COLLOQUIUM MATHEMATICUM

VOL. 84/85 2000 PART 1

TWO REMARKS ABOUT PICARD–VESSIOT EXTENSIONS AND ELEMENTARY FUNCTIONS

BY

HENRYK ŻOŁĄDEK (WARSZAWA)

Dedicated to the memory of Anzelm Iwanik

Abstract. We present a simple proof of the theorem which says that for a series of extensions of differential fields $K \subset L \subset M$, where $K \subset M$ is Picard–Vessiot, the extension $K \subset L$ is Picard–Vessiot iff the differential Galois group $\mathrm{Gal}_L M$ is a normal subgroup of $\mathrm{Gal}_K M$. We also present a proof that the probability function $\mathrm{Erf}(x)$ is not an elementary function.

1. Introduction. Let (K, ∂) be a *differential field* with algebraically closed *field of constants* $C = C_K = \ker \partial$ of zero characteristic. Here K is an algebraic field (with $+$, $\times$, 0, 1) and the *derivation* ∂ satisfies the Leibniz rule. It is useful to think about K as some field of multi-valued holomorphic functions of $x \in \mathbb{C}$ (with singularities) with $\partial = d/dx$ and $C = \mathbb{C}$; e.g. the field $\mathbb{C}(x)$ of rational functions. We shall also use the notation $\partial a = a'$. Analogously one defines a *differential ring* R (usually over some differential field) and a *differential ideal*.

Let

$$D = \partial^n + a_{n-1}\partial^{n-1} + \ldots + a_0$$

be a linear differential operator with coefficients in K and let $y_1, \ldots, y_n$ be solutions of the equation $Dy = 0$ (in some large field $\widetilde{K}$). By the *Picard–Vessiot extension* $K \subset M$ *associated with* D we understand the differential field $M = K\langle y_1, \ldots, y_n\rangle$ (the field generated by y_i's and their derivatives) provided that the following conditions hold:

(i) the field M does not contain new constants, $C_M = C_K = C$;

(ii) y_i are linearly independent over the field of constants.

2000 *Mathematics Subject Classification*: Primary 12H05.
Supported by Polish KBN Grant No 2 P03A 041 15.

The latter means that the *Wronskian*

$$W = W(y_1, \dots, y_n) = \det \begin{bmatrix} y_1 & y_2 & \dots & y_n \\ y_1' & y_2' & \dots & y_n' \\ \vdots & \vdots & \vdots & \vdots \\ y_1^{(n-1)} & y_2^{(n-1)} & \dots & y_n^{(n-1)} \end{bmatrix}$$

is nonzero (in M).

The *differential Galois group* $\mathrm{Gal}_K M$ of an extension $K \subset M$ (Picard–Vessiot or not) is the group of automorphisms of the differential field M which are the identity on K.

The differential Galois group of the Picard–Vessiot extension $K \subset M$ is identified with a subgroup of the group $\mathrm{GL}(V, C) = \mathrm{GL}(n, C)$, where V is the space of solutions of the equation $Dy = 0$. Indeed, let y_i, $i = 1, \dots, n$, be a basis of solutions and let $\sigma \in \mathrm{Gal}_K M$. Each element σy_j is a solution and is expressed as a linear combination of y_i's, $\sigma y_i = \sum_j y_j d_{ji}$, where the elements $d_{ji} \in M$ are given by the Cramer formula $d_{ji} = W_1/W_2$ and W_1, W_2 are the Wroński determinants of suitable systems of n solutions. Both Wronskians satisfy the same differential equation $W' + a_{n-1}W = 0$. Thus the derivative of their ratio is equal to zero, $d_{ji} \in C$. Note also that the matrix from $\mathrm{Gal}_K M \subset \mathrm{GL}(n, C)$ acts from the right on $(y_1, \dots, y_n)$.

There is a theorem (of Kolchin) about the existence and uniqueness of the Picard–Vessiot extension. Let us recall its construction, following the book of Magid [Mag].

We take the differential ring $K[X] = K \otimes_C C[X]$ of regular functions on $X = \mathrm{GL}(n, C)$ with values in the field K. We have $K[X] = K[u_{11}, \dots, u_{n1}, u_{12}, \dots, u_{nn}, W^{-1}]$, where u_{ij} are formal variables with derivatives $u_{ij}' = u_{i,j+1}$ and $u_{in}' = -a_{n-1}u_{in} - \dots - a_0 u_{i1}$ and $W = W(u_1, \dots, u_n)$, $u_i = u_{i1}$. Let $I \subset K[X]$ be some maximal differential ideal (over K). The following two algebraic results are proven in [Mag].

