

ON
APPROXIMATIONS IN VALUED
FIELDS

F. KUIPER

UvA

STELLINGEN

I

Indien in Stelling 3.1 van dit proefschrift aangenomen wordt, dat het lichaam F compleet is, kan in de bewering van deze stelling de hoogte van elk der beschouwde veeltermen vervangen worden door het maximum van de waarden van begin- en eindcoëfficiënt. Een analoge bewering geldt voor Stelling 3.2.

De volgende twee stellingen hebben betrekking op het proefschrift van J. G. DIJKMAN, Convergentie en divergentie in de intuitionistische wiskunde (Amsterdam 1952). Zie ook B. VAN ROOTSELAAR, On intuitionistic notions of divergence and convergence, Nieuw Arch. Wisk. (3), 12, 19–24 (1964).

II

Van Stelling D₃ op pag. 32 van de genoemde dissertatie geldt eveneens de omkeering.

III

De bewering in 13.5 op pag. 33 wordt niet gerechtvaardigd door verwijzing naar Stelling D₂.

IV

Het is niet mogelijk de commutatieve woordrekenkonden van VUČKOVIĆ algebraïsch te karakteriseren door specialisatie van de door VAN ROOTSELAAR gegeven karakterisering der vrije woordrekenkonden van VUČKOVIĆ.

B. VAN ROOTSELAAR, Algebraische Kennzeichnung freier Wortarithmetiken, Compositio Math., Vol. 15, Fasc. 2, 156–168 (1963).

V. VUČKOVIĆ, Partially ordered recursive arithmetics, Math. Scand., 7, 305–320 (1959).

V. VUČKOVIĆ, Rekursive Wortarithmetik, Acad. Serbe Sci., Publ. Inst. Math., 14, 9–60 (1960).

V

De bewering van KUIPERS, dat $\frac{\partial^2 f}{\partial x \partial y} = \frac{\partial^2 f}{\partial y \partial x}$ in (x_0, y_0) , indien in een omgeving van (x_0, y_0) de functies

$$f, \frac{\partial f}{\partial x}, \frac{\partial f}{\partial y}, \frac{\partial^2 f}{\partial x \partial y}, \frac{\partial^2 f}{\partial y \partial x}, \frac{\partial^2 f}{\partial x^2} \text{ en } \frac{\partial^2 f}{\partial y^2}$$

bestaan, is onjuist.

L. KUIPERS, Leerboek der Analyse (Deel II), Groningen, 1962 (p. 15).

VI

Een invariante “Vollfastordnung” bepaalt in een scheef lichaam een algemeene valuatie. VAN DER WAERDEN’s bewering, dat de valuatiegroep in dit geval abels is, wordt door het verband, waarin deze is gedaan, niet gerechtvaardigd. Een juiste vorm van de verscherpte driehoeksongelijkheid van deze valuatie is

$$\varphi(x-y) \leq \max [\varphi(x), \varphi(y)] \cdot \varphi(s^{-1}).$$

B. L. VAN DER WAERDEN, Algebra II (4. Aufl.).
Berlin-Göttingen-Heidelberg, 1959 (§ 104).

VII

Zij α het homomorfisme (dat tevens tweevoudige overdekking is) van de speciale lineaire groep $SL(2, \mathbb{C})$ op de continue Lorentz-groep $L \subset GL(4, \mathbb{R})$. H is de verzameling der Hermitische matrices in $SL(2, \mathbb{C})$. S is de verzameling der symmetrische matrices in L . Ten onrechte beweert A. S. WIGHTMAN: $\alpha(H) = S$.

Relations de dispersion et particules élémentaires,
Ecole d’été de physique théorique, 1960, Les
Houches, p. 168.

VIII

Recente abundantiebepalingen van ijzer in de corona van de Zon geven een waarde, die minstens twintig maal groter is dan de resultaten, verkregen voor de fotosfeer. Er zijn aanwijzingen, dat dit groote verschil voornamelijk het gevolg is van fouten in de bepalingen der fotosferische abundantie.

IX

Incidenteele behandeling van vliegtechnische problemen in het kader van het wis- en natuurkundeonderwijs aan middelbare scholen is een middel om te komen tot verhooging der prestaties in deze vakken en kan culmineeren in het kiezen van een loopbaan bij de Koninklijke Luchtmacht.

ON APPROXIMATIONS IN VALUED FIELDS

ON APPROXIMATIONS IN VALUED FIELDS

ACADEMISCH PROEFSCHRIFT

TER VERKRIJGING VAN DEN GRAAD VAN DOCTOR
IN DE WISKUNDE EN NATUURWETENSCHAPPEN
AAN DE UNIVERSITEIT VAN AMSTERDAM, OP GEZAG VAN
DEN RECTOR MAGNIFICUS MR. J. VAN DER HOEVEN,
HOOGLEERAAR IN DE FACULTEIT DER RECHTSGELEERDHEID,
IN HET OPENBAAR TE VERDEDIGEN IN DE AULA DER UNIVERSITEIT
(TIJDELIJK IN DE LUTHERSCHE KERK, INGANG SINGEL 411, HOEK SPUI)
OP WOENSDAG 3 FEBRUARI 1965, DES NAMIDDAGS TE 4 UUR

DOOR

FRANS KUIPER

GEBOREN TE SLOTEN (N.H.)

1965

DRUKKERIJ HOLLAND N.V. — AMSTERDAM

Promotor : PROF. DR. J. POPKEN

VOORWOORD

Als oud-leerling van de Universiteit te Amsterdam wil ik dit proefschrift niet laten verschijnen zonder van mijn dankbaarheid te getuigen jegens allen, die tot mijn wetenschappelijke vorming hebben bijgedragen, waarbij mij in het bijzonder de boeiende colleges van U, Hooggeleerde BROUWER, voor den geest staan.

Dat ik, vele jaren na mijn doctoraal examen, den euvelen moed had mij met promotieplannen tot U, Hooggeleerde POPKEN, te wenden, gelieve U toe te schrijven aan mijn onkunde betreffende den huidige stand der ontwikkelingen in de wiskunde. Voor Uw bereidwilligheid mij nochtans Uw onmisbaren steun in onbeperkte mate te verleen ben ik U ten zeerste erkentelijk.

Hooggeleerde LEKKERKERKER, naar U gaat mijn oprechte dank uit wegens Uw opbouwende critiek na het doorlezen van het manuscript, waarvan eenige essentiele verbeteringen het gevolg zijn geweest.

CONTENTS

INTRODUCTION	1
CHAPTER I. VON NEUMANN-NUMBERS	3
CHAPTER II. ON ALGEBRAIC INDEPENDENCE IN DIFFERENTIAL RINGS	13
CHAPTER III. ON THE THEOREM OF BOMBIERI-MAHLER	26
SAMENVATTING	41

INTRODUCTION

In this thesis we discuss generalizations of two different, though related, problems occurring in the theory of numbers. The first problem is taken from the theory of transcendental numbers, the second from the theory of the approximation of an algebraic number by other algebraic numbers.

In the first case our starting-point is the well-known proof, due to VON NEUMANN [5], that there exists a set of real numbers with the power of the continuum such that the elements of any finite subset are algebraically independent over the rationals. The elements of this set, the so-called Von Neumann-numbers, are given by the formula

$$A_\varrho = \sum_{\nu=0}^{\infty} 2^{2^{[\varrho\nu]}} - 2^{\nu^2} \text{ for any } \varrho > 0.$$

VON NEUMANN's proof is an extension of LIOUVILLE's method to prove the existence of transcendental numbers by means of rapidly converging series with rational terms. In fact, it is easy to verify that every Von Neumann-number A_ϱ is also a Liouville-number.

The aim of Chapter I of this thesis is first to simplify VON NEUMANN's proof as far as possible and then to generalize his method.

Without going into details we mention here that the field of real numbers in the classical case is in our theory replaced by a complete valued field. We confine ourselves to the case that the range of values of the valuation consists of non-negative numbers. For the valuation of an element a we shall always use the notation $|a|$.

In Chapter II we generalize this method even further by considering elements in a valued differential field. KOLCHIN [3], in a beautiful paper of 1959, has already generalized the simpler method of LIOUVILLE to the case of a valued differential field and we are able to use some of his lemmas for our own purpose.

In our last chapter we turn to a different problem, which goes back to a result of BRAUER [2] obtained in 1929. It reads as follows:

Let α be a fixed algebraic number of degree m . Then there exists a positive constant C , depending only on α , such that for any algebraic number $\beta \neq \alpha$ of degree n and of height $H(\beta)$ one has

$$|\alpha - \beta| > C^n H(\beta)^{-m}.$$

For the definition of the height of an algebraic number see Chapter III, section 1; also the height of a polynomial is introduced there.

More recently this theorem was generalized successively by BOMBIERI [1] and by MAHLER [4]. MAHLER considered two polynomials f and g over the field of complex numbers with resultant R . Let α be a zero of f and β a zero of g . Then MAHLER determined a lower bound for $|\alpha - \beta|$

in terms of R and of the degrees and heights of the two polynomials f and g . Moreover he gave a similar result in case α and β satisfy the same equation $f=0$.

In Chapter III we investigate what becomes of MAHLER's theory if we consider zeros of polynomials over a field F endowed with a non-Archimedean valuation and satisfying certain conditions. Due to the non-Archimedean character of our valuation the formulas become simpler than in MAHLER's case.

Our deepest result in this direction is obtained by specializing to polynomials over the field $\mathbf{Q}_p$ of p -adic numbers. In this case we find the following result (compare Theorem 3.7):

Let f and g be two polynomials over $\mathbf{Q}_p$ of degrees m and n and of heights $H(f)$ and $H(g)$, respectively. Let Φ be a finite extension of $\mathbf{Q}_p$ such that f and g both resolve into linear factors in $\Phi[x]$:

$$f(x) = a_m(x - \alpha_1) \cdots (x - \alpha_m),$$

$$g(x) = b_n(x - \beta_1) \cdots (x - \beta_n).$$

Let $|\gamma|_p$ denote for any element γ of Φ the valuation of γ , if we extend the p -adic valuation of $\mathbf{Q}_p$ to Φ . Suppose that the resultant $R = R(f, g)$ of f and g does not vanish and set

$$\Delta = \min_{\substack{1 \leq \mu \leq m \\ 1 \leq \nu \leq n}} |\alpha_\mu - \beta_\nu|_p.$$

Then

$$\text{either } \Delta \geq 1 \text{ or } \Delta \geq H(f)^{-n} H(g)^{-m} |R|_p.$$

There is a similar result for two distinct zeros of a single polynomial over $\mathbf{Q}_p$ (compare Theorem 3.8).

We remark that the fields considered in this thesis are always commutative.

The reader may find more detailed information in the introductory sections of the different chapters.

REFERENCES

1. BOMBIERI, E., Sull' approssimazione di numeri algebrici mediante numeri algebrici, Boll. Un. Mat. Ital. III, 13, 351-354 (1958).
2. BRAUER, A., Über die Approximation algebraischer Zahlen durch algebraische Zahlen, Jber. Deutsch. Math.-Verein., 38, 47 (1929).
3. KOLCHIN, E. R., Rational approximation to solutions of algebraic differential equations, Proc. Amer. Math. Soc., 10, 238-244 (1959).
4. MAHLER, K., On a theorem by E. Bombieri, Proc. Nederl. Akad. Wetensch. A, 63, 245-253 (1960); Indag. Math., 22, 245-253 (1960).
5. NEUMANN, J. VON, 1. Collected works, Vol. I. Oxford-London-New York-Paris, 312-319 (1961); 2. Ein System algebraisch unabhängiger Zahlen, Math. Ann., 99, 134-141 (1928).

CHAPTER I

VON NEUMANN-NUMBERS

1. In a well-known paper VON NEUMANN [7] has effectively given a set of real numbers (the “Von Neumann-numbers”) with the power of the continuum and with the property that n arbitrarily chosen different numbers of this set are always algebraically independent with respect to the field of rational numbers.

This result has been used a.o. for the purpose of constructing free groups with certain properties. Compare e.g. DE GROOT [2], DEKKER [1], MYCIELSKI and ŚWIERCZKOWSKI [6].

The idea basic to VON NEUMANN’s paper is very simple, but it is obscured in some way by lengthy calculations. Recently, HELLMUTH KNESER [4] has given another treatment of the same problem which is much simpler and at the same time more general. As a special case he finds the following result:

Let
$$f(u) \stackrel{\text{def}}{=} \sum_{m=1}^{\infty} 2^{-[m^{m+u}]}, \quad 0 \leq u < 1,$$

$[m^{m+u}]$ denoting, as is usual, the largest integer $\leq m^{m+u}$. If $u_1, u_2, \dots, u_n$ are arbitrarily chosen different numbers from the interval $[0, 1)$, then the n numbers $f(u_1), f(u_2), \dots, f(u_n)$ are algebraically independent.

In this chapter we shall give another treatment of the same problem, which shows, in our opinion, the principles basic to VON NEUMANN’s paper even better. In order to explain our method we begin by considering a very special case.

Let u, v denote positive integers such that $u < v$, put

$$\alpha = \sum_{m=1}^{\infty} 2^{m^u - m^m}, \quad \beta = \sum_{m=1}^{\infty} 2^{m^v - m^m}.$$

Then α and β are algebraically independent over the field of rational numbers.

Proof. We shall show that the assumption that α and β are algebraically dependent leads to a contradiction. Suppose that there exists a polynomial $f(x, y)$ with integral coefficients—not all zero—such that

$$f(\alpha, \beta) = 0.$$

We may assume that $f(x, y)$ has minimal total degree. Put for any positive integer k

$$A_k = \sum_{m=1}^k 2^{m^u - m^m}, \quad B_k = \sum_{m=1}^k 2^{m^v - m^m},$$

then

$$\alpha - A_k = 2^{(k+1)u - (k+1)^{k+1}} + \dots = (1 + o(1)) 2^{(k+1)u - (k+1)^{k+1}} \text{ if } k \rightarrow \infty,$$

$$\beta - B_k = 2^{(k+1)v - (k+1)^{k+1}} + \dots = (1 + o(1)) 2^{(k+1)v - (k+1)^{k+1}} \text{ if } k \rightarrow \infty.$$

By Taylor's formula

$$\begin{aligned} f(A_k, B_k) &= f(\alpha, \beta) + (A_k - \alpha)f_x(\alpha, \beta) + (B_k - \beta)f_y(\alpha, \beta) \\ &\quad + \frac{(A_k - \alpha)^2}{2!} f_{xx}(\alpha, \beta) + \dots \\ &= (A_k - \alpha)f_x(\alpha, \beta) + (B_k - \beta)f_y(\alpha, \beta) + \dots, \end{aligned}$$

with a finite number of terms in the right-hand sides. At least one of the partial derivatives f_x and f_y does not vanish identically. Suppose first $f_y \neq 0$, then, by the minimal condition for $f(x, y)$,

$$f_y(\alpha, \beta) \neq 0.$$

It follows from Taylor's formula as given above (and using $u < v$) that

$$f(A_k, B_k) = -(1 + o(1)) 2^{(k+1)v - (k+1)^{k+1}} f_y(\alpha, \beta) \text{ if } k \rightarrow \infty,$$

so that $f(A_k, B_k)$ does not vanish for sufficiently large k . Now we observe that A_k and B_k are rational numbers with denominators 2^{k^k} . Let g denote the total degree of $f(x, y)$, then

$$2^{gk^k} f(A_k, B_k)$$

is integral, but does not vanish for sufficiently large k . This gives a contradiction, since

$$2^{gk^k} f(A_k, B_k) = -(1 + o(1)) 2^{gk^k + (k+1)v - (k+1)^{k+1}} f_y(\alpha, \beta)$$

tends to zero if $k \rightarrow \infty$.

If $f_y = 0$, then $f_x \neq 0$, hence $f_x(\alpha, \beta) \neq 0$, and a reasoning quite similar to the one given above leads to a contradiction also in this case.

By using essentially the same method we can easily generalize the above result as follows:

Theorem 1.1. *Consider the function $\varphi(u)$ of the real variable u defined by*

$$\varphi(u) = \sum_{m=1}^{\infty} 2^{[m^u] - m^m}, \quad u \geq 0.$$

If $u_1, u_2, \dots, u_n$ are arbitrarily chosen different non-negative numbers, then $\varphi(u_1), \varphi(u_2), \dots, \varphi(u_n)$ are algebraically independent over the field of rational numbers.

Instead of this theorem we prove in the next sections a much more general result. Instead of sets of real numbers we consider more generally sets of elements of a complete valued field.

