Chapter 3

A TEST FOR ALGEBRAIC OR TRANSCENDENTAL NUMBERS

Suppose a field K has been extended to its completion K_w with respect to some valuation or pseudo-valuation w(a). The element α of K_w is then said to be *algebraic* over K if it satisfies an equation

$$a_0x^n + a_1x^{n-1} + \dots + a_n = 0 \qquad (a_0 \neq 0, n \geq 1)$$

with coefficients in K, and it is otherwise called *transcendental* over K. The corresponding extension field $K(\alpha)$ is likewise algebraic, or transcendental, respectively.

Much of the following investigations are concerned with the problem whether a given real, p-adic, g-adic, or g*-adic number α is algebraic or transcendental over the rational field Γ. There is one, relatively elementary, approach to this problem where one studies the values of variable polynomials F(x) with rational integral coefficients at the point $x = \alpha$; it will be studied in the present chapter. A much deeper method, due to Thue, Siegel, and Roth, uses properties of the *rational approximations* of α. For the explicit construction of such approximations a simple algorithm will be given in the next chapter. It is based on the continued fraction algorithm for real numbers and forms its natural extension to p-adic, g-adic, and g*-adic numbers. The deep theorem of Roth shows that these approximations cannot be too good in the case of an algebraic number α. The theorem is best-possible and has many interesting consequences. The long and involved proof fills all the remaining chapters.

Before starting with these investigations, it has perhaps some interest to collect certain general properties that are basic for the theory of Diophantine approximations.

One such property was already mentioned in the first chapter. This was the

$$\textit{Fundamental Inequality:}\quad |a| \prod_{j=1}^{r} |a|_{p_j} \geq 1$$

where $a \neq 0$ is any rational integer, and $p_1, \dots, p_r$ are finitely many distinct primes. Thus, in particular,

$$|a| \geq 1 \quad \text{and} \quad |a|_p \geq \frac{1}{|a|}\ .$$

The second property makes a statement on the density of the rational integers on the real axis:

If α and β are real numbers such that $\alpha < \beta$, then there are exactly $[\beta] - [\alpha]$ rational integers g such that $\alpha < g \leq \beta$. In particular, the interval $0 \leq g \leq \beta$ contains exactly $[\beta] + 1$, and the interval $-\beta \leq g \leq \beta$ exactly $2[\beta] + 1$ rational integers.

Here $[\alpha]$ denotes as usual the integral part of α, i.e., the greatest rational integer that does not exceed α.

The third property is the famous

> *Principle of Dirichlet* (Schubfachprinzip): *If* n+1 *elements are distributed among* n *sets, then at least one set contains more than one element.*

As we shall find, all three properties will again and again be applied on the following pages.

1. Notation.

Let $\alpha \epsilon \dot{P}$, $\alpha_0 \epsilon P_p$, $A \epsilon P_g$, and $A^* \epsilon P_{g^*}$ be any real, p-adic, g-adic, and g*-adic number, respectively, and let

$$|a|, \ |a|_p, \ |a|_g, \text{ and } |a|_{g^*}$$

be the corresponding valuations or pseudo-valuations. When properties in common to all four kinds of numbers are being discussed, we shall use the letter a for any one of them; and the symbol $\omega(a)$ will then stand for the corresponding valuation or pseudo-valuation.

By integer, without any qualifying term, we always mean a *rational integer*. All polynomials that occur in this chapter lie in the polynomial ring $\Gamma[x]$, thus have rational coefficients. If

$$g(x) = b_0x^q + b_1x^{q-1} + \dots + b_q$$

is such a polynomial, the maximum

$$\overline{|g(x)|} = \max(|b_0|, |b_1|, \dots, |b_q|)$$

is called the *height of* g(x). Throughout this chapter,

$$F(x) = A_0x^m + A_1x^{m-1} + \dots + A_m$$

is an arbitrary polynomial with integral coefficients, of a degree not exceeding m and of height $A = \overline{|F(x)|}$.

2. The minimum polynomial of an algebraic number.

Let a be a fixed number (real, p-adic, g-adic, or g*-adic) which is algebraic over Γ. There exists thus at least one polynomial $g(x) \neq 0$ in $\Gamma[x]$ such that $g(a) = 0$. Among all polynomials with this property we select one of lowest degree, the polynomial

$$f(x) = a_0x^n + a_1x^{n-1} + \dots + a_n, \quad \text{where } a_0 \neq 0, \ n \geqslant 1,$$

say.

If g(x) *vanishes for* $x=a$, *then* g(x) *is divisible by* f(x). For g(x) may be divided by f(x) and then takes the form

$$g(x) = f(x)h(x) + k(x),$$

where h(x) and k(x) are again in $\Gamma[x]$, and k(x) is of lower degree than

$f(x)$ or vanishes identically. Since $k(\mathbf{a}) = g(\mathbf{a}) - f(\mathbf{a})\, h(\mathbf{a}) = 0$, $k(x)$ is divisible by $f(x)$, whence $k(x) \equiv 0$.

We call $f(x)$ the ***minimum polynomial***, and $f(x) = 0$ the ***minimum equation***, for $\mathbf{a}$. Except for a constant factor distinct from zero, the minimum polynomial evidently is unique, and hence so is its degree n. The number $\mathbf{a}$ is then likewise said to have the degree n.

> *If the algebraic number* $\mathbf{a}$ *is real or* p-*adic, then the minimum polynomial* $f(x)$ *is irreducible over* Γ, *but this need not be true if* $\mathbf{a}$ *is a* g-*adic or* g*-*adic number.*

First let $\mathbf{a}$ belong to either P or P_p; thus $\mathbf{a}$ is element of a ***field***. Further suppose that $f(x) = g(x)h(x)$ where $g(x)$ and $h(x)$ are nonconstant polynomials in $\Gamma[x]$ and therefore are of lower degrees than $f(x)$. It follows that $g(\mathbf{a}) \neq 0$ and $h(\mathbf{a}) \neq 0$, hence that also the product $g(\mathbf{a})h(\mathbf{a}) = f(\mathbf{a})$ is distinct from zero, which is false.