PROPOSITION 1. *Let $I \subset K[X]$ be a maximal (under inclusion) differential ideal. Then the ideal I is prime.*

Proof. Let $R = K[X]/I$; we have to show that the ring R does not contain zero divisors.

Assume that $ab = 0$ for $a, b \in R \setminus 0$. Then the identities $(ab)'b = a'b^2 + abb' = a'b^2$ show that $a'b^2 = 0$. Generally $a^{(k)}b^{k+1} = 0$. Take the differential ideal $I_1 = (a, a', \dots)$ of R. For any $e \in I_1$ we have $eb^m = 0$ for some m. If all $b^m \neq 0$, I_1 would be a proper ideal, because $1 \cdot b^m \neq 0$ and hence $1 \notin I_1$. This contradicts the maximality of I.

Therefore any zero divisor (e.g. b or a) is nilpotent. In particular, $a^n = 0$ for some minimal n and the formula $na^{n-1}a' = 0$ shows that a' is also a zero divisor (and also nilpotent). Repeating this, we see that $a^{(j)}$ are all

nilpotent zero divisors. Thus a generates an ideal I_2 consisting of nilpotent elements. Because the latter does not contain 1, it should be proper. ∎

PROPOSITION 2. *Let R be a differential integral domain finitely generated over a differential field K (with algebraically closed field of constants of zero characteristic) and without proper differential ideals. Then the field of quotients $Q(R)$ does not contain new constants, $C_M = C_K = C$.*

Proof. (a) Firstly we notice that the elements from $C_M \setminus C_K$ cannot be algebraic over K. This follows from the fact that the differentiation in K extends uniquely to algebraic elements. If $d \in \overline{K} \setminus K$ satisfies a minimal algebraic equation $p(d) = d^r + a_{r-1}d^{r-1} + \ldots + a_0$, $p(x) \in K[x]$, then $d' = -p'(d)/\frac{dp}{dx}(d)$, where $p'(x) = a'_{r-1}x^{r-1} + \ldots + a'_0$. Thus $d' = 0$ implies $p \in C[x]$ and $d \in C$.

(b) Next, we have $C_M \subset R$. Indeed, for any $d = f/g \in C_M$, $f, g \in R$, consider the ideal of denominators of d, $J = \{h \in R : hd \in R\}$. It is a nonzero differential ideal, because $g \in J$ and $h'd = (hd)' \in R$ for $h \in J$. By assumption, R does not contain proper differential ideals (i.e. $\neq 0, R$). Thus $J = R$, which means that $d = 1 \cdot d \in R$.

(c) Here we show that for any $d \in C_M$ there exists an element $c \in C$ such that $d - c$ is not invertible in R. Then the ideal $(d-c)R$ is different from R and therefore it is zero. Thus $d = c \in C$.

We use some methods from algebraic geometry. We replace the field K (of coefficients) by its algebraic closure $\overline{K}$ and the ring R (over K) by $\overline{R} = R \otimes \overline{K}$ (over $\overline{K}$). We shall prove that the element $d \otimes 1 - c \otimes 1 \in \overline{R}$ is not invertible for some $c \in C$. Then, of course, also the element $d - c$ will be nonunit in R.

The element $d \otimes 1$ (which we still denote by d) can be treated as a regular function on the space $Y = \operatorname{spec}_{\overline{K}} \overline{R}$ of maximal ideals of the ring $\overline{R}$, $d : Y \to \overline{K}$. Here Y is an affine algebraic variety (equipped with the Zariski topology) and d is a morphism of algebraic varietes (see [Bor, Ch. AG, 5.2]). The image $Z = d(Y)$ is a constructible set, i.e. a finite union of sets Z_i such that Z_i are open in their closures $\overline{Z}_i$ (see [Bor, Ch. AG, 10.1]). This result (of Chevalley) implies that Z contains a dense open subset of its closure $\overline{Z}$. We have two possibilities: $\overline{Z} \neq \overline{K}$ or $\overline{Z} = \overline{K}$.

