Math. Ann. 309, 491–503 (1997)

Mathematische Annalen

Hilbert's irreducibility theorem and G-functions

Pierre Dèbes[1], **Umberto Zannier**[2]

[1] Département de Mathématiques, Université Lille, F-59655, Villeneuve d'Ascq Cedex, France
(e-mail: pde@ccr.jussieu.fr)
[2] Istituto Universita Arch. D.C.A., Santa Croce, 191, I-30135 Venezia, Italy
(e-mail: zannier@cidoc.iuav.unive.it)

Received: 16 September 1996

Mathematics Subject Classification (1997): 11J72, 12E25, 33E20, 33E30

1 Introduction

The present paper arose in connection with the applications of techniques from transcendental number theory in the context of algebraic functions and Hilbert's irreducibility theorem.

Let k be a number field and $f \in k[X, Y]$ be an absolutely irreducible polynomial with $n := \deg_Y(P) \geq 1$. We may view Y as a rational function on the curve defined by f. Hilbert's irreducibility theorem may be restated by saying that for infinitely many $\xi \in k$ the values $1, Y(\xi), \ldots, Y^{n-1}(\xi)$ are k-linearly independent (for any choice of the branch). It is classical that, away from ramification points of X, each branch may be represented as a power series in $\overline{\mathbb{Q}}[[X]]$ which is a G-function. Moreover the vectors $\mathbf{Y} := (1, Y(X), \ldots, Y^{n-1}(X))$, where Y runs through such power series, satisfy a linear differential system over $k(X)$. It seems natural to ask whether such a linear independence result holds in general for vectors of G-functions satisfying similar conditions, where now the values of $\mathbf{Y}$ should be taken for ξ lying in the circle of convergence of the relevant power series with respect to a given absolute value of K. The purpose of the present paper is to provide an affirmative answer.

Special values of G-functions, which go back to Siegel [Sie], have been widely investigated. After some results of Bundschuh [Bun] and Schneider [Sch] in the case of algebraic functions, explicit applications to Hilbert's irreducibility theorem were obtained by Sprindzuk in a series of papers around 1980 (see *e.g.* [Spr]). Later on, Bombieri and Dèbes, working with methods stemming respectively from Siegel's and Gelfond's, obtained certain crucial inequalities which led to independence statements for special values of vectors $(Y_1(X), \ldots, Y_n(X))$ of G-functions satisfying a linear differential system over

$\overline{\mathbb{Q}}(X)$. The results, however, were weaker than those available for E-functions satisfying similar conditions (see *e.g.* [Ba; Chap. 11])[1], and allowed to prove linear independence of values at algebraic arguments only in special cases. For instance, though interesting consequences in the context of algebraic functions were drawn both by Bombieri [Bo1], [Bo2] and Dèbes [De1], [De2], Hilbert's irreducibility theorem did not follow in its full generality by a direct application. The main reason is that the basic inequality of Bombieri and Dèbes is particularly effective when the field generated by the coefficients of the relevant G-functions has "low" degree over the ground field, a condition which is often not true for power expansions of algebraic functions. In certain cases Bombieri managed to overcome this difficulty by replacing the original differential system with a suitable symmetric power of it (see for instance Theorem 5 in [Bo1]), but the assumptions involve algebraic independence conditions that are not satisfied in the case of algebraic functions: some ratio $Y_j(X)/Y_1(X)$ is required to be a transcendental function. In contrast here, we obtain results on *linear independence* over K of values at rational points, assuming *linear independence* over $K(X)$ of the relevant functions.

Around 1986, Dèbes realized that a certain trick introduced by Weissauer [Wei] and Fried [Fr] could be successfully combined with the inequality obtained by him and Bombieri to produce a new complete proof of Hilbert's irreducibility theorem (see *e.g.* [De2]). This method was recently developed to obtain new results on Hilbert's theorem ([De3], [De4], [De5]). Here we follow the same method, supplementing it with the necessary modifications for an application to more general G-functions. The above mentioned difficulty related with the degree of the field of coefficients is completely overcome by this method.

2 Statement of the main result

We first introduce some notation. Let k be a number field, n be a positive integer and $A = A(X)$ be an $n \times n$ matrix with entries $a_{i,j}(X) \in k(X)$. Consider the differential operator $\mathscr{D} := D - A$, where $D := \mathrm{d}/\mathrm{d}X$.

Assume that there is a (column) vector solution $\mathbf{Y} = (Y_1(X), \ldots, Y_n(X))^t$ of $\mathscr{D}\mathbf{Y} = 0$ such that each component $Y_i(X)$ is a power series with coefficients in $\overline{\mathbb{Q}}$. (This holds for example if 0 is an ordinary point of $\mathscr{D}$, that is, if 0 is not a pole of any $a_{i,j}(X)$). The field generated over k by the coefficients of these power series is then necessarily a number field. Here is a brief argument for this more or less standard fact.

Define the order at zero of a vector with entries in $\overline{\mathbb{Q}}[[x]]$ as the minimum order of its entries. Nonzero vectors with pairwise different orders are linearly independent over the constants. Therefore the order of a nonzero vector solution of our system is bounded. That is, there exists a positive integer N such that two vector solutions which agree modulo x^N must in fact be equal. Take now a vector solution $\mathbf{Y}$ with entries in $\overline{\mathbb{Q}}[[x]]$ and let L be the number field generated

[1] In fact equally general results would be false in the case of G-functions [Wol].

by the coefficients of the system and the first N coefficients of all the entries of $\mathbf{Y}$. If $\sigma \in Gal(\overline{\mathbb{Q}}/L)$, then $\sigma(\mathbf{Y})$ is a new vector solution congruent to $\mathbf{Y}$ mod x^N. So the two solutions coincide, thus proving that $\mathbf{Y}$ has coefficients in L.

