition on G'; hence one can always take $G' = G$, $d_0 = d_1 = 0$; but if G is linear one can take $d_2 = 0$). With this notation the conclusion can be refined as follows:

$$\dim_{\mathbf{Q}} V \cap \mathcal{L}_G \leq (d_1 + 2d_2)\dim_{\mathbf{C}} V.$$

<u>Example</u>: take $d_0 = d_2 = 0$, $d_1 = 2$, and let V be a $\mathbf{C}$-vector subspace of $\mathbf{C}^2$ of dimension 1; the conclusion is

$$\dim_{\mathbf{Q}} V \cap (\mathcal{L}^2) < 3;$$

this is nothing else than the six exponentials Theorem.

The second refinement arises by considering a subspace W of $T_G(\mathbf{C})$, which is included in V, and is rational over $\bar{\mathbf{Q}}$; of course $W = 0$ is always such a subspace. Then the following upper bound holds:

$$\dim_{\mathbf{Q}} V \cap \mathcal{L}_G \leq (d_1 + 2d_2)\dim_{\mathbf{C}}(V/W).$$

For instance if V itself is defined over $\bar{\mathbf{Q}}$, we can take $W = V$, and we find $V \cap \mathcal{L}_G = \{0\}$, which is the generalization by Wüstholz of Baker's Theorem to algebraic groups.

A further refinement is possible by considering the periods of $\exp_G$ which lie into V: if $\kappa = \mathrm{rk}_{\mathbf{Z}}(V \cap \ker \exp_G)$; then

$$\boxed{\dim_{\mathbf{Q}} V \cap \mathcal{L}_G \leq (d_1 + 2d_2 - \kappa)\dim_{\mathbf{C}}(V/W)}$$

We give now a consequence of this estimate.

Corollary. – *Let A be a simple abelian variety of dimension g which is defined over $\mathbf{Q}$; assume that the group $A(\mathbf{Q})$ contains at least $g^2 - g + 1$ points which are $\mathbf{Q}$-linearly independent. Then the rational points are dense in the connected component of the origin in $A(\mathbf{R})$.*

According to a Conjecture of Mazur, the same conclusion should hold under the only assumption that $A(\mathbf{Q})$ is infinite [Maz 1992].

The Theorem of the algebraic subgroup provides lower bounds for the rank of matrices:

$$\left(\underline{b}_1, \ldots, \underline{b}_{\ell_0}, u_1, \ldots, u_{\ell_1}\right),$$

where $\underline{b}_i \in \bar{\mathbf{Q}}^d$, and $u_j \in \mathcal{L}_G$. For instance the matrix

$$\begin{pmatrix} & & & \log\alpha_1 \\ & I_n & & \vdots \\ & & & \log\alpha_n \\ \beta_1 & \cdots & \beta_n & \beta_0 \end{pmatrix}$$

is of this form, with $G = {\mathbf{G}_{\mathrm{m}}}^n \times \mathbf{G}_{\mathrm{a}}$; the determinant of this matrix is

$$\beta_0 - \beta_1\log\alpha_1 - \cdots - \beta_n\log\alpha_n.$$

One can transpose this matrix, in this case the corresponding algebraic group is $G = {\mathbf{G}_{\mathrm{a}}}^n \times \mathbf{G}_{\mathrm{m}}$; the initial matrix is related to Schneider's solution of Hilbert's seventh problem, the second to Gel'fond's solution. This *duality* can be explained by means of the Fourier-Borel transform.

Another application of this result (D. Roy) is to derive lower bounds for the rank of matrices whose coefficients are *linear combinations with algebraic coefficients of elements of $\mathcal{L}_G$.*

An effective version of the algebraic subgroup Theorem is in preparation; it should contain also the qualitative aspects which we have discussed, like the lower bounds for non-vanishing linear combinations of logarithms.

