LECTURES ON TRANSCENDENTAL NUMBERS

KURT MAHLER

I. In this introductory lecture I shall collect certain properties of transcendental numbers which are of interest in themselves and may suggest further work.

We shall be concerned only with real or complex numbers, but analogous theories can be developed for p-adic numbers and for formal power series, say with coefficients in a finite field.

The number ξ is called algebraic if there is at least one polynomial

$$(1) \qquad a(n) = a_0 + a_1x + \cdots + a_mx^m, \qquad a_m \neq 0,$$

with integral coefficients such that $a(\xi) = 0$, and it is called transcendental if no such polynomial exists.

That there are transcendental numbers was first proved by Liouville in 1844, and the transcendency of e was established by Hermite in 1873. Since then much progress has been made and still is being made, and I shall in the following lectures report on some of this work. However, let us begin with a general necessary and sufficient, condition for transcendency. For this purpose, it is convenient to use the notations

$$L(a) = |a_0| + |a_1| + \cdots + |a_m|, \qquad \Lambda(a) = 2^mL(a).$$

The use of $L(a)$, the length of a, is advantageous because this function has much simpler properties than the height of a. Thus

$$L(a \mp b) \leq L(a) + L(b), \qquad L(ab) \leq L(a)L(b),$$

and if a and b are of the degrees m and n, respectively,

$$L(ab) \geq 2^{-(m+n)}L(a)L(b),$$

that is, $\Lambda(ab) \geq L(a)L(b)$. Roth's theorem establishes a necessary, but *not* sufficient, condition for transcendence. A necessary and sufficient condition is given by the following theorem:

THEOREM. *The number ξ is transcendental if and only if there exist*
(i) *an infinite sequence of distinct polynomials*

$$\{a_1(x), a_2(x), a_3(x), \ldots\}$$

with integral coefficients, and
(ii) *an infinite sequence of positive numbers*

$$\{\omega_1, \omega_2, \omega_3, \ldots\}$$

tending to ∞, such that

$$0 < |a_r(\xi)| < \Lambda(a_r)^{-\omega_r} \qquad (r = 1, 2, 3, \ldots).$$

Thus transcendental numbers, but not algebraic ones, can be approximated very closely by algebraic numbers distinct from them.

I shall not deal with the old classification of transcendental numbers into S, T, and U-numbers, but would like to mention a new classification which may possibly become useful.

If ξ is any real or complex number and t is a positive integer, let $\Sigma = \Sigma(\xi \mid t)$ be the set of all polynomials of arbitrary degree n, $a(z) = a_0 + \cdots + a_n z^n$, with integer coefficients such that

$$a(\xi) \neq 0, \qquad \Lambda(a) = 2^n L(a) \leq t,$$

and then put

$$\Omega(\xi \mid t) = \inf_{a(z) \in \Sigma} |a(\xi)|,$$

so that $0 \leq \Omega(\xi \mid t) \leq 1$, and $\Omega(\xi \mid t)$ is a decreasing function of t. On putting

$$\omega(\xi \mid t) = \log \{1/\Omega(\omega \mid t)\},$$

we obtain a nondecreasing function of t, with the following properties:
(1) $\omega(\xi \mid t) = O(\log t)$ if ξ is algebraic;
(2) $\omega(\xi \mid t) > c(\log t)^2$ if ξ is transcendental ($c > 0$ depends only on ξ);
(3) if ξ and η are two transcendental numbers which are algebraically dependent over $\mathbf{Q}$, then there exist constants $c_1 > 0$, $c_2 > 0$, $\gamma_1 > 0$, $\gamma_2 > 0$, $t_0 > 0$, such that for all $t \geq t_0$

$$(*) \qquad \omega(\xi \mid t^{c_1}) \geq \gamma_1 \omega(\eta \mid t) \quad \text{and} \quad \omega(\eta \mid t^{c_2}) \geq \gamma_2 \omega(\xi \mid t).$$

We may distribute transcendental numbers ξ into classes according to the order of magnitude for $t \to \infty$ of $\omega(\xi \mid t)$. Then algebraically dependent numbers fall into the same class provided that functions satisfying (*) are put into the same class.

The most interesting classes of numbers for which transcendency has been proved are given as the values of suitable analytic functions. These functions in many cases are defined as power series with integral or rational or algebraic coefficients. Since the time of Weierstrass, many mathematicians have posed conjectures on values of such functions at algebraic points, e.g. that they cannot always be algebraic numbers. Surprisingly, most of these conjectures turned out to be wrong, and mathematicians like Häckel, Faber, Hurwitz, Gelfond, Lekkerkerker have obtained results as follows:

(1) There are entire transcendental functions

$$f(z) = \sum_{h=0}^{\infty} f_h z^h$$

with rational coefficients f_h such that, for every algebraic α, all values

$$f(\alpha), f'(\alpha), f''(\alpha), \ldots$$

are algebraic.

(2) There exist transcendental power series

$$f(z) = \sum_{h=0}^{\infty} f_h z^h$$

with integral coefficients f_h, which converge for $|z| < 1$, such that, for every algebraic α satisfying $|\alpha| < 1$, all values

$$f(\alpha), f'(\alpha), f''(\alpha), \ldots$$

are algebraic.

(3) There exists a transcendental power series

$$f(z) = \sum_{h=0}^{\infty} f_h z^h$$

with rational coefficients f_h which converges at least for $|z| < \rho$ and is here algebraic for algebraic z and transcendental for transcendental z.

(4) Let

$$f(z) = \sum_{h=0}^{\infty} f_h z^h$$

be a power series with real coefficients which represents an entire transcendental function, say with exactly the zeros $\{\zeta_1, \zeta_2, \zeta_3, \ldots\}$. Then there exists also an entire transcendental function

$$F(z) = \sum_{h=0}^{\infty} F_h z^h$$

with *rational* coefficients and exactly the same zeros

$$\{\zeta_1, \zeta_2, \zeta_3, \ldots\}.$$

(5) Let $(\alpha_1, \beta_1), \ldots, (\alpha_n, \beta_n)$ be finitely many pairs of real or complex numbers,

as follows:

(a) $0 < |\alpha_k| < 1$ (for $k = 1, 2, \ldots, n$).
(b) If α_k is real for any k, so is β_k.
(c) If α_k is not real, there is an α_l, $l \neq k$, such that

$$\alpha_l = \bar{\alpha}_k, \qquad \beta_l = \bar{\beta}_k.$$

Then there exists a power series

$$f(z) = \sum_{k=0}^{\infty} f_h x^h$$

with bounded integral coefficients f_s such that

$$f(\alpha_k) = \beta_k \qquad (k = 1, 2, \ldots, n).$$

We may choose for the a_k conjugate algebraic numbers. The result shows then that $f(z)$ may be algebraic in one of these points and transcendental in the conjugate algebraic points.

All these theorems make quite clear that for general power series with rational or integral coefficients *no general assertions on transcendency can be made* with respect to their values at algebraic points. Such values will sometimes be algebraic and sometimes transcendental.

One has succeeded in proving the transcendence of function values $f(\alpha)$, α algebraic, mainly in the case where $f(z)$ satisfies one or more functional equations. Thus Hermite's proof of the transcendence of e is based on the pair of functional equations

$$\frac{d}{dz} e^z = e^z, \qquad e^{z+w} = e^z e^w.$$

Siegel's proof of the transcendency of $J_0(\alpha)$ uses the linear differential equation for $J_0(z)$, and Shidlovski's more general results apply to the solutions of systems of linear differential equations.

Let us mention at this point several unsolved problems. They are all in some way connected with the problem of the digits of a transcendental decimal fraction.

(I). Does there exist a transcendental power series

$$f(z) = \sum_{h=0}^{\infty} f_h z^h$$

with *bounded* integral coefficients which is algebraic in all algebraic points $z = \alpha$ where $|\alpha| < 1$?

