JOURNAL OF ALGEBRA **204,** 108–115 (1998)
ARTICLE NO. JA977359

A Note on the Axioms for Differentially Closed Fields of Characteristic Zero

David Pierce

University of Maryland, College Park, Maryland 20742, and The Fields Institute

and

Anand Pillay*

Department of Mathematics, University of Illinois at Urbana-Champaign, 1409 West Green Street, Urbana, Illinois 61801, and The Fields Institute

Communicated by Leonard Lipshitz

Received February 5, 1997

We rework the foundations of the theory of differentially closed fields of characteristic zero in a geometric setting. The "new" axioms will say that if V is an irreducible variety and W is an irreducible subvariety of the appropriate torsor $\tau(V)$ projecting generically onto V, then W has a generic point of the form $(a, D(a))$. © 1998 Academic Press

1. INTRODUCTION AND PRELIMINARIES

In this paper we restrict our attention to fields of characteristic 0. A differential field is a field k equipped with a *derivation*, that is, an additive homomorphism $D\colon k \to k$ satisfying $D(a \cdot b) = D(a) \cdot b + a \cdot D(b)$. If L_{df} is the first order language $\{+, \cdot, -, 0, 1, \delta\}$, then any differential field is naturally an L_{df} structure. Abraham Robinson [4] recognized in the 1950s that the class of existentially closed differential fields is axiomatizable, in other words the theory DF_0 of differential fields of characteristic 0 has a model companion (in fact a model completion). The model companion is usually called DCF_0, the theory of differentially closed fields of characteristic zero. In [1], L. Blum found simple axioms for DCF_0, namely, if $P(X)$, $Q(X)$ are nonzero differential polynomials in the single differential inde-

* Partially supported by grants from the NSF.

0021-8693/98 $25.00
Copyright © 1998 by Academic Press
All rights of reproduction in any form reserved.

terminate X, and the order of P is strictly greater than the order of Q, then the system $P(X) = 0 \wedge Q(X) \neq 0$ has a solution. (Notation will be explained later.) Ritt's differential algebra (division algorithm, characterization of prime differential ideals) and Seidenberg's differential elimination theory played roles in the above treatments. This is of course all now a basic and standard part of model-theoretic algebra. On the other hand, equipping a field k (say algebraically closed) with a derivation D has a clear geometric content: if, for example, V is a variety defined over the field of constants C_k of k, then for $a \in V(k)$, the derivative $D(a)$ naturally lives in the tangent space to V at a, thus D determines a (nonalgebraic) section of the tangent bundle $T(V)$. If V is not necessarily defined over the constants of k, then D determines a section of a certain torsor $\tau(V)$ under $T(V)$. In this note we shall axiomatize DCF_0 and develop some basic properties in a manner which is informed by this geometric interpretation (and avoids classical differential algebra). The results of this paper (in particular the validity of our main axiom) were already known to Hrushovski, who recognized the relevance to finding good bounds in diophantine questions. In fact the axiom leads to a strong effective non-fcp for differentially closed fields (see [2]): if $\phi(\bar{x}, \bar{y})$ is a (quantifier-free) formula in the language of differential fields, then there is a natural number N which is doubly exponential in the data appearing in the formula ϕ such that for any differentially closed field K and $\bar{a} \in K$, if the solution set of $\phi(\bar{x}, \bar{a})$ in K is finite, then it has cardinality at most N.

Let us fix notation. Throughout this paper k will be a field (of characteristic 0) equipped with a derivation D and K will be a large algebraically closed field containing k (so a "universal domain" for algebraic geometry). We do not assume that K is equipped with a derivation. If V is an affine variety defined and irreducible over k, then $I_k(V)$ denotes the set of polynomials over k which vanish on V.

If $P(X_1, \ldots, X_n)$ is a polynomial over k in the indeterminates $X_1, \ldots, X_n$ then $\partial_i P$ will denote the partial derivative of P with respect to X_i, and P^D will denote the polynomial obtained from P by applying D to the coefficients of P. If $L = k(a_1, \ldots, a_n)$ is a finitely generated extension of k, then $I(\bar{a}/k)$ denotes the ideal of polynomials $P(X_1, \ldots, X_n)$ over k which vanish at $\bar{a}$.

Our main tool will be the following well-known extension theorem for derivations (see [3, Chap. X, Sect. 7, Theorem 7]).

THEOREM 1.1. *Let $L = k(a_1, \ldots, a_n)$ be an extension of k. Let $b_1, \ldots, b_n \in L$ be such that*

$$0 = P^D(\bar{a}) + \sum_{i=1}^{n} (\partial_i P)(\bar{a}) b_i$$

for all $P(X_1, \dots, X_n) \in I(\bar{a}/k)$. *Then D extends to a unique derivation* D^* *on L such that* $D^*(a_i) = b_i$ *for* $i = 1, \dots, n$.

