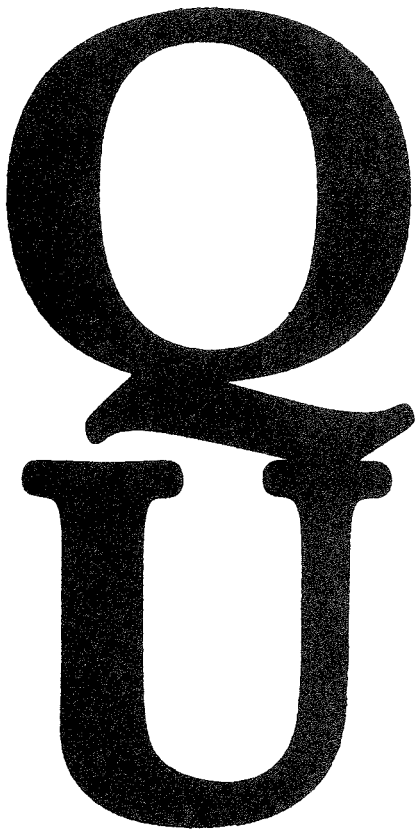
QUEEN'S PAPERS

IN PURE AND APPLIED

MATHEMATICS

EDITORS: A.J. COLEMAN
P. RIBENBOIM



No. 52

# Transcendence Methods

by

MICHEL WALDSCHMIDT

# TRANSCENDENCE METHODS

by

MICHEL WALDSCHMIDT

Queen's Papers in Pure and
Applied Mathematics - No. 52

Queen's University
Kingston, Ontario, Canada

1979

# Transcendence Methods

by

Michel Waldschmidt

Queen's Papers in Pure and Applied Mathematics, No. 52
Queen's University, Kingston, Ontario, 1979

## ERRATA

p. 1 "some recent books", in the last reference (Astérisque), replace 71 by 69–70.

p. 1.9, l.-7, displayed formula, replace the subscript $h-1$ by $h=1$

p.3.9, two lines before Theorem 3.3.1 = line which ends with "Finally in a paper to appear in Bull. Acad.", replace $>$ by $<$

p.5.2, l.11, displayed formula starting with $|F(\frac{1}{q})|$ replace the last bracket ) by $\log N$) so that the formula reads

$$|F(\frac{1}{q})| < \exp(-N^{2n^2+6n+6}\log N).$$

p.5.5, l. 9 = line which starts with $(\mu_1, \ldots,$ replace $\frac{L}{q} - \lambda_j^0$ by $\frac{L-\lambda_j^0}{q}$

p.5.6, line 2 of section c = just before the statement of Lemma 5.2.1, add: We recall that $T = N^{2n+4}$ and $L = N^{2n+2}$.

p.5.7, l. 3. Replace twice $<$ by $\leq$: read $0 \leq \lambda_j \leq L/q^S$, $(1 \leq j \leq n+1)$.

p.5.7, l. 9, displayed formula (after: From the upper bound) replace $c_3^L$ by $c_3^{L+T}$.

p.5.7, l. 11, replace $\frac{1}{4}$ by $\frac{1}{4q}$.

p.6.3, l. 5 of section 6.2. The symbol $\wp$ (Weierstrass P) is missing after $\sigma^2$: read then $\sigma^2\wp$ is entire.

p.8.4, l.2: at the end of this formula for $\omega_1$, replace $2^{8/3}$ by $2^{4/3}$ in the denominator.

p.8.13, l.2, replace $\min\{s, L_2\}$ by $\min\{t, L_2\}$.

p.9.14, last line. Replace 71 by 69–70.

p.10.10 Section c) Comparison of Bombieri's criterion... should be labelled section e)

# PREFACE

In the study of transcendental numbers, there is only one main method which is based on the construction of an auxillary function with many zeroes. However there are a lot of variations, and it is the first purpose of these lectures to describe some of the recent variations.

The subject has made very significant advances in the last few years, and it was necessary to choose in this fertile area among all the new developments. The only criterion for this choice was the taste of the author. Other aspects of the subject are described in the books listed in the short bibliography, especially in the Proceedings of the Cambridge Conference edited by Baker and Masser, and in Baker's book.

The second aim of these notes is to provide an introduction to the subject of transcendental numbers. I guess this material could be used as a text book, since the conciseness of the proofs increases only slowly along the book. The first three lectures prepare the field at an elementary level.

This course was given at Queen's University for the Conference on Recent Developments in Number Theory, organized by P. Ribenboim in July 1979. The text was written a few months before the conference, and is reproduced here essentially without modification. Therefore it does not include the beautiful and unexpected result of D. Bertrand and D. W. Masser on linear independence of elliptic logarithms, which was found only one month before the conference. This is a good illustration of the intense activity of the field.

It is a pleasure to thank here Paulo Ribenboim for the opportunity to deliver these lectures and for his kind hospitality.

M. W.

## SOME RECENT BOOKS


BAKER, A. - Transcendental number theory; Cambridge Univ. Press (1975).

BAKER, A., and MASSER, D.W. - Transcendence theory: advances and applications; Proc. Conf. Cambridge (1976), Academic Press (1977).

LANG, S. - Elliptic curves, diophantine analysis; Grund. der Math. Wiss., 231, Springer-Verlag (1978).

MAHLER, K. - Lectures on transcendental numbers; Lecture Notes in Math., 566, Springer-Verlag (1976).

MASSER, D.W. - Elliptic functions and transcendence; Lecture Notes in Math., 437, Springer-Verlag (1975).

WALDSCHMIDT, M. - Nombres transcendants; Lecture Notes in Math., 402, Springer-Verlag (1974).

WALDSCHMIDT, M. - Nombres transcendants et groupes algébriques; Astérisque, 71, Société Mathématique de France (1980).



Michel WALDSCHMIDT
Institut Henri Poincaré
11, rue P. et M. Curie
75231 PARIS CEDEX 05
FRANCE.

# TRANSCENDENCE METHODS

Michel WALDSCHMIDT

# LECTURE 1

## PRELIMINARY RESULTS

In this first lecture we introduce the three main tools of the theory of transcendental numbers. The first one is the fact that a non-vanishing rational integer has absolute value at least 1. The second is Dirichlet box principle: a map $f : A \to B$ with Card $A >$ Card $B$ is not injective. The third one is called Schwarz lemma and leads to an upper bound for an analytic function of one variable having a lot of zeroes.

### §1.1 Liouville estimates.

We consider the problem of giving a lower bound for a non-zero algebraic number. Such an estimate must depend on some "size" function which measures the "complexity" of the algebraic number. The most natural one is the "usual height"; if

$$a_0X^d + a_1X^{d-1} + \ldots + a_{d-1}X + a_d \in \mathbb{Z}[X]$$

is the minimal polynomial of an algebraic number $\alpha$, we define

$$H(\alpha) = \max_{0 \le j \le d} |a_j| .$$

Lemma 1.1.1. *If $\alpha$ is a non vanishing algebraic number, then*

$$|\alpha| \ge \frac{1}{H(\alpha)+1}$$

Proof.

Since $H(\alpha^{-1}) = H(\alpha)$, it is sufficient to prove that for any algebraic number $\beta$,

$$|\beta| \leq H(\beta)+1.$$

If $|\beta| \leq 1$ the result is clear. Otherwise, let $\sum_{i=0}^{d} a_i X^{d-i}$ be the minimal polynomial of $\beta$ over $\mathbb{Z}$. From

$$a_0\beta^d = -\sum_{i=1}^{d} a_i\beta^{d-i}$$

we deduce

$$|\beta| \leq |a_0\beta| \leq H(\beta) \sum_{i=1}^{d} |\beta|^{1-i} \leq H(\beta).\ \frac{1}{1-|\beta|^{-1}},$$

hence

$$|\beta| - 1 \leq H(\beta),$$

which is the desired result.

The very simple estimate provided by lemma 1.1.1 is not extremely useful(in fact we will never use it!) For the applications $\alpha$ is a polynomial in given algebraic numbers $\xi_1,\ldots,\xi_q$, and it is not quite obvious how to estimate the height of such a number $\alpha$.

The easiest way to get a useful estimate is to introduce the house of $\alpha$ :

$$\overline{|\alpha|} = \max_{1\leq j\leq d} |\alpha_j|$$

where $\alpha_1,\ldots,\alpha_d$ are the conjugates of $\alpha$, and the denominator of $\alpha$, den $\alpha$, which is the positive generator of the ideal of $\mathbb{Z}$ :

$$\{m \in \mathbb{Z}\ ;\ m\,\alpha \text{ is an algebraic integer}\}$$

Lemma 1.1.2. Let $\gamma$ be a non-vanishing algebraic number of degree $d$ ; then

$$\log |\gamma| \geq -(d-1)\log \lceil\gamma\rceil - d \log \operatorname{den}\gamma$$

Proof.

The number $(\operatorname{den}\gamma)\gamma$ is a non zero algebraic integer. Its norm over $\mathbb{Q}$ is a non-zero rational integer. Hence

$$1 \leq \prod_{i=1}^{d} (\operatorname{den}\gamma)\gamma_i \leq |\gamma|\,(\operatorname{den}\gamma)^d \lceil\gamma\rceil^{d-1},$$

which is the desired estimate.

We will make a systematic use of lemma 1.1.2. However we mention some refined estimate, which involves Mahler's measure. Let

$$P(x) = \sum_{j=0}^{d} a_j X^{d-j} = a_0 \prod_{i=1}^{d} (X-\alpha_i)$$

be the minimal polynomial of $\alpha$ over $\mathbb{Z}$ . From Jensen's formula we have

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

We denote this number by $M(\alpha)$. (Mahler's measure of $\alpha$).

Further, let $Q \in \mathbb{C}[X_1,\ldots,X_q]$ be a polynomial:

$$Q(X_1,\ldots,X_q) = \sum_{\lambda_1=0}^{N_1} \cdots \sum_{\lambda_q=0}^{N_q} b(\lambda_1,\ldots,\lambda_q)\, X_1^{\lambda_1}\cdots X_q^{\lambda_q}$$

$$= \sum_{(\lambda)} b(\lambda) \prod_{j=1}^{q} X_j^{\lambda_j}$$

We define the height of $Q$ by

$$H(Q) = \max_{(\lambda)} |b(\lambda)|$$

and the length of $Q$ by

$$L(Q) = \sum_{(\lambda)} |b(\lambda)|$$

Lemma 1.1.3. Let $\xi_1,\ldots,\xi_q$ be algebraic numbers of exact degrees $d_1,\ldots,d_q$ respectively. Define $D = [\mathbb{Q}(\xi_1,\ldots,\xi_q) : \mathbb{Q}]$. Let $Q \in \mathbb{Z}[X_1,\ldots,X_q]$ be a polynomial with integer coefficients such that $Q(\xi_1,\ldots,\xi_q) \neq 0$. For $1 \leq h \leq q$, let $N_h \geq \deg_{X_h} Q$. Then

$$|Q(\xi_1,\ldots,\xi_q)| \geq L(Q)^{1-D} \cdot \prod_{h=1}^{q} M(\xi_h)^{-DN_h/d_h}$$

Sketch of the proof.

Let $a_h$ be the leading coefficient of the minimal polynomial of $\xi_h$, $(1 \leq h \leq q)$. Let $\{\sigma : K \to \mathbb{C}\}$ be the $D$ embeddings of $K$ into $\mathbb{C}$, where $K = \mathbb{Q}(\xi_1,\ldots,\xi_q)$. The number

$$\left(\prod_{h=1}^{q} a_h^{N_h D/d_h}\right) \cdot \left(\prod_{\sigma} \sigma Q(\xi_1,\ldots,\xi_q)\right)$$

is a non-zero rational integer, and therefore its absolute value is at least 1. A rather straightforward estimate leads to the desired inequality.

(We have used the remark that if $\alpha_1,\ldots,\alpha_k$ are distinct roots of a polynomial $a_0X^d+\ldots+a_d \in \mathbb{Z}[X]$, then the number $a_0\alpha_1\ldots\alpha_k$ is an algebraic integer).

In the case $q = 1$, an alternative proof of lemma 1.1.3 is obtained by considering the resultant of $Q$ and the minimal polynomial of $\xi$ over $\mathbb{Z}$.

A special case of lemma 1.1.1 (with $\alpha = \xi - \frac{p}{q}$) or of lemma 1.1.2 (with $\gamma = \xi - \frac{p}{q}$) or of lemma 1.1.3 (with $Q(X) = qX-p$) is the following theorem of Liouville.

Corollary 1.1.4 Let $\xi$ be an algebraic number of degree $d \geq 2$. There exists an easily computable number $c(\xi) > 0$ such that for any rational number $p/q$, $q > 0$, we have

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

All these estimates are elementary and very simple. However Liouville theorem is the starting point of a very deep and involved method which leads to the theorem of Thue-Siegel-Roth-Schmidt (cf.9.2.2). Surprisingly up to now nobody succeeded to use, say, Schmidt's theorems in transcendence proofs in place of Liouville estimates in order to get sharper (but ineffective) results.

For convenience we end this section with some inequalities connecting together the different "size" functions that we have introduced and also with the absolute logarithmic height which is defined as follows. Let $K$ be a number field, and $\{v\}$ the set of absolutes values of $K$, which we normalize by

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

Let $N_v$ be the local degree of $v$; the product formula reads:

$$\prod_v |\alpha|_v^{N_v} = 1 \quad \text{for } \alpha \in K,\ \alpha \neq 0.$$

We define, for $\alpha \in K$,

$$h(\alpha) = \frac{1}{[K:\mathbb{Q}]} \sum_{\{v\}} N_v \log \max \{1, |\alpha|_v\}.$$

This number does not depend on the number field $K$ containing $\alpha$.

Lemma 1.1.5 For any non zero algebraic number $\alpha$ of degree $d$ we have

$$H(\alpha) \leq 2^d M(\alpha), \qquad M(\alpha) \leq (d+1)^{1/2} H(\alpha)$$

and

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

## §1.2. Siegel's lemma.

The idea of asserting the existence of certain polynomials rather than explicitly constructing them is the main feature of Thue's method. The box principle had been used earlier by Dirichlet and Minkowski, and later Siegel used it in the following form.

Lemma 1.2.1 (Siegel) Let $a_{i,j}$, $(1 \leq i \leq n, 1 \leq j \leq m)$ be rational integers, with $n > m$. Let $A$ be a positive integer such that $A \geq \max_{i,j} |a_{i,j}|$. Then there exist rational integers $x_1, \ldots, x_n$, with

$$0 < \max_{1 \leq i \leq m} |x_i| \leq (nA)^{\frac{m}{n-m}}$$

such that

$$\sum_{i=1}^{n} a_{i,j}\, x_i = 0 \qquad , \qquad (1 \le j \le m) \ .$$

Proof.

For $1 \le j \le m$, let $-V_j$ (resp. $W_j$) be the sum of the negative (resp. positive) elements of $a_{1,j},\ldots,a_{n,j}$. Thus

$$V_j + W_j \le nA$$

Let $X$ be a positive integer; to each point $(x_1,\ldots,x_n)$ of $\mathbf{Z}^n$ satisfying $0 \le x_i \le X$, $(1 \le i \le n)$, we associate the point $(y_1,\ldots,y_m) \in \mathbf{Z}^m$ such that

$$y_j = \sum_{i=1}^{n} a_{i,j}\, x_i \ , \qquad (1 \le j \le m)$$

We observe that for $1 \le j \le m$, $-V_j X \le y_j \le W_j X$. Our set of points $(x_1,\ldots,x_n)$ has $(X+1)^n$ elements, and the set of points $(y_1,\ldots,y_m)$ has at most $(nAX+1)^m$ elements. Let us choose

$$X = [(nA)^{\frac{m}{n-m}}].$$

Then

$$(X+1)^{n-m} > (nA)^m \ ,$$

and therefore

$$(X+1)^n > (X+1)^m (nA)^m \ge (nAX+1)^m \ .$$

Hence our map is not injective, and there are two distinct points $(x_1',\ldots,x_n')$, $(x_1'',\ldots,x_n'')$ which correspond to the same point $(y_1,\ldots,y_m)$. The difference $(x_1'-x_1'',\ldots,x_n'-x_n'')$ gives the required solution.

When we have an homogeneous linear system of equations with coefficients in a number field $K$, we first multiply each equation

by a positive rational integer, so that we get a new system with coefficients in the ring $\mathcal{O}_K$ of integers of $K$. Then we can solve this system in $\mathcal{O}_K$ if the number $n$ of unknowns is greater than the number $m$ of equations, in the following way: we choose a basis of $\mathcal{O}_K$ over $\mathbf{Z}$ and we expand the known and unknown elements of $\mathcal{O}_K$ on this basis; thus we get $Dm$ equations with $Dn$ unknowns with coefficients and unknowns in $\mathcal{O}_K$, with $D = [K : \mathbf{Q}]$. By this method one can even solve the given system in $\mathbf{Z}$ provided that $n > Dm$. A slightly different argument (due to M. Mignotte) avoids the choice of a basis of $\mathcal{O}_K$ and leads to the following:

Lemma 1.2.2. *Let $K$ be a number field of degree $D$ over $\mathbf{Q}$. Let $a_{i,j}$, $(1 \le i \le n,\ 1 \le j \le m)$ be integers of $K$, with $n > Dm$. Let $A$ be a positive integer with*

$$A \ge \max_{i,j} |a_{i,j}|$$

*Then there exist rational integers $x_1, \ldots, x_n$ with*

$$0 < \max_{1 \le i \le n} |x_i| \le (2^{1/D} nA)^{\frac{Dm}{n-Dm}}$$

*such that*

$$\sum_{i=1}^{n} a_{i,j} x_i = 0 \quad , \qquad (1 \le j \le m) \ .$$

*Sketch of the proof.*

For simplicity we assume that there exists a real embedding $\sigma : K \to \mathbf{R}$ (and we prove the result without $2^{1/D}$). We define

$$X = [(nA)^{\frac{Dm}{n-Dm}}] \ , \quad \ell = 1 + nAX \ ,$$

and we observe that

$$(1+X)^n > \ell^{Dm}$$

Using the Dirichlet box principle, one can find rational integers $x_1,\ldots,x_n$ with

$$0 < \max_{1\le i\le n} |x_i| \le X$$

satisfying the system of $m$ inequations

$$\left|\sum_{i=1}^{n} \sigma(a_{i,j})x_i\right| \le nAX/\ell^D ,$$

for $i\le j\le m$ . We take the norm, and the lemma follows. ...

A refined version of lemma 1.2.2 can be given in terms of Mahler's measure, when $a_{i,j} = P_{i,j}(\xi_1,\ldots,\xi_q)$ , where $\xi_1,\ldots,\xi_q$ are algebraic numbers of exact degrees $d_1,\ldots,d_q$ and $P_{i,j} \in \mathbb{Z}[X_1,\ldots,X_q]$, $\deg_{x_h} P_{i,j} \le N_h$ , $(1\le h\le q)$. In this case one can obtain a solution with

$$0 < \max_{1\le i\le n} |x_i| \le 2 + (2nV)^{\frac{Dm}{n-Dm}}$$

where

$$V = (\max_{i,j} L(P_{i,j})) \prod_{h=1}^{q} M(\xi_h)^{N_h/d_h} .$$

Such sharpened estimates have been used in the study of lower bound for linear forms in logarithms, and also in papers of Stewart and Dobrowolski on a problem of Lehmer (cf. §3.3 below).

Hermite's proof of the transcendency of $e$ rested on an explicit construction of rational approximations of the exponential function. This work has been pushed further, mainly by Mahler.

However Siegel's influence has been preponderant and all the modern proofs of transcendency use Thue's method, i.e. begin with Siegel's lemma. A few weeks ago, in his lectures at the College de France, Choodnovsky pointed out that explicit constructions can lead to sharp results in some specific examples; he is developing a new study based on Padé approximants, which replaces the use of Siegel's lemma.

## §1.3 Schwarz lemma.

In transcendental number theory the following result is called Schwarz lemma. In fact it is connected with Jensen's formula.

Lemma 1.3.1 *Let $R > r$ be positive numbers, and $f$ a non zero function of one variable which is continuous in the disc $|z| \leq R$ and analytic inside. We denote by $\nu_f(0,r)$ the number of zeros (counting multiplicities) of $f$ in the disc $|z| \leq r$. Then*

$$\log |f|_r \leq \log |f|_R - \nu_f(0,r) \log \frac{R^2+r^2}{2rR}$$

(We use the notation $|f|_r = \sup_{|z|=r} |f(z)|$) .

Proof.

Let $\zeta_1,\ldots,\zeta_\nu$ be the zeros of $f$ in $|z| \leq r$, with $\nu = \nu_f(0,r)$. The function

$$f_1(z) = f(z) \prod_{j=1}^{\nu} \frac{R^2 - z\bar{\zeta}_j}{R(z-\zeta_j)}$$

is continuous in $|z| \leq R$, analytic inside this disc. From

the maximum modulus principle

$$|f_1|_r \leq |f_1|_R$$

and from the relations

$$\sup_{|z|=R} \left| \frac{R^2 - z\zeta_j}{R(z-\zeta_j)} \right| = 1 \quad , \quad \inf_{|z|=r} \left| \frac{R^2 - z\zeta_j}{R(z-\zeta_j)} \right| \geq \frac{R^2+r^2}{2rR}$$

we conclude that

$$|f|_r \leq |f|_R \left( \frac{2rR}{R^2+r^2} \right)^{\nu} ,$$

as required.

We shall use only the weaker inequality

$$\log |f|_r \leq \log |f|_R - \nu_f (0,r) \log \frac{R}{2r} ,$$

which is interesting only when $R > 2r$ .

This lemma will be plainly sufficient to deal with transcendence methods in one variable (methods of Gel'fond, Schneider and Baker.) An important and interesting problem is to get a similar estimate for functions of several variables in order to generalize Gel'fond's method (Bombieri's theorem) and Schneider's method to the higher dimension. We shall study this problem in lectures 9 and 10.

# LECTURE 2

## GEL'FOND's METHOD

We begin with the most classical method in transcendental number theory, which was created by A.O. Gel'fond in 1934 when he solved the seventh problem of Hilbert. Following Schneider and Lang, we show how this method leads also to a new proof of Hermite-Lindemann's theorem, and more generally to a transcendence criterion concerning the values of meromorphic functions which satisfy differential equations.

### §2.1 Gel'fond's solution of Hilbert's seventh problem.

In this section we give a proof, following Gel'fond's method, of the following result.

Theorem 2.1.1. (Gel'fond-Schneider). Let $\alpha_1$, $\alpha_2$ be two non-zero algebraic numbers, and for $j = 1,2$ let $\log \alpha_j$ be any determination of the logarithm of $\alpha_j$. If $\log \alpha_1$, $\log \alpha_2$ are linearly independent over $\mathbb{Q}$, then they are linearly independent over the field $\overline{\mathbb{Q}}$ of algebraic numbers.

The theorem asserts that $a^b$ is transcendental if $a$ and $b$ are algebraic, $a \neq 0$, $\log a \neq 0$ and $b \notin \mathbb{Q}$. Specific examples are $2^{\sqrt{2}}$ and $e^{\pi}$.

Gel'fond's proof rests on the following observations. Assume $\log \alpha_2 = \beta \log \alpha_1$ with $\beta \in \overline{\mathbb{Q}}$. The two functions $e^z$, $e^{\beta z}$ are algebraically independent (because $\beta \notin \mathbb{Q}$), and take algebraic values together with their derivatives at all points $z = h \log \alpha_1$, $h \in \mathbb{Z}$. Changing $z$ in $z \log \alpha_1$, we will consider the two functions $\alpha_1^z$, $\alpha_2^z$, the derivation operator $\frac{1}{\log \alpha_1} \frac{d}{dz}$, and the points $h \in \mathbb{Z}$.

In order to get a contradiction, our aim is to construct a non zero polynomial $P \in \mathbb{Z}[X_1, X_2]$ such that the function $F(z) = P(\alpha_1^z, \alpha_2^z)$ vanishes identically. We first construct $P$ in such a way that $F$ has a lot of zeroes (at several points $h \in \mathbb{Z}$, with a high order). Then we show that $F$ has more and more zeroes, and finally $F = 0$.

Gel'fond's original proof was to construct $F$ with a zero of high order at the origin. The estimates are slightly easier if we choose several points in the first step.

We will have to derive several estimates. The most convenient way is to choose a very large number $N$, and to consider what happens when $N$ tends to infinity. A careful look through the proof shows that all our estimates are valid for $N \geq N_0$, where $N_0$ can be explicitly computed in terms of $\alpha_1, \alpha_2, \beta$. Such a computation must be done for the proofs of some diophantine inequalities (e.g. lower bounds for linear forms) but here we merely need the existence of $N_0$.

We write our unknown polynomial

$$P(X,Y) = \sum_{\lambda_1=0}^{L} \sum_{\lambda_2=0}^{L} p(\lambda_1, \lambda_2) X_1^{\lambda_1} X_2^{\lambda_2}$$

where $L$ and $p(\lambda_1, \lambda_2) \in \mathbb{Z}$ have to be chosen as functions of $N$.

Once we know $P$, our auxiliary function will be

$$F(z) = P(\alpha_1^z, \alpha_2^z) = \sum_{\lambda_1=0}^{L} \sum_{\lambda_2=0}^{L} p(\lambda_1,\lambda_2)\, \alpha_1^{\lambda_1 z} \cdot \alpha_2^{\lambda_2 z}$$

We observe that for $t \in \mathbf{N}$

$$\frac{d^t}{dz^t} F = (\log \alpha_1)^t \, F_t$$

where

$$F_t(z) = \sum_{\lambda_1=0}^{L} \sum_{\lambda_2=0}^{L} p(\lambda_1,\lambda_2)(\lambda_1+\lambda_2\beta)^t \, \alpha_1^{\lambda_1 z} \, \alpha_2^{\lambda_2 z}$$

We shall construct $P \in \mathbf{Z}[X,Y]$ such that

$$F_t(h) = 0 \qquad \text{for} \quad 0 \le t < T \,, \; 0 \le h < H \,.$$

We have to choose $L$, $T$ and $H$ as functions of our large number $N$. There is a very wide choice, as we shall see at the end of the proof. For definiteness we take here

$$L = N^4 \,, \quad T = N^6 \,, \quad H = N \,.$$

<u>First step</u>. <u>There exists a non zero polynomial</u> $P \in \mathbf{Z}[X,Y]$ <u>of degree at most</u> $L$ <u>in</u> $X_1$ <u>and</u> $X_2$, <u>and height</u>

$$H(P) = \max_{\lambda_1,\lambda_2} |p(\lambda_1,\lambda_2)| \le \exp(N^6)$$

<u>such that</u>

$$F_t(h) = 0 \quad \underline{\text{for}} \quad 0 \le t < T \,, \; 0 \le h < H \,.$$

<u>Proof</u>.

We consider the linear homogeneous system

$$\sum_{\lambda_1=0}^{L} \sum_{\lambda_2=0}^{L} p(\lambda_1,\lambda_2)\, (\lambda_1+\lambda_2\,\beta)^t \, \alpha_1^{\lambda_1 h} \, \alpha_2^{\lambda_2 h} = 0 \,, \quad (0 \le t < T,\; 0 \le h < H)$$

of $TH$ equations in $(L+1)^2$ unknowns. We multiply each equation by $(\text{den } \beta)^t \, (\text{den } \alpha_1)^{LH} \, (\text{den } \alpha_2)^{LH}$, and the new system has coefficients

in the ring $\mathcal{O}_K$ of integers of the field $K = \mathbf{Q}(\alpha_1, \alpha_2, \beta)$ .