If the condition of boundedness is dropped, we found that such series do exist. I conjecture that for transcendental power series with bounded integral coefficients f_h the sequence $\{\alpha_1, \alpha_2, \alpha_3, \ldots\}$ of algebraic points $z = \alpha_k$ for which $f(\alpha_k)$ also is algebraic always satisfies $\lim_{k\to\infty} |\alpha_k| = 1$. Such points have thus no limit point in the interior of the unique circle. A simple example is

$$f(z) = \prod_{n=0}^{\infty} (1 - 2z^{2^n}).$$

If my conjecture is wrong, $f(z)$ may be algebraic in all points $z = 1/g$, $g = 2, 3, \ldots$. It would then follow that, for sufficiently large g, the g-adic fraction

$$\sum_{h=0}^{\infty} f_h g^{-h}$$

is algebraic. Since $|f_h|$ is bounded, we could add a multiple of the rational number

$$\sum_{h=0}^{\infty} g^{-h} = \frac{g}{g-1},$$

and would then get a g-adic series where all coefficients are digits $0, 1, \ldots, c$ with $c < g - 1$. There would thus be algebraic irrationals, the g-adic series of which would not contain all digits $0, 1, \ldots, g - 1$.

In the case $g = 3$, my conjecture takes the form

(II) Cantor's set of all triadic series

$$\sum_{n=0}^{\infty} \frac{a_n}{3^n}, \quad \text{where } a_n = 0 \text{ or } = 2,$$

does not contain any irrational algebraic number. (It is obvious that there are infinitely many rational numbers in Cantor's set.)

II. As a preparation to the deep results by Siegel and Shidlovski, I shall today discuss some simpler results of mine which appeared in 1929 and 1930 in three papers in Mathematische Annalen and Mathematische Zeitschrift.

The problem to be discussed is under which additional conditions analytic functions defined, say, by convergent power series

$$f(z) = \sum_{h=0}^{\infty} f_h z^h$$

can for algebraic z inside the circle of convergence assume algebraic values.

If $f(z)$ is an algebraic function of z, it is not difficult to prove that

(i) $f(z)$ is algebraic at all regular algebraic points z if all the Taylor coefficients f_h are algebraic, but

(ii) there are at most finitely many algebraic points z for which $f(z)$ is algebraic if at least one coefficient f_h is transcendental, and these points can be determined.

We exclude now algebraic functions and impose on $f(z)$ the

1st restriction. $f(z)$ is a transcendental function of z, and, in the hope of simpler results, also

2nd restriction. The Taylor coefficients f_h of $f(z)$ are algebraic numbers, say they lie in a finite algebraic number field K.

Even if these two restrictions are combined, it is not possible to make general assertions on the function values of $f(z)$ at algebraic points. For we saw already that there exist even transcendental entire functions with *rational* coefficients f_h for which $f(z)$ is algebraic for all algebraic z. Thus still further restrictions have to be imposed on $f(z)$.

These additional restrictions on $f(z)$ usually take the form of one or more functional equations, in particular of differential equations. By way of example, Hermite's proof of the transcendency of e and Lindemann's proof of the transcendency of π are both based on the pair of functional equations

$$\frac{d}{dz}e^z = e^z \quad \text{and} \quad e^{z+z'} = e^z e^{z'}.$$

In the work of Siegel and Shidlovski, an analogous role is played by a system of linear differential equations.

Let us begin with the simpler case where the additional condition takes the following form.

3rd restriction. Let $\rho \geq 2$ be a fixed positive integer, and let m be an integer satisfying $1 \leq m < \rho$; let further

$$a_l(z),\ b_l(z) \qquad (l = 0, 1, \ldots, m)$$

be polynomials in z with algebraic coefficients where $a_m(z)$ and $b_m(z)$ do not both vanish identically. Further let $f(z)$ satisfy the functional equation

$$f(z^\rho) = \frac{\sum_{l=0}^{m} a_l(z) f(z)^l}{\sum_{l=0}^{m} b_l(z) f(z)^l}. \tag{1}$$

This class of functional equation has interest in itself, but not much seems to be known about it. It can be generalized; thus one might consider the more general kind of functional equation $P(z, f(z), f(z^\rho)) = 0$ where P is a polynomial in its arguments, at most of degree $< \rho$ in both $f(z)$ and $f(z^\rho)$. When P is of degree $\geq \rho$ in $f(z)$ and $f(z^\rho)$, difficulties arise which I have not so far overcome. This is regrettable because the transformation equations of the modular function $f(z) = j(\log z/2\pi i)$ are exactly of this kind.

Let $f(z)$ satisfy our three restrictions, and let not only the Taylor coefficients f_h, but also the coefficients of the polynomials $a_l(z)$ and $b_l(z)$ lie in the finite number field K, and so let z_0 and $f(z_0)$. The problem to solve is for which values of z_0 this can be the case. Naturally K can always be replaced by a larger algebraic number field; the hypothesis just made is therefore a natural one when both z_0 and $f(z_0)$ have algebraic values.

If $z = 0$, $f(z) = f_0$ certainly is algebraic; we exclude this trivial case and assume that $0 < |z_0| < 1$. Then $z_0^{\rho^n}$ lies for sufficiently large n in the circle of convergence of $f(z)$, and hence the functional equation (1) enables us to obtain the value of $f(z_0)$ from the series, possibly after solving an algebraic equation.

In fact, on applying (1) successively to

$$z_0^\rho,\ z_0^{\rho^2},\ \ldots,\ z_0^{\rho^n}$$

and eliminating $f(z_0^\rho), f(z_0^{\rho^2}), \ldots, f(z_0^{\rho^{n-1}})$ from the equations so obtained, we evidently obtain a relation of the form

$$(2) \qquad f(z_0^{\rho^n}) = \frac{\sum_{l=0}^{m^n} a_l^{(n)}(z_0) f(z_0)^l}{\sum_{l=0}^{m^n} b_l^{(n)}(z_0) f(z_0)^l}$$

where

$$a_l^{(n)}(z) \quad \text{and} \quad b_l^{(n)}(z) \qquad (l = 0, 1, \ldots, m^n)$$

are certain $2(m^n + 1)$ polynomials in z which have again coefficients in K, and without loss of generality *integral* coefficients. From the known value of $f(z_0^{\rho^n})$ (known from the power series), the value of $f(z_0)$ is obtained by solving (2) for $f(z_0)$. This will only then become impossible when the right-hand side becomes indeterminate because the polynomials in u,

$$\sum_{l=0}^{m^n} a_l^{(n)}(z) u^l \quad \text{and} \quad \sum_{l=0}^{m^n} b_l^{(n)}(z) u^l,$$

have a common zero $u = u_0$. A detailed discussion shows that this can happen only if z_0 satisfies one of the equations

$$\Delta(z^{\rho^k}) = 0 \qquad (k = 0, 1, 2, \ldots)$$

where $\Delta(z)$ is the resultant of

$$\sum_{l=0}^{m} a_l(z) u^l \quad \text{and} \quad \sum_{l=0}^{m} b_l(z) u^l$$

with respect to u.

Such values of z_0 may indeed lead to algebraic values of $f(z_0)$ as can be seen in simple examples. We exclude this difficulty by imposing the

4th restriction. For every integer $h \geq 0$, z_0 satisfies $\Delta(z_0^{\rho\cdot}) \neq 0$.

I would like to add that in the two special cases

$$f(z^\rho) = \frac{\sum_{l=0}^{m} a_l(z) f(z)^l}{b_0(z)} \qquad (b_0(z) \not\equiv 0)$$

and

$$f(z^\rho) = \frac{a_0(z)}{\sum_{l=0}^{m} b_l(z) f(z)^l} \qquad (a_0(z) \not\equiv 0)$$

the resultant $\Delta(z)$ is to be defined by

$$\Delta(z) = a_m(z) b_0(z) \quad \text{and} \quad \Delta(z) = a_0(z) b_m(z),$$

respectively.

The four restrictions are sufficient to settle the problem of transcendency $f(z)$.

