PACIFIC JOURNAL OF MATHEMATICS
Vol. 140, No. 1, 1989

ALGEBRAIC INDEPENDENCE OF SOLUTIONS OF DIFFERENTIAL EQUATIONS OF THE SECOND ORDER

MICHEL BRESTOVSKI

We deal with second order algebraic differential equations obtained by equating exact and logarithmic derivatives. Under the assumption that such an equation has no "first integral" (which is proven in particular cases), it is shown that two generic solutions can be algebraically independent only if they satisfy a "very special" relation. Whence is deduced the existence of an infinite algebraically free set of generic solutions over a constant differential field.

1. Introduction. Let P be a differential polynomial with coefficients in an *ordinary differential field k of characteristic zero* (in short: d.f.). Suppose that P is of the order $N > 0$ and irreducible (i.e. P is in $k[X, X', \ldots, X^{(N)}]$ and is irreducible in this UFD). We are concerned with the following algebraic questions, which are to be made more precise later.

I. *Does the equation $P = 0$ admit a "first integral"* (within the frame of differential algebra)?

In this paper, we prove that the answer is negative for equations of order 2 in a certain class; furthermore, if such an equation is "the minimal equation" over k of a non-constant element x (see infra for definitions), then it remains so for x over any d.f. extension K of k over which x is not algebraic (see Theorem 1 and Corollary).

As a consequence, the adjunction of such an element to k introduces no transcendental constant; in classical terms, this means that the general solution of this second order equation is not even parametrized by one arbitrary constant.

II. *Suppose $P = 0$ has these properties. What can be said in terms of algebraic independence over k, of the solutions of $P = 0$ in some differentially closed extension of k, e.g. in a differential closure $\hat{k}$ of k?* (See Section 3.)

In case k is a finite d.f. extension of the prime d.f. $\mathbb{Q}$, this problem is related to the classification of countable differentially closed fields, which is discussed in [8].

We consider second order equations $P = 0$ of a certain class (which contains the previous one, so that the requirements mentioned in II are fulfilled in the small class) and we prove that, if $P = 0$ is the minimal equation of x and y over k, then the algebraic dependence of x and y over k must be of a "very special" kind (see Theorem 2).

The result enables us to construct, in a differential closure $\hat{C}$ of a d.f. C of *constants*, a countable set of solutions of the given equation, which are algebraically independent over C.

A key tool in this study is the exterior algebra of the vector space of the so-called Kähler differentials and the fact that, in the case of a d.f. extension K/k, it can be provided with a structure of differential K-vector space (Section 6).

We give relevant definitions, state our results precisely and make some comments.

2. Forking. Given a d.f. k and an element x in some extension of k, the set $t(x/k)$ of all differential polynomials with coefficients in k which vanish at x is called the *type of x over k*. If we denote by $k[X]_d$ the (differential) ring of these differential polynomials, $t(x/k)$ is easily seen to be a prime differential ideal of $k[X]_d$. Conversely, every prime differential ideal p of $k[X]_d$ is the type over k of some element x (take x to be the coset of X in the residue-domain $k[x]_d = k[X]_d/p$; the quotient field $k(x)_d$ is an extension of k and obviously $t(x/k) = p$); this is the reason why prime differential ideals of $k[X]_d$ are also called *types* (in one variable) *over k*, the description of which is therefore of particular interest.

For P in $k[X]_d$, we denote by $(P)_d$ the differential ideal generated by P in $k[X]_d$. Recall the differential ring structure on $k[X]_d$; if P is of order N, then its derivative is:

$$P' = P^* + X^{(N+1)}S(P) + \sum_{i=0}^{N-1} X^{(i+1)}\partial_i P, \tag{1}$$

where P^* is the polynomial obtained from P by replacing each coefficient by its derivative, ∂_i is the usual (k-linear) derivation with respect to $X^{(i)}$ and $S(P) = \partial_N P$ is the *separant* of P. Now suppose P is irreducible and let $I(P;k)$ be the set of all F in $k[X]_d$ such that $S(P)^n F$ is in $(P)_d$ for n large enough; then it is known ([**5**], [**6**] or [**9**]) that $I(P;k)$ *is a type over k*, and conversely, *every type over k is of this form*. The proof also yields the following properties: *both $(P)_d$ and $I(P;k)$ contain no non-zero elements of order less than N and their*

elements of order N are divisible by P; also $I(P;k)$ is the smallest type over k which contains P but not $S(P)$.

Let $p = I(P;k)$ be a type over k and x an element in some extension of k; x is a *solution of p* if $t(x/k)$ contains p; if they are equal, x is a *generic solution of p*. If $P(x) = 0$, we call x a *zero of P*; if in addition $S(P)(x) \neq 0$, x is *non-singular.* Since the irreducible P associated to p is unique (up to multiplication by a non-zero element in k), we shall refer to P (resp. to $P = 0$) as *the minimal polynomial* (resp. *the minimal equation*) of the type p or, of a generic solution x of p; in this case, the degree of transcendency (t.d.) of $k(x)_d$ over k is the order of p (i.e. of P). Note that a zero of P need not be a solution of p and that the additional condition that x is non-singular is sufficient but not necessary; actually, the question of determining when a singular zero of P is a solution of p constitutes the so-called Ritt Problem (see [6]).

Here is our first result.

THEOREM 1. *Let C be a d.f. of constants. Let $f, g, A, B \in C[X]$, where B/A is a linear combination of logarithmic C-derivatives: $B/A = \sum_{i=1}^{n} c_i(\partial h_i/h_i)$, with c_i in C linearly independent over $\mathbb{Q}$ and h_i non-constant rational functions in $C(X)$, and let $F = X'f + g$. Then over any d.f. extension K of C, the only type of order 1 which contains $P = AF' - X'B$ is $I(X';K)$*

(Here, ∂ stands for ∂_0.) The proof will be given in Section 5.

