BULLETIN DE LA S. M. F.

SERGE LANG

Report on Diophantine approximations

Bulletin de la S. M. F., tome 93 (1965), p. 177-192

<http://www.numdam.org/item?id=BSMF_1965__93__177_0>

Bull. Soc. math. France,
93, 1965, p. 177 à 192.

REPORT ON DIOPHANTINE APPROXIMATIONS (*);

BY

SERGE LANG.

The theory of transcendental numbers and diophantine approximations has only few results, most of which now appear isolated. It is difficult, at the present stage of development, to extract from the literature more than what seems a random collection of statements, and this causes a vicious circle : On the one hand, technical difficulties make it difficult to enter the subject, since some definite ultimate goal seems to be lacking. On the other hand, because there are few results, there is not too much evidence to make sweeping conjectures, which would enhance the attractiveness of the subject.

With these limitations in mind, I have nevertheless attempted to break the vicious circle by imagining what would be an optimal situation, and perhaps recklessly to give a coherent account of what the theory might turn out to be. I especially hope thereby to interest algebraic geometers in the theory.

1. Measure theoretic results.

Let α be a real number. We denote by $\| \alpha \|$ its distance from the origin on $\mathbf{R}/\mathbf{Z}$ (reals mod 1), i. e. its distance from the closest integer. If q is an integer, then

$$\| q\alpha \| = | q\alpha - p |$$

for some integer p, uniquely determined if this absolute value is small enough.

We begin by quoting an old result of Dirichlet.

Let α be a real number and N a positive integer. There exists an integer q, $0 < q \leq N$ such that $\| q\alpha \| < 1/q$.

(*) This work was partially supported by the National Science Foundation under Grant NSF GP-1904.

To prove this, cut up the interval $(0, 1)$ into N equal segments of length $1/N$, and consider the $N+1$ numbers

$$0\alpha, \quad 1\alpha, \quad 2\alpha, \quad \ldots, \quad N\alpha.$$

Two of them must lie in the same segment (mod 1), say $r\alpha$ and $s\alpha$ with $r < s$. We put $q = s - r$ to get

$$\| q\alpha \| < \frac{1}{N} \leqq \frac{1}{q}.$$

We note that the inequality $|q\alpha - p| < 1/q$ is equivalent with

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

We are interested in estimates of $\| q\alpha \|$ determined somewhat more generally as follows. Let ψ be a positive function of a real variable, monotone decreasing to 0. A theorem of KHINČIN asserts :

Assume that

$$\sum_{q=1}^{\infty} \psi(q)$$

converges. Then for almost all $\alpha \in \mathbf{R}$ (i. e. *outside a set of measure* 0), *there is only a finite number of solutions to the inequality*

$$\| q\alpha \| < \psi(q).$$

Here again, the proof is quite simple. Given $\varepsilon > 0$, select q_0 such that

$$\sum_{q \geqq q_0}^{\infty} \psi(q) < \varepsilon.$$

We may restrict our attention to those numbers α lying in the interval $(0, 1)$. Consider those for which the inequality has infinitely many solutions. For each $q \geqq q_0$, consider the intervals of radius $\psi(q)/q$, surrounding the rational numbers

$$\frac{0}{q}, \quad \frac{1}{q}, \quad \ldots, \quad \frac{q-1}{q}.$$

Every one of our α will lie in one of these intervals because for such α we have

$$\left| \alpha - \frac{p}{q} \right| < \frac{\psi(q)}{q}.$$

The measure of the union of these intervals is bounded by the sum

$$\sum_{q \geq q_0} q \frac{2\psi(q)}{q} < 2\varepsilon$$

as was to be shown.

Suppose thirdly that the sum $\sum \psi(q)$ diverges. Then we have the following recent theorem of Schmidt [9] :

For almost all α the number of solutions $\lambda(B)$ for the inequality $\| q\alpha \| < \psi(q)$ with $0 < q \leq B$ is given asymptotically by

$$\lambda(B) \sim c_1 \sum_{q=1}^{B} \psi(q).$$

for some constant $c_1 > 0$. (One can in fact take $c_1 = 2$ for almost all numbers.)

The proof is too long to be given here.

The main object of the theory of diophantine approximations is to determine a wide class of numbers, which may be called classical numbers, which will behave like almost all numbers. We shall now proceed to discuss such a class.

