Michel Waldschmidt

Volume 326

Grundlehren
der mathematischen
Wissenschaften

A Series of
Comprehensive Studies
in Mathematics

DIOPHANTINE APPROXIMATION ON LINEAR ALGEBRAIC GROUPS

TRANSCENDENCE PROPERTIES OF THE EXPONENTIAL FUNCTION IN SEVERAL VARIABLES

线性代数群上的丢番图逼近

Springer

世界图书出版公司
www.wpcbj.com.cn

Michel Waldschmidt

Diophantine Approximation on Linear Algebraic Groups

Transcendence Properties of the Exponential Function in Several Variables

Springer

Michel Waldschmidt
Institut de Mathématiques de Jussieu
Université Pierre et Marie Curie (Paris VI)
Case 247
75252 Paris Cedex 05, France
e-mail: miw@math.jussieu.fr

Cataloging-in-Publication Data applied for

Die Deutsche Bibliothek - CIP-Einheitsaufnahme

Waldschmidt, Michel:
Diophantine approximation on linear algebraic groups : transcendence properties of the exponential function in several variables / Michel Waldschmidt. - Berlin ; Heidelberg ; New York ; Barcelona ; Hong Kong ; London ; Milan ; Paris ; Singapore ; Tokyo : Springer, 2000
(Grundlehren der mathematischen Wissenschaften ; 326)
ISBN 3-540-66785-7

Mathematics Subject Classification (1991):
11-02, 11Jxx, 14Lxx, 20Gxx, 33B10

ISSN 0072-7830

ISBN 3-540-66785-7 Springer-Verlag Berlin Heidelberg New York

Reprint from English language edition:
Diophantine Approximation on Linear Algebraic Groups
by Michel Waldschmidt
Copyright © Springer-Verlag Berlin Heidelberg 2000
Springer-Verlag Berlin Heidelberg is a part of Springer Science+Business Media
All Rights Reserved

图书在版编目（CIP）数据

线性代数群上的丢番图逼近 = Diophantine Approximation on Linear Algebraic Groups：英文/（法）瓦尔德施密特（Waldschmidt，M.）著．—影印本．—北京：世界图书出版公司北京公司，2015.6

ISBN 978－7－5100－9794－2

Ⅰ．①线…　Ⅱ．①瓦…　Ⅲ．①线性代数群—英文 ②丢番图逼近—英文
Ⅳ．①O187.2 ②O156.7

中国版本图书馆 CIP 数据核字（2015）第 121013 号

Diophantine Approximation on Linear Algebraic Groups
线性代数群上的丢番图逼近

著　　者：Michel Waldschmidt
责任编辑：刘　慧　岳利青
装帧设计：任志远

出版发行：世界图书出版公司北京公司
地　　址：北京市东城区朝内大街 137 号
邮　　编：100010
电　　话：010－64038355（发行）　64015580（客服）　64033507（总编室）
网　　址：http://www.wpcbj.com.cn
邮　　箱：wpcbjst@vip.163.com
销　　售：新华书店
印　　刷：三河市国英印务有限公司
开　　本：711mm×1245 mm　1/24
印　　张：27.5
字　　数：528 千
版　　次：2015 年 7 月第 1 版　　2015 年 7 月第 1 次印刷
版权登记：01－2015－2533
ISBN 978－7－5100－9794－2　　　　**定价**：98.00 元

Preface

A transcendental number is a complex number which is not a root of a polynomial $f \in \mathbb{Z}[X] \setminus \{0\}$. Liouville constructed the first examples of transcendental numbers in 1844, Hermite proved the transcendence of e in 1873, Lindemann that of π in 1882. Siegel, and then Schneider, worked with elliptic curves and abelian varieties. After a suggestion of Cartier, Lang worked with commutative algebraic groups; this led to a strong development of the subject in connection with diophantine geometry, including Wüstholz's Analytic Subgroup Theorem and the proof by Masser and Wüstholz of Faltings' Isogeny Theorem.

In the meantime, Gel'fond developed his method: after his solution of Hilbert's seventh problem on the transcendence of α^{β}, he established a number of estimates from below for $|\alpha_1^{\beta} - \alpha_2|$ and $|\beta_1 \log\alpha_1 - \log\alpha_2|$, where α_1, α_2 and β are algebraic numbers. He deduced many consequences of such estimates for diophantine equations. This was the starting point of Baker's work on measures of linear independence of logarithms of algebraic numbers. One of the most important features of transcendental methods is that they yield quantitative estimates related to algebraic numbers. This is one of the main reasons for which "there are more mathematicians who deal with the transcendency of the special values of analytic functions than those who prove the algebraicity"[1]. A first example is Baker's method which provides lower bounds for nonvanishing numbers of the form

$$\left|\alpha_1^{b_1} \cdots \alpha_m^{b_m} - 1\right|,$$

when $\alpha_1, \ldots, \alpha_m$ are algebraic numbers and $b_1, \ldots, b_m$ rational integers. Such estimates, which are of central interest, have a wide range of applications. A second important example is Schmidt's Subspace Theorem, which extends the Thue-Siegel-Roth Theorem to simultaneous diophantine approximation; its range of application is wider than Baker's Theorem, but, in contrast with Baker, Schmidt's result is so far not effective.