To interpret this, we introduce the notion of *forking.* Let K/k be a d.f. extension and p a type over k; an *extension of p over K* is a type q over K, the restriction of which to k is p: $q \cap k[X]_d = p$; q is *non-forking* if it has the same order as p. It is not difficult to find the non-forking extensions of p: they are the $I(Q;K)$ for all irreducible factors Q over K of the minimal polynomial of p. When q is a *forking* extension of p (i.e. of lower order), we also say that *q forks over k.*

A non-algebraic type (i.e. of positive order) p clearly admits at least one forking extension, namely: $I(X - x; k(x)_d)$, where x is a generic solution of p. As the property of being a forking extension is transitive, we are led to contemplate the maximal number of successive forking extensions of p, which is called the *forking rank* $\mathrm{RU}(p)$ *of p* (and was first introduced in a broader model-theoretic context by Lascar [7]). If p is of order N, we have $1 \leq \mathrm{RU}(p) \leq N$ for $N > 0$, while $\mathrm{RU}(p) = 0$ for $N = 0$. Moreover, an induction on the order proves that *the forking rank is preserved under non-forking extensions.*

COROLLARY. *Let k be a d.f. and C its constants. Let P be as in Theorem* 1 *and suppose P is irreducible over C.*

Then P is irreducible over k, $p = I(p;k)$ is of order 2, *but its forking rank is* 1. *Moreover, the finite system of equations and inequations $\mathscr{S}(X) = (P(X) = 0, X' \neq 0)$ defines the generic solution of the restriction $I(P;C)$ of p to C.*

Proof. Since P is with constant coefficients, so is each irreducible factor of P over k (up to multiplication by a non-zero element in k); hence P remains irreducible over k.

Theorem 1 proves that for any extension K of k, the only type over K of order 1 that can be a forking extension of p is $I(X';K)$; but this is not an extension of p since its restriction to k is $I(X';k)$. Therefore p has no forking extension of order 1, which means $\mathrm{RU}(p) = 1$.

But we have more, for if x is a zero of P, then P is in $t(x/k)$, so by Theorem 1, $t(x/k)$ is either $I(X';k)$ or algebraic or a second order type which contains P. Now, if in addition x is transcendental over k and non-constant, $t(x/k)$ is of order 2, contains P and therefore its minimal polynomial divides P; but P is irreducible, so eventually $t(x/k) = p$. In other words: a transcendental element over k which satisfies $\mathscr{S}(X)$ is a generic solution of p. The following known result is needed for the end of the proof and elsewhere.

LEMMA 1. *If an element is algebraic over a d.f. of constants, then it is constant.*

Finally we see that the condition $x' \neq 0$ ensures that x is transcendental over C; therefore a non-constant zero of P is a generic solution of $I(P;C)$. □

It is well known that a *linear* (homogeneous) equation $L = 0$ of order N admits a fundamental system of N solutions (their wronksian is non-zero) such that the solutions of $L = 0$ are the linear combinations with *arbitrary* constant coefficients of these N solutions. Let k be a d.f. in which the coefficients of L lie, and let l be the type over k of minimal equation $L = 0$; it is easy to find N successive forking extensions of l, e.g. by adjoining successively N constants algebraically independent over k. In other words, *the forking rank equals the order.*

The same is true for a type of order N which contains some linear polynomial of order $N+n$, for its general solution is then parametrized by $N + n$ constants among which exactly N can be supposed algebraically independent over k.

Nevertheless, Poizat remarked in [9] that the type of minimal equation $X'' = X'/X$ (which is "integrated" in $X' = \log X +$ constant) has forking 1, although it is of order 2. According to Theorem 1, the same holds for the following equations which generalize the latter: $(X'f + g)' = \sum c_i h_i'/h_i$.

3. Constants. Another consequence of Theorem 1 is the "stability" of constants; however this is a more general property.

PROPOSITION 1. *Let p be a type over k, of order $N > 1$, and x a generic solution of p. If* $\mathrm{RU}(p) = 1$, *then the constants of $k(x)_d$ are algebraic over the constants C of k.*

LEMMA 2. *Let K/k be a d.f. extension, $\mathscr{C}/C$ the corresponding extension of their constant subfields. Then $\mathscr{C}$ and k are linearly disjoint (or free) over C.*

That is: *if a constant c of K is algebraic over k, then c is algebraic over C.* Indeed, let $c^n + \lambda_{n-1}c^{n-1} + \cdots + \lambda_0 = 0$ be the minimal equation of c over k ($\lambda_i \in k$); differentiate it: $\lambda'_{n-1}c^{n-1} + \cdots + \lambda'_0 = 0$, which must be trivial by minimality of n, i.e. $\lambda'_{n-1} = \cdots = \lambda'_0 = 0$.

Thus, it is enough for proving Proposition 1 to show that any constant c of $k(x)_d$ is algebraic over k. If c were transcendental, then $k(c)$ would be a d.f. extension of k, and t.d. $k(c)/k = 1$. Now $(k(c))(x)_d = k(x)_d$ and we have: $N =$ t.d. $k(x)_d/k =$ t.d. $k(x)_d/k(c) +$ t.d. $k(c)/k$, so that t.d. $(k(c))(x)_d/k(c) = N - 1$, which means that the type of x over $k(c)$ is a forking extension of its type p over k. But, since $\mathrm{RU}(p) = 1$, this may happen only once: when x is algebraic over $k(c)$, i.e. when $N - 1 = 0$, a contradiction.

REMARK. Proposition 1 has not drawn full consequences of the strong property $\mathrm{RU}(p) = 1$. As a matter of fact, we know that the forking rank of a non-forking extension of p is also 1, so the conclusion remains true for any generic solution of any non-forking extension of p over an extension K of k. The distinction between these properties will be made more accurate by defining "weak" and "strong orthogonality to the constants."

Recall that a d.f. K is *differentially closed* if every system consisting of an equation $P(x) = 0$ and an inequation $Q(x) \neq 0$, where P and Q are in $K[X]_d$ with Q of order less than P, has a solution in K. For any d.f. k, a *differential closure* $\hat{k}$ can be constructed, which has "good" properties: $\hat{k}$ is differentially closed, $\hat{k}$ has the same cardinal

as k, $\hat{k}$ is differentially algebraic over k, the constants of $\hat{k}$ form an algebraic closure of those of k; there is a "Nullstellensatz" similar to the case of usual fields; two differential closures of k are k-isomorphic (as d.f.).... For more details, see [1], [12] or [13].

We return to orthogonality. For simplicity, we shall deal only with *stationary* types, that is, such that their minimal polynomials remain irreducible over any extension of their coefficient fields; therefore, a stationary type has *exactly one* non-forking extension over any extension of its coefficient field.