Secondly assume that $\mathbf{a}$ lies in P_g or P_{g^*}. Then the last proof is no longer valid since there are zero divisors in both rings. By way of example, the g-adic number $A \longleftrightarrow (1, 0, \ldots, 0)$ has the minimum polynomial $f(x) = x(x-1)$ which is reducible over $\Gamma[x]$.

> *A* g-*adic or* g*-*adic number is algebraic if and only if all its components are algebraic.*

The proof is the same in both cases; it suffices therefore to deal with the case of a g-adic number $A \longleftrightarrow (\alpha_1, \ldots, \alpha_r)$. If A is algebraic, let $f(x)$ be its minimum polynomial. Then

$$f(A) \longleftrightarrow [f(\alpha_1), \ldots, f(\alpha_r)] = 0, \quad \text{hence} \quad f(\alpha_1) = \ldots = f(\alpha_r) = 0.$$

It follows that all components $\alpha_1, \ldots, \alpha_r$ are algebraic, and that their minimum polynomials are divisors of $f(x)$. Conversely, let $\alpha_1, \ldots, \alpha_r$ be algebraic, with the minimum polynomials $f_1(x), \ldots, f_r(x)$, respectively, and let $f(x)$ be the least common multiple of these polynomials. Then

$$f(\alpha_1) = \ldots = f(\alpha_r) = 0 \quad \text{and hence} \quad f(A) \longleftrightarrow [f(\alpha_1), \ldots, f(\alpha_r)] = 0$$

and so A is likewise algebraic. It is clear from this proof that the minimum polynomial of A is equal to the least common multiple of the minimum polynomials of its components. The same is true for algebraic g*-adic numbers A^*.

> *The minimum polynomial of an algebraic number* $\mathbf{a}$ *has no multiple zeros, hence is relatively prime to its derivative.*

The assertion certainly holds when $\mathbf{a} = \alpha$ or $\mathbf{a} = \alpha_0$ because then $f(x)$ is irreducible over Γ, a field of characteristic 0. It still remains valid when $\mathbf{a} = A$ or $\mathbf{a} = A^*$ because the least common multiple of finitely many polynomials irreducible over Γ cannot have multiple zeros.

3. An algebraic identity.

Let $\mathbf{a}$ be again an algebraic number. We may assume that its minimum polynomial

$$f(x) = a_0x^n + a_1x^{n-1} + \dots + a_n, \quad \text{where } a_0 \neq 0,\ n \geq 1,$$

has integral coefficients, and we write

$$a = \overline{|f(x)|}\,.$$

Denote by

$$F(x) = A_0x^m + A_1x^{m-1} + \dots + A_m$$

a second polynomial with integral coefficients, of height

$$A = \overline{|F(x)|}\,.$$

We assume, for the present, that

(i): $A_0 \neq 0$, so that $F(x)$ has the exact degree m; and
(ii): $F(x)$ is relatively prime to $f(x)$.

These restrictions will later be relaxed.

As is proved in algebra, these two conditions imply that the resultant

$$R=\left|\begin{array}{ccccccccc}
a_0 & a_1 & a_2 & \cdots & a_{n-1} & a_n & 0 & \cdots & 0\\
0 & a_0 & a_1 & \cdots & a_{n-2} & a_{n-1} & a_n & \cdots & 0\\
\vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots\\
0 & 0 & 0 & \cdots & a_0 & a_1 & a_2 & \cdots & a_n\\
A_0 & A_1 & A_2 & \cdots & A_{m-1} & A_m & 0 & \cdots & 0\\
0 & A_0 & A_1 & \cdots & A_{m-2} & A_{m-1} & A_m & \cdots & 0\\
\vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots\\
0 & 0 & 0 & \cdots & A_0 & A_1 & A_2 & \cdots & A_m
\end{array}\right|
\begin{array}{l}
\left.\vphantom{\begin{array}{c}a\\a\\a\\a\end{array}}\right\}m \text{ rows}\\
\left.\vphantom{\begin{array}{c}a\\a\\a\\a\end{array}}\right\}n \text{ rows}
\end{array}$$

of $f(x)$ and $F(x)$ is distinct from zero. Denote by $g(x)$ and $G(x)$ the two determinants that are obtained from the determinant for R by leaving the first $m+n-1$ columns unchanged, while replacing the last column by a new one consisting of the successive terms

$$x^{m-1},\ x^{m-2}, \dots,\ 1,\ 0,\ 0,\ \dots,\ 0$$

and

$$0,\ 0,\ \dots,\ 0,\ x^{n-1},\ x^{n-2},\ \dots,\ 1,$$

respectively. Then the following identity holds:

(1): $$R = f(x)g(x) + F(x)G(x).$$

For multiply the 1st, 2nd,..., $(m+n-1)$st column of R by the factors

$$x^{m+n-1},\ x^{m+n-2}, \dots,\ x$$

and add to the last column. This operation does not change the value of the determinant, but transforms it into a new determinant where the last column now consists of the terms

$$x^{m-1}f(x),\ x^{m-2}f(x), \dots,\ 1\cdot f(x),\ x^{n-1}F(x),\ x^{n-2}F(x), \dots,\ 1\cdot F(x).$$

On splitting this column into the two columns

$$x^{m-1}f(x),\ x^{m-2}f(x),\ \ldots,\ 1\cdot f(x),\ 0,\ 0, \ldots\ 0,$$

and

$$0,\ 0,\ \ldots\ 0,\ x^{n-1}F(x),\ x^{n-2}F(x),\ \ldots\ ,\ 1\cdot F(x),$$

the assertion follows at once.