THEOREM. *If the function $f(z)$ and the number z_0 satisfy the four restrictions and if $0 < |z_0| < 1$, then z_0 and $f(z_0)$ cannot both lie in K, and therefore at least one of these two numbers is transcendental.*

The proof runs as follows. Denote by p a large positive integer. One can then construct $p + 1$ polynomials not all identically zero,

$$A_0(z), A_1(z), \ldots, A_p(z),$$

of degree at most p with integral coefficients in K such that in the new power series

$$E_p(z) = \sum_{l=0}^{p} A_l(z) f(z)^l = \sum_{h=0}^{\infty} B_h z^h, \quad \text{say,} \tag{3}$$

all coefficients B_h with $h \leq (p + 1)^2 - 2$ are zero. For we have $(p + 1)^2$ coefficients of the $A_l(z)$ at our disposal and need satisfy only the $(p + 1)^2 - 1$ homogeneous linear equations

$$B_0 = B_1 = \cdots = B_{(p+1)^2-2} = 0$$

for these coefficients where these linear equations have coefficients in K.

By the 1st restriction, $E_p(z)$ is not identically zero; there is thus a suffix h_0 satisfying $h_0 \geq (p + 1)^2 - 1 > p^2$ such that

$$B_{h_0} \neq 0. \tag{4}$$

Let now n be a large positive integer, and let

$$E_p^{(n)}(z) = E_p(z^{\rho^n}) \left\{ \sum_{l=0}^{m^n} b_l^{(n)}(z) f(z)^l \right\}^p.$$

By the formula (2), we can also write

$$E_p^{(n)}(z) = \sum_{l=0}^{km^n} B_l^{(n)}(z) f(z)^l \tag{5}$$

where the $B_l^{(n)}(z)$ are again polynomials with integral coefficients in K. One can easily obtain majorants for these polynomials and for $E_p^{(n)}(z)$. The hypothesis of the 4th restriction shows that, for the given z_0,

$$\sum_{l=0}^{m^n} b_l^{(n)}(z_0) f(z_0)^l \neq 0.$$

Further, for large n,

$$E_p(z_0^{\rho^n}) \sim B_{h_0} z_0^{h_0 \rho^n}, \quad \text{hence } E_p^{(n)}(z_0) \neq 0.$$

With the usual taking of the norm it follows then that

$$0 < |E_p^{(n)}(z_0)| \leq \exp(-c_1 p^2 \rho^n), \tag{6}$$

while

(7) $$|E_p^{(n)}(z_0)| > \exp(-c_2 p\rho^n).$$

Here $c_1 > 0$ and $c_2 > 0$ depend on z_0, but not on p and n. From (6) and (7), a contradiction arises as soon as p and n are sufficiently large. This proves the theorem.

By way of example, the two functions

$$f_1(z) = \prod_{n=0}^{\infty}(1 + z^{2^n}) \quad \text{and} \quad f_2(z) = \prod_{u=0}^{\infty}(1 - z^{2^n})$$

have power series convergent for $|z| < 1$, and they satisfy the functional equations

$$f_1(z^2) = \frac{f(z)}{1+z} \quad \text{and} \quad f_2(z^2) = \frac{f(z)}{1-z},$$

respectively. Further the resultants become

$$\Delta(z) = 1 + z \quad \text{and} \quad \Delta(z) = 1 - z,$$

respectively, and hence, for all n,

$$\Delta(z^{2^n}) \neq 0 \quad \text{if} \quad 0 < |z| < 1.$$

Hence if

$$0 < |z_0| < 1 \quad \text{and} \quad z_0 \text{ is algebraic,}$$

then $f_k(z_0)$ is transcendental provided $f_k(z)$ is a transcendental function. But it is easily proved that $f_1(z) \equiv 1/(1 - z)$ is an algebraic function.

The second function $f_2(z)$, however, *is* transcendental and in fact cannot be continued beyond $|z| = 1$.

Much more, and for more general classes of functions, can be proved. Thus if, e.g.

$$f(z) = \sum_{n=0}^{\infty} \frac{z^{\rho^n}}{1 - z^{\rho^n}},$$

all derivatives

$$f^{(k)}(z) \qquad (k = 0, 1, 2, \ldots)$$

are easily proved to satisfy a simple system of functional equations similar to the one studied. One can also show that $f(z)$ does not satisfy any algebraic differential equation, and that the Taylor coefficients of $f(z)$ are rational integers. From this it can again be deduced that, if

(8) $$0 < |z_0| < 1, \quad \text{and } z_0 \text{ is an algebraic number,}$$

then, for every m, the $m + 1$ function values

(9) $$f(z_0), f'(z_0), \ldots, f^{(m)}(z_0)$$

are algebraically independent over $\mathbf{Q}$.

Perhaps even more interesting is the analogous result for

$$f(z) = \sum_{h=0}^{\infty} [h\omega] z^m$$

where $\omega > 0$ is a real quadratic irrationality, and [ ] denotes the integral part. Again, if (8) holds, the function values (9) are algebraically independent.

I have discussed the functions of today's lecture because somewhat similar ideas play a role in Shidlovski's work.

III. In the remaining three lectures, I shall discuss the beautiful results obtained by Shidlovski by generalizing Siegel's ideas of 1929.

These results are concerned with entire functions satisfying linear differential equations with rational functions as coefficients. It is convenient to consider instead systems of linear differential equations

$$Q^*: w_h' = \sum_{k=1}^{m} q_{hk} w_k + q_{h0} \qquad (h = 1, 2, \ldots, m),$$

where the coefficients

$$q_{hk}, q_{h0}$$

are arbitrary rational functions of z. We shall also have to deal with the corresponding homogeneous system

$$Q: w_h' = \sum_{k=1}^{m} q_{hk} w_k \qquad (h = 1, 2, \ldots, m).$$

While there are no further restrictions on the coefficients q_{hk}, q_{h0} of Q^* and Q, the theory of Siegel and Shidlovski is specialized by restrictions on the solution vectors

$$\mathbf{w} = \begin{bmatrix} w_1 \\ \vdots \\ w_m \end{bmatrix}$$

of these systems. Not only will only that case be considered in which all the components

$$w_h = \sum_{l=0}^{\infty} w_{hl} z^l \qquad (h = 1, 2, \ldots, m)$$

are *entire* functions, but these entire functions will be restricted to a very special class, the so-called E-functions of Siegel.

These are defined as follows:

Let K be a number field of finite degree N over $\mathbf{Q}$. If $\alpha \in K$, denote as usual by

$$\overline{|\alpha|} = \max(|\alpha|, |\alpha'|, \ldots, |\alpha^{(N-1)}|)$$

the maximum of the absolute values of the conjugates of α relative to $\mathbf{Q}$.

The series

$$f(z) = \sum_{l=0}^{\infty} f_l \frac{z^l}{l!}$$

is now a Siegel E-function over K if the following conditions are satisfied:

(1) All $f_l \in K$.

(2) $\overline{|f_l|} = O(l^{\epsilon l})$ for all l and all $\epsilon > 0$.

(3) There exists for each $l \geq 0$ a positive rational integer $d_l = O(l^{\epsilon l})$ for all l and $\epsilon > 0$ such that

$$d_l f_k = \text{algebraic integer for } k = 0, 1, \ldots, l.$$

The E-functions so defined are entire functions, possibly polynomials. If $\gamma \in K$, $f(\gamma z)$ also is an E-function. Further the set of all E-functions forms a ring which is moreover closed under differentiation and under the integration $\int_0^z \ldots dz$.

The E-functions are so important because of the following lemma by Siegel.

Lemma. *Let*

$$f_h(z) = \sum_{l=0}^{\infty} f_{hl} \frac{z^l}{l!} \qquad (h = 1, 2, \ldots, m)$$

be finitely many E-functions, say over K; let $0 < \phi < 1$; *and let n be any positive integer. Then there exist n polynomials*

$$p_h(z) = \sum_{l=0}^{\infty} G_{hl} z^l \qquad (h = 1, 2, \ldots, n)$$

with integral coefficients in K not all zero where

$$\max_{h,l} \overline{|G_{hl}|} = O(n^{(1+\epsilon)n})$$

for all $\epsilon > 0$, *while, on putting*

$$p = mn - [\phi n] - 1 \quad \textit{and} \quad \sum_{h=1}^{m} p_h(z) f_h(z) = \sum_{l=0}^{\infty} a_l \frac{z^l}{l!},$$

all coefficients $a_0 = a_1 = \cdots = a_{p-1} = 0$, *and* $\overline{|a_l|} = n^n O(l^{\epsilon l})$ *for all* $l \geq p$ *and* $\epsilon > 0$.

