Modular functions and transcendence questions

1996 Sb. Math. 187 1319

(http://iopscience.iop.org/1064-5616/187/9/A04)

Sbornik: Mathematics **187**:9 1319–1348 ©1996 RAS(DoM) and LMS

Matematicheskiĭ Sbornik **187**:9 65–96 UDC 511.36

Modular functions and transcendence questions

Yu. V. Nesterenko

Abstract. We prove results on the transcendence degree of a field generated by numbers connected with the modular function $j(\tau)$. In particular, we show that π and e^{π} are algebraically independent and we prove Bertrand's conjecture on algebraic independence over $\mathbb{Q}$ of the values at algebraic points of a modular function and its derivatives.

Bibliography: 19 items.

§ 1. Statement of results

It is well known that if $\tau \in \mathbb{C}$, $\operatorname{Im} \tau > 0$, is an imaginary quadratic irrational number, then the value of the modular function $j(\tau)$ is an algebraic number (see [1], Chapter 5). For example,

$$j(i) = 1728, \quad j'(i) = 0, \qquad j(\zeta) = j'(\zeta) = j''(\zeta) = 0,$$

where $i^2 = -1$ and $\zeta = e^{2\pi i/3}$.

In 1937, Schneider [2] proved that $j(\tau)$ is transcendental if τ is algebraic but not imaginary quadratic. The purpose of the present article is to study algebraic independence of numbers connected with $j(\tau)$.

In 1916, Ramanujan [3] defined the three functions

$$P(z) = 1 - 24\sum_{n=1}^{\infty} \sigma_1(n) z^n, \qquad Q(z) = 1 + 240\sum_{n=1}^{\infty} \sigma_3(n) z^n,$$
$$R(z) = 1 - 504\sum_{n=1}^{\infty} \sigma_5(n) z^n,$$

where $\sigma_k(n) = \sum_{d|n} d^k$, and proved several identities for these functions. In particular, he showed that they satisfy the differential equations

$$\theta P = \frac{1}{12}(P^2 - Q), \qquad \theta Q = \frac{1}{3}(PQ - R), \qquad \theta R = \frac{1}{2}(PR - Q^2), \tag{1}$$

This research was carried out with the partial financial support of the Russian Foundation for Fundamental Research (grant no. 94-01-00739).

AMS 1991 *Mathematics Subject Classification.* Primary 11J89, 11J85; Secondary 11J91, 11F11.

where $\theta = z\dfrac{d}{dz}$. In 1969, Mahler proved that the functions $P(z), Q(z)$, and $R(z)$ are algebraically independent over $\mathbb{C}(z)$. (This is an easy consequence of a theorem proved in [4].)

The above properties of Ramanujan's functions, together with the fact that their Taylor coefficients are integers that do not increase very rapidly, play a crucial role in the proof of our results.

The functions $E_4(\tau) = Q(e^{2\pi i\tau})$ and $E_6(\tau) = R(e^{2\pi i\tau})$, $\operatorname{Im}\tau > 0$, are modular forms of weight 4 and 6, respectively. The function $E_2(\tau) = P(e^{2\pi i\tau})$ also has some modular properties. All of this is essential in deriving the corollaries of the theorem below, which is the basic result of the paper.

Theorem 1. *For each $q \in \mathbb{C}$ with $0 < |q| < 1$ at least three of the numbers $q, P(q), Q(q), R(q)$ are algebraically independent over $\mathbb{Q}$.*

We set

$$\Delta = \frac{1}{1728}(Q^3 - R^2) = z + \cdots, \qquad J(z) = \frac{Q(z)^3}{\Delta(z)} = \frac{1}{z} + 744 + \sum_{n=1}^{\infty} c(n)z^n.$$

The last series gives the Fourier expansion of the modular function $j(\tau) = J(e^{2\pi i\tau})$. From the differential equations (1) and the definition of $J(z)$ and $\Delta(z)$ it follows that

$$\theta\Delta = P\Delta, \qquad J = \frac{Q^3}{\Delta}, \qquad \theta J = -\frac{Q^2R}{\Delta}, \qquad \theta^2 J = \frac{-PQ^2R + 4QR^2 + 3Q^4}{6\Delta}.$$

The last three formulae can be inverted to give

$$P = 6\frac{\theta^2 J}{\theta J} - 4\frac{\theta J}{J} - 3\frac{J}{J-1728}, \qquad Q = \frac{(\theta J)^2}{J(J-1728)}, \qquad R = -\frac{(\theta J)^2}{J^2(J-1728)}.$$

If we take into account that one can have $j(\tau) = 0$, $j(\tau) = 1728$, or $j'(\tau) = 0$ only for values of τ that are equivalent to i or ζ under the modular group, then we obtain the following consequences of the above equalities.

Corollary 1. *If $\tau \in \mathbb{C}$ with $\operatorname{Im}\tau > 0$ is not equivalent to i or ζ under the modular group, and we set $q = e^{2\pi i\tau}$, then each of the quadruples*

(1) $q,\ J(q),\ J'(q),\ J''(q)$,
(2) $q,\ j(\tau),\ \pi^{-1}j'(\tau),\ \pi^{-2}j''(\tau)$

contains at least three numbers that are algebraically independent over $\mathbb{Q}$.

Corollary 2. *Suppose that q is an algebraic number with $0 < |q| < 1$. Then each set*

(1) $P(q),\ Q(q),\ R(q)$,
(2) $J(q),\ \theta J(q),\ \theta^2 J(q)$

is algebraically independent over $\mathbb{Q}$. In particular, all of these numbers are transcendental.

The first corollary follows immediately from Theorem 1. To prove Corollary 2, we note that if $q = e^{2\pi i\tau}$, then, by the Gel'fond–Schneider theorem, τ cannot be an algebraic irrationality; hence, it is not equivalent to i or ζ under the modular group. The corollary now follows from Corollary 1.

Corollary 3. *Let $\wp(z)$ be the Weierstrass $\wp$-function with algebraic invariants g_2, g_3; let ω_1, ω_2 be its periods, $\operatorname{Im}(\omega_2/\omega_1) \neq 0$, and let η_1 be the quasi-period corresponding to ω_1. Then the numbers*

$$e^{2\pi i(\omega_2/\omega_1)}, \quad \frac{\omega_1}{\pi}, \quad \frac{\eta_1}{\pi}$$

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

In proving Corollary 3, without loss of generality we may assume that ω_1 and ω_2 are fundamental periods and $\operatorname{Im}(\omega_2/\omega_1) > 0$. Setting $q = e^{2\pi i(\omega_2/\omega_1)}$, $\omega = \omega_1$, and $\eta = \eta_1$, we have (see [1], Chapter 4)

$$P(q) = 3 \cdot \frac{\omega}{\pi} \cdot \frac{\eta}{\pi}, \qquad Q(q) = \frac{3}{4}\Big(\frac{\omega}{\pi}\Big)^4 g_2, \qquad R(q) = \frac{27}{8}\Big(\frac{\omega}{\pi}\Big)^6 g_3.$$

These formulae imply that all three numbers $P(q), Q(q), R(q)$ are algebraic over the field $\mathbb{Q}(\omega/\pi, \eta/\pi)$. By Theorem 1, $\mathbb{Q}(q, \omega/\pi, \eta/\pi)$ has transcendence degree 3.

Corollary 4. *Let $\wp(z)$ be the Weierstrass $\wp$-function with algebraic invariants g_2, g_3 and with complex multiplication by the field $\mathbb{k}$. If ω is any period of $\wp(z)$, η is the corresponding quasi-period, and τ is any element of $\mathbb{k}$ with $\operatorname{Im}\tau \neq 0$, then each of the sets*

$$\{\pi,\ \omega,\ e^{2\pi i\tau}\}, \qquad \{\omega,\ \eta,\ e^{2\pi i\tau}\}$$

is algebraically independent over $\mathbb{Q}$.

In fact, without loss of generality we may assume that ω is a primitive period, that is, it is not a multiple of any other period of $\wp(z)$. We may further assume that $\tau = \omega_2/\omega$, where $\omega_1 = \omega$ and ω_2 form a basis of the period lattice of $\wp(z)$. In the complex multiplication case the numbers ω_2 and η_2 are algebraic over $\mathbb{Q}(\omega, \eta)$ (see [5], Chapter 3). Using the Legendre relation, we then find that η is algebraic over $\mathbb{Q}(\omega, \pi)$ and π is algebraic over $\mathbb{Q}(\omega, \eta)$. Corollary 4 now follows from Corollary 3.

Corollary 5. *Each of the sets*

$$\{\pi,\ e^{\pi},\ \Gamma(1/4)\}, \qquad \{\pi,\ e^{\pi\sqrt{3}},\ \Gamma(1/3)\}$$

is algebraically independent over $\mathbb{Q}$. In particular, π and e^{π} are algebraically independent over $\mathbb{Q}$.

To prove this, we apply Corollary 4 to the elliptic curves with complex multiplication given by the equations

$$y^2 = 4x^3 - 4x, \qquad y^2 = 4x^3 - 4.$$

The first has complex multiplication field $\mathbb{Q}(i)$, while the second has complex multiplication field $\mathbb{Q}(\zeta)$, where $\zeta = e^{2\pi i/3}$. Their periods ω are, respectively,

$$\omega = 2\int_1^{\infty} \frac{dx}{(4x^3 - 4x)^{1/2}} = \frac{\Gamma(1/4)^2}{(8\pi)^{1/2}} \quad \text{and} \quad \omega = 2\int_1^{\infty} \frac{dx}{(4x^3 - 4)^{1/2}} = \frac{\Gamma(1/3)^3}{\pi \cdot 2^{8/3}}.$$

For any natural number D there exists a Weierstrass $\wp$-function with algebraic invariants and with complex multiplication field $\mathbb{Q}(\sqrt{-D})$. Thus, we obtain the following corollary.

Corollary 6. *For any natural number D the numbers*

$$\pi, \quad e^{\pi\sqrt{D}}$$

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

We now make some remarks of a historical nature.

The transcendence of $J(z)$ for algebraic q, $0 < |q| < 1$, was conjectured in 1969 by Mahler [6] and proved in 1995 by Barré-Sirieix, Diaz, Gramain, and Philibert [7]. Their paper provided the impetus for the research that led to the proof of our results.

The algebraic independence over $\mathbb{Q}$ of the numbers ω_1/π and η_1/π in Corollary 3 and the numbers π and ω in Corollary 4 was first proved by Chudnovskiĭ in 1976 (see [8] and [9]). As a consequence, in the same papers Chudnovskiĭ proved algebraic independence over $\mathbb{Q}$ of the numbers π and $\Gamma(1/4)$ and the numbers π and $\Gamma(1/3)$ (see Corollary 5). In 1977, Bertrand [10] showed that the first of these results of Chudnovskiĭ is equivalent to the statement that $\theta J(q)$ and $\theta^2 J(q)$ are algebraically independent over $\mathbb{Q}$, where $J(q)$ is an algebraic number not equal to 0 or 1728. In [10] he conjectured that $J(q), \theta J(q)$, and $\theta^2 J(q)$ are algebraically independent for any algebraic q with $0 < |q| < 1$. This conjecture is proved in Corollary 2.

The statement about algebraic independence of π and e^{π} (Corollary 5) is one of the oldest conjectures in the folklore of transcendental number theory. A reference to this conjecture in print can be found in [11].

The method of proof of Theorem 1 can also be used to obtain quantitative results.

Theorem 2. *Suppose that $q \in \mathbb{C}$, $0 < |q| < 1$, and $\theta_1, \theta_2, \theta_3 \in \mathbb{C}$ are such that the numbers $q, P(q), Q(q)$ and $R(q)$ are all algebraic over the field $\mathbb{Q}(\theta_1, \theta_2, \theta_3)$. Then there exists a constant γ_1 depending only on q and the θ_i such that the following inequality holds for any polynomial $A \in \mathbb{Z}[x_1, x_2, x_3]$, $A \not\equiv 0$:*

$$|A(\theta_1, \theta_2, \theta_3)| > \exp\bigl(-\gamma_1 t(A)^4 \ln^{24} t(A)\bigr),$$

where $t(A) = \ln H(A) + \deg A$ and $H(A)$ is the maximum modulus of the coefficients of A. In particular, this estimate holds for each of the sets

$$\pi, \ e^{\pi}, \ \Gamma(1/4) \quad \text{and} \quad \pi, \ e^{\pi\sqrt{3}}, \ \Gamma(1/3).$$

As we already noted, the functions $P(z), Q(z)$ and $R(z)$ are algebraically independent over $\mathbb{C}(z)$. The next theorem, which gives a bound for the measure of their algebraic independence, plays an important role in the proof of Theorem 1.

Theorem 3. *Let L_1 and L_2 be integers with $L_1 \geqslant 1$, $L_2 \geqslant 1$. Any polynomial $A(z, x_1, x_2, x_3) \in \mathbb{C}[z, x_1, x_2, x_3]$ with $A \not\equiv 0$, $\deg_z A \leqslant L_1$ and $\deg_{x_i} A \leqslant L_2$ satisfies the inequality*

$$\operatorname{ord} A\bigl(z, P(z), Q(z), R(z)\bigr) \leqslant c L_1 L_2^3,$$

where $c = 2 \cdot 10^{45}$.

Here and in the sequel the symbol $\operatorname{ord}\varphi(z)$ denotes the multiplicity of the zero of $\varphi(z)$ at the point $z = 0$.

We conclude this section by mentioning that analogues of Theorems 1 and 2 can be proved in the p-adic domain.