This subject is growing so fast that it is hard to give a report on the state of the art which covers all aspects. Our concern here is with *commutative linear algebraic groups*. A connected and commutative algebraic subgroup of GL_n splits over a finite extension; over an algebraically closed field it is a product of additive and multiplicative groups. Hence the algebraic groups we consider are $\mathbb{G}_{\mathrm{a}}^{d_0} \times \mathbb{G}_{\mathrm{m}}^{d_1}$, with

[1] G. Shimura, Duke Math. J. 44, No 2 (1977), p. 365.

$d_0 \geq 0$ and $d_1 \geq 0$. In terms of analytic functions, our main object of study is the usual exponential function. We discuss the qualitative as well as the quantitative aspects of the subject. The latter is not restricted to measures of linear independence of logarithms of algebraic numbers, but includes also simultaneous diophantine approximation results leading to statements of algebraic independence for values of the exponential function, in either one or several variables.

We do not consider elliptic curves, abelian varieties, and more generally nonlinear algebraic groups; we do not consider either elliptic functions, Weierstraß zeta functions, theta functions nor abelian functions. A lot of results in this book have already been extended to the more general set-up of commutative algebraic groups, but a few items are specific to the linear ones. An example of a feature particular to linear algebraic groups is the Fourier-Borel duality, which relates Gel'fond's method to Schneider's. Moreover, restricting ourselves to the linear case enables us to compute more easily all constants.

Among the recent developments of the subject is the introduction, by M. Laurent, of interpolation determinants. They replace the constructions of auxiliary functions. Instead of solving some system of equations, we only consider the determinant of a matrix corresponding to this linear system. There is no need any more to appeal to Dirichlet's box principle (or pigeonhole principle, alias Thue-Siegel's Lemma). Here, we use this approach in most proofs.

The above-mentioned matrix is associated to the linear system with respect to given bases. A further step has been performed by J-B. Bost, using Arakelov theory, where he considers directly the related linear map without selecting bases. This approach will certainly be more efficient for nonlinear algebraic groups, and we mention it in passing, but we do not follow it here.

A central result in this book is the *Linear Subgroup Theorem*, which occurs in two forms. The qualitative one (Chapter 11) is a lower bound for the dimension n of the $\mathbb{C}$-vector subspace of $\mathbb{C}^d$ spanned by points η whose coordinates are either algebraic numbers, or else logarithms of algebraic numbers. The images of such points η under the exponential map of some commutative linear algebraic group are algebraic over the field of algebraic numbers. Hence the Linear Subgroup Theorem deals with n-parameter subgroups of linear algebraic groups, and involves functions of n complex variables.

The quantitative version of the Linear Subgroup Theorem concerns the simultaneous approximation of such points η. Linear combinations of logarithms of algebraic numbers arise in several ways as special cases of this general setup.

The main conjecture is that linearly independent logarithms of algebraic numbers should be algebraically independent. As a matter of fact, so far all known partial results on this topic are consequences of the Linear Subgroup Theorem.

There is a strong contrast between the simplicity of the conjectures, both for qualitative and quantitative statements, and currently known results. A comparison between the conjecture on algebraic independence of logarithms (Conjecture 1.15) on one hand, the Linear Subgroup Theorem of Chapter 11 (Theorem 11.5) on the other, illustrates this point for the qualitative aspect. For the quantitative one, an example of this contrast is illustrated by comparing the known measures of linear independence of logarithms (Theorem 9.1) with the conjectural ones (Conjectures 1.11 and 14.25).

We very much expect that, once the theory is more highly developed, the results will be simpler to state, but we have far from reached this stage at present and the statements of the results of the last chapters are not as simple as we would wish. The quantitative version of the Linear Subgroup Theorem in Chap. 13 (Theorem 13.1) is by no means a simple statement; on the other hand it includes a lot of diophantine estimates, as shown in Chap. 14. The large amount of corollaries it contains may be an excuse for its lack of simplicity, but it remains a challenge to get simpler statements which are as powerful.

The first chapters may serve as an introduction to the subject of transcendental numbers. For instance the first three chapters do not require much preliminary knowledge and include already complete proofs of a number of classical transcendence results.