Let now in particular

$$\mathbf{f}(z) = \begin{bmatrix} f_1(z) \\ \vdots \\ f_m(z) \end{bmatrix}$$

be a solution of the homogeneous system

$$Q\colon w_h' = \sum_{k=1}^{m} q_{hk} w_k \qquad (h = 1, \ldots, m).$$

Denote by $\kappa(z)$ the polynomial with leading coefficient 1 which is the least common denominator of all the q_{hk}. As can be shown easily, since the series $f_h(z)$ have Taylor coefficients in K, the same is without loss of generality true for the coefficients of the q_{hk} and thus of κ.

We put now

$$\lambda_1\{\mathbf{w}(z)\} = \sum_{k=1}^{m} p_{1k}(z)w_k(z),$$

where

$$p_{1k}(z) = p_k(z) \qquad (k = 1, \ldots, m)$$

and deduce from λ_1 infinitely many further linear forms

$$\lambda_h\{\mathbf{w}(z)\} = \sum_{k=1}^{m} p_{hk}(z)w_k(z)$$

where

$$\lambda_{h+1} = \kappa \frac{d}{dz} \lambda_h.$$

Here $\mathbf{w}(z)$ denotes a general solution of Q, and during the differentiation w_h' is replaced by its expression from Q so that

$$p_{h+1,k} = \kappa p_{hk}' + \sum_{j=1}^{m} p_{hj}\kappa q_{jk} \qquad (h = 1, 2, \ldots, k = 1, 2, \ldots, m).$$

It is clear that also the p_{hk} are polynomials in $K[z]$, and the lemma leads to simple estimates for these coefficients and their conjugates, and also for the functions

$$\lambda_h\{\mathbf{f}(z)\} = \sum_{k=1}^{m} p_{hk}(z)f_k(z) \qquad (k = 1, 2, \ldots).$$

Siegel proved in special cases, and Shidlovski under very general conditions, that the determinant

$$P(z) = \begin{vmatrix} p_{11}(z) & \cdots & p_{1m}(z) \\ \vdots & & \vdots \\ p_{m1}(z) & \cdots & p_{mm}(z) \end{vmatrix}$$

is not identically zero. I shall discuss this fundamental question in detail; but let us for the present just assume that

(H) $$P(z) \not\equiv 0.$$

Denote by $\alpha \in K$ an algebraic number such that

(A) $$\alpha \neq 0, \qquad \kappa(\alpha) \neq 0;$$

the second condition means that $z = a$ is not a singular point of $\mathbf{Q}$. It can be deduced easily from (H), and was first done by Siegel in a special case, that there exist m suffixes $h_1, \ldots, h_m$ satisfying

$$1 \leq h_1 < h_2 < \cdots < h_m \leq [\phi n] + n_0,$$

where n_0 is a constant integer independent of n, such that by (H)

$$\text{(K)}\qquad \begin{vmatrix} p_{h_1 1}(\alpha) & \cdots & p_{h_1 m}(\alpha) \\ \vdots & & \vdots \\ p_{h_m 1}(\alpha) & \cdots & p_{h_m m}(\alpha) \end{vmatrix} \neq 0.$$

One of Shidlovski's conditions for (H) is that

$$f_1(z), \ldots, f_m(z)$$

are linearly independent over $C(z)$ and hence also over $K(z)$. Let us on the other hand assume that not more than $r < m$ of the function values

$$f_1(\alpha), \ldots, f_m(\alpha)$$

are linearly independent over K. There exists then an $(m - r) \times m$ matrix of rank $m - r$,

$$\begin{bmatrix} s_{11} & \cdots & s_{1m} \\ \vdots & & \vdots \\ s_{m-r,1} & \cdots & s_{m-r,m} \end{bmatrix}$$

with elements in K such that

$$\text{(1)}\qquad s_{h1}f_1(\alpha) + \cdots + s_{hm}f_m(\alpha) = 0 \qquad (h = 1 \ldots m - r);$$

and we can select r suffixes $h_1, \ldots, h_m$, say, $j_1, \ldots, j_r$, such that

$$S \equiv \begin{vmatrix} p_{j_1 1}(\alpha) & \cdots & p_{j_1 m}(\alpha) \\ \cdot & & \cdot \\ p_{j_r 1}(\alpha) & \cdots & p_{j_r m}(\alpha) \\ \cdot & & \cdot \\ s_{11} & \cdots & s_{1m} \\ \cdot & & \cdot \\ s_{n-r,1} & \cdots & s_{m-r,m} \end{vmatrix} \neq 0.$$

The equations (1) together with

$$\text{(2)}\qquad \lambda_h(\mathbf{f}(\alpha)) = p_{h1}(\alpha)f_1(\alpha) + \cdots + p_{hm}(\alpha)f_m(\alpha) \qquad (h = j_1, \ldots, j_r)$$

lead therefore to

$$\text{(S)}\qquad Sf_k(\alpha) = \sum_{i=1}^{r} S_{ik}\lambda_{j_i}(\mathbf{f}(\alpha)) \qquad (k = 1, \ldots, m)$$

where the S_{ik} are the cofactors of S (row i, column k).

One proceeds now in (S) to take the absolute values of the conjugates on both sides, and assumes that n is large and $\epsilon > 0$ small.

The lemma leads easily to the estimates

$$\overline{|p_{hk}(\alpha)|} = O(n^{(1+\phi+\epsilon)n}) \quad \text{for } h = j_1, \ldots, j_r,$$

and

$$|\lambda_h(\mathbf{f}(\alpha))| = O(n^{-(m-1-7\phi)n}) \quad \text{for } h = j_1, \ldots, j_m.$$

Therefore

$$\overline{|S|} = O(n^{(1+\phi+\epsilon)nr}), \qquad \overline{|S_{ik}|} = O(n^{(1+\phi+\epsilon)n(r-1)}).$$

Also $S \neq 0$ lies in K, and there is a positive integer

$$T = O(e^{cn}) \qquad (c > 0 \text{ const.})$$

such that ST is an algebraic integer and thus $|\text{norm}\,(ST)| \geq 1$. This implies by the estimate for $\overline{|S|}$ a lower bound for $|S|$ which may be written as

$$|S|^{-1} = O(n^{(1+2\phi)nr(N/\sigma-1)}).$$

Here N is the degree of the field K, and

$$\begin{aligned} \sigma &= 1 \quad \text{if } K \text{ is a real field,} \\ &= 2 \quad \text{if } K \text{ is an imaginary field.} \end{aligned}$$

For in the second case two of the conjugates of S have equal absolute value.

Finally, by (S), and since we can choose k such that $f_k(\alpha) \neq 0$ (otherwise $f(z) \equiv 0$),

$$1 = O(n^{(1+2\phi)nr(N/\sigma-1)})O(n^{(1+\phi+\epsilon)n(r-1)})O(n^{-(m-1-7\phi)n}).$$

Here we make $n \to \infty$. The sum of the exponents of n is necessarily ≥ 0, hence

$$(1 + 2\phi)r\{(N/\sigma) - 1\} + (1 + \phi + \epsilon)(r - 1) - (m - 1 - 7\phi) \geq 0.$$

Now m, r, and N/σ are fixed, and both ϕ and ϵ are arbitrarily small. Thus in the limit

$$r\{(N/\sigma) - 1\} + (r - 1) - (m - 1) \geq 0,$$

which means that $r \geq \sigma m/N$. Thus if m of the functions $f_1(z), \ldots, f_m(z)$ are linearly independent over $C(z)$, then at least $\sigma m/N$ of the function values $f_1(\alpha), \ldots, f_m(\alpha)$ are linearly independent over K and hence also over $\mathbf{Q}$.

Here $\sigma = N$ if $K = \mathbf{Q}$, or if K is an imaginary quadratic field.