The house of these coefficients is at most

$$L^T \, c_1^T . c_2^{LH} \leq N^{5N^6}$$

where $c_1 = (\text{den } \beta)(1 + \overline{|\beta|})$ , $c_2 = (\text{den } \alpha_1)\ \overline{|\alpha_1|} . (\text{den } \alpha_2) . \overline{|\alpha_2|}$

(the point is that $c_1$ and $c_2$ depend only on $\alpha_1, \alpha_2, \beta$ , and not on $N$ ). The coefficient $\frac{Dm}{n - Dm}$ in Siegel's lemma 1.2.2 is at most $\frac{D}{N-D} \leq N^{-\frac{1}{2}}$ . Our claim follows immediately from lemma 1.2.2.

Second step. For any integer $M \geq N$ , we have

$$F_t(h) = 0 \quad \text{for} \quad 0 \leq t < M^6 \ , \ 0 \leq h < M \ .$$

We prove this by induction on $M$ . The case $M = N$ is our first step. Assume that the result is true for $M$ , and let $t_1, h_1$ satisfy $0 \leq t_1 < (M+1)^6$ , $0 \leq h_1 < M+1$ . From Cauchy's inequalities we derive

$$|F_{t_1}(h_1)| \leq |\log \alpha_1|^{-t_1} \ t_1! \ |F|_{h_1+1} \ .$$

From lemma 1.3.1 with $R = M^3$ and from our induction hypothesis we get $\log |F|_{h_1+1} \leq \log |F|_R - M^7 \log \frac{R}{2(h_1+1)}$

Further we have

$$|F|_R \leq (L+1)^2 \, e^{N^6} . c_3^{LR} \leq c_4^{M^7}$$

where

$$c_3 = \exp(|\log \alpha_1| + |\log \alpha_2|) \ , \ c_4 = e c_3$$

Hence

$$|F_{t_1}(h_1)| \leq M^{-M^7} \ .$$

On the other hand a denominator of $F_{t_1}(h_1)$ is

$$(\text{den } \beta)^{t_1}.(\text{den } \alpha_1.\text{den } \alpha_2)^{L h_1} \leq e^{M^7},$$

and the house of $F_{t_1}(h_1)$ is at most

$$(L+1)^2 e^{N^6}.L^{t_1}.c_1^{t_1}.c_2^{Lh_1} \leq e^{M^7}.$$

From the size inequality 1.1.2 we conclude

$$F_{t_1}(h_1) = 0 .$$

Third step. Conclusion: $F = 0$ .

Our function $F$ satisfies $\frac{d^t}{dz^t} F(0) = 0$ for all $t \in \mathbf{N}$. Therefore $F = 0$, and this is a contradiction with the linear independence of $\log \alpha_1$, $\log \alpha_2$ over $\mathbf{Q}$ .

Further comments.

a) Choice of the parameters.

We have four parameters to choose, namely $L, T, H$, and $R$. If we decide to choose them of the shape

$$L = N^{\ell}, \quad T = N^t, \quad H = N^h, \quad R = M^r$$

it is readily seen that the following inequalities are sufficient to make the proof work:

Step 1: (Siegel's lemma): $2\ell > t+h$

Step 2: (lemma 1.3.1 and comparison between the number of zeroes and $|F|_R$ ): $r > h$ , $t + h \geq \ell + r$

Our choice was to take $2\ell = t+h+1$ , $r = h+2$, $t + h = \ell + r$ , and finally $h = 1$ (this enables us to make very crude estimates).

b) It is possible to make the proof work with $H$ constant (and $0 \leq h < M$ replaced by $0 \leq h < H$ in the second step). We need only $H \geq D+2$ where $D = [\ \mathbf{Q}(\alpha_1, \alpha_2, \beta): \mathbf{Q}\ ]$ (compare with theorem 2.2.1 below).

c) There are several other ways of presenting the proof. For instance we could say after the first step that there is an integer $N_1 > N$ (and we choose the smallest one) such that one at least of the numbers

$$F_t(h) , \quad 0 \leq t < N_1^7 , \ 0 \leq h < N_1^2$$

is not zero (this means that we perform the third step before the second one). An interesting question is then to give an upper bound for $N_1$ . We do not need it here, but it is important for several problems, and in fact Gel'fond's original proof involved such a bound. It is an exercise here to prove $N_1 \leq 2N$ . The general result for an exponential polynomial is due to Tijdeman (see §4.4).

## §2.2 Schneider-Lang's criterion.

The preceeding proof leads to the following very general result.

Theorem 2.2.1 (Schneider-Lang). Let $K$ be a number field, $f_1,\dots,f_h$ be meromorphic functions. We assume that $f_1,f_2$ are algebraically independent over $\mathbf{Q}$, and of order $\leq \rho_1,\rho_2$ respectively. We assume further that the ring $K[f_1,\dots,f_h]$ is invariant under the derivation $\frac{d}{dz}$.

Then the set of $w \in \mathbf{C}$ which are not poles of $f_1,\dots,f_h$ and such that

$$f_j(w) \in K \quad \text{for} \quad 1 \leq j \leq h$$

is finite with at most $(\rho_1+\rho_2)[K:\mathbf{Q}]$ elements.

(The order of an entire function $f$ is

$$\limsup_{R \to +\infty} \frac{\log\log|f|_R}{\log R} ;$$

if $f_1$ and $f_2$ are entire functions of order $\leq \rho$ and if $f_1/f_2$ is entire, then $f_1/f_2$ is of order $\leq \rho$. This remark enables us to call a meromorphic function of order $\leq \rho$ if it can be written as quotient of two entire functions of order $\leq \rho$ ).

When $K = \mathbf{Q}(\alpha_1,\alpha_2,\beta)$, $h = 2$, $f_1(z) = e^z$, $f_2(z) = e^{\beta z}$, $\rho_1=\rho_2= 1$, we obtain the theorem of Gel'fond-Schneider as a corollary to the criterion. A second example is given by $K = \mathbf{Q}(\alpha, e^{\alpha})$, $h = 2$, $f_1(z) = z$, $f_2(z) = e^z$, $\rho_1 = 0$, $\rho_2 = 1$.

Corollary 2.2.2 (Hermite-Lindemann). Let $\alpha$ be a non-zero algebraic number. Then $e^{\alpha}$ is a transcendental number.

It will be convenient to state it in the following equivalent form: if $\log \gamma$ is a non-zero logarithm of an algebraic number $\gamma$, then $\log \gamma$ is transcendental.

We now deduce from theorem 2.2.1 the elliptic analogues, due to Schneider, to the theorems of Hermite-Lindemann and Gel'fond-Schneider. Let $\wp$ be an elliptic function of Weierstrass satisfying a differential equation

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

with $g_2, g_3$ algebraic. A point $u \in \mathbf{C}$ is called an algebraic point of $\wp$ if either $u$ is a pole of $\wp$ or $\wp(u) \in \overline{\mathbf{Q}}$ . . We denote by $k$ the field of endomorphisms of the elliptic curve attached to $\wp$ ; thus $k = \mathbf{Q}$ if $\wp$ has no complex multiplication, while $k = \mathbf{Q}(\tau)$ in the CM case, where $\tau = \omega_2/\omega_1$ is the quotient of a pair of fundamental periods.

We begin with the elliptic analogue to the transcendency of $\log \alpha$ .

Corollary 2.2.3 (Schneider). A non-zero algebraic point of $\wp$ is transcendental.

If we replace the exponential function by an elliptic function in 2.1.1, we get:

Corollary 2.2.4 (Schneider). If $u_1, u_2$ are two algebraic points of $\wp$ which are $k$-linearly independent, then they are $\overline{\mathbf{Q}}$ -linearly independent.

For the proof of corollary 2.2.3 we choose

$$K = \mathbf{Q}(u, \wp(u), \wp'(u), g_2, g_3) \; ; \; f_1(z) = z \; , \; f_2(z) = \wp(z) \; , \; f_3(z) = \wp'(z) \; .$$

For the proof of corollary 2.2.4 we put

$$K = \mathbf{Q}(\wp(u_1), \wp(u_2), \wp'(u_1), \wp'(u_2), g_2, g_3, \frac{u_2}{u_1}); \; f_1(z) = \wp(z),$$

$$f_2(z) = \wp(\frac{u_2}{u_1} z) \; , \; f_3(z) = \wp'(z) \; , \; f_4(z) = \wp'(\frac{u_2}{u_1} z) \; .$$

A very important consequence of 2.2.4 is the theorem of Schneider that the modular function $j$ which satisfies $j(\tau) = \dfrac{1728\, g_2^3}{g_2^3 - 27 g_3^2}$ takes transcendental values for $\tau$ algebraic not imaginary quadratic. An important open question (second problem of Schneider's book) is to prove this result without using elliptic functions.

Further consequences of the criterion 2.2.1 concerning group varieties have been derived by Lang (see also "Nombres transcendants et groupes algébriques", Astérisque, vol. 71, to appear in 1980).

The proof of theorem 2.2.1 is essentially the same as the one given in §2.1, apart from one technical difficulty connected with the arithmetic estimates, which is solved by the following lemma.

Lemma 2.2.5. Let $U$ be an open subset of $\mathbf{C}$, and $f_1, \ldots, f_h$ be analytic functions in $U$. There exists a positive integer $C$ with the following property.

Let $K$ be a number field, $L_1, \ldots, L_h$ be non-negative integers, and $t$ a positive integer. Assume that the ring $K[f_1, \ldots, f_h]$ is invariant under the derivation $\dfrac{d}{dz}$.

There exists a polynomial $P \in K[X_1, \ldots, X_h]$ such that

a) $\frac{d^t}{dz^t}(f_1^{L_1} \dots f_h^{L_h}) = P(f_1,\dots,f_h)$ ;

b) <u>For</u> $i \leq j \leq h$ ,

$$\deg_{X_j} P \leq L_j + Ct$$

c) <u>The coefficients of the polynomial</u> $C^t$ $P$ <u>are algebraic integers of</u> $K$ , <u>whose conjugates have absolute values at most</u>

$$C^{2t}(L_1 + \dots + L_h + t)^t .$$

Theorem 2.2.1 shows the transcendency of several numbers. In order to get transcendence measures for these numbers, one needs an upper bound for the number $N_1$ (which was introduced at the end of §2.1.). This problem has been solved only recently for the general situation of theorem 2.2.1, by D. Brownawell and D. Masser. For transcendental numbers connected with elliptic functions, the best known transcendence measures are due to E. Reyssat. Another consequence of the upper bound of $N_1$ is the possibility to extend the theorem 2.2.1 to a criterion of algebraic independence by means of Gel'fond's method (G. Wüstholz). See further comments on §7.3 and 10.3.

The long outstanding problem of translating Schneider's results on the $\wp$- function into the p-adic case has been solved by D. Bertrand, thanks to a (sharpened) p-adic version of the Schneider-Lang's criterion, which needs a clever use of the Baker-Coates lemma (§6.2).

Finally, the upper bound $(\rho_1+\rho_2)[K:\mathbb{Q}]$ for the number of $w$ which is given in theorem 2.2.1 does not seem best possible and it is not known whether it must depend on $[K:\mathbb{Q}]$. The most natural

way to attack this problem seems to be to replace the size inequality by Schmidt's theorem. Some recent results of Choodnovsky suggest a different approach. (See Annals of Math., 109 (1979), 353-376).

# LECTURE 3

## SCHNEIDER's METHOD

The solution by Schneider of Hilbert's seventh problem can be simplified and leads to an easy proof of Gel'fond-Schneider's theorem. This method can be applied to other problems (six exponentials theorem) but a further sharpening is expected (four exponentials problem ). Schneider's method has been applied by Stewart to a problem of Lehmer; we give in §3.3 a sketch of a proof due to Dobrowolski of a refined estimate.

### §3.1 Schneider's solution of Hilbert's seventh problem

In this section we give a new proof of Gel'fond-Schneider's theorem 2.1.1, along the lines of Schneider's original method in 1934. We assume $\log \alpha_2 = \beta \log \alpha_1$ , with $\beta \in \overline{\mathbf{Q}}$. The two functions $z$ , $\alpha_1^z$ are algebraically independent and take algebraic values at all points $h_1 + h_0 \beta$, $(h_0,h_1) \in \mathbf{Z} \times \mathbf{Z}$ . Our aim is to construct a polynomial $P \in \mathbf{Z}[x_1,x_2]$ , $P \neq 0$ , such that $P(z,\alpha_1^z) = 0$ , and this will be the required contradiction. We first construct $P$ such that the function $F(z) = P(z,\alpha_1^z)$ has a lot of zeros $h_1 + h_0\beta$ , $(h_0,h_1) \in \mathbf{Z} \times \mathbf{Z}$ . Then we show that $F$ vanishes at all the points $h_1 + h_0\beta$ , $(h_0,h_1) \in \mathbf{Z} \times \mathbf{Z}$ , and finally $F = 0$ .

Once more we choose a large positive integer $N$ .
We write our unknown polynomial

$$P(X,Y) = \sum_{\lambda_1=0}^{L_1} \sum_{\lambda_2=0}^{L_2} p(\lambda_1,\lambda_2)\, X_1^{\lambda_1} X_2^{\lambda_2} .$$

The auxiliary function is

$$F(z) = P(z,\alpha_1^z) = \sum_{\lambda_1=0}^{L_1} \sum_{\lambda_2=0}^{L_2} p(\lambda_1,\lambda_2)\, z^{\lambda_1}\, \alpha_1^{\lambda_2 z} .$$

We shall construct $P$ such that

$$F(h_1 + h_0\beta) = 0 , \qquad (0 \le h_0,h_1 < H)$$

We choose

$$L_1 = N^8 , \quad L_2 = N^3 , \quad H = N^5 .$$

Step 1 There exists a non-zero polynomial $P \in \mathbf{Z}[X,Y]$ of degree at most $N^8$ in $X$ and $N^3$ in $Y$, of height at most $e^{N^8}$, such that

$$F(h_1 + h_0\beta) = 0 , \qquad (0 \le h_0, h_1 < H)$$

Proof

Let us consider the system

$$\sum_{\lambda_1=0}^{L_1} \sum_{\lambda_2=0}^{L_2} p(\lambda_1,\lambda_2)(h_1 + h_0\beta)^{\lambda_1}\, \alpha_1^{\lambda_2 h_1}\, \alpha_2^{\lambda_2 h_0} = 0 , \quad (0 \le h_0, h_1 < H)$$

of $H^2$ linear homogeneous equations in $(L_1+1)((L_2+1)$ unknowns $p(\lambda_1,\lambda_2) \in \mathbf{Z}$. We multiply each equation by $(\text{den } \beta)^{L_1} (\text{den } \alpha_1 \text{ den } \alpha_2)^{L_2 H}$. The new system has coefficients in the ring $\mathcal{O}_K$ of integers of the field $K = \mathbf{Q}(\alpha_1,\alpha_2,\beta)$. The house of these coefficients is at most

$$H^{L_1}\, c_1^{L_1}\, c_2^{L_2 H} \le N^{6N^8} .$$

The exponent in Siegel's lemma is at most $\frac{D}{N-D} \le N^{-1/2}$ .

Thus the required result follows from lemma 1.2.2.

Step 2 For each integer $M \geq N$, we have

$(I)_M$ $\quad F(h_1 + h_0\beta) = 0$ for $0 \leq h_0, h_1 < M^5$

and

$(II)_M$ $\quad \log|F|_{M^6} < -M^{10}$

We perform this step by induction on $M$. For $M = N$, $(I)_N$ is step 1. We prove $(I)_M \Rightarrow (II)_M$, using lemma 1.3.1. with $R = M^7$. It is readily verified that

$$|F|_R \leq (L_1+1)(L_2+1)\, e^{N^8} \cdot R^{L_1} c_3^{L_2 R} \leq c_4^{M^{10}} .$$

Since

$$\nu_F(0,M^6) \log \frac{R}{2M^6} \geq M^{10} \log \frac{M}{2} ,$$

the desired property $(II)_M$ follows.

Finally we prove $(II)_M \Rightarrow (I)_{M+1}$. Let $(h_0,h_1) \in \mathbb{Z}^2$ satisfy $0 \leq h_0, h_1 < (M+1)^5$. By $(II)_M$ we have

$$|F(h_1+h_0\beta)| < \exp(-M^{10}) .$$

A denominator of $F(h_1+h_0\beta)$ is

$$(\text{den } \beta)^{L_1} (\text{den } \alpha_1 \text{ den } \alpha_2)^{L_2(M+1)^5} \leq e^{M^9} .$$

The house of $F(h_1+h_0\beta)$ is at most

$$(L_1+1)(L_2+1)e^{N^8} H^{L_1} c_1^{L_1} c_2^{L_2(M+1)^5} \leq e^{M^9} .$$

From the size inequality 1.1.2. we conclude $(I)_{M+1}$, as required.

Step 3. Conclusion: $F = 0$

This is a consequence of the property $(II)_M$ for all $M \geq N$.

Further comments

a) Choice of the parameters

We write for simplicity

$$L_1 = N^{\ell_1},\ L_2 = N^{\ell_2},\ H = N^h,\ R = M^r,$$

and it is sufficient to have

$$\ell_1 + \ell_2 > 2h,\quad 2h > \ell_1,\quad 2h \geq r + \ell_2,\quad r > h.$$

We leave some space with the choice

$$\ell_1 + \ell_2 = 2h + 1,\quad 2h = \ell_1 + 2,\quad 2h = r + \ell_2,\quad r = h+2$$

which implies our values.

b) If we perform the third step before the second one, we obtain the existence of an integer $N_1 > N$ such that one at least of the numbers

$$F(h_1 + h_0\beta),\qquad (0 \leq h_0, h_1 < N_1^5)$$

is not zero. It is not difficult to see that the smallest $N_1$ with this property satisfies $N_1 \leq 2N$. In his original paper, Schneider proves this by computing a determinant. In any case, this is now a consequence of Tijdeman's result.

## §3.2 Consequences of Schneider's method

We do not state a general transcendence criterion (see for instance Lecture Notes 402, Chap 2), but merely give some examples of results which can be proved by Schneider's method.

An easy exercise is to use the preceeding method with $z$, $\alpha_1^z$ replaced either by $e^{x_1 z}$, $e^{x_2 z}$, or by $e^{y_1 z}$, $e^{y_2 z}$, $e^{y_3 z}$, to deduce the theorem of the six exponentials (due to Siegel, Schneider, Lang, Ramachandra,...)

**Theorem 3.2.1** *Let $x_1$, $x_2$ be two linearly independent complex numbers. Let $y_1$, $y_2$, $y_3$ be three linearly independent complex numbers. Then at least one of the six numbers*

$$e^{x_1 y_1}, \quad e^{x_1 y_2}, \quad e^{x_1 y_3},$$

$$e^{x_2 y_1}, \quad e^{x_2 y_2}, \quad e^{x_2 y_3}$$

*is transcendental.*

The problem of replacing $y_1$, $y_2$, $y_3$ by $y_1$, $y_2$ only is yet unsolved. This "conjecture of the four exponentials" is stated in an equivalent form by Schneider (first problem): if $\log \alpha_1$, $\log \alpha_2$, $\log \alpha_3$, $\log \alpha_4$ are logarithms of algebraic numbers, with $\log \alpha_1$, $\log \alpha_2$ $\mathbb{Q}$-linearly independent, and $\log \alpha_1$, $\log \alpha_3$ $\mathbb{Q}$-linearly independent, then

$$\det \begin{vmatrix} \log \alpha_1 & \log \alpha_3 \\ \log \alpha_2 & \log \alpha_4 \end{vmatrix} \neq 0$$

Similar problems can be stated for higher dimensional determinants, in connection with the problem of the non-vanishing of the p-adic regulator, and in connection with a problem of Weil (in the complex case) and Serre (in the p-adic case) on characters associated with Hecke L-series.

Problem 3.2.2. Let $K$ be a number field of degree $n$ over $\mathbb{Q}$, $\{\sigma : K \to \mathbb{C}\}$ the set of $n$ embeddings of $K$ into $\mathbb{C}$, and $(x_\sigma) \in \mathbb{C}^n$. Assume that for all $\alpha \in K$, the number $\prod_\sigma |\sigma\alpha|^{x_\sigma}$ is algebraic. Prove that $x_\sigma \in \mathbb{Q}$ if $\sigma$ is real and $x_\sigma + x_{\bar{\sigma}} \in \mathbb{Q}$ if $\sigma$ and $\bar{\sigma}$ are congugate.

One can consider it either as a problem in several variables, or as a special case of the problem of algebraic independence of logarithms of algebraic numbers.

Another consequence of Schneider's method is the following result: there exists an absolute constant $c_0 > 0$ such that if $f$ is an entire function in $\mathbb{C}$ with $f(\mathbb{N}) \subset \mathbb{Z}$ and

$$\limsup_{R \to +\infty} \frac{1}{R} \log |f|_R < c_0$$

then $f$ is a polynomial. Another method (using interpolation formulae) enabled Pólya early in 1919 to prove this result with $c_0 = \log 2$ (which is plainly best possible). This method of Pólya was developed further by Gel'fond who solved the problem of the transcendency of $e^\pi$ in 1929 by this mean. The connection between the arithmetic properties of the values, and the growth of an entire function, is at the heart of the theory.

A further application of Schneider's method is the following result

Theorem 3.2.3. Let $G$ be an algebraic group over $\bar{\mathbf{Q}}$, $\varphi : \mathbf{C} \to G_{\mathbf{C}}$ an analytic homomorphism which is not rational, and $\Gamma$ a finitely generated subgroup of $\bar{\mathbf{Q}}$ such that $\varphi(\Gamma) \subset G_{\bar{\mathbf{Q}}}$. Then the rank of $\Gamma$ over $\mathbf{Z}$ is at most 2.

Exercise 3.2.4. In the case where $G$ is an elliptic curve, prove this result as a consequence of 2.2.4, and prove that the upper bound 2 cannot be improved.

Ramachandra used Schneider's method to prove a general result on "algebraically additive" functions. As a corollary he deduces the following interesting statement

Theorem 3.2.5. (Ramachandra). Let $a$, $b$ be two multiplivatively independent algebraic numbers, $\log a$, $\log b$ be determinations of their logarithms, and $\wp$ the Weierstrass elliptic function associated with the lattice $\mathbf{Z} \log a + \mathbf{Z}\, 2i\pi$. Then one at least of the two numbers

$$j\left(\frac{\log a}{2i\pi}\right), \qquad (\Delta(\log a, 2i\pi))^{-\frac{1}{6}}\, \wp(\log b)$$

is transcendental.

The open problem of the transcendency of $j\left(\frac{\log a}{2i\pi}\right)$ arises in papers by Mahler and Manin.

## §3.3 On the product of the conjugates outside the unit circle of an algebraic integer

Let $\alpha$ be a non-zero algebraic integer of degree $d$. We recall the definition (§1.1) of Mahler's measure:

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

Obviously $M(\alpha) \geq 1$, and $M(\alpha) = 1$ if $\alpha$ is a root of unity. A theorem of Kronecker (1857) asserts that conversely, if $M(\alpha) = 1$, then $\alpha$ is a root of unity. In 1933, D.H. Lehmer asked: is it true that for every positive $\varepsilon$ there exists an algebraic integer $\alpha$ for which $1 < M(\alpha) < 1 + \varepsilon$ ? The answer is not yet known, but the smallest value larger than one of $M(\alpha)$ which is known is 1.17628..., which is the largest root of the polynomial

$$X^{10} + X^9 - X^7 - X^6 - X^5 - X^4 - X^3 + X + 1 .$$

(This example goes back to Lehmer). This polynomial is reciprocal; it can be written $X^5 P(X + \frac{1}{X})$ where $P(Y) = (Y+1)^2(Y-1)(Y+2)(Y-2) - 1$. In fact, in 1971 C.J. Smyth showed that if $\beta_0 = 1.32471...$ denotes the real root of the polynomial $X^3 - X - 1$, and if $\alpha$ is a non-zero algebraic integer which is not conjugate of $\alpha^{-1}$, then $M(\alpha) \geq \beta_0$. Thus $\beta_0$ is the smallest P.V. number (as shown by Siegel in 1944).

Since there is no universal lower bound (greater than 1) known for $M(\alpha)$ (with $\alpha$ not root of unity), a first step towards a negative answer to Lehmer's question is to give a lower bound for $M(\alpha)$ depending on the degree of $\alpha$. Until recently the best known estimate was due to

Blanksby and Montgomery: there exists a number $C(d)$ such that

$$C(d) > 1 + (52d \log 6d)^{-1}$$

and such that the condition $M(\alpha) < C(d)$ implies that $\alpha$ is a root of unity. In 1977 C. L. Stewart got a slightly less precise constant

$$C(d) > 1 + (10^4 d \log d)^{-1}$$

by means of a completely different argument, using Schneider's method. Then Dobrowolski obtained a very simple and elegant result: if $\alpha$ (non-zero algebraic integer of degree d) satisfies

$$|\alpha| < 1 + (\log d)/6d^2 ,$$

then $\alpha$ is a root of unity (the result of Blanksby and Montgomery yields the same conclusion only with the stronger hypothesis $|\alpha| > 1 + (30\, d^2 \log 6d)^{-1}$) . Finally in a paper to appear in Bull. Acad. Polon. Sci.,Dobrowslski obtained a sharp estimate.

Theorem 3.3.1 (Dobrowolski). Let $\alpha$ be a non-zero algebraic integer of degree $d$ . If $\alpha$ is not a root of unity, then

$$M(\alpha) > 1 + \frac{1}{1200}\left(\frac{\log \log d}{\log d}\right)^3$$

Moreover for any $\varepsilon > 0$ there exists $d_0(\varepsilon)$ such that for $d > d_0(\varepsilon)$ ,

$$M(\alpha) > 1 + (1-\varepsilon)\left(\frac{\log \log d}{\log d}\right)^3$$

The proof of Dobrowolski adopts Stewart approach, together with congruence relations. We give here a simplified proof with 1200 replaced

by $10^6$ (the simplification is due to M. Mignotte).

We begin with three remarks whose proofs are left as exercises.

Remark 3.3.2. Let $\alpha$ be a non-zero algebraic number which is not a root of unity, $\alpha'$ a conjugate of $\alpha$. If $r$ and $s$ are two non-zero integers with $\alpha'^r = \alpha^s$, then $|r| = |s|$.

Remark 3.3.3. Let $\alpha$ be a non-zero algebraic number, and $p$ a prime. If $\deg \alpha^p < \deg \alpha$, then there exists $\beta \in \mathbf{Q}(\alpha^p)$ such that $1 < M(\beta) \leq M(\alpha)$.

Remark 3.3.4 In the proof of theorem 3.3.1., there is no loss of generality to assume $d \geq 16$, and to assume that for any prime $p$, $\deg \alpha^p = \deg \alpha$.

We now give a sketch of proof of theorem 3.3.1.

We define

$$T = [50(\log d)(\log\log d)^{-1}], \quad L = dT^2$$

Let $P$ be the minimal polynomial of $\alpha$ over $\mathbf{Z}$.