From its definition as a determinant of order $m+n$, R is a sum of at most $(m+n)!$ terms where each term is a positive or negative product of m factors a_ν and n factors A_μ. It follows that R satisfies the inequality

(2): $$1 \leqslant |R| \leqslant (m+n)!\, a^m A^n.$$

Here the lower bound holds because R is an integer distinct from zero.

Similarly, $g(x)$ and $G(x)$ may be written as polynomials of the form

$$g(x) = b_0 x^{m-1} + b_1 x^{m-2} + \ldots + b_{m-1}$$

and

$$G(x) = B_0 x^{n-1} + B_1 x^{n-2} + \ldots + B_{n-1},$$

where the coefficients b_μ and B_ν are the cofactors of the last column of R, hence are determinants of order $m+n-1$. They are thus integers, and an estimate just as for R leads to the inequalities

(3): $$\lceil g(x) \rceil \leqslant (m+n-1)!\, a^{m-1} A^n,$$

(4): $$\lceil G(x) \rceil \leqslant (m+n-1)!\, a^m A^{n-1}\ .$$

4. Inequalities for algebraic numbers.

On putting $x = \alpha$ in the identity (1), it follows that

$$R = F(\alpha)G(\alpha)$$

and hence that

(5): $$\omega\{F(\alpha)\} = \omega\left(\frac{R}{G(\alpha)}\right)\ .$$

In order to deduce lower bounds for $\omega\{F(\alpha)\}$ from this equation, it becomes necessary to distinguish between the four different kinds of numbers.

Case 1: $\alpha = \alpha$ *is a real algebraic number.*

Since $G(x)$ is at most of degree $n-1$, the inequality (4) implies that

$$|G(\alpha)| \leqslant \lceil G(x) \rceil\ (|\alpha|^{n-1} + |\alpha|^{n-2} + \ldots + |\alpha| + 1) \leqslant$$
$$\leqslant (m+n-1)!\, a^m A^{n-1}(|\alpha|^{n-1} + |\alpha|^{n-2} + \ldots + |\alpha| + 1).$$

On the other hand, by (2),

$$|R| \geqslant 1.$$

It follows therefore from (5) that

(I,1): $$|F(\alpha)| \geqslant c_1(m)\, A^{-(n-1)}$$

where the factor

$$c_1(m) = \{(m+n-1)!\, a^m(|\alpha|^{n-1} + |\alpha|^{n-2} + \ldots + |\alpha| + 1)\}^{-1}$$

depends on α and m, but is independent of A.

Case 2: $\mathfrak{a} = \alpha_0$ *is a* p-*adic algebraic number.*

Since the polynomial G(x) has integral coefficients and is at most of degree n-1,

$$|G(\alpha_0)|_p \leqslant \max(|\alpha_0|_p^{n-1}, |\alpha_0|_p^{n-2}, \ldots, |\alpha_0|_p, 1) = \max(|\alpha_0|_p^{n-1}, 1).$$

On the other hand, by (2) and the fundamental inequality,

$$|R|_p \geqslant \{(m+n)!\, a^m A^n\}^{-1}.$$

Hence it follows from (5) that

(I,2): $$|F(\alpha_0)|_p \geqslant c_2(m) A^{-n}$$

where the factor

$$c_2(m) = \{(m+n)!\, a^m \max(|\alpha_0|_p^{n-1}, 1)\}^{-1}$$

depends on α_0 and m, but is independent of A.

So far, the inequalities (I,1) and (I,2) have only been proved if F(x) satisfies the conditions (i) and (ii) of § 3,

(i): F(x) has the exact degree m, and
(ii): F(x) is relatively prime to f(x).

However, *both inequalities remain valid if only the following weaker conditions are imposed,*

(i'): F(x) *is at most of degree* m, *and*
(ii'): $F(\mathfrak{a}) \neq 0$.

For let m' be the exact degree of F(x). Then $m' \leqslant m$, hence

$$c_1(m') \geqslant c_1(m), \quad c_2(m') \geqslant c_2(m).$$

The inequalities (I,1) and (I,2) corresponding to the degree m' are thus at least as strong as those corresponding to the degree m and imply the latter.

Next, in both cases $\mathfrak{a} = \alpha$ and $\mathfrak{a} = \alpha_0$ the hypothesis $F(\mathfrak{a}) \neq 0$ implies that F(x) is relatively prime to f(x). For the polynomial f(x) is now irreducible over Γ, and so F(x) and f(x) cannot have a nonconstant common factor unless F(x) is divisible by f(x).

Case 3: $\mathfrak{a} = A \leftrightarrow (\alpha_1, \ldots, \alpha_r)$ *is a* g-*adic algebraic number.*

Let again F(x) be at most of degree m, and let $F(A) \neq 0$. Then

$$F(A) \leftrightarrow [F(\alpha_1), \ldots, F(\alpha_r)] \neq 0,$$

and so there is a suffix j with $1 \leqslant j \leqslant r$ such that $F(\alpha_j) \neq 0$. Let $f_j(x)$, the minimum polynomial of α_j, have the degree $n^{(j)}$ and the height $a^{(j)}$. The inequality (I,2) may be applied to the component $F(\alpha_j)$ of F(A), giving

$$|F(\alpha_j)|_{p_j} \geqslant c_2^{(j)}(m)\, A^{-n^{(j)}},$$

where $c_2^{(j)}(m)$ stands for

$$c_2^{(j)}(m) = \{(m+n^{(j)})!\, a^m \max(|\alpha_j|_{p_j}^{n^{(j)}-1}, 1)\}^{-1}.$$

Put

$$n(A) = \max\left(\frac{n^{(1)}\log g}{e_1 \log p_1}, \dots, \frac{n^{(r)}\log g}{e_r \log p_r}\right)$$

and

$$c_3(m) = \min\left(c_2^{(1)}(m)^{\frac{\log g}{e_1 \log p_1}}, \dots, c_2^{(r)}(m)^{\frac{\log g}{e_r \log p_r}}\right).$$

By the definition of the g-adic value,

$$|F(A)|_g = \max\left(|F(\alpha_1)|_{p_1}^{\frac{\log g}{e_1 \log p_1}}, \dots, |F(\alpha_r)|_{p_r}^{\frac{\log g}{e_r \log p_r}}\right).$$

It follows then, finally, that

(I,3): $$|F(A)|_g \geqslant c_3(m)\, A^{-n(A)},$$

where the exponent $n(A)$ is a positive number depending only on A, and $c_3(m)$ is a positive number that depends on A and m, but not on A.