In the first case Z is finite, which means that the function $d(\cdot)$ takes a finite number of values. Because Y is irreducible (as R is an integral domain), it is connected and $d(\cdot) \equiv \text{const}$. But then d would belong to $\overline{K}$, which contradicts (a).

In the second case Z is Zariski open (equal to $\overline{K} \setminus \{\text{finite set}\}$) and there exists a point $c \in C \cap Z$. The variety $Y_c = d^{-1}(c)$ is a proper (i.e. $\neq \emptyset, Y$) subvariety of Y corresponding to the proper ideal $(d-c) = (d-c)\overline{R} = \{f \in \overline{R} : f|_{Y_c} = 0\}$. Thus $d - c$ is nonunit in $\overline{R}$. ∎

One defines the Picard–Vessiot extension as $M = Q(K[X]/I)$.

REMARK 1. When we have a ring of regular functions on an affine algebraic variety over an algebraically closed field of characteristic zero, its maximal prime ideals are in one-to-one correspondence with the points of the variety (they define the closed points in the spectrum of the ring). In the case of a differential ring the situation is not so clear. Firstly, the underlying fields usually are not algebraically closed (e.g. $\mathbb{C}(x)$) and the assumption that the ideal is closed with respect to the differentiation is sometimes a serious restriction.

EXAMPLE 1. Consider the above construction of $M = Q(K[X]/I)$ in the case of the differential operator $\partial^2 + (1/x)\partial$ (adjoining of $\ln x$). We have the $\mathbb{C}(x)$-ring $\mathbb{C}(x)[X] = \mathbb{C}(x)[u_{11}, u_{12}, u_{21}, u_{22}, (u_{11}u_{22} - u_{12}u_{21})^{-1}]$, and the ideal $I = (u_{11} - 2, u_{12}, u_{22} - 3/x)$ is a prime differential ideal, which is maximal. Any ideal containing I should be associated with a $\mathbb{C}(x)$-point in the variety $\mathrm{GL}(2, \mathbb{C}(x))$, i.e. with a $\mathbb{C}(x)$-value of u_{21}. Because $u'_{21} = 3/x$ and $3/x$ has no rational primitive, there are no such $\mathbb{C}(x)$-points.

EXAMPLE 2. Consider the extension of $K = \mathbb{C}(x)$ by means of the equation $2xy' = y$. We have $X = \mathbb{C}^*$, $K[X] = \mathbb{C}(x)[u, u^{-1}]$ and the ideal I can be chosen as $(u^2 - x)$. Due to the fact that $\mathbb{C}(x)$ is not algebraically closed, the ideal I is maximal. If $\overline{K}$ is the algebraic closure of K (i.e. the field of all algebraic functions of x), then the ideal $\overline{K} \otimes I$ is no longer prime or maximal in $\overline{K}[X]$. Its zero set consists of the two points $\{\pm\sqrt{x}\} \subset \overline{\mathbb{C}(x)}^*$.

The representation of the Picard–Vessiot extension in the form $M = Q(K[X]/I)$ is useful in the description of the Galois group $G = \mathrm{Gal}_K M$. Of course, $\mathrm{Gal}_K M$ acts on $X = \mathrm{GL}(n, C)$ by right multiplication. This induces an action of G on the ring $C[X]$ and also on the ring $K[X] = K \otimes C[X]$ (with trivial action on the first factor).

The above action of G on $K[X]$ coincides with the action of G on the elements $[u_1], \ldots, [u_n]$ (the cosets in $K[X]/I$ of $u_i = u_{i,1}$), treated as solutions of the equation $Dy = 0$ in M. This shows that

$$\mathrm{Gal}_K M = \{\sigma \in X : \sigma(I) = I\}$$

and that $G \subset X$ is defined as the zero set of some system of algebraic functions. G is a linear algebraic group (see [Kol] and [Mag]).

Consider our above examples. In the case of the equation $xy'' + y' = 0$ and an element $\sigma = \left(\begin{smallmatrix} p & q \\ r & s \end{smallmatrix}\right) \in \mathrm{GL}(2, \mathbb{C})$, the preservation of the ideal I means that σ should preserve the algebraic variety $\left\{\left(\begin{smallmatrix} 2 & a(x) \\ 0 & 3/x \end{smallmatrix}\right) : a(x) \in \mathbb{C}(x)\right\}$. This leads to $p = s = 1$, $r = 0$, i.e. $G \simeq \mathbb{C}$.