Three proofs of Baker's transcendence theorem on linear independence of logarithms of algebraic numbers are given: in Chap. 4 we follow an argument of Bertrand and Masser who derived Baker's Theorem from the Schneider-Lang criterion concerning algebraic values of meromorphic functions on Cartesian products. In Chap. 6 (and Chap. 9 for the nonhomogeneous case) we extend Schneider's method, and in Chap. 10 we explain Baker's argument which extends Gel'fond's solution of Hilbert's seventh problem. We give also several measures of linear independence of logarithms of algebraic numbers: a comparatively simple proof is given in Chap. 7, and refined estimates are proved in Chap. 9 and 10.

We do not consider applications of such estimates to diophantine equations, but we give further examples of diophantine approximation results (in Chap. 14) together with consequences (in Chap. 15). This last chapter deals with algebraic independence; it does not cover the subject in an exhaustive way; a more complete introduction to this topic is [NeP 2000], which includes transcendence criteria with proofs.

Several results presented here are new, and the full details have not appeared in print before.

Our emphasis is not only on the results, but also on the methods; this is why we give several proofs of the same results. In the same spirit, sometimes we also propose several choices of the parameters which occur in the transcendence arguments. It turns out that the freedom in this choice is closely related to the quality of the quantitative refinements: if the proof of the qualitative transcendence result can be achieved with a broad range of choice for the auxiliary parameters, then one should expect a sharp diophantine estimate.

Another goal is to describe some of the main tools which are available. We make no attempt to be complete. In [FNe 1998] the reader will find some items which are not discussed here. An important example of a missing item is Nesterenko's proof [Ne 1996] of the algebraic independence of π and e^{π}.

Writing this book took more than 10 years. The first written parts were notes of lectures given at the Institut Henri Poincaré in the 80's for several courses of the DEA (Diplôme d'Études Approfondies) of Mathématiques at the Université P. et M. Curie (Paris VI). In 1992, I was invited by R. Balasubramanian to give a series of lectures at the MathScience Institute of Madras, and I took this opportunity to write down a preliminary version of some of the chapters below (more or less the seven first chapters). These notes were published in [W 1992]. A chapter on zero estimates by D. Roy was included, as well as an appendix by M. Laurent [Lau 1994]. The present book grew out of these Lecture Notes; the material of the last eight chapters includes a multiplicity estimate (again written by D. Roy), the Linear Subgroup Theorem (both in qualitative and quantitative form), as well as results of simultaneous approximation and algebraic independence. Some of these results are due to D. Roy (like the Strong Six Exponentials Theorem of § 11.6), others (mainly in the last two chapters) have been obtained in joint papers with D. Roy.

The influence of Damien Roy on this book is important; not only did he write two chapters, but he also contributed to the proof of many results quoted in this book, and furthermore his many comments have been very influential.

Many other colleagues and friends also sent me comments, remarks and suggestions along the many years which have been needed to complete this book. Even though I do not mention them all, I am deeply thankful to them.

Special thanks are due to Guy Diaz who sent me a long list of comments on a preliminary version of this book. I wish also to express my gratitude to Francesco Amoroso, Yann Bugeaud, François Gramain, and Paul Voutier.

The help of Sinnou David during the last stage of the TEXnical preparation of this volume is also gratefully acknowledged.

We consider mainly the Archimedean situation; the same topic has been investigated in the ultrametric domain also, and this would have deserved consideration also. In fact my main motivation to study this subject arose from Leopoldt's Conjecture on the p-adic rank of the units of algebraic number fields (solved by Ax-Baker-Brumer for abelian extension). I wish to take this opportunity to thank Jean Fresnel, who suggested this topic to me thirty years ago, and helped me take my first steps in mathematical research.

Paris, January 2000 *Michel Waldschmidt*

Prerequisites

In this book, an *algebraic number* is a complex number which is algebraic over the field of rational numbers. Given a (commutative) ring A and a subring k which is a field, an element θ in A is *algebraic* over k if there exists a nonzero polynomial $P \in k[X]$ such that $P(\theta) = 0$. An element of A is *transcendental* over k if it is not algebraic over k. Hence a *transcendental number* is a complex number which is not algebraic.

We denote by $\mathbf{N} = \{0, 1, 2, \ldots\}$ the set of nonnegative integers, by $\mathbb{Z}$ the ring of rational integers and by $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ the fields of rational numbers, real numbers and complex numbers respectively.

The set of algebraic numbers is a subfield of $\mathbb{C}$: it is the algebraic closure of $\mathbb{Q}$ into $\mathbb{C}$ (see [L 1993], Chap. V § 2). This field will be denoted by $\overline{\mathbb{Q}}$. We shall need a few properties of algebraic numbers and number fields which will be recalled in Chap. 3.