2. Classical numbers.

The classical numbers are essentially those which appear as values of classical functions or mappings, (e. g. exponential, automorphic, zeta, spherical, solutions of classical differential equations, etc.) with algebraic arguments, and similarly for their inverse functions, under suitable normalizations. The above mentioned functions are to be taken in an extended sense, e. g. Γ-functions and Γ'/Γ are to be viewed as functions of zeta type. Abelian functions are to be viewed as functions of exponential type. One must also deal with iterations of these functions, say to deal with numbers like e^e and α^β.

In a classical situation, one meets an open subset U of some complex space and a map $f: U \to V$ of U into an algebraic variety, defined over a number field. We shall give examples below, with suitable normalizations, and recall as we go along certain classical transcendence results.

EXAMPLES :

(i) Let $f: \mathbf{C} \to \mathbf{C}^*$ be given by $f(t) = e^t$. Here $\mathbf{C}^*$ is the multiplicative group, and a classical theorem of Hermite-Lindemann asserts that if α is algebraic $\neq 0$ then e^α is transcendental. The inverse function of f is the ordinary log.

(ii) Let $f: \mathbf{C}^n \to A_{\mathbf{C}}$ be the universal covering map of an abelian variety A defined over a number field. (One may realize f explicitly by theta functions.) We normalize f so that the origin in $\mathbf{C}^n$ maps on the origin on A, and so that the derivative $f'(0)$ at the origin is algebraic. It is known that if P is algebraic $\neq 0$ in $\mathbf{C}^n$, then $f(P)$ is a transcendental point on A [3]. The inverse map of f is given by abelian integrals.

(iii) Let V be a non-singular curve of genus $\geqq 2$ defined over a number field, and let U be a disc, centered at the origin in $\mathbf{C}$. Let $f: U \to V_{\mathbf{C}}$ be the universal covering map, normalized so that the origin goes to an algebraic point, and again $f'(0)$ is algebraic. One conjectures that if P is an algebraic point of the disc, $\neq 0$, then $f(P)$ is transcendental. As a side question (already related to moduli), one can ask if the radius of the disc is transcendental, and whether the radius can be defined as some real function on a suitable moduli space.

(iv) Let $f: S^n \to V$ be the moduli mapping from the Siegel upper half space to the variety of moduli. The fact that f represents the moduli normalizes it automatically. In dimension 1, one represents f explicitly by the modular function j. We recall that if τ is algebraic and the abelian variety associated with $j(\tau)$ has no complex multiplication, then $f(\tau) = j(\tau)$ is transcendental (SCHNEIDER).

(v) Let J_λ be the Bessel function with an algebraic parameter λ, and take $f = (J_\lambda, J'_\lambda)$, so that $f: \mathbf{C} \to \mathbf{C}^2$ is the integral curve of a differential equation, normalized so that the initial conditions are algebraic and the coefficients of the equation are rational functions with algebraic numbers as coefficients. We recall that if λ is such that J_λ, J'_λ are algebraically independent (as functions over the field of rational functions), then $J_\lambda(\alpha)$ and $J'_\lambda(\alpha)$ are algebraically independent for any algebraic $\alpha \neq 0$ (SIEGEL). It is natural here to view $\mathbf{C}^2$ as an algebraic variety with an algebraic differential equation over it.

Some of the above examples satisfy a differential equation and some do not, but all would be accepted as " classical ".

We shall now show how, given a classical mapping, we can generate a field of numbers with it.

Let f be a mapping as above and let Ω be the smallest field generated from the rational numbers by performing the following operations inductively, and iterating them :

Taking algebraic closure.

Adjoining values of f and its inverse function with the argument in the field obtained inductively after a finite number of steps.

We are concerned with the numbers of Ω from the point of view of diophantine approximations. We note that Ω is denumerable as would

be any field generated in a manner similar to the one we have described. We now expect (real) irrational numbers in Ω to behave like almost all numbers, with respect both to the second and third results recalled in paragraph 1. For this, one must make certain obvious restrictions on the function ψ, and we shall discuss these in the next section.

Here we make further remarks concerning known results and evidence in the direction of our expectations.

Liouville numbers do not behave like almost all numbers, and there are non-countably many of these.