Case 4: $\alpha = A^*$ is a g^*-adic algebraic number.

Let $A^* \leftrightarrow (\alpha, A)$ be the decomposition of A^* into its real and its g-adic components. We assume that $F(A^*) \neq 0$. Since

$$F(A^*) \leftrightarrow [F(\alpha), F(A)],$$

at least one of the two components $F(\alpha)$ and $F(A)$ is distinct from zero. If $F(\alpha) \neq 0$, then $|F(\alpha)|$ satisfies an inequality of the form (I,1); if, however, $F(A) \neq 0$, then an inequality of the form (I,3) holds for $|F(A)|_g$. Now, by the definition of the g^*-adic value,

$$|F(A^*)|_{g^*} = \max(|F(\alpha), |F(A)|_g).$$

It follows therefore that there exist a non-negative number $n(A^*)$ depending only on A^*, and a positive number $c_4(m)$ depending on both A^* and m, but not on A, such that

(I,4): $$|F(A^*)|_{g^*} \geqslant c_4(m) A^{-n(A^*)}.$$

On combining the four inequalities (I,1)-(I,4), the following result is obtained.

Theorem 1: *Let* α *be an algebraic number* (real, p-adic, g-adic, or g^*-adic), *and let* $F(x)$ *by a polynomial with integral coefficients, of degree at most* m *and of height* A. *There exist a non-negative number* $n(\alpha)$ *depending on* α *but not on* m *or* A, *and a positive number* $c(\alpha, m)$ *depending on* α *and* m *but not on* A, *such that*

$$\textit{either}\ F(\alpha) = 0, \text{ or } \omega\{F(\alpha)\} \geqslant c(\alpha,m)\, A^{-n(\alpha)}.$$

The importance of this theorem lies in the fact that the exponent $n(\alpha)$ is entirely independent of the polynomial $F(x)$. As we shall see, the position is very different for transcendental numbers.

There is a second theorem involving the product of the values of the components of $F(\alpha)$. Put

$$\Omega\{F(\mathsf{a})\} = \begin{cases} |F(\alpha)| & \text{if } \mathsf{a} = \alpha, \\ |F(\alpha_0)|_p & \text{if } \mathsf{a} = \alpha_0, \\ \prod_{j=1}^{r} |F(\alpha_j)|_{p_j} & \text{if } \mathsf{a} = A \longleftrightarrow (\alpha_1, \ldots, \alpha_r), \\ |F(\alpha)| \prod_{j=1}^{r} |F(\alpha_j)|_{p_j} & \text{if } \mathsf{a} = A^* \longleftrightarrow (\alpha, \alpha_1, \ldots, \alpha_r). \end{cases}$$

A proof just like that of Theorem 1 leads to the following result.

Theorem 1': *Let the hypothesis be as in Theorem* 1. *Put* $\nu(\mathsf{a})$ *equal to* n-1 *or* n, *according as* a *has, or has not, a real component; here* n *denotes the degree of* a. *There exists a positive number* $\gamma(\mathsf{a}, m)$ *depending on* a *and* m *but not on* A *such that*

$$\textit{either } \Omega\{F(\mathsf{a})\} = 0, \text{ or } \Omega\{F(\mathsf{a})\} \geqslant \gamma(\mathsf{a}, m) A^{-\nu(\mathsf{a})}.$$

The proofs of both theorems depend very essentially on the Fundamental Inequality. The other two general properties mentioned in the introduction have not been used. They form the basis for the next investigations.

5. A theorem on linear forms.

From now on the number a need no longer be algebraic. Our aim is to find polynomials F(x) for which $\omega\{F(\mathsf{a})\}$ is small. The construction makes use of Dirichlet's principle and of the density properties of the integers which were mentioned in the introduction. In the special case when F(x) is a linear polynomial, a simpler and more explicit method will be given in the next chapter.

We begin with a general theorem on linear forms[1]

Theorem 2: *Let*

$$L_h(x) = \sum_{k=1}^{n} a_{hk} x_k \qquad (h = 1, 2, \ldots, n)$$

be n *linear forms in* n *variables with real coefficients, and let*

$$a = \max_{h=1,2,\ldots,n} \sum_{k=1}^{n} |a_{hk}| > 0.$$

If $\lambda_1, \ldots, \lambda_n$ *are* n *positive numbers such that*

$$\lambda_1 \ldots \lambda_n > a^n,$$

there exist n *integers* $x_1, \ldots, x_n$ *not all zero satisfying*

$$|L_h(x)| < \lambda_h \qquad (h = 1, 2, \ldots, n).$$

[1] This is a slightly weakened form of Minkowski's theorem on linear forms (Geometrie der Zahlen, §§ 36-37). I learned the proof as given here more than 30 years ago from my teacher C. L. Siegel.