§ 2. Reduction of Theorems 1 and 2 to Theorem 3

Lemma 2.1. *For all sufficiently large integers N there exists a polynomial A in $\mathbb{Z}[z,x_1,x_2,x_3]$, $A \not\equiv 0$, such that*

$$\deg_z A \leqslant N, \qquad \deg_{x_i} A \leqslant N, \quad i=1,2,3, \qquad \ln H(A) \leqslant 85N\ln N,$$

where $H(A)$ is the maximum modulus of the coefficients of A, and the function

$$F(z) = A\bigl(z, P(z), Q(z), R(z)\bigr)$$

satisfies the equations

$$F^{(k)}(0) = 0, \qquad k = 0,1,\dots,\left[\frac{(N+1)^4}{2}\right] - 1.$$

Proof. For $k \geqslant 1$ we have

$$\sigma_k(n) = \sum_{d|n} d^k \leqslant n^k \sum_{d|n} 1 \leqslant n^{k+1}.$$

Actually, there is a more precise bound for $\sigma_k(n)$ (see [12]), but the trivial estimate is sufficient for our proof. We further have

$$1 + \sum_{n=1}^{\infty} n^k z^n \ll \sum_{n=0}^{\infty} (n+1)\cdots(n+k) z^n = \frac{k!}{(1-z)^{k+1}}, \tag{2}$$

where $\ll$ is the symbol for one function majorizing another; consequently,

$$P(z) \ll \frac{24\cdot 2!}{(1-z)^3}, \qquad Q(z) \ll \frac{240\cdot 4!}{(1-z)^5}, \qquad R(z) \ll \frac{504\cdot 6!}{(1-z)^7}, \qquad z \ll \frac{1}{1-z}.$$

For any vector $\overline{k} = (k_0,k_1,k_2,k_3)$, $k_i \in \mathbb{Z}$, $0 \leqslant k_i \leqslant N$, $i=0,1,2,3$, we have

$$z^{k_0} P(z)^{k_1} Q(z)^{k_2} R(z)^{k_3} = \sum_{n=0}^{\infty} d(\overline{k},n) z^n \ll \frac{c_1^{3N}}{(1-z)^{16N}}, \tag{3}$$

where $c_1 = 504\cdot 6!$ and $d(\overline{k},n) \in \mathbb{Z}$. From (3) and (2) it follows that

$$|d(\overline{k},n)| \leqslant c_1^{3N}(n+16N)^{16N} \leqslant (c_2 nN)^{16N} \leqslant (nN)^{17N}, \qquad n \geqslant 1, \tag{4}$$

if N is sufficiently large; and $|d(\overline{k},0)| \leqslant 1$.

Now let

$$A = \sum_{0\leqslant k_i\leqslant N} a(\overline{k}) z^{k_0} x_1^{k_1} x_2^{k_2} x_3^{k_3},$$

where the set of integers $a(\overline{k})$ is chosen to be a non-trivial solution of the system of homogeneous linear equations

$$\sum_{0\leqslant k_i\leqslant N} d(\overline{k},n)a(\overline{k})=0, \qquad n=0,1,\dots,\left[\frac{(N+1)^4}{2}\right]-1.$$

Here the number of variables $u=(N+1)^4$ and the number of equations $v=\left[(N+1)^4/2\right]$ satisfy the inequality $2v\leqslant u$. Hence, if we use (4) and Siegel's lemma on homogeneous systems of linear equations (see, for example, [11]), we see that the system has a non-trivial integer solution satisfying the inequality

$$\max_{\overline{k}}|a(\overline{k})|\leqslant (N+1)^4\left(\frac{(N+1)^4}{2}N\right)^{17N}\leqslant N^{85N}.$$

Lemma 2.1 is proved.

We introduce the notation

$$M=\operatorname{ord}F(z).$$

From Lemma 2.1 and Theorem 3 it follows that

$$\frac{1}{2}N^4\leqslant M\leqslant cN^4. \tag{5}$$

We further set $r=\min\bigl((1+|q|)/2,\ 2|q|\bigr)$. Then $|q|<r<1$.

Lemma 2.2. *If N is sufficiently large, then for all $z\in\mathbb{C}$ with $|z|\leqslant r$ we have*

$$|F(z)|\leqslant |z|^M N^{189N}.$$

Proof. Let $F(z)$ have the following Taylor expansion at the origin:

$$F(z)=\sum_{n=M}^{\infty} b_n z^n.$$

Then

$$b_n=\sum_{0\leqslant k_i\leqslant N} d(\overline{k},n)a(\overline{k})\in\mathbb{Z}$$

and, by (4),

$$|b_n|\leqslant \sum_{0\leqslant k_i\leqslant N}(nN)^{17N}N^{85N}\leqslant n^{17N}N^{103N}, \qquad n\geqslant M.$$

For $|z|\leqslant r$ we have

$$\begin{aligned}|F(z)| &\leqslant \sum_{n=M}^{\infty}|b_n|\cdot|z|^n=\sum_{n=0}^{\infty}|b_{n+M}|\cdot|z|^{n+M}\\ &\leqslant |z|^M N^{103N}\sum_{n=0}^{\infty}(n+M)^{17N}|z|^n\\ &\leqslant |z|^M N^{103N}(M+1)^{17N}\left(1+\sum_{n=1}^{\infty}n^{17N}|z|^n\right)\\ &\leqslant |z|^M N^{103N}(cN^4+1)^{17N}\frac{(17N)!}{(1-r)^{17N+1}}\leqslant |z|^M N^{189N}\end{aligned}$$

if N is sufficiently large. Lemma 2.2 is proved.

Lemma 2.3. *There exists an integer T, $0 \leqslant T \leqslant \gamma N \ln N$, for which*

$$|F^{(T)}(q)| > \left(\frac{1}{2}|q|\right)^{2M},$$

where $\gamma = 190\bigl(\ln |r/q|\bigr)^{-1}$.

Proof. Suppose that the following inequalities hold:

$$4^{L+1}|F^{(k)}(q)| \leqslant \left(\frac{1}{2}|q|\right)^{M}, \qquad 0 \leqslant k \leqslant L = [\gamma N \ln N]. \tag{6}$$

On the circle $C : |z| = r$ we have $z\overline{z} = r^2$ and

$$|r^2 - \overline{q}z| = |r^2 - \overline{q}z| \cdot \left|\frac{\overline{z}}{r}\right| = |r\overline{z} - r\overline{q}| = r|z - q|.$$

Using these relations and Lemma 2.2, we find that the integral

$$I = \frac{1}{2\pi i}\int_C \frac{F(z)}{z^{M+1}} \cdot \left(\frac{r^2 - \overline{q}z}{r(z-q)}\right)^{L+1} dz$$

can be bounded as follows:

$$|I| \leqslant N^{189N}. \tag{7}$$

Meanwhile,

$$I = \operatorname*{Res}_{z=0} G(z) + \operatorname*{Res}_{z=q} G(z), \tag{8}$$

where

$$G(z) = \frac{F(z)}{z^{M+1}} \cdot \left(\frac{r^2 - \overline{q}z}{r(z-q)}\right)^{L+1}.$$

The residues at 0 and q are computed to be

$$\operatorname*{Res}_{z=0} G(z) = b_M\left(-\frac{r}{q}\right)^{L+1}$$

and

$$\operatorname*{Res}_{z=q} G(z) = \frac{1}{L!}\left(\frac{d}{dz}\right)^{L}\left(F(z) \cdot \frac{(r^2 - \overline{q}z)^{L+1}}{z^{M+1}r^{L+1}}\right)\bigg|_{z=q} = \sum_{k=0}^{L} \frac{F^{(L-k)}(q)}{(L-k)!\,r^{L+1}} \cdot c_k, \tag{9}$$

where

$$c_k = \frac{1}{k!}\left(\frac{d}{dz}\right)^{k}\left(\frac{(r^2 - \overline{q}z)^{L+1}}{z^{M+1}}\right)\bigg|_{z=q} = \frac{1}{2\pi i}\int_{C_1} \frac{(r^2 - \overline{q}z)^{L+1}}{z^{M+1}(z-q)^{k+1}}\, dz$$

and C_1 is the circle $|z-q|=|q|/2$. Since on C_1 we have

$$|z| \geqslant |q| - |z-q| \geqslant \frac{1}{2}|q|,$$
$$|r^2 - \bar{q}z| = |r^2 - q\bar{q} + \bar{q}(q-z)| \leqslant r^2 - |q|^2 + \frac{1}{2}|q|^2 \leqslant r^2 \leqslant 2r|q|$$

and

$$\left|\frac{(r^2-\bar{q}z)^{L+1}}{(z-q)^{k+1}}\right| \leqslant (2r|q|)^{L+1}\Bigl(\frac{1}{2}|q|\Bigr)^{-k-1} \leqslant (4r)^{L+1},$$

it follows that

$$|c_k| \leqslant (4r)^{L+1}\Bigl(\frac{1}{2}|q|\Bigr)^{-M}, \qquad 0 \leqslant k \leqslant L.$$

The last inequality together with (6) and (9) gives us

$$\Bigl|\operatorname*{Res}_{z=q} G(z)\Bigr| \leqslant \sum_{k=0}^{L} \frac{1}{(L-k)!} \leqslant e.$$

Now since $b_M \in \mathbb{Z}$, from (8) and (7) we obtain

$$\left|\frac{r}{q}\right|^{L+1} \leqslant \left|b_M\Bigl(-\frac{r}{q}\Bigr)^{L+1}\right| = \Bigl|\operatorname*{Res}_{z=0} G(z)\Bigr| \leqslant |I| + \Bigl|\operatorname*{Res}_{z=q} G(z)\Bigr| \leqslant N^{189N} + e.$$

But this inequality is false for $N \geqslant 2$. This contradiction shows that there exists an integer $T \leqslant L$ for which

$$|F^{(T)}(q)| > 4^{-L-1}\Bigl(\frac{1}{2}|q|\Bigr)^{M} > \Bigl(\frac{1}{2}|q|\Bigr)^{2M}$$

if N is sufficiently large. Lemma 2.3 is proved.

Lemma 2.4. *There exists a sequence of polynomials*

$$A_N \in \mathbb{Z}[z, x_1, x_2, x_3], \qquad N \geqslant N_0,$$

such that

$$\deg A_N \leqslant 2\gamma N \ln N, \qquad \ln H(A_N) \leqslant 2\gamma N \ln^2 N, \tag{10}$$
$$\exp(-\varkappa_2 N^4) \leqslant \bigl|A_N\bigl(q, P(q), Q(q), R(q)\bigr)\bigr| \leqslant \exp(-\varkappa_1 N^4), \tag{11}$$

where

$$\varkappa_1 = \frac{1}{4}\ln\frac{1}{r}, \qquad \varkappa_2 = 3c\ln\frac{2}{|q|}$$

and c is the constant in Theorem 3.

Proof. Any polynomial $B \in \mathbb{C}[z, x_1, x_2, x_3]$ satisfies the identity

$$\frac{d}{dz}B\big(z, P(z), Q(z), R(z)\big) = z^{-1}DB\big(z, P(z), Q(z), R(z)\big), \tag{12}$$

where

$$D = z\frac{\partial}{\partial z} + \frac{1}{12}(x_1^2 - x_2)\frac{\partial}{\partial x_1} + \frac{1}{3}(x_1x_2 - x_3)\frac{\partial}{\partial x_2} + \frac{1}{2}(x_1x_3 - x_2^2)\frac{\partial}{\partial x_3} \tag{13}$$

is the operator corresponding to the system of differential equations (1). We now define the sequence of polynomial A_N (for N sufficiently large) by setting

$$A_N(z, x_1, x_2, x_3) = (12z)^T(z^{-1}D)^T A(z, x_1, x_2, x_3).$$

Here A is the polynomial that was constructed in Lemma 2.1 and T is the integer in Lemma 2.3. Using induction, it is easy to prove the identity

$$(z^{-1}D)^T = z^{-T}\prod_{k=0}^{T-1}(D-k), \qquad T \geqslant 1, \tag{14}$$

so that $A_N \in \mathbb{Z}[z, x_1, x_2, x_3]$. From (12) it follows that

$$A_N\big(z, P(z), Q(z), R(z)\big) = (12z)^T F^{(T)}(z).$$

Hence, Lemma 2.3 and (5) give the lower bound

$$\big|A_N\big(q, P(q), Q(q), R(q)\big)\big| \geqslant \Big(\frac{1}{2}|q|\Big)^{3M} \geqslant \exp(-\varkappa_2 N^4).$$

To obtain an upper bound we use the formula

$$F^{(T)}(q) = \frac{T!}{2\pi i}\int_{C_2}\frac{F(z)}{(z-q)^{T+1}}\,dz,$$

where C_2 is the circle $|z - q| = r - |q|$. Using the inequality

$$|z| \leqslant |z-q| + |q| = r,$$

along with (5), Lemma 2.2 and Lemma 2.3, we conclude that

$$\big|A_N\big(q, P(q), Q(q), R(q)\big)\big| \leqslant 12^T \cdot T! \cdot (r - |q|)^{-T} r^M \cdot N^{189N} \leqslant \exp(-\varkappa_1 N^4).$$

This proves (11).

To prove (10) we use (14). If $B \in \mathbb{C}[z, x_1, x_2, x_3]$ and $B \ll H(1+z+x_1+x_2+x_3)^S$, then for any integer k we have

$$\begin{aligned}(D+k)B &\ll |k|H(1+z+x_1+x_2+x_3)^S + HS(1+z+x_1+x_2+x_3)^{S-1}\\ &\qquad \times \big(z + (x_1^2+x_2) + (x_1x_2+x_3) + (x_1x_3+x_2^2)\big)\\ &\ll |k|H(1+z+x_1+x_2+x_3)^S + HS(1+z+x_1+x_2+x_3)^{S+1}\\ &\ll H(S+|k|)(1+z+x_1+x_2+x_3)^{S+1}.\end{aligned}$$

Hence,

$$12^T \prod_{k=0}^{T-1} (D-k)B(z,x_1,x_2,x_3) \ll 12^T H(S+2T)^T(1+z+x_1+x_2+x_3)^{S+T}$$

and, since

$$A \ll N^{85N}(1+z+x_1+x_2+x_3)^{4N},$$

we find that

$$A_N(z,x_1,x_2,x_3) \ll N^{85N}(48N+24T)^T(1+z+x_1+x_2+x_3)^{4N+T}.$$

But this means that

$$\deg A_N \leqslant 4N+T \leqslant 2\gamma N \ln N,$$
$$H(A_N) \leqslant N^{85N}(48N+24T)^T \cdot 5^{4N} \leqslant \exp(2\gamma N \ln^2 N),$$

and we have proved (10). Lemma 2.4 is proved.