A set of measure 1 on the unit circle (normalized to have length 1) is such that its sum with itself is the whole circle. For a moment, let us define a number to be *ordinary* if there is only a finite number of solutions to the standard inequality

$$\| q\alpha \| < \frac{1}{q^{1+\varepsilon}}$$

for every $\varepsilon < 0$. Then from the above remark, we see that ordinary numbers cannot form a field. Hence the fact that we deal with a field is essentially dependent on the manner of generating our numbers. We note that it is not known whether, if all elements of a field are ordinary, then the elements of its algebraic closure are ordinary. For the rational numbers, this is Roth's theorem. It is likely, however, that to prove such a result in general, one has to make a stronger assumption on the field elements, i. e. one has to load the hypothesis.

Since we wish to iterate our functions (or mappings), there should be some kind of inductive results, which, assuming that certain approximation properties are satisfied by all numbers of a certain field, similar properties are satisfied by those obtained in one of the two ways described above, starting with the given field. In particular, applying one of our two operations to the numbers of our given field, the conjecture asserts in particular that we cannot obtain a Liouville number as a value. To obtain a inductive result, it will be necessary to deal with a loaded inductive assumption, involving what is commonly known as a measure of lineari ndependence. We shall discuss this below. As special cases, one could consider the fields $\mathbf{Q}(e)$ or $\mathbf{Q}(\pi)$.

We note that it is hard to predict if one must make some restriction in the generation of a field Ω with respect to maxing mappings of various " types ", for instance, applying an exponential function to the value of a zeta function, or considering a number like $e + \zeta(3)$. For definiteness, one may therefore take a special case, letting Ω be the field generated by values of e^t and $\log t$, and their iteration, starting with the algebraic numbers. In some sense, this should also be the simplest case to treat.

3. The convergent case.

Let us now consider more closely a number α in our field Ω.

Generally speaking, it is a problem to determine a class of functions ψ (convex, monotone decreasing to 0 with convergent sum) such that the inequality

$$0 < \| q\alpha \| < \psi(q)$$

has only a finite number of solutions. Very few results are known. We shall make a list of them.

To begin with, we have Roth's theorem, taking α algebraic and $\psi(q) = 1/q^{1+\varepsilon}$ for any $\varepsilon > 0$. Taking such a ψ is in a sense the coarsest way of making the series converge.

It is an old theorem of Popken that e satisfies a similar result, and even a stronger one, namely there exists an absolute constant c' such that for all sufficiently large integers q,

$$\| qe \| > q^{-1-\frac{c'}{\log\log q}}.$$

In fact, Popken's theorem asserts that if $q_1, \ldots, q_m$ are integers and $q = \max |q_i|$ is sufficiently large, then

$$\| q_1 e + \ldots + q_m e^m \| > q^{-m-\frac{c'}{\log\log q}}$$

(c' then depends on m).

This result was improved by MAHLER. *I have analysed Mahler's proof* (reproduced in SCHNEIDER [11]), *and observed that the proof applies to the numbers* e^α with α rational $\neq 0$. When α is irrational algebraic, one obtains a result depending on the degree of α, and this leads one to hope that a mixture of the Thue-Siegel-Roth techniques with those techniques used in the theory of transcendental numbers might lead one to stronger results. In other words, one must consider an approximating sequence, and argue combinatorially on this sequence.

In this connection, SIEGEL himself observes that for the *Bessel function, the inequality*

$$\| q_1 J_0(\alpha) + q_2 J_0'(\alpha) \| < \frac{1}{q^{2+\varepsilon}}$$

has only a finite number of solutions whenever α *is rational,* $\neq 0$, and similarly for a polynomial in $J_0(\alpha)$, $J_0'(\alpha)$ [12]. Here again, the problem is open for algebraic α, or when one deals with J_λ, and λ is algebraic irrational. SIEGEL also mentions the analogous result for e, and linear combinations of powers of e. *We note in passing that the finiteness property for the inequality*

$$\| qJ_0(\alpha) \| < \frac{1}{q^{1+\varepsilon}}$$

has not yet been proved. Siegel's method does not give it as it stands.

For numbers of type α^β (with α, β algebraic, $\alpha \neq 0, 1$ and β irrational), or for values of $\wp$-functions with algebraic g_2, g_3, or their inverse functions with algebraic arguments, one has only a much weaker result, of the following type : If ξ is a number of the kind just mentioned, then GELFOND and FELDMAN [2] have shown that

$$\| q\xi \| > \frac{c_1}{q^{(\log q)^{2+\varepsilon}}}.$$

It seems clear to me, however, that all the above results point to the same direction, i. e. the finiteness statement as for almost all numbers with the function $\psi(q) = 1/q^{1+\varepsilon}$.