Given elements $\theta_1, \ldots, \theta_n$ in our ring A, we say that they are *algebraically dependent over k* if there exists a nonzero polynomial $P \in k[X_1, \ldots, X_n]$ such that $P(\theta_1, \ldots, \theta_n) = 0$. Otherwise they are *algebraically independent over k*. The *transcendence degree* of A over k is the maximal integer n such that there exist n elements in A which are algebraically independent over k. We denote it by $\operatorname{trdeg}_k(A)$. For $k_1 \subset k_2 \subset k_3$, we have (see for instance [L 1993], Chap. VIII)

$$\operatorname{trdeg}_{k_1}(k_3) = \operatorname{trdeg}_{k_1}(k_2) + \operatorname{trdeg}_{k_2}(k_3).$$

Any element of k_2 is algebraic over k_1 if and only if

$$\operatorname{trdeg}_{k_1}(k_2) = 0;$$

in this case we say that k_2 is an *algebraic extension* of k_1. As a consequence, for complex numbers, the concept of algebraic independence over $\mathbb{Q}$ or over $\overline{\mathbb{Q}}$ is the same: we shall just speak of *algebraically dependent* or *independent* numbers.

We shall use the basic notions of linear algebra. The dimension of a k-vector space V will be denoted by $\dim_k(V)$, the rank of a $\mathbb{Z}$-module M by $\operatorname{rank}_{\mathbb{Z}}(M)$ or simply $\operatorname{rank}(M)$. An abelian group is nothing else than a $\mathbb{Z}$-module; when it is written multiplicatively, one speaks of *multiplicatively dependent* or *independent* elements (which means $\mathbb{Z}$-linearly dependent or independent elements in the abelian group). For instance if k is a field and $\gamma_1, \ldots, \gamma_m$ elements in $k^\times = k \setminus \{0\}$, then $\gamma_1, \ldots, \gamma_m$

are multiplicatively dependent if and only if there exists $\underline{b} = (b_1, \dots, b_m) \in \mathbb{Z}^m \setminus \{0\}$ such that the number

$$\underline{\gamma}^{\underline{b}} = \gamma_1^{b_1} \cdots \gamma_m^{b_m}$$

is 1.

The rank of a matrix M will be denoted rank(M): this is the largest integer r for which there exists a regular $r \times r$ submatrix of M.

For a ring B, a subring A and a subset E of B, we denote by $A[E]$ the subring of B generated by $A \cup E$, namely the intersection of all subrings of B containing A and E. For a field K, a subfield k and a subset E of K, we denote by $k(E)$ the subfield of K generated by k and E. When $E = \{\gamma_1, \dots, \gamma_m\}$ is finite, we write simply $A[\gamma_1, \dots, \gamma_m]$ and $k(\gamma_1, \dots, \gamma_m)$. In particular $\mathbb{Q}(\gamma)$ (resp. $\mathbb{Q}(\underline{\gamma})$) denotes the field generated by an element $\gamma \in \mathbb{C}$ (resp. by a tuple $\underline{\gamma} = (\gamma_1, \dots, \gamma_m) \in \mathbb{C}^m$).

For U and V vector spaces over a field k, $\mathrm{Hom}_k(U, V)$ will denote the space of k-linear mappings $U \to V$.

The basic facts from algebraic geometry and commutative algebra which are needed are recalled in §§ 5.2 and 8.2 respectively.

A useful tool is *Dirichlet's box principle*, also called *Dirichlet's pigeonhole principle* (Schubfachprinzip). One of the many equivalent statements is:

- *A mapping $E \to F$ between two finite sets E and F with*

$$\mathrm{Card}(E) > \mathrm{Card}(F)$$

is not injective.

An important application of it is Thue-Siegel's Lemma (see § 4.5). We shall not need the more sophisticated version of Thue-Siegel's Lemma in [BoVa 1983], based on an idea of Mahler using geometry of numbers, but Minkowski's Theorem (see for instance [Sc 1991], Chap. I) will be used in § 7.8 for the proof of Lemma 7.19.

The notion of algebraic independence will be needed not only for numbers, but also for functions. In a single variable we take for k the field $\mathbb{C}(z)$ of rational functions and for A either the ring of analytic (i.e. holomorphic) functions over a domain (= connected open subset) D of $\mathbb{C}$, or the field of meromorphic functions over D. A function $f \in A$ is called *transcendental* if it is transcendental over $\mathbb{C}(z)$, *algebraic* otherwise. An *entire function* is a function which is analytic in the whole of $\mathbb{C}$. It is easy to check that an entire function is algebraic if and only if it is a polynomial, and that a meromorphic function in $\mathbb{C}$ is algebraic if and only if it is a rational function, i.e. an element of $\mathbb{C}(z)$.