Lemma 2.5. *Let $\overline{\omega} = (\omega_1, \dots, \omega_m) \in \mathbb{C}^m$. Suppose that there exists a sequence of polynomials $A_N \in \mathbb{Z}[x_1, \dots, x_m]$ such that*

$$\deg A_N \leqslant \sigma(N), \qquad \ln H(A_N) \leqslant \sigma(N)$$

and

$$\exp\bigl(-\varkappa_2 \lambda(N)\bigr) \leqslant |A_N(\overline{\omega})| \leqslant \exp\bigl(-\varkappa_1 \lambda(N)\bigr),$$

where $\varkappa_2 > \varkappa_1 > 0$ are constants, and $\sigma(N)$ and $\lambda(N)$ are functions that approach infinity as N increases and satisfy the conditions

$$\lim_{N\to\infty} \frac{\sigma(N+1)}{\sigma(N)} = 1 \quad \text{and} \quad \lim_{N\to\infty} \frac{\lambda(N)}{\sigma(N)^{k+1}} = \infty$$

for some integer k. Then

$$\operatorname{tr}\deg_{\mathbb{Q}} \mathbb{Q}(\omega_1, \dots, \omega_m) \geqslant k+1.$$

Proof. This lemma is an easy consequence of Theorem 2.11 of Philippon [13], in which we take $\delta(N) = \sigma(N)$, $S(N) = \varkappa_1 \lambda(N)$, $R(N) = 2\varkappa_2 \lambda(N)$ and the sequence of principal ideals I_N is taken to be (A_N).

Theorem 1 now follows from Lemmas 2.4 and 2.5 with $m = 4$, $k = 2$, $\sigma(N) = 2\gamma N \ln^2 N$, $\lambda(N) = N^4$, $\varkappa_1$ and $\varkappa_2$ as in Lemma 2.4, and $\overline{\omega} = \bigl(q, P(q), Q(q), R(q)\bigr)$.

To prove Theorem 2, instead of Lemma 2.5 we use a criterion of Ably [14]. In the notation of his paper we take $n = 4$, $k = 2$, $u(x) = \gamma_2 x \ln^{-8} x$ with a sufficiently small constant γ_2 and c_0 equal to a sufficiently large constant. For example, we can set $\gamma_2 = \varkappa_1 (3\gamma)^{-4}$ and $c_0 = 6^4 \varkappa_2 / \varkappa_1$. We further take a sequence of principal ideals $I_N = (G_N)$, where $G_N = A_S$ and S is the largest integer for which $2\gamma S \ln^2 S \leqslant N$. Then the criterion in [14] implies the following result.

Theorem 4. *Let $q \in \mathbb{C}$, $0 < |q| < 1$, and $\overline{\omega} = \big(1, q, P(q), Q(q), R(q)\big) \in \mathbb{C}^5$. There exists a positive constant γ_3 depending only on q such that the following inequality holds for any unmixed homogeneous ideal $I \subset \mathbb{Z}[x_0, \dots, x_4]$ with $h(I) = 2$ and $I \cap \mathbb{Z} = (0)$:*

$$|I(\overline{\omega})| \geqslant \exp\big(-\gamma_3 t(I)^4 \ln^{24} t(I)\big).$$

See [15] for the definitions of $h(I), t(I)$, and $|I(\overline{\omega})|$. In § 3 below we give analogous definitions for the polynomial ring $\mathbb{C}[z, x_0, \dots, x_m]$.

Remark. In an entirely similar way one can use Lemma 2.4 and Ably's criterion to prove a bound for $|I(\overline{\omega})|$ for ideals with $h(I) = 3$. The resulting inequality has the form

$$|I(\overline{\omega})| \geqslant \exp\big(-\gamma_4 t(I)^2 \ln^{8} t(I)\big).$$

We now show how to derive Theorem 2 from Theorem 4. Under the conditions in Theorem 2 we have

$$\operatorname{tr} \deg_{\mathbb{Q}} \mathbb{Q}\big(q, P(q), Q(q), R(q)\big) = 3.$$

We first consider the case when the numbers $\theta_1, \theta_2, \theta_3$ are a subset of $q, P(q), Q(q), R(q)$. Let $E \in \mathbb{Z}[x_0, \dots, x_4]$ be an irreducible homogeneous polynomial with $E(\overline{\omega}) = 0$, and let B be the homogeneous polynomial defined by setting $B = x_0^{\deg A} A(x_1/x_0, \dots, x_4/x_0)$. Applying Proposition 1 of [15] to the prime ideal $\mathfrak{p} = (E)$, we find that $|\mathfrak{p}(\overline{\omega})| = 0$. If we now use Theorem 4 and Proposition 3 of [15], then we obtain

$$|\overline{\omega}|^{-\deg B} |B(\overline{\omega})| \geqslant \exp\big(-96 t(E) t(B) - \gamma_3 T_1^4 \ln^{24} T_1\big),$$

where $T_1 \leqslant 32 t(\mathfrak{p}) t(B)$. Since $t(B) = t(A)$, this gives us the inequality in Theorem 2.

We now consider the general case when the numbers $q, P(q), Q(q)$ and $R(q)$ are algebraic over $\mathbb{Q}(\theta_1, \theta_2, \theta_3)$. Among these four numbers exactly three are algebraically independent over $\mathbb{Q}$; let us denote them $\omega_1, \omega_2, \omega_3$. Then all of the θ_i are algebraic over $\mathbb{Q}(\omega_1, \omega_2, \omega_3)$. If $C \in \mathbb{Z}[x_1, x_2, x_3]$ is such that $\xi = C(\omega_1, \omega_2, \omega_3)$ has the property that all of the $\xi\theta_i$ are integral over the ring $\mathbb{Z}[\omega_1, \omega_2, \omega_3]$, then, computing the norm of $\xi^{3 \deg A} A(\theta_1, \theta_2, \theta_3)$ over the field $\mathbb{Q}(\omega_1, \omega_2, \omega_3)$, we obtain a polynomial A_1 in $\omega_1, \omega_2, \omega_3$ with integer coefficients. If the inequality proved above is applied to this polynomial, then we find that

$$\big|\operatorname{Norm}\big(\xi^{3 \deg A} A(\theta_1, \theta_2, \theta_3)\big)\big| = |A_1(\omega_1, \omega_2, \omega_3)| \geqslant \exp\big(-\gamma_4 t(A_1)^4 \ln^{24} t(A_1)\big),$$

from which (just as in the proof of Liouville's theorem) we easily derive the required lower bound for $|A(\theta_1, \theta_2, \theta_3)|$. This completes the proof of Theorem 4.

§ 3. Theorem 5 and the derivation of Theorem 3 from Theorem 5

The proof of Theorem 3 is based on a method that uses ideas of commutative algebra and elimination theory. In [16] this method was used to prove a similar result for $m \geqslant 1$ functions that form a solution of an algebraic system of differential equations with constant coefficients; and in [17] it was used for $m \geqslant 1$ functions that satisfy linear differential equations with coefficients in $\mathbb{C}(z)$. We shall apply the general lemmas proved in those papers to the case of the polynomial ring $\mathcal{A} = \mathbb{C}[z, x_0, x_1, x_2, x_3]$ $(m = 3)$. We shall also use lemmas from [18] and [19]. Our notation and definitions will be compatible with those in [15] and [19]; in each case we shall give the appropriate reference.

We consider an unmixed ideal I of $\mathcal{A}$ that is homogeneous in the x_i and has the property that $r = 4 - h(I) \geqslant 1$. As in [16] and [17], $h(I)$ denotes the height of the ideal I. In § 1 of [18] the ideal I was associated with a certain principal ideal $\overline{I}(r)$ of the ring $\mathbb{C}[z, \overline{u}_1, \ldots, \overline{u}_r]$, where $\overline{u}_i$ is the set of variables $u_{i0}, \ldots, u_{i3}$. Let F be a generator of $\overline{I}(r)$ (the associated form of the ideal I); it is defined up to a factor in $\mathbb{C}$. We set

$$N(I) = \deg_{\overline{u}_1} F, \qquad B(I) = \deg_z F.$$

For each element φ of the field $\mathbb{C}\big((z)\big)$ of formal power series with complex coefficients, we let $\operatorname{ord}\varphi$ denote the exponent of the first power of z with non-zero coefficient. We let $\mathcal{K}$ denote the algebraic closure of $\mathbb{C}\big((z)\big)$. The function ord extends uniquely to $\mathcal{K}$ and maps that field to the set $\mathbb{Q} \cup \{\infty\}$.

For $\overline{\varphi} = (\varphi_0, \ldots, \varphi_3) \in \mathcal{K}^4$ we set $|\overline{\varphi}| = \min_j(\operatorname{ord}\varphi_j)$.

We now define $\operatorname{ord} I(\overline{\varphi})$; it will play a role similar to $\operatorname{ord} P(\varphi)$ for $P \in \mathcal{A}$. As in § 1 of [18], we consider r skew-symmetric matrices $S^{(i)} = \|s_{jk}^{(i)}\|$, where i, j, k vary in the range $1 \leqslant i \leqslant r$, $0 \leqslant j \leqslant 3$, $0 \leqslant k \leqslant 3$. We suppose that, except for the skew-symmetry relation $s_{jk}^{(i)} + s_{kj}^{(i)} = 0$, there is no other algebraic relation over $\mathcal{A}$ among the $s_{jk}^{(i)}$. Given a polynomial $E \in \mathcal{K}[\overline{u}_1, \ldots, \overline{u}_r]$ and a vector $\overline{\varphi} = (\varphi_0, \ldots, \varphi_3) \in \mathcal{K}^4$ we let $\varkappa(E)$ denote the polynomial in $s_{jk}^{(i)}$, $0 \leqslant j < k \leqslant 3$, $1 \leqslant i \leqslant r$, with coefficients in $\mathcal{K}$ that is obtained by substituting the vector $S^{(i)}\overline{\varphi}$ in place of the variable $\overline{u}_i = (u_{i0}, \ldots, u_{i3})$ in E for $i = 1, \ldots, r$. The map $\varkappa$ is clearly a homomorphism from the ring $\mathcal{K}[\overline{u}_1, \ldots, \overline{u}_r]$ to the polynomial ring $\mathcal{K}[s_{jk}^{(i)}, \ 0 \leqslant j < k \leqslant 3, \ 1 \leqslant i \leqslant r]$. We now define $\operatorname{ord}\varkappa(E)$ to be the smallest value that ord takes on the coefficients of the polynomial $\varkappa(E)$.

We set

$$\operatorname{ord} I(\overline{\varphi}) = \operatorname{ord}\varkappa(F) - rN(I)|\overline{\varphi}|,$$

where F is the associated form of the ideal I.

Theorem 5. *Let I be an unmixed ideal of $\mathcal{A}$ that is homogeneous in the variables $x_0, \ldots, x_3$ and satisfies $I \cap \mathbb{C}[z] = (0)$ and $r = 4 - h(I) \geqslant 1$. Then*

$$\operatorname{ord} I(\overline{f}) \leqslant \rho^{2r-1}\big(B(I)N(I)^{r/(4-r)} + N(I)^{3/(4-r)}\big),$$

where $\overline{f} = \big(1, P(z), Q(z), R(z)\big)$ and $\rho = 10^9$.

Theorem 5 is proved by induction on r as r goes from 1 to 3.

Theorem 3 can easily be derived from Theorem 5 using the following lemma.

Lemma 3.1. *Suppose that the polynomial $C \in \mathcal{A}$ is homogeneous in the variables x_i and $I = (C)$ is the corresponding principal ideal of $\mathcal{A}$. Then $N(I) = \deg_{\overline{x}} C$, $B(I) = \deg_z C$, and for every $\overline{\varphi} \in \mathcal{K}^4$ one has*

$$\operatorname{ord} C(\overline{\varphi}) \leqslant \operatorname{ord} I(\overline{\varphi}) + |\overline{\varphi}| \deg_{\overline{x}} C.$$

Proof. See [17], Proposition 1.

Now let A be the polynomial in Theorem 3, and set

$$C = x_0^{\deg A} A\left(z, \frac{x_1}{x_0}, \frac{x_2}{x_0}, \frac{x_3}{x_0}\right),$$

where $\deg A$ is the total degree of A in the x_i and $I = (C)$ is the corresponding principal ideal of $\mathcal{A}$. Since $h(I) = 1$, we see that Theorem 3 follows easily from Lemma 3.1 and Theorem 5 with $r = 3$. According to Lemma 3.1, we have $B(I) \leqslant L_1$, $N(I) \leqslant L_2$, and

$$\operatorname{ord} A\big(z, P(z), Q(z), R(z)\big) \leqslant \operatorname{ord} I(\overline{f}) \leqslant \rho^5 (L_1 + 1) L_2^3 \leqslant c L_1 L_2^3.$$

This completes the derivation of Theorem 3 from Theorem 5.

§ 4. Ideals invariant with respect to the operator D

In § 2 (see (13)) we defined the differential operator D acting on the ring $\mathfrak{R} = \mathbb{C}[z, x_1, x_2, x_3]$. Recall that for any $G(z, x_1, x_2, x_3)$ in this ring we have the identity

$$\theta G\big(z, P(z), Q(z), R(z)\big) = DG\big(z, P(z), Q(z), R(z)\big). \tag{15}$$

If an ideal I of the ring $\mathfrak{R}$ or $\mathbb{C}[x_1, x_2, x_3]$ has the property that $DI \subset I$, then we say that I is *D-invariant*.