Note that it follows from the case $n = 1$ of Theorem 1.1 that a derivation D on a field k has a unique extension to a derivation on $\tilde{k}$, the algebraic closure of k. For this reason we assume henceforth that k is algebraically closed, although this is not required for all the results that follow.

We now recall tangent bundles and their torsors.

DEFINITION 1.2. Let $V \subset K^n$ be an irreducible variety defined over k. Let $\bar{a} = (a_1, \dots, a_n) \in V$. By the tangent space to V at $\bar{a}$, denoted $T_{\bar{a}}(V)$, we mean $\{\bar{v} \in K^n \colon \sum_{i=1}^{n} (\partial_i P)(\bar{a}) v_i = 0$ for all $P(X_1, \dots, X_n) \in I_k(V)\}$. By the tangent bundle of V, denoted $T(V)$, we mean $\{(\bar{a}, \bar{v}) \in K^{2n} \colon \bar{v} \in T_{\bar{a}}(V), \bar{a} \in V\}$.

LEMMA 1.3 (with above notation). *Let* $d = \dim(V)$ ($=$ *tr.degree*$(k(\bar{a})/k)$ *for* $\bar{a}$ *generic point of V over k*). *Then*

(i) $\dim(T_{\bar{a}}(V)) \geq d$ *for all* $\bar{a} \in V$. *Moreover, the set of* $\bar{a} \in V$ *such that* $\dim(T_{\bar{a}}(V)) = d$ *is a nonempty Zariski open subset of V defined over k. In particular, for* $\bar{a}$ *a generic point of V over k,* $\dim(T_{\bar{a}}(V)) = d$.

(ii) *Let* $P_1, \dots, P_m$ *be a set of generators for* $I_k(V)$. *Then for any* $\bar{a} \in V$, $T_{\bar{a}}(V) = \{\bar{v} \colon \sum_{i=1}^{n} (\partial_i P_j)(\bar{a}) v_i = 0$ *for* $j = 1, \dots, m\}$.

(iii) *Let* $\bar{a}$ *be a generic point of V over k. We may assume that* $a_1, \dots, a_d$ *are algebraically independent over k* (*and so* a_j *is in the algebraic closure of* $k(a_1, \dots, a_d)$ *for* $j = d+1, \dots, n$). *For* $j = d+1, \dots, n$, *let* $Q_j(X_1, \dots, X_d, X_j)$ *be an irreducible nonzero polynomial over k such that* $Q_j(a_1, \dots, a_d, a_j) = 0$. *Then* $T_{\bar{a}}(V) = \{(v_1, \dots, v_n) \colon \sum_{i=1}^{d} (\partial_i Q_j)(\bar{a}) v_i + (\partial_j Q_j)(\bar{a}) v_j = 0$ *for* $j = d+1, \dots, n\}$.

Proof. Part (ii) is clear, and (i) is standard basic algebraic geometry (see [5], for example). For (iii) note first that by the choice of Q_j we have that $(\partial_j Q_j)(\bar{a})$ is nonzero, and thus the right hand side in (iii) is a d-dimensional linear subspace of K^n containing $T_{\bar{a}}(V)$. By the "in particular" clause in (i), we see that it must equal $T_{\bar{a}}(V)$.

If V is an irreducible variety over k, then by a torsor under $T(V)$ we mean a morphism $S \to V$ and a fibrewise regular action of $T(V)$ on S, all defined over k.

DEFINITION 1.4. Let $V \subset K^n$ be an irreducible variety defined over k. By $\tau(V)$ we mean $\{(\bar{a}, \bar{v}) \colon \bar{a} \in V$ and $\sum_{i=1}^{n} (\partial_i P)(\bar{a}) v_i + P^D(\bar{a}) = 0$ for all $P(X_1, \dots, X_n) \in I_k(V)\}$. For $\bar{a} \in V$, $\tau_{\bar{a}}(V)$ denotes the fibre of $\tau(V)$ above $\bar{a}$.

Note that in this definition of $\tau(V)$ we may restrict the polynomials P to a finite generating set $P_1, \ldots, P_m$ of $I_k(V)$.