Proof: Denote by N a very large positive integer, and define n further positive integers $t_1,\ldots, t_n$ by the formulae

$$t_h = \left[\frac{2aN}{\lambda_h}\right] + 1 \qquad (h = 1,2,\ldots, n).$$

Since, asymptotically,

$$t_1 \ldots t_n \sim \frac{a^n}{\lambda_1 \ldots \lambda_n} (2N+1)^n \qquad \text{as } N \to \infty,$$

N can be chosen so large that

$$t_1 \ldots t_n < (2N+1)^n.$$

The ordered system $(x_1,\ldots, x_n)$ is said to be *admissible* if each x_h equals one of the 2N+1 integers $0, \mp 1, \mp 2, \ldots, \mp N$ between -N and +N. There are then $(2N+1)^n$ admissible systems. For such systems,

$$|L_h(x)| = | \sum_{k=1}^{n} a_{hk}x_k | \leq N \sum_{k=1}^{n} |a_{hk}| \leq aN,$$

so that

$$-aN \leq L_h(x) \leq +aN.$$

Divide the interval [-aN, +aN], for each suffix h=1, 2,..., n, into t_h subintervals of equal length $\frac{2aN}{t_h}$, the subintervals $J_1^{(h)}, J_2^{(h)}, \ldots, J_{t_h}^{(h)}$, say; points on the boundary of two adjacent intervals should be counted as belonging to only one of them. In accordance with the values assumed by the forms $L_1(x),\ldots, L_n(x)$, there corresponds to each admissible system $(x_1,\ldots, x_n)$ a unique ordered system $(J_{l_1}^{(1)},\ldots, J_{l_n}^{(n)})$ of n subintervals such that $L_h(x) \epsilon J_{l_h}^{(h)}$. By the construction, the number of all such systems of n subintervals is exactly $t_1 \ldots t_n$, hence is less than the number of admissible systems $(x_1,\ldots, x_n)$.

It follows then, from Dirichlet's principle, that there exist two distinct admissible systems $(x_1',\ldots, x_n')$ and $(x_1'',\ldots, x_n'')$ for which the values of $L_1(x'),\ldots, L_n(x')$ and of $L_1(x''),\ldots, L_n(x'')$ lie in the same system of subintervals $(J_{l_1}^{(1)},\ldots, J_{l_n}^{(n)})$. Therefore

$$|L_h(x') - L_h(x'')| \leq \frac{2aN}{t_h} \qquad (h = 1,2,\ldots, n).$$

Put

$$x_1 = x_1' - x_1'', \ldots, x_n' = x_n' - x_n''.$$

Then $x_1,\ldots, x_n$ are integers not all zero for which

$$|L_h(x)| = |L_h(x') - L_h(x'')| \leq \frac{2aN}{t_h} < \lambda_h \quad (h = 1,2,\ldots \ n)$$

because

$$t_h = \left[\frac{2aN}{\lambda_h}\right] + 1 > \frac{2aN}{\lambda_h}\ .$$

6. On a system of both real and p-adic linear forms.

From Theorem 2 we shall now deduce a result on the values of systems of linear forms that have coefficients in different completions of the rational field.

Denote by

$$l(x) = \alpha_1 x_1 + \ldots + \alpha_M x_M$$

a linear form with real coefficients not all zero for which

$$|\alpha_1| + \ldots + |\alpha_M| \leqslant 1,$$

further by $p_1, \ldots, p_r$ finitely many distinct primes, and by

$$l_j(x) = \alpha_{j1}x_1 + \ldots + \alpha_{jM}x_M \qquad (j = 1,2,\ldots, r)$$

a linear form with p_j-adic coefficients satisfying

$$\max(|\alpha_{j1}|_{p_j}, \ldots, |\alpha_{jM}|_{p_j}) \leqslant 1 \quad (j = 1,2,.,., r).$$

Since $l(x)$ has at least one non-zero coefficient, there is no loss of generality in assuming that

$$\alpha_M \neq 0;$$

for, if necessary, it suffices to renumber the variables.

Let $E_1, \ldots, E_r$ be r arbitrary positive integers. By hypothesis, the coefficients $\alpha_{j\mu}$ of each form $l_j(x)$ are p_j*-adic integers*. Hence there exist rational integers $a_{j\mu}$ satisfying the inequalities

$$|\alpha_{j\mu} - a_{j\mu}|_{p_j} \leqslant p_j^{-E_j},\ 0 \leqslant a_{j\mu} \leqslant p_j^{E_j} - 1 \quad \begin{pmatrix} j = 1,2,\ldots, r \\ \mu = 1,2,\ldots, M \end{pmatrix}$$

Now put

$$l_j^*(x) = a_{j1}x_1 + \ldots + a_{jM}x_M \qquad (j = 1,2,\ldots, r)$$

and

$$L_j(x) = \begin{cases} p_j^{-E_j}(M+1)^{-1}\{l_j^*(x) + p_j^{E_j}x_{M+j}\} & \text{if } j = 1,2,\ldots, r, \\ x_\mu & \text{if } j = r+\mu,\ \mu = 1,2,\ldots, M-1, \\ l(x) & \text{if } j = M+r \end{cases}$$

The linear forms $L_j(x)$ so defined have real coefficients such that *the sum of the absolute values of the coefficients of each form is not greater than* 1.

Therefore, on applying Theorem 2, with $n=M+r$ and $a=1$, it follows that *there exist integers* $x_1, x_2, \ldots, x_{M+r}$ *not all zero satisfying the system of inequalities*

$$|L_j(x)| < \lambda_j \qquad (j = 1,2,\ldots,M+r),$$

whenever $\lambda_1, \lambda_2, \ldots, \lambda_{M+r}$ are positive numbers such that

$$\lambda_1 \lambda_2 \ldots \lambda_{M+r} > 1.$$

Let us now specialize this result in two different ways.

First specialization: Denote by T a number greater than 1 and define a number $t > 1$ by

$$t^{M-1} = 2(M+1)^r p_1^{E_1} \ldots p_r^{E_r} T;$$

further put

$$\lambda_j = \begin{cases} p_j^{-E_j}(M+1)^{-1} & \text{if } j = 1,2,\ldots, r, \\ t & \text{if } j = r+\mu,\ \mu = 1,2,\ldots, M-1, \\ \frac{1}{T} & \text{if } j = M+r. \end{cases}$$

Then

$$\lambda_1 \lambda_2 \ldots \lambda_{M+r} = 2,$$

and so we may apply the last result. It follows then from the formulae for $L_j(x)$ and λ_j that there exist integers $x_1, x_2, \ldots, x_{M+r}$ not all zero satisfying the inequalities

$$|l_j^*(x) + p_j^{E_j} x_{M+j}| < 1 \qquad (j = 1,2,\ldots, r),$$

$$|x_\mu| < t \qquad (\mu = 1,2,\ldots, M-1),$$

$$|l(x)| < \frac{1}{T}.$$

The first r of these formulae imply that already $x_1, \ldots, x_M$ cannot all vanish; for otherwise also $x_{M+1} = \ldots = x_{M+r} = 0$.