Step 1. There exists a non-zero polynomial $F \in \mathbf{Z}[X]$ of degree at most $L-1$ and height at most

$$H(F) \leq 2 + (2^T L^{T^2} d_{M(\alpha)}^{TL})^{1/(L-Td)}$$

and which is divisible by $P(x)^T$.

This means that Dobrowolski needs a polynomial $F$ satisfying $\frac{d^t}{dz^t} F(\alpha) = 0$ for $0 \leq t < T$. An obvious choice is $P^T$. But $P^T$ has too large coefficients. Thus one allows the degree of $F$ to be larger than $\deg P^T = dT$, but one asks for smaller coefficients. The answer is provided by a sharpened version of Siegel's lemma (§1.2).

Step 2 There exists a prime number $p$ with

$$\frac{L}{d} \leq p \leq 3 \frac{L}{d} \log \frac{L}{d}$$

such that

$$F(\alpha^p) \neq 0$$

This is a consequence of the remarks 3.3.2. and 3.3.4.

Step 3 The norm of $F(\alpha^p)$ over $\mathbb{Q}$ satisfies

$$p^{Td} \leq |N(F(\alpha^p))| \leq (L.H(F))^d \, M(\alpha)^{Lp}$$

The upper bound is obvious. It is a very special feature of Dobrowolski's proof that he succeeds to improve the trivial lower bound $1 \leq |N(F(\alpha^p))|$. The point is that by the small theorem of Fermat

$$F(X)^p \equiv F(X^p) \mod p\mathbb{Z}[X] ,$$

thus $p^{dT}$ divides the norm of $F(\alpha^p)$.

Conclusion. The result follows from an easy computation.

# LECTURE 4

## BAKER'S METHOD

The theorem of Gel'fond-Schneider states that two logarithms of algebraic numbers which are linearly independent over $\mathbb{Q}$ are also linearly independent over $\overline{\mathbb{Q}}$. In 1935 Gel'fond extended his method to derive a non-trivial effective lower bound for a linear form $|\beta_1 \log \alpha_1 + \beta_2 \log \alpha_2|$. Later he derived several interesting applications of this estimate. As a consequence of the Thue-Siegel theorem, he obtained a non-trivial (but ineffective) lower bound for linear forms in $n$ logarithms with integer coefficients; in connection with diophantine equations and class number problems, he proved the significance of obtaining explicit estimates.

Baker was the first to see how to deal with more than two logarithms by the effective methods of the theory of transcendental numbers. The crucial point is that he succeeded to reduce the problem to the one variable case by means of a new interpolation procedure.

We give here a first proof of Baker's theorem. In the next lecture we discuss later developments of the subject.

### §4.1 The results (qualitative form).

Theorem 4.1.1. (Baker). Let $\alpha_1,\ldots,\alpha_n$ be non-zero algebraic numbers, and for $j = 1,\ldots,n$, let $\log \alpha_j$ be any determination of the logarithm of $\alpha_j$. If $\log \alpha_1,\ldots,\log \alpha_n$ are $\mathbb{Q}$-linearly independent, then $1, \log \alpha_1,\ldots,\log \alpha_n$ are $\overline{\mathbb{Q}}$-linearly independent.

This result obviously generalizes the theorems of Hermite-Lindemann 2.2.2 and of Gel'fond-Schneider 2.1.1. It shows that numbers like

$$e^{\beta_0}\ \alpha_1^{\beta_1}\ \ldots\ \alpha_n^{\beta_n}$$

or

$$\frac{\beta_0 + \beta_1 \log \alpha_1 + \ldots + \beta_s \log \alpha_s}{\beta_0' + \beta_1' \log \alpha_1' + \ldots + \beta_t' \log \alpha_t'}$$

(with algebraic $\alpha$'s and $\beta$'s) can be algebraic only in trivial circumstances.

For simplicity we will give the proof only of the homogeneous result that $\log \alpha_1, \ldots, \log \alpha_n$ are $\bar{\mathbf{Q}}$-linearly independent (without 1).

## §4.2 Sketch of the proof.

The proof uses a generalization of Gel'fond's method. Let us assume that

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

with $\log \alpha_1, \ldots, \log \alpha_{n+1}$ $\mathbf{Q}$-linearly independent, and the $\alpha$'s and $\beta$'s are algebraic numbers. Our auxiliary function will be

$$F(z) = P(\alpha_1^z, \ldots, \alpha_{n+1}^z) ,$$

where $P \in \mathbf{Z}[X_1, \ldots, X_{n+1}]$ is some polynomial to be chosen. Let us write

$$F(z) = \sum_{\lambda_1} \ldots \sum_{\lambda_{n+1}} p(\lambda_1, \ldots, \lambda_{n+1}) \alpha_1^{\lambda_1 z} \ldots \alpha_{n+1}^{\lambda_{n+1} z}$$

$$= \sum_{(\lambda)} p(\lambda) \prod_{j=1}^{n+1} \alpha_j^{\lambda_j z}$$

where $(\lambda)$ stands for $(\lambda_1,\dots,\lambda_{n+1})$. Using our assumption we have also

$$F(z) = \sum_{(\lambda)} p(\lambda)\, \alpha_1^{\gamma_1 z} \dots \alpha_n^{\gamma_n z} ,$$

where $\gamma_i = \lambda_i + \lambda_{n+1}\beta_i$, $(1 \le i \le n)$. In order to use the assumption that the $\beta$'s are algebraic, we differentiate this function: for $t \in \mathbf{N}$ we have

$$\frac{d^t}{dz^t} F = \sum_{|\tau|=t} \binom{t}{\tau} (\log \alpha_1)^{\tau_1} \dots (\log \alpha_n)^{\tau_n} F_\tau ,$$

where

$$\tau = (\tau_1,\dots,\tau_n),\ \binom{t}{\tau} = \frac{t!}{\tau_1! \dots \tau_n!},\ |\tau| = \tau_1+\dots+\tau_n ,\ \text{and}$$

$$F_\tau(z) = \sum_{(\lambda)} p(\lambda)\, \gamma_1^{\tau_1} \dots \gamma_n^{\tau_n} \alpha_1^{\gamma_1 z} \dots \alpha_n^{\gamma_n z}$$

The very crucial point is the following.

Lemma 4.2.1. Let $s, \tau_1,\dots,\tau_n$ be non-negative integers

Then
$$\frac{d^s}{dz^s} F_\tau = \sum_{|\sigma|=s} \binom{s}{\sigma} (\log \alpha_1)^{\sigma_1} \dots (\log \alpha_n)^{\sigma_n} F_{\tau+\sigma} .$$

This formula is readily verified by use of Leibnitz formula:

$$\frac{d^s}{dz^s} F_\tau(z) = \sum_{(\lambda)} p(\lambda)\, \gamma_1^{\tau_1} \dots \gamma_n^{\tau_n} \sum_{|\sigma|=s} \binom{s}{\sigma} (\gamma_1 \log \alpha_1)^{\sigma_1} \dots$$

$$\dots (\gamma_n \log \alpha_n)^{\sigma_n} \alpha_1^{\gamma_1 z} \dots \alpha_n^{\gamma_n z}$$

One can also see it by writing

$$F(z) = \Phi(z,\dots,z)$$

where

$$\Phi(z_1,\dots,z_n) = \sum_{(\lambda)} p(\lambda)\, \alpha_1^{\gamma_1 z_1} \dots \alpha_n^{\gamma_n z_n} .$$

Thus

$$F_\tau(z) = (\log \alpha_1)^{\tau_1} \dots (\log \alpha_n)^{\tau_n} \frac{\partial^{|\tau|}}{\partial z_1^{\tau_1} \dots \partial z_n^{\tau_n}} \Phi(z,\dots,z) ,$$

and the formula of lemma 4.2.1 merely expresses the relation for an analytic function $\Psi$ of $n$ variables:

$$\frac{d^s}{dz^s} \Psi(z,\dots,z) = \sum_{|\sigma|=s} \binom{s}{\sigma} \frac{\partial^s}{\partial z_1^{\sigma_1} \dots \partial z_n^{\sigma_n}} \Psi(z,\dots,z) .$$

This lemma 4.2.1 will be used in the following way. Assume that $z_0 \in \mathbb{C}$ and $T \in \mathbb{N}$ are such that

$$F_{(\tau)}(z_0) = 0 \quad \text{for all} \quad |\tau| < T .$$

This implies that $F$ has a zero at $z_0$ of order at least $T$. But this last condition involves only $T$ conditions, while our assumption involves $\binom{T+n}{n}$ equations (roughly $T^n$). Thus one can expect more information from our assumption. Indeed lemma 4.2.1 implies that <u>each function</u> $F_\tau$, $|\tau| < T$ <u>has a zero at</u> $z_0$ <u>of order at least</u> $T-|\tau|$. In particular for $|\tau| \leq \frac{T}{2}$, $F_\tau$ has a zero of order at least $\frac{T}{2}$.

The sketch of the proof is the following. We construct $P \in \mathbb{Z}[X_1,\ldots,X_{n+1}]$, not zero, such that

$$F_\tau(h) = 0 \quad \text{for} \quad |\tau| < T , \ 0 \leq h < N .$$

Then we show that

$$F_\tau(h) = 0 \quad \text{for} \quad |\tau| < \frac{T}{2} , \ 0 \leq h < N^2 .$$

For this we observe that these numbers are values of a function having a lot of zeroes, by Schwarz lemma they are small; being algebraic they cannot be too small without vanishing.

It is not known how to get immediately a contradiction from this new set of equations. But we can use the same argument and prove

$$F_\tau(h) = 0 \quad \text{for} \quad |\tau| < \frac{T}{4} , \ 0 \leq h < N^3 .$$

We cannot push this process up to infinity, because the order of the derivatives is decreasing. Thus we need a new device to get a contradiction after a finite number of steps. In the present lecture we shall use some analytic results on exponential polynomials. In the

next chapter we shall use an arithmetic method which rests on Kummer's theory.

§4.3 The proof.

Let $\log \alpha_1, \ldots, \log \alpha_{n+1}$ be $\mathbb{Q}$-linearly independent logarithms of algebraic numbers, and $\beta_1, \ldots, \beta_n$ be algebraic numbers. Assume

$$\log \alpha_{n+1} = \beta_1 \log \alpha_1 + \ldots + \beta_n \log \alpha_n .$$

We shall eventually derive a contradiction. Define

$$K = \mathbb{Q}(\alpha_1, \ldots, \alpha_{n+1}, \beta_1, \ldots, \beta_n) .$$

Let $N$ be a sufficiently large integer. We put

$$L = N^{2n+2} , \quad T = N^{2n+4}$$

First step. There exists a non-zero polynomial $P \in \mathbb{Z}[X_1, \ldots, X_{n+1}]$, of degree at most $L$ in $X_j$, $(1 \leq j \leq n+1)$ and height at most $\exp(N^{2n+4})$, such that $F_\tau(h) = 0$ for $|\tau| < T$ and $0 \leq h < N$.

Proof

We consider the homogeneous linear system

$$\sum_{(\lambda)} p(\lambda)\, \gamma_1^{\tau_1} \ldots \gamma_n^{\tau_n}\, \alpha_1^{\lambda_1 h} \ldots \alpha_{n+1}^{\lambda_{n+1} h} = 0 , \qquad \text{for } |\tau| < T , \ 0 \leq h < N ,$$

of $\binom{T+n}{n} N \leq T^n N$ equations in $(L+1)^{n+1}$ unknowns $p(\lambda)$. (We write as above $\gamma_i = \lambda_i + \lambda_{n+1} \beta_i$). We multiply each equation by

$$\Big(\prod_{i=1}^{n} (\text{den } \beta_i)^{\tau_i}\Big)\Big(\prod_{j=1}^{n+1} (\text{den } \alpha_j)^{Lh}\Big) ,$$

and the new system has coefficients in the ring of integers of $K$. The house of these coefficients is at most

$$L^T c_1^T c_2^{LN} \leq \exp((2n+3)\, N^{2n+4} \log N) ,$$

where $c_1$ and $c_2$ do not depend on $N$ :

$$c_1 = \prod_{i=1}^{n} (\text{den } \beta_i)(1 + \lceil \beta_i \rceil) ,$$

$$c_2 = \prod_{j=1}^{n+1} (\text{den } \alpha_j)\, \lceil \alpha_j \rceil$$

The exponent in Siegel's lemma is at most $N^{-\frac{1}{2}}$. Our claim follows immediately from lemma 1.2.2.

Second Step: induction. Let $S$ be a positive integer which does not depend on $N$ (we shall choose $S = 2(n+1)^2$ .) For any non-negative integer $s$ with $s \leq S$ , we have

$$F_\tau(h) = 0 \quad \text{for} \quad |\tau| < 2^{-s}T \quad \text{and} \quad 0 \leq h < N^{s+1}$$

The case $s = 0$ is our first step. We assume that the result holds for some integer $s-1$ , $1 \leq s \leq S$ , and we prove it for $s$ .

By induction hypothesis, and thanks to lemma 4.2.1, for $|\tau| < 2^{-s}T$ the function $F_\tau$ has a zero at each point $h \in \mathbf{Z}$ , $0 \leq h < N^s$ , of order at least $2^{-s}T$ . From lemma 1.3.1 we deduce for $N^s < r < R$

$$\log|F_\tau|_r \leq \log|F_\tau|_R - 2^{-s}TN^s \log\frac{R}{2r} .$$

We choose $r = N^{s+1}$ , $R = N^{s+2}$ . From the definition of $F_\tau$ we deduce

$$|F_\tau|_R \leq (L+1)^{n+1} \; e^{N^{2n+4}} \; (c_3L)^{|\tau|} \; c_4^{LR} \leq c_5^{N^{2n+s+4}} ,$$

where $c_3 = \max_{1\leq i\leq n}(1 + |\beta_i|)$ , $c_4 = \exp(\sum_{j=1}^{n+1} |\log \alpha_j|)$ , $c_5 = ec_4$ .

Hence

$$|F_\tau(h)| < \exp(-2^{-s-1} N^{2n+s+4} \log N) \quad \text{for} \quad |\tau| < 2^{-s}T, \; 0 \leq h < N^{s+1}$$

On the other hand $F_\tau(h)$ is an algebraic number in $K$ , of denominator at most

$$(\prod_{i=1}^{n} \text{den } \beta_i)^T . (\prod_{j=1}^{n+1} \text{den } \alpha_j)^{Lh} \leq \exp(N^{2n+4+s})$$

and of house at most

$$(L+1)^{n+1} \; e^{N^{2n+4}} \; L^T . c_1^T . \; c_2^{Lh} \leq \exp(N^{2n+4+s}) .$$

From the size inequality 1.1.2 we conclude

$$F_\tau(h) = 0 \quad \text{for} \quad |\tau| < 2^{-s}T , \; 0 \leq h < N^{s+1}$$

We postpone the third step (conclusion) to the next section.

§4.4 Conclusion of the proof.

From step 2 we know that our function $F$ satisfies

$$\frac{d^t}{dz^t} F(h) = 0 \quad \text{for} \quad 0 \leq t < 2^{-S}T \ , \ 0 \leq h < N^{S+1} \ .$$

Hence $F$ has more than $N^{2n^2+6n+6}$ zeroes in the disc $N^{2n^2+4n+3}$. We proceed to prove that this condition is untenable since $F \not\equiv 0$. We begin with the case where $\log \alpha_1, \ldots, \log \alpha_{n+1}$ are real numbers; in this case our desired contradiction is a straightforward consequence of the following simple lemma (with $M = (L+1)^{n+1}$).

Lemma 4.4.1 Let $w_1, \ldots, w_M$ be distinct real numbers. Let $a_1, \ldots, a_M$ be real numbers, not all of which are zero. Then the number of real zeroes (counting multiplicities) of the function

$$F(x) = \sum_{m=1}^{M} a_m e^{w_m x}$$

is at most $M - 1$.

Proof

We prove the lemma by induction on $M$. For $M = 1$ the result is clear. Assume the result is proved for $M - 1$. Then the function $G'(x)$, where $G(x) = e^{-w_M x} F(x)$, has at most $M - 2$ zeroes. From Rolle's theorem it follows that $G$, and therefore $F$, has at most $M - 1$ zeroes (cf. Pólya-Szegö, Part V no.75).

(It is easy to generalize this proof to the case where $a_m$ are polynomials with real coefficients.)

By means of a complex generalization of Rolle's theorem, M. Voorhoeve has proved two years ago the following very sharp result.

Theorem 4.4.2. Let $p_1,\ldots,p_\ell$ be positive integers, $a_{k,j}$, $(1 \le j \le p_k\ ,\ 1 \le k \le \ell)$ be complex numbers, not all zero, $w_1,\ldots,w_\ell$ be pairwise distinct complex numbers, and $R$ a positive real number. Define

$$\Omega = \max_{1\le k\le \ell} |w_k| \quad , \quad M = \sum_{k=1}^{\ell} p_k \ .$$

Then the number $\nu_F(0,r)$ of zeroes in the disc $|z| \le r$ of the function

$$F(z) = \sum_{k=1}^{\ell} \sum_{j=1}^{p_k} a_{k,j}\, z^{j-1}\, e^{w_k z}$$

satisfies

$$\nu_F(0,r) \le 2(M-1) + \frac{4}{\pi}\, r\, \Omega$$

A previous result due to R. Tijdeman was

$$\nu_F(0,r) \le 3(M-1) + 4r\Omega$$

Of course this is sufficient for our purpose. It is even sufficient to use earlier bounds (going back to Gel'fond) involving

$$\min_{k\ne k'} |w_k - w_{k'}| \ .$$

Here is a sketch of the proof of Tijdeman in the case where $p_1 = \ldots = p_\ell = 1$ (i.e. $F(z) = \sum_{m=1}^{M} a_m e^{w_m z}$) which is sufficient for our purpose.

Let $R > r > 0$ be real numbers, and let $u \in \mathbb{C}$, $|u| = R$ be such that $|F(u)| = |F|_R$. We consider the polynomial $P \in \mathbb{C}[z]$ of degree less than $M$ such that

$$P(w_h) = e^{w_h u}, \quad (1 \leq h \leq M)$$

Clearly $P$ is given by the Lagrange interpolation formula

$$P(z) = \sum_{h=1}^{M} e^{w_h u} \cdot \prod_{k \neq h} \frac{z - w_k}{w_h - w_k}$$

However we get a better upper bound (independent of $\min_{h \neq k} |w_h - w_k|$) for the coefficients $b_m$ of $P$ :

$$P(z) = \sum_{m=1}^{M} b_m z^{m-1}$$

if we express these coefficients by means of integral formulae.

Now we observe that

$$F(u) = \sum_{k=1}^{M} a_k P(w_k)$$

$$= \sum_{m=1}^{M} b_m \sum_{k=1}^{M} a_k w_k^{m-1}$$

$$= \sum_{m=1}^{M} b_m \frac{d^{m-1}}{dz^{m-1}} F(0) .$$

From Cauchy's inequalities we derive an upper bound for the numbers $|\frac{d^{m-1}}{dz^{m-1}} F(0)|$ , $(1 \leq m \leq M)$ , in terms of $|F|_r$ . Thus we get an upper bound for $|F|_R$ in terms of $|F|_r$ , and this is the main point. The very estimate of Tijdeman is

$$|F|_R \leq |F|_r \cdot e^{(r+R)\Omega} \cdot \frac{R^M - r^M}{r^{M-1}(R-r)} , \quad (R > r > 0) .$$

Then the desired upper bound for $\nu_F(0,r)$ follows from Schwarz lemma 1.3.1 (with a suitable choice for $R$ ).

## §4.5 Further results and comments.

The proof of the non homogeneous case of theorem 4.1.1.:

$$\log \alpha_{n+1} = \beta_0 + \beta_1 \log \alpha_1 + \ldots + \beta_n \log \alpha_n$$

uses an auxiliary function

$$P(z , \alpha_1^z, \ldots, \alpha_{n+1}^z)$$

and the method is the same.

One conjectures that with the hypotheses of Baker's theorem 4.1.1, the numbers $\log \alpha_1, \ldots, \log \alpha_n$ are algebraically independent (special case of Schanuel's conjecture). However very little is known in this direction. One does not even know that for $n$ large the transcendence degree is at least $2$ . However some progress have been made in recent years by Choodnovsky in direction of Schanuel's conjecture.

We postpone a general discussion of Baker's method to §10.3, in the light of Bombieri's transcendence criterion.

# LECTURE 5

## KUMMER'S THEORY

The introduction of arguments of Kummer's style in transcendental number theory is due to J. Coates. In 1970, he gave a lower bound for $\beta_1 u_1 + \beta_2 \log \alpha_2$, where $\beta_1$, $\beta_2$, $\alpha_1 = \wp(u_1)$ and $\alpha_2$ are algebraic numbers, and $\wp$ is a Weierstrass elliptic function with $g_2$, $g_3$ algebraic. In his proof, he used a result of Tate on the division points of elliptic functions. One year later, while considering the linear independence of periods of exponential and elliptic functions, he used a result of Serre on the torsion points. Then Baker and Stark, in a joint work, introduced the Kummer theory in the multiplicative case for a lower bound of linear forms in logarithms.

We first give a new argument for the last step of the preceeding lecture, which occured in the paper of Baker and Stark, and which will occur again in the elliptic case (lecture 6.) Then we produce another proof of Baker's result, which is originated in the paper of Baker usually quoted as "Sharpening III" (Acta Arith., 27 (1975), 247-252).

## §5.1 An alternative method for the last step.

We go back to the end of §4.3. At the end of the second step, our auxiliary function $F$ satisfies

$$\frac{d^t}{dz^t} F(h) = 0 \quad \text{for} \quad 0 \leq t < 2^{-S}T , \quad 0 \leq h < N^{S+1} .$$

Let $q$ be a prime number with $L < q \leq 2L$. We prove that

$$F(\tfrac{1}{q}) = 0 .$$

To prove this assertion we begin by noting that the Schwarz lemma 1.3.1 with

$$r = N^{2n^2+4n+3}, \quad R = Nr , \quad v_F(0,r) > N^{2n^2+6n+6}$$

gives

$$|F(\tfrac{1}{q})| < \exp(-N^{2n^2+6n+6}).$$

On the other hand $F(\frac{1}{q})$ is an algebraic number, of house at most

$$(L+1)^{n+1} e N^{2n+4} \overline{|\alpha_1|} \ldots \overline{|\alpha_{n+1}|} \leq \exp(2N^{2n+4}),$$

of denominator at most

$$[(\text{den } \alpha_1) \ldots (\text{den } \alpha_{n+1})]^L \leq \exp(N^{2n+3})$$

and of degree at most $q^{n+1}D \leq C_6 N^{2(n+1)^2}$. From the size inequality 1.1.2 we conclude $F(\frac{1}{q}) = 0$, as claimed.

Now the required contradiction follows from the next lemma.

*Lemma* 5.1.1. *Let* $\log \alpha_1, \ldots, \log \alpha_r$ *be* $\mathbb{Q}$*-linearly independent logarithms of algebraic numbers. There exists a positive integer* $L_0$ *such that if* $P \in \mathbb{Z}[X_1, \ldots, X_r]$ *is a non-zero polynomial of degree at most* $L$ *in* $X_i$, $(1 \leq i \leq r)$ *with* $L \geq L_0$, *then for all prime* $q > L$ *we have*

$$P(\alpha_1^{1/q}, \ldots, \alpha_r^{1/q}) \neq 0 ,$$

where $\alpha_j^{1/q} = \exp\left(\frac{1}{q}\log\alpha_j\right)$ , $(1\leq j\leq r)$ .

Proof of the lemma.

There is no loss of generality to assume $\log\alpha_1 = i\pi$ . We define $K = \mathbb{Q}(\alpha_1,\ldots,\alpha_r)$ , $K_j = K(\alpha_1^{1/q},\ldots,\alpha_j^{1/q})$ , $(1\leq j\leq r)$ . By Kummer's theory for $q$ sufficiently large we have

$$[K_1 : K] = q - 1 ,$$

and $$[K_j : K_{j-1}] = q \quad , 2\leq j\leq r$$

If $\alpha_r^{1/q}$ is a root of the polynomial $P(\alpha_1^{1/q},\ldots,\alpha_{r-1}^{1/q}, X)$ (of degree $\leq L$ and coefficients in $K_{r-1}$) this polynomial is identically zero. Recursively we get the contradiction that $P$ itself is identically zero.

## §5.2 A second proof of Baker's theorem.

### a) Introduction.

In all the methods we are considering we start with Siegel's lemma, and therefore for the first step we need more unknowns (namely the coefficients of the auxiliary function) than equations. In the methods of Gel'fond and Schneider the number of equations is in fact the number of zeroes of our auxiliary function, while in Baker's method the number of equation (roughly $T^nN$) is larger than the number of zeroes ($TN$).

For the final contradiction we need much more equations than unknowns (in §5.1, we use only one equation $F(\frac{1}{q}) = 0$ , but this equation involves a field of large degree, $Dq^{n+1}$ , and this amounts to $Dq^{n+1}$ equations.)

In all the previous methods we have increased the number of equations, while the number of coefficients was fixed. Here we shall work with a fixed number of equations, and change our auxiliary function at each step of the inductive argument in such a way that the number of coefficients is decreasing.

Let $\alpha_1,\ldots,\alpha_{n+1}$, $\beta_1,\ldots\beta_n$ be algebraic numbers, the $\alpha$'s being all different from zero; let $\log \alpha_1,\ldots,\log \alpha_{n+1}$ be determinations of the logarithms of the $\alpha$'s. We assume

$$\log \alpha_{n+1} = \beta_1 \log \alpha_1 + \ldots + \beta_n \log \alpha_n .$$

Moreover we assume that there is a prime number $q$ such that

$$[K(\alpha_1^{1/q},\ldots,\alpha_{n+1}^{1/q}) : K] = q^{n+1} ,$$

where $K = \mathbb{Q}(\alpha_1,\ldots,\alpha_{n+1}, \beta_1,\ldots,\beta_n)$ , and

$$\alpha_j^{1/q} = \exp(\tfrac{1}{q} \log \alpha_j) , \qquad (1\le j\le n+1)$$

We shall derive a contradiction, and then show (in §5.3) how to deduce Baker's theorem from this contradiction.

b) Sketch of the proof.