Two stationary types $p = I(P;k)$ and $q = I(Q;k)$ over a d.f. k are *weakly orthogonal* if, x and y being any generic solutions of respectively p and q, the type of x over $k(y)_d$ does not fork over k (which is equivalent to the symmetric requirement obtained by permuting x and y); p and q are *strongly orthogonal* if for any differentially closed extension K of k, $I(P;K)$ and $I(Q;K)$ are weakly orthogonal (because of the Nullstellensatz, it suffices to consider $K = \hat{k}$, a differential closure of k). When $q = I(X';k)$ is *the type of transcendental constants over* k, we talk about "orthogonality to the constants." Strong orthogonality clearly implies the weak one, but $I(X' - 1;C)$ and $I(X';C)$, with C a constant d.f., provides a counterexample for the converse.

Now we see that *Proposition* 1 *merely asserts the weak orthogonality of* p *to the constants*, while the above Remark explains that *this orthogonality is in fact strong.*

This is the point where another distinct problem arises: for a type of order 1, the forking rank no longer has meaning since it is also 1; but orthogonality to the constants still occurs: in [10], Rosenlicht proved that the type of minimal equation $X' + X'/X = 1$ (among others) is strongly orthogonal to the constants.

4. Algebraic independence of solutions. In his paper [10], Rosenlicht constructed, in a differential closure $\hat{C}$ of a d.f. C of constants, a countable set of generic solutions of $I(X' + X'/X = 1;C)$ which are algebraically independent over C; this answers question II for this type and was enough to prove the non-minimality of $\hat{C}$ over C (there exists a differentially closed field strictly between C and $\hat{C}$). For the construction, it was proved that the algebraic dependence over k of two generic solutions x and y of $I(X' + X'/X = 1;k)$ reduced to a "very special" relation: $x = y$.

We prove a similar result and make similar constructions for types of order 2, under the supplementary assumption that the forking rank

is 1. The types we consider include those of the Corollary to Theorem 1, in which case we know RU = 1.

THEOREM 2. *Let k be a d.f. with constants C. Let p be a stationary type over k, of order 2 and such that its minimal equation is of the following form:*

$$\text{(E)} \qquad F' = \sum_{i=1}^{n} c_i \frac{G_i'}{G_i},$$

where F is a non-constant differential polynomial in $C[X]_d$, G_i is a non-constant differential rational function in $C(X)_d$ $(i = 1, \ldots, n)$ and $c_1, \ldots, c_n$ in C are linearly independent over $\mathbb{Q}$.

Suppose that the forking rank of p is 1.

There exists a positive integer m such that if two generic solutions x and y of p are algebraically dependent over k, then $F(x)^m = F(y)^m$.

The proof is postponed to Section 7.

COROLLARY. *Let C be a d.f. of constants and p a stationary type over C with minimal equation* (E) *as above. Suppose* $\mathrm{RU}(p) = 1$. *Then there exists, in a differential closure $\hat{C}$ of C, an infinite countable set of generic solutions of p which is algebraically free over C.*

We need first a technical lemma in order to "isolate" (see [1] or [9]) the type P, that is, to produce a *finite* system of equations and inequations which defines the generic solution of p.

LEMMA 3. *Let C and p be as in the above corollary. Let $P = 0$ be the minimal equation* (E) *of p. Then the system $\mathscr{S}(X) = (P(X) = 0, S(P)(X) \neq 0, X' \neq 0, F(X)' \neq 0)$ defines the generic solution of p.*

Proof. See Section 7.

Proof of the Corollary. Let x_0 be a generic solution of p in $\hat{C}$; according to the lemma, this only means that x_0 solves the system $\mathscr{S}(X)$ which is always possible in $\hat{C}$ since it is differentially closed. Let m be the integer supplied by Theorem 2; by solving the system $\mathscr{S}_1(X) = \mathscr{S}(X) \wedge (F(X)^m \neq F(x_0)^m)$ in $\hat{C}$, we get another generic solution x_1 which is algebraically independent from x_0 over C. By induction, we build a countable set $\{x_0, x_1, x_2, \ldots\}$ of generic solutions of p in $\hat{C}$: x_i is defined as a solution in $\hat{C}$ of the system $\mathscr{S}_i(X) = \mathscr{S}(X) \wedge ((F(x)^m - F(x_0)^m) \cdots (F(X)^m - F(x_{i-1})^m) \neq 0)$. Consequently

x_i and x_j are algebraically independent over C for all $i \neq j$. It remains to prove that the *set* $\{x_0, x_1, x_2, \dots\}$ is algebraically free over C. Otherwise, let i be the minimal index such that $x_0, x_1, \dots, x_i$ are dependent over C; therefore $i \geq 2$, and x_i and x_{i-1} are algebraically dependent over $k = C(x_0, \dots, x_{i-2})_d$, while both of them are transcendental over k. Since $\mathrm{RU}(p) = 1$, p has no forking extensions over k, so that x_i and x_{i-1} are generic solutions of the unique non-forking extension p_k of p over k, which has the same minimal equation and satisfies as well $\mathrm{RU}(p_k) = 1$. So, we may apply Theorem 2 to $x = x_i$, $y = x_{i-1}$ and p (of Theorem 2) $= p_k$, and we obtain: $F(x_i)^m = F(x_{i-1})^m$, a contradiction. □

REMARK. Let us point out certain particular results which follow easily from Theorems 1 and 2. In [4], we gave Theorem 2 for the equations $(X'f + g)' = \sum c_i h_i'/h_i$ concerned by Theorem 1, in which case the "special" relation obtained involves only x and y (not their derivatives), namely: $\Phi(x)^m = \Phi(y)^m$ where Φ is a primitive polynomial of f in $C[X]$. For example, the condition of algebraic dependence of two generic solutions x and y of $X'' = X'/X$ reduces to: $x = y$. Consequently: *two distinct non-constant zeros x and y of $X'' = X'/X$ are always algebraically independent over the constants, and also over a d.f. k as soon as they are transcendental over k; in fact, it can be proven that x, x', y, y' are algebraically independent over k.*

5. Proof of Theorem 1; Other similar results.

LEMMA 4. *Let K be a field and ϕ, ψ be non-zero elements in $K[X]$ such that ϕ divides $\psi \cdot \partial\phi$ in $K[X]$. Then each irreducible factor of ϕ in $K[X]$ is a factor of ψ.*

LEMMA 5. *Let K/C be a d.f. extension with C consisting of constants. Let ϕ be in $K[X]$ and ψ in $C[X]$, both non-zero. If ϕ divides $\psi \cdot \phi^*$ in $K[X]$, then $\phi^* = \alpha \cdot \phi$ for some α in K.*