Lemma 4.1. *There exist only two D-invariant principal prime ideals of $\mathfrak{R}$, namely, the ideals generated by z and by $\Delta = x_2^3 - x_3^2$.*

Proof. We have $Dz = z$ and

$$D\Delta = x_2^2(x_1 x_2 - x_3) - x_3(x_1 x_3 - x_2^2) = x_1 \Delta.$$

Thus, the principal ideal generated by z or by Δ is D-invariant.

Now suppose that $A \in \mathfrak{R}$ is any irreducible polynomial with the property that $A \mid DA$. In other words, we have $DA = BA$ for some $B \in \mathfrak{R}$. Given a polynomial $F(z, x_1, x_2, x_3) \in \mathfrak{R}$, we define its weight $\omega(F)$ as follows:

$$\omega(F) = \deg_t F(z, t x_1, t^2 x_2, t^3 x_3).$$

Then

(1) if all monomials of F have the same weight, then either $DF = 0$ or else $\omega(DF) \geqslant \omega(F)$;
(2) $\omega(DF) \leqslant \omega(F) + 1$ for any $F \in \mathfrak{R}$;
(3) $\omega(FG) = \omega(F) + \omega(G)$ for any two polynomials $F, G \in \mathfrak{R}$.

These properties follow trivially from the definition of the weight and the definition of D. Using (2) and (3) we find that the relation $DA = BA$ implies that

$$\omega(B) + \omega(A) = \omega(DA) \leqslant \omega(A) + 1,$$

so that $\omega(B) \leqslant 1$. This inequality means that

$$DA = (ax_1 + b)A, \tag{16}$$

where $a, b \in \mathbb{C}[z]$. If we compare the degrees in z of the polynomials in (16), we conclude that $a, b \in \mathbb{C}$.

Let C denote the sum of the monomials of A that have minimal weight. If we compare the sum of the monomials of weight $\omega(C)$ on both sides of (16) and use property (1), then we find that

$$z\frac{\partial C}{\partial z} = bC.$$

In this equality we compare the coefficients of the highest power of z in $C \in \mathfrak{R}$; we conclude that $b \in \mathbb{Z}$.

Now let

$$A\bigl(z, P(z), Q(z), R(z)\bigr) = c_m z^m + c_{m+1} z^{m+1} + \cdots, \quad c_m \neq 0, \qquad m \geqslant 0.$$

If we apply the operator θ to both sides of this equation and use (15), (16) and the definition of $P(z)$, we find that

$$mc_m z^m + \cdots = \bigl(a(1 - 24z + \cdots) + b\bigr)(c_m z^m + \cdots),$$

and hence $a + b = m$. We have thereby shown that a and b are integers.

The differential operator D can be extended in a natural way to the field $\mathbb{C}(z, x_1, x_2, x_3)$. It is easy to verify that the identify (15) remains valid for any element F of this field. By (15), the relation $DF = 0$ for $F \in \mathbb{C}(z, x_1, x_2, x_3)$ means that

$$\theta F\bigl(z, P(z), Q(z), R(z)\bigr) = 0,$$

and hence $F\bigl(z, P(z), Q(z), R(z)\bigr) = c \in \mathbb{C}$. But since the functions P, Q and R are algebraically independent over $\mathbb{C}(z)$, this implies that $F = c \in \mathbb{C}$; thus, the field of constants of the operator D in $\mathbb{C}(z, x_1, x_2, x_3)$ is simply $\mathbb{C}$.

We easily verify that

$$D(\Delta^{-a} z^{-b}) = -(ax_1 + b)\Delta^{-a} z^{-b},$$

and so, using (16), we obtain

$$D(A \cdot \Delta^{-a} z^{-b}) = 0,$$

that is, by what was just proved, we have $A \cdot \Delta^{-a} z^{-b} = c$ and $A = c\Delta^a z^b$ for some constant $c \in \mathbb{C}$. Since A is an irreducible polynomial, only two cases are possible: $a = 1, b = 0$, and $a = 0, b = 1$. This completes the proof of Lemma 4.1.

Remark. What we have actually proved is that every D-invariant principal ideal of $\mathfrak{R}$ has the form $(\Delta^a z^b)$, where a and b are non-negative integers.

We next determine all D-invariant prime ideals of the ring $\mathbb{C}[x_1, x_2, x_3]$.

Corollary. *There is one and only one D-invariant principal prime ideal in $\mathbb{C}[x_1, x_2, x_3]$. It is generated by Δ.*

In fact, if A is an irreducible polynomial that generates a D-invariant principal prime ideal in $\mathbb{C}[x_1, x_2, x_3]$, then the principal ideal of $\mathfrak{R}$ generated by A is also a D-invariant prime ideal. Lemma 4.1 then implies that $A = \Delta$.

Lemma 4.2. *All of the D-invariant prime ideals of $\mathbb{C}[x_1, x_2, x_3]$ of dimension 0 have the form $(x_1 - c, x_2 - c^2, x_3 - c^3)$, where $c \in \mathbb{C}$.*

Proof. Every prime ideal $\mathfrak{p}$ of $\mathbb{C}[x_1, x_2, x_3]$ of dimension 0 has the form $(x_1 - c_1, x_2 - c_2, x_3 - c_3)$ with $c_i \in \mathbb{C}$. Suppose that $D\mathfrak{p} \subset \mathfrak{p}$. Applying the operator D to the polynomials $x_1 - c_1$, we find that the three polynomials

$$x_1^2 - x_2, \quad x_1x_2 - x_3, \quad x_1x_3 - x_2^2 \tag{17}$$

belong to $\mathfrak{p}$. Since they all must vanish at the point (c_1, c_2, c_3), we conclude that $c_2 = c_1^2$ and $c_3 = c_1c_2 = c_1^3$, that is, $\mathfrak{p} = (x_1 - c, x_2 - c^2, x_3 - c^3)$ with $c = c_1$. Conversely, every ideal of the form $\mathfrak{p} = (x_1 - c, x_2 - c^2, x_3 - c^3)$ contains the polynomials (17) and hence is D-invariant.

Lemma 4.3. *The system of differential equations*

$$\begin{aligned}(x^2 - f)f' &= 4(xf - g),\\ (x^2 - f)g' &= 6(xg - f^2)\end{aligned} \tag{18}$$

has a unique solution in algebraic functions $f(x)$, $g(x)$ with $f(1) = 1$, $g(1) = 1$, namely, $f = x^2$, $g = x^3$.

Proof. The functions $f = x^2$, $g = x^3$ form a solution of the system (18). Hence, in what follows we may suppose that $f \not\equiv x^2$. We set $u = x^2 - f \not\equiv 0$, $v = xf - g$. Then

$$xg - f^2 = x^2u - u^2 - xv$$

and

$$uu' = 2ux - uf' = 2ux - 4v,$$

$$uv' = uf + 4xv - 6x^2u + 6u^2 + 6xv = 5u^2 - 5x^2u + 10xv = 5u^2 - \frac{5}{2}xuu'.$$

We obtain the system of differential equations

$$\begin{aligned}uu' &= 2xu - 4v,\\ 2v' &= 10u - 5xu'.\end{aligned} \tag{19}$$

Since $u(x)$ and $v(x)$ are algebraic functions, there exists a natural number e and a parametrization (here we are considering parametrizations of branches at $x = 1$; recall that $u(1) = v(1) = 0$)

$$x = 1 + t^e, \qquad u = \sum_{k=\lambda}^{\infty} a_k t^k, \qquad v = \sum_{k=\mu}^{\infty} b_k t^k,$$

where $\lambda \geqslant 1$, $\mu \geqslant 1$, and $a_\lambda b_\mu \neq 0$. We may assume that e has been chosen to be as small as possible.

The expansions of the functions in (19) have the following initial terms:

$$xu = a_\lambda t^\lambda + \cdots, \qquad xu' = \frac{\lambda}{e} a_\lambda t^{\lambda-e} + \cdots,$$
$$uu' = \frac{\lambda}{e} a_\lambda^2 t^{2\lambda-e} + \cdots, \qquad v' = \frac{\mu}{e} b_\mu t^{\mu-e} + \cdots.$$

If we substitute these expansions into the second equation in (19), then we obtain

$$2\frac{\mu}{e} b_\mu t^{\mu-e} + \cdots = 10 a_\lambda t^\lambda + \cdots - 5\frac{\lambda}{e} a_\lambda t^{\lambda-e} + \cdots. \tag{20}$$

Comparing exponents of the smallest powers of t on the left and right, we conclude that $\lambda = \mu$. If we now substitute these expansions into the first equation in (19), then we obtain

$$\frac{\lambda}{e} a_\lambda^2 t^{2\lambda-e} + \cdots = 2a_\lambda t^\lambda + \cdots - 4b_\lambda t^\lambda - \cdots. \tag{21}$$

This implies that the inequality $2\lambda - e \geqslant \lambda$ must hold, and hence $\lambda \geqslant e$.

We next compare the coefficients of $t^{\lambda-e}$ on the left and right in (20). We obtain:

$$2b_\lambda = -5a_\lambda. \tag{22}$$

If $\lambda > e$, then a comparison of the coefficients of t^λ in (21) gives

$$2a_\lambda - 4b_\lambda = 0,$$

which, combined with (22), contradicts the assumption that $a_\lambda \neq 0$. Hence $\lambda = e$, and from (21) we find that

$$a_e^2 = 2a_e - 4b_e.$$

By (22), this means that $a_e^2 = 12a_e$. Since $a_e \neq 0$, we conclude that $a_e = 12$ and $b_e = -30$.

Now suppose that $e \geqslant 2$. Let r be the smallest number for which the conditions $a_r \neq 0$ and $r \not\equiv 0 \pmod e$ hold. This number exists because e was chosen to be minimal (otherwise, the first equation in (19) would imply that all of the non-zero coefficients b_k have index divisible by e). If we now compare the coefficients of t^r on the left and right of the first equation in (19), then we find that

$$\frac{r+e}{e} a_r a_e = 2a_r - 4b_r$$

or, since $a_e = 12$,

$$12\frac{r+e}{e} a_r = 2a_r - 4b_r. \tag{23}$$

By making the same substitution in the second equation in (19) and comparing the coefficients of t^{r-e}, we find that

$$2\frac{r}{e}b_r = -5\frac{r}{e}a_r$$

or

$$2b_r + 5a_r = 0.$$

The last equation along with (23) give us $ra_r = 0$; since $r > e$, this means that $a_r = 0$, which is impossible. Thus, $e = 1$, the functions $u(x)$ and $v(x)$ are single-valued in a neighbourhood of the point $x = 1$, and

$$u(1) = v(1) = 0, \qquad u'(1) = 12, \quad v'(1) = -30. \tag{24}$$

We now prove that all the derivatives of $u(x)$ and $v(x)$ are uniquely determined, that is, there exists a unique solution of the system of differential equations (19) that is analytic in a neighbourhood of $x = 1$ and satisfies the conditions in (24). Let $k \geqslant 2$. If we differentiate the first equation in (19) k times, then we find that the function

$$uu^{(k+1)} + (k+1)u'u^{(k)} - 2xu^{(k)} + 4v^{(k)}$$

can be expressed as a polynomial in x and $u, u', \ldots, u^{(k-1)}$. Taking (24) into account, we then find that the quantity

$$(6k+5)u^{(k)}(1) + 2v^{(k)}(1)$$

is uniquely determined by $u(1), u'(1), \ldots, u^{(k-1)}(1)$. In exactly the same way, if we differentiate the second equation in (19) $k-1$ times, we find that the quantity

$$5u^{(k)}(1) + 2v^{(k)}(1)$$

can be expressed uniquely in terms of $u^{(j)}(1)$ and $v^{(j)}(1)$, $0 \leqslant j \leqslant k-1$. But then the derivatives $u^{(k)}(1)$ and $v^{(k)}(1)$ are also uniquely determined. This proves uniqueness of a solution to (19) that is analytic in a neighbourhood of $x = 1$ and satisfies initial conditions (24).

In some neighbourhood of the point $x = 1$ the equation $x = P(z)$ determines z uniquely as an analytic function of x that vanishes at $x = 1$. We set

$$F(x) = Q\big(P^{-1}(x)\big), \qquad G(x) = R\big(P^{-1}(x)\big).$$

Then $F(x)$ and $G(x)$ are analytic functions in a neighbourhood of $x = 1$ that, as we easily verify, satisfy the system of differential equations (18) and the initial conditions $F(1) = 1$, $G(1) = 1$. In addition,

$$z = -\frac{1}{24}(x-1) + \cdots, \quad F(x) = 1 - 10(x-1) + \cdots, \quad G(x) = 1 + 21(x-1) + \cdots.$$

But then it is easy to see that the functions $U(x) = x^2 - F(x)$ and $V(x) = xF(x) - G(x)$ satisfy the system of differential equations (19) and the initial conditions (24). By the uniqueness proved above, we conclude that $u(x) = U(x)$, $v(x) = V(x)$, and hence $f(x) = F(x)$, $g(x) = G(x)$. Thus, $F(x)$ and $G(x)$ are algebraic functions. But if we substitute $x = P(z)$ into the identity $A\big(x, F(x)\big) = 0$, $A(x,y) \in \mathbb{C}[x,y]$, then it becomes an algebraic relation $A\big(P(z), Q(z)\big) = 0$ between the functions $P(z)$ and $Q(z)$. Since $P(z)$, $Q(z)$ and $R(z)$ are algebraically independent over $\mathbb{C}(z)$, such an algebraic relation is impossible. This contradiction completes the proof of Lemma 4.3.

Proposition 1. *All non-trivial D-invariant prime ideals of* $\mathbb{C}[x_1, x_2, x_3]$ *having a zero at the point* $(1, 1, 1)$ *are given by the following list:*

(1) $(x_1 - 1, x_2 - 1, x_3 - 1)$;
(2) $(x_1^2 - x_2, x_1^3 - x_3)$;
(3) $(x_2^3 - x_3^2)$.

They all contain the polynomial $\Delta = x_2^3 - x_3^2$.