LEMMA 1.5. *$\tau(V) \to V$ is a torsor under $T(V) \to V$ (where the fibrewise action is addition in K^n).*

Proof. All that has to be checked is that for any $\bar{a} \in V$, $\tau_{\bar{a}}(V)$ is nonempty (for then it will be clearly a translate of $T_{\bar{a}}(V)$). Now if $\bar{a} \in V(k)$, then it is easy to check that $(\bar{a}, D(\bar{a})) \in \tau(V)$. As k is algebraically closed, we conclude that for any $\bar{a} \in V$ there is some $\bar{v}$ such that $(\bar{a}, \bar{v}) \in \tau(V)$.

LEMMA 1.6. *Let $\bar{a}, \bar{b}$ be n-tuples from K. Let V be the variety over k of which $\bar{a}$ is the generic point, and let W be the variety over k of which $(\bar{a}, \bar{b})$ is the generic point. Let π be the projection map from $\tau_{(\bar{a},\bar{b})}(W)$ onto the first n coordinates. Then π is onto $\tau_{\bar{a}}(V)$.*

Proof. It is first clear that π maps $\tau_{(\bar{a},\bar{b})}(W)$ into $\tau_{\bar{a}}(V)$. On the other hand the corresponding map onto the first n-coordinates clearly maps $T_{(\bar{a}\bar{b})}(W)$ onto $T_{\bar{a}}(V)$ (using Lemma 1.3(iii), for example). As all the maps and actions commute, it follows that π is surjective.

COROLLARY 1.7. *Let $V \subset K^n$ be an irreducible variety defined over k. Let $\bar{a} \in K^n$ be a generic point of V over k. Let $\bar{b} \in K^n$ be such that $(\bar{a}, \bar{b}) \in \tau(V)$. Let $W \subset \tau(V)$ be the irreducible variety over k of which $(\bar{a}, \bar{b})$ is a generic point (over k). Then there is $\bar{c} \in k(\bar{a}, \bar{b})$ such that $(\bar{b}, \bar{c}) \in \tau_{(\bar{a},\bar{b})}(W)$.*

Proof. By Lemma 1.6, $\{\bar{w} \in K^n : (\bar{b}, \bar{w}) \in \tau_{(\bar{a},\bar{b})}(W)\}$ is nonempty. But this set is defined by a finite set of linear equations over $k(\bar{a}, \bar{b})$, so has a solution in $k(\bar{a}, \bar{b})$.

2. THE AXIOMS

Our proposed new axioms for differentially closed fields say the following about a differential field (k, D):

(i) The field k is algebraically closed.

(ii) Let $V \subset K^n$ and $W \subset \tau(V)$ be irreducible varieties defined over k such that W projects generically on V (that is, a generic point of W over k is of the form $(\bar{a}, \bar{b})$ where $\bar{a}$ is a generic point of V over k). Let U be a nonempty Zariski-open subset of W defined over k. Then there is a point $(\bar{a}, \bar{b}) \in U(k)$ such that $\bar{b} = D(\bar{a})$.

Let us remark that by passing to a variety in a higher-dimensional affine space, it would be equivalent in (ii) to take $U = W$. However, in the applications, the apparently stronger form in (ii) is useful.

THEOREM 2.1. *The models of* (i) *and* (ii) *are precisely the existentially closed differential fields.*

Proof. Let (k, D) be an existentially closed differential field. As D extends to a derivation on $\tilde{k}$, it follows that k is algebraically closed. Now let V, W, U be as in (ii). Let $(\bar{a}, \bar{b})$ be a generic point of W over k. Note that $(\bar{a}, \bar{b}) \in U$. By Corollary 1.7 and Theorem 1.1, D extends to a derivation D^* on $L = k(\bar{a}, \bar{b})$ such that $D^*(\bar{a}) = \bar{b}$. The formula $(\bar{x}, \bar{y}) \in U \wedge \delta(\bar{x}) = \bar{y}$ is a quantifier-free formula satisfied in (L, D^*), so also in (k, D) as the latter is existentially closed.