Proof. The first lemma is obvious. For the second, we may assume $\phi^* \neq 0$ and ψ of positive degree. Let $\overline{K}$ be an algebraic closure of K and $\overline{C}$ the relative algebraic closure of C in $\overline{K}$; by Lemma 1, $\overline{C}$ consists of constants. Set $\phi \cdot q = \psi \cdot \varphi^*$ with q in $K[X]$; a G.C.D. d of q and ψ in $\overline{K}[X]$ may be chosen in $\overline{C}[X]$, for ψ has coefficients in C. Divide ψ and q by d: $\psi = \psi_1 \cdot d$ and $q = q_1 \cdot d$ with ψ_1 in $\overline{C}[X]$; the initial equation becomes: $\phi \cdot q_1 = \psi_1 \cdot \phi^*$. Thus ψ_1 divides

ϕ, say ν times: $\phi = \psi_1^\nu \cdot \phi_1$. Now $\psi_1^* = 0$, so that the equation yields: $\phi_1 \cdot q_1 = \psi_1 \cdot \phi_1^*$; with all the above conditions, this can happen only if $q_1 = \alpha \cdot \psi_1$ for some α in $\overline{K}$, and eventually $\phi^* = \alpha \cdot \phi$ and α is in K.

Proof of Theorem 1. We are looking for an irreducible $Q \in K[X]_d$ of order 1 such that $P \in I(Q;K)$. Let $Q = X'^N a_N + \cdots + a_0$ with $a_i \in K[X]$ and $a_N \neq 0$. Develop P: $P = X''Af - X'(B - A\partial g - X'A\partial f)$; from (1) in Section 2, we have: $X''S(Q) \equiv -(X'\partial Q + Q^*)$ modulo $(Q)_d$, and therefore: $S(Q)P \equiv -\overline{P}$ modulo $(Q)_d$, where $\overline{P} = Af(X'\partial Q + Q^*) + X'(B - A\partial g - X'A\partial f)S(Q)$ is of order 1 (or vanishes), so that $P \in I(Q;K)$ if and only if Q divides $\overline{P}$ (or $\overline{P} = 0$).

As a polynomial in X', $\overline{P}$ is of degree $N+1$ and the coefficients of the highest and lowest powers of X' are respectively $Af\partial a_n - NAa_N\partial f$ and Afa_0^*.

If $\overline{P} = 0$, then $Af\partial a_N - NAa_N af = Af^{N+1}\partial(a_N/f^N) = 0$ implies that a_N/f^N is an element in K; since Q is defined up to a non-zero coefficient in K, we may assume $a_N = f^N$. Equating then the coefficient of X'^N in $\overline{P}$ to 0, we get: $\partial(g - a_N/Nf^{N-1}) = B/A = \sum c_i \partial h_i/h_i$, which is impossible since g, a_{N-1}, f, h_i are all rational functions.

If $\overline{P} \neq 0$ is divisible by Q, then a_N (resp. a_0) divides $Af\partial a_N - NAa_N\partial f$ (resp. Afa_0^*). So a_N divides $Af\partial a_N$; apply Lemma 4 to $\phi = a_N$ and $\psi = Af$: each irreducible factor of a_N in $K[X]$ is a factor of Af; but the latter has constant coefficients, so we may assume a_N too. Thus $a_N^* = 0$.

Suppose in addition $a_0 \neq 0$, and apply Lemma 5 to $\phi = a_0$ and $\psi = Af$: $a_0^* = \alpha\beta_0$, for some α in k. It follows that $P = Q \cdot (X'Af\partial(a_N/f^N) + \alpha Af)$ and the identification of the coefficients of X'^N yields: $\partial(g - \alpha\Phi/N - a_{N-1}f/Na_N) = B/A = \sum c_i \partial h_i/h_i$, where Φ is a primitive polynomial of f in $C[X]$ (i.e. $\partial\Phi = f$); again this equation has no polynomial solution a_{N-1}.

Finally, if $a_0 = 0$, then $N = 1$ and a_1 is in K because of the irreducibility of Q; that is: $I(Q;K) = I(X';K)$. □

REMARK. As already noticed, the equations involved in Theorem 1 belong to the class of those concerned by Theorem 2, namely:

(E) $F' = \sum c_i G_i'/G_i$, with F a differential polynomial and G_i differential rational functions such that the equation is of order 2 (and is *really of this form*: we mean that at least F or one of the G_i is of positive order and the c_i are linearly independent over $\mathbb{Q}$).

In both theorems, the coefficients of F, G_i and the c_i must be constant. Moreover, in Theorem 1 F must be of the first order and first

degree in X' ($F = X'f + g$) and the G_i must be of order 0 (G_i written h_i).

However, Theorem 1 should also hold for "most" of the equations in the class (E) without such restrictions; there are, of course, equations in (E) which cannot fit: for instance $X' = X''/X'$, or any equation which does not involve X will be of forking rank 2. Indeed, $X' = X''/X'$ may be turned into $(1/X') = -1$ and this provides a first integral $1/X' = c - t$, where t is some element of derivative 1 and c an *arbitrary* constant; this proves simultaneously that RU = 2 and the non-orthogonality to the constants.

But there is no such phenomenon in the following examples (where f, g, h_i *denote polynomials of order* 0):

(a) $X'f = X''/X'$, *with* f *of positive degree*;

(b) $X'f = X''/X' - X'/X$, *with* f *as above*;

(c) *Same equations as in Theorem* 1;

in each of these cases it turns out that, *without any assumption on the coefficients of the polynomial* f, *the analog of Theorem* 1 *holds* (so that (c) generalizes Theorem 1). This is proved along quite the same lines; for (c), Lemma 5 and 6 appear to be of no more help. As far as Theorem 2 is concerned, see the final Remark in Section 7.

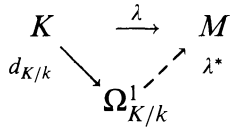
6. Technical results for Theorem 2. So far, we have not yet met those Kähler differentials we announced but we shall make much use of them in proving Theorem 2; here is a review of classical constructions, followed by general results in the case of differential fields.