Proof. Let $\mathfrak{p}$ be a D-invariant prime ideal of $\mathbb{C}[x_1, x_2, x_3]$. If $\dim \mathfrak{p} = 0$, then $\mathfrak{p}$ has the form in (1), by Lemma 4.2 (in this case $c = 1$, by assumption).

If $\dim \mathfrak{p} = 2$, that is, if $\mathfrak{p}$ is a principal ideal, then its extension $\mathfrak{p}^e$ to $\mathfrak{R}$ is also a D-invariant principal prime ideal. Since $z \notin \mathfrak{p}^e$, it follows from Lemma 4.1 that $\mathfrak{p}^e = (\Delta)$. But then $\mathfrak{p} = (\Delta)$, that is, we have case (3).

Now suppose that $\dim \mathfrak{p} = 1$. If $\mathfrak{p} \cap \mathbb{C}[x_1] \neq (0)$, then, since the ideal $\mathfrak{p}$ is prime, we have $x_1 - c \in \mathfrak{p}$ for some constant c. But then $x_1^2 - x_2 = 12D(x_1 - c) \in \mathfrak{p}$, and so $x_2 - c^2 \in \mathfrak{p}$. Also, $x_1 x_2 - x_3 = 3D(x_2 - c^2) \in \mathfrak{p}$ and $x_3 - c^3 \in \mathfrak{p}$. However, the inclusion $(x_1 - c, x_2 - c^2, x_3 - c^3) \subset \mathfrak{p}$ is impossible, since $\dim \mathfrak{p} = 1$. Thus, $\mathfrak{p} \cap \mathbb{C}[x_1] = (0)$; hence, $\mathfrak{p} \cap \mathbb{C}[x_1, x_2] \neq (0)$ and $\mathfrak{p} \cap \mathbb{C}[x_1, x_3] \neq (0)$. Let $A(x_1, x_2)$ and $B(x_1, x_3)$ denote irreducible polynomials of $\mathbb{C}[x_1, x_2, x_3]$ that lie in $\mathfrak{p}$. By assumption, we have $A(1,1) = B(1,1) = 0$; hence, there exist algebraic functions $y = y(x)$, $z = z(x)$ such that

$$A\big(x, y(x)\big) = 0, \quad B\big(x, z(x)\big) = 0, \qquad y(1) = z(1) = 1, \tag{25}$$

and the triple of functions $\big(x, y(x), z(x)\big)$ is a zero of the ideal $\mathfrak{p}$. If we differentiate the first equation in (25) with respect to x, then we obtain

$$\frac{\partial A}{\partial x}\big(x, y(x)\big) + \frac{\partial A}{\partial y}\big(x, y(x)\big) y'(x) = 0. \tag{26}$$

If we then take into account that the triple $\big(x, y(x), z(x)\big)$ is a zero of the ideal $\mathfrak{p}$ and, in particular, of the polynomial $DA \in \mathfrak{p}$, then we conclude that

$$\frac{1}{12}\big(x^2 - y(x)\big)\frac{\partial A}{\partial x}\big(x, y(x)\big) + \frac{1}{3}\big(xy(x) - z(x)\big)\frac{\partial A}{\partial y}\big(x, y(x)\big) = 0. \tag{27}$$

Multiplying (26) by $\frac{1}{12}\big(x^2 - y(x)\big)$, subtracting the resulting expression from (27), and using the fact that

$$\frac{\partial A}{\partial y}\big(x, y(x)\big) \not\equiv 0,$$

we find that the functions $y(x), z(x)$ satisfy the first differential equation in (18). Similarly, if we differentiate the second equation in (25), then we find that $y(x), z(x)$ also satisfy the second differential equation in (18). By Lemma 4.3, we now know that $y(x) = x^2$ and $z(x) = x^3$, that is, $A(x_1, x_2) = x_1^2 - x_2$, $B(x_1, x_3) = x_1^3 - x_3$. This means that $\mathfrak{p}$ contains the prime ideal in part (2) of Proposition 1. Since these two ideals have the same dimension, we conclude that they are the same ideal. Proposition 1 is proved.

Proposition 2. *Every D-invariant prime ideal of $\mathbb{C}[z, x_1, x_2, x_3]$ with a zero at $(0,1,1,1)$ contains either the polynomial z, or else the polynomial $\Delta = x_2^3 - x_3^2$.*

Proof. If $\mathfrak{p}$ is a D-invariant prime ideal of $\mathfrak{R}$, then $\mathfrak{q} = \mathfrak{p} \cap \mathbb{C}[x_1, x_2, x_3]$ is a D-invariant prime ideal of $\mathbb{C}[x_1, x_2, x_3]$. If $\mathfrak{q} \neq (0)$, then, by Proposition 1, we have $\Delta \in \mathfrak{q} \subset \mathfrak{p}$. If $\mathfrak{q} = (0)$, then $\mathfrak{p}$ is a principal ideal, in which case, by Lemma 4.1, $z \in \mathfrak{p}$. Proposition 2 is proved.

§ 5. Auxiliary lemmas

The proof of the next lemma can be found in [17]; it is part of the proof of Theorem 2 of that paper (see pp. 44–45, and also [16], pp. 267–268). For convenience we shall give the proof of Lemma 5.1 in the general case when $\mathcal{A} = \mathbb{C}[z, x_0, \dots, x_m]$ with $m \geqslant 1$. We shall say that an ideal of $\mathcal{A}$ is *homogeneous* if it is homogeneous in the variables $x_0, \dots, x_m$.

Lemma 5.1. *Let $\mathfrak{p}$ be a homogeneous prime ideal in $\mathcal{A}$ with $\mathfrak{p} \cap \mathbb{C}[z] = (0)$. Suppose that the vector $\overline{\varphi} \in \mathcal{K}^{m+1}$ is not a zero of the ideal $\mathfrak{p}$, $|\overline{\varphi}| = 0$, C and A are homogeneous polynomials in $\mathcal{A}$ with $A \in \mathfrak{p}$ and $C \notin \mathfrak{p}$, and the following inequality holds for some $s \geqslant 0$:*

$$\operatorname{ord} C(\overline{\varphi}) \geqslant \operatorname{ord} A(\overline{\varphi}) - s.$$

If $r = m + 1 - h(I) \geqslant 2$, then there exists an unmixed homogeneous ideal $J \subset \mathcal{A}$ such that its set of zeros in projective space over the algebraic closure of $\mathbb{C}(z)$ is the same as the set of zeros of the ideal $(\mathfrak{p}, C)$ and, in addition,

(1) $N(J) \leqslant N(\mathfrak{p}) \deg_{\overline{x}} C$,
(2) $B(J) \leqslant B(\mathfrak{p}) \deg_{\overline{x}} C + N(\mathfrak{p}) \deg_z C$,
(3) $\operatorname{ord} \mathfrak{p}(\overline{\varphi}) \leqslant \operatorname{ord} J(\overline{\varphi}) + B(\mathfrak{p}) \deg_{\overline{x}} C + N(\mathfrak{p})(\deg_z C + s)$.

If $r = 1$, then (3) still holds if we formally set $\operatorname{ord} J(\overline{\varphi}) = 0$ in this case.

Proof. Without loss of generality we may assume that $x_0 \notin \mathfrak{p}$. From Lemmas 2 and 3 of [17] we know that there exists a finite normal extension $\mathbb{K}$ of the field $\mathbb{C}(z, \overline{u}_1, \dots, \overline{u}_{r-1})$ such that the associated form F of $\mathfrak{p}$ splits over $\mathbb{K}$ into a product of linear forms

$$F = a \prod_{j=1}^{N(\mathfrak{p})} (u_{r0} + \alpha_1^{(j)} u_{r1} + \dots + \alpha_m^{(j)} u_{rm}),$$

where $a \in \mathbb{C}[z, \overline{u}_1, \dots, \overline{u}_{r-1}]$ and $\alpha_i^{(j)} \in \mathbb{K}$, and where each of the points $(1 : \alpha_1^{(j)} : \dots : a_m^{(j)}) \in \mathbb{P}_{\mathbb{K}}^m$ is a common zero of $\mathfrak{p}$. Moreover, if

$$G = a^{\deg_{\overline{x}} Q} \prod_{j=1}^{N(\mathfrak{p})} C(1, \alpha_1^{(j)}, \dots, \alpha_m^{(j)}), \tag{28}$$

then $G \in \mathbb{C}[z, \overline{u}_1, \dots, \overline{u}_{r-1}]$, $G \not\equiv 0$, and

$$\deg_z G \leqslant B(\mathfrak{p}) \deg_{\overline{x}} C + N(\mathfrak{p}) \deg_z C. \tag{29}$$

Furthermore, if $r \geqslant 2$, then

$$\deg_{\overline{u}_1} G \leqslant N(\mathfrak{p}) \deg_{\overline{x}} C, \tag{30}$$

and there exists an unmixed homogeneous ideal $J \subset \mathcal{A}$ with $h(J) = m - r + 2$, with associated form $w^{-1}G$ for some $w \in \mathbb{C}[z]$, and with the same set of zeros as $(\mathfrak{p}, C)$ in projective space over the algebraic closure of $\mathbb{C}(z)$. For $r \geqslant 2$ the inequalities (29) and (30) imply (1) and (2) of Lemma 5.1.

It remains to prove (3). According to Lemma 5 of [17] and the remark following the proof of Lemma 6 of [17], there exists a ring homomorphism

$$\tau \colon \mathbb{C}\big[z, \overline{u}_1, \dots, \overline{u}_{r-1}, a^{-1}, \alpha_1^{(1)}, \dots, \alpha_m^{(N(\mathfrak{p}))}\big] \to \mathcal{K}$$

over $\mathbb{C}[z]$ such that

$$\operatorname{ord} \tau(a) = \operatorname{ord} \varkappa(a), \qquad \operatorname{ord} \tau(G) = \operatorname{ord} \varkappa(G) \tag{31}$$

(the map $\varkappa$ was defined in § 3) and, in addition, if we set $\beta_i^{(j)} = \tau(\alpha_i^{(j)})$, then the vectors $\overline{\beta}_j = (1, \beta_1^{(j)}, \dots, \beta_m^{(j)})$, $j = 1, \dots, N(\mathfrak{p})$, are zeros of $\mathfrak{p}$ and satisfy the inequalities

$$\operatorname{ord} \varkappa(a) + \sum_{j=1}^{N(\mathfrak{p})} |\overline{\beta}_j| \geqslant (r-1) N(\mathfrak{p}) |\overline{\varphi}| \geqslant 0, \tag{32}$$

$$\operatorname{ord} \varkappa(a) + \sum_{j=1}^{N(\mathfrak{p})} \big(\|\overline{\varphi} - \overline{\beta}_j\| + |\overline{\beta}_j| \big) \geqslant \operatorname{ord} \mathfrak{p}(\overline{\varphi}) + (r-1) N(\mathfrak{p}) |\overline{\varphi}| \geqslant \operatorname{ord} \mathfrak{p}(\overline{\varphi}). \tag{33}$$

Here and in the sequel, for two vectors $\overline{\varphi} = (\varphi_0, \dots, \varphi_m) \in \mathcal{K}^{m+1}$ and $\overline{\psi} = (\psi_0, \dots, \psi_m) \in \mathcal{K}^{m+1}$ we use the notation

$$\|\overline{\varphi} - \overline{\psi}\| = \min_{0 \leqslant i < j \leqslant m} \operatorname{ord}(\varphi_i \psi_j - \varphi_j \psi_i) - |\overline{\varphi}| - |\overline{\psi}|.$$

We note that always $\|\overline{\varphi} - \overline{\psi}\| \geqslant 0$.

Let j be a fixed index, $1 \leqslant j \leqslant N(\mathfrak{p})$. We choose n so that $|\overline{\beta}_j| = \operatorname{ord} \beta_n^{(j)}$. Since $A(\overline{\beta}_j) = 0$, it follows from Lemma 1 of [17] applied with $V = A$ and $W = x_n^{\deg_{\overline{x}} R}$ that

$$\operatorname{ord} A(\overline{\varphi}) \geqslant \|\overline{\varphi} - \overline{\beta}_j\|.$$

By assumption, we now know that

$$\operatorname{ord} C(\overline{\varphi}) \geqslant \|\overline{\varphi} - \overline{\beta}_j\| - s. \tag{34}$$

If we again apply Lemma 1 of [17], this time with $V = C$ and $W = x_i^{\deg_{\overline{x}} Q}$, where i is chosen so that $\operatorname{ord} \varphi_i = |\overline{\varphi}| = 0$, then we find that

$$\operatorname{ord}\big(C(\overline{\varphi})(\beta_i^{(j)})^{\deg_{\overline{x}} C} - C(\overline{\beta}_j)\varphi_i^{\deg_{\overline{x}} C}\big) \geqslant \|\overline{\varphi} - \overline{\beta}_j\| + |\overline{\beta}_j| \deg_{\overline{x}} C. \tag{35}$$

Furthermore, from the identity

$$C(\overline{\beta}_j)\varphi_i^{\deg_{\overline{x}} C} = C(\overline{\varphi})(\beta_i^{(j)})^{\deg_{\overline{x}} C} - \left(C(\overline{\varphi})(\beta_i^{(j)})^{\deg_{\overline{x}} C} - C(\overline{\beta}_j)\varphi_i^{\deg_{\overline{x}} C}\right)$$

and the inequalities (34) and (35) we conclude that

$$\operatorname{ord} C(\overline{\beta}_j) \geqslant \|\overline{\varphi} - \overline{\beta}_j\| + |\overline{\beta}_j| \deg_{\overline{x}} C - s. \tag{36}$$

Since, by (28), we have

$$\tau(G) = \tau(a)^{\deg_{\overline{x}} C} \prod_{j=1}^{N(\mathfrak{p})} C(1, \beta_1^{(j)}, \dots, \beta_m^{(j)}),$$

it follows from (31) and (36), along with (32) and (33), that

$$\begin{aligned}
\operatorname{ord} \varkappa(G) = \operatorname{ord} \tau(G) &= \deg_{\overline{x}} C \cdot \operatorname{ord} \tau(a) + \sum_{j=1}^{N(\mathfrak{p})} \operatorname{ord} C(\overline{\beta}_j) \\
&\geqslant \deg_{\overline{x}} C \cdot \operatorname{ord} \varkappa(a) + \sum_{j=1}^{N(\mathfrak{p})} \left(\|\overline{\varphi} - \overline{\beta}_j\| + |\overline{\beta}_j| \deg_{\overline{x}} C - s\right) \\
&\geqslant \operatorname{ord} \varkappa(a) + \sum_{j=1}^{N(\mathfrak{p})} \left(\|\overline{\varphi} - \overline{\beta}_j\| + |\overline{\beta}_j|\right) - sN(\mathfrak{p}) \\
&\geqslant \operatorname{ord} \mathfrak{p}(\overline{\varphi}) - sN(\mathfrak{p}).
\end{aligned} \tag{37}$$

Suppose that $r = 1$. Then $G \in \mathbb{C}[z]$, and from (37) and (29) we obtain

$$\operatorname{ord} \mathfrak{p}(\overline{\varphi}) \leqslant \operatorname{ord} G + sN(\mathfrak{p}) \leqslant \deg_z G + sN(\mathfrak{p}) \leqslant B(\mathfrak{p}) \deg_{\overline{x}} C + N(\mathfrak{p})(\deg_z C + s).$$

We have thus proved the required inequality in the case $r = 1$.