In the case of the equation $2xy' = y$ we find $G \simeq \mathbb{Z}/2\mathbb{Z}$.

In what follows we shall also use the following property of Picard–Vessiot extensions, the normality.

PROPOSITION 3. *If $K \subset M$ is a Picard–Vessiot extension and G is its Galois group, then $M^G = K$, i.e. the set of elements from M which are fixed under the action of G coincides with the subfield K.*

P r o o f. We follow [Mag]. It is enough to show that for any $x \in M \setminus K$ there is an element σ from G such that $\sigma(x) \neq x$. Take the model $M = Q(R)$, $R = K[X]/I$ (as above). We have $x = a/b$, $a, b \in R$; so x belongs to the ring $R[b^{-1}]$. It is easy to see that $R[b^{-1}]$ does not contain proper differential ideals (like R); thus we can take the Picard–Vessiot extension in the form $M = Q(R[b^{-1}])$. Then $Q(R[b^{-1}])$ contains the subspace V of solutions of $Dy = 0$.

We consider the differential algebra $S = R[b^{-1}] \otimes_K R[b^{-1}] \subset M \otimes_K M$. Put

$$z = x \otimes 1 - 1 \otimes x \in S.$$

Because $x \notin K$, we have $z' \neq 0$ and $z^j \neq 0$, $j = 1, 2, \ldots$ (if $z^n = 0$ for a minimal n, then $0 = nz^{n-1}z' \neq 0$). Take the differential ring $S_z = \{v/z^i : v \in R,\ i \geq 0\}$, one of its maximal prime ideals J and the quotient S_z/J. Note that the element $[z/1]$ is nonzero in S_z/J.

We have two fields of quotients $M = Q(R[b^{-1}])$ and $N = Q(S_z/J)$, both without new constants (see Proposition 2). The two maps $w \mapsto w \otimes 1$ and $w \mapsto 1 \otimes w$ define two embeddings σ_1 and σ_2 of M into N. Moreover, $\sigma_1(M) = \sigma_2(M)$, because this equality holds for the vector spaces $\sigma_1(V) = \sigma_2(V)$ which equal the space of solutions of the equation $Dy = 0$ in N (by counting the dimensions over C). So, $\sigma = \sigma_1^{-1}\sigma_2$ is an automorphism of M. Because $\sigma_1(x) - \sigma_2(x) = [z/1] \neq 0$, we have $\sigma(x) \neq x$.

(In the same way the uniqueness of the Picard–Vessiot extension is proved in [Mag].) ∎

Consider a series of extensions of differential fields $K \subset L \subset M$ and such that $K \subset M$ is Picard–Vessiot. Then, of course, the extension $L \subset M$ is also Picard–Vessiot (being with the same fields of constants and generated by the same solutions of the differential equation with coefficients in $K \subset L$). The Galois group $H = \mathrm{Gal}_L M$ forms a subgroup of G.

Moreover, it is also clear that if $K \subset L$ is a Picard–Vessiot extension, then the subfield L is preserved by the elements from G. The latter easily implies that the Galois group H is a normal subgroup of G. One of the aims of this paper is the proof of the following result.

THEOREM 1. *If $K \subset L \subset M$, $K \subset M$ is Picard–Vessiot with Galois group G and the Galois group $H = \mathrm{Gal}_L M$ is a normal subgroup of G, then the extension $K \subset L$ is also Picard–Vessiot.*

We could not find any theorem of this form in [Kap] and [Kol]; it is only proven that if H is a normal subgroup of G, then the extension $K \subset L$ is normal (i.e. $L^H = K$) and $\mathrm{Gal}_K L = G/H$. One proof of this theorem is given in [Mag]. In the next section we present a new proof based on some ideas from [Mag] and on the above construction of the Picard–Vessiot extension.

Finally, in the third section we shall present a proof of the fact that the function

$$\mathrm{Erf}(x) = \int_0^x e^{-t^2}\,dt$$

is not elementary.