According to the general definition, analytic functions $f_1, \dots, f_d$ of n variables are algebraically independent over $\mathbb{C}$ if and only if, for any nonzero polynomial $P \in \mathbb{C}[X_1, \dots, X_d]$, the function $P(f_1, \dots, f_d)$ is not the zero function. Also $f_1, \dots, f_d$ are algebraically independent over $\mathbb{C}(z_1, \dots, z_n)$ if and only if, for any nonzero polynomial P in the ring of polynomials $\mathbb{C}[X_1, \dots, X_n, Y_1, \dots, Y_d]$ in $n+d$ variables, the function

$$P\big(z_1, \dots, z_n, f_1(\underline{z}), \dots, f_d(\underline{z})\big)$$

is not the zero function.

A function f is called *transcendental* if the $n+1$ functions $z_1, \dots, z_n, f(\underline{z})$ are algebraically independent: this means that f is transcendental over the field $\mathbb{C}(z_1, \dots, z_n)$.

The exponential function

$$1 + z + \frac{z^2}{2} + \frac{z^3}{6} + \cdots = \sum_{n=0}^{\infty} \frac{z^n}{n!}$$

is denoted either by e^z or by $\exp(z)$, and

$$e = \exp(1) = 2.71828182\ldots$$

is the natural basis of Napierian logarithms. For $\alpha \in \mathbb{C}^\times$, a determination of the logarithm of α is any complex number λ such that $\exp(\lambda) = \alpha$. For a given $\alpha \in \overline{\mathbb{Q}}^\times$, the set of λ in $\mathbb{C}$ with $\alpha = e^\lambda$ is a whole class of the additive group $\mathbb{C}$ modulo $2i\pi\mathbb{Z}$. In order to avoid confusion, we shall not use too often the notation $\log \alpha$ which depends on the choice of the branch of the logarithmic function. Nevertheless we remark that the $\mathbb{Q}$-vector space of logarithms of nonzero complex algebraic numbers

$$\mathcal{L} = \exp^{-1}(\overline{\mathbb{Q}}^\times) = \left\{\lambda \in \mathbb{C}\,;\ e^\lambda \in \overline{\mathbb{Q}}^\times\right\}$$

is the set of all numbers of the form $\log \alpha$ where α runs over the set of nonzero complex algebraic numbers and where we take all possible values for log:

$$\mathcal{L} = \{\log \alpha; \alpha \in \overline{\mathbb{Q}}^\times\}.$$

When a determination λ of the logarithm of α is chosen, for $\beta \in \mathbb{C}$ we write α^β in place of $\exp(\beta\lambda)$.

We shall say that a complex function f of one variable is *analytic in a closed disc* $\{z \in \mathbb{C}\,;\ |z| \le R\}$ *of* $\mathbb{C}$ if f is continuous on this disc and analytic in the open disc $|z| < R$. In this case we denote by $|f|_R$ the number $\sup\{|f(z)|\,;\ |z| \le R\}$. By *maximum modulus principle* we also have

$$|f|_R = \sup\{|f(z)|\,;\ |z| = R\}.$$

We shall also work with functions of several variables. For $\underline{z} = (z_1, \dots, z_n) \in \mathbb{C}^n$ (and therefore also for $\underline{z}$ in $\mathbb{N}^n$ or in $\mathbb{Z}^n$), we set

$$|\underline{z}| = \max_{1 \le i \le n} |z_i| \quad \text{and} \quad \|\underline{z}\| = |z_1| + \cdots + |z_n|.$$

If, further, $\underline{\sigma} = (\sigma_1, \dots, \sigma_n) \in \mathbb{N}^n$, then we define

$$\underline{z}^{\underline{\sigma}} = z_1^{\sigma_1} \cdots z_n^{\sigma_n}, \qquad \underline{\sigma}! = \sigma_1! \cdots \sigma_n!$$

(with $0! = 1$) and

$$\mathcal{D}^{\underline{\sigma}} = \left(\frac{\partial}{\partial z_1}\right)^{\sigma_1} \cdots \left(\frac{\partial}{\partial z_n}\right)^{\sigma_n}.$$

For $\underline{z}$ and $\underline{z}'$ in $\mathbb{C}^n$, let

$$\underline{z}\underline{z}' = z_1 z_1' + \cdots + z_n z_n'$$

denote the standard scalar product.