These first r inequalities are equivalent to

$$l_j^*(x) + p_j^{E_j} x_{M+j} = 0 \qquad (j = 1,2,\ldots, r),$$

because the expressions on the left-hand sides are integers. Hence

$$l_j^*(x) \equiv 0 (\text{mod } p_j^{E_j}) \qquad (j = 1,2,\ldots, r)$$

and therefore

$$|l_j^*(x)|_{p_j} \leqslant p_j^{-E_j} \qquad (j = 1,2,\ldots, r).$$

Now

$$|l_j(x) - l_j^*(x)|_{p_j} = \left|\sum_{\mu=1}^{M} (\alpha_{j\mu} - a_{j\mu}) x_\mu\right|_{p_j} \leqslant \max_{\mu = 1,2,..,M} |\alpha_{j\mu} - a_{j\mu}|_{p_j} \leqslant p_j^{-E_j},$$

so that also

$$|l_j(x)|_{p_j} = |l_j^*(x) + (l_j(x) - l_j^*(x))|_{p_j} \leqslant \max(|l_j^*(x)|_{p_j}, |l_j(x) - l_j^*(x)|_{p_j}) \leqslant p_j^{-E_j}$$

$$(j = 1,2,\ldots, r).$$

Finally, from $T > 1$ and $t > 1$ and from the last M inequalities, we deduce that

$$|\alpha_M x_M| = |l(x) - (\alpha_1 x_1 + \ldots + \alpha_{M-1} x_{M-1})| \leqslant |l(x)| + (|\alpha_1| + \ldots + |\alpha_{M-1}|)t < \frac{1}{T} + t < 2t.$$

Since $|\alpha_M| \leqslant 1$, it follows that

$$\max(|x_1|, \ldots, |x_M|) < \frac{2t}{|\alpha_M|}.$$

Second specialisation: Put

$$l(x) = x_M$$

which is evidently allowed, and choose

$$T = \frac{1}{t} \quad \text{where} \quad t^M = 2(M+1)^r p_1^{E_1} \ldots p_r^{E_r}.$$

Otherwise leave the notation just as in the first specialisation. On repeating the last computations, it now follows that there exist integers $x_1, \ldots, x_M$ not all zero such that

$$|l_j(x)|_{p_j} \leqslant p_j^{-E_j} \qquad (j = 1,2,\ldots, r),$$
$$\max(|x_1|, \ldots, |x_M|) < t.$$

The two results just proved contain the following theorem.

Theorem 3: *Let*

$$l(x) = \alpha_1 x_1 + \ldots + \alpha_M x_M, \quad \text{where} \quad 0 < |\alpha_1| + \ldots + |\alpha_M| \leqslant 1,$$

be a linear form with real coefficients; let $p_1, \ldots, p_r$ *be finitely many distinct primes; let*

$$l_j(x) = \alpha_{j1} x_1 + \ldots + \alpha_{jM} x_M, \quad \textit{where} \quad \max(|\alpha_{j1}|_{p_j}, \ldots, |\alpha_{jM}|_{p_j}) \leqslant 1,$$

be, for $j = 1,2,\ldots, r$, *a linear form with* p_j*-adic coefficients; let* $E_1, \ldots, E_r$ *be positive integers; and let* $T > 1$.

(i): *There exists a positive constant* Δ_1 *independent of* $E_1, \ldots, E_r$, *and* T, *such that there are integers* $x_1, \ldots, x_M$ *for which*

$$|l(x)| < \frac{1}{T}, \; |l_1(x)|_{p_1} \leqslant p_1^{-E_1}, \ldots, |l_r(x)|_{p_r} \leqslant p_r^{-E_r},$$

$$0 < \max(|x_1|, \ldots, |x_M|) < \Delta_1 (p_1^{E_1} \ldots p_r^{E_r} T)^{\frac{1}{M-1}}.$$

(ii): *There exists a positive constant* Δ_2 *independent of* $E_1, \ldots, E_r$ *such that there are integers* $x_1, \ldots, x_M$ *for which*

$$|l_1(x)|_{p_1} \leqslant p_1^{-E_1}, \ldots, |l_r(x)|_{p_r} \leqslant p_r^{-E_r},$$

$$0 < \max(|x_1|, \ldots, |x_M|) < \Delta_2 (p_1^{E_1} \ldots p_r^{E_r})^{\frac{1}{M}}.$$

Remark: Theorem 3 may be extended to systems that contain more than one real linear form, more than one p_1-adic linear form, etc., and more than one p_r-adic linear form. The best method is to apply either Minkowski's theorem on linear forms or his theorem on lattice points in convex bodies.

7. Polynomials $F(x)$ for which $\omega\,\{F(\boldsymbol{\alpha})\}$ is small.

Let $\boldsymbol{\alpha}$ be an arbitrary algebraic or transcendental number (real, p-adic, g-adic, or g*-adic). Theorem 3 leads to the construction of polynomials

$$F(x) = A_0x^m + A_1x^{m-1} + \ldots + A_m$$

with integral coefficients, of degree at most m and of height $A > 0$, for which $\omega\{F(\boldsymbol{\alpha})\}$ is small. They are obtained by specialising the linear forms $l(x)$ and $l_j(x)$ and choosing the parameters $E_1,\ldots, E_r$, and T suitably. The theorem is applied with $M=m+1$, and with $A_0, A_1,\ldots, A_m$ instead of $x_1,\ldots,x_M$ as the variables. One must again distinguish between the different kinds of numbers.