The first step is the same as in §4.3. Thus we have an auxiliary function $F$ such that

$$F_\tau(h) = 0 \qquad \text{for } |\tau| < T , \ 0 \le h < N.$$

The second step is an inductive argument. We shall give and prove the inductive statement below; here we first explain how it works. We consider the numbers $F_\tau(\frac{h}{q})$ for $|\tau| < \frac{T}{q}$ and $0 \le h < qN$, with $(h,q) = 1$ . Our parameter $N$ is large with respect to $q$ , and the usual arguments (Schwarz lemma and Liouville inequality) show that these numbers all vanish. Using our assumption on the independence of the $q$-th roots of the $\alpha$'s, we express each $F_\tau(h/q)$ on the basis

$$\{\alpha_1^{\ell_1/q} \ldots \alpha_{n+1}^{\ell_{n+1}/q} , \ 0\le \ell_j < q , \quad 1\le j\le n+1\} .$$

Remark that

$$F_\tau(\frac{h}{q}) = \sum_{(\lambda)} p(\lambda)\Big(\prod_{i=1}^{n} (\lambda_i+\lambda_{n+1}\beta_i)^{\tau_i}\Big)\, \alpha_1^{\lambda_1 h/q} \cdots \alpha_{n+1}^{\lambda_{n+1} h/q} .$$

Thus from one equation $F_\tau(\frac{h}{q}) = 0$ we get $q^{n+1}$ equations, each of which can be written

$$\sum_{\substack{\lambda_j \equiv \lambda_j^0 \bmod q \\ (1\le j\le n+1)}} p(\lambda)\Big(\prod_{i=1}^{n} (\lambda_i+\lambda_{n+1}\beta_i)^{\tau_i}\Big)\, \alpha_1^{\lambda_1 h/q} \cdots \alpha_{n+1}^{\lambda_{n+1} h/q} = 0 ,$$

for $0 \le \lambda_j^0 < q$ , $(1\le j\le n+1)$. We choose $(\lambda_1^0,\ldots,\lambda_{n+1}^0)$ with $0\le\lambda_j^0<q$ , $(1\le j\le n+1)$, in such a way that at least one of the numbers $p(\lambda)$, $\lambda_j \equiv \lambda_j^0 \bmod q$ $(1\le j\le n+1)$ is not zero. Then we define, for $(\mu_1,\ldots,\mu_{n+1}) \in \mathbb{Z}^{n+1}$ with $0 \le \mu_j \le \frac{L}{q} - \lambda_j^0$ , $(1\le j\le n+1)$,

$$p_1(\mu_1,\ldots,\mu_{n+1}) = p(\lambda_1^0 + q\mu_1,\ldots,\lambda_{n+1}^0+q\mu_{n+1}) .$$

We deduce that for $|\tau| < T/q$ and $0\le h<qN$, $(h,q)=1$ , we have

$$\sum_{(\mu)} p_1(\mu)\Big(\prod_{i=1}^{n} (\lambda_i^0+\mu_i q+\lambda_{n+1}^0\beta_i+\mu_{n+1}q\beta_i)^{\tau_i}\Big)\, \alpha_1^{\mu_1 h} \ldots \alpha_{n+1}^{\mu_{n+1} h} = 0 .$$

We proceed to prove that this system of linear equations is equivalent to the system

$$\sum_{(\mu)} p_1(\mu)\Big(\prod_{i=1}^{n} (\mu_i + \mu_{n+1}\beta_i)^{\tau_i}\Big)\, \alpha_1^{\mu_1 h} \ldots \alpha_{n+1}^{\mu_{n+1} h} = 0$$

for the same values of $\tau$ and $h$ . It is easy to express each system as a linear combination of the other, but it is more elegant to introduce the two functions

$$\Phi_2(z_1,\ldots,z_n) = \sum_{(\mu)} p_1(\mu) \prod_{i=1}^{n} \alpha_i^{(\mu_i+\mu_{n+1}\beta_i)z_i}$$

and

$$\Phi_1(z_1,\ldots,z_n) = \Phi_2(z_1,\ldots,z_n) \cdot \prod_{i=1}^{n} \alpha_i^{(\lambda_i^0+\lambda_{n+1}^0\beta_i)z_i/q}$$

and to write the first (respectively the second) system:

$$\frac{\partial^{|\tau|}}{\partial z_1^{\tau_1}\ldots\partial z_n^{\tau_n}}\Phi_j(h,\ldots,h) = 0, \quad 0\le|\tau|<T\ ,\ 0\le h<H$$

with $j=1$ (resp. $j=2$). This amounts to say that $\Phi_1$ (resp. $\Phi_2$) has a zero at $(h,\ldots,h)$ of order at least $T$, and both conditions are plainly equivalent.

The new system involves parameters $\mu_1,\ldots,\mu_{n+1}$ with $0\le\mu_j\le L/q$, while the previous one $F_\tau(h/q) = 0$ involved $(\lambda_1,\ldots,\lambda_{n+1})$ with $0\le\lambda_j\le L$. By going further we reduce the number of parameters, and after a finite (but large) number of steps we get our contradiction that all the coefficients vanish.

c) The second step.

The precise inductive statement is the following. (The assumptions are stated above, at the end of a ).

Lemma 5.2.1 Let $S$ be a non-negative integer satisfying $q^S < T$. There exist rational integers

$$p_S(\lambda_1,\ldots,\lambda_{n+1})\ ,\quad 0\le\lambda_j\le L/q^S\ ,\ (1\le j\le n+1)$$ not all zero, bounded in absolute value by $\exp(N^{2n+4})$, such that

$$\sum_{(\lambda)} p_S(\lambda)\Big(\prod_{i=1}^{n}(\lambda_i+\lambda_{n+1}\beta_i)^{\tau_i}\Big)\prod_{j=1}^{n+1}\alpha_j^{\lambda_j h} = 0$$

for $|\tau| < T/q^S$ and $0 \le h < q^S N$ with $(h,q) = 1$.

Proof.

For $S = 0$ we choose $p_0(\lambda) = p(\lambda)$ and use step 1 of §4.3. Assume that the assertion in lemma 5.2.1 is correct for some integer $S$

with $1 \le q^S < T/q$ . We consider the functions

$$F_{S,\tau}(z) = \sum_{(\lambda)} p_S(\lambda) \Big( \prod_{i=1}^{n} (\lambda_i + \lambda_{n+1}\beta_i)^{\tau_i} \Big) \prod_{j=1}^{n+1} \alpha_j^{\lambda_j z} ,$$

where the sum is for $0 \le \lambda_j < L/q^S$ , $(1 \le j < n+1)$, and where $\tau = (\tau_1, \ldots, \tau_n)$ , $|\tau| < T/q^{S+1}$ . By our induction hypothesis, and by lemma 4.2.1, these functions satisfy

$$\frac{d^\sigma}{dz^\sigma} F_{S,\tau}(h) = 0 \qquad \text{for } 0 \le \sigma \le T/q^{S+1},\ 0 \le h < q^S N ,\ (h,q) = 1$$

We use the Schwarz lemma with $r = q^{S+1}N$, $R = Nr$ . From the upper bound

$$|F_{S,\tau}|_R \le (L+1)^{n+1} e^{N^{2n+4}} . L^T . c_3^L . c_4^{qLN^2} \le e^{N^{2n+5}}$$

(which is independent of $S$), we deduce

$$|F_{S,\tau}(\tfrac{h}{q})| < \exp(-\tfrac{1}{4}N^{2n+5} \log N) \quad \text{for } 0 \le h < q^{S+1}N$$

On the other hand $F_{S,\tau}(\frac{h}{q})$ is an algebraic number of degree at most $Dq^{n+1}$ , of denominator and height at most $\exp(N^{2n+5})$. From the size inequality 1.1.2 we deduce

$$F_{S,\tau}(\tfrac{h}{q}) = 0 \quad \text{for } |\tau| < T/q^{S+1} ,\ 0 \le h < q^{S+1}N.$$

We use only these equations for $(h,q) = 1$ . We express each number $F_{S,\tau}(\frac{h}{q})$ on the basis $\alpha_1^{\ell_1/q} \ldots . \alpha_{n+1}^{\ell_{n+1}/q}$ , $(1 \le \ell_j < q,\ 1 \le j \le n+1)$, as explained above, and the conclusion of the lemma follows from the previously given arguments.

d) The conclusion.

The conclusion of lemma 5.2.1 is untenable as soon as $q^S > L$ . We choose for instance

$$S = \left\lceil \frac{2n+3}{\log q} . \log N \right\rceil$$

then

$$L < q^S < T ,$$

and the desired contradiction follows.

## §5.3 Final descent.

It remains to show that there is no loss of generality, in the proof of Baker's theorem 4.1.1, to assume that there is a prime $q$ such that $\alpha_1^{1/q},\ldots,\alpha_{n+1}^{1/q}$ generate an extension of $K = \mathbf{Q}(\alpha_1,\ldots,\alpha_{n+1},\beta_1,\ldots,\beta_n)$ of degree $q^{n+1}$. In fact we can choose the prime number $q$ arbitrarily (e.g. $q = 2$).

Lemma 5.3.1. *Let $\mathbf{K}$ be a number field, and $\ell_1,\ldots,\ell_r$ be linearly independent complex numbers such that*

$$\alpha_j = e^{\ell_j} \in K , \quad (1\le j\le r);$$

*Then there exist complex numbers $\ell'_1,\ldots,\ell'_r$, which generate the same $\mathbf{Q}$-vector space as $\ell_1,\ldots,\ell_r$, such that*

$$\alpha'_j = e^{\ell'_j} \in K , \qquad (1\le j\le r) ,$$

*and such that for each prime $q$ for which the $q$-th roots of unity belong to $K$, we have*

$$[K((\alpha'_1)^{1/q},\ldots,(\alpha'_r)^{1/q}) : K] = q^r$$

*where*

$$(\alpha'_j)^{1/q} = e^{\ell'_j/q}, \qquad (1\le j\le r)$$

Proof.

Let $M$ be the $\mathbf{Z}$-module generated by $\ell_1,\ldots,\ell_r$, and let $M'$ be the set of $\ell \in \mathbf{C}$ such that $e^{\ell}\in K$ and $\ell,\ell_1,\ldots,\ell_r$ are linearly dependent. Since $M'$ is a finitely generated free $\mathbf{Z}$-

module, we can choose a basis $\ell'_1,\dots,\ell'_r$ .

Let $q$ be a prime such that $K$ contains the $q$-th roots of unity. We assume that the numbers $(\alpha'_j)^{1/q} = \exp(\ell'_j/q)$ , $(1\le j\le r)$ generate an extension of $K$ of degree less than $q^r$ , and we want a contradiction.

From Kummer's theory this assumption implies that there exist rational integers $a_1,\dots,a_r$ , with $a_j \ge 0$ , $1 \le \max a_j \le q-1$, and an element $\eta \in K^*$, such that

$$(\alpha'_1)^{a_1} \dots (\alpha'_r)^{a_r} = \eta^q$$

Let $\log \eta$ be any determination of the logarithm of $\eta$ . Taking the logarithm yields a rational integer $a_0$ such that

$$\sum_{j=1}^{r} a_j \ell'_j = q \log \eta + 2i\pi a_0 .$$

Let us define $\ell = \log \eta + 2i\pi \frac{a_0}{q}$ . Then $q\ell \in M'$, hence $\ell \in M'$, and therefore

$$\ell = b_1\ell'_1 + \dots + b_r\ell'_r ,$$

with $b_1,\dots,b_r \in \mathbb{Z}$ . From

$$\sum_{j=1}^{r} (a_j - b_j q)\, \ell'_j = 0$$

we deduce $a_j = b_j q$ , $(1\le j\le r)$, which is untenable with $1 \le \max_{1\le j\le r} a_j \le q-1$ .

This completes the proof of the lemma.

Remark. There is a classical method to construct $\ell'_1,\dots,\ell'_r$ : let $u$ be the index of $M$ in $M'$. For $1\le s\le r$ , let $k_{s,1},\dots,k_{s,s}$ be rational integers such that

$$\sum_{j=1}^{s} k_{s,j}\ell_j \in uM' ,$$

with $k_{s,s} > 0$ minimal $(1\le k_{s,s}\le u)$ and $0\le k_{s,j}\le u-1$ , $(1\le j\le s-1)$ .

We define $\ell'_1,\ldots,\ell'_r$ by

$$u\ell'_s = \sum_{j=1}^{s} k_{s,j}\ell_j \quad , \qquad (1\leq s\leq r) \quad .$$

## §5.4 Lower bounds for linear forms in logarithms

The method of §5.2 is the basis for the proofs of the sharpest known lower bounds for linear forms in logarithms. For the effective results it is important that in this method, the estimates in step 2 are always the same along the inductive argument.

The proofs of effective lower bounds involve some new technical complications which did not occur here. The most accessible place to become acquainted with them is the second part of Lang's "Elliptic Curves, Diophantine Analysis" (Springer Verlag 1978). The next one is "The theory of linear forms in logarithms" by Baker, Chapter 1 of "Trancendence Theory: Advances and Applications", ed. A. Baker and D. W. Masser (Academic Press 1977); (see also the chapter 2 by van der Poorten for the p-adic case.)

All the subject was initiated by Baker in 1966, and no fundamental progress in the method has been made since Baker's Sharpening III in 1973. It should be emphasized that the results are far from best possible. We do not mention general conjectures here (see Lang, op. cit.) but only two open problems whose solutions could lead to important consequences for the method.

If one uses the best known lower bounds for the linear form $|i\pi - i \log \frac{p}{q}|$, one deduces

$$|e^{\pi} - \frac{p}{q}| > q^{-2^{60}\log\log q}$$

for all rational numbers $p/q$ with $q \geq 3$. The unsolved problem is the existence of an absolute constant $c_1$ such that

$$|e^{\pi} - \frac{p}{q}| > q^{-c_1}$$

for all $p/q \in \mathbb{Q}$ with $q \geq 3$ .

If we consider now the inhomogeneous linear form $|m-\log p|$ with $m$ and $p$ positive integer, we obtain

$$|e^{m} - p| > p^{-c_2 \log \log p}$$

for all positive integers $m$ and $p$ (and $p \geq 3$) with $c_2 \leq 2^{42}$ . (In fact Mahler and Mignotte proved $c_2 \leq 17.7$ by quite different techniques.) It is not yet known whether there exists an absolute constant $c_3 > 0$ such that

$$|e^{m} - p| > p^{-c_3}$$

for all positive integers $m$ and $p$ .

# LECTURE 6

## LINEAR INDEPENDENCE OF ELLIPTIC LOGARITHMS

The elliptic statement analogous to Baker's theorem is not yet known in the general case, but it has been proved by Masser in 1974 for the case of complex multiplication. One of the main difficulties he had to solve concerned the last step: the result of Tijdeman on exponential polynomials (§4.4) has not yet been extended to elliptic polynomials. The proof of Masser used rather complicated arguments involving Wronskian determinants.

Already in 1972, in an unpublished manuscript, J. Coates had shown how Baker's theorem could be extended to elliptic curves with complex multiplication provided one had an appropriate theorem for the degree of the field of division of algebraic points. This appropriate Kummer's statement had been proved in fact by Bashmakov in 1970 and extended to abelian varieties of C.M. type by Ribet in 1975 . We follow here a joint paper of Coates and Lang, but as usual we prove only the transcendence result without giving a lower bound.

### §6.1 The results (qualitative form)

We recall the definition of an algebraic point of an elliptic function $\wp$ with algebraic $g_2$, $g_3$ : it is a point u which either is a pole of $\wp$ or satisfies $\wp(u) \in \bar{\mathbf{Q}}$.

Theorem 6.1.1. (Masser). *Let $\wp$ be a Weierstrass elliptic function with algebraic invariants $g_2$, $g_3$. Assume that $\wp$ has complex multiplication, and let k be the field of complex multiplication. Let $u_1,\dots,u_n$ be k-linearly independent algebraic points of $\wp$. Then the numbers $1, u_1,\dots,u_n$ are $\bar{\mathbf{Q}}$-linearly independent.*

An analogous result should hold when there is no complex multiplication.

Conjecture 6.1.2.(*) Let $\wp$ be a Weierstrass elliptic function with algebraic invariants $g_2$, $g_3$, and without complex multiplication. Let $u_1,\ldots,u_n$ be $\mathbb{Q}$-linearly independent algebraic points of $\wp$. Then the numbers $1, u_1,\ldots,u_n$ are $\bar{\mathbb{Q}}$-linearly independent.

Only two cases of the conjecture 6.1.2 are known (cf. 2.2.3 and 2.2.4), namely a) the case $n = 1$ and b) the homogeneous part (i.e. without 1) of the case $n = 2$. The inhomogeneous part of the case $n = 2$, i.e. the transcendency of $\beta_1 u_1 + \beta_2 u_2$ (when $\beta_1,\beta_2$ are algebraic numbers not both zero) is yet unsolved.

One can state similar conjectures for several $\wp$ functions, where $u_j$ is an algebraic point of $\wp_j$, $(1 \leq j \leq u)$. The assumption on the linear independence of the $u_j$ must be that the functions $\wp_j(u_j z)$ are algebraically independent. Even the case where $u_j$ is a pole of $\wp_j$ for all $j$ is unsolved for $n \geq 3$.

The hypothesis of complex multiplication is needed to make the extrapolation procedure succeed, because the Weierstrass functions have order 2, and one needs much more zeroes of the approximating auxiliary function. Let us mention two possibilities to avoid this difficulty when there is no complex multiplication. We first remark that the first steps of the induction work quite well, the problem being that one is not able to go sufficiently far to get the contradiction. The first suggestion is to use the method of §5.2 where the estimates were always the same along the inductive arguments.

(*) See the preface, and the paper of D. BERTRAND in the Proceedings of this Conference.

The trouble comes from the differential equation of $\wp$ , which is far more involved than in the exponential case, and which seems to prevent us to use an assumption like $[K(\wp(\frac{u_1}{2}),\dots\wp(\frac{u_n}{2})) : K] = 4^n$ . The second suggestion is to try to increase the order of derivatives in Baker's method. Such a result would have tremendous consequences.

## §6.2 The lemma of Baker-Coates-Anderson

The proof of theorem 6.1.1 will follow closely that of §4.3 and §5.1 , with the same estimates (mutatis mutandis). Before we perform this we need to solve some technical problems. Firstly our $\wp$-functions are no more entire, but have poles. However, if $\sigma$ is the Weierstrass sigma function corresponding to $\wp$ , then $\sigma^2$ is entire. Secondly the entire functions $\sigma$ and $\sigma^2\wp$ have order 2 , and this is why we need much more points. Since $\wp$ has complex multiplication, the ring of endomorphisms of the elliptic curve is (isomorphic to) an order $\mathcal{O} = \mathbb{Z} + \mathbb{Z}\eta$ in the imaginary quadratic field $k$ . For any positive integer $H$ , we denote by $\mathcal{O}(H)$ the set of $\gamma \in \mathcal{O}$ such that $|\gamma| \leq H$ . The number of such elements is asymptotic to $cH^2$ . If $u$ is an algebraic point of $\wp$ , then so is $\gamma u$ . Here comes the third difficulty, which is the main one, namely to estimate the house and denominator of $\wp(\gamma u)$ (when $\gamma u$ is not a pole), and more generally of

$$\frac{d^t}{dz^t}\wp^\lambda(z)\Big|_{z=\gamma u}$$

We first consider the differential equation

Lemma 6.2.1 Let $t \geq 0$, $\lambda \geq 1$ be integers. There exists a polynomial $P_{t,\lambda} \in \mathbb{Z}[X,X',T_2,T_3]$, of degree at most $\lambda + 2t$ in $X$, $1$ in $X'$, $t$ in $T_2$ and $t$ in $T_3$, such that

$$\frac{d^t}{dz^t} \wp^\lambda = P_{t,\lambda}(\wp, \wp', \frac{g_2}{2}, g_3)$$

Moreover the sum of the absolute values (length) $L(P_{t,\lambda})$ of the coefficients of $P_{t,\lambda}$ satisfies

$$L(P_{t,\lambda}) \leq 2^{4t}(\lambda+t)^t$$

The proof is easy by induction on $t$, starting from $\wp'^2 = 4\wp^3 - g_2\wp - g_3$. (Some authors prefer to express $\frac{d^t}{dz^t}\wp^\lambda$ as a polynomial in $\wp, \wp', \wp''$, without $g_2, g_3$, thanks to the differential equation $\wp''' = 12\wp\wp'$).

We now consider the multiplication formulae.

Lemma 6.2.2 Let $m$ be a positive integer. There exist two polynomials $A_m, B_m$ in $\mathbb{Z}[X,T_2,T_3]$ such that

$$\wp(mz) = \frac{A_m}{B_m}(\wp(z), \frac{g_2}{4}, g_3) \quad .$$

If we give to $X$, $T_2$, $T_3$ the weights 1, 2, 3 respectively, then $A_m$ is homogeneous of weight $m^2$, and $B_m$ is homogeneous of weight $m^2-1$. Each polynomial $A_m, B_m$ has a length at most $e^{m^2}$. Further the polynomials $A_m(X, \frac{g_2}{4}, g_3)$ and $B_m(X, \frac{g_2}{4}, g_3)$ are

relatively prime. Furthermore if $u \in \mathbb{C}$ is not a m-torsion point of $\wp$, i.e. if mu is not a pole of $\wp$, then $B_m(\wp(u), \frac{g_2}{4}, g_3) \neq 0$.

One gets a similar result with $m \in \mathbb{Z}$ replaced by $\gamma \in \mathcal{O}$ (and $m^2$ replaced by $|\gamma|^2$) by writing $\gamma = h_1 + h_2\tau$.

Now we come back to our number $\frac{d^t}{dz^t}\wp^\lambda(z)|_{z=\gamma u}$. It is plain that this number can be expressed as a rational function of $\wp(u), \wp'(u), g_2, g_3$, with coefficients in $\mathbb{Z}$. We need an upper bound for the degrees and heights of this rational function. For simplicity we look here only to the degree in $\wp(u)$. The natural way is to compute first $\frac{d^t}{dz^t}\wp^\lambda(z)$; from lemma 6.2.1 we get a polynomial of degree $\leq \lambda + 2t$ in $\wp(z)$. Now we replace $z$ by $\gamma u$; from lemma 6.2.2 one deduces that $\wp(\gamma u)$ is a rational function of degree $\leq |\gamma|^2$ in $\wp(u)$. Therefore our number $\frac{d^t}{dz^t}\wp^\lambda(z)|_{z=\gamma u}$ can be expressed as a rational function of degree at most $(\lambda+2t)|\gamma|^2$ in $\wp(u)$. However this is too much for our purpose.

Here comes the idea which is attributed to Baker and Coates and has been developed by Masser (Lecture Notes 437), Bertrand and others: we first compute $\wp^\lambda(\gamma z)$ in terms of $\wp(z)$, and then write

$$\frac{d^t}{dz^t}\wp^\lambda(z)\Big|_{z=\gamma u} = \gamma^{-t}\frac{d^t}{dz^t}\wp^\lambda(\gamma z)\Big|_{z=u}$$

Thus our number is expressed as a rational function of degree at most

$\lambda|\gamma|^2 + 2t$ in $\wp(u)$ . There is a corresponding improvement for the upper bound of the height. We give now a precise statement.

Using lemma 6.2.2, we write $\wp(\gamma z) = \frac{A_\gamma}{B_\gamma}(\wp(z))$ where $A_\gamma$ and $B_\gamma$ have coefficients in $\mathcal{O}[\frac{g_2}{4}, g_3]$ .

Lemma 6.2.3 There exists a positive number $c_1$ depending only on $\wp$ , with the following property. Let $u_1,\ldots,u_n$ be non-zero complex numbers, $\beta_1,\ldots,\beta_n$ complex numbers which are not all zero, and $P \in \mathbf{Z}[X_1,\ldots,X_{n+1}]$ a non-zero polynomial of degree $\leq L_j$ in $X_j$ , $(1 \leq j \leq n+1)$ . We define

$$\phi(z_1,\ldots,z_n) = P(\wp(u_1z_1),\ldots,\wp(u_nz_n),\wp(\beta_1u_1z_1+\ldots+\beta_nu_nz_n)) ,$$

and, for $\gamma \in \mathcal{O}$ ,

$$\Psi_\gamma(z_1,\ldots,z_n) = \Big(\prod_{j=1}^{n} B_\gamma(\wp(u_jz_j))\Big) B_\gamma(\wp(\beta_1u_1z_1+\ldots+\beta_nu_nz_n))$$

$$\phi(\gamma z_1,\ldots,\gamma z_n) .$$

Then for each $(t_1,\ldots,t_n) \in \mathbf{N}^n$ , the function

$$\prod_{j=1}^{n}\left(\frac{1}{u_j}\frac{\partial}{\partial z_j}\right)^{t_j} \psi_\gamma(z_1,\ldots,z_n)$$

is a polynomial in $\wp(u_jz_j)$ (of degree $\leq |\gamma|^2L_j + 2t$) , in $\wp'(u_jz_j)$ (of degree $\leq 1$), in $\beta_j$ (of degree $\leq t$), and in $g_2/4$ and $g_3$

(of degree $\leq (L_1+\ldots+L_n)|\gamma|^2 + t$), with coefficients in $\mathcal{O}$ of absolute value at most

$$H(P)|t|^{|t|} \exp(c_1|\gamma|^2(L_1+\ldots+L_{n+1}) + c_1|t|)$$

where $|t| = t_1+\ldots t_n$

Remark A further trick, due to M. Anderson, is to write

$$\frac{d^t}{dz^t}\wp^\lambda(z)\Big|_{z=\gamma u} = \frac{d^t}{dz^t}\wp^\lambda(z+\gamma u)\Big|_{z=0} ,$$

which yields a rational function of degree $\leq \lambda|\gamma|^2$ in $\wp(u)$. This argument is not necessary for us, but is useful to get a good dependence in terms of $u_j$ for linear forms in elliptic logarithms, and also for proofs of algebraic independence (Choodnovsky).

## §6.3 The main lemma

Let $\wp$ be an elliptic functions with algebraic $g_2$, $g_3$, and complex multiplication in $k$. Let us assume

$$u_{n+1} = \beta_1 u_1+\ldots+\beta_n u_n ,$$

where $\beta_1,\ldots,\beta_n$ are algebraic numbers, $u_1$ is a period of $\wp$, $u_1,\ldots,u_{n+1}$ are $k$-linearly independent and $\wp(u_j)$ are algebraic for $2 \leq j \leq n+1$. We shall eventually derive a contradiction. The aim of this section is to prove the following result

Lemma 6.3.1. There exists an integer $L_0$, depending only on $\wp$, $u_1,\dots,u_{n+1}$, $\beta_1,\dots,\beta_n$, with the following property. For each integer $L \geq L_0$ there exists a prime $q > (2L)^{1/2}$ and a non-zero polynomial $P \in \mathbb{Z}[X_1,\dots,X_{n+1}]$, of degree at most $L$ in $X_j$, $(1 \leq j \leq n+1)$, such that the function

$$F(z) = P(\wp(u_1 z),\dots,\wp(u_{n+1} z))$$

satisfies

$$F(\tfrac{1}{q}) = 0 .$$

The proof of lemma 6.3.1 follows closely (*) the proof of §4.3. We choose a sufficiently large integer L, and we define a real number N by

$$L = N^{2n+2}$$

Further let $T = N^{2n+4}$ and $H = N^{1/2}$. The constants $c_2,\dots,c_{12}$ are easily computable in terms of $\wp$, $u_1,\dots,u_{n+1}$, $\beta_1,\dots,\beta_n$, and do not depend on L, N, T, H. A convenient way to avoid some problems connected with the poles is to use the following result: for each $H_1 \geq H$ there exists a subset $\mathcal{O}'(H_1)$ of $\mathcal{O}(H_1)$, with

$$\operatorname{card} \mathcal{O}'(H_1) \geq c_2 H_1^2 ,$$

---

(*) One could reinforce the similarity by working with a meromorphic function g of order 1 with $g(z^2) = \wp(z)$.

such that for $\gamma \in \mathcal{O}'(H_1)$ and $1 \leq j \leq n+1$

$$\overline{|\wp(\gamma u_j)|} \leq c_3 \ , \quad \overline{|\wp'(\gamma u_j)|} \leq c_3 \ , \quad |\sigma(\gamma u_j)| \geq c_3$$

(The idea of the proof is as follows. Let $K$ be a number field containing $g_2$, $g_3$, $\wp(u_j)$, $\wp'(u_j)$ (and also $\beta_1,\ldots,\beta_n$). For each embedding $\sigma : K \longrightarrow \mathbb{C}$ one considers the elliptic function $\wp^\sigma$ of invariants $g_2^\sigma$, $g_3^\sigma$, one considers a small disc in $\mathbb{C}$ far from the poles of $\wp^\sigma$, and one proceeds by induction using Dirichlet box principle).