Before doing so, however, we observe that the result given above solves the problem of VON NEUMANN. In fact, from the definition it is clear that $\varphi(u)$ is non-decreasing; it follows that $\varphi(u)$ is even strictly increasing for $u \geq 0$, since the assertion of the theorem implies $\varphi(u_1) \neq \varphi(u_2)$ if $u_1 > u_2 \geq 0$. Hence the set of functional values $\varphi(u)$ for $u \geq 0$ is a set of positive numbers which satisfies the conditions of VON NEUMANN: it has the power of the continuum and n arbitrarily chosen numbers from the set are always algebraically independent over the rationals.

2. *In the sequel let F denote a valued field. If a is an arbitrary element of F , then let $|a|$ denote its valuation, so that a) $|0| = 0$, $|a| > 0$ for $a \neq 0$, b) $|ab| = |a| + |b|$ and c) $|a + b| \leq |a| + |b|$. We suppose in the following that F is complete with respect to this valuation. Moreover let R denote a sub-ring of F with the property that $|a| \geq 1$ for any $a \neq 0$ from R . Finally we suppose that R contains at least one element a with $|a| > 1$.*

Before stating the main result we let precede three lemmas, from which our main theorem follows easily.

Lemma 1. Let n denote an arbitrary positive integer, let

$$A_\nu = \sum_{m=0}^{\infty} \frac{a_{\nu m}}{\beta_0 \beta_1 \dots \beta_m} \quad (\nu = 1, 2, \dots, n),$$

where $a_{\nu m}$, β_m are non-vanishing elements of the sub-ring R with $|\beta_m| \rightarrow \infty$ if $m \rightarrow \infty$. Moreover let, if $m \rightarrow \infty$,

$$(1) \quad \begin{cases} |a_{\nu m}| = o(|a_{nm}|) \text{ for } \nu = 1, 2, \dots, n-1 \\ |a_{nm}| = O(|b_{m-1}|), \text{ where } b_m = \beta_0 \beta_1 \dots \beta_m, \\ \log |b_{m-1}| = o(\log |b_m|). \end{cases}$$

Let

$$f(x_1, \dots, x_n) = \sum_{(h)} c_{(h)} x_1^{h_1} \dots x_n^{h_n}$$

denote an arbitrarily chosen polynomial in the indeterminates $x_1, \dots, x_n$ over R . Then the two relations

$$(2) \quad f(A_1, \dots, A_n) = 0 \text{ and } \frac{\partial f}{\partial x_n}(A_1, \dots, A_n) \neq 0$$

cannot be satisfied simultaneously.¹⁾

Proof. Let us suppose that there exists a polynomial $f(x_1, \dots, x_n)$ over R satisfying both relations (2). We shall reach a contradiction by applying Taylor's formula in the form

$$\begin{aligned} f(x_1 + y_1, \dots, x_n + y_n) &= f(x_1, \dots, x_n) + \sum_{\nu=1}^n y_\nu f_\nu(x_1, \dots, x_n) \\ &\quad + \sum_{1 \leq \nu < \mu \leq n} y_\nu y_\mu f_{\nu\mu}(x_1, \dots, x_n) + \dots, \end{aligned}$$

¹⁾ From the conditions (1) it follows easily that the series for $A_1, \dots, A_n$ converge.

where the right-hand side contains only a finite number of terms, and where

$$\begin{aligned} f_{\nu}(x_1, \dots, x_n) &= \frac{\partial f}{\partial x_{\nu}}(x_1, \dots, x_n) = \sum_{(h)} \binom{h_{\nu}}{1} c_{(h)} x_1^{h_1} \dots x_{\nu}^{h_{\nu}-1} \dots x_n^{h_n} \\ f_{\nu\nu}(x_1, \dots, x_n) &= \sum_{(h)} \binom{h_{\nu}}{2} c_{(h)} x_1^{h_1} \dots x_{\nu}^{h_{\nu}-2} \dots x_n^{h_n} \\ f_{\nu\mu}(x_1, \dots, x_n) &= \sum_{(h)} \binom{h_{\nu}}{1} \binom{h_{\mu}}{1} c_{(h)} x_1^{h_1} \dots x_{\nu}^{h_{\nu}-1} \dots x_{\mu}^{h_{\mu}-1} \dots x_n^{h_n} \quad (\text{if } \nu < \mu), \end{aligned}$$

etc.

Let k denote a positive integer, later to be chosen arbitrarily large. Let

$$B_{\nu k} \stackrel{\text{def}}{=} \sum_{m=0}^{k-1} \frac{a_{\nu m}}{b_m}, \quad v_{\nu k} \stackrel{\text{def}}{=} - \sum_{m=k}^{\infty} \frac{a_{\nu m}}{b_m} \quad (\nu = 1, 2, \dots, n),$$

so that $B_{\nu k} = A_{\nu} + v_{\nu k}$. Applying Taylor's formula with $x_{\nu} = A_{\nu}$, $y_{\nu} = v_{\nu k}$ and using $f(A_1, \dots, A_n) = 0$, we obtain

$$\begin{aligned} f(B_{1k}, \dots, B_{nk}) &= \sum_{\nu=1}^n v_{\nu k} f_{\nu}(A_1, \dots, A_n) \\ (3) \quad &+ \sum_{1 \leq \nu < \mu \leq n} v_{\nu k} v_{\mu k} f_{\nu\mu}(A_1, \dots, A_n) \\ &+ \dots \end{aligned}$$

From the definition of $v_{\nu k}$ one obtains

$$v_{\nu k} + \frac{a_{\nu k}}{b_k} = - \sum_{m=k+1}^{\infty} \frac{a_{\nu m}}{b_m},$$

hence, by (1),

$$\begin{aligned} \left| v_{\nu k} + \frac{a_{\nu k}}{b_k} \right| &= O\left(\sum_{m=k+1}^{\infty} \frac{|b_{m-1}|}{|b_m|} \right) \\ &= O\left(\sum_{m=k+1}^{\infty} |b_{m-1}|^{-2} \right) \\ &= O(|b_k|^{-2}) \text{ if } k \rightarrow \infty, \end{aligned}$$

or

$$(4) \quad v_{\nu k} = - \frac{a_{\nu k}}{b_k} + O(|b_k|^{-2}) \text{ if } k \rightarrow \infty \quad (\nu = 1, 2, \dots, n).$$

It follows therefore from (1) that

$$v_{\nu k} \rightarrow 0 \text{ if } k \rightarrow \infty \quad (\nu = 1, 2, \dots, n)$$

and also

$$|v_{\nu k}| = o(|v_{nk}|) \text{ if } k \rightarrow \infty \text{ for } \nu < n.$$

Hence, using (3),

$$(5) \quad f(B_{1k}, \dots, B_{nk}) = v_{nk} f_n(A_1, \dots, A_n) + o(|v_{nk}|) \text{ if } k \rightarrow \infty.$$

We have assumed $f_n(A_1, \dots, A_n) \neq 0$ and from (4) we derive $v_{nk} \neq 0$ for sufficiently large k . Therefore

$$f(B_{1k}, \dots, B_{nk}) \neq 0 \text{ for } k \geq k_0.$$

From the definition of B_{vk} it follows that

$$b_{k-1}B_{vk} = \beta_0\beta_1 \dots \beta_{k-1}B_{vk} = \sum_{m=0}^{k-1} a_{vm}\beta_{m+1}\beta_{m+2} \dots \beta_{k-1} \in R,$$

hence, if the total degree of $f(x_1, \dots, x_n)$ is denoted by s ,

$$b_{k-1}^s f(B_{1k}, \dots, B_{nk}) \in R.$$

For $k \geq k_0$ this element does not vanish, hence, on account of the definition of the sub-ring R ,

$$(6) \quad |b_{k-1}^s f(B_{1k}, \dots, B_{nk})| \geq 1.$$

On the other hand it follows from (5) and (4) for $k \rightarrow \infty$ that

$$(7) \quad |f(B_{1k}, \dots, B_{nk})| = O(|v_{nk}|) = O\left(\frac{|a_{nk}|}{|b_k|}\right) = O\left(\frac{|b_{k-1}|}{|b_k|}\right).$$

Comparing (6) and (7), we obtain for sufficiently large k

$$|b_{k-1}|^{-s} < C \frac{|b_{k-1}|}{|b_k|},$$

where C stands for a positive number independent of k . This last inequality contradicts (1), which proves our lemma.

Lemma 2. Let the valued field F and its sub-ring R be given as before. Moreover let F be of characteristic zero.

Let $A_1, A_2, \dots, A_n$ be defined as in the preceding lemma. Then A_n is transcendental over the ring $R[A_1, \dots, A_{n-1}]$ generated from R by $A_1, A_2, \dots, A_{n-1}$.

Proof. Suppose that A_n is algebraic over $R[A_1, \dots, A_{n-1}]$, so that A_n satisfies an equation

$$D_0 + D_1x + \dots + D_rx^r = 0,$$

where the coefficients

$$D_\varrho = \sum_{(h)} d_{\varrho, h_1, \dots, h_{n-1}} A_1^{h_1} \dots A_{n-1}^{h_{n-1}} \quad (\varrho = 0, 1, \dots, r)$$

do not vanish simultaneously and where $d_{\varrho, h_1, \dots, h_{n-1}} \in R$. We may suppose that the equation is of minimal degree r . It follows that $D_r \neq 0$, hence $rD_r \neq 0$, and therefore A_n cannot satisfy the equation

$$D_1 + 2D_2x + \dots + rD_rx^{r-1} = 0.$$

Put

$$D_\varrho(x_1, \dots, x_{n-1}) \stackrel{\text{def}}{=} \sum_{(h)} d_{\varrho, h_1, \dots, h_{n-1}} x_1^{h_1} \dots x_{n-1}^{h_{n-1}}$$

and

$$f(x_1, \dots, x_n) \stackrel{\text{def}}{=} \sum_{\varrho=0}^r D_\varrho(x_1, \dots, x_{n-1}) x_n^\varrho.$$

Then $f(x_1, \dots, x_n)$ represents a polynomial over R with

$$f(A_1, \dots, A_n) = 0, \frac{\partial f}{\partial x_n}(A_1, \dots, A_n) \neq 0.$$

But this contradicts the assertion of our preceding lemma 1.

Lemma 3. Let $\mathfrak{B}$ be a ring with identity-element and let R be any sub-ring containing the identity-element. Then the elements $u_1, u_2, \dots, u_n$ of $\mathfrak{B}$ are algebraically independent over R if and only if each u_k , $k=1, 2, \dots, n$, is transcendental over $R[u_1, u_2, \dots, u_{k-1}]$, i.e. the ring generated from R by $u_1, u_2, \dots, u_{k-1}$ (compare e.g. JACOBSON [3], p. 105, lemma).

3. Our main result is the following theorem:

Theorem 1.2. *Let the valued field F and its sub-ring R be defined as before. Let F be of characteristic zero and let R contain the identity-element of F . Let*

$$A_\nu = \sum_{m=0}^{\infty} \frac{a_{\nu m}}{\beta_0 \beta_1 \dots \beta_m} \quad (\nu = 1, 2, \dots, n),$$

where $a_{\nu m}, \beta_m$ denote non-vanishing elements of the sub-ring R with $|\beta_m| \rightarrow \infty$ if $m \rightarrow \infty$. Moreover let for $m \rightarrow \infty$

$$\begin{aligned} |a_{1m}| &= o(|a_{2m}|), \quad |a_{2m}| = o(|a_{3m}|), \quad \dots, \quad |a_{n-1,m}| = o(|a_{nm}|) \\ |a_{nm}| &= O(|b_{m-1}|), \quad \text{where } b_m = \beta_0 \beta_1 \dots \beta_m, \\ \log |b_{m-1}| &= o(\log |b_m|). \end{aligned}$$

Then $A_1, A_2, \dots, A_n$ are algebraically independent over R .

Proof. Let k denote an arbitrary integer from the sequence $1, 2, \dots, n$. Then clearly for $m \rightarrow \infty$

$$\begin{aligned} |a_{\kappa m}| &= o(|a_{km}|) \quad \text{for } \kappa = 1, 2, \dots, k-1 \\ |a_{km}| &= O(|b_{m-1}|), \quad \log |b_{m-1}| = o(\log |b_m|). \end{aligned}$$

Therefore we can apply lemma 2 with $A_1, \dots, A_k$ instead of $A_1, \dots, A_n$. It follows that A_k is transcendental over the ring $R[A_1, \dots, A_{k-1}]$. This is true for $k=1, 2, \dots, n$. Hence, by lemma 3, the elements $A_1, \dots, A_n$ of F are algebraically independent over R .

4. As an application of the preceding theorem we shall now prove Theorem 1.1.

Proof. Take in our theorem for F the field of real numbers, for R the ring of integers. We may suppose $0 < u_1 < u_2 < \dots < u_n$. Then take

$$a_{vm} = 2^{\lfloor m^{u_v} \rfloor}, \quad b_m = 2^{m^m}.$$

Then

$$\begin{aligned} |\beta_m| &= \frac{|b_m|}{|b_{m-1}|} = 2^{m^m - (m-1)^{m-1}} \\ &= 2^{m^m \left(1 - \frac{(m-1)^{m-1}}{m^m}\right)} \rightarrow \infty \text{ if } m \rightarrow \infty. \end{aligned}$$

Next, if $v = 2, 3, \dots, n$,

$$\begin{aligned} \frac{|a_{v-1, m}|}{|a_{vm}|} &= 2^{\lfloor m^{u_{v-1}} \rfloor - \lfloor m^{u_v} \rfloor} < 2^{m^{u_{v-1}} - m^{u_v+1}} \\ &= 2^{m^{u_{v-1}}(1 - m^{u_v - u_{v-1} - 1}) + 1} \rightarrow 0 \text{ if } m \rightarrow \infty, \end{aligned}$$

since $u_v > u_{v-1} > 0$. It follows for $m \rightarrow \infty$ that

$$|a_{v-1, m}| = o(|a_{vm}|) \quad (v = 2, 3, \dots, n).$$

Further

$$\frac{|a_{nm}|}{|b_{m-1}|} = 2^{\lfloor m^{u_n} \rfloor - (m-1)^{m-1}} \rightarrow 0,$$

hence $|a_{nm}| = o(|b_{m-1}|)$ if $m \rightarrow \infty$.

Finally

$$\frac{\log |b_{m-1}|}{\log |b_m|} = \frac{(m-1)^{m-1}}{m^m} = \left(\frac{m-1}{m}\right)^{m-1} \frac{1}{m} \rightarrow 0 \text{ if } m \rightarrow \infty.$$

Consequently $\log |b_{m-1}| = o(\log |b_m|)$ if $m \rightarrow \infty$.

The conditions of Theorem 1.2 are thus satisfied. It follows that the numbers $\varphi(u_1), \varphi(u_2), \dots, \varphi(u_n)$ are algebraically independent over R , hence also over the field of rational numbers.

For a second application of Theorem 1.2 we need the following lemma. Although this result is well-known, it is usually derived from much deeper theorems. Here we give an elementary direct proof.

Lemma 4. Let F_0 denote the field of formal power series

$$A = \sum_{e=r}^{\infty} a_e x^e$$

over a given field K . (Here r denotes an arbitrarily chosen integer.) Then F_0 is complete with respect to the valuation

$$|A| = 0 \text{ for } A = 0, \quad |A| = e^{-r} \text{ if } a_r \neq 0.$$

Proof. If $a_r \neq 0$, then $|A| = e^{-r} < \varepsilon$ ($0 < \varepsilon \leq 1$) clearly means $r > |\log \varepsilon|$.

Now consider in F_0 an arbitrary fundamental sequence $\{A_\nu\}$, where

$$A_\nu = \sum_{\varrho=r_\nu}^{\infty} a_{\nu\varrho} x^\varrho, \quad a_{\nu, r_\nu} \neq 0.$$

We have to show that there exists in F_0 a power series A such that $\lim_{\nu \rightarrow \infty} A_\nu = A$.

Since any fundamental sequence is bounded, there exists a positive number M such that

$$e^{-r_\nu} < M \text{ for } \nu = 1, 2, \dots$$

Let r be the minimal value of the r_ν ($\nu = 1, 2, \dots$), so that we may write

$$A_\nu = \sum_{\varrho=r}^{\infty} a_{\nu\varrho} x^\varrho \quad (\nu = 1, 2, \dots).$$

For every ε ($0 < \varepsilon < 1$) there exists an integer $N(\varepsilon)$ such that for $\mu, \nu \geq N(\varepsilon)$

$$|A_\mu - A_\nu| = \left| \sum_{\varrho=r}^{\infty} (a_{\mu\varrho} - a_{\nu\varrho}) x^\varrho \right| < \varepsilon.$$

It follows that $a_{\mu\varrho} = a_{\nu\varrho}$ if simultaneously $\varrho \leq |\log \varepsilon|$ and $\mu, \nu \geq N(\varepsilon)$.