§3. Drinfeld modules

Another important advance concerning transcendental numbers is a spectacular development of the theory in finite characteristic. This started in the 40's with the work of Wade on Carlitz functions. Until the end of the 80's, most results were merely analogs of known transcendence results in zero characteristic. With the work of Jing Yu on Drinfeld modules, impressive progress has been made in the last few years, including the transcendence of values of Carlitz zeta function. The results which have been achieved recently in this domain correspond to open problems in the classical case: *what is the arithmetic nature of the values $\zeta(2n+1)$ of the Riemann zeta function at odd positive numbers? Is Euler constant an irrational number? a transcendental number? Are the numbers e and π algebraically independent?*

There are several approaches to the study of transcendental numbers in finite characteristic: The work of Jing Yu involves Drinfeld modules as well as t-motives of G. Anderson; L. Denis, D. Thakur, A. Thiery, have made important contributions to this subject; W.D. Brownawell, P.G. Becker and R. Tubbs recently obtained results of algebraic independence. Wade's method also yields the transcendence of values of Carlitz zeta function, as shown by G. Damamme and Y. Hellegouarch. Very sharp results of diophantine approximations have been worked out recently by H. Cherif and B. de Mathan. A quite different approach, related to automata theory (involving a theorem of Christol, Kamae, Mendes France and Rauzy) has been introduced by J-P. Allouche and developed by V. Berthé.

In 1992 a conference was organized by D. Goss in Ohio, and the proceedings of this conference is the best source of information on this field: *The arithmetic of function fields*; Proc. Workshop Ohio State Univ. 1991, D. Goss, D.R. Hayes and M.I. Rosen eds, W. de Gruyter 1992.

Conclusion.

At the MSRI (Berkeley) a special semester is just ending, and many new results which have been anounced there show how active the subject is. One aim of the present lectures was to point out a few of many unsolved problems in this domain; it is hoped that more people will try to solve them.

REFERENCES

[AE 1944] L. Alaoglu and P. Erdős. – On highly composite and similar numbers; Trans. Amer. Math. Soc., **56** (1944), 448–469.

[Ba 1966] A. Baker. – Linear forms in the logarithms of algebraic numbers; (I), Mathematica, **13** (1966), 204–216; (II), id., **14** (1967), 102–107; (III), id., **14** (1967), 220–228; (IV), id., **15** (1968), 204–216.

[Ba 1976] A. Baker. – The theory of linear forms in logarithms; Chap.1 of: *Transcendence Theory: Advances and Applications*; Proc. Conf. Cambridge 1976, ed. A.Baker and D.W.Masser, Academic Press (1977), 1–27.

[Ba 1975] A. Baker. – *Transcendental Number Theory;* Cambridge Univ. Press, 1975; 2nd ed., 1979.

[Ba 1991] A. Baker. – The evolution of transcendence theory; Mitt. Math. Ges. Hamb., **12**, N°3 (1991), 513–521.

[Be 1985] D. Bertrand. – Lemmes de zéros et nombres transcendants; Sém. Bourbaki, 38ème Année 1985–86, N° 652; Soc. Math. France, Astérisque, **145–146** (1987), 21–44.

[BeMa 1980] D. Bertrand and D.W. Masser. – Linear forms in elliptic integrals; Invent. Math., **58** (1980), 283–288.

[BGMMS 1990] 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 VI), **88**, N°2, 31p.

[Bo 1993] E. Bombieri. – Effective diophantine approximation on $\mathbf{G}_{\mathrm{m}}$; Ann. Scuola Norm. Sup. Pisa, (IV) **20** (1993), 61–89.

[Br] W.D. Brownawell; Bounds for the degree in the Nullstellensatz; Ann. of Math., **126** (1987), 577–591.

[CLa 1976] J. Coates and S. Lang. – Diophantine approximation on abelian varieties with complex multiplication; Invent. Math., **34** (1976) 129–133.

[Da 1993] S. David. – Minorations de formes linéaires de logarithmes elliptiques; manuscript.

[Di 1989] G. Diaz. – Grands degrés de transcendance pour des familles d'exponentielles en plusieurs variables; J. Number Theory, **31** (1989), 1–23.

[Do 1979] E. Dobrowolski. – On a question of Lehmer and the number of irreducible factors of a polynomial; Acta Arith., **34** (1979), 391–401.

[Dpp 1992] Dong Ping Ping. – Minorations de combinaisons linéaires de logarithmes de nombres algébriques p-adiques; C. R. Acad. Sci. Paris, Sér. I, **315** (1992), 103–106.

[Dub 1993] A. Dubickas. – On a conjecture of A.Schinzel and H.Zassenhaus; Acta Arith., **63** (1993), 15–20.