First step. There exists a non-zero polynomial $P \in \mathbb{Z}[X_1,\ldots,X_{n+1}]$ of degree at most $L$ in $X_j$, $(1 \leq j \leq n+1)$, and height at most $\exp(N^{2n+4})$, such that the function

$$\phi(z_1,\ldots,z_n) = P(\wp(u_1 z_1),\ldots,\wp(u_n z_n), \wp(\beta_1 u_1 z_1+\ldots+\beta_n u_n z_n))$$

satisfies

$$F_\tau(\gamma) = 0 \quad \text{for} \quad |\tau|<T \quad \text{and} \quad \gamma \in \mathcal{O}'(H)$$

where

$$F_\tau(z) = \prod_{j=1}^{n} \left(\frac{\partial}{u_j \partial z_j}\right)^{\tau_j} \phi(z,\ldots,z) \ .$$

Proof: Using lemma 6.2.3, we consider the system of linear homogeneous equations

$$\prod_{j=1}^{n} \left(\frac{1}{u_j} \frac{\partial}{\partial z_j}\right)^{\tau_j} \psi_\gamma(1,\ldots,1) = 0 ,$$

of at most $c_4 T^n H^2$ equations with $(L+1)^{n+1}$ unknowns. From the estimates of lemma 6.2.3 and the inequality

$$T \log T + LH^2 \leq 2 N^{2n+4} \log N$$

we get the desired result.

Second step: induction. Let S be a positive integer which does not depend on N (we shall choose $S = 2(n+1)^2$). For any non-negative integer $s \leq S$, we have

$$F_\tau(\gamma) = 0 \quad \text{for} \quad |\tau| < 2^{-s}T , \ \gamma \in \Gamma'(H^{s+1})$$

The case $s = 0$ is our first step. We assume that the result holds for some integer $s-1$, $1 \leq s \leq S$. We choose $|\tau| < 2^{-s}T$, and we introduce the entire function of one variable

$$G_\tau(z) = F_\tau(z) \prod_{j=1}^{n+1} \sigma(u_j z)^{2L}$$

We choose $r = H^{s+1}$, $R = H^{s+2}$. It is readily verified that

$$\log |G_\tau|_R \leq c_5 (N^{2n+4} + T \log N + LR^2)$$

$$\leq c_6 N^{2n+s+4}$$

(the functions $\sigma$ and $\sigma^2 p$ are entire of order $\leq 2$) .
By induction hypothesis $G_\tau$ has at least $2^{-s-1}c_2 TN^s$ zeroes in $|z| \leq r$ ; from Schwarz lemma 1.3.1 one gets

$$\log |G_\tau|_r \leq - c_7 N^{2n+s+4} \log N .$$

Now let $\gamma \in \vartheta'(H^{s+1})$. From the definition of $\vartheta'(H_1)$ we get

$$\log |F_\tau(\gamma)| \leq - c_8 N^{2n+s+4} \log N$$

We fix $\gamma$ , and we choose $\tau$ with the smallest $|\tau|$ for which $F_\tau(\gamma) \neq 0$ . We assume $|\tau| < 2^{-s}T$ . From lemma 6.2.3 and the size inequality 1.1.2 we conclude

$$\log |F_\tau(\gamma)| \geq - c_9 N^{2n+s+4}$$

This contradiction completes the proof of step 2.

Step 3 Proof of lemma 6.3.1

We follow the proof of §5.1 . The function $F(z) = \phi(z,\ldots,z)$ satisfies

$$\frac{d^t}{dz^t} F(\gamma) = 0 \quad \text{for} \quad 0 \leq t < 2^{-S}T , \quad \gamma \in \vartheta'(H^{S+1})$$

Let $q$ be a prime number with $(2L)^{1/2} < q \leq 3L^{1/2}$ . From Schwarz lemma 1.3.1 with

$$r = H^{2n^2+4n+3} , \quad R = Hr , \quad \nu_F(0,r) \geq c_{10} N^{2n^2+6n+10}$$

we get

$$|F(\tfrac{1}{q})| < \exp(-N^{2n^2+6n+6})$$

On the other hand $F(\frac{1}{q})$ is an algebraic number of degree at most $c_{11}q^{2n+2}$ and house and denominator at most $\exp(c_{12}N^{2n+4})$. From the size inequality we conclude $F(\frac{1}{q}) = 0$, as claimed.

## §6.4 Bashmakov's theorem

In order to complete the proof of theorem 6.1.1 one needs a result like lemma 5.1.1, where exp is replaced by $\wp$. For this we use a result of Bashmakov, which gives for elliptic curves the analogue of Kummer's theory for the multiplicative group.

We have assumed that $u_1$ is a period of $\wp$. A classical result of class field theory (Hasse, Deuring) implies that for $q$ sufficiently large,

$$[K(\wp(\tfrac{u_1}{q}), \wp'(\tfrac{u_1}{q})) : K] = \begin{cases} q^2-1 & \text{if } q \text{ is prime in } k \\ (q-1)^2 & \text{if } q \text{ is decomposed in } k. \end{cases}$$

For $1 \leq s \leq n$, let $K_s$ be the field generated over $K$ by $\wp(\frac{u_j}{q})$, $\wp'(\frac{u_j}{q})$, $(1 \leq j \leq s)$. Let $E_q$ be the kernel of the multiplication by $\ell$ on the elliptic curve associated with $\wp$; thus $K(E_q) = K_1$, and $E_q \simeq \frac{\mathbb{Z}}{q\mathbb{Z}} \times \frac{\mathbb{Z}}{q\mathbb{Z}}$. We have an injective homomorphism

$$\mathrm{Gal}\,(K_n/K_1) \longrightarrow E_q^{n-1}$$

which sends $\sigma$ to $(\sigma Q_2 - Q_2, \ldots, \sigma Q_n - Q_n)$, where $Q_j$ is any point on the curve such that $qQ_j = P_j$, with $P_j$ corresponding to $\wp(u_j)$. Bashmakov's result is that this map is surjective as soon as $q$ is

sufficiently large. As a consequence

$$[K_s : K_{s-1}] = q^2 , \qquad 2 \leq s \leq n ,$$

and this completes the proof of theorem 6.1.1.

## §6.5 Further results and comments

In 1963, Lang described a new method for the study of integral points on an elliptic curve, based on a conjectural lower bound for linear forms in elliptic logarithms (i.e. in algebraic points of a $\wp$-function). A similar treatment in the multiplicative case had been done already by Gel'fond (see lecture 4). In 1970, Coates derived a non-effective lower bound from the Thue-Siegel-Roth theorem. Until now an effective result is known only in the case of complex multiplication. The first result was due to Masser, then it has been improved, mainly by Coates and Lang, using the method we just described. The best known result to date is due to M. Anderson (unless we take for granted some claims of Choodnovsky). Two good references are Anderson's Chapter 7 of the book edited by Baker and Masser, and Chapter 9 of Lang's book "Elliptic curves,diophantine analysis".

For the application to diophantine equations, Lang's approach needs a basis for the group of Mordell-Weil. One way of getting such a basis is to assume the conjecture of Birch and Swinnerton-Dyer. The details have been worked out by H. Groscot. G.V. Choodnovsky announces better results assuming moreover the generalized Riemann Hypothesis.

The p-adic case has been solved by D. Bertrand who proved also an effective lower bound and derived remarkable consequences on the denominators of rational points on elliptic curves.

These results have been extended to abelian varieties of C.M. type (Masser, Lang, Coates and Lang, Masser again for the complex case, Bertrand and Flicker for the p-adic case). The theorem of $\text{Bash}_{\text{makov}}$ (Kummer's theory for elliptic curves) and Ribet (for abelian varieties of C.M. type) has been extended by Bertrand to the product of an elliptic curve by the multiplicative group, by Ribet to non trivial extensions of an elliptic curve by the multiplicative group, and by Ribet to a very wide class of commutative algebraic groups.

# LECTURE 7

## TRANSCENDENCE AND LINEAR INDEPENDENCE OF PERIODS

In the present lecture we study the transcendence and the linear independence over $\overline{\mathbb{Q}}$ of periods of integrals, mainly of elliptic integrals. We begin with an historical survey of this question, then we give some details about the more recent results (which concern elliptic integrals of the third kind) and finally we mention some further results and problems.

### §7.1 Historical survey.

Lindemann's theorem (1882) asserts the transcendency of the number $2\pi i$, which is a period of the usual exponential function. Now let $\wp$ be an elliptic function of Weierstrass satisfying a differential equation $\wp'^2 = 4\wp^3 - g_2\wp - g_3$ with algebraic $g_2, g_3$. The problem of the transcendency of the periods of $\wp$ was first studied by Siegel (1932) who proved that if $(\omega_1, \omega_2)$ is a basis of the period lattice $L$, then at least one of the two numbers $\omega_1, \omega_2$ is transcendental. Therefore in the case of complex multiplication each non-vanishing period of $\wp$ is transcendental. Further partial results were obtained by Schneider (1934) and Popken and Mahler (1935), and in 1936 Th. Schneider published the most important work on the subject; from 3 general theorems he deduced a lot of consequences, and in particular got the transcendence of periods of elliptic integrals of the first and second kind. His results involve

the zeta function of Weierstrass, which is connected to $\wp$ by $\zeta' = -\wp$ (and $\zeta$ is odd) and is quasi-periodic with respect to the lattice $L$:

$$\zeta(z+\omega) = \zeta(z) + \eta \qquad \text{for } \omega \in L ,$$

where $\eta = m_1\eta_1 + m_2\eta_2$ if $\omega = m_1\omega_1 + m_2\omega_2$, and

$$\eta_1 = 2\zeta(\frac{\omega_1}{2}) , \quad \eta_2 = 2\zeta(\frac{\omega_2}{2}) .$$

The three main theorems of Schneider are the following.

1. If a,b are algebraic numbers not both zero, and u a complex number with $u \notin L$, then one at least of the two numbers $\wp(u)$, $au + b\zeta(u)$ is transcendental.

2. If $\wp, \wp^*$ are two algebraically independent elliptic functions with algebraic invariants, and u a complex number with $u \notin L$, $u \notin L^*$, then one at least of the two numbers $\wp(u), \wp^*(u)$ is transcendental.

3. If u is a complex number, $u \notin L$, then one at least of the two numbers $e^u, \wp(u)$ is transcendental.

It is easy to deduce these results from Schneider-Lang's criterion 2.2.1, and then to deduce corollaries 2.2.3 and 2.2.4 from the first and second result above.

We give here the consequences on the periods and pseudo- periods. Let $\omega$ be a non-zero period of $\wp$, and $\eta$ the corresponding pseudo-period of $\zeta$. From the first result of Schneider one deduces:

Theorem 7.1.1(Schneider) The three numbers $1,\omega,\eta$ are linearly independent over $\overline{\mathbb{Q}}$.

(Proof: assume $a\omega + b\eta = c$; let $h$ be the smallest positive integer such that $\frac{\omega}{2^h} \notin L$; choose $u = \frac{\omega}{2^h}$; then $\zeta(u) = \frac{\eta}{2^h}$ ).

Therefore each of the numbers $\omega$, $\eta$, $\eta/\omega$, $\eta+\omega$ is transcendental.

It is well known that a period of an elliptic integral of the first or second kind which is defined over $\overline{\mathbf{Q}}$ is a linear combination of $\omega$, $\eta$, with algebraic coefficients. Therefore we deduce from 7.1.1:

Corollary 7.1.2. The non-vanishing periods of an elliptic integral of the first or second kind over $\overline{\mathbf{Q}}$ are transcendental.

From the second result of Schneider one deduces that the quotient of two non-zero periods of elliptic integrals of the first kind is either rational, or imaginary quadratic, or else transcendental.

Finally from the third result of Schneider one obtains

Theorem 7.1.3.(Schneider) If $\omega$ is a non zero period of $\wp$ and $\beta$ a non-zero algebraic number, then $e^{\beta\omega}$ is transcendental.

(It is sufficient to prove this with $\beta=1$, since $\beta\omega$ is a period of the Weierstrass elliptic function $\beta^{-2}\wp(\beta^{-1}z)$). Therefore the number $\omega/\pi$ is transcendental.

After Schneider's fundamental paper of 1936, the next step was provided by Baker in 1968. Using his method (see lecture 4) he proved the transcendency of non-vanishing linear forms in $\omega_1$, $\omega_2$, with algebraic coefficients. In 1969 he extended this result to linear forms in $\omega_1$, $\omega_2$, $\eta_1$, $\eta_2$ ,and then Coates (1970) added $2\pi i$. Then Coates (1971) showed that $1$, $\omega_1$, $\omega_2$, $2i\pi$ are $\overline{\mathbf{Q}}$-linearly independent when there is no complex multiplication. Finally, the

problem of the linear independence of $1, \omega_1, \omega_2, \eta_1, \eta_2, 2i\pi$ has been completely solved by D. W. Masser in his thesis (Lecture Notes 437, 1975).

Theorem 7.1.4.(Masser)1) When $\mathcal{P}$ has no complex multiplication, the six numbers $1, \omega_1, \omega_2, \eta_1, \eta_2, 2i\pi$ are $\overline{\mathbf{Q}}$-linearly independent.

2) When $\mathcal{P}$ has complex multiplication, the six numbers $1, \omega_1, \omega_2, \eta_1, \eta_2, 2i\pi$ span over $\overline{\mathbf{Q}}$ a vector space of dimension 4 .

In the case of complex multiplication, there is a linear relation between the six numbers, which is independent of the obvious one $\omega_2 - \tau\omega_1 = 0$ with $\tau \in \overline{\mathbf{Q}}$. This extra relation

$$\frac{1}{\omega_2}(\eta_2 - \bar{\tau}\eta_1) \quad \in \mathbf{Q}(g_2, g_3, \tau)$$

seems to be classical (Eisenstein) but was not widely known. It has been rediscovered by Masser, and Brownawell and Kubota.

There are further results on periods of several elliptic functions, but we postpone them to §7.3. For one elliptic curve over $\overline{\mathbf{Q}}$ the problem of transcendence and linear independence of periods of integrals of the first and second kind is completely solved by Masser's theorem 7.1.4. Until recently no result was known on integrals of the third kind. (Schneider's third problem.) The periods of such integrals are of the form

$$\sum_{j=1}^{k} c_j(\omega\, \zeta(u_j) - \eta\, u_j) + a\omega + b\eta$$

where $c_1, \ldots, c_k$ are the residues at the points distinct from the origin (one gets an integral of the first or second kind by subtracting

$$\frac{1}{2} \sum_{j=1}^{k} c_j \frac{y+y_j}{x-x_j} \frac{dx}{y}$$

where $(x_j,y_j)$ are the points distinct from the origin where the differential form has non-zero residue). The numbers $c_1,\ldots,c_k$ are algebraic, (the integral being defined over $\bar{\mathbf{Q}}$), but we need to assume that they are rational. Multiplying by a common denominator we can assume that they are rational integers. Finally, using the addition theorem of the zeta function, one reduces the problem to the transcendency of the number

$$\omega\zeta(u) - \eta u + a\omega + b\eta ,$$

where $u$ is a complex number which is not a torsion point (i.e. $u \notin \mathbf{Q}.L$), and $a,b,\wp(u)$ are algebraic.

In §7.2 we shall prove the transcendency of the number

$$\exp\{\omega\zeta(u) - \eta u + a\omega\}$$

as a consequence of Schneider-Lang's criterion 2.2.1. This shows that if the differential form has no poles of order $\geq 2$, then the exponential of a period is either a root of unity (which occurs only in trivial circumstances) or a transcendental number. It should be noted that the transcendency of $\zeta(u) - \frac{\eta}{\omega} u$ (which is obviously a special case) had been obtained already by Choodnovsky a few years ago, as a consequence of a result of algebraic independence (see lecture 8).

The transcendency of the period itself has been obtained very recently by M. Laurent. Let $\omega$ be a non zero period of $\wp$ and $u$ an algebraic point of $\wp$ which is not a torsion point.

Theorem 7.1.5(M. Laurent). 1. The four numbers

$$1, \omega, \eta, \eta u - \omega\zeta(u)$$

are linearly independent over $\bar{\mathbf{Q}}$.

2. In the case of complex multiplication, the five numbers,

$$1,\ \omega,\ \eta,\ \eta u - \omega\zeta(u),\ 2i\pi$$

are linearly independent over $\overline{\mathbf{Q}}$ .

In §7.2 we give a sketch of the proof of the first part of Laurent's theorem.

## §7.2 Elliptic integrals of the third kind.

Through this section we denote by $\wp$ an elliptic function of Weierstrass with invariants $g_2$, $g_3$ in $\overline{\mathbf{Q}}$ and of period lattice $L$ , by $\zeta$ the associated zeta function, by $\omega$ a non-zero period of $\wp$ with $\frac{\omega}{2} \notin L$, by $\eta$ the associated pseudo-period of $\zeta$ , and by $u$ an algebraic point of $\wp$ which is not a torsion point. Finally let $\beta$ be any algebraic number.

We first prove the following result.

Theorem 7.2.1. The number $\exp\{\omega\zeta(u) - \eta u + \beta\omega\}$ is transcendental.

As already mentioned, a consequence is the transcendency of $\zeta(u) - \frac{\eta}{\omega} u$ .

Proof of the theorem 7.2.1.

The main tool is Schneider-Lang criterion 2.2.1; we need a suitable function associated with our number (which we assume to be algebraic) satisfying a differential equation and a theorem of addition. Such a function was provided to me by J.-P. Serre, in connection with the parametrization of the exponential map of the extension of an elliptic curve by the multiplicative group. (See

Astérisque no.71, 1980).

We define

$$f(u,z) = \frac{\sigma(z-u)}{\sigma(z)\sigma(u)}\, e^{z\zeta(u)}$$

and our first function in the criterion 2.2.1 is

$$f_1(z) = f(u,z)e^{\beta z}$$

We recall the definition of the sigma function of Weierstrass:

$$\sigma(z) = z \prod_{\substack{\lambda\in L \\ \lambda\neq 0}} (1 - \frac{z}{\lambda}) \exp\,(\frac{z}{\lambda} + \frac{z^2}{2\lambda^2})$$

and the properties

$$\sigma(z+\omega_j) = -\sigma(z)\exp\{\eta_j(z+\frac{\omega_j}{2})\}\ ,\ (j=1,2),$$

$$\sigma'/\sigma = \zeta$$

and $$\sigma(mz) = (-1)^{m-1}\sigma(z)^{m^2}\,\psi_m(\wp(z),\wp'(z))\ ,\ (m\in\mathbf{Z},\ m>0)$$

where $\psi_m$ is a rational function with coefficients in $\mathbf{Q}(g_2,g_3)$, and

$$B_m(\wp(z)) = [\psi_m(\wp(z),\wp'(z))]^2$$

is the polynomial in $\wp(z)$, $g_2,g_3$ of lemma 6.2.2.

An easy (and useful) consequence of the multiplication formula for $\sigma$ is the fact that the numbers

$$\sigma(\frac{\omega}{2})\, e^{-\eta\omega/8}\ ,\ \frac{\sigma(\frac{\omega}{2}-u)}{\sigma(u)}\exp\{\eta(\frac{u}{2}-\frac{\omega}{8})\}$$

are algebraic. Therefore $f_1(\frac{\omega}{2})$ is algebraic. Moreover from the quasi-periodicity of $f_1$:

$$f_1(z+\omega_j) = f_1(z)\exp\{\omega_j\zeta(u) - \eta_j(u) + \beta\omega_j\}\ ,\ (j=1,2),$$

one deduces that all the numbers $f_1(\frac{\omega}{2}+h\omega)$, $h\in\mathbf{Z}$ are algebraic.

Further $f_1$ satisfies a differential equation:

$$\frac{f_1'}{f_1}(z) = \zeta(z-u) - \zeta(z) + \zeta(u) + \beta$$

$$= \beta + \frac{1}{2}\,\frac{\wp'(z)+\wp'(u)}{\wp(z)-\wp(u)}$$

It is now easy to use the criterion 2.2.1. Let $K$ be the field generated over $\mathbb{Q}$ by $g_2$, $g_3$, $\wp(u)$, $\wp'(u)$, $\beta$, $f_1(\frac{\omega}{2})$ and $\exp\{\omega\zeta(u) - \eta u + \beta\omega\}$. Let $f_2(z) = \wp(z)$, $f_3(z) = \wp'(z)$, $f_4(z) = \frac{1}{\wp(z) - \wp(u)}$. The set of $w = (h+\frac{1}{2})\omega$, $h \in \mathbb{Z}$ is infinite, these $w$ are not poles of $f_1$, $f_2$, $f_3$, $f_4$ (since $u$ is not a torsion point), and $f_j(w) \in K$ for $1 \leq j \leq 4$. From the criterion we deduce that $f_1(z)$ is algebraically dependent from $\wp(z)$; therefore $f_1$ is an elliptic function associated with a lattice $L_1$ such that $\mathbb{Q}L_1 = \mathbb{Q}L$. From the quasi-periodicity of $f_1$ one deduces

$$\omega_j\zeta(u) - \eta_j u + \beta\omega_j \in 2i\pi\mathbb{Q}, \quad (j=1,2).$$

From Legendre's relation

$$\omega_2\eta_1 - \eta_2\omega_1 = 2i\pi$$

we get the contradiction that $u \in \mathbb{Q}L$, i.e. that $u$ is a torsion point. Theorem 7.2.1 follows.

Now we give a sketch of the proof of the following theorem of Laurent.

Theorem 7.2.2. (Laurent) Let $\xi$ be an elliptic differential form which is defined over $\bar{\mathbb{Q}}$. We assume that all the residues of $\xi$ are rational numbers. Then the non-vanishing periods of $\xi$ are transcendental.

As already shown previously, it is sufficient to prove that a relation

$$1 = a\omega + b\eta + c\,\lambda(u,\omega)$$

with algebraic $a,b,c$ and $\lambda(u,\omega) = \omega\zeta(u) - \eta u$ is impossible.

We introduce two meromorphic functions of two complex variables

$$F(z_1, z_2) = f(u,z_1)\, e^{z_2} = \frac{\sigma(z_1-u)}{\sigma(z_1)\sigma(u)}\, e^{z_1\zeta(u)+z_2}$$

and

$$G(z_1,z_2) = az_1 + b\zeta(z_1) - cz_2 \ .$$

Further define $\Omega = (\omega, -\lambda(u,\omega)) \in \mathbb{C}^2$ . It is readily verified that

$$G(\Omega z) = b\zeta(\omega z) - b\eta z + z \ , \quad F(\Omega z) = \frac{\sigma(\omega z-u)}{\sigma(\omega z)\sigma(\frac{\omega}{2})}\, e^{\eta u z} \ ,$$

and consequently $G(\frac{1}{2}\Omega) = \frac{1}{2}$ and $F(\frac{1}{2}\Omega)$ are algebraic. We choose as usual a large integer $N$ (the number $c_1$ will not depend on $N$ ) and we define

$$H = N^2 \ , \ T = N^{15} \ , \ L = N^{11} \ .$$

First step. There exists a non-zero polynomial $P \in \mathbb{Z}[X_0,X_1,X_2]$ of degree at most $L$ in $X_0$, $X_1$, $X_2$, and height at most $\exp(c_1 N^{15} \log N)$ , such that the function

$$\Phi(z_1,z_2) = P(G(z_1,z_2) \ , \wp(z_1), F(z_1,z_2))$$ has a zero of order $\geq T$ at each point

$$(h+\tfrac{1}{2})\Omega = ((h+\tfrac{1}{2})\omega \ , \ -(h+\tfrac{1}{2})\lambda(u,\omega)), \qquad 1 \leq h \leq H \ .$$

For the proof one needs to write $f(u, mz)/ f(u,z)^m$ as a rational function of $\wp(z)$, $\wp'(z)$, $\wp(u)$, $\wp'(u)$, to give upper bounds for the degree and coefficients of this rational function, and also to check that the denominator does not vanish. (These estimates are due to E. Reyssat who obtained a transcendence measure for the number of theorem 7.2.1).

Second step. (Induction). Let $J$ be an integer, $0 \leq J \leq 300$. Then $\Phi$ has a zero at each point $(h+\frac{p}{q})\Omega$ with

$$1 \leq h \leq N^{2+J/2}, \ 1 \leq p < q \leq 2\, N^{J/4} \ , \ q \text{ even, of order at least } T/2^J \ .$$

The proof is by induction on $J$. One needs upper bounds for the degrees and heights of the division equations of $f(u,z)$. It should be noted that Ribet's recent work on Kummer's theory for the extension of an elliptic curve by the multiplicative group (cf.§6.5) gives the exact degree.

Third step. Upper bound for the number of zeros of $\phi(z\Omega)$.

At the end of the second step the function of one variable

$$\phi(z\Omega) = P(G(\Omega z), \wp(\omega z), F(\Omega z))$$

has a zero of order $\geq 2^{-300}T$ at each point $p/q$ with $1 \leq p \leq q \leq 2T^{75}$ and $q$ even. The desired contradiction follows from the next proposition.

Proposition 7.2.3 (Laurent). Let $P \in \mathbf{C}[X_0, X_1, X_2, X_3]$ be a non-zero polynomial of degree $\leq L$. Define

$$g(z) = b(\zeta(\omega z) - \eta z) + z ,$$

and

$$f_*(z) = f(u,z) \exp(-\lambda(u,\omega) \frac{z}{\omega})$$

$$= \frac{\sigma(z-u)}{\sigma(z)\sigma(u)} \exp (\frac{\eta u}{\omega} z) .$$

Then the number $\nu_\varphi(0,R)$ of zeros in $|z| \leq R$ of the function

$$\varphi(z) = P(g(z), \wp(\omega z), f_*(\omega z), e^{2i\pi z})$$

satisfies for all $R > 0$

$$\nu_\varphi(0,R) \leq c\,(LR^2 + L^8)$$

where $c$ depends only on $\wp$, $u$, $\omega$, $b$.

(The introduction of $e^{2i\pi z}$ is useful for the second part of theorem 7.1.5 only.)

This proposition is of course an important part of the proof

of theorems 7.1.5 and 7.2.2. The arguments which are used go back to Masser's thesis; we shall indicate them in the next lecture, in an easier case.