Let K be an algebra over a field k of characteristic 0. Recall ([**2**], Ch. III, §10, No 2) that, if the algebra K is $\mathbb{Z}$-graded, if M is a $\mathbb{Z}$-graded K-module and n an integer, a *k-derivation* (resp. *k-antiderivation*) *of degree n from K to M* is a k-linear map λ from K to M, homogeneous of degree n, and such that: $\lambda(ab) = b\lambda(a) + a\lambda(b)$ for all a and b in K (resp. $\lambda(ab) = b\lambda(a) + (-1)^{n\cdot|a|}a\lambda(b)$ for all a in K homogeneous of degree $|a|$ and all b in K). If a module is not graded over $\mathbb{Z}$, it will be provided with the trivial graduation: every element is of degree 0.

We denote by $\mathrm{Der}_k(K, M)$ the K-module of k-derivations from K to M.

PROPOSITION 2. *There exist a K-module (called the module of Kähler differentials of K over k and denoted by $\Omega^1_{K/k}$) and a k-derivation (called the exterior differential and denoted by $d_{K/k}$ from K to $\Omega^1_{K/k}$ which have the following universal property: for any k-derivation λ from K to a K-module M, there is a unique K-linear map λ^* from $\Omega^1_{K/k}$ to*

M which factors λ through $d_{K/k}$.



$$\lambda = \lambda^* \cdot d_{K/k}$$

The pair $(\Omega^1_{K/k}, d_{K/k})$ may be seen as: The submodule of the dual of the K-module $\mathrm{Der}_k(K,K)$ which is generated by the da, $a \in K$, where $da(D) = Da$ for $D \in \mathrm{Der}_k(K,K)$. Or else: ([**2**], Ch. II, §10, n° 11). The quotient I/I^2, where I is the kernel of the canonical algebra homomorphism from $K \otimes_k K$ onto K which maps $a \otimes b$ onto ab. Or else: Simply the K-module generated by the *symbols* da, $a \in K$, submitted to the following *relations*: $d(a+b) = da + db$ and $d(ab) = dba + adb$ for a and b in K, and $da = 0$ for all a in the image of k in K.

Henceforth, *K/k is a field extension of characteristic* 0. Then ([**11**], Prop. 3) $\Omega^1_{K/k}$ is a K-vector space for which $(d_{K/k}u_i)_{i\in I}$ is a linear basis if and only if $(u_i)_{i\in I}$ is a basis of transcendency for K/k; hence $\dim_K \Omega^1_{K/k} = \text{t.d. } K/k$. We shall need the following ([**2**], Ch. III, §10, n° 9, Prop. 14).

PROPOSITION 3. *Let A be a commutative ring, M an A-module and E a bimodule over the exterior algebra $\Lambda(M)$. Let d_0 be a derivation from Λ to E (i.e. $d_0(ab) = d_0(a) + ad_0(b)$) and d_1 a homomorphism of additive groups from M to E such that:*

$$d_1(ax) = ad_1(x) + d_0(a)x \quad \textit{for all } a \textit{ in } A \textit{ and } x \textit{ in } M.$$

If $xd_1(x) + d_1(x)x = 0$ for all x in M, then there exists a unique derivation d of the $\mathbb{Z}$-algebra $\Lambda(M)$, the restrictions of which to A and M are respectively d_0 and d_1.

Put in this proposition: $A = K$, $M = \Omega^1_{K/k}$ and $E = \Lambda(\Omega^1_{K/k})$, which is usually denoted by $\Omega_{K/k}$. We already have $d_0 = d_{K/k}$, so that it suffices to build a map d_1 (and this is done in [**3**], §2, n° 10) meeting the above conditions. Whence is deduced *the extension of $d = d_{K/k}$ into a k-derivation (still denoted by d) of degree* 1 *such that $d^2 = 0$, of the exterior algebra $\Omega_{K/k}$*. We have the formula: $d(v\,du_1 \wedge \cdots \wedge du_n) = dv \wedge du_1 \wedge \cdots \wedge du_n$, for all $v, u_1, \ldots, u_n$ in K.

We turn to the *Case of Differential Fields*. Let K/k be a d.f. extension; we simply write d for $d_{K/k}$. The following, quoted from [**11**] (Prop. 2), makes $\Omega^1_{K/k}$ a "differential K-vector space."

PROPOSITION. *There exists an endomorphism D^1 of the additive group $\Omega^1_{K/k}$ with the following properties:*

$$D^1(u\omega) = u'\omega + uD^1\omega \quad \text{and} \tag{2}$$
$$D^1(du) = d(u') \quad \text{for } u \text{ in } K \text{ and } \omega \text{ in } \Omega^1_{K/k}.$$

Now, putting $A = K$, $M = \Omega^1_{K/k}$, $E = \Omega_{K/k}$, $d_0 =$ "$'$" (the given derivation on K extending that of k) and $d_1 = D^1$ in Proposition 3, we see that *there exists a unique derivation D of degree 0 of $\Omega_{K/k}$ which extends "$'$" and D^1*. Since D is a derivation, it verifies:

$$D(\omega_1 \wedge \cdots \wedge \omega_n) \tag{3}$$
$$= \sum_{i=1}^{n} \omega_1 \wedge \cdots \wedge \omega_{i-1} \wedge (D^1\omega_i) \wedge \omega_{i+1} \wedge \cdots \wedge \omega_n$$
$$\text{for } \omega_1, \ldots, \omega_n \text{ in } \Omega^1_{K/k}.$$

We arrive now at a key proposition for proving Theorem 2. First here is a preliminary result of linear algebra.

LEMMA 6. *Let E be a vector space over a field K. Suppose that elements $a_0, \ldots, a_n$ not all zero in K, $\omega_0, \ldots, \omega_n$ in E and $\lambda_0, \ldots, \lambda_n$ in K satisfy:*

$$\sum_{i=0}^{n} a_i\omega_i = 0 \quad \text{in } E \quad \text{and} \quad \sum_{i=0}^{n} a_i\lambda_i = 0 \quad \text{in } K.$$

Then we have the following in $\Lambda^n(E)$:

$$\sum_{i=0}^{n} (-1)^i \lambda_i \omega_0 \wedge \cdots \wedge \widehat{\omega_i} \wedge \cdots \wedge \omega_n = 0.$$

The proof is straightforward.