We now define elements a_ϱ ($\varrho = r, r+1, \dots$) of K as follows:

For every ϱ choose ε ($0 < \varepsilon < 1$) so small that $|\log \varepsilon| \geq \varrho$ and put

$$a_\varrho \stackrel{\text{def}}{=} a_{\nu\varrho} \text{ with } \nu \geq N(\varepsilon).$$

Then define the power series A over K by

$$A = \sum_{\varrho=r}^{\infty} a_\varrho x^\varrho.$$

Clearly $\lim_{\nu \rightarrow \infty} A_\nu = A$, since $|A - A_\nu| < \varepsilon$ for $\nu \geq N(\varepsilon)$.

Q.e.d.

The application we had in mind is the following theorem:

Theorem 1.3. *Let K be a field of characteristic zero. Let $\varphi_m(u)$ ($m = 1, 2, \dots$) be functions of the variable $u \geq 0$ with functional values in K such that $\varphi_m(u) \neq 0$ for all $m = 1, 2, \dots, u \geq 0$. Consider the set of all formal power series*

$$A(u) = \sum_{m=1}^{\infty} \varphi_m(u) x^{m - [m^u]}.$$

If $u_1, u_2, \dots, u_n$ are arbitrarily chosen different non-negative numbers, then $A(u_1), A(u_2), \dots, A(u_n)$ are algebraically independent over the ring $K[x]$.

Proof. We take for F the field of formal power series

$$A = \sum_{\varrho=r}^{\infty} a_\varrho x^\varrho$$

over K , where r denotes an arbitrary integer. Hence, by lemma 4, F is complete with respect to the valuation

$$|A| = 0 \text{ for } A = 0, \quad |A| = e^{-r} \text{ if } a_r \neq 0.$$

Take for R the ring of all polynomials in x^{-1} over K .

We may suppose $0 \leq u_1 < u_2 < \dots < u_n$. Put $a_{v0} = 0, \beta_0 = b_0 = 1$,

$$a_{vm} = \varphi_m(u_v) x^{-[m^{u_v}]}, \quad b_m = x^{-m^m} \quad (v = 1, 2, \dots, n; m = 1, 2, \dots).$$

Then

$$\begin{aligned} |\beta_m| &= \frac{|b_m|}{|b_{m-1}|} = |x^{(m-1)^{m-1} - m^m}| \\ &= e^{m^m - (m-1)^{m-1}} \rightarrow \infty \text{ if } m \rightarrow \infty. \end{aligned}$$

Next, if $v = 2, 3, \dots, n$,

$$\begin{aligned} \frac{|a_{v-1,m}|}{|a_{vm}|} &= \left| \frac{\varphi_m(u_{v-1})}{\varphi_m(u_v)} x^{[m^{u_v}] - [m^{u_{v-1}}]} \right| \\ &= e^{[m^{u_v-1}] - [m^{u_v}]} < e^{m^{u_v-1} - m^{u_v+1}}. \end{aligned}$$

Since $u_v > u_{v-1} \geq 0$, it follows for $m \rightarrow \infty$ that

$$|a_{v-1,m}| = o(|a_{vm}|) \quad (v = 2, 3, \dots, n).$$

Further

$$\begin{aligned} \frac{|a_{nm}|}{|b_{m-1}|} &= |\varphi_m(u_n) x^{(m-1)^{m-1} - [m^{u_n}]}| \\ &= e^{[m^{u_n}] - (m-1)^{m-1}}, \text{ so that} \end{aligned}$$

$$|a_{nm}| = o(|b_{m-1}|) \text{ if } m \rightarrow \infty.$$

Finally

$$\frac{\log |b_{m-1}|}{\log |b_m|} = \frac{(m-1)^{m-1}}{m^m} \rightarrow 0 \text{ if } m \rightarrow \infty.$$

Consequently $\log |b_{m-1}| = o(\log |b_m|)$ if $m \rightarrow \infty$.

The conditions of Theorem 1.2 are thus satisfied. It follows that the power series $A(u_1), A(u_2), \dots, A(u_n)$ are algebraically independent over R , hence also over $K[x]$.

Final remark. The contents of the sections 2, 3 and partly of section 4 have already been published in KUIPER and POPKEN [5].

REFERENCES

1. DEKKER, T. J., 1. On free groups of motions without fixed points, Proc. Nederl. Akad. Wetensch. A, 61, 348–353 (1958); Indag. Math., 20, 348–353 (1958); 2. Paradoxical decompositions of sets and spaces, thesis, Amsterdam, p. 15 ff. (1958).

2. GROOT, J. DE, Orthogonal isomorphic representations of free groups, *Canad. J. Math.*, **8**, 256–262 (1956).
3. JACOBSON, N., *Lectures in abstract algebra I*. London, 1953.
4. KNESER, HELLMUTH, Eine kontinuumsmächtige, algebraisch unabhängige Menge reeller Zahlen, *Bull. Soc. Math. Belg.*, **12**, 23–27 (1960).
5. KUIPER, F. and J. POPKEN, On the so-called Von Neumann-numbers, *Proc. Nederl. Akad. Wetensch. A*, **65**, 385–390 (1962); *Indag. Math.*, **24**, 385–390 (1962).
6. MYCIELSKI, J. and S. ŚWIERCZKOWSKI, On free groups of motions and decompositions of the Euclidean space, *Fund. Math.*, **45**, 283–291 (1958).
7. NEUMANN, J. VON, 1. *Collected works*, Vol. I. Oxford–London–New York–Paris, 312–319 (1961); 2. Ein System algebraisch unabhängiger Zahlen, *Math. Ann.*, **99**, 134–141 (1928).

CHAPTER II

ON ALGEBRAIC INDEPENDENCE IN DIFFERENTIAL RINGS

1. We consider a so-called *valued differential field* F (compare e.g. KAPLANSKY [2]); this is a field F with the following three properties A, B and C:

A) There exists for all elements $a, b, c, \dots$ of F a formal differentiation, i.e. there exists a mapping $a \rightarrow a'$ of F into itself such that

$$(a+b)' = a' + b', \quad (ab)' = ab' + a'b.$$

It follows easily, if e denotes the identity-element of F , that $0' = 0$, $e' = 0$, $(b^{-1})' = -b'b^{-2}$ and $(a/b)' = (a'b - ab')/b^2$.

Moreover, if $a', a'' = (a')', \dots, a^{(n)} = (a^{(n-1)})', \dots$ are the successive derivatives of a , then

$$(ab)^{(n)} = \sum_{\nu=0}^n \binom{n}{\nu} a^{(\nu)} b^{(n-\nu)}.$$

B) F has a non-Archimedean valuation. If a is an arbitrary element of F , then $|a|$ will denote its valuation, so that a) $|0| = 0$, $|a| > 0$ for $a \neq 0$, b) $|ab| = |a| |b|$ and c) $|a+b| \leq \max(|a|, |b|)$. It is well-known that it follows that $|a+b| = \max(|a|, |b|)$, provided $|a| \neq |b|$. Moreover $|e| = 1$. We always suppose that this valuation is not the trivial valuation.

C) Further we require, following KOLCHIN [3], that there exist positive numbers α and β such that

$$(1) \quad \alpha|a| \leq |a'| \leq \beta|a| \text{ for every } a \in F \text{ with } |a| < 1.$$

F is then called a valued differential field. The elements α and β are called, respectively, *lower* and *upper bounds* of the valued differential field F .

An example of such a field is given by the set F_0 of all formal power series

$$A = \sum_{\varrho=r}^{\infty} a_{\varrho} x^{\varrho},$$

where r denotes an arbitrary integer and where the coefficients a_{ϱ} are taken from a field K of characteristic zero. F_0 admits, as is well-known, the following non-Archimedean valuation

$$|A| = 0 \text{ for } A = 0, \quad |A| = e^{-r} \text{ if } a_r \neq 0.$$

We define $A' = \sum_{\varrho=r}^{\infty} \varrho a_{\varrho} x^{\varrho-1}$ as the derivative of $A = \sum_{\varrho=r}^{\infty} a_{\varrho} x^{\varrho}$.

One easily verifies that also the conditions A and C are satisfied for F_0 . In this case the lower and upper bounds α and β may both be put equal to the number e .

In the preceding chapter we developed a method to find in an effective way a set of "Von Neumann-numbers", i.e. a set of real numbers with the power of the continuum and such that n arbitrarily chosen numbers from this set are always algebraically independent over the rationals.

The same method could even be applied to a much more general problem, where instead of the real numbers elements of a complete valued field were taken, in which a certain sub-ring R played the part of the ring of integers in the field of real numbers.

It is the purpose of this chapter to generalize this result even more. Here we consider a differential field F as introduced before. In section 4 we give a method to find elements $A_1, A_2, \dots, A_n$ of F such that these elements together with all their derivatives $A_1^{(\tau)}, A_2^{(\tau)}, \dots, A_n^{(\tau)}$ ($\tau = 0, 1, 2, \dots$) are algebraically independent over a certain sub-ring R of F . For this main result we refer the reader to section 4.

The scope of this generalization might become clearer if we cite at this point already an application of our main theorem to the special case of the field F_0 of formal power series over K .

Theorem 2.1. *Let K be a field of characteristic zero. Let $u_1, u_2, \dots, u_n$ denote positive numbers such that $u_1 > u_2 > \dots > u_n$. Let $\varphi_m(u)$ ($m = 1, 2, \dots$) be functions of the variable $u \geq 0$ with functional values in K such that $\varphi_m(u) \neq 0$ for all $m = 1, 2, \dots, u \geq 0$. Let t be an arbitrary integer ≥ 0 . Consider the n power series*

$$A_v = \sum_{m=1}^{\infty} \varphi_m(u_v) x^{m - [m u_v]} \quad (v = 1, 2, \dots, n).$$

Then $A_1, \dots, A_1^{(t)}, \dots, A_n, \dots, A_n^{(t)}$ are algebraically independent over the ring of all polynomials in x over K .

This theorem clearly is a generalization of Theorem 1.3.

Before stating the main result we let precede several lemmas. One of the most important is a lemma we already used in the previous chapter (compare lemma 3), namely the following

Lemma 1. Let $\mathfrak{B}$ be a ring with identity-element and let R be any sub-ring containing the identity-element. Then the elements $u_1, u_2, \dots, u_n$ of $\mathfrak{B}$ are algebraically independent over R if and only if each $u_k, k = 1, 2, \dots, n$, is transcendental over $R[u_1, u_2, \dots, u_{k-1}]$, i.e. the ring generated from R by $u_1, u_2, \dots, u_{k-1}$ (compare e.g. JACOBSON [1], p. 105, lemma).

2. In the following we shall use the lemmas 2, 3 and 4, all due to KOLCHIN [3], p. 240 and 241. For the convenience of the reader we also give here the proofs.

Lemma 2. If F is a valued differential field with lower bound α and upper bound β , then the second inequality in (1) holds for every $a \in F$, and the first inequality in (1) holds for every $a \in F$ with $|a| \neq 1$ (KOLCHIN [3], p. 240, lemma 1).

Proof. If $|a| < 1$ then (1) holds by definition. If $|a| > 1$ then $a \neq 0$ and $|a^{-1}| < 1$; since $\left|\frac{a'}{a}\right| = \left|\frac{(a^{-1})'}{a^{-1}}\right|$, on account of $\frac{(a^{-1})'}{a^{-1}} = \frac{-a'a^{-2}}{a^{-1}} = -\frac{a'}{a}$, again (1) holds.

It remains to prove the second part of (1) if $|a| = 1$.

By hypothesis there exists a non-zero element $b \in F$ with $|b| \neq 1$, whence $|ab| \neq 1$. Now $\left|\frac{b'}{b}\right| \leq \beta$ and $\left|\frac{a'}{a} + \frac{b'}{b}\right| = \left|\frac{(ab)'}{ab}\right| \leq \beta$; if $\left|\frac{a'}{a}\right| \leq \left|\frac{b'}{b}\right|$ then obviously $\left|\frac{a'}{a}\right| \leq \beta$, whereas if $\left|\frac{a'}{a}\right| > \left|\frac{b'}{b}\right|$ then $\left|\frac{a'}{a}\right| = \left|\frac{a'}{a} + \frac{b'}{b}\right| \leq \beta$.

Corollary. Hypothesis as in lemma 2, let n be a positive integer. Then $|a^{(n)}| \leq \beta^n |a|$ for every $a \in F$ and $|a^{(n)}| \geq \alpha^n |a|$ for every $a \in F$ with $|a| > 1$ and $|a| > \alpha^{-(n-1)}$ (KOLCHIN [3], p. 240, corollary 1).

Proof. By mathematical induction with respect to n .

If $(a_1, \dots, a_n)$ is a finite sequence of elements of a differential ring with identity-element, we denote the Wronskian $\det(a_j^{(i-1)})$, $i = 1, 2, \dots, n$; $j = 1, 2, \dots, n$, by $W(a_1, \dots, a_n)$. The Wronskian equals a_1 if $n = 1$. If $n > 0$ and we expand the determinant by the minors of the last row, we obtain the formula

$$(2) \quad \sum_{j=1}^n (-1)^{n+j} a_j^{(n-1)} W(a_1, \dots, a_{j-1}, a_{j+1}, \dots, a_n) = W(a_1, \dots, a_n).$$

Applying the same device to the determinant, obtained on replacing the last row by one of the other rows, we obtain the formula

$$(3) \quad \sum_{j=1}^n (-1)^{n+j} a_j^{(i)} W(a_1, \dots, a_{j-1}, a_{j+1}, \dots, a_n) = 0 \quad (i = 0, 1, \dots, n-2).$$

Lemma 3. If $b, a_1, \dots, a_n$ are elements of a differential field, then $W(ba_1, \dots, ba_n) = b^n W(a_1, \dots, a_n)$ (KOLCHIN [3], p. 241, lemma 2).

Proof. If $n = 1$ this is obvious. Let $n > 1$ and suppose the result already proved for lower values of n . Then, by (2) and (3),

$$\begin{aligned} W(ba_1, \dots, ba_n) &= \sum_{j=1}^n (-1)^{n+j} (ba_j)^{(n-1)} W(ba_1, \dots, ba_{j-1}, ba_{j+1}, \dots, ba_n) \\ &= \sum_{j=1}^n (-1)^{n+j} \sum_{i=0}^{n-1} \binom{n-1}{i} b^{(n-1-i)} a_j^{(i)} b^{n-1} W(a_1, \dots, a_{j-1}, a_{j+1}, \dots, a_n) \\ &= b^{n-1} \sum_{i=0}^{n-1} \binom{n-1}{i} b^{(n-1-i)} \sum_{j=1}^n (-1)^{n+j} a_j^{(i)} W(a_1, \dots, a_{j-1}, a_{j+1}, \dots, a_n) \\ &= b^{n-1} b W(a_1, \dots, a_n) = b^n W(a_1, \dots, a_n). \end{aligned}$$

Lemma 4. Let $a_1, \dots, a_n$ be elements of a valued differential field with lower bound α and upper bound β . Then

- a) $|W(a_1, \dots, a_n)| \leq \beta^{\frac{1}{2}n(n-1)} |a_1 \dots a_n|$
b) $|W(a_1, \dots, a_n)| \geq \alpha^{\frac{1}{2}n(n-1)} |a_1 \dots a_n|$ if $|a_j| < (\alpha/\beta)^{j-2} |a_{j-1}|$ ($j = 2, 3, \dots, n$)
(KOLCHIN [3], p. 241, lemma 3).

Proof. The lemma is obvious if $n = 1$, and also if $a_j = 0$ for some j . Let $n > 1$ and $a_j \neq 0$ for every j , and suppose the lemma already proved for lower values of n . By lemma 3 and using $e' = e'' = \dots = e^{(n-1)} = 0$,

$$W(a_1, \dots, a_n) = a_1^n W\left(e, \frac{a_2}{a_1}, \dots, \frac{a_n}{a_1}\right) = a_1^n W\left(\left(\frac{a_2}{a_1}\right)', \dots, \left(\frac{a_n}{a_1}\right)'\right).$$

Then, by lemma 2,

$$\begin{aligned} |W(a_1, \dots, a_n)| &\leq |a_1|^n \beta^{\frac{1}{2}(n-1)(n-2)} \left| \left(\frac{a_2}{a_1}\right)' \dots \left(\frac{a_n}{a_1}\right)' \right| \\ &\leq |a_1|^n \beta^{\frac{1}{2}(n-1)(n-2)} \beta \left| \frac{a_2}{a_1} \right| \dots \beta \left| \frac{a_n}{a_1} \right| = \beta^{\frac{1}{2}n(n-1)} |a_1 \dots a_n|, \end{aligned}$$

which proves the inequality a).