Fix a number field K containing k and the coefficients of $Y_1(X), \ldots, Y_n(X)$. Assume in addition that $Y_1(X), \ldots, Y_n(X)$ are G-functions (see below for a definition). For each valuation v of K, let R_v denote the (non-zero) v-adic radius of convergence of $\mathbf{Y}$. Then we may regard $\mathbf{Y}$ as a vector function $\mathbf{Y}_v$ on the open ball $B(0, R_v) := \{\xi \in K_v \mid 0 \leq |\xi|_v < R_v\}$ and with values in the completion K_v. We will prove the following

Theorem 1. *If $Y_1(X), \ldots, Y_n(X)$ are linearly independent over $\overline{\mathbb{Q}}(X)$ then, for every positive number $R < R_v$, there exist infinitely many $\xi \in \mathbb{Q} \cap B(0, R)$ such that the elements $Y_{i,v}(\xi)$ of K_v, $i = 1, \ldots, n$, are linearly independent over K.*

The proof will provide a more precise result, stated as Theorem 2 at the end.

Remark 1. More generally, the assumption "$Y_1(X), \ldots, Y_n(X)$ linearly independent over $\overline{\mathbb{Q}}(X)$" can be removed to conclude that there exist infinitely many rational points $\xi \in B(0, R)$ (with $0 < R < R_v$) such that the rank over K of the values $Y_1(\xi), \ldots, Y_n(\xi)$ (we omit here the reference to v, supposed to be fixed) is at least equal to the rank over $\overline{\mathbb{Q}}(X)$ of $Y_1(X), \ldots, Y_n(X)$. Namely, we show below how to deduce the following more general statement from Theorem 1:

(*) *There exists an infinite set $S \subset \mathbb{Q} \cap B(0, R)$ with the following property: if J is any subset of $\{1, \ldots, n\}$ such that the power series $Y_j(X)$ $(j \in J)$ are linearly independent over $\overline{\mathbb{Q}}(X)$, then for all but finitely many $\xi \in S$, the values $Y_j(\xi)$, $j \in J$, are linearly independent over K.*

Observe first that we may renumber indices to suppose that $Y_1(X), \ldots, Y_r(X)$ are linearly independent over $\overline{\mathbb{Q}}(X)$, while we have relations

$$Y_m(X) = \sum_{i=1}^{r} c_{i,m}(X) Y_i(X), \qquad m = 1, \ldots, n \tag{1}$$

where $c_{i,m}(X) \in \overline{\mathbb{Q}}(X)$ for all i, m. Next enlarge the number field K to assume that it contains the coefficients of all the $c_{i,m}(X)$. Relations (1) imply that $(Y_1(X), \ldots, Y_r(X))^t$ satisfies a linear differential system over $K(X)$. Applying Theorem 1 to $Y_1(X), \ldots, Y_r(X)$ yields an infinite set $S \subset \mathbb{Q} \cap B(0, R)$, disjoint from the set of poles of the $c_{i,m}$ and such that, for $\xi \in S$, $Y_1(\xi), \ldots, Y_r(\xi)$ are linearly independent over K.

Let now J be a subset of $\{1, \ldots, n\}$ such that the power series $Y_j(X)$ $(j \in J)$ are linearly independent over $\overline{\mathbb{Q}}(X)$. Then the matrix $c_{i,j}(X)$ $(i = 1, \ldots, r, j \in J)$ has maximal rank. Throwing away a finite subset from S we may assume that the specialized matrix at $\xi \in S$ has still maximal rank, so the $Y_j(\xi)$ $(j \in J)$ are linearly independent over K.

Remark 2. The more precise conclusion in Remark 1 allows to deduce directly the general form of Hilbert's irreducibility theorem involving any number of absolutely irreducible polynomials $f_1, \dots, f_s \in K[X, Y]$. Namely, let Z_i be an algebraic function solution of $f_i(X, Z_i) = 0$ (in some algebraic closure of $k(X)$), $i = 1, \dots, s$. Set $n_i := \deg_Y f_i$, $i = 1, \dots, s$. The vector $\mathbf{Y} := (1, Z_1, \dots, Z_1^{n_1-1}, \dots, 1, Z_s, \dots, Z_s^{n_s-1})$ satisfies a differential system over $K(X)$. After a translation on X if necessary, one may assume that 0 is an ordinary point. Then, each algebraic function Z_i can be expanded in a power series $Z_i \in \overline{\mathbb{Q}}[[X]]$, which is a G-function, $i = 1, \dots, s$. Apply the conclusion in Remark 1, for any choice of v. Since $1, Z_i, \dots, Z_i^{n_i-1}$ are linearly independent over $\overline{\mathbb{Q}}(X)$ for every $i = 1, \dots, s$, we obtain that their values at the elements ξ of an infinite set $S \in \mathbb{Q}$ (the same for all i), are linearly independent over K. This means that, for every $\xi \in S$, $f_i(\xi, Y)$ is irreducible over K, $i = 1, \dots, s$.