Now suppose that $r \geqslant 2$. Using (37) and (29), we obtain

$$\begin{aligned}
\operatorname{ord} \mathfrak{p}(\overline{\varphi}) &\leqslant \operatorname{ord} \varkappa(G) + sN(\mathfrak{p}) = \operatorname{ord} w + \operatorname{ord} J(\overline{\varphi}) + sN(\mathfrak{p}) \\
&\leqslant \operatorname{ord} J(\overline{\varphi}) + sN(\mathfrak{p}) + \deg_z G \\
&\leqslant \operatorname{ord} J(\overline{\varphi}) + B(\mathfrak{p}) \deg_{\overline{x}} C + N(\mathfrak{p})(\deg_z C + s).
\end{aligned}$$

This proves the required inequality for $r \geqslant 2$.

We shall want to apply this lemma with $m = 3$, $s = 0$ and $r = 1$ or 2. We shall also refer to the lemmas in [17] in the case $m = 3$. We now return to our earlier notation $\mathcal{A} = \mathbb{C}[z, x_0, x_1, x_2, x_3]$.

Lemma 5.2. *Let $\mathfrak{p} \subset \mathcal{A}$ be a homogeneous prime ideal with $\mathfrak{p} \cap \mathbb{C}[z] = (0)$ and $r = 4 - h(\mathfrak{p}) \geqslant 1$ and let ν and μ be non-negative integers satisfying the inequalities*

$$\nu^{4-r} \geqslant \lambda N(\mathfrak{p}), \qquad (\mu + 1)\nu^{3-r} \geqslant \lambda B(\mathfrak{p}), \tag{38}$$

where $\lambda = 18^3 = 5832$. *There exists a polynomial* $E \in \mathfrak{p}$ *that is homogeneous in* $\overline{x}$ *and satisfies the inequalities*

$$\deg_z E \leqslant \mu, \qquad \deg_{\overline{x}} E \leqslant \nu.$$

Proof. See [19], Corollary 2 of Theorem 2 with $m = 3$.

We note that the inequalities in (38) hold if, for example,

$$\nu = 1 + \left[\lambda N(\mathfrak{p})^{1/(4-r)}\right], \qquad \mu = \left[\lambda B(\mathfrak{p}) N(\mathfrak{p})^{-(3-r)/(4-r)}\right], \tag{39}$$

where $[\cdot]$ denotes the integer part.

We now define a homogeneous analogue of the operator D in (13) for the ring $\mathcal{A}$:

$$T = z\frac{\partial}{\partial z} + \frac{1}{12}(x_1^2 - x_0x_2)\frac{\partial}{\partial x_1} + \frac{1}{3}(x_1x_2 - x_0x_3)\frac{\partial}{\partial x_2} + \frac{1}{2}(x_1x_3 - x_2^2)\frac{\partial}{\partial x_3}.$$

Then $Tx_0 = 0$.

Lemma 5.3. *If* $\mathfrak{p}$ *is a homogeneous prime ideal of* $\mathcal{A}$ *with*

$$\operatorname{ord}\mathfrak{p}(\overline{f}) > B(\mathfrak{p}) + 3N(\mathfrak{p}),$$

then there do not exist homogeneous prime ideals $\mathfrak{q} \subset \mathfrak{p}$, $\mathfrak{q} \neq (0)$, *with* $T\mathfrak{q} \subset \mathfrak{q}$.

In this lemma, as in Theorem 3, we use the notation $\overline{f} = \bigl(1, P(z), Q(z), R(z)\bigr)$.

Proof. We shall follow the proof of Lemma 7 in [17] and use the facts about D-invariant ideals that were proved in § 3. Suppose that Lemma 5.3 is false and there exists a homogeneous prime ideal $\mathfrak{q} \subset \mathfrak{p}$, $\mathfrak{q} \neq (0)$, that satisfies the condition that $T\mathfrak{q} \subset \mathfrak{q}$.

According to Lemma 6 of [17], there exists a zero $\overline{\beta} \in \mathcal{K}^4$ of the ideal $\mathfrak{p}$ for which

$$\operatorname{ord}\mathfrak{p}(\overline{f}) \leqslant rN(\mathfrak{p}) \cdot \|\overline{f} - \overline{\beta}\| + B(\mathfrak{p}).$$

Taking into account the inequality in the lemma, we conclude that $\|\overline{f} - \overline{\beta}\| > 1$.

Let n be chosen so that $\operatorname{ord}\beta_n = |\overline{\beta}|$. Let V be any homogeneous polynomial in $\mathfrak{p}$, and let $W = x_n^d$, where $d = \deg_{\overline{x}} V$. If we apply Lemma 1 of [17] to the polynomials V and W, then we obtain the inequality

$$\operatorname{ord}\bigl(V(\overline{f})W(\overline{\beta}) - V(\overline{\beta})W(\overline{f})\bigr) \geqslant \|\overline{f} - \overline{\beta}\| + \bigl(|\overline{f}| + |\overline{\beta}|\bigr)d$$

or, since $V(\overline{\beta}) = 0$, $|\overline{f}| = 0$, and $\|\overline{f} - \overline{\beta}\| > 1$, we have the inequality

$$\operatorname{ord} V(\overline{f}) + d \cdot \operatorname{ord}\beta_n > 1 + |\overline{\beta}| \cdot d.$$

Recalling the definition of n, we finally obtain

$$V(\overline{f}) > 1. \tag{40}$$

The inequality (40) does not hold for the polynomial $V = x_0$. Hence, $x_0 \notin \mathfrak{p}$ and so $x_0 \notin \mathfrak{q}$.

Let $\mathfrak{q}_0$ denote the ideal of $\mathfrak{R} = \mathbb{C}[z, x_1, x_2, x_3]$ consisting of all polynomials C for which there exist polynomials $C_0 \in \mathfrak{q}$ and $B \in \mathcal{A}$ such that

$$C = C_0 + (x_0 - 1)B, \tag{41}$$

where C_0 is homogeneous. We claim that $\mathfrak{q}_0$ is a prime ideal. In fact, if $U, V \in \mathfrak{R}$ are such that $UV \in \mathfrak{q}_0$, then there exist homogeneous polynomials U_0, V_0 and W_0 with

$$U = U_0 + (x_0 - 1)U_1, \qquad V = V_0 + (x_0 - 1)V_1, \qquad UV = W_0 + (x_0 - 1)W_1, \quad W_0 \in \mathfrak{q},$$

where $U_1, V_1, W_1 \in \mathcal{A}$. We may suppose that $\deg_{\overline{x}} U_0 + \deg_{\overline{x}} V_0 = \deg_{\overline{x}} W_0$, since otherwise we could multiply any of the polynomials U_0, V_0 or W_0 by a suitable power of x_0 to obtain the equality. From the above relations it follows that

$$W_0 - U_0V_0 = (x_0 - 1)G, \qquad G \in \mathcal{A},$$

and, since $W_0 - U_0V_0$ is a homogeneous polynomial, we conclude that $W_0 - U_0V_0 = 0$ and $U_0V_0 = W_0 \in \mathfrak{q}$. Since $\mathfrak{q}$ is a prime ideal, either U_0 or V_0 lies in $\mathfrak{q}$. But then, by the definition of $\mathfrak{q}_0$, either U or V must belong to $\mathfrak{q}_0$. This proves that $\mathfrak{q}_0$ is a prime ideal.

Applying the operator T to (41), we obtain

$$TC = TC_0 + (x_0 - 1)TB$$

and for some $B_1 \in \mathcal{A}$ we have

$$DC = TC_0 + (x_0 - 1)B_1.$$

Since $T\mathfrak{q} \subset \mathfrak{q}$, it follows that $TC_0 \in \mathfrak{q}$, and so $DC \in \mathfrak{q}_0$.We have thus proved that $\mathfrak{q}_0$ is a D-invariant ideal. From (41) and (40) it follows that for any $C \in \mathfrak{q}_0$

$$\operatorname{ord} C(\overline{f}) = \operatorname{ord} C_0(\overline{f}) > 1. \tag{42}$$

In particular, this means that the point $(0, 1, 1, 1)$ is a zero of the ideal $\mathfrak{q}_0$. By Proposition 4.2, either $z \in \mathfrak{q}_0$, or else $\Delta = x_2^3 - x_3^2 \in \mathfrak{q}_0$. However, neither of these two polynomials satisfies (42). This contradiction completes the proof of Lemma 5.3.

Lemma 5.4. *Let $\mathfrak{p} \subset \mathcal{A}$ be a homogeneous prime ideal with $\mathfrak{p} \cap \mathbb{C}[z] = (0)$, $r = 4 - h(\mathfrak{p}) \geqslant 1$, and*

$$\operatorname{ord} \mathfrak{p}(\overline{f}) > B(\mathfrak{p}) + 3N(\mathfrak{p}).$$

Then there exists a homogeneous polynomial $A \in \mathfrak{p}$ such that $C = TA \notin \mathfrak{p}$ and

$$\deg_{\overline{x}} C \leqslant 9\lambda^2 N(\mathfrak{p})^{1/(4-r)}, \quad \deg_z C \leqslant 3\lambda\big(B(\mathfrak{p}) + 1\big)N(\mathfrak{p})^{-(3-r)/(4-r)}, \tag{43}$$

where, as in Lemma 5.2, $\lambda = 18^3 = 5832$.

Proof. Let E be a homogeneous polynomial in $\mathfrak{p}$, for which the following expression attains its minimum value:

$$N(\mathfrak{p}) \deg_z E + \big(B(\mathfrak{p}) + 1\big) \deg_{\overline{x}} E.$$

The polynomial E is obviously irreducible. For brevity we set $L = \deg_{\overline{x}} E$ and $M = \deg_z E$. We define μ and ν using (39). By Lemma 5.2, we find that

$$N(\mathfrak{p})M + \big(B(\mathfrak{p}) + 1\big)L \leqslant N(\mathfrak{p})\mu + \big(B(\mathfrak{p}) + 1\big)\nu \leqslant 3\lambda\big(B(\mathfrak{p}) + 1\big)N(\mathfrak{p})^{1/(4-r)},$$

from which it follows that

$$L \leqslant 3\lambda N(\mathfrak{p})^{1/(4-r)}, \qquad M \leqslant 3\lambda\big(B(\mathfrak{p}) + 1\big)N(\mathfrak{p})^{-(3-r)/(4-r)}. \tag{44}$$

Since $\mathfrak{p} \cap \mathbb{C}[z] = (0)$, we have $L \geqslant 1$.

We set $E_0 = E$ and $E_1 = TE$. We have

$$\deg_z E_1 \leqslant M, \qquad \deg_{\overline{x}} E_1 \leqslant L + 1.$$

If $E_1 \notin \mathfrak{p}$, then we set $A = E$ and $C = E_1$, and Lemma 5.4 holds. Hence, from now on we suppose that $E_1 \in \mathfrak{p}$.

We set $J_0 = (E_0)$ and $J_1 = (E_0, E_1)$. We have $h(J_0) = 1$. The polynomial E_0 is irreducible, and $E_0 \nmid E_1$, since otherwise the principal prime ideal J_0 would be T-invariant, and this is impossible by Lemma 5.3. But then J_1 is an unmixed ideal with $h(J_1) = 2$. According to Lemma 4 of [17] applied to the ideals J_0 and J_1 and the polynomial E_1 we have

$$N(J_1) \leqslant N(J_0) \deg_{\overline{x}} E_1 \leqslant (L + 1)^2,$$
$$B(J_1) \leqslant B(J_0) \deg_{\overline{x}} E_1 + N(J_0) \deg_z E_1 \leqslant M(2L + 1) \leqslant 2M(L + 1).$$

We have used the relations in Lemma 3.1 to bound $N(J_0)$ and $B(J_0)$.

We set

$$\chi_0 = 0, \quad \chi_1 = a_1 = c_1 = 1, \quad b_1 = 2$$

and define χ_i, a_i, b_i, c_i as follows for $i = 2, 3$:

$$\chi_{i+1} = \chi_i + 2\lambda b_i, \qquad i = 1, 2, \tag{45}$$
$$c_{i+1} = c_i + \lambda b_i, \qquad i = 1, 2, \tag{46}$$
$$a_{i+1} = a_i c_{i+1}, \qquad i = 1, 2, \tag{47}$$
$$b_{i+1} = b_i c_{i+1} + a_i, \qquad i = 1, 2. \tag{48}$$

For each $k = 0, 1, 2, 3$ we now let J_k denote the ideal of $\mathcal{A}$ that is generated by the polynomials $T^i E$, $0 \leqslant i \leqslant \chi_k$.