Also, under the condition of part b), on account of lemma 3 and 2,

$$\begin{aligned} |W(a_1, \dots, a_n)| &\geq |a_1|^n \alpha^{\frac{1}{2}(n-1)(n-2)} \left| \left(\frac{a_2}{a_1}\right)' \dots \left(\frac{a_n}{a_1}\right)' \right| \\ &\geq |a_1|^n \alpha^{\frac{1}{2}(n-1)(n-2)} \alpha \left| \frac{a_2}{a_1} \right| \dots \alpha \left| \frac{a_n}{a_1} \right| \\ &= \alpha^{\frac{1}{2}n(n-1)} |a_1 \dots a_n|. \end{aligned}$$

3. We require moreover

D) The valued differential field F is complete with respect to its valuation. We then have the following simple lemma

Lemma 5. If the series $a_0 + a_1 + a_2 + \dots$, consisting of elements from F , is convergent with sum s , then the series $a_0' + a_1' + a_2' + \dots$ is convergent with sum s' .

Proof. $s \in F$, as F is complete. Put $s_n = a_0 + a_1 + \dots + a_n$, then $s_n \in F$ and, on account of the convergence, for $\varepsilon > 0$

$$|s - s_n| < \varepsilon \quad (n \geq n_0(\varepsilon)).$$

Now $s_n' = a_0' + a_1' + \dots + a_n'$ with $s_n' \in F$. Applying lemma 2, we obtain for the derivative $s' \in F$ of s

$$|s' - s_n'| = |(s - s_n)'| \leq \beta |s - s_n| < \beta \varepsilon,$$

so $a_0' + a_1' + a_2' + \dots$ is convergent with sum s' .

Remark. If the valued differential field F is not yet complete with respect to its valuation, we can make F complete by means of the well-

known Cantor-method (compare e.g. VAN DER WAERDEN [6], § 68). Then, for the complete field Ω_F , each fundamental sequence from Ω_F has a limit in Ω_F . We shall prove: Ω_F is again a differential field.

Quite similar to the proof of lemma 5 we can show: if $\{a_n\}$ is a fundamental sequence in F with $A = \lim_{n \rightarrow \infty} a_n$, where $A \in \Omega_F$, then also $\{a_n'\}$ is a fundamental sequence. Now we introduce $A' \stackrel{\text{def}}{=} \lim_{n \rightarrow \infty} a_n'$, where A' is an element of Ω_F depending on A , but, as one easily sees, not on the choice of the sequence $a_0, a_1, \dots$. Let in the same way $B = \lim_{n \rightarrow \infty} b_n$ for a fundamental sequence $\{b_n\}$ of F and $B' \stackrel{\text{def}}{=} \lim_{n \rightarrow \infty} b_n'$, where B' is an element of Ω_F depending on B and not on the choice of the sequence $b_0, b_1, \dots$.

We have to show that Ω_F has the properties A, B and C.

Ad A:

$$\begin{aligned} 1^\circ \quad (A+B)' &= (\lim_{n \rightarrow \infty} (a_n + b_n))' \stackrel{\text{def}}{=} \lim_{n \rightarrow \infty} (a_n + b_n)' = \lim_{n \rightarrow \infty} a_n' + \lim_{n \rightarrow \infty} b_n' \stackrel{\text{def}}{=} A' + B'; \\ 2^\circ \quad (AB)' &= (\lim_{n \rightarrow \infty} a_n b_n)' \stackrel{\text{def}}{=} \lim_{n \rightarrow \infty} (a_n b_n)' \\ &= \lim_{n \rightarrow \infty} a_n' \lim_{n \rightarrow \infty} b_n' + \lim_{n \rightarrow \infty} a_n' \lim_{n \rightarrow \infty} b_n \stackrel{\text{def}}{=} AB' + A'B. \end{aligned}$$

Ad B:

It is well-known that Ω_F has a valuation, namely if for any $A \in \Omega_F$ we define $|A|$ as $\lim_{n \rightarrow \infty} |a_n|$.

Ad C:

We have $|A| = \lim_{n \rightarrow \infty} |a_n|$, $|A'| = \lim_{n \rightarrow \infty} |a_n'|$. Since $|a_n'| \leq \beta |a_n|$, we have $|A'| \leq \beta |A|$ and, if $|A| \neq 1$, clearly $|a_n| \neq 1$ for $n \geq n_0$, hence $\alpha |a_n| \leq |a_n'|$, which implies $\alpha |A| \leq |A'|$.

4. For our purpose we also need that the valued field F moreover has the property

E) There exists in F a sub-ring R containing the identity-element of F , such that each non-zero element of R has value ≥ 1 , and that there exists at least one element a of R with $|a| > 1$.

The field F_0 of all formal power series $\sum_{q=r}^{\infty} a_q x^q$, introduced before, has all the properties A through E: it is complete with respect to its valuation, introduced in section 1, and for the sub-ring R we can take the set of all polynomials in x^{-1} . Moreover it is of characteristic zero, since the coefficients a_q of the power series are contained in a field of characteristic zero by hypothesis.

Our main result is the following theorem:

Theorem 2.2. *Let the valued differential field F and its sub-ring R satisfy the conditions A, B, C, D and E. Let F be of characteristic zero. Let n and t denote arbitrary positive integers, let*

$$A_\nu = \sum_{m=0}^{\infty} \frac{a_{\nu m}}{\beta_0 \beta_1 \dots \beta_m} \quad (\nu = 1, 2, \dots, n),$$

where $a_{\nu m}, \beta_m$ denote non-vanishing elements of the sub-ring R with $|\beta_m| \rightarrow \infty$ if $m \rightarrow \infty$. Moreover let for $m \rightarrow \infty$

$$\begin{aligned} |a_{nm}| &= o(|a_{n-1,m}|), |a_{n-1,m}| = o(|a_{n-2,m}|), \dots, |a_{2m}| = o(|a_{1m}|) \\ |a_{1m}| &= O(|b_{m-1}|), \text{ where } b_m = \beta_0 \beta_1 \dots \beta_m, \\ \log |b_{m-1}| &= o(\log |b_m|) \end{aligned}$$

(i.e. these are essentially the same conditions as in Theorem 1.2).

Then $A_1, A_1', \dots, A_1^{(t)}, A_2, A_2', \dots, A_2^{(t)}, \dots, A_n, A_n', \dots, A_n^{(t)}$ are algebraically independent over R ²⁾.

We remark without proof that the case $n=1$ of this theorem easily follows from KOLCHIN's Approximation theorem (KOLCHIN [3], p. 244):

Let F be a valued differential field, let Z be a non-zero differential sub-ring of F such that $|a| \geq 1$ for every non-zero element $a \in Z$, let $u \in F$ be differentially algebraic over Z , let s be any natural number ≥ 1 , and denote the s -denomination of u over Z ³⁾ by d_s . Then there exists a positive number γ such that

$$\left| u - \frac{a}{b^s} \right| \geq \frac{\gamma}{|b|^{d_s}}$$

for all elements $a, b \in Z$ with $b \neq 0$ and $u \neq a/b^s$.

5. Lemma 6. Let the valued differential field F and its sub-ring R satisfy the conditions A, B, C, D and E. Let n and t denote arbitrary positive integers, let

$$A_\nu = \sum_{m=0}^{\infty} \frac{a_{\nu m}}{\beta_0 \beta_1 \dots \beta_m} \quad (\nu = 1, 2, \dots, n),$$

where $a_{\nu m}, \beta_m$ are non-vanishing elements of the sub-ring R with $|\beta_m| \rightarrow \infty$ if $m \rightarrow \infty$.

Moreover let for $m \rightarrow \infty$

$$(4) \quad \begin{cases} |a_{\nu m}| = o(|a_{1m}|) \text{ for } \nu = 2, 3, \dots, n \\ |a_{1m}| = O(|b_{m-1}|), \text{ where } b_m = \beta_0 \beta_1 \dots \beta_m, \\ \log |b_{m-1}| = o(\log |b_m|). \end{cases}$$

²⁾ From the conditions it is easily seen that the terms $\frac{a_{\nu m}}{\beta_0 \beta_1 \dots \beta_m}$ tend to zero if $m \rightarrow \infty$, so that the series for A_ν given above converge.

³⁾ For the definition of the s -denomination of u over Z see KOLCHIN [3], p. 243, 244.

Let

$$f(x_{10}, x_{11}, \dots, x_{1t}, x_{20}, x_{21}, \dots, x_{2t}, \dots, x_{n0}, x_{n1}, \dots, x_{nt}) = \sum_{(h)} c(h) x_{10}^{h_{10}} \dots x_{nt}^{h_{nt}}$$

denote an arbitrarily chosen polynomial over R in the indeterminates

$$x_{10}, x_{11}, \dots, x_{1t}, x_{20}, x_{21}, \dots, x_{2t}, \dots, x_{n0}, x_{n1}, \dots, x_{nt}.$$

Let τ be chosen arbitrarily in the sequence $0, 1, \dots, t$.

Then the two relations

$$(5) \quad \begin{cases} f(A_1, A_1', \dots, A_1^{(t)}, \dots, A_n, A_n', \dots, A_n^{(t)}) = 0 \\ \frac{\partial f}{\partial x_{1\tau}}(A_1, A_1', \dots, A_1^{(t)}, \dots, A_n, A_n', \dots, A_n^{(t)}) \neq 0 \end{cases}$$

cannot be satisfied simultaneously.

Proof. Since $A_v = \sum_{m=0}^{\infty} \frac{a_{vm}}{b_m}$, we have by lemma 5 clearly

$$A_v^{(\tau)} = \sum_{m=0}^{\infty} \left(\frac{a_{vm}}{b_m} \right)^{(\tau)} \quad (\tau = 1, 2, \dots, t).$$

Let us suppose that there exists a polynomial

$$f(x_{10}, x_{11}, \dots, x_{1t}, \dots, x_{n0}, x_{n1}, \dots, x_{nt})$$

over R satisfying both relations (5).

We shall reach a contradiction by applying Taylor's formula in the form as used in Chapter I, section 2. Let k denote a positive integer, later to be chosen arbitrarily large. Let

$$B_{vk} \stackrel{\text{def}}{=} \sum_{m=0}^{k-1} \frac{a_{vm}}{b_m}, \quad v_{vk} \stackrel{\text{def}}{=} - \sum_{m=k}^{\infty} \frac{a_{vm}}{b_m},$$

so that

$$B_{vk}^{(\tau)} = A_v^{(\tau)} + v_{vk}^{(\tau)} \quad (v = 1, 2, \dots, n; \tau = 0, 1, \dots, t).$$

Applying Taylor's formula and using

$$f(A_1, A_1', \dots, A_1^{(t)}, \dots, A_n, A_n', \dots, A_n^{(t)}) = 0,$$

we obtain

$$(6) \quad \begin{cases} f(B_{1k}, B_{1k}', \dots, B_{1k}^{(t)}, \dots, B_{nk}, B_{nk}', \dots, B_{nk}^{(t)}) \\ = \sum_{\tau=0}^t v_{1k}^{(\tau)} f_{1\tau}(A_1, A_1', \dots, A_1^{(t)}, \dots, A_n, A_n', \dots, A_n^{(t)}) \\ + \dots + \sum_{\tau=0}^t v_{nk}^{(\tau)} f_{n\tau}(A_1, A_1', \dots, A_1^{(t)}, \dots, A_n, A_n', \dots, A_n^{(t)}) \\ + \text{terms of degree } \geq 2 \text{ in the } v_{vk}^{(\tau)}\text{'s,} \end{cases}$$

where

$$f_{v\tau} = \frac{\partial f}{\partial x_{v\tau}} \quad (v = 1, 2, \dots, n; \tau = 0, 1, \dots, t),$$

or

$$(6a) \quad \begin{cases} f(B_{1k}, B'_{1k}, \dots, B_{1k}^{(t)}, \dots, B_{nk}, B'_{nk}, \dots, B_{nk}^{(t)}) \\ = \sum_{\tau=0}^t v_{1k}^{(\tau)} f_{1\tau}(A_1, A_1', \dots, A_1^{(t)}, \dots, A_n, A_n', \dots, A_n^{(t)}) - \varepsilon_k, \end{cases}$$

where

$$\begin{aligned} -\varepsilon_k &= \sum_{\tau=0}^t v_{2k}^{(\tau)} f_{2\tau}(A_1, A_1', \dots, A_1^{(t)}, \dots, A_n, A_n', \dots, A_n^{(t)}) \\ &\quad + \dots + \sum_{\tau=0}^t v_{nk}^{(\tau)} f_{n\tau}(A_1, A_1', \dots, A_1^{(t)}, \dots, A_n, A_n', \dots, A_n^{(t)}) \\ &\quad + \text{terms of degree } \geq 2 \text{ in the } v_{\nu k}^{(\tau)} \text{'s.} \end{aligned}$$

From the definition of $v_{\nu k}$ one obtains

$$v_{\nu k} + \frac{a_{\nu k}}{b_k} = - \sum_{m=k+1}^{\infty} \frac{a_{\nu m}}{b_m},$$

hence, by (4),

$$\begin{aligned} \left| v_{\nu k} + \frac{a_{\nu k}}{b_k} \right| &= O\left(\sum_{m=k+1}^{\infty} \frac{|b_{m-1}|}{|b_m|} \right) \\ &= O\left(\sum_{m=k+1}^{\infty} |b_{m-1}|^{-2} \right) \\ &= O(|b_k|^{-2}) \text{ if } k \rightarrow \infty, \end{aligned}$$

or

$$(7) \quad v_{\nu k} = -\frac{a_{\nu k}}{b_k} + O(|b_k|^{-2}) \text{ if } k \rightarrow \infty \quad (\nu = 1, 2, \dots, n).$$

It follows therefore from (4) that

$$(8) \quad \begin{cases} v_{\nu k} \rightarrow 0 \text{ if } k \rightarrow \infty & (\nu = 1, 2, \dots, n) \\ |v_{\nu k}| = o(|v_{1k}|) \text{ if } k \rightarrow \infty & (\nu = 2, 3, \dots, n) \\ v_{\nu k} \neq 0 & (\nu = 1, 2, \dots, n) \text{ for } k \geq k_0. \end{cases}$$

Moreover, according to the corollary of lemma 2, we have

$$(9) \quad |v_{\nu k}^{(\tau)}| \leq \beta^{\tau} |v_{\nu k}| \quad (\nu = 1, 2, \dots, n; \tau = 0, 1, \dots, t).$$

Let P_k be the sum of the terms of degree ≥ 2 in the $v_{\nu k}^{(\tau)}$'s in (6) and let

$$\begin{aligned} Q_k &\stackrel{\text{def}}{=} \sum_{\tau=0}^t v_{2k}^{(\tau)} f_{2\tau}(A_1, A_1', \dots, A_1^{(t)}, \dots, A_n, A_n', \dots, A_n^{(t)}) \\ &\quad + \dots + \sum_{\tau=0}^t v_{nk}^{(\tau)} f_{n\tau}(A_1, A_1', \dots, A_1^{(t)}, \dots, A_n, A_n', \dots, A_n^{(t)}), \end{aligned}$$

then we derive from (8) and (9)

$$|P_k| = O(|v_{1k}|^2) = o(|v_{1k}|) \text{ if } k \rightarrow \infty$$

and

$$|Q_k| = O(\max_{j=2, \dots, n} |r_{jk}|) = o(|r_{1k}|) \text{ if } k \rightarrow \infty.$$

Now, by the definition of ε_k ,

$$|\varepsilon_k| \leq \max(|P_k|, |Q_k|),$$

hence

$$(10) \quad |\varepsilon_k| = o(|v_{1k}|) \text{ if } k \rightarrow \infty.$$

From (6a) we have the following system of $t+1$ linear equations for $f_{10}, f_{11}, \dots, f_{1t}$:

$$(11) \left\{ \begin{aligned} & f(B_{1k}, \dots, B_{1k}^{(t)}, \dots, B_{nk}, \dots, B_{nk}^{(t)}) \\ & \quad = \sum_{\tau=0}^t v_{1k}^{(\tau)} f_{1\tau}(A_1, \dots, A_1^{(t)}, \dots, A_n, \dots, A_n^{(t)}) - \varepsilon_k \\ & f(B_{1,k+1}, \dots, B_{1,k+1}^{(t)}, \dots, B_{n,k+1}, \dots, B_{n,k+1}^{(t)}) \\ & \quad = \sum_{\tau=0}^t v_{1,k+1}^{(\tau)} f_{1\tau}(A_1, \dots, A_1^{(t)}, \dots, A_n, \dots, A_n^{(t)}) - \varepsilon_{k+1} \\ & \text{-----} \\ & f(B_{1,k+t}, \dots, B_{1,k+t}^{(t)}, \dots, B_{n,k+t}, \dots, B_{n,k+t}^{(t)}) \\ & \quad = \sum_{\tau=0}^t v_{1,k+t}^{(\tau)} f_{1\tau}(A_1, \dots, A_1^{(t)}, \dots, A_n, \dots, A_n^{(t)}) - \varepsilon_{k+t}. \end{aligned} \right.$$

Using (10), we have here

$$|\varepsilon_{k+j}| = o(|v_{1,k+j}|) \text{ if } k \rightarrow \infty \quad (j = 0, 1, \dots, t).$$

Now assume the $t+1$ left-hand sides of (11) to vanish simultaneously, then we shall reach a contradiction if k is sufficiently large. Solving (11) for

$$f_{1\tau} = f_{1\tau}(A_1, \dots, A_1^{(t)}, \dots, A_n, \dots, A_n^{(t)}) \quad (\tau = 0, 1, \dots, t),$$

we find then by Cramer's rule

$$(12) \quad f_{1\tau} = \frac{\begin{vmatrix} v_{1k} & v'_{1k} & \dots & v_{1k}^{(\tau-1)} & \varepsilon_k & v_{1k}^{(\tau+1)} & \dots & v_{1k}^{(t)} \\ v_{1,k+1} & v'_{1,k+1} & \dots & v_{1,k+1}^{(\tau-1)} & \varepsilon_{k+1} & v_{1,k+1}^{(\tau+1)} & \dots & v_{1,k+1}^{(t)} \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ v_{1,k+t} & v'_{1,k+t} & \dots & v_{1,k+t}^{(\tau-1)} & \varepsilon_{k+t} & v_{1,k+t}^{(\tau+1)} & \dots & v_{1,k+t}^{(t)} \end{vmatrix}}{W(v_{1k}, v_{1,k+1}, \dots, v_{1,k+t})},$$

where $W(v_{1k}, v_{1,k+1}, \dots, v_{1,k+t})$ denotes the Wronskian of $v_{1k}, v_{1,k+1}, \dots, v_{1,k+t}$, provided that this last expression does not vanish.