## §7.3 Further results and comments.

Some of the results of §7.1 have beed extended to the case where $\omega_1$ is a period of $\wp_1$ and $\omega_2$ is a period of another function $\wp_2$. The best reference to date is Chapter 6 of "Transcendence Theory : Advances and Applications" (ed. A. Baker and D. W. Masser). In this chapter Masser proves

$$\dim \{1, \omega_1,\omega_2,\eta_1,\eta_2,2i\pi\} = 1 + \dim \{\omega_1,\omega_2,\eta_1,\eta_2,2i\pi\}$$

and

$$\dim \{\omega_1, \omega_2, \eta_1, \eta_2\} = 2 \dim \{\omega_1,\omega_2\} ,$$

where dim is the dimension of the vector space spanned over $\bar{\mathbf{Q}}$ by the considered numbers. An important open problem is to investigate the linear independence over $\bar{\mathbf{Q}}$ of 3 periods $\omega_1, \omega_2, \omega_3$ of three Weierstrass functions $\wp_1, \wp_2, \wp_3$. More generally one would like to know the dimension of the vector space spanned over $\bar{\mathbf{Q}}$ by numbers

$$1, \omega_1, \eta_1, \ldots,\omega_k, \eta_k, 2i\pi ,$$

where $\omega_j$ is a period of an elliptic function $\wp_j$ and $\eta_j$ is the corresponding quasi-period of $\zeta_j$, $(1\leq j\leq k)$.

Another problem connected with §7.2 is to remove the assumption that the residues are rational (this assumption comes in fact from the correspondence between extensions of an elliptic curve by the multiplicative group and differentials of the third kind with integral residues). As already seen this amounts to the problem of the linear independence (over $\bar{\mathbf{Q}}$) of numbers

$$\omega\ \zeta(u_j) - \eta u_j\ ,\ \omega,\ \eta, \qquad (1 \leq j \leq k).$$

There are rather few results on abelian integrals of genus $\geq 2$ (Schneider's fourth problem.) The most significant result is due to Schneider (1940) which improves an earlier result of Siegel (1932) and implies the transcendency of $B(a,b)$ for rational $a,b$ with $a,b,a+b$ not integers. (The only recent progress is due to D. W. Masser and concern curves of genus 2.) A transcendence measure for $B(a,b)$ has been derived by Laurent. It is usually far more difficult to give a transcendence measure than to prove the transcendence of the considered number. In the exponential case most of the work is due to N. I. Feldman. In the elliptic case a similar achievement has just been done by E. Reyssat. His results are extremely sharp and provide a lot of numbers with finite transcendence type. In his book on transcendental numbers (1966) Lang mentioned "the problem of proving that certain numbers have definite types" and said that "to solve this problem, one expects a higher order of complication, of the nature encountered by Feldman in his papers". The most difficult problem **is connected with the elliptic analog of Tijdeman's result. The main contribution to this subject is due to D.W. Masser, whose methods enabled him and Reyssat to get in several special cases essentially best possible estimates.** On the other hand there are now some new estimates for the number of zeroes of certain auxiliary functions, which are usually less precise, but far more general, due to D. Brownawell and D.W. Masser. As a consequence they get an effective version of Schneider-Lang's criterion.

In 7.2.3 we have seen an example of an upper bound for the number of zeroes. We will see another one in the next lecture.

# LECTURE 8

# ALGEBRAIC INDEPENDENCE OF PERIODS

The problem of the transcendence of $\Gamma(1/4)$ was considered as a very difficult one, and it was a real surprise when Choodnovsky announced, in 1975, a result on algebraic independence of numbers connected with exponential and elliptic functions which solves this problem (as remarked by Masser). The proof used a transcendence measure for the number $\pi$. Later he produced a new proof which gives further results. We give here this second proof.

## §8.1 Choodnovsky's results

Let $\wp$ be an elliptic function of Weierstrass with invariants $g_2$, $g_3$ algebraic. Let $\omega_1$, $\omega_2$ be a basis of the lattice $L$ of periods of $\wp$, and $\eta_j = 2\zeta(\frac{\omega_j}{2})$ as usual. We know already the linear relations over $\bar{\mathbf{Q}}$ connecting the six numbers $1, \omega_1, \omega_2, \eta_1, \eta_2, 2i\pi$. We are now interested with the algebraic relations. The Legendre relation $\eta_1 \omega_2 - \eta_2 \omega_1 = 2i\pi$ reduces the problem to the determination of the transcendence degree of the field $\mathbf{Q}(\omega_1,\omega_2,\eta_1,\eta_2)$ over $\mathbf{Q}$. In the case of complex multiplication it is now clear that this degree is at most 2 and we shall see that in fact it is 2. When there is no complex multiplication it seems natural to expect a degree 4, but we know only that the degree is at least 2, and we still do not know for instance if $\omega_1,\omega_2$ are algebraically independent.

All the known results follow from the next theorem of Choodnovsky.

Theorem 8.1.1 (Choodnovsky) Let $\wp$ be an elliptic function of Weierstrass with invariants $g_2$, $g_3$ in $\overline{\mathbb{Q}}$, $\omega$ a non-zero period of $\wp$, $\eta$ the corresponding quasi-period of $\zeta$, $u$ an algebraic point of $\wp$ which is not a pole of $\wp$, with $u$, $\omega$ $\mathbb{Q}$-linearly independent. Then the two numbers

$$\zeta(u) - \frac{\eta}{\omega} u \ , \quad \frac{\eta}{\omega}$$

are algebraically independent.

When $\omega = m_1 \omega_1 + m_2 \omega_2$, and when we choose $u = \omega'/2^h$ where $\omega' = m_1 \omega_1 - m_2 \omega_2$, and $h$ is the smallest integer such that $\omega'/2^h$ is not a pole of $\wp$, one gets

Corollary 8.1.2. The two numbers $\frac{\pi}{\omega}$, $\frac{\eta}{\omega}$ are algebraically independent.

A remark due to D. Bertrand is that this statement is equivalent to the following: for $q \in \mathbb{C}$ with $0 < |q| < 1$, write $q = e^{2i\pi\tau}$ and $J(q) = j(\tau)$ ; assume that $J(q)$ is algebraic and different from 0 and 1728; then the two numbers $q \frac{d}{dq} J(q)$, $(q \frac{d}{dq})^2 J(q)$ are algebraically independent. (We still do not know whether $q$ itself is transcendental ; cf.the last remark of §3.2).

From corollary 8.1.2 it is plain that the field $\mathbb{Q}(\omega_1, \omega_2, \eta_1, \eta_2)$ has transcendence degree at least 2 over $\mathbb{Q}$. This is specially interesting in the case of complex multiplication, since we can choose $(\omega, 2i\pi)$ as a transcendence basis.

Corollary 8.1.3 Assume that $\wp$ has complex multiplication then the

two numbers $\omega, \pi$ are algebraically independent.

Example 1. The curve $y^2 = 4x^3 - 4x$ has complex multiplication by $i$ ; a period $\omega_1$ (with $\wp(\frac{\omega_1}{2}) = 1$) is

$$\omega_1 = 2\int_1^\infty \frac{dx}{\sqrt{4x^3-4x}} = \int_1^\infty \frac{dx}{\sqrt{x^3-x}}$$

We put $u = x^{-2}$ , and we use the relations

$$\Gamma(\tfrac{1}{2}) = \sqrt{\pi} \quad , \quad \Gamma(\tfrac{3}{4})\,\Gamma(\tfrac{1}{4}) = \frac{\pi}{\sin\frac{3\pi}{4}} = \pi\sqrt{2}$$

Therefore

$$\omega_1 = \tfrac{1}{2}\int_0^1 u^{-3/4}\,(1-u)^{-1/2}\,du = \tfrac{1}{2}\,B(\tfrac{1}{4}\,,\,\tfrac{1}{2}) = \frac{\Gamma(\frac{1}{4})^2}{2\sqrt{2\pi}}\,.$$

Thus the two numbers $\Gamma(\frac{1}{4})$ , $\pi$ are algebraically independent, and in particular $\Gamma(\frac{1}{4})$ is transcendental.

Example 2. The curve $y^2 = 4x^3-4$ has complex multiplication by $\rho$ with $\rho^3 = 1$ ; a period $\omega_1$ (with $\wp(\frac{\omega_1}{2}) = 1$) is

$$\omega_1 = 2\int_1^\infty \frac{dx}{\sqrt{4x^3-4}} = \int_1^\infty \frac{dx}{\sqrt{x^3-1}} = \frac{1}{3}\int_0^1 u^{-5/6}\,(1-u)^{-1/2}\,du\,.$$

From the relations

$$\Gamma(\tfrac{2}{3})\,\Gamma(\tfrac{1}{3}) = \frac{2\pi}{\sqrt{3}} \quad , \quad \Gamma(\tfrac{1}{6})\,\Gamma(\tfrac{2}{3}) = 2^{2/3}\,\pi^{1/2}\,\Gamma(\tfrac{1}{3}) \ ,$$

one gets

$$\omega_1 = \frac{1}{3} B(\tfrac{1}{6},\tfrac{1}{2}) = \frac{1}{3} \frac{\Gamma(\frac{1}{6})\,\Gamma(\frac{1}{2})}{\Gamma(\frac{2}{3})} = \frac{\Gamma(\frac{1}{3})^3}{2^{8/3}\pi}$$

Therefore the two numbers $\Gamma(\frac{1}{3})$, $\pi$ are algebraically independent, and in particular $\Gamma(\frac{1}{3})$ is transcendental.

Remark. The number $B(\frac{1}{n}, \frac{1}{2})$ occurs as a period of the hyperelliptic curve $y^2 = 1-x^n$, which is of genus $[\frac{n-1}{2}]$ (integral part). Therefore for $n \geq 5$ we get curves of genus greater than 1. The only rational points between 0 and 1 where $\Gamma$ is known to take transcendental values are those with denominator 2, 3, 4 or 6.

We go back to corollary 8.1.3 and give a further consequence on the modular function $j$. In 1964, using Schneider's results 7.1.1 and 7.1.3, Siegel deduced from the differential equation

$$j'(\tau) = 18 \frac{\omega_1^2}{2i\pi} \cdot \frac{g_3}{g_2} j(\tau)$$

the transcendency of the two numbers $\pi j'(\tau)$ and $j'(\tau)/\pi$ when $\tau$ is imaginary quadratic and $g_2 \cdot g_3 \neq 0$. He asked whether $j'(\tau)$ itself was transcendental. The answer is provided by Masser's theorem 7.1.4, since

$$\frac{2i\pi}{\omega_1^2} = (\tau\eta_1 - \eta_2)/\omega_1 .$$

However corollary 8.1.3 yields a stronger result.

Corollary 8.1.6. Let $\tau$ be a quadratic number of positive imaginary part, which is not congruent to $i$ or $\rho$ modulo $SL_2(\mathbb{Z})$. Then

$\pi$, $j'(\tau)$ are algebraically independent.

## §8.2 Gel'fond's transcendence criterion

There are three main methods for algebraic independence. The oldest one is that of Lindemann-Weierstrass, developed by Siegel, Shidlovskii,.., which deals with functions satisfying linear differential equations. The second is due to Mahler and has been developed recently by K. Kubota, J. Loxton and A.J. van der Poorten, and D.W. Masser; it works with functions satisfying some functional equations (e.g. connecting $f(z^k)$ with $f(z)$ for some integer k). The third one, which will be used here, was introduced by A.O. Gel'fond in 1949; it works with exponential and elliptic functions mainly. The general sketch of the proof is the same as usual, but we work with numbers in a finitely generated extension K of $\mathbb{Q}$ of transcendence degree 1, (instead of a number field), and we need a new device to replace the size inequality 1.1.2. We cannot give a lower bound for each element of K in general (for instance if K contains a Liouville number). The idea, due to Gel'fond, is to consider a sequence of elements of K. Here is an improved version of Gel'fond's criterion.

Theorem 8.2.1. Let $\theta$ be a complex number. Assume that there exist a sequence $(t_n)$ of positive real numbers, together with a sequence $(P_n)$ of non-zero polynomials of $\mathbb{Z}[X]$, of degree $\delta_n$, such that

$$\delta_n + \log H(P_n) \leq t_n ,$$

$$\lim_{n\to\infty} t_n = +\infty$$

and

$$\log|P_n(\theta)| \leq -\delta_n t_n - \max\{\delta_{n-1}t_n+\delta_n t_{n-1};\ 2\delta_n t_n;\ \delta_n t_{n+1}+\delta_{n+1}t_n\} .$$

Then $\theta$ is algebraic and $P_n(\theta) = 0$ for each $n$ such that $t_n \geq 2$ .

Sketch of the proof of theorem 8.2.1.

Since $P_n(\theta)$ is small, $\theta$ is closed to a root of $P_n$ ; let $Q_n$ be the maximal power of the irreducible polynomial of this root which divides $P_n$ . Then $Q_n(\theta)$ is small:

$$\log|Q_n(\theta)| \leq -\max\{\delta_{n-1}t_n+\delta_n t_{n-1};\ 2\delta_n t_n;\ \delta_n t_{n+1}+\delta_{n+1}t_n\} .$$

The resultant of $Q_n$ and $Q_{n+1}$ is a rational integer; one can derive an upper bound for the absolute value of this number in terms of $\max(|Q_n(\theta)|, |Q_{n+1}(\theta)|)$ , and the degrees and heights of $Q_n$ and $Q_{n+1}$ ; as soon as $t_n + t_{n+1} \geq 3$ , the upper bound is less than 1, and therefore the resultant vanishes. For large $n$ one can write $Q_n = R^{q_n}$ with $1 \leq q_n \leq \delta_n$ , and the inequality

$$\log|R(\theta)| \leq -2\,\frac{\delta_n t_{n+1}}{q_n}$$

implies $R(\theta) = 0$ .

## §8.3 Zeroes of polynomials in $z$ , $\wp(z)$, $\zeta(z)$ .

For the proof of theorem 8.1.1 we shall use Gel'fond's method

together with the criterion 8.2.1. We shall need an upper bound for the number of zeroes of our auxiliary function. The arguments we shall use go back to Masser's thesis. The next result is a special case of a several (complex) variables statement due to P. Philippon which he used to prove a p-adic version of theorem 8.1.1.

Theorem 8.3.1(Masser, Philippon). Let $\wp$ be an elliptic function of Weierstrass, and $\zeta$ the associated zeta function. There exists a constant $c_1 > 0$ such that if $P \in \mathbb{C}[X_0,X_1,X_2]$ is a non-zero polynomial of degree at most $L_j$ in $X_j$, $(j=0,1,2)$ with $L_j \geq 1$, then the number $\nu_F(0,r)$ of zeroes of the function

$$F(z) = P(z, \wp(z), \zeta(z))$$

in a disc $|z| \leq r$ satisfies

$$\nu_F(0,r) \leq c_1(L_1+L_2)r^2 \quad \text{for} \quad r \geq L_0+L_2 .$$

This upper bound is obvious for $r$ sufficiently large (using Schwarz lemma 1.3.1 and the fact that $\wp$ and $\zeta$ are of order $\leq 2$). However for us it will be important to have an explicit condition on $r$.

From §4.4 we know already that it is sufficient to get an upper bound for $|G|_R$ with

$$G = \sigma^{2L_1+L_2} F$$

in terms of $|G|_r$, with $R > r$, and then to use Schwarz lemma 1.3.1.

It is possible to prove the theorem 8.3.1 (with the slightly

weaker estimate $r \geq L_0 + L_2 + (\log L_1)^{1/2}$ which would be quite sufficient for us) by means of Lagrange interpolation formula in several variables. However we prefer to use the following result of Moreau which will play a central role in the next lecture where it will be proved.

For $z = (z_1,\ldots,z_n) \in \mathbb{C}^n$ we write $|z| = \max_{1\leq j\leq n} |z_j|$. When $f$ is an entire function in $\mathbb{C}^n$, we define $|f|_r = \sup_{|z|=r} |f(z)|$ for $r \geq 0$. Further for $S \subset \mathbb{C}^n$ we write $|f|_S = \sup_{z\in S} |f(z)|$.

Theorem 8.3.2 (Moreau). Let $n$ be a positive integer. There exist two constants $c_2$, $c_3$ depending only on $n$ with the following property. Let $L$ be a positive integer, $Q \in \mathbb{C}[X_1,\ldots,X_n]$ a polynomial of total degree at most $L$, and $S$ a subset of $\mathbb{C}^n$, with the property that for each $\zeta = (\zeta_1,\ldots,\zeta_n) \in \mathbb{R}^n$, with $|\zeta| \leq 1$ there exists $\sigma = (\sigma_1,\ldots,\sigma_n) \in S$ with

$$|\sigma_j - \zeta_j| \leq \frac{1}{c_2 L}, \quad (1\leq j\leq n).$$

Then

$$|P|_1 \leq e^{c_3 L} |P|_S$$

(In fact one can choose $c_2 = e^{2n+7}$ and $c_3 = 2^{n+5}$).

In this section we shall use this theorem only for the case where $S$ is a cartesian product $S_1\times\ldots\times S_n$ (in this case interpolation

formulae yield the result with $e^{c_3 L}$ replaced by $L^{c_3 L}$ ) .

We begin the proof of theorem 8.3.1 with the following lemma.

Lemma 8.3.3. Let $\omega_1,\omega_2$ be a pair of fundamental periods of $\wp$ . Let E be the subset of $\mathbf{C}$ defined by

$$E = \{\frac{\omega_1}{6} x + \ell_1\omega_1+\ell_2\omega_2 \ ; \ x\in[1,2],\ 0 \leq \ell_1 \leq L_0+L_2 \ ,\ 0 \leq \ell_2 \leq L_0+L_2\}$$

where x is real and $\ell_1,\ell_2$ integers. Then

$$H(P) \leq c_4^{L_0+L_1+L_2} |F|_E$$

where $c_4$ depends only on $\wp$ .

Proof

Let $z_0 \in [\frac{\omega_1}{6} , \frac{\omega_1}{3}]$ . For $(\ell_1,\ell_2) \in \mathbf{Z}\times\mathbf{Z}$, the number

$$F(z_0+\ell_1\omega_1+\ell_2\omega_2) = P(z_0+\ell_1\omega_1+\ell_2\omega_2, \wp(z_0), \zeta(z_0)+\ell_1\eta_1+\ell_2\eta_2)$$

is a polynomial in $\ell_1,\ell_2$, say $T_{z_0}(\ell_1,\ell_2)$ . From the theorem 8.3.2 (with n = 2) we deduce

$$H(T_{z_0}) \leq c_5^{L_0+L_2} |F|_E \ .$$

Let us define

$$S_{z_0}(X_0,X_2) = P(X_0, \wp(z_0),X_2) \ .$$

From Legendre relation one easily gets

$$H(S_{z_0}) \leq c_6^{L_0+L_2} H(T_{z_0}) .$$

The coefficients of $S_{z_0}$ are polynomials in $\wp(z_0)$

If $Q \in \mathbb{C}[X_1]$ is a polynomial of degree $\leq L_1$, and if

$$E_1 = \{\frac{\omega}{6}(1+\frac{\ell}{L_1}) , 0 \leq \ell \leq L_1 , \ell \in \mathbb{Z}\} ,$$

then the theorem 8.3.2 (with n=1) implies

$$H(Q) \leq c_7^{L_1} |\phi|_{E_1}$$

where $\phi = Q(\wp)$ .

This proves lemma 8.3.3.

Lemma 8.3.4 With the notations of theorem 8.3.1 we have for $R \geq r \geq c_8 (L_0+L_2)$

$$|G|_R \leq |G|_r \, c_9^{(L_1+L_2)R^2}$$

where $c_8, c_9$ depend only on $\wp$ and $G(z) = \sigma(z)^{2L_1+L_2} F(z)$ .

Proof

We begin with the obvious upper bound

$$\log |G|_R \leq c_{10} (L_1+L_2)R^2 + L_0 \log R + \log H(P) .$$

From the functional equation of $\sigma$ one gets for $z \in E$

$$|\sigma(z)| \geq c_{11}^{-(L_0+L_2)^2} .$$

Hence

$$|F|_E \leq c_{11}^{(L_0+L_2)^2(2L_1+L_2)} |G|_{r_0}$$

with $r_0 = c_8(L_0+L_2)$ . From lemma 8.3.3 we deduce

$$\log H(P) \leq c_{12} (L_0+L_2)^2(L_1+L_2) + \log |G|_{r_0}$$

and the lemma follows.

Theorem 8.3.1 is an immediate consequence of lemma 8.3.4 and Schwarz lemma 1.3.1.

## §8.4 Proof of Choodnovsky's theorem

We give the proof of theorem 8.1.1. We already know (from Schneider's theorem 7.1.1) the transcendency of $\eta/\omega$ . We assume that the transcendence degree over $\mathbb{Q}$ of the field $\mathbb{Q}(\zeta(u)-\frac{\eta}{\omega} u, \frac{\eta}{\omega})$ is 1, and we shall eventually get a contradiction using the transcendence criterion 8.2.1.

Let $K_0$ be the number field

$$K_0 = \mathbb{Q}(g_2, g_3, \wp(u), \wp'(u)) ,$$

and let $K$ be the field

$$K = K_0(\zeta(u)-\frac{\eta}{\omega} u, \frac{\eta}{\omega}) .$$

By assumption the transcendence degree of $K$ over $\mathbf{Q}$ is 1. We are going to use the property that the two functions

$$\wp(z), \quad \zeta(z) - \frac{\eta}{\omega} z$$

are algebraically independent, have a common period $\omega$, and take together with their derivatives values in $K$ at each point $hu$, $h \in \mathbf{Z}$ which is not a pole of $\wp$.

Let $N$ be a sufficiently large integer. We define

$$L_1 = N^4 , \quad L_2 = N^3 , \quad T = N^6 (\log N)^{-1} .$$

First step. There exists a non zero polynomial $P \in \mathbf{Z}[X_0, X_1, X_2]$ of degree at most $L_2$ in $X_0$, $L_1$ in $X_1$ and $L_2$ in $X_2$, and height at most $e^{N^6}$, such that the function

$$F(z) = P(\tfrac{\eta}{\omega}, \wp(z), \zeta(z) - \tfrac{\eta}{\omega} z)$$

has a zero of order at least $T$ at each point $hu$, $0 \leq h < N$ which is not a pole of $\wp$.

Using the Baker-Coates-Anderson method (§6.2), one computes the $t$-th derivatives of the function

$$(2h)^{L_2} B_h(\wp(z))^{L_1+L_2} \wp(hz)^{\lambda_1} (\zeta(hz) - \tfrac{\eta}{\omega} hz)^{\lambda_2} ;$$

one gets a polynomial in $\wp$, $\zeta - \frac{\eta}{\omega} z$, $\wp'$, $\frac{\eta}{\omega}$, $\frac{g_2}{4}$, $g_3$ with coefficients in $\mathbf{Z}$ of absolute value at most

$$c_1^{(L_1+L_2)h^2+t} \quad [(L_1+L_2)h^2+t]^t$$

and degrees at most $(L_1+L_2)h^2+2t$ , $L_2$ , $1$ , $\min\{s,L_2\}$ , $(L_1+L_2)h^2+t$ and $(L_1+L_2)h^2+t$ respectively. Expanding our numbers on the transcendence basis $\frac{\eta}{\omega}$ , we get a system of $c_2\ L_2\ NT$ equations with $L_1L_2^2$ unknowns, with coefficients in $\mathbb{Z}$. Siegel's lemma 1.2.1 does the rest.

Second step. Put $T_1 = N^6 \log N$. There exists two integers $t_1$ , $h_1$ , with $0 \leq t_1 < T_1$ , $0 \leq h_1 < N$ , such that $h_1 u$ is not a pole of $\wp$ , and

$$\gamma = F^{(t_1)}(h_1 u) \neq 0$$

We use the theorem 8.3.1 with $L_0 = L_2$ , $r = N^3$ . The number of zeroes of $F$ in $|z| \leq N^3$ is at most $c_3 N^{10}$ (where as usual $c_3$ does not depend on $N$); therefore one of the numbers

$$F^{(t)}(hu + \ell\omega) ,$$

$(0 \leq t < T_1$ , $0 \leq h < N$, $0 \leq \ell < \frac{1}{2|\omega|} N^3$ and $hu$ not pole of $F)$ is not zero. The periodicity of $F$ with respect to $\omega$ yields what we wanted.

We choose $t_1$ such that $F^{(t)}(h_1 u) = 0$ for $0 \leq t < t_1$ .

Third step. We have

$$\log|\gamma| \leq - c_4 N^{10} (\log N)^{-3}$$

This is a consequence of Schwarz lemma 1.3.1 with $r = N^3(\log N)^{-2}$ ,

$R = 3r$, for the function

$$G = \sigma^{2L_1+L_2} \Gamma .$$

From the upper bound

$$\log |G|_R \leq c_5 (L_1 R^2 + N^6) \leq 2c_5 N^{10} (\log N)^{-4}$$

and the periodicity of $F$ which yields

$$\nu_G(0,r) \geq \frac{1}{2} R_1 TN = \frac{1}{2} N^{10} (\log N)^{-3}$$

we deduce

$$\log |G|_r \leq -\frac{1}{3} N^{10} (\log N)^{-3}$$

From Cauchy's inequalities

$$\log |G^{(t_1)}(h_1 u)| \leq -\frac{1}{4} N^{10} (\log N)^{-3} ,$$

and from the minimality of $t_1$

$$G^{(t_1)}(h_1 u) = \sigma(h_1 u)^{2L_1+L_2} \gamma .$$

Using the multiplication formula for $\sigma$ and the size inequality for $\Psi_{h_1}(\wp(u), \wp'(u))$, we have

$$\log|\sigma(h_1 u)| \geq -c_7 N^2 .$$

The result follows (with $c_4 = \frac{1}{5}$, say).

Fourth step. There exists a non-zero polynomial $P_N \in \mathbf{Z}[X]$ with

$$\deg P_N \leq c_8 N^3$$

$$\log H(P_N) \leq c_9 N^6 (\log N)^2 ,$$

$$\log |P_N(\eta/\omega)| \leq - c_{10} N^{10} (\log N)^{-3}$$

Our number $\gamma$ is a non-zero element of $K$. We multiply it by a denominator in such a way that it is integral over $\mathbf{Z}[\eta/\omega]$, and we take the norm. (These estimates are a little bit delicate, but we do not give the technical details).

Conclusion

From the criterion 8.2.1 we get the contradiction that $\eta/\omega$ is algebraic.

## §8.5 Further results and comments

When Gel'fond developed his method in 1949 he succeeded to prove the algebraic independence of $a^b$, $a^{b^2}$, when a and b are algebraic, $a \neq 0$, $\log a \neq 0$ and $[\mathbf{Q}(b):\mathbf{Q}] = 3$. He got a lot of other results but all of them were asserting that two numbers at least of a certain set of numbers were algebraically independent, and the only case where he could actually reduce this set to 2 elements, and thus get the actual independence of 2 numbers, was the above mentioned one. Several authors developed Gel'fond's method, especially in the 70's, but their results suffered from

the same defect. However it is worth to mention a paper of Brownawell and Kubota (Acta Arith. 33 (1977) 111-149) where they get nice results of algebraic independence of numbers related to elliptic functions (in one example they show that of three numbers at least two are algebraically independent). Their results were extremely general (in fact they used a much more general criterion) and it turned out that this was not the best way to look at the situation: Choodnovsky's proof of the transcendency of $\Gamma(1/4)$ rests on the same method, but uses in a more efficient way the properties of the special case he considers, and especially the periodicity.

The other results of Choodnovsky on algebraic independence concern values of exponential functions, of elliptic functions (where it is not always necessary to assume $g_2$, $g_3$ algebraic), and abelian functions. Specially worth mentioning is his work on elliptic version of the Lindemann-Weierstrass theorem.