For more general functions ψ, the situation is more complicated. First, let ξ be a number with the following property :

(★) *There exists a constant $c > 0$ such that for all integers $q > 0$ we have*

$$\| q\xi \| > \frac{c}{q}.$$

Then for any monotone decreasing ψ such that $\sum \psi(q)$ converges, the inequality

$$\| q\xi \| < \psi(q)$$

has only a finite number of solutions.

Proof. — Suppose that ψ is a monotone decreasing function such that $\psi(q) > 1/q$ for infinitely many q, say $q_1 < q_2 < \ldots$. Then we contend that $\sum \psi(q)$ diverges. Indeed, let us make ψ smaller by supposing that

$$\psi(q) = \frac{1}{q_n}$$

for $q_{n-1} < q \leq q_n$. Then

$$\sum \psi(q) \geqq \frac{1}{q_1} + (q_2 - q_1)\frac{1}{q_2} + (q_3 - q_2)\frac{1}{q_3} + \ldots.$$

Take $n = n_1$ large. The first n terms of this series have a lower bound given by

$$(q_2 - q_1)\frac{1}{q_n} + \ldots + (q_n - q_{n-1})\frac{1}{q_n} = \frac{q_n - q_1}{q_n}.$$

Thus for n large, we get a contribution $> 1/2$ to our sum. We repeat this procedure with a number n_2 which will give a contribution greater than

$$\frac{q_{n_2} - q_{n_1}}{q_{n_2}} > 1/2$$

to our sum, and so on with n_3, ... In this manner, we see that the sum diverges.

S. SCHANUEL *has pointed out to me that the converse is also true,* i. e. *if* α *is a number such that for every smooth convex monotone decreasing function* ψ *with convergent sum the inequality*

$$\| q\alpha \| < \psi(q)$$

has only a finite number of solutions, then α *satisfies* (★).

To prove this, SCHANUEL argues as follows. Suppose α does not satisfy (★). Then we can find a sequence of integers q_i, with $1 < q_1 < q_2 < \ldots$ such that $\| q_i\alpha \| < 1/2^i q_i$. Let

$$\psi(t) = \sum \frac{e}{2^i q_i} e^{-\frac{t}{q_i}}.$$

Then $\psi(q_j) > 1/2^j q_j$, and the sum (or integral) for ψ converges. This achieves what we wanted. (Also, Schanuel's function is as good as possible from the point of view of convexity.)

It is a problem to determine specific numbers which have, and have not, property (★). It is trivial to prove that quadratic numbers have this property, and hence behave maximally well in the convergent case. It is unknown whether any other algebraic numbers (irrational) have the property.

One is thus faced with a problem in two directions concerning the finiteness statement : For which numbers does it apply, and for what class of functions ψ.

We note that the set of numbers satisfying (★) has measure 0, and so the description of functions ψ for which the finiteness statement holds appears as subtle. If the general philosophy that classical numbers behave like almost all numbers holds in the present instance, then one would expect only the real quadratic numbers among them to satisfy (★). Admittedly, the range in which one tries to guess the answer here is delicate.

It is already clear from the ideas of the Thue-Siegel-Roth proof that in a certain sense, the difficulty of extending the proof to the usual transcendental numbers does not lie so much in the transcendentality as in an intrinsic weakness of the structure of the proofs, even for algebraic numbers. That such a weakness exists is clear, since the proof is unable to decide whether algebraic numbers satisfy property (★), or if they satisfy the finiteness property with respect to a function like $\psi(q) = 1/q(\log q)^{1+\varepsilon}$.

It is therefore necessary to start investigations of the theory from the beginning, and to have essentially completely new ideas which would exhibit the finiteness by means of a more canonical combinatorial treatment of the approximating sequence.

4. Asymptotic approximations.

Suppose that ψ is smooth, convex, strictly decreasing to 0 (for sufficiently large numbers), and that its integral to infinity diverges. Modulo an additional restriction on ψ which will be discussed below, one expects that *for all classical numbers* α (*real and irrational*), *the number* $\lambda(B)$ *of solutions of the inequality*

$$\| q\alpha \| < \psi(q), \qquad 0 < q \leq B$$

is given asymptotically by

$$\lambda(B) \sim c_1 \int_1^B \psi(t)\, dt,$$

with some constant c_1 (possibly depending on α, ψ).