3 Auxiliary propositions

Following mainly [An], [De1] and [DGS], we recall some notation and definitions concerning G-functions. Given a number field F denote by M_F (resp. M_F^o) the set of places (resp. finite places) of F. For each $v \in M_F$ denote the absolute value extending the usual one on $\mathbb{Q}$ by $|\cdot|_v$, denote the completion of F at v by F_v and the local degree $[F_v : \mathbb{Q}_v]$ by d_v^F. Then define the local height h_v to be $h_v(x) := \log^+ |x|_v$ (where as usual $\log^+ y = \log \max\{1, y\}$). The Weil logarithmic height is then defined by the following formula: for $\xi \in F$,

$$h(\xi) := \frac{1}{[F : \mathbb{Q}]} \sum_{v \in M_F} d_v^F h_v(\xi)$$

Given a formal power series $Z = \sum_{m=0}^{\infty} c_m X^m \in F[[X]]$, we now define

$$\sigma(Z) := \limsup_{m \to \infty} \frac{1}{m} \sum_{v \in M_F} \frac{d_v^F}{[F : \mathbb{Q}]} \sup_{s \le m} h_v(c_s).$$

Definition 1. *The formal power series Z is said to be a G-function if $\sigma(Y) < \infty$ and if Z is a solution of a linear differential equation with coefficients in $\overline{\mathbb{Q}}(X)$.*

This condition is equivalent to the following ([An; Chap. 1 Sect. 1.3] or [DGS; Chap. 8, Proposition 1.1, p.265]): *Z has a non-zero radius of convergence for each embedding of F in $\mathbb{C}$ and there exist positive integers N_m such that $N_m c_s$, $0 \le s \le m$ are algebraic integers and $N_m < N^m$ for a suitable N and all $m \ge 0$.* Using for instance this characterization it is immediate to prove the following

Lemma 1. *Let $Z \in F[[X]]$ be a G-function and $\alpha, \beta \in F$, $\alpha \neq 0$. Then $Z(\frac{\alpha X}{1-\beta X})$ is a G-function.*[2] *Furthermore, sums and products of G-functions are G-functions.*

[2] Of course we mean the composition of the formal power series z and $\alpha X \sum \beta^m X^m$

Following [An; Chap. 4 Sect. 5] or [DGS; Chap. 7 Sect. 2] we now define the *Galochkin condition* for a linear differential system. Let $B = B(X)$ be an $n \times n$ matrix with entries $b_{i,j}(X) \in F(X)$ and $\mathscr{D}$ be the differential operator $\mathscr{D} := D - B$. Consider the sequence of matrices $B_m = B_m(X)$ defined inductively by

$$\begin{cases} B_0 &= I \\ B_1 &:= B \\ B_{m+1} &= B_m B + \dfrac{\mathrm{d}}{\mathrm{d}X} B_m \end{cases}$$

Plainly each B_m is an $n \times n$ matrix over $F(X)$. For $v \in M_F^o$ set

$$h(m, v) = \max_{s \le m} \log^+ \left| \frac{B_s}{s!} \right|_{v,\mathrm{Gauss}}$$

(For the definition of Gauss norm see [An; Chap. 4 Sect. 1] or [DGS; Chap. 1 Sect. 4]) and

$$\sigma(B) := \limsup_{m \to \infty} \frac{1}{m} \sum_{v \in M_F^o} \frac{d_v^F}{[F : \mathbb{Q}]} h(m, v)$$

and say that $\mathscr{D}$ satisfies the Galochkin condition if $\sigma(B) < \infty$.

From [DGS; Chap. 3, (5.2)] the matrix

$$\mathscr{U}(t, X) := \sum_{m=0}^{\infty} \frac{B_m(t)}{m!} (X - t)^m$$

is the solution of $\mathscr{D}\mathscr{U} = 0$ at the generic point t that satisfies $\mathscr{U}(t) = I$. Then the Galochkin condition is immediately seen to be equivalent to $\mathscr{D}$ being a G-operator, as defined in [De1; p.375, eq.(4)]. We will need the following theorem of Chudnovsky, stated here as Lemma 2.

In Lemma 2 and Lemma 3 below, B is an $n \times n$ matrix with entries in $F(X)$ and $\mathscr{D}$ is the differential operator $\mathscr{D} := D - B$.

Lemma 2. *Let $\mathbf{Z} := (Z_1, \ldots, Z_n)^t \in F[[X]]^n$ be a (column) vector of G-functions satisfying $\mathscr{D}\mathbf{Z} = 0$. Suppose that $Z_1, \ldots, Z_n$ are linearly independent over $\overline{\mathbb{Q}}(X)$. Then $\mathscr{D} = D - B$ satisfies the Galochkin condition.*

Lemma 3. *Assume the differential operator $\mathscr{D}$ satisfies the Galochkin condition. Then the following holds.*

(a) if $\mathbf{Z}$ is a column vector with entries $Z_1, \ldots, Z_n \in \overline{\mathbb{Q}}[[X]]$ such that $\mathscr{D}\mathbf{Z} = 0$, then $Z_1, \ldots, Z_n$ are G-functions.

(b) With $\mathbf{Z}$ as in (a), denote, for each $v \in M_F$, the v-adic radius of convergence of $\mathbf{Z}$ by $R_v(\mathbf{Z})$. Then the operator satisfies Bombieri's condition

$$\sum_{v \in M_F} d_v^F \log^+ \frac{1}{R_v(\mathbf{Z})} < \infty$$

(c) All the singularities of the differential operator $\mathscr{L}$ are regular and have only rational exponents.