PROPOSITION 4. *Let K/k be a d.f. extension. If elements $u_0, \ldots, u_n$ in K are algebraically dependent over the constants C of k, then:*

$$D(u_0\, du_1 \wedge \cdots \wedge du_n)$$
$$= d\left(u_0 \sum_{i=1}^{n} (-1)^{i-1} u_i'\, du_1 \wedge \cdots \wedge \widehat{du_i} \wedge \cdots \wedge du_n\right).$$

The interest lies in the following fact: the algebraic dependence over k of $n+1$ elements in K is equivalent to the vanishing of a

$(n+1)$-form; assuming the dependence to be over the constants of k, we obtain a relation in $\Omega^n_{K/k}$ (i.e. $\Lambda^n(\Omega^1_{K/k})$).

Proof. By virtue of formulae (2) and (3), we calculate:

$$D(u_0\,du_1\wedge\cdots\wedge du_n)$$
$$= u_0'\,du_1\wedge\cdots\wedge du_n$$
$$+ u_0\sum_{i=1}^{n} du_1\wedge\cdots\wedge du_{i-1}\wedge du_i'\wedge du_{i+1}\wedge\cdots\wedge du_n$$

(*convention*: du' means $d(u')$).

On the other hand, since $u_0,\ldots,u_n$ are algebraically dependent over C, there is a polynomial F in $n+1$ variables and with coefficients in c such that $F(u_0,\ldots,u_n)=0$; we choose such an F of minimal degree. Now apply to this relation the given derivation "$'$" and the exterior differential d:

$$\sum_{i=0}^{n}\partial_i F(u_0,\ldots,u_n)u_i' = 0 \quad \text{in } K \quad \text{and}$$
$$\sum_{i=0}^{n}\partial_i F(u_0,\ldots,u_n)\,du_i = 0 \quad \text{in } \Omega^1_{K/k},$$

($\partial_i F$ is the partial derivative of f with respect to the ith variable). Let $E=\Omega^1_{K/k}$, $a_i=\partial_i F(u_0,\ldots,u_n)$, $\omega_i=du_i$ and $\lambda_i=u_i'$ $(i=0,\ldots,n)$; because of the minimality of the degree of F and the 0-characteristic, not all a_i are zero. Therefore, we may apply Lemma 6, which yields:

$$\sum_{i=0}^{n}(-1)^i u_i'\,du_0\wedge\cdots\wedge\widehat{du_i}\wedge\cdots\wedge du_n = 0.$$

Comparing this relation to that obtained at the beginning of the proof, the result follows from some computations that we skip.

REMARK. Proposition 4 generalizes Lemma 1 of [**10**], which corresponds to $n=1$. We shall also need this slightly improved version of Proposition 4 of [**11**].

PROPOSITION 5. *Let K/k be a field extension, $u_1,\ldots,u_n$ non-zero elements in K and v in K. Let $c_1,\ldots,c_n$ in K be algebraic over k and linearly independent over $\mathbb{Q}$.*

If $c_1\,du_1/u_1 + \cdots + c_n\,du_n/u_n = dv$ *in* $\Omega^1_{K/k}$, *then* $u_1, \ldots, u_n$ *and* v *are algebraic over* k (*i.e. such a relation is necessarily trivial*).

In [11], the c_i were lying *in* k, but our version is easily obtained by regarding the algebraic closure $\bar{k}$ of k in K and using the K-linear map from $\Omega^1_{K/k}$ into $\Omega^1_{K/\bar{k}}$ which is induced by the universal property of $\Omega^1_{K/k}$ and merely replaces $d_{K/k}$ by $d_{K/\bar{k}}$.

7. Proofs of Theorem 2 and Lemma 3 to its Corollary. We first prove Lemma 3. Let x be a solution of $\mathscr{S}(X)$ and suppose that x is not a generic solution of p. Yet, x is a solution of p, for the type q of x over C contains P but not $S(P)$, so that q contains p (as already noted in Section 2). Therefore, we are reduced to looking for the types q over C which strictly contain p. Clearly q cannot be of order 2 and cannot be algebraic either since this would make x algebraic over c, hence constant (Lemma 1) while x satisfies $\mathscr{S}(X)$. Thus q is of the first order and t.d. $C(x)_d/C = 1$. By computing the minimal polynomial P of p and then $S(P)$, we see that $S(P)(x) \neq 0$ implies $G_i(x) \neq 0$ for all i; now $F(x)$ and $1/G_i(x)$ are algebraically dependent over c; apply Proposition 4: $D^1(dF(x)/G_i(x)) = d(F(x)'/G_i(x))$, which we rewrite: $G_i(x)'dF(x) = F(x)'dG_i(x)$. Multiply both sides by $c_i/G_i(x)$, sum over i and take the fact that x satisfies $P(x) = 0$ and $F(x)' \neq 0$ into account; it yields: $dF(x) = \sum c_i\,dG_i(x)/G_i(x)$ in $\Omega^1_{C(x)_d/C}$. Apply Proposition 5: $dF(x) = 0$ in $\Omega^1_{C(x)_d/C}$, that is: $F(x)$ is algebraic over C, hence constant, a contradiction. □

Proof of Theorem 2. Set $K = k(x,y)_d$ and $d = d_{K/k}$. Since the minimal equation of x over k is (E), which has constant coefficients, it remains the same under restriction to C so that x satisfies the system $\mathscr{S}(X)$ mentioned in Lemma 3: in particular $G_i(x) \neq 0$ for all i, and $F(x) \neq 0$; also t.d. $C(x)_d/C = 2$ so that the three elements $u_0 = 1/(F(x)'G_i(x))$, $u_1 = G_i(x)$ and $u_2 = F(x)$ in $C(x)_d$ are algebraically dependent over c. Apply Proposition 4:

$$D\left(\frac{dG_i(x) \wedge dF(x)}{F(x)'G_i(x)}\right) = d\left(\frac{G_i(x)'\,dF(x) - F(x)'\,dG_i(x)}{F(x)'G_i(x)}\right)$$
$$= d\left(\frac{G_i(x)'\,dF(x)}{F(x)'G_i(x)}\right)$$

by developing. Sum over i and use equation (E) for x:

$$D\left(\sum c_i \frac{dG_i(x) \wedge dF(x)}{F(x)'G_i(x)}\right) = \sum c_i D\left(\frac{dG_i(x) \wedge dF(x)}{F(x)'G_i(x)}\right)$$
$$= d\left(\left(\sum c_i \frac{G_i(x)'}{G_i(x)}\right)\frac{dF(x)}{F(x)'}\right)$$
$$= d(dF(x)) = 0,$$

since $d^2 = 0$. Doing the same with y instead of x, we get

(i) $$D\left(\frac{dF(x)}{F(x)'} \wedge \sum c_i \frac{dG_i(x)}{G_i(x)}\right)$$
$$= D\left(\frac{dF(y)}{F(y)'} \wedge \sum c_i \frac{dG_i(y)}{G_i(y)}\right) = 0 \quad \text{in } \Omega^2_{K/k}.$$