The result just obtained is in this generality due to Shidlovski. He has extended it in the following way:

(I) Let not all m functions $f_h(z)$ be linearly independent over $f(z)$, but say only $\rho(z) \leq m$, and let similarly $\rho(\alpha)$ denote the maximum number of function values $f_h(\alpha)$ that are linearly independent over K or $\mathbf{Q}$. Then

(I) $$\rho(\alpha) \geq \sigma\rho(z)/N.$$

Thus again $\rho(\alpha) = \rho(z)$ if $K = \mathbf{Q}$, or if K is an imaginary quadratic field; for $\rho(\alpha)$ cannot be larger than $\rho(z)$.

(II) The results so far deal with linear independence of the components of $\mathbf{f}(z)$ or $\mathbf{f}(\alpha)$. The factor σ/N on the right hand side of (I) depends only on the field K. It is this fact which will allow us to deduce from (I) the following final theorems of Shidlovski.

1ST THEOREM. *Let* $\mathbf{f}(z)$ *be a solution in terms of E-functions of*

$$Q^*\colon w_h' = q_{h0} + \sum_{k=1}^{m} q_{hk} w_k \qquad (h = 1, 2, \ldots, m).$$

Let α *be an algebraic number* $\neq 0$ *which is a regular point of* Q^*. *Here as many of the components*

$$f_1(z), f_2(z), \ldots, f_m(z)$$

of $\mathbf{f}(z)$ *are algebraically independent over* $\mathbf{C}(z)$ *as there are components*

$$f_1(\alpha), f_2(\alpha), \ldots, f_m(\alpha)$$

of $\mathbf{f}(\alpha)$ *that are algebraically independent over* $\mathbf{Q}$.

2ND THEOREM. *Let* $\mathbf{f}(z)$ *be a solution in terms of E-functions of*

$$Q\colon w_h' = \sum_{k=1}^{m} q_{hk} w_k \qquad (h = 1, 2 \ldots m).$$

Then for α *as above as many of the function ratios*

$$f_1(z) \mid f_2(z)\colon \ldots \colon f_m(z)$$

are algebraically independent over $\mathbf{C}(z)$ *as there are function value ratios*

$$f_1(\alpha)\colon f_2(\alpha)\colon \ldots\colon f_m(\alpha)$$

that are algebraically independent over $\mathbf{Q}$.

These two general theorems have many important specializations, and I hope to find the time in my last lecture to say a little about it.

IV. This fourth lecture is to deal with the discussion of the determinant P of the last lecture, and like the next lecture, depends essentially on the work of Shidlovski. However, I shall for the present slightly generalize his method because this will bring out the basic ideas in a clearer way.

Let K be any field of characteristic 0, c any constant in K, and $K\langle z - c\rangle$ the field of formal series

$$f = \sum_{l=\lambda}^{\infty} f_l (z - c)^l, \qquad f_l \in K,$$

where λ is any integer. If $f_\lambda \neq 0$, we put

$$\text{ord}\, f = \text{ord}_c\, f = \lambda.$$

We consider a fixed system of formal differential equations

$$Q\colon w_h' = \sum_{k=1}^{m} q_{hk} w_k \qquad (h = 1, 2 \ldots m)$$

where the q_{hk} lie in $K(z)$. We shall be concerned in particular with the solutions $\mathbf{f}$ of Q that have components $f_1, \ldots, f_m$ in $K\langle z - c\rangle$.

Denote by V_Q the set of all such solutions; then V_Q is a vector space over K. A basic result asserts that if $f_1, \ldots, f_M$ are finitely many solutions in V_Q which are linearly independent over K, they are also linearly independent over $K\langle z - c\rangle$. Hence the dimension of V_Q over K, M say, satisfies $0 \leq M \leq m$.

In the special case when the least common denominator κ of all the q_{hk} is such that $\kappa(c) \neq 0$, i.e. when c is not a pole of any q_{hk}, always $M = m$.

For the deeper study of Q one introduces also a vector space over $K(z)$. Let for the present $p_1, \ldots, p_m$ be m rational functions in $K(z)$. One can then form the linear space of all forms

$$\lambda = \lambda(\mathbf{w}) = p_1 w_1 + \cdots + p_m w_m$$

where $\mathbf{w}$ denotes any solution in $K\langle z - c\rangle$ of Q.

Denote by Λ not this whole linear space, but any linear subspace; thus $\lambda_1, \lambda_2 \in \Lambda$ implies $\lambda_1 \mp \lambda_2 \in \Lambda$, and $r\lambda \in \Lambda$ if $r \in K(z)$.

We can differentiate linear forms $\lambda(\omega)$,

$$\frac{d}{dz}\lambda(w) = \frac{d}{dz}\sum_{k=1}^{m} p_k w_k = \sum_{k=1}^{m} (p_k' w_k + p_k w_k'),$$

and hence by Q,

$$\kappa \frac{d}{dz}\lambda(w) = \sum_{h=1}^{m} p_h^* w_h$$

where

$$p_h^* = \kappa\left(p_h' + \sum_{j=1}^{m} p_j q_{jh}\right).$$

On putting $D = \kappa d/dz$, $D\lambda$ is then a linear form of the same type as λ. In particular, if the p_h are polynomials, so are the p_h^*.

The following definition is now basic:

DEFINITION. The vector space Λ is said to be closed under D if $\lambda \in \Lambda$ implies $D\lambda \in \Lambda$.

THEOREM A. *Let V_Q be of dimension M over K and Λ of dimension n over $K(z)$ where $M > n$; let further Λ be closed under D. Then there exists a basis*

$$\mathbf{w}_1, \ldots, \mathbf{w}_M$$

of V_Q over K such that

$$\lambda(\mathbf{w}_1) = \cdots = \lambda(\mathbf{w}_{M-n}) = 0 \quad \text{for all } \lambda \in \Lambda.$$

I come now to the main lemma of Shidlovski. Let

$$p_{11} = p_1, \ldots, p_{1m} = p_m$$

be any polynomials in $K[z]$, and let

$$\lambda_1(\mathbf{w}) = p_{11}w_1 + \cdots + p_{1m}w_m;$$

let further, as in yesterday's lecture,

$$p_{h+1,k} = \kappa p_{hk}^* + \sum_{j=1}^{m} p_{hj}\kappa q_{jk}.$$

Then all the p_{hk} are polynomials, and the linear forms

$$\lambda_h(\mathbf{w}) = p_{h1}w_1 + \cdots + p_{hm}w_m \qquad (\mathbf{w} \in V_Q)$$

satisfy the recursive relations $\lambda_{h+1}(\mathbf{w}) = D\lambda_h(\mathbf{w})$. It is clear that the definition of the p_{hk} and λ_h is independent of c; hence we are allowed to assume that $\kappa(c) \neq 0$ so that $z = c$ is a regular point of Q. This means that V_Q has the dimension $M = m$ and that for every solution of Q,

$$\mathbf{w} = \begin{bmatrix} w_1 \\ \vdots \\ w_m \end{bmatrix}$$

with components in $K\langle z - c\rangle$, $\text{ord}_c\, w_h \geq 0$.

Having fixed λ_1 and hence λ_h for $h = 1, 2, 3, \ldots$, let Λ be the vector space over $K(z)$ spanned by these vectors, and let μ be the dimension of Λ over $K(z)$. Since $D\lambda_h = \lambda_{h+1}$, Λ is closed under D. If $\mu = m$,

$$\lambda_1, \lambda_2, \ldots, \lambda_m$$

are linearly independent forms, and hence

$$\begin{vmatrix} p_{11} & \cdots & p_{1m} \\ \vdots & & \vdots \\ p_{m1} & \cdots & p_{mm} \end{vmatrix} \neq 0.$$

For the present let this easy case be excluded so that $1 \leq \mu \leq m - 1$. Since $\lambda_1, \ldots, \lambda_\mu$ are linearly independent over $K(z)$, the matrix

$$p^* = \begin{bmatrix} p_{11} & \cdots & p_{1m} \\ \vdots & & \vdots \\ p_{\mu 1} & \cdots & p_{\mu m} \end{bmatrix}$$

has the rank μ. Therefore, without loss of generality, the minor

$$P = \begin{vmatrix} p_{11} & \cdots & p_{1\mu} \\ \vdots & & \vdots \\ p_{\mu 1} & \cdots & p_{\mu\mu} \end{vmatrix}$$

does not vanish identically. Thus the first μ columns of p^* are linearly independent over $K(z)$, and the other columns are linearly dependent on them. This means that there exist rational functions e_{ij} in $K(z)$ such that

$$p_{hj} = \sum_{i=1}^{\mu} p_{hi}e_{ij} \qquad (1 \leq h \leq \mu,\ \mu + 1 \leq j \leq m).$$

These e_{ij} naturally are unique since $P \not\equiv 0$, and they depend only on the p_{hk} and q_{hk} and not on c.