Comments on proofs. A proof of Lemma 2 can be found in [An; Chap. 6 Sect. 4] or in [DGS; Chap. 8, Theorem 1.5 p. 268]. Lemma 3 (a) is easy if 0 is an ordinary point (e.g. [De1; Sect. 1.1 Remarque 3]); the general case is proved in [An; Chap. 5 Sect. 6.6]. Lemma 3 (b) is the "Galochkin $\Rightarrow$ Bombieri" part of the Bombieri-André theorem ([An; Chap. 4 Sect. 5.2] or [DGS; Chap. 7 Theorem 2.1]) (the second part of the Bombieri-André theorem is the converse, that is, Bombieri's condition implies Galochkin's condition). Lemma 3 (c) follows from works of Katz and Honda ([An; Chap. 4 Sect. 5.3] or [DGS; Chap. 3 and p. 228]). □

For the convenience of the reader we now briefly recall some well-known facts about monodromy of linear differential systems (see *e.g.* [DGS; p.101]). Consider the differential system

$$\frac{\mathrm{d}}{\mathrm{dX}}\mathbf{Z} = B\mathbf{Z}$$

where B is now a matrix of meromorphic functions in a neighborhood I of z_0, such that z_0 is the only (possibly) singular point of B in I. For $z \in I' := I \setminus \{z_0\}$ we have a matrix solution $\mathscr{U}$ of the above system such that its column vectors are analytic functions at z, linearly independent over $\mathbb{C}$. Starting with a given point $z = z_1 \in I$, we can analytically continue such a matrix along a closed loop γ at z, entirely contained in I' and wrapping once, counterclockwise, around z_0. After analytic continuation along the whole γ we obtain another matrix solution of the same system, denoted $T(\mathscr{U})$, where T is the so-called monodromy map. Necessarily $T(\mathscr{U})$ will be of the form $\mathscr{U}C$ for some constant non-singular matrix C (which depends on $\mathscr{U}$ in general). Now, letting A be a constant matrix such that $\exp(2\pi iA) = C$ and setting

$$\begin{cases} (X - z_0)^A & := & \exp(A\log(X - z_0)) := \displaystyle\sum_{s=0}^{\infty} \frac{(A\log(X - z_0))^s}{s!} \\ W & := & \mathscr{U}(X - z_0)^{-A} \end{cases} \tag{1}$$

it can be checked that W has trivial monodromy around z_0, *i.e.*, remains unchanged after analytic continuation along γ (essentially the reason is that the monodromy of $(X - z_0)^A$ is $\exp(2\pi iA) = C$, *i.e.*, the same as $\mathscr{U}$). Hence the entries of W are analytic in I'. Now it is known (or may be taken as definition) that the system has a regular singularity at z_0 precisely if W has at worst a pole as a singularity at z_0.

Assume that is the case and fix a determination of $\log(X - z_0)$, *e.g.* in the domain $I'' := I' \setminus \{z_0 + t \mid t \in \mathbf{R}^+\}$. Then, considering for instance a Jordan form of A, it easily follows from (1) that each entry of the matrix $\mathscr{U}$ is a linear combination of functions of the form

$$(\log(X - z_0))^a \cdot (X - z_0)^\alpha w(X)$$

where $a \in \mathbb{N}$, $\alpha \in \mathbb{C}$ and where w is analytic in I. It follows that, if ϕ is any rational function in X and in the entries of $\mathscr{U}$, then ϕ is a quotient of linear combinations of the same type. This proves that near z_0 we have a bound

$$|\phi(X)| \ll |X - z_0|^{-N}$$

for some integer N. Suppose now that ϕ has trivial monodromy, namely suppose that it remains unchanged after analytic continuation along any loop γ in I', wrapping around z_0, as above. Then ϕ is single valued and analytic in I' whence, *e.g.* by Riemann's removable singularities theorem (*e.g.* [For; p.5]) applied to $(X - z_0)^N \phi(X)$, the above inequality implies that it has at worst a pole at z_0.

Fix now an ordinary point P_o of $\mathscr{D}$ and let $\mathscr{U}$ be a solution matrix at P_o as above. Let $P_1, \ldots, P_s$ be the singular points of $\mathscr{D}$ on the Riemann sphere $\mathbf{S}$ and fix non-intersecting paths $\lambda_1, \ldots, \lambda_s$ from P_o near $P_1, \ldots, P_s$. Next, for each $i = 1, \ldots, s$, define a loop γ_i based at P_o, constructed by traveling first along λ_i from P_o near P_i, then wrapping once along a "small" loop around P_i, then finally go along λ_i^{-1}, back to P_o. Classically the loops $\gamma_1, \ldots, \gamma_s$ generate the fundamental group of $\mathbf{S} \setminus \{P_1, \ldots, P_s\}$. We may then define the monodromy around P_i of any rational function ϕ in X and in the entries of $\mathscr{U}$ by analytic continuation along γ_i, $i = 1, \ldots, s$. From the above we can deduce at once the following

Lemma 4. *Let $\mathscr{D} := D - B$ be a differential operator with only regular singularities. Let $\mathscr{U}$ be a solution matrix at some ordinary point and let ϕ be a rational function in X and in the entries of $\mathscr{U}$. Suppose that ϕ has trivial monodromy around any singular point of $\mathscr{D}$. Then ϕ is a rational function.*

Proof. By the above arguments ϕ is then analytic in the whole Riemann sphere, made exception for finitely many points, where it has at most a pole as a singularity. We recall a classical argument to prove the rationality of ϕ. Let $z_1, \ldots, z_r$ be the finite singular points of ϕ and consider the function $\Phi := \phi \prod_{i=1}^{r} (z - z_i)^N$, where N is a sufficiently large integer such that Φ is bounded around each z_i. By Riemann's removable singularities theorem, Φ is entire and, having at most a pole at ∞, must be a polynomial. □