For short, we write $\omega(x)$ and $\omega(y)$ for the 2-forms inside parentheses in (i). We have $\omega(x) = \phi(x)\,dx \wedge dx'$ and $\omega(y) = \phi(y)\,dy \wedge dy'$, with $\phi = \sum c_i(\partial_0 F \cdot \partial_1 G_i - \partial_0 G_i \cdot \partial_1 F)/F'G_i$ in $C(X)_d$; as it is written, ϕ may involve X'', but equation (E) gives $\phi(x) = \psi(x, x')$ and $\phi(y) = \psi(y, y')$, where

(ii) $$\psi = \frac{1}{X'}\left(\sum_{i=1}^{n} c_i \frac{\partial_1 G_i}{G_i} - \partial_1 F\right) \text{ is a rational function in } C(X, X').$$

Note that ψ is not identically zero; since x and x' (resp. y and y') are algebraically independent over k, it follows that $\omega(x) \neq 0$ (resp. $\omega(y) \neq 0$) in $\Omega^2_{K/k}$.

Now if x and y are algebraically dependent over k, then $\dim_K \Omega^1_{K/k}$ = t.d. $K/k = 2$, so $\dim_K \Omega^2_{K/k} = 1$ and $\omega(x), \omega(y)$ are proportional:

(iii) $$\omega(y) = c\omega(x), \quad \text{with } c \neq 0 \text{ in } K.$$

Recall (i) and apply D to (iii): $0 = D(\omega(y)) = D(c\omega(x)) = c'\omega(x) + c.0$. Hence, c is a constant of K; but K is algebraic over $k(x)_d$, so by Lemma 2, c is algebraic over the constants of $k(x)_d$ which are algebraic over C (Proposition 1 and $\mathrm{RU}(p) = 1$). So *c is algebraic over C (as will be all constants of K)* and $dc = 0$.

On the other hand, the dependence of x and y is expressed by

(iv) $$dy = \alpha\,dx, \quad \text{for some } \alpha \neq 0 \text{ in } K.$$

Apply d and D^1 to (iv):

(v) $$0 = d\alpha \wedge dx, \quad \text{and}$$

(vi) $$dy' = \alpha'\,dx + \alpha\,dx', \quad \text{whence}$$

(vii) $$dy \wedge dy' = \alpha^2\,dx \wedge dx'.$$

Compare (vii) to (iii):

(viii) $$\alpha^2/c = \psi(x,x')/\psi(y,y').$$

Compute logarithmic exterior differentials of both sides: $2\,d\alpha/\alpha = d\psi(x,x')/\psi(x,x') - d\psi(y,y')/\psi(y,y')$, make the exterior product with dx and use (iv), (v) and (vi): $0 = (\partial_1\psi(x,x')/\psi(x,x') - \alpha\partial_1\psi(y,y'))\,dx \wedge dx'$, that is

(ix) $$\alpha = \frac{\partial_1\psi(x,x')/\psi(x,x')}{\partial_1\psi(y,y')/\psi(y,y')}.$$

Replacing this value of α in (viii) finally yields:

(x) $$c = \frac{\partial_1\psi(x,x')^2/\psi(x,x')^3}{\partial_1\psi(y,y')^2/\psi(y,y')^3}.$$

Now there are two possibilities: *either* the rational function $(\partial_1\psi)^2/\psi^3$ in $C(X,X')$ is a constant in C, in which case the relation (x) becomes: $c = 1$; *or* this function is not constant.

The first case easily implies that there is some f in $C(X)$ and some a in C such that: $\psi = a/(X'+f)^2$. But, remembering (ii), we have:

$$\partial_1\left(F + \frac{af}{X'+f}\right) = \sum_{i=1}^{n} c_i\frac{\partial_1 G_i}{G_i} - a\frac{\partial_1(X'+f)}{X'+f},$$

which is an equality between an exact C-derivative and a linear combination of logarithmic C-derivatives of rational functions and must therefore be trivial. Since F is a polynomial, it follows that f *is zero* and F *is of order* 0. Consequently $\psi = a/X'^2$ and, since $c = 1$, the relations (ix) and (iv) respectively yield:

(xi) $$\alpha = \frac{y'}{x'} \quad \text{and} \quad \frac{dy}{y'} = \frac{dx}{x'}.$$

Note, *quite generally* (no matter in which case we are), that $u_0 = 1/G_i(x)$ and $u_1 = 1/u_0$ are algebraically dependent over C, so that Proposition 4 gives: $D^1(dG_i(x)/G_i(x)) = d(G_i(x)'/G_i(x))$; multiply by c_i, sum over i, and use properties of D^1 (relations (2) in previous section):

(xii) $$D^1\left(dF(x) - \sum_{i=1}^{n} c_i\frac{dG_i(x)}{G_i(x)}\right) = 0 \quad \text{in } \Omega^1_{K/k},$$

and the analog for y.

Working with $(dF(x), \sum c_i\, dG_i(x)/G_i(x))$ as a basis for $\Omega^1_{K/k}$, set:

$$\text{(xiii)} \qquad dF(y) - \sum_{i=1}^{n} c_i \frac{dG_i(y)}{G_i(y)} = u\, dF(x) - v \sum_{i=1}^{n} c_i \frac{dG_i(x)}{G_i(x)},$$

with u and v in K.

By making the exterior product with $dF(y)/F(y)' = dy/y'$ (since F is of order 0) and using (xi), we get: $v = 1$, which we put back in (xiii) on which we apply D^1, while taking (xii) into account; we get: $u = 1$. Now (xiii) reads as follows:

$$d(F(y) - F(x)) = \sum_{i=1}^{n} c_i \frac{d(G_i(y)/G_i(x))}{G_i(y)/G_i(x)}.$$

Apply Proposition 5: $d(F(y) - F(x)) = 0$; with (xi) this implies: $F(y)' = F(x)'$, i.e.

$$\text{(xiv)} \qquad F(y) = F(x) + b, \text{ where } b \text{ is some constant in } K$$

(thus algebraic over C). The final arguments are then the same as in the other event determined by (x), so that both will be concluded simultaneously.