Recall that an extension $K \subset M$ of differential fields is *elementary* iff there is a chain of extensions $K = K_0 \subset K_1 \subset \ldots \subset K_r = M$ such that each $K_{i+1} = K_i\langle z_i\rangle$ where z_i is of one of the following types:

(i) it is a logarithm of an element from K_i, i.e. $z_i' = a_i'/a_i$, $a_i \in K_i$;

(ii) it is an exponent of an element from K_i, i.e. $z_i' = a_i' z_i$, $a_i \in K_i$;

(iii) it is algebraic over K_i, i.e. satisfies an equation $\sum_{j=0}^m a_j z^j = 0$, $a_j \in K_i$.

If $K = \mathbb{C}(x)$, then the elements of M are called the *elementary functions*.

We have taken this definition from the books of Ritt [Rit] and Davenport [Dav]; as far as we know, it is the standard definition. In the book of Magid [Mag] there is another definition of "elementary functions": they are defined as elements of an extension $M = \mathbb{C}(x)(\ln(x-x_1), \ldots, \ln(x-x_m); z_1, \ldots, z_n)$, where the z_j are either algebraic over $K_j = \mathbb{C}(x, z_1, \ldots, z_{j-1})$ or are exponents over K_j.

Magid [Mag] has proved that the Galois group $\mathrm{Gal}_K M$ of such an extension $K = \mathbb{C}(x) \subset M$ must be abelian, whereas the Galois group of the extension $K \subset K\langle\mathrm{Erf}\rangle$ is isomorphic to the nonabelian group of affine diffeomorphisms of the complex line. Thus Erf cannot be elementary in Magid's sense.

However, it is widely known that Erf is not elementary in the sense used already by Liouville [Lio] (see also [Rit]), but it is impossible to find the proof of this fact in the literature. In fact, this proof is not very complicated and uses one result of Liouville.

2. Proof of Theorem 1. The main idea relies on the following construction. Assume that we have a finitely generated K-algebra T (without divisors of zero) consisting of elements t such that the linear space $\mathrm{span}\{\sigma t : \sigma \in G = \mathrm{Gal}_K M\}$ (over C) is finite-dimensional. We also assume that T is G-invariant and its field of quotients $Q(T)$ is equal to M. The algebra $K[X]/I$ is a good example.

Take $T^H = \{t \in T : Ht = \{t\}\}$, the set of invariants of the action of the normal subgroup H. The normality of H means that for any $\tau \in H$, $\sigma \in G$ and $s \in T^H$ we have $\sigma^{-1}\tau\sigma s = s$, or $\tau(\sigma s) = (\sigma s)$. This shows that any $\sigma \in G$ preserves the subdomain T^H, $\sigma(T^H) = T^H$. Thus T^H is a finitely generated G-invariant subalgebra and the restriction of the action of G to T^H coincides with the action of the quotient group G/H on T^H. We claim that:

T^H is generated (over K) by solutions of a linear differential equation with coefficients in K.

Indeed, take a finite-dimensional subspace $V_1 \subset T^H$ over C which generates T^H as a K-algebra and which is G/H-invariant. Let $z_1, \dots, z_m$ be a basis of V_1; its Wronskian $W(z_1, \dots, z_m) \in K \setminus 0$. Then any element z from V satisfies the equation $D_1 z = 0$, where

$$D_1 = W(\partial, z_1, \dots, z_n)/W(z_1, \dots, z_m).$$

The coefficients of this operator are ratios of determinants which behave in the same way under the action of the group G.

By Proposition 3 we find that the coefficients of D_1 belong to K. Thus $T^H = K[V_1]$, where V_1 is the space of solutions of a linear differential equation with coefficients in K.

If we knew that $L = M^H = Q(T^H)$ (i.e. that the field of invariants of H in M is the field of quotients of the domain of invariants in T), then we would have the proof of the Picard–Vessiot property of $K \subset L$

LEMMA 1. *If we choose $T = K[X]/I$, where $X = \mathrm{GL}(n, C)$ and I is a maximal prime ideal, then*

$$M^H = Q(T^H).$$

Proof. Take any $f \in M^H \setminus 0$. We shall represent it as a ratio of invariants from T. Let $J = \{t \in T : tf \in T\} \subset T$ be the ideal of denominators of f. Since f is H-invariant, J is H-stable ($HJ = J$). Let $s \in J \setminus 0$. The elements τs, $\tau \in H$ generate a finite-dimensional space Z (over C). Choose a basis $s_1, \dots, s_p$ of Z and let $w = W(z_1, \dots, z_p)$ be the Wroński determinant. Expansion of this determinant with respect to the first row shows that $w \in J$.