[E 1991] N. Elkies. – *abc* implies Mordell; Duke Math. J., **64** (1991), 99–109.

[F 1968] N.I. Feldman. – Improved estimates for a linear form of the logarithms of algebraic numbers; Mat. Sb., **77** (1968), 423-436; English transl. Math. USSR Sb., **77** (1968), 393–406.

[FS 1967] N.I. Feldman and A.B. Shidlovskii. – The development and present state of the theory of transcendental numbers; Usp. Mat. Nauk SSSR, **22** (1967), 3–81; engl. transl., Russian Math. Surveys, **22** (1967), 1–79.

[G 1934] A.O. Gel'fond. – On Hilbert's seventh problem; Dokl. Akad. Nauk SSSR, **2** (1934), 1–3 (in Russian) and 4–6 (in French); Sur le septième problème de Hilbert; Izv. Akad. Nauk SSSR, **7** (1934), 623–630.

[G 1952] A.O. Gel'fond. – *Transcendental Number Theory;* Moscow, 1952; English transl. Dover Publ., N.Y., 1960.

[GL 1962] A.O.Gel'fond and Yu.V.Linnik. – *Analytic methods in analytic number theory;* Fizmatgiz, Moscow 1962; trad. franç.: *"Méthodes élémentaires dans la théorie analytique des nombres";* Gauthier Villars 1965; English transl. MIT Press, Mass. 1966.

[He 1873] C. Hermite. – Sur la fonction exponentielle; C.R. Acad. Sci. Paris, **77** (1873), 18–24; 74–79; 226–233; 285–293; *Oeuvres* III, 150–181. Voir aussi *Oeuvres* III, 127–130, 146–149, et *Correspondance Hermite–Stieltjes*, II, lettre 363, 291–295.

[Hi 1900] D. Hilbert. – Mathematische Probleme; Nachr. Ges. Wiss. Göttingen, (1900), 253–297; Archiv der Math. and Phys., **1** (1901), 44–63 and 213–237; engl. transl., Bull. Amer. Math. Soc., **8** (1902), 437–479; *Ges. Werke* III, 290–329.

[HK 1991] N. Hirata-Kohno. – Formes linéaires de logarithmes de points algébriques sur les groupes algébriques; Invent. Math., **104** (1991), 401–433.

[La 1965] S. Lang.– Nombres transcendants; Sém. Bourbaki 18ème année (1965/66), N° 305.

[La 1966a] S. Lang.– Algebraic values of meromorphic functions; (II), Topology, **5** (1966), 363–370.

[La 1966b] S. Lang. – *Introduction to Transcendental Numbers;* Addison-Wesley 1966.

[La 1970] S. Lang. – *Algebraic Number Theory;* Addison-Wesley 1970.

[La 1978] S. Lang. – *Elliptic Curves Diophantine Analysis;* Springer Verlag, Grund. der Math. Wiss., **231**, 1978.

[La 1983] S. Lang. – *Fundamentals of Diophantine Geometry;* Springer Verlag, 1983.

[La 1991] S. Lang. – *Number theory III;* Springer Verlag, Encycl. of Math. Sciences, **60**, 1991.

[La 1993] S. Lang. – *Algebra;* Addison–Wesley, 3rd Ed., 1993.

[Lau 1989] M.Laurent. – Sur quelques résultats récents de transcendance; *Journées arithmétiques Luminy* 1989, Astérisque, **198–200** (1991), 209–230.

[Lau 1990] M.Laurent. – Hauteurs de matrices d'interpolation; *Approximations Diophantiennes et Nombres Transcendants*, Luminy 1990, éd. P. Philippon, de Gruyter 1992, 215–238.

[Lau 1992] M. Laurent. – Linear forms in two logarithms and interpolation determinants; Appendix of [Wa 1992].

[LauMiNe 1993] M. Laurent, M. Mignotte et Yu.V. Nesterenko. – Formes linéaires en deux logarithmes et déterminants d'interpolation; manuscript.

[Lin 1882a] F. Lindemann. – Über die Zahl π; Math. Ann., **20** (1882), 213–225.

[Lin 1882b] F. Lindemann. – Über die Ludolph'sche Zahl; S.B. Preuss. Akad. Wiss., (1882), 679–682.