To each $\underline{w} = (w_1, \ldots, w_n) \in \mathbb{C}^n$ we attach a *derivative operator of order* 1:

$$\mathcal{D}_{\underline{w}} = w_1 \frac{\partial}{\partial z_1} + \cdots + w_n \frac{\partial}{\partial z_n}$$

on the ring of entire functions in $\mathbb{C}^n$. More generally, for S a positive integer, a *derivative operator D of order S* is a linear combination, with complex coefficients, of

$$\left(\frac{\partial}{\partial z_1}\right)^{\sigma_1} \cdots \left(\frac{\partial}{\partial z_n}\right)^{\sigma_n},$$

where $\underline{\sigma}$ runs over the set of elements in $\mathbb{N}^n$ satisfying $\|\underline{\sigma}\| = S$. This amounts to say that D is a linear combination, with complex coefficients, of products $\mathcal{D}_{\underline{w}_1} \cdots \mathcal{D}_{\underline{w}_S}$, where $(\underline{w}_1, \ldots, \underline{w}_S)$ ranges over a finite subset of $(\mathbb{C}^n)^S$.

Most often, tuples of numbers are underlined, like $\underline{w} = (w_1, \ldots, w_d) \in \mathbb{C}^d$; for $\underline{w}_1, \ldots, \underline{w}_{\ell_0}$ in $\mathbb{C}^d$ we write $\boldsymbol{w} = (\underline{w}_1, \ldots, \underline{w}_{\ell_0}) \in (\mathbb{C}^d)^{\ell_0}$. For $\underline{\sigma} \in \mathbb{N}^{\ell_0}$, $\underline{\tau} \in \mathbb{N}^{d_0}$, $\underline{t} \in \mathbb{Z}^{d_1}$ and $\underline{z} \in \mathbb{C}^d$ with $d = d_0 + d_1$, the function

$$\mathcal{D}_{\boldsymbol{w}}^{\underline{\sigma}}\left(\underline{z}^{\underline{\tau}} e^{\underline{t}\underline{z}}\right) = \mathcal{D}_{\underline{w}_1}^{\sigma_1} \cdots \mathcal{D}_{\underline{w}_{\ell_0}}^{\sigma_{\ell_0}} \left(z_1^{\tau_1} \cdots z_{d_0}^{\tau_{d_0}} e^{t_1 z_{d_0+1} + \cdots + t_{d_1} z_d}\right)$$

is an exponential polynomial for which explicit expressions will be given (see Lemmas 4.9 and 13.6).

For a complex function f which is continuous in a *polydisc*

$$\left\{\underline{z} \in \mathbb{C}^n \, ; \, |\underline{z}| \leq R\right\}$$

and analytic inside, we have again

$$\sup\{|f(\underline{z})| \, ; \, |\underline{z}| \leq R\} = \sup\{|f(\underline{z})| \, ; \, |\underline{z}| = R\};$$

this number will be denoted $|f|_R$.

Our main tool will be Schwarz' Lemma, which is a sharp upper bound for the modulus of a complex function, taking into account its zeroes. See § 2.2.3 for one variable, § 6.2.1 for one point and several variables, § 4.3 for Cartesian products.

We shall use only very simple properties of analytic functions in $\mathbb{C}^n$ (see for instance [LelGru 1986], Chap. I, § 1). Cauchy's inequalities will occur in §§ 4.6 and 4.7: an entire function f in $\mathbb{C}^n$, whose Taylor expansion at the origin is

$$\sum_{\underline{\sigma} \in \mathbb{N}^n} a_{\underline{\sigma}} \underline{z}^{\underline{\sigma}} \quad \text{with} \quad a_{\underline{\sigma}} = \frac{1}{\underline{\sigma}!} \mathcal{D}^{\underline{\sigma}} f(0)$$

satisfies, for all $r > 0$:

$$|\mathcal{D}^{\underline{\sigma}} f(0)| \leq \frac{\underline{\sigma}!}{r^{\|\underline{\sigma}\|}} |f|_r .$$

One deduces, for $\underline{\zeta} \in \mathbb{C}^n$ and $r \geq 1 + |\underline{\zeta}|$,

$$|\mathcal{D}^{\underline{\sigma}} f(\underline{\zeta})| \leq \frac{\underline{\sigma}!}{(r - |\underline{\zeta}|)^{\|\underline{\sigma}\|}} |f|_r \leq \underline{\sigma}! |f|_r .$$

In § 4.3 we shall also use the fact that a continuous mapping $f : \mathbb{C}^n \to \mathbb{C}$ is analytic if and only if it is analytic in each z_j when the other variables are fixed. This is a consequence of Cauchy's integral formula for polydiscs; see for instance [Hö 1973], Th. 2.2.1.

Notation

Some notation has already been fixed in the prerequisites section. We complete it with the following ones which will be used throughout the book.