That some restriction is needed on ψ is clear from the possibility of property ($\bigstar$). We are thus led to introduce the function

$$\omega(t) = t\,\psi(t).$$

If ($\bigstar$) is satisfied, one must then assume that ω is not decreasing to 0. Furthermore, it is entirely reasonable to require that ω is not oscillating, and is itself convex. It is then naturel to split the theory into two cases, according as ω is constant, or strictly increasing to infinity (for all sufficiently large t). When we take ω constant, we must assume that there actually exist infinitely many solutions for the inequality

$$\| q\alpha \| < \frac{\omega(t)}{t},$$

so that for definiteness, one may take $\omega(t) = c \geq 1$. There are various ways of preventing ω from oscillating.

Actually, it is not clear if there is an *a priori* characterization of those functions ψ for which everything works out as expected. However, one expects all reasonable functions (built up out of exponentials, logs, essentially the elementary functions in a finite number of steps) to be acceptable, provided there is no oscillation. The point is that any idea for a proof will carry with it an explicit error term which will determine automatically the range of validity of the asymptotic estimate.

This is in fact precisely the situation which occurs in [8] *where the expected theorem is proved for quadratic irrationalities* (*real*), with a definite error term which shows the estimate to be good when ω is a

power of the log, or iterated logs (i. e. ω can grow quite slowly). However, the estimate is not valid for all ω.

Even for quadratic irrationalities, the problem is open when $\omega(t) = t^{\delta}$ with $0 < \delta < 1$. When $\omega(t) = ct$ with $0 < c < 1$, then the situation is the classical one of equidistribution, and the answer is known. There exist several papers dealing with it by HECKE, BEHNKE, HARDY-LITTLEWOOD, etc. (cf. *Abhandl. math. Sem. Hamburg. Univ.*, t. 1, 1922 et t. 2, 1923).

Some machine computations for a few classical numbers (e, π, $e + \pi$, $\log 2$, $\log 3$, γ) tend to support the present conjecture [1]. In any case, the classical transcendental numbers seem to be no different from the present point of view than the algebraic numbers. It should also be pointed out that no paper had considered the asymptotic problem for specific numbers previous to [8].

5. **Generalizations.**

Let $\alpha_1, \ldots, \alpha_m$ be (real) numbers in our field Ω. Then one may study the inequality

$$\| q_1\alpha_1 + \ldots + q_m\alpha_m \| < \frac{1}{q^m}$$

or

$$\| q_1\alpha_1 + \ldots + q_m\alpha_m \| < \psi(q),$$

with a suitable function ψ, subject to similar restrictions as before. Here we put $q = \max |q_i|$, and the exponent m generalizes the exponent 1 considered previously. Similarly, the convergence condition now applies to the sum of $\psi(q)$ taken for all m-tuples $(q_1, \ldots, q_m)$, with $\max |q_i| \leqq B$.

If the sum converges, then one expects a finite number of solutions for the inequality

$$0 < \| q_1\alpha_1 + \ldots + q_m\alpha_m \| < \psi(q).$$

If the sum diverges, and if $1, \alpha_1, \ldots, \alpha_m$ are linearly independent over the rationals, or equivalently, linearly independent mod $\mathbf{Z}$ on the circle, then one expects the usual asymptotic estimate for the number of solutions of the inequality

$$\| q_1\alpha_1 + \ldots + q_m\alpha_m \| < \psi(q), \qquad 0 < q \leqq B.$$

(Cf. SCHMIDT's paper again for the corresponding theorem holding almost everywhere.)

In the present context we therefore see the theory of transcendental numbers as determining which classical numbers are linearly independent or alge-

braically independent, and the theory of diophantine approximations then gives quantitative results concerning such numbers. Quantitative results are known as measures of linear independence or measures of transcendence. If α is a classical transcendental number, then one may put

$$\alpha_i = \alpha^i,$$

and a measure of linear independence for $\alpha, \ldots, \alpha^m$ becomes a measure of transcendence for α.

One can also work on the torus. Let L be a lattice in $\mathbf{R}^n$, having a basis whose elements consist of vectors with coordinates in our field Ω. For any vector X in $\mathbf{R}^n$, define $\| X \|$ to be its distance from the origin on the torus $\mathbf{R}^n/L$. One then considers the inequality

$$0 < \| q_1 X_1 + \ldots + q_m X_m \| < \psi_{m,n}(q)$$

with a suitable function $\psi_{m,n}$. This is a problem in simultaneous approximations of vectors.