Lemma 5. *Let $\mathbf{Z} := (Z_1, \ldots, Z_n)^t \in F[[X]]^n$ be a (column) vector of G-functions satisfying $\mathscr{D}\mathbf{Z} = 0$. Suppose that $Z_1, \ldots, Z_n$ are linearly independent over $\overline{\mathbb{Q}}(X)$. For each loop γ in the group Γ generated by $\gamma_1, \ldots, \gamma_s$, denote by $\mathbf{Z}^{(\gamma)} := (Z_1^{(\gamma)}, \ldots, Z_n^{(\gamma)})^t$ the vector obtained from $\mathbf{Z} := (Z_1, \ldots, Z_n)^t$ by analytic continuation along γ. Then the linear space spanned over $\mathbb{C}$ by all the vectors $\mathbf{Z}^{(\gamma)}$ has dimension n.*

Proof. Plainly we have $\mathscr{D}\mathbf{Z}^{(\gamma)} = 0$ for all $\gamma \in \Gamma$, so the dimension of the space in question is at most n. To complete the proof we show below that there exist n vectors of the form $\mathbf{Z}^{(\gamma)}$ with $\gamma \in \Gamma$ that are linearly independent over $\mathbb{C}$.

The entries $Z_1, \ldots, Z_n$ of $\mathbf{Z}$ span a linear space over $\mathbb{C}(X)$ which is in fact a differential module M in an obvious way. Namely, since the entries $Z_1, \ldots, Z_n$

of $\mathbf{Z}$ are linearly independent over $\overline{\mathbb{Q}}(X)$, whence over $\mathbb{C}(X)$ (since they have algebraic coefficients), M is isomorphic to the differential module over $\mathbb{C}(X)$ with basis $e_1,\dots,e_n$ and derivation given by $D(e_1,\dots,e_n)^t := B(e_1,\dots,e_n)^t$. From the theorem of the cyclic vector [DGS; Chap. 3, Theorem 4.2], there exists then $m \in M$ such that $m, Dm, \dots, D^{n-1}m$ are linearly independent over $\mathbb{C}(X)$. Write $m = \sum_{i=1}^n R_i(X)Z_i$, where $R_1,\dots,R_n$ are rational functions. We may assume that $\gamma_1,\dots,\gamma_s$ do not contain any pole of any such function, so we may analytically continue m along any $\gamma \in \Gamma$ to obtain functions near P_o of type $\sum_{i=1}^n R_i(X)Z_i^{(\gamma)}$. Consider the space spanned over $\mathbb{C}$ by all such functions and select h of them, say $m_1,\dots,m_h$ (with $m_1 = m$), which constitute a basis. We may write $m_j = \sum_{i=1}^n R_i(X)Z_i^{(j)}$, where the vectors $\mathbf{Z}^{(j)} := (Z_1^{(j)},\dots,Z_n^{(j)})^t$, $j = 1\dots,h$, are linearly independent elements of the space generated over $\mathbb{C}$ by the $\mathbf{Z}^{(\gamma)}$, $\gamma \in \Gamma$ [3]. It suffices to prove that $h = n$. For this consider the differential operator defined by

$$\mathbf{W}(Y) := \frac{W(Y, m_1,\dots,m_h)}{W(m_1,\dots,m_h)}$$

where W is the Wronskian and Y is a differential indeterminate. We may write

$$\mathbf{W}(Y) = D^h Y + \phi_1 D^{h-1}Y + \cdots + \phi_h$$

where the ϕ_is are rational functions in the m_is and their derivatives. In particular the ϕ_is are rational functions of X and of the entries of some solution matrix of $\mathscr{D}\mathscr{U} = 0$ at P_o.

Let $\gamma \in \Gamma$. We observe that analytic continuation along γ of $m_1,\dots,m_h$ produces, by assumption, functions $\tilde{m}_1,\dots,\tilde{m}_h$ which generate the same linear space over $\mathbb{C}$. Namely we can write $\tilde{m}_j = \sum_i c_{i,j}m_i$ for an invertible matrix $(c_{i,j}) \in GL_h(\mathbb{C})$. Using the very definition of the Wronskian as a determinant, we see that replacing $m_1,\dots,m_h$ respectively with $\tilde{m}_1,\dots,\tilde{m}_h$ in the definition of $\mathbf{W}(Y)$ merely multiplies the coefficients of the numerator (as a polynomial in Y) by $\det(c_{i,j})$ and the same holds for the denominator. This shows that the coefficients $\phi_1,\dots,\phi_h$ are left fixed by analytic continuation along any $\gamma \in \Gamma$, so they have trivial monodromy. Since our operator satisfies the Galochkin condition (Lemma 2), it has only regular singularities (Lemma 3). We may thus apply Lemma 4 and obtain that $\phi_1,\dots,\phi_h$ are rational functions. Since $\mathbf{W}(m) = 0$ we obtain that $m, Dm, \dots, D^h m$ are linearly dependent over $\mathbb{C}(X)$, so $h \geq n$ whence in fact $h = n$. □

Let now $\mathscr{D}_1 := D - A_1, \mathscr{D}_2 := D - A_2$ be operators over $F(X)$ as above, of respective orders n_1 and n_2. Denote respectively by Σ_1 and Σ_2 their singular set. For $i = 1, 2$, let $\mathbf{Y}^{(i)} := (Y_1^{(i)},\dots,Y_{n_i}^{(i)})^t \in F[[X]]^{n_i}$ be a column vector solution of $\mathscr{D}_i\mathbf{Y}^{(i)} = 0$ and assume that the entries $Y_1^{(i)},\dots,Y_{n_i}^{(i)}$ are G-functions linearly independent over $\overline{\mathbb{Q}}(X)$. Form the column vector $\mathbf{Z}$ with entries (in some order) the n_1n_2 power series $Y_a^{(1)}Y_b^{(2)}$, $a = 1,\dots,n_1$, $b = 1,\dots,n_2$. We have then the following

[3] Since m is a cyclic vector, the $\mathbf{z}^{(j)}$ actually constitute a basis of the space in question.