These problems are much more difficult to solve in the p-adic case; the exponential and $\wp$ functions are defined only locally, and it is not possible to take a large radius in Schwarz lemma. However D. Bertrand found a new device: he works with Tate elliptic functions. Because of the essential singularity at the origin he needs a Schwarz lemma for an annulus which he proved both in the complex and the p-adic case. As an example he considers the Eisenstein series

$$E_{2k}(q) = 1 + (-1)^k (4k/B_k) \sum_{n=1}^{\infty} n^{2k-1} (q^n/(1-q^n))$$

and shows that for any $q$ in the p-adic domain of convergence, two of the numbers $E_2(q)$, $E_4(q)$, $E_6(q)$ are algebraically independent. Further p-adic results corresponding to Choodnovsky's theorems of §8.1 have been obtained recently by P. Philippon.

# LECTURE 9

## SCHNEIDER'S METHOD IN SEVERAL VARIABLES.

Baker's solution to the problem of linear independence of logarithms uses a generalization of Gel'fond's method. It is natural to ask whether another proof can be derived from a generalization of Schneider's method. There are at least two reasons to make some efforts in this direction; the first one is the fundamental importance of getting lower bounds for linear forms in logarithms, the second one is the hope to solve new problems, and especially to study the rank of determinants whose coefficients are logarithms of algebraic numbers (cf. problem 3.2.2).

We give here a first partial solution, which yields a new proof of Baker's theorem in the real case. Our main tool is Moreau's theorem 8.3.2 , and we first give a sketch of his proof.

There is only one serious difficulty when dealing with several variables, namely to get a Schwarz lemma corresponding to 1.3.1. For the case of finitely generated subgroups of $\mathbf{C}^n$ we have a precise conjecture (see § 9.4)

## §9.1 Polynomials in several variables.

In his thesis (L.N. 437, appendix 2), Masser investigated some properties of polynomials in several variables. He showed in particular that a non-zero polynomial in $\mathbf{C}[z_1,\ldots,z_n]$ of degree $\leq L$ cannot have a zero within $c_1(n)L^{-1/2}$ of every point of the unit ball, and cannot have a zero within $c_2(n)\ (L \log L)^{-1}$ of every real point of the unit ball. The first result is plainly best possible (on the basis of simple counting arguments), while for the second Masser conjectured that the log L could be removed. This problem was solved in 1975 by Moreau, who then obtained a stronger version (theorem 8.3.2). In 1976 Masser derived a similar refinement of his first result (J. Approximation Theory, 24 (1978), 18 - 36). It should be mentioned that Masser's conjecture (without the refinement of Moreau) can be solved in a very different way by means of Berndtsson's work on zeroes of analytic functions of several variables (Arkiv för Mat. 16 (1978) 251-262).

We give here a sketch of Moreau's proof of theorem 8.3.2. In his first proof (C.R. Acad. Sci. Paris, A 282 (1976), 771-774), and also in Masser's earlier work, an important auxiliary result was the following result of Bernstein: for a polynomial $Q \in \mathbf{C}[z]$ of a single variable and of degree at most $L$, $|Q'|_1 \leq L|Q|_1$. Recently Moreau found a nice proof of the slightly weaker estimate $|Q'|_1 \leq eL|Q|_1$, which is quite sufficient for his purpose (and enables him to extend his theorem to the p-adic case.) We first begin with a simple lemma.

Lemma 9.1.1. Let $P \in \mathbb{C}[z_1,\ldots,z_n]$ be a polynomial of total degree at most $L$. Then for $R \geq r > 0$ we have

$$|P|_R \leq (\frac{R}{r})^L |P|_r .$$

Proof.

Let $z_0 \in \mathbb{C}^n$ with $|z_0| = R$ and $|P(z_0)| = |P|_R$. Define $Q \in \mathbb{C}[t]$ by $Q(t) = t^L P(\frac{z_0}{t})$. By the maximum modulus principle $|Q(1)| \leq |Q|_{R/r}$. Thus

$$|P|_R \leq (\frac{R}{r})^L \sup_{|t|=R/r} |P(\frac{z_0}{t})| \leq (\frac{R}{r})^L |P|_r .$$

Lemma 9.1.2. Let $Q \in \mathbb{C}[z]$ be a polynomial of degree at most $L \geq 1$. Then

$$|Q'|_1 \leq (eL) |Q|_1 .$$

Proof.

Let $z_0 \in \mathbb{C}$ with $|z_0| = 1$ and $|Q'(z_0)| = |Q'|_1$. By Cauchy's inequalities

$$|Q'(z_0)| \leq L |Q|_{1+L^{-1}} .$$

From lemma 9.1.1 we conclude

$$|Q'|_1 \leq L(1+L^{-1})^L |Q|_1 \leq eL|Q|_1 .$$

Another important tool in the proof of theorem 8.3.2 is a lemma of Popken and Koksma , improved by Gel'fond.

Lemma 9.1.3. Let $P_1,\ldots,P_m$ be polynomials in $\mathbb{C}[X_1,\ldots,X_n]$ and let the degree of $P_1\ldots P_m$ be at most $L$ in each variable $X_j$. Then

$$H(P_1)\ldots H(P_m) \leq e^{nL} H(P_1\ldots P_m) .$$

Mahler's proof of this result uses the measure $M(P)$ for $P \in \mathbb{C}[X_1,\ldots,X_n]$:

$$M(P) = \exp\{\int_0^1 \ldots \int_0^1 \log|P(e^{2i\pi u_1},\ldots,e^{2i\pi u_n})|\,du_1\ldots du_n\}$$

so that

$$M(P_1\ldots P_m) = M(P_1)\ldots M(P_m).$$

It is then sufficient to relate $M(P)$ and $H(P)$.

(Lemma 9.1.3 was used already implicitely in the proof of Gel'fond's criterion 8.2.1.)

Sketch of the proof of Moreau's theorem 8.3.2.

The letters $c_3$, $c_4$, $c_5$ will denote positive numbers which depend only on $n$ (and are easily estimated).

First step. Let $P \in \mathbb{C}[X_1,\ldots,X_n]$ be a polynomial of degree at most $L$ in each $X_j$, and $S$ be a subset of $\mathbb{C}^n$ such that for each $\zeta=(\zeta_1,\ldots,\zeta_n) \in \mathbb{C}^n$ with $|\zeta_1|=\ldots=|\zeta_n|=1$ (i.e. $\zeta$ is on the distinguished boundary of the unit polydisc), the distance (*) from $\zeta$ to $S$ is less than $c_3L^{-1}$. Then

$$|P|_1 \leq 2|P|_S .$$

We choose $\zeta$ with $|P(\zeta)| = |P|_1$, and $\sigma \in S$ with $|\sigma-\zeta| \leq c_3L^{-1}$. From the mean value theorem one has

$$|P|_1 \leq |P|_S + c_3L^{-1} \sum_{j=1}^{n} \left|\frac{\partial}{\partial z_j} P\right|_{1+c_3L^{-1}}$$

From lemmas 9.1.1 and 9.1.2 this inequality gives

$$|P|_1 \leq |P|_S + \tfrac{1}{2}|P|_1$$

which yields the desired result.

Second step. Let $P \in \mathbb{C}[X_1,\ldots,X_n]$ be a polynomial of degree at most $L$ in each $X_j$, and $S$ be a subset of $\mathbb{C}^n$ such that for

(*) We use always the sup norm: $|z| = \max_{1\leq j\leq n} |z_j|$ for $z = (z_1,\ldots,z_n) \in \mathbb{C}^n$.

*each* $\zeta = (\zeta_1,\ldots,\zeta_n) \in \mathbf{C}^n$ *with* $|\zeta_j| = 1$ *and* $\mathrm{Im}\zeta_j \geq 0$, *the distance from* $\zeta$ *to* $S$ *is less than* $c_4 L^{-1}$. *Then*

$$|P|_1 \leq c_5^L |P|_S$$

One applies the first step to the polynomial

$$\prod P(\varepsilon_1 X_1,\ldots,\varepsilon_n X_n) ,$$

where $(\varepsilon_1,\ldots,\varepsilon_n)$ runs over the $2^n$ n-tuples $\varepsilon_j = \pm 1$. For this second step lemma 9.1.3 is needed.

*Third step. Proof of the theorem.*

Define $h(u) = \frac{iu+1}{u+i}$ for $u \in \mathbf{C} - \{-i\}$. For $\zeta \in \mathbf{C}$ with $|\zeta| = 1$ and $\mathrm{Im}\zeta \geq 0$ one has $h(\zeta) \in \mathbf{R}$, $|h(\zeta)| \leq 1$. Then one applies the second step to the polynomial

$$\Big(\prod_{j=1}^{n} (X_j + i)^L\Big)\, P(h(X_1),\ldots,h(X_n)).$$

## §9.2. A Schwarz lemma in several variables.

The first generalization of lemma 1.3.1 to several variables goes back to Schneider (1940) where he used iterated interpolation formulae. This method works only for cartesian products which is a degenerated situation. The first study of a non degenerate case is due to J. P. Serre (1966) in the p-adic case (*), and to Bombieri and Lang four years later in the complex case. We shall deal with a further extension of Bombieri-Lang's result in the next lecture; it is fair to mention that this result together with Berndtsson's

---

(*) See also P. Robba, Invent. Math. 48 (1978), 245-277.

above mentioned paper leads to another proof of the main result of the present section. However our method is simpler (modulo Moreau's theorem) and yields better estimates.

Theorem 9.2.1. Let $n$ be a positive integer. There exist positive numbers $c_1, c_2, c_3$ depending only on $n$ and easily computable, with the following property. Let $R \geq r \geq r_1 > 0$ be real numbers, and $L$ a positive integer. Let $S$ be a subset of $\mathbf{C}^n$ such that for each $\zeta = (\zeta_1, \ldots, \zeta_n) \in \mathbf{R}^n$ with $|\zeta| \leq r_1$, the distance from $\zeta$ to $S$ is less than $c_1 r_1 / L$. Then

$$|f|_r \leq \left(\frac{c_2 r}{R}\right)^L |f|_R + \left(\frac{c_3 r}{r_1}\right)^L |f|_S .$$

If one applies this theorem to a polynomial of degree $\leq \frac{L}{2}$ (with say $r = r_1 = 1$, $R \to \infty$) one gets Moreau's theorem as a corollary. But in fact we will deduce theorem 9.2.1 from Moreau's theorem.

Proof of theorem 9.2.1.

We write the Taylor expansion of $f$ at the origin, and we cut it in two parts: $f = P + g$, where $P$ is a polynomial of degree $< L$, and $g$ has a zero of order at least $L$ at the origin. It is easily checked that for $0 \leq \rho \leq R$, $|g|_\rho < (\frac{\rho}{R})^L |g|_R$ (this is the classical Schwarz lemma for one zero with high multiplicity). Since there is no loss of generality to assume $|\sigma| \leq 2r_1$ for $\sigma \in S$, we have

$$|P|_S \leq |f|_S + |g|_{2r_1} .$$

Further from Cauchy's inequalities we have

$$|P|_R \leq L^n |f|_R ,$$

and therefore

$$|g|_R \leq 2L^n |f|_R .$$

We perform a contraction to come inside the unit polydisc: we define

$$S' = \{\frac{1}{r_1} \sigma , \sigma \in S\} ,$$

and

$$Q(z) = P(r_1 z) .$$

Thus

$$|Q|_{\frac{r}{r_1}} = |P|_r , \quad |Q|_{S'} = |P|_S .$$

From lemma 9.1.1 we have

$$|Q|_{\frac{r}{r_1}} \leq (\frac{r}{r_1})^L |Q|_1 .$$

Now we use Moreau's theorem 8.3.2:

$$|Q|_1 \leq c_4^L |Q|_{S'} .$$

From these inequalities we deduce

$$|P|_r \leq (c_4 r/r_1)^L |P|_S .$$

Finally

$$\begin{aligned} |f|_r &\leq |P|_r + |g|_r \\ &\leq (c_4 r/r_1)^L (|f|_S + (\frac{2r_1}{R})^L |g|_R + (\frac{r}{R})^L |g|_R \\ &\leq (\frac{c_2 r}{R})^L |f|_R + (\frac{c_3 r}{r_1})^L |f|_S . \end{aligned}$$

We now give an example of a set $S$ satisfying the density condition of theorem 9.2.1.

Lemma 9.2.2. Let $\beta_1,\ldots,\beta_n$ be algebraic real numbers. We assume that $1,\beta_1,\ldots,\beta_n$ are $\mathbb{Q}$-linearly independent. Let

$\varepsilon$ *be a positive real number. There exists a positive number* $c_5$ *depending only on* $n, \beta_1,\ldots,\beta_n$ *and* $\varepsilon$, *such that for all* $H \geq 1$ *and* $\zeta \in \mathbf{R}^n$ *with* $|\zeta| \leq 1$, *there exists* $(h_0, h_1,\ldots,h_n) \in \mathbf{Z}^{n+1}$ *with* $-H \leq h_j \leq H$, $(0\leq j\leq n)$ *such that the point* $\gamma = (h_1+h_0\beta_1,\ldots,h_n+h_0\beta_n)$ *satisfies*

$$|\gamma - \zeta| \leq c_5 H^{-\frac{1}{n}+\varepsilon} .$$

Once we know this property for $|\zeta| \leq 1$, we deduce it for $|\zeta| \leq \frac{1}{2}H$ (with $c_5$ replaced by $c_6$) using translations by $\mathbf{Z}^n$. Thus the assumption of theorem 9.2.1 is fulfilled with $r_1 = H/2$, $L = c_7 H^{1+\frac{1}{n}-\varepsilon}$

*Proof of lemma* 9.2.2. We use a very deep result of W. M. Schmidt: there exists $c_8 = c_8(n, \beta_1,\ldots, \beta_n, \varepsilon)$ such that

$$\min \{|\gamma| \ ; \ \gamma=(h_1+h_0\beta_1,\ldots,h_n+h_0\beta_n),\ \gamma\neq 0,\ -H\leq h_j\leq H\} > c_8 H^{-\frac{1}{n}-\varepsilon} .$$

The lemma follows from a classical transference theorem.

Our purpose was to establish the following result, which is an easy consequence of 9.2.1 and 9.2.2.

*Corollary* 9.2.3. *Let* $\beta_1,\ldots,\beta_n$ *be algebraic real numbers. We assume that* $1,\beta_1,\ldots,\beta_n$ *are* $\mathbf{Q}$*-linearly independent. Let* $\varepsilon$ *be a positive real number. There exists a positive number* $c_9$ *depending only on* $n,\beta_1,\ldots,\beta_n$, *and* $\varepsilon$, *such that for all* $H \geq 1$ *and for all non-zero entire functions* $f$ *satisfying*

$$f(h_1+h_0\beta_1,\ldots,h_n+h_0\beta_n) = 0 , \quad (-H\leq h_j\leq H,\ 0\leq j\leq n) ,$$

we have

$$\log |f|_r \le \log |f|_R - c_9 H^{1+\frac{1}{n}-\varepsilon} \log \frac{R}{c_2 r}$$

for $R \ge r \ge H$.

Apart from the $\varepsilon$ this estimate is best possible.

## §9.3 A new proof of the real case of Baker's theorem.

We prove that if $\alpha_1,\dots,\alpha_n$ are non-zero algebraic numbers, and $\log \alpha_1,\dots,\log \alpha_n$ are $\mathbf{Q}$-linearly independent, (where $\log \alpha_j$ is any determination of the logarithm of $\alpha_j$), then $\log \alpha_1,\dots,\log \alpha_n$ are linearly independent over the field $\bar{\mathbf{Q}} \cap \mathbf{R}$ of real algebraic numbers. It is an easy exercise of linear algebra to check that this statement is equivalent to the following.

(9.3.1) Let $\alpha_1,\dots,\alpha_n$ be non-zero algebraic numbers, and $\beta_1,\dots,\beta_n$ be real algebraic numbers; for $1 \le j \le n$ let $\log \alpha_j$ be any non-zero determination of the logarithm of $\alpha_j$. Further assume $1,\beta_1,\dots,\beta_n$ $\mathbf{Q}$-linearly independent. Then the number

$$\alpha_1^{\beta_1} \dots \alpha_n^{\beta_n} = \exp\{\sum_{j=1}^{n} \beta_j \log \alpha_j\}$$

is transcendental.

We assume that this number is algebraic, and we define

$$\log \alpha_0 = \beta_1 \log \alpha_1 + \dots + \beta_n \log \alpha_n .$$

We shall ultimately derive a contradiction. The hypothesis that the $\beta$'s are real will be used only through the Schwarz lemma 9.2.3.

The proof follows closely that of §3.1. The $n+1$ functions $z_1,\dots,z_n,\alpha_1^{z_1}\dots\alpha_n^{z_n}$ are algebraically independent and take

algebraic values at all points $(h_1+h_0\beta_1,\dots,h_n+h_0\beta_n)$, $(h_0,\dots,h_n) \in \mathbf{Z}^{n+1}$.

Let $N$ be a sufficiently large integer. We choose

$$L = N^{2n^2+5n+1}, \quad \Lambda = N^{2n+1}, \quad H = N^{2n^2+3n}.$$

Notice that

$$L = \Lambda H, \quad L^n\Lambda = H^{n+1}N, \quad H^{1+\frac{1}{n}} = LN^2.$$

Step 1. *There exists a non-zero polynomial* $P \in \mathbf{Z}[X_1,\dots,X_n,Y]$ *of degree at most* $L$ *in* $X_1,\dots,X_n$ *and at most* $\Lambda$ *in* $Y$, *of height at most* $e^L$, *such that the function*

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

*satisfies*

$$F(h_1+h_0\beta_1,\dots,h_n+h_0\beta_n) = 0$$

*for* $(h_0,\dots,h_n) \in \mathbf{Z}^{n+1}$, $-H \le h_j \le H$, $(0\le j\le n)$.

This is easily obtained by means of Siegel's lemma for the system

$$\sum_{\lambda_1=0}^{L} \dots \sum_{\lambda_n=0}^{L} \sum_{\lambda=0}^{\Lambda} p(\lambda_1,\dots,\lambda_n,\lambda) \Big(\prod_{j=1}^{n}(h_j+h_0\beta_j)^{\lambda_j}\Big) \alpha_0^{\lambda h_0}\dots\alpha_n^{\lambda h_0} = 0$$

of $(2H+1)^{n+1}$ equations with $L^n\Lambda$ unknowns.

Step 2. *For each integer* $M \ge N$ *we have*

$(I)_M$ $\quad F(h_1+h_0\beta_1,\dots,h_n+h_0\beta_n) = 0$ *for* $(h_0,\dots,h_n) \in \mathbf{Z}^{n+1}$

*with* $\quad |h_j| \le M^{2n^2+3n}$, $(0\le j\le n)$

*and*

$(II)_M$ $\quad \log |F|_r \le -M^{2n^2+5n+\frac{5}{2}}$ *for* $r = M^{2n^2+3n+1}$

The proof is done by induction on $M$, the property $(I)_N$ being given by the first step. The proof that $(II)_M \Rightarrow (I)_{M+1}$ is

exactly the same as in §3.1: the house and denominator of $F(h_1+h_0\beta_1,\ldots,h_n+h_0\beta_n)$, with the condition on $h_0,\ldots,h_n$ given by $(I)_{M+1}$, are bounded by $\exp(M^{2n^2+5n+2})$.

For the proof that $(I)_M$ implies $(II)_M$, we use our Schwarz lemma 9.2.3 with $R = r\,M^{1/2}$, $\varepsilon = 1/(10n^2)$, and

$$\log |F|_R \leq c_1 M^{2n^2+5n+\frac{5}{2}} .$$

The exponent of $M$ in Schwarz lemma is at least

$$(2n+3)(n+1) - \varepsilon(2n^2+3n) \geq 2n^2+5n+\tfrac{5}{2} ,$$

therefore

$$\log|F|_r \leq -c_2 M^{2n^2+5n+\frac{5}{2}} \log M$$

which gives the announced bound.

Step 3. Conclusion: $F = 0$.

This contradiction completes the proof.

Remarks. This proof suggests several comments.

1. The assumption that $\beta_1,\ldots,\beta_n$ are real is of course undesirable. This suggest that the Schwarz lemma 9.2.3 could be extended to the case where $\beta_1,\ldots,\beta_n$ are not assumed to be real. We can go further and ask whether the assumption that they are algebraic is necessary. We shall discuss the matter in the next section.

2. The constants $c_5$ and $c_9$ of §9.2 are not effectively computable. This is not a too much serious defect for two reasons. Firstly one can hope that the corollary 9.2.3 holds without assuming $\beta_1,\ldots,\beta_n$ to be algebraic (as already mentioned), and this ask for a proof which does not use Schmidt's theorem. Secondly for the

applications the most important effective results concern linear forms in logarithms with integer coefficients. In this case by the present method there is no need of Schmidt's results (however up to now the lower bounds which could be reached by the present method seem less sharp than by the method of §5.2).

3. It is not straightforward to get by the method of this section a non-homogeneous result for

$$\log \alpha_0 = \beta_0 + \beta_1 \log \alpha_1 + \ldots + \beta_n \log \alpha_n .$$

However the technical difficulties have been solved very recently by J. C. Moreau. This means that it is possible to combine the methods of Gel'fond and Schneider.

## §9.4. Generalized Dirichlet exponent.

Let $\Gamma = \mathbb{Z}\gamma_1 + \ldots + \mathbb{Z}\gamma_\ell$ be a finitely generated subgroup of $\mathbb{C}^n$ of rank $\ell$. For $N \geq 1$ we define

$$\Gamma_N = \{h_1\gamma_1 + \ldots + h_\ell\gamma_\ell \ ; \ (h_1, \ldots, h_\ell) \in \mathbb{Z}^\ell, |h_j| \leq N, \ 1 \leq j \leq \ell\}$$

Definition. Let $\theta$ be a positive real number. We say that $\Gamma$ satisfies a Schwarz lemma with exponent $\theta$ if there exist positive numbers $c_1$, $c_2$, $c_3$, $c_4$, depending only on $n, \theta, \gamma_1, \ldots, \gamma_\ell$, such that for all $N \geq c_1$ and all entire functions $f \neq 0$ having a zero at each point of $\Gamma_N$, we have

$$\log |f|_r \leq \log |f|_R - c_2 N^\theta \log \frac{R}{c_3 r}$$

for $R \geq r \geq c_4 N$.

(It is easy to check that this definition does not depend on the basis $\gamma_1, \ldots, \gamma_\ell$).

For instance 9.2.3 means that if $\ell = n+1$ with $\gamma_1, \ldots, \gamma_n$

$\mathbb{C}$-linearly independent and $\gamma_{n+1} = \beta_1\gamma_1 + \ldots + \beta_n\gamma_n$, with $1, \beta_1, \ldots, \beta_n$ $\mathbb{Q}$-linearly independent and $\beta_j \in \bar{\mathbb{Q}} \cap \mathbb{R}$, then $\Gamma$ satisfies a Schwarz lemma with exponent $1 + \frac{1}{n} - \varepsilon$ for all $\varepsilon > 0$.

In the degenerated case of a cartesian product $\Gamma = \Gamma_1 \times \ldots \times \Gamma_n$, where $\Gamma_j$ is a subgroup of $\mathbb{C}$, $(1 \leq j \leq n)$, it is not hard to prove that $\Gamma$ satisfies a Schwarz lemma with exponent $\theta = \min_{1 \leq j \leq n} \operatorname{rank}_{\mathbb{Z}} \Gamma_j$, and this is best possible.

The first study of a non degenerated case is due to Bombieri and Lang (1970). Their point of view was to ask which conditions are sufficient on $\Gamma$ in such a way that $\theta$ can be chosen large. We choose a slightly different point of view. We take any $\Gamma$, and we ask for the best possible value of $\theta$.

The upper bound $\theta \leq \ell/n$ is easy: using Dirichlet box principle, one constructs a non-zero polynomial of degree at most $c_5 N^{\ell/n}$ which has a zero at each point of $\Gamma_N$; then we fix $r$ (say $r = c_4 N$) and let $R$ go to infinity. It is clear that this upper bound is not always best possible. Assume for instance that there is a surjective linear map $L : \mathbb{C}^n \to \mathbb{C}^\nu$ such that $\Gamma' = L(\Gamma)$ has a rank $\lambda$ with $\frac{\lambda}{\nu} < \frac{\ell}{n}$. From the above argument we have a polynomial $P$ of degree $\leq c_6 N^{\lambda/\nu}$ which vanishes on $\Gamma'_N$. Then $P \circ L$ is a polynomial of the same degree which vanishes on $\Gamma_N$, and therefore $\theta \leq \frac{\lambda}{\nu}$.

Notation. We denote by $\mu(\Gamma)$ the minimum of the numbers

$$\frac{\operatorname{rank}_{\mathbb{Z}} s_W(\Gamma)}{\operatorname{codim}_{\mathbb{C}} W} = \frac{\ell - \operatorname{rank}_{\mathbb{Z}}(\Gamma \cap W)}{n - \dim_{\mathbb{C}} W}$$

where $W$ runs over the $\mathbb{C}$-vector subspaces of $\mathbb{C}^n$ distinct from $\mathbb{C}^n$, and $s_W$ is the canonical surjective map $\mathbb{C}^n \to \mathbb{C}^n/W$.

We have proved:

Lemma 9.4.1. Let $\Gamma$ be a finitely generated subgroup of $\mathbb{C}^n$ which satisfies a Schwarz lemma with exponent $\theta$. Then

$$\theta \leq \mu(\Gamma) .$$

The problem is to give a lower bound for $\theta$. Being optimistic I propose the following conjecture.

Conjecture 9.6.2. Let $\Gamma$ be a finitely generated subgroup of $\mathbb{C}^n$, and let $\varepsilon > 0$. Then $\Gamma$ satisfies a Schwarz lemma with exponent $\mu(\Gamma) - \varepsilon$.

Using the method of §9.2, it is possible to prove this conjecture in the case $\Gamma \subset \bar{\mathbb{Q}}^n \cap \mathbb{R}^n$. The conjecture is also true for almost all $\Gamma \subset \mathbb{R}^n$, and also for almost all $\Gamma \subset \mathbb{C}^n$ of rank $\geq 2n$. (Ref.: Astérisque n° 71, 1980).

# LECTURE 10

## GEL'FOND'S METHOD IN SEVERAL VARIABLES.

The study of arithmetic properties of functions of several variables began in 1940 when Schneider investigated the abelian integrals of first and second kind (cf. §7.3). His method was extended by Lang in 1963, who got a generalization of theorem 2.2.1 to several variables; the conclusion is not that the corresponding set of $w \in \mathbb{C}^n$ is finite (this is too much to hope for), but that this set cannot contain a product $S_1 \times \ldots \times S_n$ with $S_j \subset \mathbb{C}$ and Card $S_j$ all large. Nagata suggested that this set is contained in an algebraic hypersurface. This problem has been solved by Bombieri in 1970. It is now possible to give Bombieri's proof in two distinct parts. The first one is a Schwarz lemma which is connected with the singularities of algebraic hypersurfaces, and the second one is the classical transcendence argument.