[Lin 1882c] F. Lindemann. – Sur le rapport de la circonférence au diamètre, et sur les logarithmes népériens des nombres commensurables ou des irrationnelles algébriques; C.R. Acad. Sci. Paris, **95** (1882), 72–74.

[Lio 1844a] J. Liouville. – Sur des classes très étendues de quantités dont la valeur n'est ni algébrique, ni même réductible à des irrationnelles algébriques; C.R. Acad. Sci. Paris, **18** (1844), 883–885.

[Lio 1844b] J. Liouville. – Nouvelle démonstration d'un théorème sur les irrationnelles algébriques inséré dans le compte-rendu de la dernière séance; C.R. Acad. Sci. Paris, **18** (1844), 910–911.

[Lio 1851] J. Liouville. – Sur des classes très étendues de quantités dont la valeur n'est ni algébrique, ni même réductible à des irrationnelles algébriques; J. Math. Pures et Appl., **1** (1851), 133–142.

[M 1976] K. Mahler. – *Lectures on transcendental numbers;* Springer Verlag, Lecture Notes in Math., **546** (1976).

[Ma 1975] D.W. Masser. – *Elliptic functions and transcendence;* Springer Verlag, Lecture Notes in Math., **437** (1975).

[Ma 1978] D.W. Masser. – Diophantine approximation and lattices with complex multiplication; Invent. Math., **45** (1978), 61–82.

[MaWü 1990] D.W. Masser and G. Wüstholz. – Estimating isogenies on elliptic curves; Invent. Math., **100** (1990), 1–24.

[MaWü 1993a] D.W. Masser and G. Wüstholz. – Periods and minimal abelian subvarieties; Annals of Math., **137** (1993), 407–458.

[MaWü 1993b] D.W. Masser and G. Wüstholz. – Isogeny estimates for abelian varieties, and finiteness theorems; Annals of Math., **137** (1993), 407–458.

[Maz 1992] B. Mazur. – The topology of rational points; Experimental Mathematics, **1** (1992), 35–45.

[Na 1993] M. Nakamaye. – Multiplicity estimates and the product theorem; manuscript, 1993.

[P 1986] P. Philippon. – Lemme de zéros dans les groupes algébriques commutatifs; Bull. Soc. Math. France, **114** (1986), 355–383, et **115** (1987), 397–398.

[PW 1986] P. Philippon and M. Waldschmidt. – Lower bounds for linear forms in logarithms; Chap. 18 of *New Advances in Transcendence Theory*, Proc. Conf. Durham 1986, ed. A.Baker, Cambridge Univ. Press (1988), 280–312.

[PW 1987] 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.

[PW 1988] P. Philippon and M. Waldschmidt. – Formes linéaires de logarithmes sur les groupes algébriques commutatifs; Illinois J. Math., **32** (1988), 281–314.

[Pi 1991] J. Pila. – Geometric postulation of a smooth function and the number of rational points; Duke Math. J., **63** (1991), 449–463.

[Pi 1993] J. Pila. – Geometric and arithmetic postulation of the exponential function; J. Austral. Math. Soc., **54** (1993), 111–127.

[PS 1924] G.Pólya and G.Szegő. – *"Problems and theorems in analysis";* (English ed.), Volume 2, Springer Verlag, Grund. der Math. Wiss., **216**, 1976.

[Ra 1968] K. Ramachandra. – Contributions to the theory of transcendental numbers; Acta Arith., **14** (1968), 65–88.