Lemma 6. *The vector* $\mathbf{Z}$ *has* G*-functions entries and satisfies a differential system over* $F(X)$ *of order* $n_1 n_2$ *and with singular set contained in* $\Sigma_1 \cup \Sigma_2$*. If in addition* Σ_1 *and* Σ_2 *are disjoint, then the entries of* $\mathbf{Z}$ *are also linearly independent over* $\overline{\mathbb{Q}}(X)$*.*

Proof. The first assertions follow from Lemma 1 and from a trivial inspection, after differentiating $Y_a^{(1)} Y_b^{(2)}$ (actually, the new system, which is the tensor product of the original ones, corresponds to the matrix $A_1 \otimes A_2$). To complete the proof, suppose given a relation of linear dependence

$$\sum_{a,b} R_{a,b}(X) Y_a^{(1)} Y_b^{(2)} = 0 \tag{2}$$

where the $R_{a,b}$ are rational functions with coefficients in $\overline{\mathbb{Q}}$. Construct loops $\gamma_1, \ldots, \gamma_s$ as before around the singular points of the operator $\mathscr{D}_1$, such that no singularity of any $R_{a,b}$ or of $\mathscr{D}_2$ lies on any such loop or in its interior (made exception possibly for poles of some $R_{a,b}$ coinciding with a singularity of $\mathscr{D}_1$). We may then analytically continue each entry of $\mathbf{Z}$ along any such path. Both the rational functions and the terms $Y_b^{(2)}$ will remain unchanged, while the vector $\mathbf{Y}^{(1)}$ will be transformed into another vector solution of the first differential system. Plainly the relation (2) still holds after replacing the terms $Y_a^{(1)}$ with the corresponding entries of the new solution. Since, from Lemma 5, analytic continuation produces n_1 linearly independent solutions of the first system, we obtain some relations

$$\sum_{a,b} R_{a,b}(X) Y_{\mu,a} Y_b^{(2)} = 0$$

where now $\mathbf{Y}_\mu := (Y_{\mu,1}, \ldots, Y_{\mu,n_1})^t$, $\mu = 1, \ldots, n_1$, are column vector solutions of the first system which are linearly independent over $\mathbb{C}$. The determinant $\det(Y_{\mu,a})$ does not vanish in a neighborhood of P_o. Hence we have

$$\sum_b R_{a,b}(X) Y_b^{(2)} = 0$$

for each $a = 1, \ldots, n_1$. However the power series $Y_b^{(2)}$ are assumed to be linearly independent over $\overline{\mathbb{Q}}(X)$. Therefore $R_{a,b} = 0$ for all a, b. □

Remark 3. *(a)* Since the fundamental group $\pi_1(\mathbf{S} \setminus \{P_1, \ldots, P_s\})$ is generated by any $s - 1$ loops out of $\gamma_1, \ldots, \gamma_s$, the monodromy is in fact determined by all loops but one. This implies that the lemma continues to hold if Σ_1 and Σ_2 are assumed to intersect in at most one point. Lemma 6 generalizes the fact that algebraic functions fields in one variable with disjoint sets of ramification points of X are linearly disjoint over $\mathbb{C}(X)$.

(b) Y. André and D. Bertrand mentioned to us that Lemma 5 and Lemma 6 could also be proved by invoking the theory of Picard-Vessiot extensions and using the action of the differential Galois group instead of the monodromy action.

By induction we obtain at once the following

Corollary 1. *For $j = 1, \dots, r$, let $\mathscr{D}_j := D - A_j$, be an operator over $F(X)$ as above, of order n_j and with singular set Σ_j. Assume that the sets $\Sigma_1, \dots, \Sigma_r$ are pairwise disjoint. Let $\mathbf{Y}^{(j)} := (Y_1^{(j)}, \dots, Y_{n_j}^{(j)})^t$ be a column vector solution of $\mathscr{D}_j \mathbf{Y}^{(j)} = 0$, the entries of which are G-functions in $F[[X]]$, linearly independent over $\overline{\mathbb{Q}}(X)$, $j = 1, \dots, r$. Form the column vector $\mathbf{Z}$ with entries (in some order) the $n_1 \cdots n_r$ power series $Y_{a_1}^{(1)} \cdots Y_{a_r}^{(r)}$, $a_1 = 1, \dots, n_1$, ..., $a_r = 1, \dots, n_r$. Then the vector $\mathbf{Z}$ has G-functions entries (over F) and satisfies a differential system of order $n_1 \cdots n_r$ over $F(X)$ and with singular set contained in $\Sigma_1 \cup \ldots \cup \Sigma_r$. Furthermore the entries of $\mathbf{Z}$ are linearly independent over $\overline{\mathbb{Q}}(X)$.*