As stated above, the problem is on $\mathbf{R}^n$. However, it has applications to elliptic curves and abelian varieties [6]. For instance, if A is an abelian variety defined over a number field K, and $f: \mathbf{C}^n \to A_{\mathbf{C}}$ is as in Example (ii) of paragraph 2 the representation of $A_{\mathbf{C}}$ as a quotient of the universal covering space, then we may identify $\mathbf{C}^n$ with $\mathbf{R}^{2n}$. If $P = f(X)$, we also write $X = \log P$. Taking $P_1, \ldots, P_m$ points of A_K (i. e. algebraic points) linearly independent over $\mathbf{Z}$, we see that the approximation question concerning

$$\| q_1 P_1 + \ldots + q_m P_m \| < \psi_{m,n}(q)$$

becomes equivalent with an approximation as described above, with vectors X_i having transcendental coordinates. A similar situation exists with respect to the multiplicative group [6], and one obtains in this way generalizations of statements of SIEGEL and MAHLER in diophantine geometry, concerning integral points (*cf.* for instance [5], Corollary of Theorem 1, Chapter VI, § 1 and Theorem 1 of Chapter VII, § 1). For instance, the theorem in diophantine approximations needed to prove Siegel's finiteness of integral points on curves of genus ≥ 1 over number fields, is the following :

Let V be a complete non-singular curve of genus ≥ 1 defined over a number field K. Let g be a non-constant rational function in $K(V)$. Let I_K be the ring of algebraic integers of K. Let $c > 0$. Then the set of points P in V_K which are not poles of g and such that

$$| g(P) | \leq \frac{1}{H(P)^c}$$

is finite.

For elliptic curves, the inhomogeneous analogues of conjectures expressed in this paper would imply the finiteness only under the assumption that

$$|g(P)| \leq \frac{1}{(\log H(P))^{\frac{rm}{2}+\varepsilon}}$$

where r is the maximum of the multiplicities of the zeros of g, m is the rank of A_K, and H is the height in a fixed projective embedding.

I cannot resist mentioning other applications to diophantine geometry. In [5], I have proved the following statement : Let Γ_0 be a finitely generated multiplicative group of complex numbers, say. Let $f(X, Y) = 0$ be the equation of a curve (irreducible) and assume that there exist infinitely many points (x, y) such that $x, y \in \Gamma_0$ and $f(x, y) = 0$. Then f has a " multiplicative " structure, i. e. there exist integers $n, m \neq 0$ and non-zero constants a, b such that we have identically $f(at^n, bt^m) = 0$. It follows then easily that f consists of at most two monomials.

As a special case, it follows that *if g is a rational function with complex coefficients, and if there exist infinitely many elements $x \in \Gamma_0$ such that $g(x) \in \Gamma_0$ then g is of type aX^n for some integer n and some constant a.*

The proof uses the ideas of Siegel's theorem, combined with an additional combinatorial argument on coverings. Thus in effect, the proof depends on the above-mentioned result in diophantine approximations.

Let Γ be the multiplicative group of complex numbers z such that some integral power z^m lies in Γ_0 (some $m \neq 0$). *I would conjecture that the same results as above hold when Γ_0 is replaced by Γ.* As a special case, one has the following very elementary statement :

Let g be a rational function with complex coefficients, and assume that there exist infinitely many roots of unity ζ such that $g(\zeta)$ is a root of unity. Then g is of type $g(X) = aX^n$ for some integer n, and some root of unity a.

A proof for this last statement was shown to me by Ihara, Serre and Tate. We can reformulate and generalize the above statements as follows :

Let A be a group variety in characteristic 0 which is either an abelian variety or a product of multiplicative groups, or a group extension of an abelian variety by such a product. Let Γ_0 be a finitely generated subgroup, and let Γ be the subgroup of points $x \in A$ such that there exists an integer $n \neq 0$ such that $nx \in \Gamma_0$. Let V be an irreducible algebraic curve in A, and assume that the intersection of V with Γ is infinite. Then V is the translation of a group subvariety.

The above formulation implies the Mordell conjecture, as pointed out in [5]. It also implies a conjecture of Mumford, who, a few years ago, asked me the following question : If a curve embedded in its Jacobian

contains infinitely many points of finite order, is the curve of genus 1 ? (The question was also raised independently by MANIN in his work on Picard-Fuchs equations. MANIN pointed out that although it takes infinitely many algebraic equations to define the points of finite order on an abelian variety, it takes only a finite number of differential equations.) The question concerning our polynomial $f(X, Y)$ and roots of unity is the analogous question for the multiplicative group. As an example, one always has the straight line $X + Y = 1$. The theorem proved in [5] shows that this line contains only a finite number of points whose coordinates lie in a finitely generated multiplicative group.