We have the property $\tau w = \det(\tau|_Z) \cdot w$, which means that w is a *semi-invariant* with *weight* $\chi = \det|_Z$. The weight is a *character* of the algebraic group H, i.e. an algebraic homomorphism from H to $\mathrm{GL}(1, C) = C^*$.

Let $t = wf$. It belongs to T (because $w \in J$) and is a semi-invariant with the same weight as w. So, we have the representation of f as the ratio of semi-invariants, $f = t/w$. Assume that we can find a nonzero semi-invariant u with weight χ^{-1}. Then we would have the desired representation of f as a ratio of invariants $f = (tu)/(wu)$.

To show that such a u exists, we study in detail the representation of the group H in the space T.

In fact, we consider the group H/H_0, where $H_0 = \bigcap_\omega \operatorname{Ker}\omega$ is the intersection of kernels of all characters of H (it is a normal subgroup of H). Because $\omega|_{[H,H]} = \{1\}$, the group H/H_0 is abelian. It is isomorphic to $(H/H_0)_s \times (H/H_0)_u$ (see [Bor, Ch. 1, Theorem 4.7]), where $(H/H_0)_s$ is a semisimple group (product of finite cyclic groups and a torus $(C^*)^l$) and $(H/H_0)_u$ is a unipotent group (isomorphic to the additive group C^q). But there are no nontrivial characters on the unipotent group $(H/H_0)_u$ (there are only transcendental ones, like $a \mapsto e^a$). This means that $H/H_0 = (H/H_0)_s$ is *reductive* and any its representation in a vector space V is diagonalizable. (The reader can prove himself that any algebraic homomorphism from the torus C^*, or from the cyclic group $\mathbb{Z}/p\mathbb{Z}$, to the unipotent group of upper triangular matrices is trivial.) The space is split into weight subspaces $V = \bigoplus_\omega V_\omega$.

The natural spaces where the group H/H_0 acts are $C[H/H_0]$ and $C[G/H_0]$; moreover H acts on $C[G]$. We claim that

$$C[G]_{1/\chi} \neq 0.$$

Indeed, because the homomorphism $H/H_0 \to G/H_0$ is injective and the homomorphism $G \to G/H_0$ is surjective, the restriction $C[G/H_0] \to C[H/H_0]$ is surjective and the homomorphism $C[G/H_0] \to C[G]$ is an embedding. But of course $C[H/H_0]_{1/\chi} \neq 0$ and hence $C[G]_{1/\chi} \neq 0$.

Recall that we have the K-algebra $T = K[X]/I$, where I is a maximal prime differential ideal. Denote also by $\overline{K}$ the algebraic closure of K. We shall use the following.

LEMMA 2. *There is a canonical H-equivariant isomorphism* $\overline{T} = \overline{K} \otimes (K[X]/I) \simeq \overline{K} \otimes C[G]$.

Lemma 2 allows us to finish the proof of Theorem 1. The group H acts on the second factors in the above tensor products. Thus the component $C[G]_{1/\chi}$ gives the nonzero component $\overline{K} \otimes C[G]_{1/\chi}$. We have $\overline{T}_{1/\chi} = \overline{K} \otimes T_{1/\chi} = \overline{K} \otimes C[G]_{1/\chi} \neq 0$ and hence $T_{1/\chi} \neq 0$. ∎

Proof of Lemma 2. We begin with Example 1: with the initial field $K = \mathbb{C}(x)$, the equation $2xy' = y$, the ring $K[X] = \mathbb{C}(x)[u, u^{-1}]$ and the ideal $I = (u^2 - x)$. Here $G = \{\pm 1\}$ and $I_G = \{f \in C[X] : f|_G = 0\} = (u^2 - 1)$ is not a prime ideal in $\mathbb{C}[X]$. Also the ideal $\overline{\mathbb{C}(x)} \otimes I = (u - \sqrt{x}, u + \sqrt{x})$ is not prime in $\overline{\mathbb{C}(x)}[X]$. In fact, we have $\overline{\mathbb{C}(x)} \otimes I = \overline{\mathbb{C}(x)} \otimes I_G$, which implies the equality from Lemma 2. The reader can check that in Example 2 with adjoining $\ln x$, Lemma 2 is also true.