[Ra 1969] K. Ramachandra. – *Lectures on transcendental numbers;* The Ramanujan Institute, Vol. I, Univ. of Madras, 1969.
[Rh 1986] G. Rhin. – Approximants de Padé et mesures effectives d'irrationalité; Sém. Théor. Nombres, Paris 1985–86, Birkhäuser Verlag, Prog. in Math., **71** (1987), 155–164.
[Ro 1955] K.F. Roth. – Rational approximations to algebraic numbers; Mathematika, **2** (1955), 1–20 and 168.
[R 1989] 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 VI), **90**, N° 6, 12 p.
[R 1990a] D. Roy. – Matrices dont les coefficients sont des formes linéaires de logarithmes; Sém. Théorie Nombres Paris (1987-88), Birkhäuser Verlag, Prog. in Math., **81** (1990), 273–281.
[R 1990b] 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 1992a] D. Roy. – Matrices whose coefficients are linear forms in logarithms; J. Number Theory, **41** (1992), 22–47.
[R 1992b] D. Roy. – Simultaneous approximations in number fields; Invent. Math., **109** (1992), 547–556.
[RW 1993] D. Roy et M. Waldschmidt. – Autour du théorème du sous-groupe algébrique; Canadian Bull. Math., to appear.
[Sc 1934] Th. Schneider. – Transzendenzuntersuchungen periodischer Funktionen; J. reine angew. Math., **172** (1934), 65–74.
[Sc 1949] Th. Schneider. – Ein Satz über ganzwertige Funktionen als Prinzip für Transzendenzbeweise, Math. Ann., **121** (1949), 131–140.
[Sc 1957] Th. Schneider. – *Einführung in die transzendenten Zahlen;* Springer Verlag, 1957; trad. franç., *Introduction aux Nombres Transcendants,* Paris, Gauthier-Villars.
[Sh 1989] A.B. Shidlovskii. – Transcendental numbers; W. de Gruyter, 1989.
[Si 1929] C. Siegel. – Über einige Anwendungen diophantischer Approximationen; Abh. Preuss. Akad. Wiss., Phys.-Math., **1** (1929), 1–70; Gesam. Abh., Springer-Verlag 1966, Band **1**, N° 16, 209–266.
[SY 1991] C. L. Stewart and Yu Kunrui. – On the *abc* conjecture; Math. Ann., **1991**, 225–230.
[T 1976] R. Tijdeman. – On the equation of Catalan; Acta Arith., **29** (1976), 197–209.
[Ts 1991] Yu. Tschinkel. – Finite heights and rational points on surfaces; *Advances in Number Theory*, ed. F.Q. Gouvea and N. Yui, Proc. Conf. Kingston 1991, Oxford Science Publ. (1993), 319–329.
[Wa 1988] I. Wakabayashi. – Algebraic values of functions on the unit disk ; Proc. Prospects of Math. Sci., World Sci. Pub., (1988), 235–266.
[W 1978] M. Waldschmidt. – Simultaneous approximation of numbers connected with the exponential function ; J. Austral. Math. Soc., **25** (1978), 466–478.
[W 1986] M. Waldschmidt. – On the transcendence methods of Gel'fond and Schneider in several variables; *New Advances in transcendence theory;* Proc. Conf. Durham 1986, ed. A. Baker, Cambridge Univ. Press (1988), 375–398.

[W 1987] M. Waldschmidt. – Dependence of logarithms of algebraic points; Coll. Math. Soc. János Bolyai, **51** (1987), 1013-1035.
[W 1992] M. Waldschmidt. – *Linear independence of logarithms of algebraic numbers;* The Institute of Mathematical Sciences, IMSc Report No. 116, Madras (1992).
[W 1993] M. Waldschmidt. – Minorations de combinaisons linéaires de logarithmes de nombres algébriques ; Canadian J. Math., **45** (1993), 176–224.
[We 1885] K. Weierstrass. – Zu Lindemann's Abhandlung: "Über die Ludolph'sche Zahl"; S.B. Preuss. Akad. Wiss., (1885), 1067–1085; = *Math. Werke* II, 341–362.
[Wü 1985] G. Wüstholz. – A new approach to Baker's theorem on linear forms in logarithms; (I), *Diophantine approximations and transcendence theory,* Sem. Bonn 1985, Springer Verlag, Lecture Notes in Math., **1290** (1987), 189–202; (II), id., 203–211; (III), Chap. 25 of *New Advances in Transcendence Theory;* Proc. Conf. Durham 1986, ed. A.Baker, Cambridge Univ. Press (1988), 399–410.
[Wü 1989] G. Wüstholz. – Algebraische Punkte auf analytischen Untergruppen algebraischer Gruppen; Ann. Math., **129** (1989), 501–517.
[Yu 1989] Yu Kunrui. – Linear forms in p-adic logarithms; Acta Arith., **53** (1989), 107–186; (II), Compositio Math., **74** (1990), 15–113.

Michel Waldschmidt
Univ. P. et M. Curie (Paris VI)
Math. T.45-46, 4, Place Jussieu
75252 Paris Cedex 05 FRANCE
e-mail: `miw@ccr.jussieu.fr`