Since Λ is closed under D and evidently has the dimension

$$n = \mu \quad \text{where} \quad \mu < m = M,$$

it follows from Theorem A that there exists a basis

$$\mathbf{w}_1, \ldots, \mathbf{w}_m$$

of V_Q such that

(*) $$\lambda_h(\mathbf{w}_k) = 0 \quad \text{if } 1 \leq h \leq \mu;\ 1 \leq k \leq m - \mu.$$

Let in explicit form

$$\mathbf{w}_k = \begin{bmatrix} w_{1k} \\ \vdots \\ w_{mk} \end{bmatrix}.$$

Then

$$\lambda_h(\mathbf{w}_k) = \sum_{i=1}^{m} p_{hi}w_{ik} = \sum_{i=1}^{\mu} + \sum_{i=\mu+1}^{m}$$

$$= \sum_{i=1}^{\mu} p_{hi}\left(w_{ik} + \sum_{j=\mu+1}^{m} e_{ij}w_{jk}\right) = \sum_{i=1}^{\mu} p_{hi}W_{ik},$$

where we have put

$$W_{ik} = w_{ik} + \sum_{j=\mu+1}^{m} e_{ij}w_{jk}.$$

By (*) we have now for each $k = 1, 2, \ldots, m - \mu$

(**) $$\lambda_h(\mathbf{w}_k) = \sum_{i=1}^{\mu} p_{hi}W_{ik} = 0 \qquad (h = 1, 2, \ldots, \mu).$$

Since $P \neq 0$, this requires that

$$W_{ik} = 0 \qquad (i = 1, 2, \ldots, \mu;\ k = 1, 2, \ldots, m - \mu),$$

for (**) is a system of μ homogeneous equations for μ unknowns.

We have thus the result that

(1) $$W_{ik} \equiv w_{ik} + \sum_{j=\mu+1}^{m} e_{ij}w_{jk} = 0 \qquad (1 \leq i \leq \mu,\ 1 \leq k \leq m - \mu).$$

It is then not difficult to deduce that the matrix of order $m - \mu$

$$w^{(0)} = \begin{bmatrix} w_{\mu+1,1} & \cdots & w_{\mu+1,m-\mu} \\ \vdots & & \vdots \\ w_{m1} & \cdots & w_{m,m-\mu} \end{bmatrix}$$

is nonsingular,

$$\det w^{(0)} \neq 0.$$

For the full solution matrix

$$w = \begin{bmatrix} w_{11} & \cdots & w_{1m} \\ \vdots & & \vdots \\ w_{m1} & \cdots & w_{mm} \end{bmatrix}$$

certainly is regular, and if $\det w^{(0)}$ were $= 0$, one could use the identities (1) to deduce that also $\det w = 0$.

Put $\Omega = \det w^{(0)}$ so that $\Omega \neq 0$. One can solve the equations (1) for the rational functions e_{ij} in the form

$$e_{ij} = -\frac{\Omega_{ij}}{\Omega} \qquad (1 \leq i \leq \mu;\ \mu + 1 \leq j \leq m) \tag{2}$$

where Ω_{ij} is obtained from Ω on replacing the row

$$w_{j1}, \ldots, w_{j,m-\mu}$$

by the new row

$$w_{i1}, \ldots, w_{i,m-\mu}.$$

The formulae (2) lead to deeper results on these rational functions e_{ij}.

For this purpose, let us vary the coefficients

$$p_{11}, \ldots, p_{1m} \tag{3}$$

of λ_1 in all ways such that $1 \leq \mu \leq m - 1$. Naturally for each choice of the coefficients (3) we can expect different e_{ij} and also different bases

$$\mathbf{w}_1, \ldots, \mathbf{w}_m$$

of V_Q. Thus the determinants Ω, Ω_{ij} in (2) will vary.

However, if $\mathbf{w}_1^0, \ldots, \mathbf{w}_m^0$ is any one basis of V_Q chosen once for all, the most general basis $\mathbf{w}_1, \ldots, \mathbf{w}_m$ has the form

$$\mathbf{w}_h = \sum_{k=1}^{m} a_{hk}\mathbf{w}_k^0 \qquad (h = 1, \ldots, m)$$

where

$$(a_{hk}) \qquad (h, k = 1, 2, \ldots, m)$$

is an arbitrary nonsingular matrix with elements in K. Thus we arrive at the following results for the e_{ij}.

Form the matrix of the vectors

$$\mathbf{w}_1^0, \ldots, \mathbf{w}_m^0$$

and denote by

$$\phi_1, \phi_2, \ldots, \phi_s$$

the set which consists of all the elements of this matrix, all its minors of order 2, of order 3, etc., and finally of its determinant. Then clearly Ω and Ω_{ij} can be written as

$$\Omega = c_1\phi_1 + \cdots + c_s\phi_s$$
$$-\Omega_{ij} = c_{ij1}\phi_1 + \cdots + c_{ijs}\phi_s$$

where the c's are certain elements in K. Then

$$e_{ij} = \frac{c_{ij1}\phi_1 + \cdots + c_{ijs}\phi_s}{c_1\phi_1 + \cdots + c_s\phi_s} \tag{4}$$

where the e_{ij} are rational functions while the ϕ by their definition lie in $K\langle z - c\rangle$.

If we change now the p_{hk} so that $\mu < m$ remains fixed, only the constant coefficients c in (4), but not the ϕ's are changed. From this it can easily be deduced that

THEOREM B. *While the rational functions e_{ij} may vary with the changes of the polynomials p_{hk}, the degrees of their numerators and their denominators remain bounded.*

We come finally to the consideration of the determinant

$$\begin{vmatrix} p_{11} & \cdots & p_{1m} \\ \vdots & & \vdots \\ p_{m1} & \cdots & p_{mm} \end{vmatrix}.$$

Let us assume that Q has a solution

$$\mathbf{f} = \begin{bmatrix} f_1 \\ \vdots \\ f_m \end{bmatrix}$$

with components in $K\langle z - c\rangle$ which are linearly independent over $K(z)$.

Denote by ∂p the degree of a polynomial p, by $\mathrm{ord}_c\, w$ the order of any element w in $K\langle z - c\rangle$. For a polynomial obviously

$$\mathrm{ord}_c\, p \le \partial p \quad \text{if } p \not\equiv 0.$$

Let us now assume that the p_{hk} are such that $1 \le \mu \le m - 1$, that further X and Y are two integers such that

$$\partial p_{1k} \le X \quad \text{and} \quad \mathrm{ord}_c\, \lambda_1(\mathbf{f}) \ge Y.$$

We have found already that

$$P = \begin{vmatrix} p_{11} & \cdots & p_{1\mu} \\ \vdots & & \vdots \\ p_{\mu 1} & \cdots & p_{\mu\mu} \end{vmatrix} \not\equiv 0.$$

It is not difficult to deduce from the recursive formulae for the p_{hk} that $\partial P \le \mu X + \mu(\mu - 1)/2C_1$ where C_1 depends only on the q_{hk}. Hence also

$$\mathrm{ord}_c\, P \le \mu X + \frac{\mu(\mu - 1)}{2} C_1.$$

Let us put

$$\text{(O)} \qquad F_i = f_i + \sum_{j=\mu+1}^{m} e_{ij} f_j \qquad (i = 1 \ldots \mu),$$

so that certainly all $F_i \not\equiv 0$ because $f_1, \ldots, f_m$ are linearly independent over $K(z)$. It is easily verified that

$$\lambda_h(\mathbf{f}) = \sum_{i=1}^{\mu} p_{hi} F_i \qquad (h = 1 \ldots \mu)$$

and since $P \not\equiv 0$, for all i

$$(+) \qquad PF_i = \sum_{h=1}^{\mu} P_{ih} \lambda_h(\mathbf{f}) \qquad (1 \leq i \leq \mu).$$

The P_{ih} are cofactors of the polynomials in P, hence are themselves polynomials, and so $\operatorname{ord}_c P_{ih} \geq 0$. The e_{ij}, as we saw, have numerators and denominators of bounded degrees. Let ϵ be their common denominator which is also of bounded degree.