Other generalizations are possible. One can consider approximations $|q\alpha - p|$ where q, p lie in a number field K, and similarly for

$$q_0\alpha_0 + \ldots + q_m\alpha_m.$$

One lets q be the height of the point $(q_0, \ldots, q_m)$ in projective space. When dealing with points on abelian varieties, one could let the q_i range over the ring of endomorphisms.

Finally, one can ask for approximations questions on group varieties and homogeneous spaces or transformation spaces, defined over number fields. For instance let G be a group variety and V a homogeneous space defined over the number field K. Let x_0, y_0 be points of V with coordinates in our field Ω. One can then ask for those points $g \in G$, rational over K, such that dist $(gx_0, y_0) < \psi(g)$, where dist is the distance in a suitably normalized metric on V, and ψ is a function of the height of g. When G operates on itself by translation, and is commutative, we are led to considering an inequality

$$\text{dist}(x, x_0) = \| x_0 - x \| < \psi(x)$$

which looks formally like the inequality that is usually written down in the simplest case of approximation on the circle. This gives rise to homogeneous or inhomogeneous approximation problems in globalized setting, on linear groups or abelian varieties.

6. **Relation with transcendental numbers.**

We shall conclude this report by pointing out a more technical connection between the theory of diophantine approximations, and the theory of transcendental numbers, due to GELFOND, whose result is as follows.

THEOREM. — *Let σ be a strictly monotone increasing real function tending to infinity, and assume that there is a number $a_0 > 1$ such that $\sigma(N+1) < a_0\sigma(N)$ for all integers $N > N_0$. Let w be a complex*

number. Assume that for each integer $N > N_0$ there exists a non-zero polynomial F_N with integer coefficients such that

$$|F_N(w)| < e^{-C\sigma^2(N)}$$

where $C = 50\, a_0^2$, and

$$\max(\deg F_N, \log|F_N|) \leqq \sigma(N),$$

Then w is algebraic.

As usual, $|F_N|$ denotes the maximum of the absolute value of the coefficients. Since in his book [2], GELFOND gives the proof of a weaker result, it is worth while to summarize roughly the argument here. First one proves that if F is a polynomial in one variable with integer coefficients, relatively prime, and σ, C are numbers > 0 such that

$$|F(w)| < e^{-\sigma^2 C}$$

and $\deg F < \sigma$, $\log|F| < \sigma$, then there exists an irreducible factor P of F (with integer coefficients) such that

$$|P(w)| < e^{-\frac{\sigma^2 C}{2s}}$$

with some integer $s \leqq \sigma$, and $\max(\deg P, \log|P|) \leqq \sigma/s$.

The proof proceeds first by factoring F into relatively prime polynomials which are powers of irreducible polynomials, and using the estimate given by the resultant of the factors expressed as a determinant. One sees that each factor must have a small absolute value, and then one takes some s-th root with $s \leqq \sigma$.

To prove the theorem, one can then assume the coefficients of each F_N to be relatively prime, and $F_N(w) \neq 0$. Given a sufficiently large integer q (say $q > q_0$) we can find an irreducible factor P_q of F_q such that

$$|P_q(w)| < e^{-\frac{\sigma^2(q)C}{2s}}$$

with some integer $s \leqq \sigma(q)$, and

$$\max(\deg P, \log|P_q|) \leqq \frac{1}{s}\sigma(q).$$

Let x_q be the number such that

$$\sigma(x_q) = \max(\deg P_q, \log|P_q|).$$

Then x_q goes to infinity with q, and trivially

$$|P_q(w)| < e^{-\frac{\sigma^2(x_q)G}{2s}}.$$

Now find an integer N such that

$$\sigma(N-1) < \frac{\sigma(x_q)}{4a_0} \leqq \sigma(N).$$

Then $\sigma(N) \leqq a_0\sigma(N-1) \leqq \sigma(x_q)/4$. Take $F = F_N$ so that

$$|F(w)| < e^{-\sigma^2(N)C}$$

and $\max(\deg F, \log|F|) \leqq \sigma(N)$. Then P_q and F are relatively prime. Otherwise P_q divides F, whence

$$\max(\deg P_q, \log|P^q|) < \sigma(x_q)$$

which is impossible.