### §10.1. Singularities of algebraic hypersurfaces and $L^2$ estimates.

#### a) The results.

Let $S$ be a non empty finite subset of $\mathbb{C}^n$, and $t$ a positive integer. We denote by $\omega_t(S)$ the smallest of the degrees of the hypersurfaces having at each point of $S$ a singularity of order at least $t$:

$$\omega_t(S) = \min \{\deg P \; ; \; P \in \mathbb{C}[z_1,\ldots,z_n], \; P \neq 0, \; D^\tau P(\sigma)=0 \text{ for } \sigma \in S \text{ and } \tau \in \mathbb{N}^n, \; |\tau| < t\}.$$

We have written $D^\tau$ for $\dfrac{\partial^{|\tau|}}{\partial z_1^{\tau_1} \ldots \partial z_n^{\tau_n}}$ and $|\tau|$ for $\tau_1+\ldots+\tau_n$.

Using $L^2$ estimates of Hörmander-Bombieri-Skoda, we shall prove

Lemma 10.1.1. *For $t_1$, $t_2$ positive integers we have*

$$\omega_{t_1}(S) \leq \frac{t_1+n-1}{t_2}\ \omega_{t_2}(S) .$$

It is easy to deduce

Theorem 10.1.2. *Let $S$ be a finite subset of $\mathbb{C}^n$. The sequence $(\frac{1}{t}\ \omega_t(S))_{t\geq 1}$ has a limit $\Omega(S)$ and*

$$\frac{1}{n}\ \omega_1(S) \leq \Omega(S) \leq \omega_1(S) .$$

*Moreover for each integer $t \geq 1$*

$$\frac{1}{t+n-1}\ \omega_t(S) \leq \Omega(S) \leq \frac{1}{t}\ \omega_t(S) \leq \omega_1(S).$$

As another application of the $L^2$ estimates, we shall indicate the proof of the following Schwarz lemma for finite subsets of $\mathbb{C}^n$.

Theorem 10.1.3. *Let $S$ be a finite subset of $\mathbb{C}^n$, and $\varepsilon > 0$ a real number. There exists a positive real number $r_0 = r_0(S,\varepsilon)$ such that for any positive integer $t$ and any non-zero function $f$, which is entire in $\mathbb{C}^n$ and has a zero of order at least $t$ at each point of $S$, one has for $R \geq r \geq r_0$*

$$\log |f|_r \leq \log |f|_R - t(\Omega(S) - \varepsilon) \log \frac{R}{4nr} .$$

The proof does not enable us to compute $r_0$ ; it would be interesting to do it, especially when $S$ is of the form $\Gamma_N$ (cf.§9.4). We shall see later (§10.3) a recent improvement of the theorem 10.1.3 due to J. C. Moreau.

b) $L^2$ estimates.

The existence theorems for the $\bar{\partial}$ operator, due to Hörmander, lead to the following

Theorem 10.1.4 (Hörmander-Bombieri-Skoda). Let $V$ be a plurisubharmonic function in $\mathbb{C}^n$, $V \not\equiv -\infty$, and let $\varepsilon > 0$. There exists a function $F$, entire in $\mathbb{C}^n$ and $F \not\equiv 0$, such that

$$\int_{\mathbb{C}^n} |F(z)|^2 e^{-V(z)}(1+|z|^2)^{-n-\varepsilon} d\lambda(z) < +\infty .$$

We show how to deduce lemma 10.1.1 from this estimate. We choose $V = \mu \log |P|$, where $P$ is a polynomial of degree $\omega_{t_2}(S)$ which has a zero of order $\geq t_2$ at each point of $S$, and $\mu > \frac{2t_1+2n-2}{t_2}$. Let $\varepsilon > 0$. From 10.1.4 we get an entire function $F \not\equiv 0$; since the integral converges, one has firstly

$$|F|_R^2 \leq c_1 R^{\mu\omega_{t_2}(S)+2\varepsilon} ,$$

hence $F$ is a polynomial of degree $\leq \frac{1}{2}\mu\,\omega_{t_2}(S)+\varepsilon$, and secondly

$$|F(\zeta)|^2 \leq c_2 |\zeta - \sigma|^{\mu t_2 - 2n}$$

when $\zeta$ is close to a point $\sigma \in S$, hence $F$ has a zero at $\sigma$ of order $> t_1 - 1$. This proves lemma 10.1.1.

c) Sketch of the proof of theorem 10.1.3.

The first part is due to Bombieri and Lang. They consider the average mass $\nu_f(0,r)$ of the zeroes of $f$ in a ball $||z|| \leq r$ (quotient of the $(2n-2)$ Hausdorff measure in Euclidean space of the analytic divisor $f = 0$ in $||z|| \leq r$, by the Lebesgue measure of the ball of radius $r$ in the real $(2n-2)$ space; here $||z||$ is the Euclidean norm), and they prove a statement similar

to 1.3.1, say

$$\log |f|_r \leq \log|f|_R - \nu_f(0,r) \log \frac{R}{4nr} .$$

The second part is the proof of

$$\nu_f(0,r) \geq t(\Omega(S) - \varepsilon) \quad \text{for} \quad r \geq r_0 .$$

This proof rests on arguments and results of Bombieri's paper. One assumes that the result is false; we get a sequence $f_N$ of entire functions and a sequence $t_N$ of positive integers such that $f_N$ has a zero at each point of $S$ of order $\geq t_N$, and

$$\nu_{f_N}(0,N) \leq t_N(\Omega(S) - \varepsilon).$$

One constructs a plurisubharmonic function $V$ (which is in some sense associated with a limit of $\frac{1}{t_N} \log |f_N|$) such that

$$V(z) \leq (\Omega(S) - \varepsilon + o(1)) \log |z| \quad \text{as} \quad |z| \to \infty$$

and

$$V(z) \leq (1 + o(1)) \log |z-\sigma| \quad \text{as} \quad z \to \sigma \in S.$$

Then one applies the existence theorem 10.1.4 with a function $\mu V$, $\mu > 2(t+n-1)$ and $t$ positive integer. We get (as in the proof of lemma 10.1.1)

$$\frac{\omega_t(S)}{t+n-1} \leq \Omega(S) - \varepsilon \quad \text{for all} \quad t \geq 1,$$

which is untenable as $t \to \infty$.

## §10.2 Bombieri's theorem.

The generalization of Schneider-Lang's criterion to several variables is the following

Theorem 10.2.1. (Bombieri). Let $K$ be a number field, $f_1,\dots,f_h$ be meromorphic functions in $\mathbf{C}^n$, with $h \geq n+1$. We assume that $f_1,\dots,f_{n+1}$ are algebraically independent over $\mathbf{Q}$ and of order $\leq \rho_1,\dots,\rho_{n+1}$ respectively. We assume further that the ring $K[f_1,\dots,f_h]$ is invariant under the derivations $\frac{\partial}{\partial z_i}$, $(1 \leq i \leq n)$.

Then the set of $w \in \mathbf{C}^n$ where $f_1,\dots,f_h$ are regular and such that

$$f_j(w) \in K \qquad \text{for } 1 \leq j \leq h$$

is contained in an algebraic hypersurface of degree at most

$$n(\rho_1+\dots+\rho_{n+1})\,[K:\mathbf{Q}]\,.$$

Proof of the theorem 10.2.1.

Without loss of generality, one can assume that $f_1,\dots,f_{n+1}$ are quotients of entire functions of strict order $\leq \rho_1,\dots,\rho_{n+1}$, where an entire function $g$ in $\mathbf{C}^n$ is said to be of strict order $\leq \rho$ if

$$\log |g|_R \leq O(R^\rho) \qquad \text{for } R \to +\infty\,.$$

Let $S = \{w_1,\dots,w_m\}$ be any finite set of $w \in \mathbf{C}^n$ satisfying the desired property. Let $\varepsilon > 0$, with $\varepsilon < 1$, and let $r_0 = r_0(S,\varepsilon)$ be the positive number whose existence is claimed in theorem 10.1.3. Further let $r$ satisfy $r \geq r_0$ and $r \geq |w_k|$ for $1 \leq k \leq m$.

Now let $N$ be a sufficiently large integer. We denote by $\varepsilon_1$, $\varepsilon_2$, $\varepsilon_3$ positive functions of $N$ which tend to $0$ as $N$ tends to infinity. We define

$$L_j = [N^{\kappa_j} (\log N)^{1/n}]\,, \qquad 1 \leq j \leq n+1\,,$$

with

$$\kappa_j = 1 - \frac{\rho_j}{\rho_1+\dots\rho_{n+1}}$$

Step 1. There exists a non-zero polynomial $P \in \mathbf{Z}[X_1,\ldots,X_{n+1}]$ of degree at most $L_j$ in $X_j$, $(1 \le j \le n+1)$, and height at most $N^{\varepsilon_1 N}$, such that $F = P(f_1,\ldots,f_{n+1})$ satisfies

$$D^t F(w) = 0 \qquad \text{for } t \in \mathbf{N}^n,\ |t| < N, \text{ and } w \in S.$$

One first writes $D^t(f_1^{\lambda_1}\ldots f_{n+1}^{\lambda_{n+1}})$ as a polynomial in $f_1,\ldots,f_h$ (see lemma 2.2.5), and then one applies Siegel's lemma.

Step 2. Let $t_0 \in \mathbf{N}^n$ minimal in the lexicographic order be such that there exists $w_0 \in S$ with

$$\gamma = D^{t_0} F(w_0) \neq 0 .$$

Let $M = |t_0|$. Then

$$\log |\gamma| > (\delta - 1 + \varepsilon_2)\, M \log M$$

with $\delta = [K : \mathbf{Q}]$.

Since $F \neq 0$, the existence of $t_0$ is straightforward. From the first step we deduce $M \ge N$. The lower bound for $\gamma$ comes from the size inequality.

Step 3. Let $g_1,\ldots,g_{n+1}$ be non-zero entire functions of strict order at most $\rho_1,\ldots,\rho_{n+1}$ such that $f_1 g_1,\ldots,f_{n+1}g_{n+1}$ are entire. Then the function

$$\Phi = F \prod_{j=1}^{n+1} g_j^{L_j}$$

is entire and satisfies

$$D^t \Phi(w) = 0 \qquad \text{for } |t| < M, \sigma \in S$$

and

$$\log |\Phi|_r \ge -(\delta - \varepsilon_3)\, M \log M .$$

This lower bound of $|\Phi|_r$ is a consequence of the minimality of $t_0$ and of the Cauchy's inequalities.

Step 4. One has

$$\Omega(S) \leq \delta(\rho_1+\ldots+\rho_{n+1}) .$$

One uses theorem 10.1.3 for $\Phi$ with $R = M^{1/(\rho_1+\ldots+\rho_{n+1})}$.

Conclusion. The set $S$ is contained in an algebraic hypersurface of degree $\leq n\delta(\rho_1+\ldots+\rho_{n+1})$. Since this bound does not depend on $S$, the theorem follows by a compacity argument (for each $\Delta > 0$ the set of polynomials in $\mathbb{C}[z_1,\ldots,z_n]$ of height 1 and degree $\leq \Delta$ is compact).

## §10.3. Further results and comments.

### a) Schwarz lemma for fixed finite subsets of $\mathbb{C}^n$.

Let $S$ be a finite subset of $\mathbb{C}^n$ and $t$ a positive integer. Using the remark that on the space of polynomials $P \in \mathbb{C}[z_1,\ldots,z_n]$ of degree $< \omega_t(S)$, one defines a norm by

$$|P|_{S,t} = \max \{\frac{1}{\tau!}|D^\tau P(\sigma)| \; ; \; |\tau| < t, \sigma \in S\} ,$$

J. C. Moreau derived the following result from the arguments of §9.2.

Theorem 10.3.1 (Moreau) Let $S$ be a finite subset of $\mathbb{C}^n$ and $t$ a positive integer. There exists a positive number $r_1(S,t) = r_1$ such that for all $R > r > r_1$, if $f$ is a non-zero entire function having a zero of order $\geq t$ at each point of $S$, then

$$\log |f|_r \leq \log |f|_R - \omega_t(S) \log \frac{R}{e^n r} .$$

Combining this result with theorem 10.1.3 , Moreau deduces

Corollary 10.3.2. With the same notations, for $R > r > r_2$ with $r_2 = r_2(S,\varepsilon)$ one has

$$\log |f|_r \leq \log |f|_R - (\omega_t(S) - t\varepsilon) \log \frac{R}{2e^n r} .$$

Up to the term $t\varepsilon$ this is plainly best possible.

b) Generic sets and Hilbert fourteen's problem.

It has been pointed out to me by G. V. Choodnovsky and L. Begueri-Poitou that in his construction of a counterexample to Hilbert's fourteen problem, M. Nagata proved the following result: let $S$ be a finite subset of $\mathbb{C}^2$ containing $M^2$ independent generic points with $M \geq 4$ , then $\omega_t(S) > t\,M$ . He conjectures that $\omega_t(S) > t(\text{Card } S)^{1/2}$ as soon as $S$ is generic in $\mathbb{C}^2$ with Card $S \geq 10$.

G. V. Choodnovsky gave a simple proof of

$$\omega_t(S) \geq t(\text{Card } S)^{1/n}$$

for $S$ generic in $\mathbb{C}^n$ when Card $S$ is the $n^{\text{th}}$ power of a positive integer. He conjectures that there exists an integer $c(n)$ such that for $S$ generic in $\mathbb{C}^n$ with Card $S \geq c(n)$ ,

$$\Omega(S) = (\text{Card } S)^{1/n} .$$

c) Degrees of algebraic hypersurfaces.

Let $S$ be a finite set in $\mathbb{C}^n$ (which we do not assume to be generic). We proved that

$$\Omega(S) \geq \frac{1}{n} \omega_1(S) .$$

There are two natural questions. Firstly is this best possible? When Card $S = n+1$, and $\omega_1(S) = 2$ (i.e. $S$ contains $n+1$ points which are not in a hyperplane), then obviously

$$\omega_{nt}(S) \leq (n+1)t ,$$

thus $\Omega(S) \leq 1 + \frac{1}{n}$. Choodnovsky conjectures that for any finite subset $S$ of $\mathbb{C}^n$,

$$\Omega(S) \geq \frac{1}{n} (\omega_1(S) + n - 1) .$$

He claimed to be able to solve this problem in the case $n = 2$, by using the theory of intersections.

The second question is to prove similar results when $\mathbb{C}$ is replaced by any field $K$. $L^2$ estimates are powerful, but not quite natural here and purely algebraic methods should apply. The case $n = 2$ seems easier.

d) Finitely generated subgroups of $\mathbb{C}^n$.

Let $\gamma_1,\ldots,\gamma_\ell$ be $\mathbb{Q}$-linearly independent elements of $\mathbb{C}^n$, $\Gamma = \mathbb{Z}\gamma_1+\ldots+\mathbb{Z}\gamma_\ell$, and for $N \geq 1$

$$\Gamma_N = \{h_1\gamma_1+\ldots+h_\ell\gamma_\ell \in \Gamma \; ; \; -N \leq h_j \leq N \; , \; (1\leq j\leq \ell)\} .$$

From the proof of lemma 9.4.1 one easily obtains

$$\omega_1(\Gamma_N) \leq c_1 \, N^{\mu(\Gamma)}$$

where $c_1 = c_1(\gamma_1,\ldots,\gamma_\ell)$ does bot depend on $N$. A special case of conjecture 9.4.2 is the following

Conjecture 10.3.3. Let $\Gamma$ be a finitely generated subgroup of $\mathbb{C}^n$ and let $\varepsilon > 0$. There exists a positive real number $c_2$ such that for $N \geq 1$

$$\omega_1(\Gamma_N) \geq c_2 N^{\mu(\Gamma)-\varepsilon} .$$

For simplicity let us consider the case $\ell = n+1$, $\gamma_{n+1} = x_1\gamma_1+\ldots+x_n\gamma_n$ with $\gamma_1,\ldots,\gamma_n$ $\mathbf{C}$-linearly independent. Then $\mu(\Gamma)$ is 1 or $1+\frac{1}{n}$ according as $1,x_1,\ldots,x_n$ are $\mathbf{Q}$-linearly dependent or not. From the remark at the end of §9.4 we see that for almost all $(x_1,\ldots,x_n) \in \mathbf{R}^n$, the conjecture 9.4.3 holds. It has been pointed out to me by D. Lazard that as soon as the conjecture is satisfied by at least one generic point $(x_1,\ldots,x_n) \in \mathbf{R}^n$, it is satisfied by all generic points. Combining this result with 9.2.3, one gets.

Lemma 10.3.4. Assume $\Gamma = \mathbf{Z}\gamma_1+\ldots+\mathbf{Z}\gamma_{n+1}$ with $\gamma_1,\ldots,\gamma_n$ $\mathbf{C}$-linearly independent and $\gamma_{n+1} = x_1\gamma_1+\ldots+x_n\gamma_n$, $x_1,\ldots,x_n$ being real numbers. We assume that $x_1,\ldots,x_n$ are either algebraic or else algebraically independent. Then conjecture 10.3.3 holds.

It should not be difficult to remove the $\varepsilon$ in the generic case.

c) Comparison of Bombieri's criterion with Baker's method.

One can view Baker's method as a method dealing with meromorphic functions of several variables satisfying differential equations with algebraic coefficients (exactly the same as in Bombieri's criterion 10.2.1). With this point of view the particular feature of Baker's method is to consider the restriction of these functions to a complex line $\mathbf{C}u$ where $u$ is a point in the space say $\mathbf{C}^n$, and the assumption is that these restrictions, i.e. the functions of one variable

$$f_1(tu),\ldots,f_{n+1}(tu)$$

are algebraically independent. There is not yet a general criterion (the reason is that the order of derivation is decreasing along

the inductive argument) but a lot of examples, for instance

- in theorem 4.1.1, one considers the functions

$$z_0,\ e^{z_1},\ldots,\ e^{z_{n-1}},\ e^{\beta_0 z_0+\beta_1 z_1+\ldots+\beta_{n-1}z_{n-1}},$$

and the complex line in $\mathbf{C}^n$ is determined by the point

$$u = (1,\ \log\alpha_1,\ldots,\ \log\alpha_{n-1})\ ;$$

- in theorem 6.1.1 the functions are

$$z_0,\ \wp(z_1),\ldots,\wp(z_{n-1}),\ \wp(\beta_0 z_0+\beta_1 z_1+\ldots+\beta_n z_n)$$

and the point

$$u = (1,\ u_1,\ldots,\ u_{n-1}) \in \mathbf{C}^n\ ;$$

- in theorem 7.1.4, Masser uses 4 functions of 3 variables

$$\wp(z_1),\ \wp(z_2),\ e^{z_3},\ \alpha_1 z_1+\alpha_2 z_2+\beta_1\zeta(z_1)+\beta_2\zeta(z_2)+\gamma z_3\ ,$$

restricted to the complex line $\mathbf{C}.u$ with

$$u = (\omega_1,\ \omega_2,\ 2i\pi)\ .$$

- in theorem 7.1.5, Laurent considers the 4 functions

$$\wp(z_1),\ F(z_1,z_2) = \frac{\sigma(z_1-u)}{\sigma(z_1)\sigma(u)}\ e^{z_1\zeta(u)+z_2},\ e^{z_3}$$

and

$$az_1 + b\zeta(z_1) - cz_2 + dz_3\ ,$$

with

$$u = (\omega\ ,\ \eta u-\omega\zeta(u),\ 2i\pi)\ .$$

Further developments of the work of Brownawell and Masser on the zeroes of entire functions could lead to a general criterion. Notice that in the situation of §9.3, it is easy to give a criterion (without differential equations).

QUEEN'S PAPERS IN PURE AND APPLIED MATHEMATICS

No. 1 RIESZ VECTOR SPACES AND RIESZ ALGEBRAS, L. Fuchs, 85 pp.

No. 2 THE RIEMANN-ROCH THEOREM FOR ALGEBRAIC CURVES, P. Ribenboim, 159 pp.

No. 3 THE MORSE THEORY AND ITS APPLICATIONS TO SOLID STATE PHYSICS, J. Veverka, 103 pp.

No. 4 INDUCED REPRESENTATIONS WITH APPLICATIONS TO $S_n$ AND GL(n), A.J. Coleman, 99 pp.

No. 5 LINEAR REPRESENTATIONS OF FINTE GROUPS, P. Ribenboim, 380 pp.

No. 6 REPORT ON INJECTIVE MODULES, C.T. Tsai, 250 pp.

No. 7 TRANSCENDENTAL NUMBERS, J. Lipman, 83 pp.

No. 8 TOPICS IN THE THEORY OF ELLIPTIC FUNCTIONS, P. Scherk, 308 pp.

No. 9 PARAMETRIC ESTIMATION, M.T. Wasan, (available only as a book, McGraw-Hill).

No. 10 PROCEEDINGS OF THE SYMPOSIUM IN ANALYSIS, Queen's University, June 1967; Papers by: N. Dinculeanu, E. Hewitt, L. Koudryavtsev, Q.A.J. Luxemburg, M.A. Naimark, L. Schwartz, A. Ionescu Tulcea, Abstracts of contributed papers, 250 pp.

No. 11 REDUCED DENSITY MATRICES WITH APPLICATION TO PHYSICAL AND CHEMICAL SYSTEMS - Survey Lectures and Contributed Papers of a Conference held at Queen's University, August 28 - September 1, 1967 Edited by A.J. Coleman and R.M. Erdahl, 435 pp. (Vol. I).

No. 12 MULTIPLICATIVE IDEAL THEORY, R.W. Gilmer, 700 pp.

No. 13 THE ROLE OF COMPUTERS IN TEACHING, K.E. Iverson, 53 pp.

No. 14 LA CONJECTURE D'ARTIN SUR LES EQUATIONS DIOPHANTIENNES, P. Ribenboim, 160 pp.

No. 15 LECTURES ON ALGEBRAIC NUMBERS AND ALGEBRAIC FUNCTIONS, P.M. Cohn, 174 pp.

No. 16 CONFORMAL DEFORMATIONS OF RIEMANNIAN MANIFOLDS, S.I. Goldberg and W.C. Weber, 210 pp.

No. 17 COHOMOLOGY OF FINITE GROUPS, A. Babakhanian, 216 pp.

No. 18 ANALYSIS IN CATEGORIES, S. Takahashi 131 pp.

No. 19 FIRST PASSAGE TIME DISTRIBUTION OF BROWNIAN MOTION WITH POSITIVE DRIFT, (Inverse Gaussian Distribution), M.T. Wasan, 311 pp.

No. 20 HOMOLOGY OF LOCAL RINGS, T.H. Gulliksen, 200 pp.

No. 21 WHEN ARE PROJECTIVE MODULES FREE? A. Simis, 255 pp.

No. 22 QUADRATIC FORMS, W. Scharlau, 163 pp.

No. 23 AN INTRODUCTION TO LIE ALGEBRAS, R. Pollack, 264 pp.

No. 24 INTRODUCTION TO PROFINITE GROUPS AND GALOIS COHOMOLOGY, L. Ribes, 316 pp.

No. 25 PROCEEDINGS OF THE CONFERENCE ON UNIVERSAL ALGEBRA October 1969, Papers by: G. Grätzer, R.S. Pierce, B. Banaschewski, R. Balbes, D. Tamari, P. Dwinger, K.B. Lee, M. Gould, D. Haley, G.H. Wenzel, 275 pp.

No. 26 MATHEMATICAL ASPECTS OF LIFE SCIENCES, Papers by: Z.A. Malzak, R. Theodorescu, P.S. Puri, J.J. Gart, W.M. Siebert, R.S. Shirley, Abstracts of Contributed Papers, Edited by M.T. Wasan, 255pp.

No. 27 A SURVEY OF OPERATOR ALGEBRAS, I. Kaplansky; THE OPENING OF JEFFERY HALL, R.L. Jeffery and A.J. Coleman THE RESPONSIBILITY OF THE SCIENTIST TODAY, A. Grothendieck; 130 pp.

No. 28 EQUIMEASURABLE REARRANGEMENTS OF FUNCTIONS, K.M. Chang and N.M. Rice, 177 pp.

No. 29 DIFFERENTIALS OF COMMUTATIVE RINGS, S. Suzuki, 162 pp.

No. 30 MATHEMATICAL PROBABILITY, M.T. Wasan

No. 31 CLASSICAL HAMILTONIAN LINEAR SYSTEMS, A. Ciampi, 116 pp.

No. 32 RESOLUTIONS IN ADDITIVE AND NON-ADDITIVE CATEGORIES, H. Kleisli, 209 pp.

No. 33 MONADS AND THEIR EILENBERG - MOORE ALGEBRAS IN FUNCTIONAL ANALYSIS, Z. Semadeni, 98 pp.

No. 34 CW-COMPLEXES, HOMOLOGY THEORY, A. Piccinini, 129 pp.

No. 35 SYSTEMES DE POLYNOMES, A. Robert, 108 pp.

No. 36 REPORT OF THE ALGEBRA GROUP, September 1972 - August 1973, edited by P. Ribenboim and A.V. Geramita, 351 pp.

No. 37 RADICAL AND SEMISIMPLE CLASSES OF RINGS, R. Wiegandt, 248 pp.

No. 38 OPERATOR THEORY OF PSEUDO-INVERSE, S.R. Caradus, 67 pp.

No. 39 AN INTRODUCTION TO STOCHASTIC PROCESSES, M.T. Wasan, 598 pp.

No. 40 REDUCED DENSITY OPERATORS WITH APPLICATION TO PHYSICAL AND CHEMICAL SYSTEMS, Vol. II, R.M. Erdahl, 234 pp.

No. 41 REPORT OF THE ALGEBRA GROUP - September 1973-August 1974, edited by P. Ribenboim and A.V. Geramita, 306 pp.

No. 42 CONFERENCE ON COMMUTATIVE ALGEBRA, A.V. Geramita (editor) July 7-11, 1975, 268 pp.

No. 43 INTRODUCTION TO HOMOLOGICAL METHODS IN COMMUTATIVE RINGS, A. Geramita & C. Small, 352 pp.

No. 44 INTRODUCTION TO ALGEBRAIC GEOMETRY THROUGH AFFINE ALGEBRAIC GROUPS, A. Robert, 298 pp.

No. 45 INTRODUCTION TO MODULAR FORMS, A. Robert, 98 pp.

No. 46 CONFERENCE ON QUADRATIC FORMS, August 1-21, 1976, G. Orzech (editor). 656 pp.

No. 47 AN EXPOSITION OF CATASTROPHE THEORY AND ITS APPLICATIONS TO PHASE TRANSITIONS, Donal B. O'Shea, 200 pp.

No. 48 LIE THEORIES AND THEIR APPLICATIONS (Proceedings of the 1977 Annual Seminar of the Canadian Mathematical Congress), W. Rossmann (editor), 577 pp.

No. 49 AN INTRODUCTION TO HOMOTOPY THEORY VIA GROUPOIDS AND UNIVERSAL CONSTRUCTIONS, P.R. Heath, 118 pp.

No. 50 GENERALIZED INVERSES AND OPERATOR THEORY, S.R. Caradus, 206 pp.

No. 51 ADAMS COMPLETION AND ITS APPLICATIONS, Sribatsa Nanda, 57 pp.

No. 52 TRANSCENDENCE METHODS, Michel Waldschmidt, 132 pp.

QUEEN'S PAPERS IN PURE AND APPLIED MATHEMATICS

may be purchased from:

Campus Bookstore
Queen's University
Kingston, Ontario
K7L 3N6 Canada