From (O),

$$\epsilon F_i = \epsilon f_i + \sum_{j=\mu+1}^{m} (\epsilon e_{ij}) f_j,$$

a formula from which it can be deduced that

$$\max_{1 \leq i \leq \mu} (\operatorname{ord}_c F_i) \quad \text{is bounded.}$$

It can then easily be proved from (+) that

$$\operatorname{ord}_c P \geq Y - (\mu - 1) - C_2$$

where also C_2 is an integer independent of the p_{hk}.

Since on the other hand

$$\operatorname{ord}_c P \leq \mu X + \frac{\mu(\mu - 1)}{2} C_1,$$

we deduce that for $\mu \leq m - 1$

$$\begin{aligned} Y - (m-1)X \leq Y - \mu X &\leq \frac{\mu(\mu-1)}{2} C_1 + (\mu - 1) + C_2 \\ &\leq \frac{m(m-1)}{2} C_1 + (m-1) + C_2, = C \quad \text{say.} \end{aligned}$$

Hence, conversely, if

$$\text{(S)} \qquad Y - (m - 1)X > C,$$

then we cannot have $1 \leq \mu \leq m - 1$ and therefore

$$\mu = m,$$

thus

$$\begin{vmatrix} p_{11} & \cdots & p_{1m} \\ \vdots & & \vdots \\ p_{m1} & \cdots & p_{mm} \end{vmatrix} \neq 0$$

(S) is Shidlovski's main lemma. In the application, we had

$$X = \max \partial p_{1k} \leq n - 1, \qquad Y = \operatorname{ord} \lambda_1(f) \geq mn - [\phi n] - 1,$$

where $0 < \phi < 1$; hence

$$\begin{aligned} Y - (m-1)X &\geq mn - [\phi n] - 1 - (m-1)(n-1) \\ &\geq (1-\phi)n - \text{const.}, \end{aligned}$$

and so (S) can certainly be applied as soon as n is sufficiently large.

V. Let again K be a finite number field,

$$Q\colon w'_h = \sum_{k=1}^{m} q_{hk} w_k \qquad (h = 1, 2, \ldots, m),$$

a system of homogeneous linear differential equations with coefficients $q_{hk} \in K(z)$, and κ the least common denominator of these coefficients. Let further α be any algebraic number satisfying $\alpha \neq 0$, $\kappa(\alpha) \neq 0$, and let

$$\mathbf{f}(z) = \begin{bmatrix} f_1(z) \\ \vdots \\ f_m(z) \end{bmatrix}$$

be a solution of Q with components that are Siegel E-functions. We saw that Shidlovski proved the following result.

THEOREM 1. *Denote by $\rho(z)$ the maximum number of components of $\mathbf{f}(z)$ that are linearly independent over $K(z)$, by $\rho(\alpha)$ the maximum number of components of $\mathbf{f}(\alpha)$ that are linearly independent over K. Then*

$$\rho(\alpha) \geq \frac{\sigma}{N} \rho(z).$$

Here N is the degree of K over $\mathbf{Q}$, and $\sigma = 1$ if K is real, $\sigma = 2$ if K is imaginary.

From Theorem 1 we shall deduce two general results on algebraic independence.
Denote by L and L^* any two fields of characteristic zero such that $L \subset L^*$, and by $x_1, \ldots, x_n$ any finite number of elements of L^*. These elements are called

algebraically $\left\{\begin{matrix} H\text{-dependent} \\ H\text{-independent} \end{matrix}\right\}$ over L if there $\left\{\begin{matrix} \text{exists} \\ \text{does not exist} \end{matrix}\right\}$ a homogeneous polynomial with coefficients in L,

$$P_H(X_1, \ldots, X_n) \neq 0,$$

such that

$$P_H(x_1, \ldots, x_n) = 0.$$

They are similarly called

$$\text{algebraically} \begin{Bmatrix} \text{dependent} \\ \text{independent} \end{Bmatrix} \text{ over } L \text{ if there } \begin{Bmatrix} \text{exists} \\ \text{does not exist} \end{Bmatrix}$$

a polynomial with coefficients in L,

$$P(X_1, \ldots, X_n) \not\equiv 0,$$

such that

$$P(x_1, \ldots, x_n) = 0.$$

If $x_1, \ldots, x_n$ are H-independent, evidently $x_n \neq 0$, and

$$y_1 = \frac{x_1}{x_n}, \ldots, y_{n-1} = \frac{x_{n-1}}{x_n}$$

are independent, and vice versa.

We denote by $d_H = d_H(x_1, \ldots, x_n)$ the maximum number of the $x_1, \ldots, x_n$ that are H-independent, by $d = d(x_1, \ldots, x_n)$ the maximum number that are independent, and we put

$$D_H = d_H - 1.$$

Consider now the set $V(t)$ of all the homogeneous polynomials

$$P_H(X_1, \ldots, X_n) = \sum_{h_1 \geq 0} \cdots \sum_{\substack{h_n \geq 0 \\ h_1 + \cdots + h_n = t}} P^{(H)}_{h_1 \ldots h_n} X_1^{h_1} \ldots X_n^{h_n}$$

with coefficients in L, of exact degree t, and the subset $S(t)$ of all such polynomials for which

$$P_H(x_1, \ldots, x_n) = 0.$$

Evidently $V(t)$ is a linear vector space over L of dimension

$$v(t) = \binom{n + t - 1}{n - 1},$$

and $S(t)$ is a subspace, say of dimension $s(t)$. The difference $h(t) = v(t) - s(t)$ gives the number of linearly independent homogeneous linear equations with coefficients in L which the coefficients of $P_H \in S(t)$ must satisfy.

As a special case of a much more general theorem by Hilbert of 1890, it can be proved that

$$h(t) = h_0\binom{t}{D_H} + h_1\binom{t}{D_{H^{-1}}} + \cdots + h_{D_H} \quad \text{for } t \geq t_0,$$

where $h_0 > 0, h_1, \ldots, h_d$ are certain constant integers. Thus at $t \to \infty$,

$$h(t) \sim ct^{D_H}$$

where $c > 0$ is a certain constant.

We return now to the study of the solutions $\mathbf{f}(z)$ of Q where as before $f_1(z), \ldots, f_m(z)$ are E-functions. As before let $\alpha \neq 0$, $\alpha \in K$, $\kappa(\alpha) \neq 0$. In difference from the previous notation denote by $D_H(z) + 1$ the maximum number of the functions

$$f_1(z), \ldots, f_m(z)$$

that are algebraically H-independent over $K(z)$, by $D_H(\alpha) + 1$ the maximum number of function values

$$f_1(\alpha), \ldots, f_m(\alpha)$$

that are algebraically H-independent over K.