In order to prove that this last condition is satisfied for sufficiently large k , we first remark that $v_{1k}, v_{1,k+1}, \dots, v_{1,k+t}$ do not vanish because of (8). Moreover we derive from (7) and (4), on account of $|a_{1m}| \geq 1$, for $j = 1, 2, \dots, t$

$$\begin{aligned}
\frac{|v_{1,k+j}|}{|v_{1,k+j-1}|} &= \frac{\left| -\frac{\alpha_{1,k+j}}{b_{k+j}} + O(|b_{k+j}|^{-2}) \right|}{\left| -\frac{\alpha_{1,k+j-1}}{b_{k+j-1}} + O(|b_{k+j-1}|^{-2}) \right|} \\
&= O\left(\left| \frac{\alpha_{1,k+j}}{\alpha_{1,k+j-1}} \frac{b_{k+j-1}}{b_{k+j}} \right| \right) \\
&= O\left(\frac{|\alpha_{1,k+j}| |b_{k+j-1}|}{|b_{k+j}|} \right) \\
&= O\left(\frac{|b_{k+j-1}|^2}{|b_{k+j}|} \right) \rightarrow 0 \text{ if } k \rightarrow \infty.
\end{aligned}$$

It follows for sufficiently large k that

$$|v_{1,k+j}| < (\alpha/\beta)^{j-1} |v_{1,k+j-1}| \quad (j = 1, 2, \dots, t),$$

hence, applying lemma 4, part b), with $v_{1k}, v_{1,k+1}, \dots, v_{1,k+t}$ instead of $a_1, a_2, \dots, a_n$,

$$(13) \quad |W(v_{1k}, v_{1,k+1}, \dots, v_{1,k+t})| \geq \alpha^{\frac{1}{2}t(t+1)} |v_{1k} v_{1,k+1} \dots v_{1,k+t}| > 0.$$

Working out the determinant of (12), using formula (9), we find as an upperbound of its valuation

$$\max_{j=0,1,\dots,t} (|\varepsilon_{k+j}| \cdot \beta^{\frac{1}{2}t(t+1)-\tau} \cdot |v_{1k} \dots v_{1,k+j-1} v_{1,k+j+1} \dots v_{1,k+t}|),$$

hence we obtain from (12) and (13)

$$|f_{1\tau}| \leq \max_{j=0,1,\dots,t} \left(\frac{\beta^{\frac{1}{2}t(t+1)-\tau}}{\alpha^{\frac{1}{2}t(t+1)}} \frac{|\varepsilon_{k+j}|}{|v_{1,k+j}|} \right),$$

therefore $f_{1\tau} \rightarrow 0$ if $k \rightarrow \infty$, by (10).

Hence, since the $f_{1\tau}$ are independent of k , we have

$$f_{10} = f_{11} = \dots = f_{1t} = 0.$$

This contradicts (5), so the left-hand sides of (11) cannot vanish simultaneously for sufficiently large k .

Therefore we may assume

$$f(B_{1,k+p}, \dots, B_{1,k+p}^{(t)}, \dots, B_{n,k+p}, \dots, B_{n,k+p}^{(t)}) \neq 0$$

for some $p=p(k)$, chosen from the sequence $0, 1, \dots, t$.

By mathematical induction one can see that for $\sigma=0, 1, 2, \dots$

$b_m^{\sigma+1}(b_m^{-1})^{(\sigma)}$ is a polynomial expression with integral coefficients in $b_m, b'_m, \dots, b_m^{(\sigma)}$, so that

$b_m^{\sigma+1} \left(\frac{a_{vm}}{b_m} \right)^{(\sigma)}$ is a polynomial expression in $a_{vm}, a'_{vm}, \dots, a_{vm}^{(\sigma)}, b_m, b'_m, \dots, b_m^{(\sigma)}$.

It follows therefore from the definition of $B_{\nu k}^{(\sigma)}$ for $\sigma = 0, 1, \dots, t$ that

$$\begin{aligned} b_{k+p-1}^{t+1} B_{\nu, k+p}^{(\sigma)} &= (\beta_0 \beta_1 \dots \beta_{k+p-1})^{t+1} B_{\nu, k+p}^{(\sigma)} \\ &= \sum_{m=0}^{k+p-1} \left(\frac{a_{\nu m}}{b_m} \right)^{(\sigma)} b_m^{t+1} (\beta_{m+1} \dots \beta_{k+p-1})^{t+1} \in R, \end{aligned}$$

hence, if the total degree of $f(x_{10}, \dots, x_{1t}, \dots, x_{n0}, \dots, x_{nt})$ is denoted by s ,

$$b_{k+p-1}^{(t+1)s} f(B_{1, k+p}, \dots, B_{1, k+p}^{(t)}, \dots, B_{n, k+p}, \dots, B_{n, k+p}^{(t)}) \in R.$$

For sufficiently large k and suitably chosen $p=p(k)$ this element does not vanish, hence, on account of the definition of the sub-ring R ,

$$(14) \quad |b_{k+p-1}^{(t+1)s} f(B_{1, k+p}, \dots, B_{1, k+p}^{(t)}, \dots, B_{n, k+p}, \dots, B_{n, k+p}^{(t)})| \geq 1.$$

On the other hand it follows from (6a), (9), (10), (7) and (4) for $k \rightarrow \infty$ that

$$(15) \quad \begin{cases} |f(B_{1, k+p}, \dots, B_{1, k+p}^{(t)}, \dots, B_{n, k+p}, \dots, B_{n, k+p}^{(t)})| \\ = O(|v_{1, k+p}|) = O\left(\frac{|a_{1, k+p}|}{|b_{k+p}|}\right) = O\left(\frac{|b_{k+p-1}|}{|b_{k+p}|}\right). \end{cases}$$

Comparing (14) and (15), we obtain for sufficiently large k and $p=p(k)$

$$|b_{k+p-1}|^{-(t+1)s} < C \frac{|b_{k+p-1}|}{|b_{k+p}|},$$

where C stands for a positive number independent of k . This last inequality contradicts (4), which proves our lemma.

6. Lemma 7. Let the valued differential field F and its sub-ring R satisfy the conditions A, B, C, D and E. Moreover let F be of characteristic zero.

Let $A_1^{(\tau)}, A_2^{(\tau)}, \dots, A_n^{(\tau)}$ ($\tau=0, 1, \dots, t$) be defined as in the preceding lemma. Then, for $\tau=0, 1, \dots, t$, $A_1^{(\tau)}$ is transcendental over the ring

$$R[A_1, A_1', \dots, A_1^{(\tau-1)}, A_1^{(\tau+1)}, \dots, A_1^{(t)}, A_2, A_2', \dots, A_2^{(t)}, \dots, A_n, A_n', \dots, A_n^{(t)}],$$

generated from R by

$$A_1, A_1', \dots, A_1^{(\tau-1)}, A_1^{(\tau+1)}, \dots, A_1^{(t)}, A_2, A_2', \dots, A_2^{(t)}, \dots, A_n, A_n', \dots, A_n^{(t)}.$$

Proof. Suppose that $A_1^{(\tau)}$ is algebraic over

$$R[A_1, A_1', \dots, A_1^{(\tau-1)}, A_1^{(\tau+1)}, \dots, A_1^{(t)}, A_2, A_2', \dots, A_2^{(t)}, \dots, A_n, A_n', \dots, A_n^{(t)}],$$

so that $A_1^{(\tau)}$ satisfies an equation

$$D_0 + D_1 x + \dots + D_r x^r = 0,$$

where the coefficients

$$\begin{aligned} D_\varrho = \sum_{(h)} d_{\varrho, (h)} A_1^{h_{10}} \dots (A_1^{(\tau-1)})^{h_{1, \tau-1}} (A_1^{(\tau+1)})^{h_{1, \tau+1}} \dots \\ \dots (A_1^{(t)})^{h_{1t}} \dots A_n^{h_{n0}} \dots (A_n^{(t)})^{h_{nt}} \quad (\varrho = 0, 1, \dots, r) \end{aligned}$$

do not vanish simultaneously and where $d_{e,(h)} \in R$. We may suppose that the equation is of minimal degree r . It follows that $D_r \neq 0$, hence $rD_r \neq 0$, and therefore $A_1^{(\tau)}$ cannot satisfy the equation

$$D_1 + 2D_2x + \dots + rD_rx^{r-1} = 0.$$

Put

$$\begin{aligned} D_e(x_{10}, \dots, x_{1,\tau-1}, x_{1,\tau+1}, \dots, x_{1t}, x_{20}, \dots, x_{2t}, \dots, x_{n0}, \dots, x_{nt}) \\ \stackrel{\text{def}}{=} \sum_{(h)} d_{e,(h)} x_{10}^{h_{10}} \dots x_{1,\tau-1}^{h_{1,\tau-1}} x_{1,\tau+1}^{h_{1,\tau+1}} \dots x_{1t}^{h_{1t}} \dots x_{n0}^{h_{n0}} \dots x_{nt}^{h_{nt}} \end{aligned}$$

and

$$\begin{aligned} f(x_{10}, \dots, x_{1t}, x_{20}, \dots, x_{2t}, \dots, x_{n0}, \dots, x_{nt}) \\ \stackrel{\text{def}}{=} \sum_{e=0}^r D_e(x_{10}, \dots, x_{1,\tau-1}, x_{1,\tau+1}, \dots, x_{1t}, x_{20}, \dots, x_{2t}, \dots, x_{n0}, \dots, x_{nt}) x_{1\tau}^e. \end{aligned}$$

Then $f(x_{10}, \dots, x_{1t}, x_{20}, \dots, x_{2t}, \dots, x_{n0}, \dots, x_{nt})$ represents a polynomial over R with

$$f(A_1, \dots, A_1^{(t)}, A_2, \dots, A_2^{(t)}, \dots, A_n, \dots, A_n^{(t)}) = 0$$

and

$$\frac{\partial f}{\partial x_{1\tau}}(A_1, \dots, A_1^{(t)}, A_2, \dots, A_2^{(t)}, \dots, A_n, \dots, A_n^{(t)}) \neq 0.$$

But this contradicts the assertion of our preceding lemma.

Remark. A fortiori we have for $\tau = 0, 1, \dots, t$: $A_1^{(\tau)}$ is transcendental over the ring

$$R[A_1^{(\tau+1)}, \dots, A_1^{(t)}, A_2, \dots, A_2^{(t)}, \dots, A_n, \dots, A_n^{(t)}],$$

generated from R by

$$A_1^{(\tau+1)}, \dots, A_1^{(t)}, A_2, \dots, A_2^{(t)}, \dots, A_n, \dots, A_n^{(t)}.$$

7. We now come to the proof of our Theorem 2.2, mentioned in section 4.

Proof. Let k denote an arbitrary integer from the sequence $1, 2, \dots, n$. Then clearly for $m \rightarrow \infty$

$$\begin{aligned} |a_{\varkappa m}| &= o(|a_{km}|) \text{ for } \varkappa = k+1, k+2, \dots, n, \\ |a_{km}| &= O(|b_{m-1}|), \log |b_{m-1}| = o(\log |b_m|). \end{aligned}$$

Therefore we can apply lemma 7 with

$$A_k, A_k', \dots, A_k^{(t)}, A_{k+1}, A_{k+1}', \dots, A_{k+1}^{(t)}, \dots, A_n, A_n', \dots, A_n^{(t)}$$

instead of

$$A_1, A_1', \dots, A_1^{(t)}, A_2, A_2', \dots, A_2^{(t)}, \dots, A_n, A_n', \dots, A_n^{(t)}.$$

It follows that $A_k^{(\tau)}$ is transcendental over the ring

$$R[A_k^{(\tau+1)}, \dots, A_k^{(t)}, A_{k+1}, \dots, A_{k+1}^{(t)}, \dots, A_n, \dots, A_n^{(t)}].$$

This is true for $k=1, 2, \dots, n$; $\tau=0, 1, \dots, t$.

Hence, according to lemma 1, the elements

$$A_1, \dots, A_1^{(t)}, A_2, \dots, A_2^{(t)}, \dots, A_n, \dots, A_n^{(t)}$$

of F are algebraically independent over R .

Finally we remark that Theorem 2.1 is a consequence of Theorem 2.2. The proof is almost identical to the proof which we derived for Theorem 1.3.

REFERENCES

1. JACOBSON, N., Lectures in abstract algebra I. London, 1953.
2. KAPLANSKY, I., An introduction to differential algebra. Paris, 1957.
3. KOLCHIN, E. R., Rational approximation to solutions of algebraic differential equations, Proc. Amer. Math. Soc., 10, 238–244 (1959).
4. KUIPER, F. and J. POPKEN, On the so-called Von Neumann-numbers, Proc. Nederl. Akad. Wetensch. A, 65, 385–390 (1962); Indag. Math., 24, 385–390 (1962).
5. KUIPER, F., On algebraic independence in differential rings, Proc. Nederl. Akad. Wetensch. A, 67, 90–103 (1964); Indag. Math., 26, 90–103 (1964).
6. WAERDEN, B. L. VAN DER, Algebra I (5. Aufl.). Berlin–Göttingen–Heidelberg, 1960.

CHAPTER III

ON THE THEOREM OF BOMBIERI-MAHLER

1. Let $f(x) = \sum_{\mu=0}^m a_{\mu} x^{\mu}$ be an arbitrary polynomial with complex coefficients and with leading coefficient $a_m \neq 0$. We denote its *height* by $H(f) = \max(|a_0|, |a_1|, \dots, |a_m|)$. If α is an algebraic number we define its height $H(\alpha)$ as the height of the minimal polynomial of α , the coefficients of which are integers and relatively prime.

BOMBIERI [3], in 1958, proved the following theorem:

Let α and β be two different algebraic numbers which are not conjugates of one another and are of degrees m and n , and of heights $H(\alpha)$ and $H(\beta)$, respectively. Then

$$|\alpha - \beta| > (4mn)^{-3mn} H(\alpha)^{-n} H(\beta)^{-m}.$$

MAHLER [7] generalized this result to a theorem concerning the zeros of two polynomials with arbitrary complex coefficients. He obtained the following result:

Let f and g be two polynomials with complex coefficients, of degrees m and n , and of heights $H(f)$ and $H(g)$.

Let α be any zero of f , let β be any zero of g , and let $R(f, g)$ denote the resultant of f and g .

Then

$$\text{either } |\alpha - \beta| \geq 1$$

$$\text{or } |\alpha - \beta| \geq \{(m+1)^{2n}(n+1)^{2m}4^{mn}c(f, g)^{mn}H(f)^nH(g)^m\}^{-1}|R(f, g)|,$$

where $c(f, g) = 1$ when at least one of the polynomials has only real zeros and where otherwise $c(f, g) = \min(m+1, n+1)$. MAHLER also obtained a lower bound for the difference $|\alpha_1 - \alpha_2|$ of distinct zeros α_1 and α_2 of a single polynomial. He proved in this respect:

Let f be a polynomial with complex coefficients, of degree m and of height $H(f)$. Let α_1 and α_2 be two different zeros of f and let $D(f)$ denote the discriminant of f . Then

$$|\alpha_1 - \alpha_2| \geq \{(m+1)^{4m}4^{m^2}c(f)^{m^2}H(f)^{2m-1}\}^{-1}|a_m D(f)|,$$

where a_m denotes the leading coefficient of f and where $c(f) = 1$ when all zeros of f are real, while otherwise $c(f) = m+1$.