4 Proof of Theorem 1

Consider, given an homography (linear fractional transformation) $\tau(X) = \frac{\alpha X}{1-\beta X}$, the vector $\mathbf{Y}^\tau := \mathbf{Y}(\tau(X))$. It satisfies the system defined by the operator

$$\mathscr{D}^\tau := D - \frac{\alpha}{(1-\beta X)^2} A(\tau(X))$$

If Σ is the set of singular points of $\mathscr{D}$, then the set of singular points of $\mathscr{D}^\tau$ is contained in $(\tau^{-1}(\Sigma)) \cup \{1/\beta\}$. For every positive integer r, pick $2r$ algebraic numbers $\alpha_1, \dots, \alpha_r, \beta_1, \dots, \beta_r \in K^\times$ such that, setting $\tau_j(X) = \frac{\alpha_j X}{1-\beta_j X}$, the systems defined by $\mathscr{D}_j := \mathscr{D}^{\tau_j}$, $j = 1, \dots, r$ have singular sets $\Sigma_1, \dots, \Sigma_r$ that are pairwise disjoint. The entries of the vectors $\mathbf{Y}^{(j)} := \mathbf{Y} \circ \tau_j$ are G-functions over K (Lemma 1) and are linearly independent over $\overline{\mathbb{Q}}(X)$, $j = 1, \dots r$. As in the corollary to Lemma 6, form the vector $\mathbf{Z}$ with entries (in some order) the n^r G-functions $Y_{a_1}^{(1)} \cdots Y_{a_r}^{(r)}$, $a_1 = 1, \dots, n$, ..., $a_r = 1, \dots, n$. From the above corollary such entries (which have coefficients in K) are linearly independent over $\overline{\mathbb{Q}}(X)$. The vector $\mathbf{Z}$ satisfies a differential system defined by $\mathscr{D} := D - B$, where B is a square matrix over $K(X)$ of order n^r. Such system satisfies the Galochkin condition, by the theorem of Chudnovski (the present Lemma 2). Also, by Lemma 3, if we denote by R_v^* the v-adic radius of convergence of $\mathbf{Z}$, we have

$$\sum_{v \in M_K} d_v^K \log^+ \frac{1}{R_v^*} < \infty.$$

We are in position to apply to $\mathbf{Z}$ the "*Théorème principal*" of [De1; p.378]. We apply that theorem (with $k = K$) to the entries Z_i of $\mathbf{Z}$, thus replacing n with n^r. Also, we select one absolute value v of K and consider the values of the power series Z_i with respect to the v-adic convergence. In our situation the statement of that theorem reads:

Let $\xi \in K^\times$ be such that $|\xi|_v < \min(1, R_v^*)$, $\rho > 0$ an integer, $\Lambda := (\lambda_{i,j})$ a $\rho \times n^r$ matrix over K of rank ρ. Assume that

$$\sum_{j=1}^{n^r} \lambda_{i,j} Z_{j,v}(\xi) = 0, \qquad i = 1, 2, \ldots, \rho. \tag{3}$$

Then we have this inequality

$$\frac{d_v^K}{[K:\mathbb{Q}]} \log |\xi|_v + \frac{n^r - \rho}{n^r}\, h(\xi) \geq -C_1 - C_2\sqrt{h(\xi)} \tag{4}$$

where C_1, C_2 do not depend on ξ.

Assume now that, for $j = 1, \ldots, r$, the values $Y_{1,v}^{(j)}(\xi), \ldots, Y_{n,v}^{(j)}(\xi)$ are linearly dependent over K. Thus they span a linear space of dimension $\leq n-1$ over K. Clearly if this holds for all $j = 1, \ldots, r$, then the values $Y_{a_1,v}^{(1)}(\xi) \cdots Y_{a_r,v}^{(r)}(\xi)$, for $1 \leq a_1, \ldots, a_r \leq n$, span a linear space of dimension $\delta \leq (n-1)^r$. These values are precisely the values $Z_{j,v}(\xi)$, $j = 1, \ldots, n^r$, in some order. Thus we can take $n^r - \rho \leq (n-1)^r$ in (4), whence

$$\frac{d_v^K}{[K:\mathbb{Q}]} \log |\xi|_v + \left(\frac{n-1}{n}\right)^r h(\xi) \geq -C_1 - C_2\sqrt{h(\xi)} \tag{5}$$

Choose now real numbers c, R, such that $0 < c < 1$, $0 < R < R_v^*$ and consider the set

$$K_{c,R} := \{\xi \in K \mid \log |\xi|_v \leq -ch(\xi) \text{ and } |\xi|_v < R\} \tag{6}$$

Plainly $K_{c,R} \cap \mathbb{Q}$ is infinite, for all c, R as above. Combining (5) and (6) we obtain that for all $\xi \in K_{c,R}$,

$$\left(\frac{n-1}{n}\right)^r \geq \frac{cd_v^K}{[K:\mathbb{Q}]} + O\left(\frac{1}{\sqrt{h(\xi)}}\right) \tag{7}$$

Therefore, if r, c have been chosen such that $\left(\frac{n-1}{n}\right)^r < c/[K:\mathbb{Q}]$, (7) implies that the set of ξ which verify our assumptions has bounded height, whence is a finite set. Conclude that for all $\xi \in K_{c,R}$ outside this finite set, there exists at least one index $j = 1, \ldots, r$ such that the values $Y_{1,v}^{(j)}(\xi), \ldots, Y_{n,v}^{(j)}(\xi)$ are linearly independent over K.