Let k be the largest integer such that $J_k \subset \mathfrak{p}$ and there exist homogeneous polynomials $E_0, \dots, E_k$ satisfying the conditions

(1) $\deg_{\overline{x}} E_j \leqslant c_j(L + 1)$ and $\deg_z E_j \leqslant M$ for $j = 1, \dots, k$;
(2) the ideal $\mathfrak{a}_k = (E_0, \dots, E_k)$ is contained in J_k;
(3) all the primary components of $\mathfrak{a}_k$ contained in $\mathfrak{p}$ have height $k + 1$, and if $\mathfrak{u}_k$ is the unmixed ideal that is the intersection of these components, then

$$N(\mathfrak{u}_k) \leqslant a_k(L + 1)^{k+1}, \qquad B(\mathfrak{u}_k) \leqslant b_k M(L + 1)^k. \tag{49}$$

For $k = 1$ it is easy to see that these conditions hold with the polynomials E_0 and E_1 that we constructed before; hence, $k \geqslant 1$. On the other hand, the inclusion $\mathfrak{u}_k \subset \mathfrak{p}$ implies that $k+1 = h(\mathfrak{u}_k) \leqslant h(\mathfrak{p}) = 4 - r$, so that $k \leqslant 3 - r$. We suppose that $J_{k+1} \subset \mathfrak{p}$ and show how this would lead to a contradiction.

Let $\mathfrak{b}$ be a primary component of the ideal $\mathfrak{u}_k$, set $\mathfrak{q} = \sqrt{\mathfrak{b}}$, and let l be the exponent of $\mathfrak{q}$, that is, the smallest natural number such that $\mathfrak{q}^l \subset \mathfrak{b}$. We now prove that

$$l \leqslant 2\lambda b_k. \tag{50}$$

Suppose that, on the contrary, $l > 2\lambda b_k$. Then, according to (49) and the relation (1) in Proposition 2 of [17], we have

$$a_k(L+1)^{k+1} \geqslant N(\mathfrak{u}_k) \geqslant lN(\mathfrak{q}) \geqslant l > 2\lambda b_k \geqslant 2\lambda a_k.$$

This implies that $(L+1)^3 \geqslant (L+1)^{k+1} > 2\lambda$ and $L \geqslant 22$. Furthermore,

$$\left(\frac{L-1}{L+1}\right)^3 \geqslant \left(\frac{21}{23}\right)^3 > \frac{1}{2}$$

and $(L+1)^3 < 2(L-1)^3$. Using Proposition 2 of [17] and (49), from this we see that

$$\lambda B(\mathfrak{q}) \leqslant \frac{\lambda B(\mathfrak{u}_k)}{l} \leqslant \frac{B(\mathfrak{u}_k)}{2b_k} \leqslant \frac{1}{2}(M+1)(L+1)^k < (M+1)(L-1)^k,$$
$$\lambda N(\mathfrak{q}) \leqslant \frac{\lambda N(\mathfrak{u}_k)}{l} \leqslant \frac{N(\mathfrak{u}_k)}{2b_k} \leqslant \frac{1}{2}(L+1)^{k+1} < (L-1)^{k+1}.$$

We have also used the fact that $a_k \leqslant b_k$. Thus, the ideal $\mathfrak{q}$ satisfies (38) with $\nu = L-1$ and $\mu = M$. By Lemma 5.2, there exists a homogeneous polynomial $G \in \mathfrak{q}$ that satisfies the inequalities

$$\deg_{\overline{x}} G \leqslant L-1, \qquad \deg_z G \leqslant M.$$

Since $G \in \mathfrak{q} \subset \mathfrak{p}$, these inequalities contradict the definition of the polynomial E. This proves (50).

We next prove that there exist i, j with $0 \leqslant i \leqslant k$ and $0 \leqslant j \leqslant 2\lambda b_k$ such that $T^j E_i \notin \mathfrak{q}$. The ideal $\mathfrak{q}$ is isolated in the set of associated prime ideals of $\mathfrak{a}_k$. Hence, there exists a polynomial $H \notin \mathfrak{q}$ such that $G^l H \in \mathfrak{a}_k$ for any $G \in \mathfrak{q}$. Suppose that there did not exist i, j with the desired properties. Then, since $l \leqslant 2\lambda b_k$, we should have $T^l(G^l H) \in \mathfrak{q}$. Since $G \in \mathfrak{q}$, this implies that $(TG)^l H \in \mathfrak{q}$; and, since $\mathfrak{q}$ is a prime ideal and $H \notin \mathfrak{q}$, we have $TG \in \mathfrak{q}$. Thus, $T\mathfrak{q} \subset \mathfrak{q}$, which contradicts Lemma 5.3. This proves the existence of indices i, j with the desired properties.

Let $\mathfrak{q}_1, \ldots, \mathfrak{q}_s$ be all of the associated prime ideals of $\mathfrak{u}_k$. By what was proved above for every v with $1 \leqslant v \leqslant s$ there exist i_v, j_v with $0 \leqslant i_v \leqslant k$ and $0 \leqslant j_v \leqslant 2\lambda b_k$ such that $T^{j_v} E_{i_v} \notin \mathfrak{q}_v$. We set

$$E_{k+1} = \sum_{v=1}^{s} \eta_v T^{j_v} E_{i_v},$$

where the $\eta_v \in \mathbb{C}$ are chosen so that $E_{k+1} \notin \mathfrak{q}_v$ for $1 \leqslant v \leqslant s$, and we prove that the polynomials $E_0, \ldots, E_{k+1}$ satisfy the conditions (1)–(3) with k replaced by $k+1$.

Since the operator T does not increase the degree in z of a polynomial, it follows that $\deg_z E_{k+1} \leqslant M$. Using (46), we also obtain

$$\deg_{\overline{x}} E_{k+1} \leqslant c_k(L+1) + 2\lambda b_k \leqslant c_{k+1}(L+1).$$

Thus, (1) holds with k replaced by $k+1$. Condition (2) follows from (45).

Let $\mathfrak{r}$ be an associated prime ideal of $\mathfrak{a}_{k+1}$ that is contained in $\mathfrak{p}$ (such ideals exist because $\mathfrak{a}_{k+1} \subset J_{k+1} \subset \mathfrak{p}$). Since $\mathfrak{r} \supset \mathfrak{a}_{k+1} = (\mathfrak{a}_k, E_{k+1})$, we have $\mathfrak{p} \supset \mathfrak{r} \supset \mathfrak{a}_k$. If we take into account the fact that the set of all associated prime ideals of $\mathfrak{a}_k$ contained in $\mathfrak{p}$ coincides with the set $\mathfrak{q}_1, \ldots, \mathfrak{q}_s$, then we conclude that there exists an ideal $\mathfrak{q}_j \subset \mathfrak{r}$. Hence, $h(\mathfrak{r}) \geqslant h(\mathfrak{q}_j) = k+1$. If $h(\mathfrak{r}) = k+1$, then $\mathfrak{r} = \mathfrak{q}_j$. But this is impossible, since $E_{k+1} \in \mathfrak{r}$ and $E_{k+1} \notin \mathfrak{q}_j$. Thus, $h(\mathfrak{r}) \geqslant k+2$; since $\mathfrak{a}_{k+1}$ is generated by $k+2$ polynomials, this means that $h(\mathfrak{r}) = k+2$. We have proved that all the primary components of $\mathfrak{a}_{k+1}$ that are contained in $\mathfrak{p}$ have height $k+2$.

Let $\mathfrak{a}_k = \mathfrak{u}_k \cap \mathfrak{a}'$, where $\mathfrak{a}'$ is the intersection of the primary components of $\mathfrak{a}_k$ that do not occur in $\mathfrak{u}_k$. If I were a primary component of $\mathfrak{u}_{k+1}$ and $\mathfrak{r} = \sqrt{I}$, then the inclusion $\mathfrak{r} \supset \mathfrak{a}'$ would imply that $\mathfrak{p} \supset \mathfrak{r} \supset \mathfrak{a}'$, which is impossible. Hence, $\mathfrak{a}'$ is not contained in $\mathfrak{r}$; so from the inclusion $\mathfrak{u}_k \cap \mathfrak{a}' = \mathfrak{a}_k \subset \mathfrak{a}_{k+1} \subset I$ we obtain $\mathfrak{u}_k \subset I$. Thus, $\mathfrak{u}_k \subset \mathfrak{u}_{k+1}$, and since $E_{k+1} \in \mathfrak{a}_{k+1} \subset \mathfrak{u}_{k+1}$, we have $(\mathfrak{u}_k, E_{k+1}) \subset \mathfrak{u}_{k+1}$. Using Lemma 4 of [17], (49), (47) and (48), we see that this inclusion implies that

$$N(\mathfrak{u}_{k+1}) \leqslant N(\mathfrak{u}_k) \deg_{\overline{x}} E_{k+1} \leqslant a_{k+1}(L+1)^{k+2},$$
$$B(\mathfrak{u}_{k+1}) \leqslant B(\mathfrak{u}_k) \deg_{\overline{x}} E_{k+1} + N(\mathfrak{u}_k) \deg_z E_{k+1} \leqslant b_{k+1} M (L+1)^{k+1}.$$

We have proved that the polynomials $E_0, \ldots, E_{k+1}$ satisfy all the conditions (1)–(3) with k replaced by $k+1$. In other words, the assumption that $J_{k+1} \subset \mathfrak{p}$ led us to a contradiction with the definition of k. Thus, J_{k+1} is not contained in $\mathfrak{p}$ and, since $k \leqslant 3 - r \leqslant 2$, the inclusion $J_3 \subset \mathfrak{p}$ is impossible. This means that there exists an index i ($0 \leqslant i \leqslant \chi_3 - 1$) such that $A = T^i E \in \mathfrak{p}$ but $C = TA \notin \mathfrak{p}$. From (45)–(48) it follows that $\chi_3 = 8\lambda^2 + 10\lambda + 1$. Finally, using (44) we find that

$$\deg_z C \leqslant M \leqslant 3\lambda\big(B(\mathfrak{p}) + 1\big) N(\mathfrak{p})^{-(3-r)/(4-r)},$$
$$\deg_{\overline{x}} C \leqslant \deg_{\overline{x}} E + \chi_3 = L + \chi_3 \leqslant 9\lambda^2 N(\mathfrak{p})^{1/(4-r)}.$$

Lemma 5.4 is proved.

§ 6. End of the proof of Theorem 5

We now proceed directly to the proof of Theorem 5. Suppose that there exist ideals that satisfy the hypothesis of the theorem but not its conclusion. Let I be such an ideal having maximal height $h(I)$ and let $r = 4 - h(I)$. Then

$$\operatorname{ord} I(\overline{f}) > \rho^{2r-1}\big(B(I) N(I)^{r/(r-4)} + N(I)^{3/(4-r)}\big). \tag{51}$$

Let $I_1, \ldots, I_s$ be all the primary components of I that have trivial intersection with $\mathbb{C}[z]$, let k_j be their exponents and let $\mathfrak{p}_j = \sqrt{I_j}$ be their radicals. By assumption,

$s \geqslant 1$. The following equalities hold for some $b \in \mathbb{C}[z]$ by Proposition 2 of [17]:

$$\sum_{j=1}^{s} k_j N(\mathfrak{p}_j) = N(I), \tag{52}$$

$$\deg_z b + \sum_{j=1}^{s} k_j B(\mathfrak{p}_j) = B(I), \tag{53}$$

$$\operatorname{ord} b + \sum_{j=1}^{s} k_j \operatorname{ord} \mathfrak{p}_j(\overline{f}) = \operatorname{ord} I(\overline{f}). \tag{54}$$

If for all j one has $\operatorname{ord} \mathfrak{p}_j(\overline{f}) \leqslant \rho^{2r-1}\big(B(\mathfrak{p}_j)N(\mathfrak{p}_j)^{r/(4-r)} + N(\mathfrak{p}_j)^{3/(4-r)}\big)$, then from (52)–(54) we obtain

$$\begin{aligned}
\operatorname{ord} I(\overline{f}) &= \operatorname{ord} b + \sum_{j=1}^{s} k_j \operatorname{ord} \mathfrak{p}_j(\overline{f}) \\
&\leqslant \deg_z b + \sum_{j=1}^{s} k_j \rho^{2r-1} B(\mathfrak{p}_j) N(\mathfrak{p}_j)^{r/(4-r)} + \rho^{2r-1} \sum_{j=1}^{s} k_j N(\mathfrak{p}_j)^{3/(4-r)} \\
&\leqslant \rho^{2r-1} N(I)^{r/(4-r)} \bigg(\deg_z b + \sum_{j=1}^{s} k_j B(\mathfrak{p}_j)\bigg) + \rho^{2r-1} \bigg(\sum_{j=1}^{s} k_j N(\mathfrak{p}_j)\bigg)^{3/(4-r)} \\
&\leqslant \rho^{2r-1}\big(B(I)N(I)^{r/(4-r)} + N(I)^{3/(4-r)}\big),
\end{aligned}$$

which contradicts (51). This contradiction means that there exists a prime ideal $\mathfrak{p}$ with $\mathfrak{p} \cap \mathbb{C}[z] = (0)$ and $h(\mathfrak{p}) = 4 - r$ such that

$$\operatorname{ord} \mathfrak{p}(\overline{f}) > \rho^{2r-1}\big(B(\mathfrak{p})N(\mathfrak{p})^{r/(4-r)} + N(\mathfrak{p})^{3/(4-r)}\big). \tag{55}$$

Let A and C be the polynomials whose existence was proved in Lemma 5.4.