Case 1: $\boldsymbol{\alpha} = \alpha$ is a real number.

In Theorem 3(i) choose $r=0$ and

$$l(x) = \kappa^{-1}(A_0\alpha^m + A_1\alpha^{m-1} + \ldots + A_m)$$

where

$$\kappa = |\alpha|^m + |\alpha|^{m-1} + \ldots + |\alpha| + 1.$$

Further denote by s an arbitrary number greater than 1 and put

$$T = \kappa s^m.$$

Since the hypothesis of the theorem evidently is satisfied, it follows that there exists a polynomial $F(x)$ for which

$$\text{(IV,1):}\qquad |F(\alpha)| \leqslant s^{-m}, \qquad 0 < A \leqslant \Delta_1\kappa^{1/m}\cdot s.$$

Cases 2 *and* 3: $\boldsymbol{\alpha}$ *is a* p*-adic or a* g*-adic number.*

Let $\boldsymbol{\alpha} = A\leftrightarrow(\alpha_1,\ldots,\alpha_r)$ be a g-adic number; for $r=1$ this includes the case of a p-adic number. Define non-negative integers $f_1,\ldots, f_r$ by the equations

$$p_j^{f_j} = \max(1, |\alpha_j|_{p_j}) \qquad (j = 1,2,\ldots, r)$$

and apply Theorem 3(ii) to the linear forms

$$l_j(A) = p_j^{mf_j}(A_0\alpha_j^m + A_1\alpha_j^{m-1} + \ldots + A_m) \quad (j = 1,2,\ldots,r)$$

the coefficients of which obviously are p_j-adic *integers*. Also put

$$E_j = mf_j + (m+1)e_jt \qquad (j = 1,2,\ldots, r)$$

where t is an arbitrarily large positive integer and $e_1,\ldots, e_r$ are, as usual, the exponents in

$$g = p_1^{e_1}\ldots p_r^{e_r}.$$

The hypothesis of the theorem is again satisfied. It follows that *there exists a polynomial* F(x) *with the properties*

$$(\mathrm{IV},2): \qquad |F(A)|_g \leq g^{-(m+1)t}, \quad 0 < A \leq \Delta_2 \left(\prod_{j=1}^{r} p_j^{f_j}\right)^{\frac{m}{m+1}} \cdot g^t .$$

For we first obtain the second inequality together with the formulae

$$|F(\alpha_j)|_{p_j} \leq p_j^{-(m+1)e_j t} \qquad (j = 1,2,\ldots, r),$$

and these imply the first inequality by the definition of the g-adic value.

Let, in particular, $\alpha = \alpha_0$ be a p-adic number. We now define a single non-negative integer f by

$$p^f = \max(1, |\alpha_0|_p)$$

and apply the inequality (V,2) with g=p and r=1. It follows that if t is an arbitrarily large positive integer, *there exists a polynomial* F(x) *with the properties*

$$(\mathrm{IV},3): \qquad |F(\alpha_0)|_p \leq p^{-(m+1)t}, \quad 0 < A \leq \Delta_2 p^{\frac{fm}{m+1}} \cdot p^t.$$

Case 4: $\alpha = A^* \longleftrightarrow (\alpha, \alpha_1, \ldots, \alpha_r)$ *is a* g^**-adic number.*

Define κ, $f_1, \ldots, f_r$, $l(x)$, $l_1(x), \ldots, l_r(x)$ exactly as in the first two cases, and put

$$T = \kappa g^{mt}; \qquad E_j = m(f_j + e_j t) \qquad (j = 1,2,\ldots, r),$$

where t is again an arbitrarily large positive integer. The hypothesis of Theorem 3(i) is then satisfied, and it follows that *there exists a polynomial* F(x) *for which*

$$(\mathrm{IV},4): \qquad |F(A^*)|_{g^*} \leq g^{-mt}, \quad 0 < A \leq \Delta_1 \kappa^{\frac{1}{m}} \prod_{j=1}^{r} p_j^{f_j} \cdot g^{2t} .$$

For the second inequality is obtained exactly in the form given, but instead of the first inequality we obtain the r+1 relations

$$|F(\alpha)| \leq g^{-mt}, \qquad |F(\alpha_j)|_{p_j} \leq p_j^{-e_j mt} \qquad (j = 1,2,\ldots, r).$$

These, however, imply that

$$|F(A)|_g \leq g^{-mt}, \qquad \text{hence that} \qquad \max(|F(\alpha)|, |F(A)|_g) \leq g^{-mt},$$

so that the assertion follows from the definition of the g*-adic value.

In the four cases denote by u the upper bounds

$$\Delta_1 \kappa^{\frac{1}{m}} . s, \quad \Delta_2 \left(\prod_{j=1}^{r} p_j^{f_j}\right)^{\frac{m}{m+1}} . g^t, \quad \Delta_2 p^{\frac{fm}{m+1}} \cdot p^t, \quad \Delta_1 \kappa^{\frac{1}{m}} \prod_{j=1}^{r} p_j^{f_j} . g^{2t},$$

respectively, that were obtained for A. The results just proved may be combined to give the following theorem.

Theorem 4: *Let* α *be an arbitrary number* (real, p-adic, g-adic, or g*-adic), *and let* m *be any positive integer. Put*

$$\mu(\alpha, m) = \begin{cases} m & \text{if } \alpha \text{ is real,} \\ m+1 & \text{if } \alpha \text{ is p-adic or g-adic,} \\ \frac{m}{2} & \text{if } \alpha \text{ is g*-adic.} \end{cases}$$

There exists a positive constant $\gamma(\alpha, m)$ *depending on* α *and on* m *but not on* A, *as follows. If* u *is any sufficiently large positive number, there is a polynomial* F(x) *with integral coefficients, of degree at most* m *and of height* A, *such that*

$$\omega\{F(\alpha)\} \leq \gamma(\alpha, m)\, u^{-\mu(\alpha, m)}, \quad 0 < A \leq u.$$

Hence also

$$\omega\{F(\alpha)\} \leq \gamma(\alpha, m) A^{-\mu(\alpha, m)}.$$

This theorem has again an analogue for the function $\Omega\{F(\alpha)\}$, defined in § 4, which is proved just like Theorem 4.