If t is any positive integer, let $V_z(t)$ and $V_\alpha(t)$ be the sets of all H-polynomials of exact degree t with coefficients in $K(z)$, and K, respectively, and $S_z(t)$ and $S_\alpha(t)$ the subsets of the polynomials in these sets for which

$$(z) \qquad P_H(f_1(z), \ldots, f_m(z)) = 0$$

and

$$(\alpha) \qquad P_H(f_1(\alpha), \ldots, f_m(\alpha)) = 0,$$

respectively. Let similarly

$$v_z(t),\ v_\alpha(t), \qquad s_z(t),\ s_\alpha(t)$$

be the dimensions of these vector spaces, and

$$h_z(t) = v_z(t) - s_z(t), \qquad h_\alpha(t) = v_\alpha(t) - s_\alpha(t)$$

the corresponding dimensions. By Hilbert's theorem there exist then positive constants c_z and c_α such that, as $t \to \infty$,

$$(\mathrm{A}) \qquad h_z(t) \sim c_z t^{D_H(z)}, \qquad h_\alpha(t) \sim c_\alpha t^{D_H(\alpha)}.$$

We finally derive relations between $h_z(t)$ and $h_\alpha(t)$. For this purpose let

$$\mathbf{w} = \begin{bmatrix} w_1 \\ \vdots \\ w_m \end{bmatrix}$$

be the general solution of

$$Q\colon w_h' = \sum_{k=1}^{m} q_{hk} w_k \qquad (h = 1, 2, \ldots, m).$$

With each set of integers $h_1, \ldots, h_m$ satisfying

$$h_1 \geq 0, \ldots, h_m \geq 0, \qquad h_1 + \cdots + h_m = t$$

we associate the two products

$$W_{(h)} = W_{h_1 \ldots h_m} = w_1^{h_1} \ldots w_m^{h_m}$$

and

$$F_{(h)}(z) = F_{h_1 \ldots h_m}(z) = f_1^{h_1}(z) \ldots f_m^{h_m}(z).$$

The equations (z) have now on their left-hand side linear forms in the

$$\tau = v_z(t) = \binom{t+m-1}{m-1}$$

products $F_{(h)}(z)$, and the equations (α) have similarly linear forms in the τ products $F_{(h)}(\alpha)$. In either case there are $h_z(t)$ and $h_\alpha(t)$ such linearly independent homogeneous linear forms.

The original system Q for $\mathbf{w}$ and $\mathbf{f}$ implies an analogous system for the vectors $\mathbf{W}_{(h)}$ and $\mathbf{F}_{(h)}(e)$. Thus

$$W'_{(h)} = W_{(h)} \sum_{j=1}^{m} h_j w_j^{-1} w'_j = W_{(h)} \sum_{j=1}^{m} h_j w_j^{-1} \sum_{k=1}^{m} q_{jk} w_k,$$

and this is equivalent to a new system

$$Q(t)\colon \quad W'_{(h)} = \sum_{(k)} q_{(h)(k)} W_{(k)},$$

where the coefficients $q_{(h)(k)}$ are linear forms in the q_{hk} with numerical integral coefficients. Thus also the $q_{(h)(k)}$ have κ as denominator, and α, by $\kappa(\alpha) \neq 0$, is a regular point also for $Q(t)$.

A particular solution for $Q(t)$ is the vector $\mathbf{F}(z)$ with the components $F_{(h)}(z)$ which evidently are Siegel E-functions. Denote by $\rho_z(t)$ and $\rho_\alpha(t)$ the maximal number of components of $\mathbf{F}(z)$ and $\mathbf{F}(\alpha)$ that are linearly independent over $K(z)$ and K, respectively. By Shidlovski's first result,

(B) $$\rho_\alpha(t) \geq \frac{\sigma}{N} \rho_z(t).$$

We assert now that

$$\rho_z(t) = h_z(t), \qquad \rho_\alpha(t) = h_\alpha(t),$$

i.e. these ranks are simply the Hilbert functions. The proofs being the same, it suffices to prove the first relation. There are $\tau = v_z(t)$ components of $\mathbf{F}(z)$, and these satisfy $s_z(t)$ linearly independent homogeneous linear equations. Hence the number of linearly independent components of $\mathbf{F}(z)$ is indeed

$$v_z(t) - s_z(t) = h_z(t).$$

Thus, by (A) and (B),

$$c_\alpha t^{D_H(\alpha)} \sim h_\alpha(t) \geq \frac{\sigma}{N} h_z(t) \sim \frac{\sigma}{N} c_z t^{D_H(z)}.$$

Allow here $t \to \infty$. Then it follows that $D_H(\alpha) \geq D_H(z)$. In fact,

(C) $$D_H(\alpha) = D_H(z).$$

For assume that $D_H(\alpha) > D_H(z)$. We can then without loss of generality assume that

$$f_1(\alpha), \ldots, f_\delta(\alpha), \quad \text{where } \delta = D_H(\alpha) + 1,$$

are algebraically H-independent over K. On the other hand,

$$f_1(z), \ldots, f_\delta(z)$$

are certainly algebraically H-dependent over K. Thus there is an H-polynomial $P_H(X_1, \ldots, H, z) \not\equiv 0$ such that

$$P_H(f_1(z), \ldots, f_\sigma(z), z) = 0$$

identically in z. The coefficients of this polynomial are polynomials in $K(z)$, and we can assume that these polynomials are relatively prime. But then

$$P_H(X_1, \ldots, X_\delta, \alpha)$$

is not identically zero, and

$$P_H(f_1(\alpha), \ldots, f_\delta(\alpha), \alpha) = 0$$

is a nontrivial homogeneous algebraic equation for $f_1(\alpha), \ldots, f_m(\alpha)$, which is impossible.

The relation (C) is equivalent to the

First Main Theorem by Shidlovski. *Let* $\mathbf{f}(z)$ *be a solution of* Q *in E-functions, and let* α *be an algebraic number such that*

$$\alpha \neq 0, \qquad (\alpha) \neq 0.$$

Then the number of components of $\mathbf{f}(z)$ *that are algebraically H-independent over* $K(z)$ *is equal to the number of components of* $\mathbf{f}(\alpha)$ *that are algebraically H-independent over* K.

It is not difficult to show that in this independence $K(z)$ may be replaced by $\mathbf{C}(z)$ and K by $\mathbf{Q}$.

From this first result we can immediately deduce a perhaps even more striking result.

Second Main Theorem by Shidlovski. *Let* $\mathbf{f}(z)$ *be a solution of the inhomogeneous equations*

$$Q^*\colon w'_h = q_{h0} + \sum_{k=1}^{m} q_{hk} w_k \qquad (h = 1, 2, \ldots, m)$$

in terms of E-functions, and let again $\alpha \neq 0$ *be a regular algebraic point so that* $\kappa(\alpha) \neq 0$. *Then the number of components of* $\mathbf{f}(z)$ *that are algebraically independent over* $\mathbf{C}(z)$ *is equal to the number of components of* $\mathbf{f}(\alpha)$ *that are algebraically independent over* $\mathbf{Q}$.

For put $w_0 \equiv 1, f_0(z) \equiv 1$ and consider the two vectors with the components

$$w_0, w_1, \dots, w_m \quad \text{and} \quad f_0(z), f_1(z), \dots, f_m(z).$$

Both vectors satisfy the homogeneous equations

$$w_0' = 0, \qquad w_h' = q_{h0}w_0 + \sum_{k=1}^{m} q_{hk}w_k \qquad (h = 1, 2, \dots, m).$$

The result is thus an immediate consequence of the First Main Theorem.

Siegel, Shidlovski, and Shidlovski's students like Oleinikov, have applied the main theorems to special E-functions and obtained many striking results. Thus Siegel was the first to show that, for algebraic $\alpha \neq 0$, $J_0(\alpha)$ and $J_0'(\alpha)$ are algebraically independent over $\mathbf{Q}$.

That the transcendency of e and π is contained in our results is obvious. For consider Q: $w' = w$ with the solution $f(z) = e^z$ which is an E-function and is moreover transcendental. Hence e^α, for algebraic $\alpha \neq 0$, is a transcendental number by the Second Main Theorem.

Of the many other consequences I mention only two. Firstly, any finite number of the integrals

$$\int_0^1 e^{-z} (\log z)^n \, dr \qquad (n = 0, 1, 2, \dots)$$

are algebraically independent over $\mathbf{Q}$. Secondly, the very complicated number

$$\frac{\pi}{2} \frac{Y_0(\alpha)}{J_0(\alpha)} - \left(\gamma + \log \frac{\alpha}{2}\right), \qquad \alpha \neq 0 \text{ algebraic}$$

is transcendental. Here γ is Euler's constant.

Early in 1967 I thought I had a proof of the transcendency of γ itself. I made a mistake.

Ohio State University
Columbus, Ohio 43210