We first consider the case $r = 1$. If we apply Lemma 5.1 to the ideal $\mathfrak{p}$, the polynomials A and C, and the vector $\overline{f}$ (in our case $s = 0$), and if we use (43) with $r = 1$, then we find that

$$\operatorname{ord} \mathfrak{p}(\overline{\varphi}) \leqslant B(\mathfrak{p}) \deg_{\overline{x}} C + N(\mathfrak{p}) \deg_z C \leqslant (9\lambda^2 + 3\lambda) B(\mathfrak{p}) N(\mathfrak{p})^{1/3} + 3\lambda N(\mathfrak{p}),$$

which contradicts (55) for $r = 1$. Thus, this case is impossible.

In the case $r \geqslant 2$ we consider the ideal J whose existence is ensured by Lemma 5.1. We apply the lemma to the ideal $\mathfrak{p}$ and the polynomials A and C that are constructed in Lemma 5.4. Using (43), according to Lemma 5.1 we have the bounds

$$N(J) \leqslant N(\mathfrak{p}) \deg_{\overline{x}} C \leqslant 9\lambda^2 N(\mathfrak{p})^{(5-r)/(4-r)}, \tag{56}$$

$$\begin{aligned}
B(J) &\leqslant B(\mathfrak{p}) \deg_{\overline{x}} C + N(\mathfrak{p}) \deg_z C \\
&\leqslant (9\lambda^2 + 3\lambda) B(\mathfrak{p}) N(\mathfrak{p})^{1/(4-r)} + 3\lambda N(\mathfrak{p})^{1/(4-r)}.
\end{aligned} \tag{57}$$

The ideal J satisfies the relation: $h(J) = h(\mathfrak{p}) + 1 > h(I)$. From the definition of I it follows that

$$\operatorname{ord} J(\overline{f}) \leqslant \rho^{2r-3}\big(B(J)N(J)^{(r-1)/(5-r)} + N(I)^{3/(5-r)}\big).$$

Using this inequality, the inequality (3) of Lemma 5.1, and also (56), (57) and (43), we find that

$$\begin{aligned}\operatorname{ord}\mathfrak{p}(\overline{f}) &\leqslant \operatorname{ord} J(\overline{f}) + B(\mathfrak{p})\deg_{\overline{x}} C + N(\mathfrak{p})\deg_z C\\ &\leqslant \rho^{2r-3}\Big((9\lambda^2+3\lambda)B(\mathfrak{p})N(\mathfrak{p})^{\frac{1}{4-r}} + 3\lambda N(\mathfrak{p})^{\frac{1}{4-r}}\Big)\Big(9\lambda^2 N(\mathfrak{p})^{\frac{5-r}{4-r}}\Big)^{\frac{r-1}{5-r}}\\ &\qquad + \rho^{2r-3}\Big(9\lambda^2 N(\mathfrak{p})^{\frac{5-r}{4-r}}\Big)^{\frac{3}{5-r}} + (9\lambda^2+3\lambda)B(\mathfrak{p})N(\mathfrak{p})^{\frac{1}{4-r}} + 3\lambda N(\mathfrak{p})^{\frac{1}{4-r}}\\ &< \rho^{2r-1}\big(B(\mathfrak{p})N(\mathfrak{p})^{r/(4-r)} + N(\mathfrak{p})^{3/(4-r)}\big).\end{aligned}$$

This inequality contradicts (55) and thereby completes the proof of Theorem 5.

This proof of Theorem 5 was presented in such a way as to open up the possibility of obtaining a more general result. We consider an arbitrary system of differential equations

$$t(z)y_j' = F_j(z, y_1, \dots, y_m), \qquad j = 1, \dots, m, \tag{58}$$

where $t(z)$ and $F_j(z, y_1, \dots, y_m)$ are polynomials in all the indicated variables.

Definition. We say that a solution $f_1(z), \dots, f_m(z)$ of the system (58) *has the D-property at the point* $\xi \in \mathbb{C}$ if these functions are analytic at ξ and the set of all prime ideals of $\mathbb{C}[z, y_1, \dots, y_m]$ having the following two properties has non-zero intersection: (1) the ideal is invariant relative to the operator

$$D = t(z)\frac{\partial}{\partial z} + \sum_{j=1}^{m} F_j(z, y_1, \dots, y_m)\frac{\partial}{\partial y_j},$$

and (2) its variety of zeros in $\mathbb{C}^{m+1}$ does not contain the analytic curve $\big(z, f_1(z), \dots, f_m(z)\big)$, but contains the point of this curve corresponding to $z = \xi$.

If the functions $f_i(z)$ are algebraically independent over $\mathbb{C}(z)$, then this condition means that either the set of D-invariant prime ideals having zero at $\big(\xi, f_1(\xi), \dots, f_m(\xi)\big)$ has non-trivial intersection, or else there are no such ideals at all.

For example, in Proposition 2 of §4 we saw that the set of functions $\big(P(z), Q(z), R(z)\big)$ has the D-property at the point $\xi = 0$. The polynomial $z(y_2^3 - y_3^2)$ is contained in the intersection of all D-invariant prime ideals with zero at $(0, 1, 1, 1)$. In [17] we used the fact that if a set of functions $f_1(z), \dots, f_m(z)$ is algebraically independent over $\mathbb{C}(z)$ and satisfies a homogeneous (in y_j) linear system of differential equations (58), then it has the D-property at any point $\xi \in \mathbb{C}$.

It is easy to prove that if ξ is not a zero of the polynomial $t(z)$ (that is, ξ is not a singular point), then any solution to (58) that is analytic at ξ has the D-property. In fact, suppose that $\big(\xi, f_1(\xi), \dots, f_m(\xi)\big)$ is one of the zeros of the D-invariant prime ideal $\mathfrak{p}$. Since we have the identity $t(z)^n\varphi^{(n)}(z) = B\big(z, f_1(z), \dots, f_m(z)\big)$ for any polynomial $A \in \mathfrak{p}$ and any $n \geqslant 0$, where $\varphi(z) = A\big(z, f_1(z), \dots, f_m(z)\big)$ and $B = t(z)^n\big(t(z)^{-1}D\big)^n A \in \mathfrak{p}$, it follows that, in view of the condition $t(\xi) \neq 0$, we have $\varphi^{(n)}(\xi) = 0$ for $n \geqslant 0$; that is, $\varphi(z) \equiv 0$, and so the entire curve $\big(z, f_1(z), \dots, f_m(z)\big)$ belongs to the variety of zeros of $\mathfrak{p}$. Thus, in this case there do not exist any prime ideals with the properties in the definition. A similar situation occurred in [16], where we considered a set of functions that satisfies a system of differential equations (58) with constant coefficients ($t(z) \equiv 1$ and the F_j do not depend on z), and hence has the D-property at any point ξ.

The next result is a generalization of Theorem 3.

Theorem 6. *Suppose that the solution $f_1(z), \dots, f_m(z)$ of the system (58) consists of functions that are algebraically independent over $\mathbb{C}(z)$ and have the D-property at a point $\xi \in \mathbb{C}$. Then for any $A \in \mathbb{C}[z, x_1, \dots, x_m]$ with $A \not\equiv 0$ one has*

$$\operatorname{ord}_{z=\xi} A\bigl(z, f_1(z), \dots, f_m(z)\bigr) \leqslant \gamma_5(\deg_z A + 1)(\deg_{\overline{x}} A)^m,$$

where γ_5 is a constant that depends only on the point ξ and the functions $f_i(z)$.

Proof. The proof of this theorem is almost identical to the proof of Theorem 3. Instead of the inequality in Theorem 5, one uses induction on r, $1 \leqslant r \leqslant m$, to prove that the inequality

$$\operatorname{ord} I(\overline{f}) \leqslant \rho^{2r-1}\bigl(B(I)N(I)^{r/(m+1-r)} + N(I)^{m/(m+1-r)}\bigr) \tag{59}$$

(with ρ a sufficiently large constant) holds for any unmixed homogeneous ideal $I \subset \mathcal{A} = \mathbb{C}[z, x_0, \dots, x_m]$ for which $I \cap \mathbb{C}[z] = (0)$ and $h(I) = m + 1 - r$. To do this it suffices to make some natural modifications in the proof of Lemma 5.3. One makes a new choice of sequences a_i, b_i, c_i, χ_i; and the bound on the degrees in z of the E_j in the proof of Lemma 5.4 is written in the form $\deg_z E_j \leqslant c_j(M + 1)$. No significant changes in the proof are needed.

The algebraic independence condition for the functions $f_j(z)$ in Theorem 6 can be omitted, and one can also prove a bound for the sum of the multiplicities of the zeros at different points. The next result is a generalization of Theorem 6 and the main theorems of [16] and [17].

Theorem 7. *Suppose that the solution $f_1(z), \dots, f_m(z)$ of the system (58) has the D-property at each of the distinct complex points $\xi_1, \dots, \xi_q$. Then for any $A \in \mathbb{C}[z, x_1, \dots, x_m]$ with $A\bigl(z, f_1(z), \dots, f_m(z)\bigr) \not\equiv 0$ one has*

$$\sum_{j=1}^{q} \operatorname{ord}_{z=\xi_j} A\bigl(z, f_1(z), \dots, f_m(z)\bigr) \leqslant \gamma_6(\deg_z A + q)(\deg_{\overline{x}} A)^k,$$

where γ_6 is a constant that depends only on the points ξ_j, the functions $f_i(z)$ and the system (58), and k is the maximum number of functions $f_i(z)$ that are algebraically independent over $\mathbb{C}(z)$.

This theorem is proved by the method used above. In Lemma 5.3 the condition that $\mathfrak{q} \neq (0)$ must be replaced by the condition that $\mathfrak{q}$ not be contained in the ideal $\mathfrak{E}$ consisting of all the algebraic relations among the functions $f_j(z)$ over $\mathbb{C}[z]$. The analogue of the inequality in Theorem 5 has the form

$$\sum_{j=1}^{q} \operatorname{ord}_{z=\xi_j} I(\overline{f}) \leqslant \rho^{2r-1}\bigl(B(I)N(I)^{r/(k+1-r)} + qN(I)^{k/(k+1-r)}\bigr),$$

where, as before, $r = m + 1 - h(I)$; this is proved by induction on r for $1 \leqslant r \leqslant k$. In [16] and [17] one can find all of the modifications in the proof that are needed because one has a large number of points.

This research was carried out when the author was a guest at the Institute of Mathematics of the Universities of Paris VI and VII. The excellent conditions and creative ambiance contributed greatly to the work.

In conclusion, I should like to thank M. Waldschmidt for bringing [7] and related problems to my attention. I should also like to thank D. Bertrand and P. Philippon for many valuable discussions.

Bibliography

[1] S. Lang, *Elliptic functions*, Addison Wesley, Reading, MA 1973.
[2] Th. Schneider, "Arithmetische Untersuchungen elliptischer Integrale", *Math. Ann.* **113** (1937), 1–13.
[3] S. Ramanujan, "On certain arithmetical functions", *Trans. Cambridge Philosoph. Soc.* **22**:9 (1916), 159–184; *Collected papers of Srinivasa Ramanujan*, Chelsea Publishing Co., New York 1962, pp. 136–162.
[4] K. Mahler, "On algebraic differential equations satisfied by automorphic functions", *J. Austral. Math. Soc.* **10** (1969), 445–450.
[5] D. Masser, *Elliptic functions and transcendence,* Lecture Notes in Mathematics, vol. 437, Springer-Verlag, Berlin 1975.
[6] K. Mahler, "Remarks on a paper by W. Schwarz", *J. Number Theory* **1** (1969), 512–521.
[7] K. Barré-Sirieix, G. Diaz, F. Gramain and G. Philibert, "Une preuve de la conjecture de Mahler–Manin", *Invent. Math.* **124** (1996), 1–9.
[8] G. V. Chudnovskiĭ, "Algebraic independence of constants connected with the exponential and elliptic functions", *Dokl. Akad. Nauk Ukr. SSR* **1976**:8, 698–701. (Russian)
[9] M. Waldschmidt, *Les travaux de G. V. Chudnovskii sur les nombres transcendants,* Lecture Notes in Mathematics, vol. 567, Springer-Verlag, Berlin 1977, pp. 274–292.
[10] D. Bertrand, "Fonctions modulaires, courbes de Tate et indépendance algébrique", *Semin. Delange–Pisot–Poitou. 19e année. 1977/78,* no. 36.
[11] A. B. Shidlovskiĭ, *Transcendental numbers*, Nauka, Moscow 1987; English transl., Walter de Gruyter, Berlin 1989.
[12] J.-P. Serre, *A course in arithmetic*, Springer-Verlag, New York 1973.
[13] P. Philippon, "Critères pour l'indépendance algébrique", *Publ. Math. IHES* 1986, no. 64, 5–52.
[14] M. Ably, "Résultats quantitatifs d'indépendance algébrique pour les groupes algébriques", *J. Number Theory.* **42**:2 (1992), 194–231.
[15] Yu. V. Nesterenko, "On algebraic independence of algebraic powers of algebraic numbers", *Mat. Sb.* **123 (165)** (1984), 435–459; English transl. in *Math. USSR-Sb.* **51** (1985).
[16] Yu. V. Nesterenko, "Estimates for the number of zeros of certain functions", *New advances in transcendence theory* (A. Baker, ed.), Cambridge Univ. Press, Cambridge 1988, pp. 263–269.
[17] Yu. V. Nesterenko, "Estimates for the number of zeros of functions of certain classes", *Acta Arith.* **LIII**:1 (1989), 29–46.
[18] Yu. V. Nesterenko, "Estimates for the orders of zeros of functions of a certain class and applications in the theory of transcendental numbers", *Izv. Akad. Nauk SSSR Ser. Mat.* **41** (1977), 253–284; English transl. in *Math. USSR-Izv.* **11** (1977).
[19] Yu. V. Nesterenko, "Estimates for the characteristic function of a prime ideal", *Mat. Sb.* **123 (165)** (1984), 11–34; English transl. in *Math. USSR-Sb.* **51** (1985).

Moscow State University
E-mail address: nest@nw.math.msu.su

Received 7/MAR/96
Translated by N. KOBLITZ

Typeset by $\mathcal{A}\mathcal{M}\mathcal{S}$-TEX