Theorem 4': *Let* α *and* m *be as in Theorem* 4, *and let*

$$M(\alpha, m) = \begin{cases} m & \text{if } \alpha \text{ is real or g*-adic,} \\ m+1 & \text{if } \alpha \text{ is p-adic or g-adic.} \end{cases}$$

There exists a positive constant $\Gamma(\alpha, m)$ *depending on* α *and on* m *but not on* A, *as follows. If* u *is any sufficiently large positive number, there is a polynomial* F(x) *with integral coefficients, of degree at most* m *and of height* A, *such that*

$$\Omega\{F(\alpha)\} \leq \Gamma(\alpha, m)\, u^{-M(\alpha, m)}, \quad 0 < A \leq u.$$

Therefore also

$$\Omega\{F(\alpha)\} \leq \Gamma(\alpha, m) A^{-M(\alpha, m)}.$$

8. A necessary and sufficient condition for transcendency.

From now on let α be a transcendental number. The polynomial f(x) of Theorem 4 then satisfies the inequalities

$$0 < \omega\{F(\alpha)\} \leq \gamma(\alpha, m) u^{-\mu(\alpha, m)}, \quad 0 < A \leq u,$$

because $F(\alpha) \neq 0$ by the hypothesis.

Assume further that the parameter u tends to infinity, so that $\omega\{F(\alpha)\}$ tends to zero. This implies that F(x) cannot remain fixed, but must run over an infinite sequence of distinct polynomials with heights A tending to infinity. For there are only finitely many polynomials F(x) with integral coefficients, of degrees not greater than m and of bounded heights; and for such a set of polynomials $\omega\{F(\alpha)\}$ necessarily has a positive minimum.

Hence, if α is transcendental, there exist infinitely many distinct polynomials $F(x)$ with integral coefficients, of degrees not exceeding m and of heights tending to infinity, such that

$$0 < \omega\{F(\alpha)\} \leqslant \gamma(\alpha,m)A^{-\mu(\alpha,m)}.$$

This is true whatever the value of m. We may then choose m so large that $\mu(\alpha,m)$ is greater than any prescribed positive number Λ and that therefore

$$\gamma(\alpha,m)A^{-\mu(\alpha,m)} < A^{-\Lambda}$$

as soon as A is sufficiently large.

This result may be combined with Theorem 1, leading to the following test for transcendency.

Theorem 5: *The number* α (which may be real, p-adic, g-adic, or g*-adic) *is transcendental if and only if, given any positive number* Λ, *there exist a positive integer* m *and infinitely many distinct polynomials* $F(x)$ *with integral coefficients, of degrees not exceeding* m *and of heights* A *tending to infinity, such that*

$$0 < \omega\{F(\alpha)\} \leqslant A^{-\Lambda}.$$

This test leads immediately to a special class of transcendental numbers, the Liouville numbers[2]. A number α is said to be a Liouville number if there exist, (i) an infinite sequence of distinct rational numbers

$$\left\{\frac{P_1}{Q_1}, \frac{P_2}{Q_2}, \frac{P_3}{Q_3}, \ldots\right\} \quad \text{where} \quad (P_n,Q_n) = 1,\ H_n = \max(|P_n|,|Q_n|),$$

and (ii) an infinite sequence of positive numbers

$$\{\Lambda_1, \Lambda_2, \Lambda_3, \ldots\}$$

tending to infinity, such that

$$0 < \omega\left(\alpha - \frac{P_n}{Q_n}\right) < H_n^{-\Lambda_n} \qquad (n = 1,2,3,\ldots).$$

Every Liouville number is transcendental.

For put

$$F_n(x) = Q_u x - P_n$$

so that $F_n(x)$ is a polynomial of the first degree of height H_n. Then

$$\omega\{F_n(\alpha)\} \leqslant \omega(Q_n)\omega\left(\alpha - \frac{P_n}{Q_n}\right) < H_n^{-(\Lambda_n - 1)}$$

because, by the definition of ω,

$$\omega(Q_n) \leqslant |Q_n| \leqslant H_n.$$

The assertion is thus contained in the special case $m=1$ of Theorem 5.

There is no difficulty in constructing Liouville numbers, and thus transcendental numbers, of each of the four kinds. Thus the real number

[2] The real Liouville numbers were discovered by Liouville in 1844; for the reference see the introduction to the second part. These numbers gave the first explicit examples of transcendental numbers.

$\sum\limits_{1}^{\infty} 2^{-n!}$, the g-adic number $\sum\limits_{1}^{\infty} g^{n!}$, and the g*-adic number $\sum\limits_{1}^{\infty} \left(\frac{g}{g+1}\right)^{(n^2)!}$ all are Liouville numbers. This is proved easily by taking as rational approximations $\frac{P_n}{Q_n}$ the sums of the first n terms of these series.

However, Liouville numbers are the least interesting examples of transcendental numbers. None of the more important constants of real analysis, like e, π, and log 2, are Liouville numbers, although they are transcendental. Actually, proofs of their transcendency may be based of Theorem 5, but it then is necessary to consider polynomials $F(x)$ of arbitrarily high degree.

We shall later prove some theorems by means of which it is possible to construct transcendental numbers that are not Liouville numbers. But our aim is not to give a general theory of transcendental numbers and of proofs of transcendency. For this important and beautiful theory the reader is referred to the following three books:

A. *Gelfond,* Transcendental and algebraic numbers (in Russian), Moscow 1952.
C. L. *Siegel,* Transcendental numbers, Princeton 1949.
Th. *Schneider,* Transzendente Zahlen, Berlin 1957.