If the field K were algebraically closed, then the ideal $I \subset K[X]$ would define its set of zeros $A_K = A(I) = \{a \in X_K : f(a) = 0,\ f \in I\}$, a

subset of the variety $X_K = \mathrm{GL}(X, K)$ defined over the field K. The ring of regular functions on A_K would be $K[A] = K[X]/I$. The variety A_K would be irreducible (because I is prime). If K is not algebraically closed, then we introduce the ideal $\overline{I} = \overline{K} \otimes I \subset \overline{K}[X]$ with the set of zeros $A_{\overline{K}} \subset X_{\overline{K}}$, and the ring $\overline{K}[X]/\overline{I}$ consists of regular functions on $A_{\overline{K}}$.

Recall the definition of the Galois group G from the introduction. It consists of $\sigma \in X$ such that $\sigma I = I$. This gives $\sigma\overline{I} = \overline{I}$ (when acting on $\overline{K}[X]$), which means that G acts on $X_{\overline{K}}$ leaving the variety $A_{\overline{K}}$ invariant. The action of $G = G_C$ on $A_{\overline{K}}$ is naturally prolonged to an action of the group $G_{\overline{K}}$ on $A_{\overline{K}}$.

The ideal corresponding to the subvariety $G_{\overline{K}} \subset X_{\overline{K}}$ is equal to $\overline{I}_G = \overline{K} \otimes I_G$, where $I_G \subset C[X]$ is the ideal of C-valued functions vanishing on $G \subset X$. Thus the statement of Lemma 2 means that the ring of regular functions on $A_{\overline{K}}$ is isomorphic to the ring of regular functions on $G_{\overline{K}}$ and this isomorphism commutes with the action of the group H.

The action of $G_{\overline{K}}$ on $X_{\overline{K}}$ is *effective* (i.e. the stabilizer of any point is the trivial subgroup of G). This means that $A_{\overline{K}}$ is a union of whole orbits, each of them isomorphic to $G_{\overline{K}}$. We have to show that $A_{\overline{K}}$ consists of exactly one orbit.

Suppose that $A_{\overline{K}} = B_{\overline{K}} \cup C_{\overline{K}} \cup \ldots$ where $B_{\overline{K}}$, $C_{\overline{K}}, \ldots$ are disjoint orbits and $B_{\overline{K}} \neq A_{\overline{K}}$. The ideal $\overline{I}$ is strictly contained in the larger ideal $\overline{I}_B$ (of functions vanishing on $B_{\overline{K}}$). There is an isomorphism $\psi : \overline{I}_G \to \overline{I}_B$, which is defined over the field C (because the group G is defined over C). The ideal $\overline{I}$ forms an extension of the ideal I (over K) and the ideal $\overline{I}_B$ is also an extension of the ideal $I_B = \psi(\overline{K} \otimes I_G) \subset K[X]$, $\overline{I}_B = \overline{K} \otimes I_B$. The ideal I_B is differential (because algebraic extensions uniquely define extensions of the differentiation) and strictly contains the maximal differential ideal I. This gives a contradiction. ∎

REMARK 2. Magid in his proof uses for the ring T the set of elements in M which satisfy some linear differential equation. He also obtains the identity $\overline{K} \otimes T = \overline{K}[X]$.

Singer [Sin] was also working in this direction.

EXAMPLE 3 (An extension which is not Picard–Vessiot). The example is $K = \mathbb{C}(x) \subset M = K\langle \ln(1 + e^x) \rangle$.

Indeed, we have $K \subset K(e^x) \subset M$, where $K \subset L = K(e^x)$ is Picard–Vessiot with Galois group $\mathbb{C}^*$ and $L \subset M$ is Picard–Vessiot with Galois group $\mathbb{C}$. If $K \subset M$ were Picard–Vessiot, then its Galois group should be a semidirect product of $\mathbb{C}^* \times \mathbb{C}$. On the other hand, the elements of M, treated as multi-valued functions, should have singular sets invariant with respect to the action of the Galois group. This means that any automorphism of M should be of the form $\ln(1 + e^x) \mapsto \ln(1 + e^x) + a$. ∎

3. The probability function is not elementary

THEOREM OF LIOUVILLE ([Lio]). *If $K \subset M$ is an elementary extension and an element $F \in M$ has derivative in K, then*

$$F = g + \sum c_i \ln h_i$$

with $g, h_j \in K$ and $c_i \in C$.