We shall use Kronecker's diagonal symbol:

$$\delta_{ij} = \begin{cases} 1 & \text{if } i = j, \\ 0 & \text{if } i \neq j. \end{cases}$$

For $x \in \mathbb{R}$, we set

$$\log_+ x = \log \max\{e, x\}$$

and we denote by $[x] \in \mathbb{N}$ the integral part of x, with $0 \leq x - [x] < 1$.

The binomial coefficient

$$\binom{n}{k} = \frac{n!}{k!(n-k)!}$$

is 0 unless $0 \leq k \leq n$. More generally, an empty sum is equal to 0, while the value of an empty product is 1.

The number of elements in a finite set E will be denoted either by $\mathrm{Card}(E)$ or else by $|E|$.

- $\mathrm{Mat}_{d\times\ell}$ denotes the space of $d \times \ell$ matrices

- ${}^t\mathrm{M}$ is the transposed of a matrix M.

- $\mathrm{I}_d = \begin{pmatrix} 1 & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 1 \end{pmatrix}$ is the identity $d \times d$ matrix.

- For a positive integer d and a real number $S \geq 0$, the set of d-tuples

$$\mathbb{Z}^d[S] = \left\{ \underline{s} \in \mathbb{Z}^d \; ; \; |\underline{s}| \leq S \right\}$$

  has $(2[S]+1)^d$ elements.

- For $\underline{S} = (S_1, \ldots, S_d) \in \mathbb{R}^d_{>0}$, the set of d-tuples

$$\mathbb{Z}^d[\underline{S}] = \left\{ \underline{s} \in \mathbb{Z}^d \; ; \; |s_i| \leq S_i \;\; \text{for} \;\; 1 \leq i \leq d \right\}$$

  has $(2[S_1]+1)\cdots(2[S_d]+1)$ elements.

- When $\mathcal{V}$ is a vector subspace of $\mathbb{C}^d$, we set
$$\mathcal{V}[S] = \mathcal{V} \cap \mathbb{Z}^d[S] \quad \text{and} \quad \mathcal{V}[\underline{S}] = \mathcal{V} \cap \mathbb{Z}^d[\underline{S}]$$
for $S \in \mathbb{R}_{>0}$ and $\underline{S} = (S_1, \ldots, S_d) \in \mathbb{R}^d_{>0}$.
- For a finite subset E of an additive group G, and for m a positive integer,
$$E[m] = \{x_1 + \cdots + x_m \, ; \, x_i \in E\} \subset G.$$

In the successive chapters we introduce further notation as follows.

In Chapter 1

The distance between two matrices of the same size M and M′ is the maximum absolute value of the difference between the entries: for
$$\mathsf{M} = \bigl(x_{ij}\bigr)_{\substack{1 \le i \le d \\ 1 \le j \le \ell}} \quad \text{and} \quad \mathsf{M}' = \bigl(x'_{ij}\bigr)_{\substack{1 \le i \le d \\ 1 \le j \le \ell}},$$
in $\mathrm{Mat}_{d \times \ell}(\mathbb{C})$,
$$\mathrm{dist}(\mathsf{M}, \mathsf{M}') = \max_{\substack{1 \le i \le d \\ 1 \le j \le \ell}} |x_{ij} - x'_{ij}|.$$

In Chapter 2

- The degree of a polynomial f in one variable X is denoted by $\deg f$ or $\deg_X f$. For a polynomial f in several variables we denote by $\deg_X f$ and $\deg_{\underline{X}} f$ the partial degree with respect to one variable X and the total degree with respect to a set of variables $\underline{X} = (X_1, \ldots, X_m)$.
- For $f \in \mathbb{C}[\mathrm{X}_1, \ldots, \mathrm{X}_m]$, let $\mathrm{H}(f)$ be the maximum absolute value of the coefficients of f.
- $K[X_1^{\pm 1}, \ldots, X_n^{\pm 1}]$ denotes the subring of $K(X_1, \ldots, X_n)$ generated by K and
$$\{X_1, X_1^{-1}, \ldots, X_n^{-1}, X_n\}$$
(see § 2.2.1).

In Chapter 3

- $v_p(\alpha)$ is the p-adic absolute value.
- M_k, M_k^∞ are the sets of normalized absolute values and of Archimedean normalized absolute values of a number field k.
- $d_v(k)$ is the local degree of k at v.
- $[k\colon \mathbb{Q}]$ is the degree of k over $\mathbb{Q}$.