Our purpose in this chapter is to obtain in analogy with MAHLER's results theorems with respect to polynomials over a field F with a non-Archimedean valuation and satisfying certain conditions. The *height of a polynomial* can again be defined as the maximum of the valuations of its coefficients.

In the case of a complex field the results obtained by MAHLER have been sharpened by GÜTING [5], but we have no results in that direction.

2. In the sequel let F be a field with a *non-Archimedean* valuation. We suppose in the following that there exists an arithmetical function φ with $\varphi(n) \geq 1$ ($n = 1, 2, \dots$) and with the property: for any n elements $a_1, a_2, \dots, a_n$ of F there exists an element A of F with $1 \leq |A| \leq \varphi(n)$, $|a_\nu - A| \geq 1$ ($\nu = 1, 2, \dots, n$).

In such fields the theorems of MAHLER have the following analoga:

Theorem 3.1. *Let*

$$\begin{aligned} f(x) &= a_m x^m + a_{m-1} x^{m-1} + \dots + a_0, \quad a_m \neq 0, \\ g(x) &= b_n x^n + b_{n-1} x^{n-1} + \dots + b_0, \quad b_n \neq 0, \end{aligned}$$

be two polynomials over F of degrees m and n , and of heights $H(f)$ and $H(g)$. Suppose that f has exactly m zeros $\alpha_1, \alpha_2, \dots, \alpha_m$ and g exactly n zeros $\beta_1, \beta_2, \dots, \beta_n$ in F . Assume that the resultant $R(f, g)$ ⁴⁾ of f and g does not vanish and set

$$\Delta(f, g) = \min_{\substack{1 \leq \mu \leq m \\ 1 \leq \nu \leq n}} |\alpha_\mu - \beta_\nu|.$$

Then

$$\text{either } \Delta(f, g) \geq 1 \text{ or } \Delta(f, g) \geq \varphi(m+n)^{-2mn} H(f)^{-n} H(g)^{-m} |R(f, g)|.$$

Theorem 3.2. *Let*

$$f(x) = a_m x^m + a_{m-1} x^{m-1} + \dots + a_0, \quad a_m \neq 0,$$

be a polynomial over F of degree $m \geq 2$ and of height $H(f)$. Suppose that f has exactly m zeros $\alpha_1, \alpha_2, \dots, \alpha_m$ in F . Assume that the discriminant $D(f)$ ⁵⁾ of f does not vanish and set

$$\Delta(f) = \min_{1 \leq \mu < \nu \leq m} |\alpha_\mu - \alpha_\nu|.$$

Then

$$\Delta(f) \geq \varphi(m)^{-(2m^2-2m+1)} H(f)^{-(2m-1)} |a_m D(f)|.$$

⁴⁾ $R(f, g)$ is an element of F , as follows immediately from the determinant-form of the resultant

$$R(f, g) = \begin{vmatrix} a_m & a_{m-1} & \dots & a_0 & 0 & \dots & 0 \\ 0 & a_m & a_{m-1} & \dots & a_0 & \dots & 0 \\ \hline 0 & \dots & 0 & a_m & a_{m-1} & \dots & a_0 \\ b_n & b_{n-1} & \dots & b_0 & 0 & \dots & 0 \\ 0 & b_n & b_{n-1} & \dots & b_0 & \dots & 0 \\ \hline 0 & \dots & 0 & b_n & b_{n-1} & \dots & b_0 \end{vmatrix}.$$

⁵⁾ $D(f)$ is an element of F , as follows immediately from the relation $\pm a_m D(f) = R(f, f')$, where $R(f, f')$ is the resultant of f and f' .

Remarks.

1. It is sometimes possible to choose the element A such that $|A| = 1$. Theorem 3.1 yields in this case

$$\text{either } \Delta(f, g) \geq 1 \text{ or } \Delta(f, g) \geq H(f)^{-n} H(g)^{-m} |R(f, g)|,$$

while, by Theorem 3.2,

$$\Delta(f) \geq H(f)^{-(2m-1)} |a_m D(f)|.$$

2. If f and g are arbitrary polynomials over F , then the condition that the zeros $\alpha_1, \alpha_2, \dots, \alpha_m; \beta_1, \beta_2, \dots, \beta_n$ must be contained in F is in general not satisfied. But also in this case our theorems can be applied by taking a suitable extension field Φ of F and extending the given valuation of F to Φ .

3. Proof of Theorem 3.1.

By hypothesis there exists for the m elements $\alpha_1, \alpha_2, \dots, \alpha_m$ and the n elements $\beta_1, \beta_2, \dots, \beta_n$ of F an element A of F with $1 \leq |A| \leq \varphi(m+n)$ and such that

$$(1) \quad \begin{cases} |\alpha_\mu - A| \geq 1 & (\mu = 1, 2, \dots, m), \\ |\beta_\nu - A| \geq 1 & (\nu = 1, 2, \dots, n). \end{cases}$$

Then put

$$f^*(x) = f(x + A), \quad g^*(x) = g(x + A),$$

so that

$$f^*(x) = \sum_{\mu=0}^m a_\mu^* x^\mu \text{ and } g^*(x) = \sum_{\nu=0}^n b_\nu^* x^\nu \quad (a_m^* = a_m, \quad b_n^* = b_n)$$

are polynomials over F with zeros $\alpha_\mu^* = \alpha_\mu - A$ ($\mu = 1, 2, \dots, m$) and $\beta_\nu^* = \beta_\nu - A$ ($\nu = 1, 2, \dots, n$), respectively.

Hence, by (1),

$$(2) \quad |\alpha_\mu^*| \geq 1 (\mu = 1, 2, \dots, m), \quad |\beta_\nu^*| \geq 1 (\nu = 1, 2, \dots, n).$$

Clearly

$$\alpha_\mu^* - \beta_\nu^* = \alpha_\mu - \beta_\nu.$$

By hypothesis the resultant

$$R(f, g) = a_m^n b_n^m \prod_{\mu=1}^m \prod_{\nu=1}^n (\alpha_\mu - \beta_\nu) = a_m^n b_n^m \prod_{\mu=1}^m \prod_{\nu=1}^n (\alpha_\mu^* - \beta_\nu^*)$$

of f and g does not vanish, thus the minimal distance $\Delta(f, g)$ between the zeros of f and g is different from zero. Moreover $\Delta(f^*, g^*) = \Delta(f, g)$.

We choose the notation such that

$$\Delta(f, g) = |\alpha_1 - \beta_1|.$$

We assume, without loss of generality, that

$$\Delta(f, g) = |\alpha_1 - \beta_1| = |\alpha_1^* - \beta_1^*| < 1.$$

Hence, since $|\alpha_1^*| \geq 1$ by (2),

$$|\alpha_1^* - \beta_1^*| < |\alpha_1^*|,$$

so that

$$(3) \quad |\beta_1^*| = |\alpha_1^* - (\alpha_1^* - \beta_1^*)| = \max(|\alpha_1^*|, |\alpha_1^* - \beta_1^*|) = |\alpha_1^*|.$$

Since $a_m^* = a_m$, $b_n^* = b_n$, we may write the resultant in the form

$$(4) \quad R(f, g) = a_m^n \prod_{\mu=1}^m g^*(a_\mu^*).$$

We have

$$\begin{aligned} g^*(\alpha_1^*) &= b_n^*(\alpha_1^*)^n + b_{n-1}^*(\alpha_1^*)^{n-1} + \dots + b_0^*, \\ g^*(\beta_1^*) &= b_n^*(\beta_1^*)^n + b_{n-1}^*(\beta_1^*)^{n-1} + \dots + b_0^* = 0. \end{aligned}$$

Consequently

$$\begin{aligned} |g^*(\alpha_1^*)| &= |g^*(\alpha_1^*) - g^*(\beta_1^*)| \\ &= |b_n^*\{(\alpha_1^*)^n - (\beta_1^*)^n\} + b_{n-1}^*\{(\alpha_1^*)^{n-1} - (\beta_1^*)^{n-1}\} + \dots + b_1^*(\alpha_1^* - \beta_1^*)| \\ &= |b_n^*\{(\alpha_1^*)^{n-1} + (\alpha_1^*)^{n-2}\beta_1^* + \dots + \alpha_1^*(\beta_1^*)^{n-2} + (\beta_1^*)^{n-1}\} \\ &\quad + b_{n-1}^*\{(\alpha_1^*)^{n-2} + (\alpha_1^*)^{n-3}\beta_1^* + \dots + \alpha_1^*(\beta_1^*)^{n-3} + (\beta_1^*)^{n-2}\} \\ &\quad + \dots + b_1^*| \cdot |\alpha_1^* - \beta_1^*| \\ &\leq \max_{\substack{v=1, \dots, n \\ i=0, \dots, n-1}} (|b_v^*| |\alpha_1^*|^i |\beta_1^*|^{v-1-i}) \Delta(f, g). \end{aligned}$$

It follows from (2) and (3) that

$$(5) \quad |g^*(\alpha_1^*)| \leq H(g^*) |\alpha_1^*|^n \Delta(f, g).$$

By (2) we have for $\mu = 2, 3, \dots, m$

$$(6) \quad |g^*(\alpha_\mu^*)| = \left| \sum_{v=0}^n b_v^*(\alpha_\mu^*)^v \right| \leq H(g^*) |\alpha_\mu^*|^n.$$

From the definition of g^* we derive

$$\sum_{v=0}^n b_v^* x^v = \sum_{v=0}^n b_v (x + A)^v,$$

hence

$$b_v^* = b_v + \binom{v+1}{1} A b_{v+1} + \dots + \binom{n}{n-v} A^{n-v} b_n \quad (v = 0, 1, \dots, n).$$

Moreover $|A| \geq 1$, so that, using the non-Archimedean character of the valuation,

$$|b_v^*| \leq |A|^n H(g) \quad (v = 0, 1, \dots, n),$$

hence

$$(7) \quad H(g^*) \leq |A|^n H(g).$$

Similarly we get

$$(8) \quad H(f^*) \leq |A|^m H(f).$$

(5) and (7) imply

$$(9) \quad |g^*(\alpha_1^*)| \leq |A|^n H(g) |\alpha_1^*|^n \Delta(f, g).$$

By (6) and (7) we have for $\mu = 2, 3, \dots, m$

$$(10) \quad |g^*(\alpha_\mu^*)| \leq |A|^n H(g) |\alpha_\mu^*|^n.$$

Since $|a_m^* \alpha_1^* \alpha_2^* \dots \alpha_m^*| = |a_0^*| \leq H(f^*) \leq |A|^m H(f)$ by (8), and $a_m^* = a_m$, we have, by (4), (9) and (10),

$$\begin{aligned} |R(f, g)| &\leq |a_m|^n |A|^n H(g) |\alpha_1^*|^n \Delta(f, g) \prod_{\mu=2}^m \{|A|^n H(g) |\alpha_\mu^*|^n\} \\ &= |a_m^* \alpha_1^* \alpha_2^* \dots \alpha_m^*|^n |A|^{mn} H(g)^m \Delta(f, g) \\ &\leq |A|^{2mn} H(f)^n H(g)^m \Delta(f, g), \end{aligned}$$

hence

$$\Delta(f, g) \geq |A|^{-2mn} H(f)^{-n} H(g)^{-m} |R(f, g)|.$$

Moreover $1 \leq |A| \leq \varphi(m+n)$, so that

$$\text{either } \Delta(f, g) \geq 1 \text{ or } \Delta(f, g) \geq \varphi(m+n)^{-2mn} H(f)^{-n} H(g)^{-m} |R(f, g)|.$$

4. Proof of Theorem 3.2.

Here we use the following analogon of a lemma of SIEGEL (compare MAHLER [7], p. 251 and 252, lemma 2):

Lemma. If α is a zero of $f(x) = \sum_{\mu=0}^m a_\mu x^\mu$, $|\alpha| \geq 1$ and $G(x) = \frac{f(x)}{x-\alpha}$, then $H(G) \leq H(f)$.

Proof. Let

$$G(x) = \sum_{\mu=0}^{m-1} d_\mu x^\mu.$$

From the definition of $G(x)$ we obtain (putting $d_{-1} = d_m = 0$)

$$d_{\mu-1} - \alpha d_\mu = a_\mu \quad (\mu = 0, 1, \dots, m).$$

Solving for $-d_0, -d_1, \dots, -d_{m-1}$, we get

$$-d_\mu = \frac{a_\mu}{\alpha} - \frac{d_{\mu-1}}{\alpha} = \frac{a_\mu}{\alpha} + \frac{a_{\mu-1}}{\alpha^2} + \dots + \frac{a_0}{\alpha^{\mu+1}} \quad (\mu = 0, 1, \dots, m-1).$$

Hence, using $|\alpha^{-1}| \leq 1$, we obtain

$$|d_\mu| \leq \max(|a_0|, |a_1|, \dots, |a_\mu|)$$

and therefore $H(G) \leq H(f)$.

Q. e. d.

For the sake of convenience we shall denote f' by g , hence

$$g(x) = a_1 + 2a_2x + \dots + ma_mx^{m-1},$$

so that clearly

$$(11) \quad H(g) \leq H(f).$$

By hypothesis there exists for the m elements $\alpha_1, \alpha_2, \dots, \alpha_m$ of F an element A of F with $1 \leq |A| \leq \varphi(m)$ and such that

$$(12) \quad |\alpha_\mu - A| \geq 1 \quad (\mu = 1, 2, \dots, m).$$

Then put

$$f^*(x) = f(x + A), \quad g^*(x) = g(x + A) = f'(x + A),$$

so that

$$f^*(x) = \sum_{\mu=0}^m a_\mu^* x^\mu$$

is a polynomial over F with zeros $\alpha_\mu^* = \alpha_\mu - A$ ($\mu = 1, 2, \dots, m$). Hence, by (12),

$$(13) \quad |\alpha_\mu^*| \geq 1 \quad (\mu = 1, 2, \dots, m).$$

Clearly $\alpha_\mu^* - \alpha_\nu^* = \alpha_\mu - \alpha_\nu$.

By hypothesis the discriminant

$$D(f) = a_m^{2m-2} \prod_{1 \leq \mu < \nu \leq m} (\alpha_\mu - \alpha_\nu)^2 = a_m^{2m-2} \prod_{1 \leq \mu < \nu \leq m} (\alpha_\mu^* - \alpha_\nu^*)^2$$

of f does not vanish; thus all m zeros of f are distinct and the minimal distance $\Delta(f)$ of these zeros is a positive number. Moreover $\Delta(f^*) = \Delta(f)$. We choose the order of the zeros such that $\Delta(f) = |\alpha_1 - \alpha_2|$. As in the proof of Theorem 3.1 we obtain

$$H(f^*) \leq |A|^m H(f), \quad H(g^*) \leq |A|^{m-1} H(g) \quad (\text{compare (8) and (7)}).$$

It follows then from (11) that

$$(14) \quad H(g^*) \leq |A|^{m-1} H(g) \leq |A|^{m-1} H(f).$$

Since the definition of f^* implies $a_m^* = a_m$, we have

$$f^*(x) = a_m(x - \alpha_1^*)(x - \alpha_2^*) \dots (x - \alpha_m^*).$$

Put ⁶⁾

$$G(x) = a_m(x - \alpha_2^*)(x - \alpha_3^*) \dots (x - \alpha_m^*),$$

$$K(x) = a_m(x - \alpha_3^*)(x - \alpha_4^*) \dots (x - \alpha_m^*),$$

so that

$$G(x) = \frac{f^*(x)}{x - \alpha_1^*}, \quad K(x) = \frac{G(x)}{x - \alpha_2^*}.$$

According to the lemma derived at the beginning of this proof, we have

$$H(K) \leq H(G) \leq H(f^*).$$

⁶⁾ If $m=2$ we put $K(x) = a_m$.