In the second case (when $(\partial_1 \psi)^2/\psi^3$ is not a constant), the left-hand side of (x) may happen to be 1, like in the first case, but this does not alter the fact that (x) is a non-trivial relation of algebraic dependence over C between x, x', y and y'. In other words: the type of y over $C(x)_d$ forks over C; but the minimal equation of y over C is still (E), so that $t(y/C)$ also has forking rank 1. Therefore, *y is algebraic over* $C(x)_d$ and t.d. $C(x,y)_d/C = 2$.

Denote by Γ the d.f. $C(x,y)_d$, by δ the exterior differential $d_{\Gamma/C}$ and by Δ^1 the "derivation" of $\Omega^1_{\Gamma/C}$ which is induced by that of Γ. This latter derivation "$'$" is C-linear, so the universal property of $(\Omega^1_{\Gamma/C}, \delta)$ provides a unique *linear form* λ on the Γ-space $\Omega^1_{\Gamma/C}$ such that: $\lambda(\delta u) = u'$, for u in Γ. Write an equation similar to (xiii) in $\Omega^1_{\Gamma/C}$ (here u and v are in Γ and $d_{K/k} = d$ is replaced by $d_{\Gamma/C} = \delta$); applying λ to it, we obtain $u = v$; applying Δ^1, we see that *u is constant* (for the analog of (xii) holds in $\Omega^1_{\Gamma/C}$), hence *u is algebraic over C*. Now the equation similar to (xiii) becomes:

$$\text{(xv)} \qquad \delta(F(y) - uF(x)) = \sum_{i=1}^{n} c_i \frac{\delta G_i(y)}{G_i(y)} - \sum_{i=1}^{n} uc_i \frac{\delta G_i(x)}{G_i(x)} \quad \text{in } \Omega^1_{\Gamma/C}.$$

If the coefficients c_i, uc_i, $(i = 1,\ldots,u)$ are not linearly independent over $\mathbb{Q}$, we choose a basis of the $\mathbb{Z}$-lattice that they span and gather together suitably the $G_i(y)$, $G_i(x)$. Note that every element in this lattice is algebraic over k since u is so. Apply Proposition 5: $\delta(F(y) - uF(x)) = 0$, which means that $F(y) - uF(x)$ is algebraic over C, thus a *constant* b. Some calculations show that $u = c$:

$$F(y) = cF(x) + b, \tag{xvi}$$

with c and b constants algebraic over C. If $c = 1$ (xvi) reduces to (xiv), so we are going to prove first that, *if two generic solutions and* y *of* p *are algebraically dependent over* k *and satisfy* (xiv), *then* $b = 0$.

Consider the equations: (E) for x, (E) for y and (xiv); by Seidenberg's Elimination Theorem (see [1]), there is a finite family $\mathscr{F}$ of finite systems of equations and inequations with coefficients in k such that x and y are solutions of the above equations if and only if b solves one of the systems in $\mathscr{F}$. Now, if a system in $\mathscr{F}$ happened to involve only inequations, it would have a solution b transcendental over k, which is impossible since $b = F(y) - F(x)$ is a constant of K. Consequently, all systems in $\mathscr{F}$ involve only equations and there are only *finitely* many possible values of b. Also, the set of these possible values does not depend on the solutions x and y originally given. Denote by $b(x,y)$ the constant which corresponds to such quantities x and y; it is easily seen that $b(x,y) = b(y,x) = 0$ and $b(y,z) + b(z,x) + b(x,y) = 0$, which means that these constants form an additive group; but it is finite, hence reduced to (0).

If $c \neq 1$, then we may replace F in (E) by $F + b/(c-1)$ (for (E) involves only F'), and this amounts to saying $b = 0$, so that (xvi) reduces to: $F(y) = cF(x)$. An argument similar to that of the previous paragraph shows that the possible values of c form a finite multiplicative group, thus a group of mth roots of the unity for some m. □

REMARK. Similar but weaker results hold for some classes of equations of the form (E) with *non-constant* coefficients and are proven essentially with the same methods.

This paper was written while the author was invited as a Visiting Scholar at U.C. Berkeley in 1983 ... and delayed for extra-mathematical reasons. It is his pleasure to thank here François Gramain, Bruno Poizat and Maxwell Rosenlicht for helpful conversations.

REFERENCES

[1] L. Blum, *Differentially Closed Fields: A Model-Theoretic Tour*, in *Contributions to Algebra*, a collection of papers dedicated to E. R. Kolchin (Academic Press, New York, 1977), 37–61.
[2] N. Bourbaki, *Algèbre, Chap.* I *à* III, (Hermann, Paris, 1970).
[3] ———, *Algèbre, Chap.* X, (Masson, Paris, 1980).
[4] M. Brestovski, *Déviation et indépendance algébrique de solutions génériques d'équations différentielles du second ordre*, Comptes Rendus de l'Ac. des Sc. de Paris, Sér. A. **294** (1982), 609–612.
[5] I. Kaplansky, *An Introduction to Differential Algebra*, (Hermann, Paris, 1976).
[6] E. R. Kolchin, *Differential Algebra and Algebraic Groups*, (Academic Press, New York, 1973).
[7] D. Lascar, *Rank and definability in superstable theories*, Israel J. Math., **12** (1974), 23–87.
[8] ———, *Les corps différentiellement clos dénombrables*, manuscript (to appear in "Théories Stables III," I.H.P., 11, rue P. & M. Curie, 75231 Paris Cedex 05).
[9] B. Poizat, *Rangs des types dans les corps différentiels*, in *Théories Stables* I, I.H.P. 11, rue P. & M. Curie, 75231 Paris Cedex 05.
[10] M. Rosenlicht, *The nominimality of the differential closure*, Pacific J. Math., **52** (1974), 529–537.
[11] ———, *On Liouville's theory of elementary functions*, Pacific J. Math., **65** (1976), 485–492.
[12] S. Shelah, *Differentially closed fields*, Israel J. Math., **16** (1973), 314–328.
[13] C. Wood, *The model theory of differential fields revisited*, Israel J. Math., **25** (1976), 331–352.

Received July 20, 1983 and in revised form January 30, 1989.

UNIVERSITE PARIS 6
57, RUE DES VIGNOLES
75020 PARIS, FRANCE