The resultant R of P_q and F is not zero and is an integer. Using an easy estimate arising from the expression of the resultant as a determinant, we find

$$|R| \leqq [|P_q(w)| + |F(w)|]\, e^{3\sigma^2(x_q)}$$

for q large. In the estimate for $F(w)$, we can replace $\sigma(N)$ by $\sigma(x_q)/4a_0$ This makes the resultant less than 1, contradiction.

GELFOND, in his book, proves the result only with some function instead of the constant C. It is also easy to see that the theorem applies when one deals with a rational function or an algebraic function instead of a polynomial. This is useful when one deals with a function field other than the rational field.

We note that $\max(\deg F, \log|F|)$ is essentially a height function on polynomials, which measures the speed with which both the degree and the coefficients tend to infinity. The exponent σ^2 is the " correct " one in the optic of results holding almost everywhere. GELFOND applies his theorem to prove that certain numbers are algebraically independent. Indeed, under certain circumstances connected with values of exponential functions, one knows that a number w is transcendental, and one wants to prove that it is algebraically independent of another number y. Assuming the contrary, one can construct a sequence F_N as in the theorem to lead to a contradiction, thereby giving the algebraic independence of w and y.

I have tried to use Gelfond's method to prove that e, π are algebraically independent, but an application of known ideas in the theory leads to a sequence F_N satisfying an inequality weaker than the needed one (i. e. the exponent of σ is not quite 2.) Still, Gelfond's theorem gives a good approach to these questions.

One can conjecture a generalization, using a sequence of polynomials F_N in several variables, and an n-tuple of complex numbers $(w_1, \ldots, w_n)$. In that case, the conclusion should be that $w_1, \ldots, w_n$ are algebraically

dependent, provided that in Gelfond's inequality we take the exponent σ^{n+1} instead of σ^2, and the constant C depends only on σ and n (not on the chosen numbers).

If one tries to apply the theorem for one variable inductively, one obtains some result, but with an exponent for σ which is much too large to be of interest.

The possible generalization of Gelfond's theorem to several variables gives an interesting direction for the problem of diophantine approximations, when the degree of the polynomial varies, together with its coefficients. In the discussions of preceding sections, we kept the degree constant. The theory of transcendental numbers shows that the more general behaviour also has to be considered.

BIBLIOGRAPHY.

[1] ADAMS (W.) and LANG (S.). — *J. für reine und angewandte Math.* (to appear).

[2] GELFOND (A. O.). — *Transcendental and algebraic numbers.* — New York, Dover Publications, 1960 (Dover Books on advanced Mathematics).
[See the bibliography at the end for further references to GELFOND and FELDMAN'S papers.]

[3] LANG (S.). — Transcendental points on group varieties, *Topology*, Oxford, t. 1, 1962, p. 313-318.

[4] LANG (S.). — Algebraic values of meromorphic functions, *Topology*, Oxford (to appear).

[5] LANG (S.). — *Diophantine geometry.* — New York, Interscience Publishers, 1962 (Interscience Tracts in pure and applied Mathematics, 11).

[6] LANG (S.). — Diophantine approximations on toruses, *Amer. J. of Math.*, t. 86, 1964, p. 521-533.

[7] LANG (S.). — *Transzendenten Zahlen.* Lecture notes by W. Scharlau. — Bonn, 1964.

[8] LANG (S.). — Asymptotic approximations to quadratic irrationalities, *Amer. J. of Math.*, 1965 (to appear).

[9] SCHMIDT (W. M.). — A metrical theorem in diophantine approximation, *Canadian J. of Math.*, t. 12, 1960, p. 619-631.

[10] SCHMIDT (W. M.). — Metrical theorems on fractional parts of sequences, *Trans. Amer. math. Soc.*, t. 110, 1964, p. 493-518.

[11] SCHNEIDER (T.). — *Einführung in die transzendenten Zahlen.* — Berlin, Springer-Verlag, 1957 (Die Grundlehren der mathematischen Wissenschaften, 81).
[For references to Mahler, Siegel, Popken, cf. bibliography at the end of Schneider's book.]

[12] SIEGEL (C. L.). — Über einige Anwendungen diophantischer Approximationen, *Abhandl. Preuss. Akad. Wiss.*, 1929, n° 1, 70 pages. [*cf.* especially p. 28.]

(Manuscrit reçu le 7 janvier 1965.)

Serge LANG,
Professor,
Department of Mathematics,
Columbia University,
New York 27, N. Y. (États-Unis).