Observe finally that, though R_v^* will be generally smaller than R_v (*i.e.*, the radius of convergence of the original vector $\mathbf{Y}$), we may insure, by a suitable choice of the numbers α_j, β_j, that $R_v = R_v^*$: in fact

$$R_v^* \geq \min\{R_v, \frac{R_v}{|\alpha_j|_v}, \frac{1}{|\beta_j|_v}, j = 1, \ldots, r\}$$

so it suffices to take $|\alpha_j|_v \leq 1$ and $|\beta_j|_v \leq 1/R_v$, $j = 1, \ldots, r$. □

The proof of Theorem 1 is complete. Taking also into account Remark 1, we may recapitulate and state more precisely what we have actually proved.

Theorem 2. *Let k be a number field, n be a positive integer and $A = A(X)$ be an $n \times n$ matrix with entries in $k(X)$. Let $\mathscr{D}$ be the differential operator $\mathscr{D} := D - A$. Let $\mathbf{Y} = (Y_1(X), \dots, Y_n(X))^t$ be a vector solution of $\mathscr{D}\mathbf{Y} = 0$ such that each entry $Y_i(X)$ is a G-function with coefficients in a number field $K \supset k$.*

Fix a valuation v of K and a real number $R > 0$ smaller than the (non-zero) v-adic radius of convergence of $\mathbf{Y}$. Let r and c be positive real numbers such that $0 < c < 1$ and $\left(\frac{n-1}{n}\right)^r < c$.

Then there exist r homographies $\tau_1(X), \dots, \tau_r(X)$ with the following property. There exists a real number H such that, if ξ is any element of K satisfying

$$\begin{cases} \log|\xi|_v & \leq -ch(\xi) \\ |\xi|_v & < R \\ h(\xi) & > H \end{cases}$$

then there exists at least one index $j = 1, \dots, r$ for which the rank over K of the values $Y_{1,v}(\tau_j(\xi)), \dots, Y_{n,v}(\tau_j(\xi))$ is greater or equal to the rank over $\overline{\mathbb{Q}}(X)$ of $Y_1(X), \dots, Y_n(X)$.

We have this further conclusion. Denote the singular set of the operator $\mathscr{D} := D - A$ by Σ. Then $\tau_1(X), \dots, \tau_r(X)$ can be taken to be any r homographies of the form $a_j X/(1 - b_j X)$ with a_j, b_j non-zero elements of K such that $|a_j|_v \leq 1$, $|b_j|_v \leq 1/R$ and such that the sets $\Sigma_j := \tau_j^{-1}(\Sigma) \cup \{1/b_j\}$, $j = 1, \dots, r$, are pairwise disjoint.

We finally note that all constants involved in the above estimates are effective.

Acknowledgement. We wish to thank Y. André and D. Bertrand for their interest in our paper and many valuable suggestions.

References

[An] Y. André: G-functions and geometry, Vieweg, 1989.
[Ba] A. Baker: Transcendental Number Theory, Cambridge University Press, 1975.
[Bo1] E. Bombieri: On G-functions, Recent progress in analytic number theory, H. Halberstam and C. Hooley eds. Academic Press (1981), **2**, 1–67.
[Bo2] E. Bombieri: On Weil's "Théorème de Décomposition", Amer. J. Math., **105**, (1983), 295–308.
[Bun] P. Bundschuh: Une nouvelle application de la méthode de Gel'fond, Sém. Delange-Pisot-Poitou, Théorie des Nombres, **42**, 19ème année, (1977/78).
[De1] P. Dèbes: G-fonctions et théorème d'irreductibilité de Hilbert, Acta Arith., **47**, (1986), 371–402.
[De2] P. Dèbes: Résultats recents liés au théorème d'irréductibilité de Hilbert, in Séminaire de Théorie des Nombres, Paris 1985-86, C. Goldstein ed., Progress in Mathematics, **71**, 19–37, Birkhäuser, Boston, 1988.
[De3] P. Dèbes: Hilbert subsets and s-integral points, Manuscripta Mathematica, **89**, (1966), 107–137.
[De4] P. Dèbes: On a problem of Dvornicich and Zannier, Acta Arith., **73**, 4 (1995), 379–387.
[De5] P. Dèbes: Density results for Hilbert subsets, preprint (1994).
[DGS] B. Dwork, G. Gerotto, F. Sullivan: An introduction to G-functions, Princeton University Press, 1994.

[Fr] M. Fried: On the Sprindzuk-Weissauer approach to universal Hilbert subsets, Israel J. Math., 51-4 (1985).
[For] O. Forster: Lectures on Riemann Surfaces, Springer Verlag, GTM 81, New York, 1981.
[Sch] T. Schneider: Rationale Punkte über eine algebraischen Kurve, Sém. Delange-Pisot-Poitou, Théorie des Nombres, 15ème année, (1973/74), no 20.
[Sie] C. L. Siegel: Über einige Anwendungen diophantischer Approximationen, Gesammelte Abhandlungen, **I**, pp 209–266, Springer-Verlag, (1966).
[Spr] V. G. Sprindzuk: Arithmetic specializations in polynomials, J. Reine Angew. Math., **340** (1983), 26–52.
[Wei] R. Weissauer: Der Hilbertsche Irreduzibilitätssatz, J. Reine Angew. Math., **334**, (1982), 203–220.
[Wol] J. Wolfart: Werte hypergeometrischer Funktionen, Invent. math., **92**, (1988), 187–216.