5. This section contains some simple applications of Theorem 3.1 and Theorem 3.2.

a) Consider the field F of formal Dirichlet series over the field of complex numbers. An element of F has the form

$$D = \sum_{i=0}^{\infty} a_i e^{-\lambda_i s},$$

where the coefficients a_i are complex numbers and the “exponents” λ_i are arbitrary real numbers subject to the condition $\lambda_i \uparrow +\infty$. OSTROWSKI [8], Satz D, p. 120, has shown that the field F is algebraically closed. Moreover F has a non-Archimedean valuation, defined by

$$|D| = 0 \text{ if } D = 0, \quad |D| = e^{-\lambda_0} \text{ if } a_0 \neq 0.$$

If

$$P(x) = D_m x^m + D_{m-1} x^{m-1} + \dots + D_0$$

is a polynomial over F , then we can define its height $H(P)$ as

$$H(P) = \max_{\mu=0,1,\dots,m} |D_\mu|.$$

Let $D_1, D_2, \dots, D_n$ be an arbitrarily chosen finite set of elements from F . Let $b_1, b_2, \dots, b_n$ denote the “constant terms” in $D_1, D_2, \dots, D_n$, i.e. the coefficients belonging to the exponent $\lambda_i = 0$ in the Dirichlet series (put $b_i = 0$ if such a term does not occur in the series). We can find a complex number $a \neq 0$, different from $b_1, b_2, \dots, b_n$. Then the constant term in any of the Dirichlet series

$$D_i^* = D_i - a \cdot e^{0 \cdot s} \quad (i = 1, 2, \dots, n)$$

does not vanish and therefore the exponent of the leading term is negative or zero, hence

$$|D_i^*| \geq 1 \text{ for } i = 1, 2, \dots, n.$$

From this it is clear that the conditions for the field F stated in section 2 of this chapter are satisfied in our present case, since $A = a \cdot e^{0 \cdot s}$ and thus $\varphi(n) \equiv 1$. Hence we are in a position to apply Theorem 3.1 and Theorem 3.2:

Theorem 3.3. *Let*

$$P(x) = S_m x^m + S_{m-1} x^{m-1} + \dots + S_0, \quad S_m \neq 0,$$

$$Q(x) = T_n x^n + T_{n-1} x^{n-1} + \dots + T_0, \quad T_n \neq 0,$$

be two polynomials in x of degrees m and n over the field F of formal Dirichlet series and with heights $H(P)$ and $H(Q)$. Let the Dirichlet series $\sigma_1, \sigma_2, \dots, \sigma_m$ and $\tau_1, \tau_2, \dots, \tau_n$ be the zeros of P and Q , respectively. Suppose that the resultant $R(P, Q)$ of P and Q does not vanish and set

$$\Delta(P, Q) = \min_{\substack{1 \leq \mu \leq m \\ 1 \leq \nu \leq n}} |\sigma_\mu - \tau_\nu|.$$

Therefore, using $H(f^*) \leq |A|^m H(f)$,

$$(15) \quad H(K) \leq |A|^m H(f).$$

Since $g^*(x) = (f^*(x))' = a_m \{(x - \alpha_1^*) (x - \alpha_2^*) \dots (x - \alpha_m^*)\}'$ ⁷⁾, we have for $\mu = 1, 2, \dots, m$

$$g^*(\alpha_\mu^*) = (-1)^{\mu-1} a_m (\alpha_1^* - \alpha_\mu^*) \dots (\alpha_{\mu-1}^* - \alpha_\mu^*) (\alpha_\mu^* - \alpha_{\mu+1}^*) \dots (\alpha_\mu^* - \alpha_m^*),$$

so that

$$\prod_{\mu=1}^m g^*(\alpha_\mu^*) = (-1)^{\frac{1}{2}m(m-1)} a_m^m \prod_{1 \leq \mu < \nu \leq m} (\alpha_\mu^* - \alpha_\nu^*)^2.$$

It follows that

$$(16) \quad D(f) = a_m^{2m-2} \prod_{1 \leq \mu < \nu \leq m} (\alpha_\mu^* - \alpha_\nu^*)^2 = (-1)^{\frac{1}{2}m(m-1)} a_m^{m-2} \prod_{\mu=1}^m g^*(\alpha_\mu^*).$$

From the definition of $K(x)$ we obtain

$$K(\alpha_1^*) = a_m (\alpha_1^* - \alpha_3^*) \dots (\alpha_1^* - \alpha_m^*),$$

so that, since $\Delta(f^*) = \Delta(f) = |\alpha_1^* - \alpha_2^*|$,

$$(17) \quad |g^*(\alpha_1^*)| = \Delta(f^*) |K(\alpha_1^*)| = \Delta(f) |K(\alpha_1^*)|.$$

The simple method we used in the derivation of (6) gives here

$$|K(\alpha_1^*)| \leq H(K) |\alpha_1^*|^{m-2}.$$

Hence, by (13) and (15),

$$(18) \quad |K(\alpha_1^*)| \leq |A|^m H(f) |\alpha_1^*|^{m-2} \leq |A|^m H(f) |\alpha_1^*|^{m-1}.$$

Therefore, by (17) and (18),

$$(19) \quad |g^*(\alpha_1^*)| \leq \Delta(f) |A|^m H(f) |\alpha_1^*|^{m-1}.$$

Again using the method applied to the derivation of (6), we obtain for $\mu = 2, 3, \dots, m$, by (14),

$$(20) \quad |g^*(\alpha_\mu^*)| \leq H(g^*) |\alpha_\mu^*|^{m-1} \leq |A|^{m-1} H(f) |\alpha_\mu^*|^{m-1}.$$

Since $|a_m \alpha_1^* \alpha_2^* \dots \alpha_m^*| = |a_0^*| \leq H(f^*) \leq |A|^m H(f)$ by (8), we have, by (16), (19) and (20),

$$\begin{aligned} |a_m D(f)| &\leq |a_m|^{m-1} \Delta(f) |A|^m H(f) |\alpha_1^*|^{m-1} |A|^{(m-1)^2} H(f)^{m-1} |\alpha_2^* \dots \alpha_m^*|^{m-1} \\ &\leq \Delta(f) |A|^{2m^2-2m+1} H(f)^{2m-1}, \end{aligned}$$

hence

$$\Delta(f) \geq |A|^{-(2m^2-2m+1)} H(f)^{-(2m-1)} |a_m D(f)|.$$

Moreover $1 \leq |A| \leq \varphi(m)$, so that

$$\Delta(f) \geq \varphi(m)^{-(2m^2-2m+1)} H(f)^{-(2m-1)} |a_m D(f)|.$$

⁷⁾ We use the relation $(f(x+A))' = f'(x+A)$.

5. This section contains some simple applications of Theorem 3.1 and Theorem 3.2.

a) Consider the field F of formal Dirichlet series over the field of complex numbers. An element of F has the form

$$D = \sum_{i=0}^{\infty} a_i e^{-\lambda_i s},$$

where the coefficients a_i are complex numbers and the “exponents” λ_i are arbitrary real numbers subject to the condition $\lambda_i \uparrow +\infty$. OSTROWSKI [8], Satz D, p. 120, has shown that the field F is algebraically closed. Moreover F has a non-Archimedean valuation, defined by

$$|D| = 0 \text{ if } D = 0, \quad |D| = e^{-\lambda_0} \text{ if } a_0 \neq 0.$$

If

$$P(x) = D_m x^m + D_{m-1} x^{m-1} + \dots + D_0$$

is a polynomial over F , then we can define its height $H(P)$ as

$$H(P) = \max_{\mu=0,1,\dots,m} |D_\mu|.$$

Let $D_1, D_2, \dots, D_n$ be an arbitrarily chosen finite set of elements from F . Let $b_1, b_2, \dots, b_n$ denote the “constant terms” in $D_1, D_2, \dots, D_n$, i.e. the coefficients belonging to the exponent $\lambda_i = 0$ in the Dirichlet series (put $b_i = 0$ if such a term does not occur in the series). We can find a complex number $a \neq 0$, different from $b_1, b_2, \dots, b_n$. Then the constant term in any of the Dirichlet series

$$D_i^* = D_i - a \cdot e^{0 \cdot s} \quad (i = 1, 2, \dots, n)$$

does not vanish and therefore the exponent of the leading term is negative or zero, hence

$$|D_i^*| \geq 1 \text{ for } i = 1, 2, \dots, n.$$

From this it is clear that the conditions for the field F stated in section 2 of this chapter are satisfied in our present case, since $A = a \cdot e^{0 \cdot s}$ and thus $\varphi(n) \equiv 1$. Hence we are in a position to apply Theorem 3.1 and Theorem 3.2:

Theorem 3.3. *Let*

$$\begin{aligned} P(x) &= S_m x^m + S_{m-1} x^{m-1} + \dots + S_0, \quad S_m \neq 0, \\ Q(x) &= T_n x^n + T_{n-1} x^{n-1} + \dots + T_0, \quad T_n \neq 0, \end{aligned}$$

be two polynomials in x of degrees m and n over the field F of formal Dirichlet series and with heights $H(P)$ and $H(Q)$. Let the Dirichlet series $\sigma_1, \sigma_2, \dots, \sigma_m$ and $\tau_1, \tau_2, \dots, \tau_n$ be the zeros of P and Q , respectively. Suppose that the resultant $R(P, Q)$ of P and Q does not vanish and set

$$\Delta(P, Q) = \min_{\substack{1 \leq \mu \leq m \\ 1 \leq \nu \leq n}} |\sigma_\mu - \tau_\nu|.$$

Then

$$\text{either } \Delta(P, Q) \geq 1 \text{ or } \Delta(P, Q) \geq H(P)^{-n} H(Q)^{-m} |R(P, Q)|.$$

Theorem 3.4. Let

$$P(x) = S_m x^m + S_{m-1} x^{m-1} + \dots + S_0, S_m \neq 0,$$

be a polynomial in x of degree $m \geq 2$ over the field F of formal Dirichlet series and with height $H(P)$. Let the Dirichlet series $\sigma_1, \sigma_2, \dots, \sigma_m$ be the zeros of P . Suppose that the discriminant $D(P)$ of P does not vanish and set

$$\Delta(P) = \min_{1 \leq \mu < \nu \leq m} |\sigma_\mu - \sigma_\nu|.$$

Then

$$\Delta(P) \geq H(P)^{-(2m-1)} |S_m D(P)|.$$

b) In the following example we consider the field G of formal Puiseux series over the complex numbers

$$(21) \quad P = \sum_{k=l}^{\infty} c_k z^{k/p}.$$

Here for every series p is a fixed positive integer, l a fixed arbitrary integer. This field is isomorphic to a subfield of the field of Dirichlet series considered above. In fact, by substituting

$$z = e^{-s}$$

and by setting

$$c_{l+i} = a_i, \frac{l+i}{p} = \lambda_i \quad (i = 0, 1, \dots),$$

we obtain from (21) the Dirichlet series

$$\sum_{i=0}^{\infty} a_i e^{-\lambda_i s}.$$

Clearly in this context the valuation of the series P must be defined as follows

$$|P| = 0 \text{ if } P = 0, |P| = e^{-l/p} \text{ if } c_l \neq 0.$$

By restricting ourselves to the Puiseux series (21) with $p=1$ we get an even smaller subfield: the field of formal power series over the complex numbers.

Notice that the valuation given above is the same as the valuation given in Chapter II, section 1, for a formal power series in the case of the field of complex numbers.

Now let $w = w(z)$ be an algebraic function of the complex variable z . Then w satisfies an irreducible algebraic equation

$$(22) \quad \sum_{\mu=0}^m a_\mu w^\mu = 0, a_m \neq 0,$$

where the a_μ are polynomials in z over the field of complex numbers.

The left-hand side of (22) as a polynomial in z and in w is uniquely determined by the algebraic function w , apart from a non-zero multiplicative constant (compare e.g. BEHNKE and SOMMER [2], p. 421).

Let k denote the maximal degree of the polynomials a_μ ($\mu = 0, 1, \dots, m$), then

$$H(w) = e^k$$

is called the *height* of the algebraic function w . Each polynomial a_μ has the form

$$a_\mu(z) = a_{\mu 0} + a_{\mu 1}z + \dots + a_{\mu k}z^k.$$

Now consider

$$a_\mu^*(z) = z^{-k}a_\mu(z) = a_{\mu 0}z^{-k} + a_{\mu 1}z^{-k+1} + \dots + a_{\mu k}.$$

Since the left-hand side of (22) is irreducible, at least one coefficient $a_{\mu 0}$ ($\mu = 0, 1, \dots, m$) does not vanish; therefore

$$H(w) = e^k = \max_{\mu=0,1,\dots,m} |a_\mu^*|,$$

where $|a_\mu^*|$ denotes the valuation of a_μ^* , considered as a formal power series in z .

Further we have

$$(23) \quad \sum_{\mu=0}^m a_\mu^* w^\mu = 0, a_m^* \neq 0.$$

Let $v = v(z)$ be a second algebraic function, different from w , of degree n and of height $H(v) = e^h$. Then v satisfies an irreducible equation

$$(24) \quad \sum_{\nu=0}^n b_\nu^* v^\nu = 0, b_n^* \neq 0,$$

where the b_ν^* are polynomials in z^{-1} , defined in a way similar to the a_μ^* occurring in (23). We have

$$H(v) = \max_{\nu=0,1,\dots,n} |b_\nu^*|.$$

Since the left-hand sides of (23) and (24) are different irreducible polynomials, their resultant R does not vanish. On the other hand it is clear from the determinant-form of R , that R is a polynomial in z^{-1} . Hence its valuation as a formal power series must satisfy

$$(25) \quad |R| \geq 1.$$

The algebraic function w , defined by (22), can be developed at the origin into m Puiseux series of the form

$$w_1(z) = \sum_{k=l}^{\infty} c_k z^{k/p}.$$

Similarly the function v can be developed at the origin into n Puiseux series of a similar form, which we shall denote by $v_1(z)$.

We are now able to apply Theorem 3.3 if we consider the coefficients

a_μ^* and b_ν^* in (23) and (24) as well as the Puiseux series w_1 and v_1 as Dirichlet series. In this way we get, using (25), the following analogon of BOMBIERI's original theorem:

Theorem 3.5. *Let w be an algebraic function of degree m and of height $H(w)$. Let v be an algebraic function, different from w , of degree n and of height $H(v)$. Let w_1 be a Puiseux series at the origin of w and v_1 a Puiseux series at the origin of v .*

Then we have the following inequality for the valuation of the Puiseux series $w_1 - v_1$:

$$|w_1 - v_1| \geq H(w)^{-n} H(v)^{-m}.$$

Since $H(w) = e^k$, $H(v) = e^h$, this result can be put into the form

$$|w_1 - v_1| \geq e^{-(kn+hm)}.$$

In other words:

If the algebraic function w satisfies an irreducible equation of degrees m in w and k in z and if a second algebraic function v satisfies an irreducible equation of degrees n in w and h in z , then the Puiseux series $w_1 - v_1$ cannot begin with a higher power of z than z^{kn+hm} .

In a similar way we can apply Theorem 3.4. Since the left-hand side of (23) is an irreducible polynomial, its discriminant D does not vanish. On the other hand it is clear from the determinant-form of $a_m^* D$ (compare e.g. foot-note 4) that $a_m^* D$ is a polynomial in z^{-1} . Hence its valuation as a formal power series must satisfy

$$(26) \quad |a_m^* D| \geq 1.$$

We now get, using (26), the following

Theorem 3.6. *Let w be an algebraic function of degree $m \geq 2$ and of height $H(w)$. Let w_1 and w_2 be two different Puiseux series at the origin of w . Then*

$$|w_1 - w_2| \geq H(w)^{-(2m-1)}.$$

Since $H(w) = e^k$, this result can be put into the form

$$|w_1 - w_2| \geq e^{-k(2m-1)}.$$

In other words:

If the algebraic function w satisfies an irreducible equation of degrees $m \geq 2$ in w and k in z , then the Puiseux series $w_1 - w_2$ cannot begin with a higher power of z than $z^{k(2m-1)}$.

It is possible to generalize these results by considering the finite algebraic extensions of the field of rational functions over a field of characteristic zero. It is well-known that for these more general algebraic functions the "Theorem of Puiseux" also holds (compare e.g. EICHLER [4], p. 134). We have suppressed this, since the theorems become quite complex.

6. Finally we shall give an application for the field $\mathbb{Q}_p$ of p -adic numbers.

Theorem 3.7. *Let*

$$\begin{aligned} f(x) &= a_m x^m + a_{m-1} x^{m-1} + \dots + a_0, a_m \neq 0, \\ g(x) &= b_n x^n + b_{n-1} x^{n-1} + \dots + b_0, b_n \neq 0, \end{aligned}$$

be two polynomials over $\mathbb{Q}_p$ of degrees m and n , and of heights $H(f)$ and $H(g)$. Let Φ be a finite extension of $\mathbb{Q}_p$ such that f and g both resolve into linear factors in $\Phi[x]$:

$$\begin{aligned} f(x) &= a_m (x - \alpha_1) \dots (x - \alpha_m), \\ g(x) &= b_n (x - \beta_1) \dots (x - \beta_n). \end{aligned}$$

Let $|\gamma|_p$ denote for any element γ of Φ the valuation of γ , if we extend the p -adic valuation of $\mathbb{Q}_p$ to Φ . Suppose that the resultant $R(f, g)$ of f and g does not vanish and set

$$\Delta(f, g) = \min_{\substack{1 \leq \mu \leq m \\ 1 \leq \nu \leq n}} |\alpha_\mu - \beta_\nu|_p.$$

Then

$$\text{either } \Delta(f, g) \geq 1 \text{ or } \Delta(f, g) \geq H(f)^{-n} H(g)^{-m} |R(f, g)|_p.$$

Theorem 3.8. *Let*

$$f(x) = a_m x^m + a_{m-1} x^{m-1} + \dots + a_0, a_m \neq 0,$$

be a polynomial over $\mathbb{Q}_p$ of degree $m \geq 2$ and of height $H(f)$. Let Φ be a finite extension of $\mathbb{Q}_p$ such that f resolves into linear factors in $\Phi[x]$:

$$f(x) = a_m (x - \alpha_1) \dots (x - \alpha_m).$$

Let $|\gamma|_p$ denote for any element γ of Φ the valuation of γ , if we extend the p -adic valuation of $\mathbb{Q}_p$ to Φ . Suppose that the discriminant $D(f)$ of f does not vanish and set

$$\Delta(f) = \min_{1 \leq \mu < \nu \leq m} |\alpha_\mu - \alpha_\nu|_p.$$

Then

$$\Delta(f) \geq H(f)^{-(2m-1)} |a_m D(f)|_p.$$

For the proof we consider a field F with a discrete valuation, so that the value group V_F consists of an infinite cyclic group.