- $\mathbb{Q}_p$ is the field of p-adic numbers.
- $\mathbb{P}_m$ denotes the projective space of dimension m.
- $\mathrm{H}(\alpha)$ is the usual height of an algebraic number.
- $\mathrm{L}(f)$, $\mathrm{L}(\alpha)$ are the length of a polynomial or of an algebraic number.
- $\mathrm{M}(f)$, $\mathrm{M}(\alpha)$ denote Mahler's measure of a polynomial or of an algebraic number.
- $\mathrm{den}(\gamma)$, $\overline{|\gamma}|$, $s(\alpha)$ denote the denominator, the house and the size of an algebraic number.
- $\mathrm{h}(\alpha)$, $\mathrm{h}(\gamma_0 : \cdots : \gamma_N)$ are the absolute logarithmic height of an algebraic number or of a projective point.
- $N_{K/k}$, $\mathrm{Tr}_{K/k}$ denote the norm and the trace attached to an extension K/k (see also § 4.2.3).
- $\mathrm{L}_2(f)$ is the Euclidean norm of $f \in \mathbb{C}[X]$.

In Chapter 4

- $\mathcal{A}_n$ is the space of entire functions in $\mathbb{C}^n$.

In Chapter 5

- $\mathbb{G}_a$ and $\mathbb{G}_m$ are the additive and multiplicative groups.
- res is the restriction map (§ 5.2.2).
- T_Φ is the algebraic subgroup of a torus $\mathbb{G}_m^m$ associated with a subgroup Φ of $\mathbb{Z}^m$.
- $H(V; \underline{D})$ and $\mathcal{H}(V; \underline{D})$ are respectively an Hilbert function and the normalized homogeneous part of highest degree of an Hilbert-Samuel polynomial of an algebraic set V.
- τ_g is the translation by g in an abelian group.

In Chapter 6

- $\Theta_n(L)$ is defined in § 6.2.2.
- $\|\cdot\|_2$ is the Euclidean norm in Exercise 6.4.

In Chapter 7

- $\Theta(n; T_0, L)$ is defined in § 7.2.
- $\Delta(z; \tau)$ denote Fel'dman's polynomials introduced in § 7.7.
- Let K be a field, n a positive integer and $\mathcal{V}$ a vector subspace of K^n. We denote by $\pi_{\mathcal{V}}$ the canonical surjective linear map $K^n \longrightarrow K^n/\mathcal{V}$ with kernel $\mathcal{V}$.

In Chapter 8

- G^+ and G^- are algebraic subgroups of G.
- $\mathrm{rank}(I)$ is the rank of an ideal I (§ 8.2.1).
- $H(I; \underline{D})$ and $\mathcal{H}(I; \underline{D})$ are respectively an Hilbert function and the normalized homogeneous part of highest degree of an Hilbert-Samuel polynomial of I.
- $T_e(G)$ is the tangent space at the origin of an algebraic group G.
- In § 8.3.1, $\mathcal{V}^\perp$ is the subspace of $K[\underline{X}] = K[X_1, \dots, X_{d_0}]$ consisting of the linear forms $a_1X_1 + \cdots + a_{d_0}X_{d_0}$ which vanish identically on $\mathcal{V}$.

In Chapters 9 and 10

- *General case:* for a measure of linear independence of logarithms of algebraic numbers:
$$\Lambda = \beta_0 + \beta_1\lambda_1 + \cdots + \beta_m\lambda_m.$$
- *Homogeneous case:* $\beta_0 = 0$:
$$\Lambda = \beta_1\lambda_1 + \cdots + \beta_m\lambda_m.$$
- *Homogeneous rational case:* $\beta_0 = 0$ and $\beta_i = b_i \in \mathbb{Z}$:
$$\Lambda = b_1\lambda_1 + \cdots + b_m\lambda_m.$$
- $\delta_T(z;\tau)$, $\tau \in \mathbb{N}$ denote the polynomials of Fel'dman-Matveev (§ 9.2.1).
- In § 9.2.1 also we define
$$\delta(z;\sigma,\kappa) = \left(\frac{d}{dz}\right)^\kappa \delta(z;\sigma).$$
- $\mathcal{W}^\perp$ is the orthogonal of $\mathcal{W}$ in an Euclidean vector space (§ 10.2.4).

In Chapter 11

- $\exp_G\colon \mathbb{C}^d \to G(\mathbb{C})$ denotes the exponential map of an algebraic group G and Ω_G its kernel.
- For $d_0 \geq 0$ and $d_1 \geq 0$,
$$\mathcal{L}_G = \overline{\mathbb{Q}}^{d_0} \times \mathcal{L}^{d_1} = \exp^{-1}\bigl(G(\overline{\mathbb{Q}})\bigr)$$
(see § 11.1.2).
- $V_{\max}$, $V_{\min}$, $d_{\max}$, $d_{\min}$ are defined in § 11.1.2.