The proof of this theorem is not as difficult as it seems at first sight. It uses induction with respect to the length of the chain $K = K_0 \subset K_1 \subset \ldots \subset K_r = M$ (where $K_{j+1} = K_j\langle z_j\rangle$ and z_j are either algebraic or exponents or logarithms). Note that if some expression contains an exponential function or an algebraic function (in a rational way), then the derivative of this expression also contains this exponential or this algebraic function. If such an expression contains a logarithm in a nonlinear way, then its derivative also contains this logarithm. For the details of the proof we refer the reader to the book of Ritt [Rit].

We apply this theorem to the probability function

$$\mathrm{Erf}(x) = \int^x e^{-t^2}\,dt.$$

Here we put $K = \mathbb{C}(x, W)$, $W = e^{-x^2}$.

Suppose that the function Erf is elementary. Then we should have

$$\mathrm{Erf}(x) = g(x, W) + \sum c_i \ln h_i(x, W)$$

where g is a rational function and the h_i are polynomials. Consider the singularities of the components $\ln h_i$, i.e. zeros of $h_i(x, e^{-x^2})$. If x_0 is such a zero and we have $h_i = (x-x_0)^{m_i}\widetilde{h}_i(x), \widetilde{h}_i(x_0) \neq 0$, then we find a logarithmic singularity Erf $\sim (\sum c_i m_i)\ln(x - x_0)$. Because Erf is an entire function, we get $\sum c_i m_i = 0$. Thus we can write $\sum c_i \ln h_i = \ln h(x)$, where $h(x)$ is a nonvanishing function of exponential growth of rank 2 at infinity (because $h_i \sim \exp(\mathrm{const}\cdot|x|^2)$). This means that $\ln h$ is a polynomial of degree at most 2.

We have reduced the proof to showing that Erf is not a rational function of x and W. Suppose that $\mathrm{Erf}(x) = P(x, W)/Q(x, W)$, where $P = a_n(x)W^n + \ldots$ and $Q = W^m + \ldots$ are polynomials in W. Then differentiation gives $Q^2W = (P'_x - 2xWP'_W)Q - P(Q'_x - 2xWQ'_W)$ or

$$W^{2m+1} + \ldots = [a'_n + 2(m-n)xa_n]W^{m+n} + \ldots$$

Consider three cases:

(i) $n < m + 1$. Then W^{2m+1} has no counterpart.

(ii) $n = m + 1$. Then we get $a'_n - 2xa_n = 1$. This equation has only integer solutions; so $a_n(x)$ should be a polynomial, $a_n(x) = b_r x^r + \ldots$ We see that this is impossible.

(iii) $n > m+1$. Then $a_n' = 2(n-m)xa_n$, or $a_n = \text{const} \cdot e^{2(n-m)x^2}$ is not a polynomial. ∎

Acknowledgments. The author thanks the referee for his remarks. They helped to avoid a mistake in the proof of Proposition 2.

REFERENCES

[Bor] A. Borel, *Linear Algebraic Groups*, Benjamin, New York, 1969.

[Dav] J. H. Davenport, *On the Integration of Algebraic Functions*, Springer, Berlin, 1981.

[Kap] I. Kaplansky, *An Introduction to Differential Algebra*, Hermann, Paris, 1957.

[Kol] E. Kolchin, *Differential Algebra and Algebraic Groups*, Academic Press, New York, 1973.

[Lio] J. Liouville, *Premier mémoire sur la détermination des intégrales dont la valeur est algébrique,* J. École Polytech. 14 (1833), 124–148; *Second mémoire sur la détermination des intégrales dont la valeur est algébrique*, ibid., 149–193.

[Mag] A. G. Magid, *Lectures on Differential Galois Theory*, Amer. Math. Soc., Providence, 1994.

[Rit] J. F. Ritt, *Integration in Finite Terms. Liouville's Theory of Elementary Methods*, Columbia Univ. Press, New York, 1948.

[Sin] M. F. Singer, *Algebraic relations among solutions of linear differential equations*, Trans. Amer. Math. Soc. 295 (1986), 753–763.

Institute of Mathematics
University of Warsaw
Banacha 2
02-097 Warszawa, Poland
E-mail: zoladek@mimuw.edu.pl

Received 11 June 1999;
revised 1 October 1999 (3778)