We shall now use several results contained in e.g. ARTIN [1], Chapter III.

Consider the set of elements $\alpha \in F$ such that $|\alpha| \leq 1$. This set is a ring R , called the *ring of integers*. For a unit $\varepsilon \in R$ clearly $|\varepsilon| = 1$.

The set of elements $\alpha \in R$, such that $|\alpha| < 1$, forms a maximal ideal $\mathfrak{m}$ of R (ARTIN [1], p. 49, 50), hence the residue class ring $R/\mathfrak{m}$ is a field, denoted by $\bar{F}$.

From now on let F be complete with respect to its discrete valuation.

Let E be a finite extension of F of degree $(E:F) = s$. Hereby the valuation

of F is uniquely extended to E and E is complete under the extended valuation (compare e.g. HASSE [6], p. 175).

Apparently E has again a discrete valuation, since for any $\alpha \in E$ with norm $N\alpha$

$$|\alpha| = \sqrt[s]{|N\alpha|}.$$

We denote its value group by V_E .

The index

$$e \stackrel{\text{def}}{=} (V_E : V_F)$$

is called the *ramification index* of this extended valuation.

Let, more specially, $\overline{\mathbf{Q}}_p$ be the residue class field of $\mathbf{Q}_p$, then $\overline{\mathbf{Q}}_p \cong$ the residue class field mod p with representatives $0, 1, \dots, p-1$ (ARTIN [1], p. 54).

Let E_p be a finite extension of $\mathbf{Q}_p$ of degree $(E_p : \mathbf{Q}_p) = s$. Let $\overline{E}_p$ be the residue class field of E_p with respect to the extended valuation. We may consider $\overline{E}_p$ as an extension field of $\overline{\mathbf{Q}}_p$, as there is a natural isomorphism of the residue class field $\overline{\mathbf{Q}}_p$ into the residue class field $\overline{E}_p$ (ARTIN [1], Theorem 3, p. 50). We denote the degree of this extension by $(\overline{E}_p : \overline{\mathbf{Q}}_p) = f$.

$\overline{E}_p$ is a finite extension of $\overline{\mathbf{Q}}_p$, i.e. $\overline{E}_p$ is a Galois field with p^f elements (compare e.g. VAN DER WAERDEN [9], p. 128).

Since $\mathbf{Q}_p$ has a discrete valuation, we have $ef = s$ (ARTIN [1], Theorem 6, p. 55).

Now we prove the following lemma.

Lemma. Let $\alpha_1, \alpha_2, \dots, \alpha_n$ denote elements of E_p , then there exists an element A of E_p such that

$$|\alpha_v - A|_p \geq 1 \quad (v = 1, 2, \dots, n), \quad 1 \leq |A|_p \leq n^{1/s}.$$

Proof. We may suppose that at least one element α_v differs from zero. Choose in $\mathbf{Q}_p$ an element π with maximal valuation < 1 , hence $|\pi|_p = p^{-1}$, and a similar element Π in E_p . It follows from the definition of e and the choice of π (compare e.g. ARTIN [1], p. 55) that

$$|\Pi|_p = |\pi|_p^{1/e} = p^{-1/e}.$$

E_p is a complete field with a discrete valuation. Therefore we have the following unique development into a power series for each element α of E_p

$$\alpha = c_{-k}\Pi^{-k} + c_{-k+1}\Pi^{-k+1} + \dots + c_0 + c_1\Pi + c_2\Pi^2 + \dots,$$

where the coefficients c_i are taken from the residue class field $\overline{E}_p$ (ARTIN [1], Theorem 5, p. 53).

Choose the positive integer k such that

$$\max_{v=1, \dots, n} |\alpha_v|_p \leq |\Pi|_p^{-k},$$

then we have for $v=1, 2, \dots, n$

$$\alpha_v = c_{-k,v} \Pi^{-k} + c_{-k+1,v} \Pi^{-k+1} + \dots + c_{0v} + c_{1v} \Pi + c_{2v} \Pi^2 + \dots$$

Consider the set V consisting of all elements

$$X = u_{-t} \Pi^{-t} + u_{-t+1} \Pi^{-t+1} + \dots + u_{-1} \Pi^{-1} + u_0, u_i \in \bar{E}_p,$$

such that the non-negative integer t satisfies the inequality

$$(27) \quad p^{tf} \leq n < p^{(t+1)f}.$$

For each element of V we have

$$|X|_p \geq 1.$$

For each u_i there are p^f possible choices. Consequently V has $p^{f(t+1)}$ distinct elements. We may suppose $k \geq t$. It follows from (27) that the number of elements of V exceeds the number of the α_v 's. Thus at least one element of V is incongruent $\alpha_v \pmod{\Pi}$ for $v=1, 2, \dots, n$. Denote by A such an element X , then $|A|_p \geq 1$. Moreover $|\alpha_v - A|_p \geq 1$ ($v=1, 2, \dots, n$). For assume that $|\alpha_v - A|_p < 1$.

Now

$$\begin{aligned} \alpha_v &= c_{-k,v} \Pi^{-k} + \dots + c_{-t,v} \Pi^{-t} + \dots + c_{0v} + c_{1v} \Pi + \dots \\ A &= u_{-t} \Pi^{-t} + \dots + u_0. \end{aligned}$$

It follows that $c_{-k,v} = \dots = c_{-t-1,v} = 0$, $c_{-t,v} = u_{-t}$, $\dots$, $c_{0v} = u_0$, so that the coefficients of Π^{-t} , Π^{-t+1} , $\dots$, Π^{-1} , 1, respectively, would be the same in the development of α_v as in the development of A , contrary to the choice of A . Since A is an element of V , we also have

$$|A|_p \leq |\Pi|_p^{-t} = p^{t/e} = p^{tf/ef} = p^{tf/s} \leq n^{1/s}.$$

This proves our lemma.

Now consider the polynomial

$$(28) \quad h(x) = x^k - p,$$

where k denotes an arbitrary positive integer.

We assert that this polynomial is irreducible over $\mathbf{Q}_p$. For the proof we use the following generalization of Eisenstein's irreducibility criterion (compare e.g. VAN DER WAERDEN [9], 2. Aufgabe, p. 266):

Let F denote a complete field with a non-Archimedean valuation, $\mathfrak{m}$ the maximal ideal in the ring of integers with elements a such that $|a| < 1$ ⁸⁾.

If in the polynomial

$$h(x) = x^k + a_{k-1}x^{k-1} + \dots + a_0$$

the coefficients $a_0, a_1, \dots, a_{k-1}$ are contained in $\mathfrak{m}$ and if moreover a_0 cannot be factored into two elements of $\mathfrak{m}$, then $h(x)$ is irreducible over F .

⁸⁾ This condition is equivalent to $w(a) > 0$ in the exponential valuation used by VAN DER WAERDEN loc. cit.

In the special case $F = \mathbb{Q}_p$ the maximal ideal $\mathfrak{m}$ consists of all p -adic numbers such that $|a|_p \leq p^{-1}$.

If a p -adic number a_0 can be factored into two elements of $\mathfrak{m}$, then $|a_0|_p \leq p^{-2}$. Applying the irreducibility criterion to the polynomial $h(x)$, defined in (28), we find that it must be irreducible over $\mathbb{Q}_p$.

Let α denote a zero of (28), then α is algebraic of degree k over $\mathbb{Q}_p$.

It is our intention to prove Theorem 3.7 and Theorem 3.8. In the first theorem f and g are polynomials over $\mathbb{Q}_p$ and Φ is a finite extension of $\mathbb{Q}_p$. Now we adjoin the zero α of (28) to Φ . In this way we obtain an extension E_p of $\mathbb{Q}_p$ of degree $s \geq k$.

Applying our lemma, we find that to every set $(\alpha_1, \alpha_2, \dots, \alpha_n)$ of n elements contained in E_p there exists an element A of E_p such that

$$1 \leq |A|_p \leq n^{1/s}, |\alpha_\nu - A|_p \geq 1 \quad (\nu = 1, 2, \dots, n).$$

Since this condition for the field E_p is satisfied, we are in a position to apply Theorem 3.1 in the special case $F = E_p$, $\varphi(n) = n^{1/s}$. It follows for

$$\Delta(f, g) = \min_{\substack{1 \leq \mu \leq m \\ 1 \leq \nu \leq n}} |\alpha_\mu - \beta_\nu|_p$$

that

$$\text{either } \Delta(f, g) \geq 1 \text{ or } \Delta(f, g) \geq (m+n)^{-2mn/s} H(f)^{-n} H(g)^{-m} |R(f, g)|_p.$$

However we can take the positive integer k , and therefore s , arbitrarily large. It follows that

$$\text{either } \Delta(f, g) \geq 1 \text{ or } \Delta(f, g) \geq H(f)^{-n} H(g)^{-m} |R(f, g)|_p,$$

which proves Theorem 3.7.

The proof of Theorem 3.8 is quite similar and is therefore omitted here.

REFERENCES

1. ARTIN, E., Algebraic numbers and algebraic functions I. Princeton University, New York University, 1950–1951.
2. BEHNKE, H. and F. SOMMER, Theorie der analytischen Funktionen einer komplexen Veränderlichen. Berlin–Göttingen–Heidelberg, 1955.
3. BOMBIERI, E., Sull' approssimazione di numeri algebrici mediante numeri algebrici, Boll. Un. Mat. Ital. III, 13, 351–354 (1958).
4. EICHLER, M., Einführung in die Theorie der algebraischen Zahlen und Funktionen. Basel, 1963.
5. GÜTING, R., Approximation of algebraic numbers by algebraic numbers, Michigan Math. J., Vol. 8, no. 2, 149–159 (1961).
6. HASSE, H., Zahlentheorie (2. Aufl.). Berlin, 1963.
7. MAHLER, K., On a theorem by E. Bombieri, Proc. Nederl. Akad. Wetensch. A, 63, 245–253 (1960); Indag. Math., 22, 245–253 (1960).
8. OSTROWSKI, A., Über algebraische Funktionen von Dirichletschen Reihen, Math. Z., 37, 98–133 (1933).
9. WAERDEN, B. L. VAN DER, Algebra I (5. Aufl.). Berlin–Göttingen–Heidelberg, 1960.

SAMENVATTING

In dit proefschrift behandelen wij uitbreidingen van twee verschillende, hoewel verwante, problemen, welke voorkomen in de getallentheorie. Het eerste probleem is ontleend aan de theorie der transcendente getallen, het tweede aan de theorie van de benadering van een algebraïsch getal door andere algebraïsche getallen.

In het eerste geval gaan wij uit van het bekende bewijs van VON NEUMANN, dat er een verzameling reële getallen bestaat met de machtigheid van het continuüm en met de eigenschap, dat de elementen van elke eindige deelverzameling algebraïsch onafhankelijk zijn t.o.v. het lichaam der rationale getallen. De elementen dezer verzameling, de z.g. Von Neumann-getallen, worden voorgesteld door

$$A_\varrho = \sum_{\nu=0}^{\infty} 2^{2^{[\varrho\nu]} - 2^{\nu^2}} \text{ voor iedere } \varrho > 0.$$

Het bewijs van VON NEUMANN is een uitbreiding van de methode, door LIOUVILLE gebruikt om het bestaan van transcendente getallen aan te toonen door middel van snel convergeerende reeksen met rationale termen. Het is eenvoudig in te zien, dat ieder Von Neumann-getal A_ϱ tevens een Liouville-getal is.

Het doel van Hoofdstuk I van dit proefschrift is in de eerste plaats het bewijs van VON NEUMANN zooveel mogelijk te vereenvoudigen en vervolgens zijn methode uit te breiden.

Zonder in bijzonderheden te treden deelen wij hier mede, dat de rol van het lichaam der reële getallen in het klassieke geval in onze theorie door een compleet gewaardeerd lichaam wordt overgenomen. Wij beperken ons tot het geval, dat op grond van de gebruikte waardeering slechts als waarden niet-negatieve reële getallen worden toegelaten. Voor de waardeering van een element a zullen wij steeds de notatie $|a|$ gebruiken.

In Hoofdstuk II breiden wij deze methode nog verder uit door elementen van een gewaardeerd differentiaallichaam te beschouwen. In een publicatie van 1959 heeft KOLCHIN de eenvoudiger methode van LIOUVILLE reeds uitgebreid tot het geval van een gewaardeerd differentiaallichaam en wij kunnen eenige zijner lemma's voor ons doel gebruiken.

In ons laatste hoofdstuk vatten wij een ander probleem in het oog, dat zijn oorsprong vindt in een door BRAUER in 1929 verkregen resultaat. Dit luidt als volgt:

Laat α een vast algebraïsch getal van den graad m zijn. Er bestaat dan een positieve constante C , die alleen van α afhangt en waarbij voor

elk algebraïsch getal $\beta \neq \alpha$ van den graad n en met de hoogte $H(\beta)$ geldt:

$$|\alpha - \beta| > C^n H(\beta)^{-m}.$$

Men zie voor de definitie van de hoogte van een algebraïsch getal Hoofdstuk III, § 1; ook wordt daar de definitie van de hoogte van een veelterm gegeven.

Later werd deze stelling eerst door BOMBIERI en daarna door MAHLER uitgebreid.

MAHLER beschouwde twee veeltermen f en g met complexe coëfficiënten en met resultante R . α zij een nulwaarde van f en β een nulwaarde van g . Voor $|\alpha - \beta|$ werd nu door MAHLER een ondergrens bepaald, waarin R , de graden en de hoogten der beide veeltermen f en g optreden. Bovendien gaf hij een overeenkomstig resultaat, indien α en β voldoen aan dezelfde vergelijking $f = 0$.

In Hoofdstuk III onderzoeken wij, waar de theorie van MAHLER toe leidt, als wij nulwaarden beschouwen van veeltermen met coëfficiënten uit een niet-Archimedisch gewaardeerd lichaam F , waarbij aan zekere voorwaarden moet zijn voldaan. Dank zij het niet-Archimedische karakter van onze waardeering, worden de uitkomsten eenvoudiger dan in MAHLER's geval.

Ons verfstrekkende resultaat in deze richting wordt verkregen door in het bijzonder veeltermen met p -adische coëfficiënten te beschouwen. In dit geval vinden wij het volgende resultaat (vgl. Stelling 3.7):

Laten f en g twee veeltermen zijn met p -adische coëfficiënten, van den graad m resp. n en met de hoogte $H(f)$ resp. $H(g)$. Laat Φ een zoodanige eindige uitbreiding van het lichaam $\mathbb{Q}_p$ der p -adische getallen zijn, dat zoowel f als g in een product van lineaire factoren in $\Phi[x]$ kan worden ontbonden:

$$f(x) = a_m(x - \alpha_1) \dots (x - \alpha_m),$$

$$g(x) = b_n(x - \beta_1) \dots (x - \beta_n).$$

Laat $|\gamma|_p$ voor elk element γ van Φ de waarde van γ aangeven, indien wij de p -adische waardeering van $\mathbb{Q}_p$ tot Φ uitbreiden. Veronderstel dat de resultante $R = R(f, g)$ van f en g ongelijk aan nul is en stel

$$\Delta = \min_{\substack{1 \leq \mu \leq m \\ 1 \leq \nu \leq n}} |\alpha_\mu - \beta_\nu|_p.$$

Dan is

$$\text{òf } \Delta \geq 1, \text{ òf } \Delta \geq H(f)^{-n} H(g)^{-m} |R|_p.$$

Er is een overeenkomstig resultaat voor twee verschillende nulwaarden van een enkelen veelterm met p -adische coëfficiënten (vgl. Stelling 3.8).

Wij merken op, dat alle lichamen, beschouwd in dit proefschrift, commutatief zijn.

Ten behoeve van den lezer zijn wij meer in bijzonderheden getreden in de inleidende paragrafen der diverse hoofdstukken.