Conversely, suppose (k, D) is a model of (i) and (ii). Let (L, D^*) be an extension of (k, D), let $\bar{a}$ be a tuple from L, and let $\phi(\bar{x})$ be a quantifier-free L_{df} formula over k true of $\bar{a}$. Now $\phi(\bar{x})$ can be written in the form $\psi(\bar{x}, \delta(\bar{x}), \ldots, \delta^{(r)}(\bar{x}))$ for some r and quantifier-free formula $\psi(\bar{x}_0, \ldots, \bar{x}_r)$ over k in the language of rings. Let $\bar{c} = (\bar{a}, D^*(\bar{a}), \ldots, (D^*)^{(r-1)}(\bar{a}))$. Let V be the variety over k of which $\bar{c}$ is the generic point, and let W be the variety over k of which $(\bar{c}, D^*(\bar{c}))$ is the generic point. Let $\chi(\overline{x_0}, \ldots, \overline{x_{r-1}}, \overline{y_0}, \ldots, \overline{y_{r-1}})$ be the formula $\psi(\overline{x_0}, \ldots, \overline{x_{r-1}}, \overline{y_{r-1}}) \wedge \overline{y_0} = \overline{x_1} \wedge \cdots \wedge \overline{y_{r-2}} = \overline{x_{r-1}}$. Then χ is a quantifier-free formula over k in the language of rings which is true of $(\bar{c}, D^*(\bar{c}))$. So there is a Zariski-open subset U of V defined over k such that $\bar{e} \in U$ implies that $\bar{e}$ satisfies χ. Clearly $(\bar{c}, D^*(\bar{c})) \in \tau(V)$ and thus W is a subvariety of $\tau(V)$ projecting generically onto V. By axiom (ii), there is some $\overline{c_1} \in k$ such that $(\overline{c_1}, D(\overline{c_1})) \in U$. Writing $\overline{c_1}$ as $(\overline{d_0}, \ldots, \overline{d_{r-1}})$, we see that $(\overline{d_0}, \ldots, \overline{d_{r-1}}, D(\overline{d_0}), \ldots, D(\overline{d_{r-1}})$ satisfies χ, whereby $(\overline{d_0}, D(\overline{d_0}), \ldots, D^r(\overline{d_0}))$ satisfies ψ and thus $\overline{d}_0$ satisfies $\phi(\bar{x})$.

Remark 2.2. It follows from the theorem above that (i) and (ii) axiomatize DCF_0, and so are equivalent to the Blum axioms. In fact the Blum axioms are a special case of (i) and (ii).

(Recall that if (k, D) is a differential field, then a differential polynomial over k in one differential indeterminate X is something of the form $P(X, D(X), \ldots, D^{(n)}(X))$ for some polynomial P over k. The order of this differential polynomial is n (namely the order is the greatest m such that $D^{(m)}(X)$ appears). The Blum axioms say that whenever $f(X)$, $g(X)$ are differential polynomials over k and the order of f is strictly greater than the order of g then the system $f(X) = 0 \wedge g(X) \neq 0$ has a solution in k. Assume that the order of f is n and $f(X) = P(X, \ldots, D^{(n)}(X))$, with P an ordinary polynomial over k. If $n = 0$ then the Blum axiom is implied by (i) (k is algebraically closed). So assume $n > 0$. Without loss of generality P is irreducible (as an ordinary polynomial over k in $n + 1$ indeterminates). Let V be the irreducible variety K^n. Then $\tau(V)$ is the same as

$T(V)$, namely K^{2n}. Let W be the irreducible subvariety of K^{2n} defined by

$$y_1 = x_2, y_2 = x_3, \ldots, y_{n-1} = x_n, \qquad P(x_1, x_2, \ldots, x_n, y_n) = 0.$$

Note that W projects generically onto V. Write $g(X)$ as $Q(X, \ldots, D^{(m)}(X))$ for some $m < n$. Axiom (ii) then yields some $(a_1, \ldots, a_n, b_1, \ldots, b_n)$ in k such that $(\bar{a}, \bar{b}) \in W$, $Q(a_1, \ldots, a_m) \neq 0$, and $\bar{b} = D(\bar{a})$. It follows that $f(a_1) = 0$ and $g(a_1) \neq 0$.)

Remark 2.3. From axioms (i) and (ii) it is again easy to deduce directly completeness and quantifier elimination for DCF_0.

Sketch of Proof. Let (K_1, D_1), (K_2, D_2) be saturated models of axioms (i) and (ii). We have to show that the family I of partial isomorphisms between (say) countably generated differential subfields of K_1 and K_2 has the back-and-forth property, as well as being nonempty. I is nonempty as the field of rationals (on which the derivations must be trivial) is a common subfield of both K_1 and K_2. Now suppose that f is an isomorphism between differential subfields k_1 of K_1 and k_2 of K_2, and let a be a finite tuple from K_1. We may assume that both k_1 and k_2 are algebraically closed (as f will extend uniquely to a differential isomorphism between the algebraic closures of k_1 and k_2). Let $p(x)$ be the quantifier-free type of a over k_1, and let $q(x) = f(p(x))$. We must show that $q(x)$ is realized in K_2. By the saturation assumption on K_2 it is enough to show that for each n, if $p_n(x_0, \ldots, x_n)$ is the quantifier-free type of $(a, D(a), .., D^n(a))$ over k in the language of rings, and $q_n = f(p_n)$ then there is $b \in K_2$ such that $(b, D(b), \ldots, D^n(b))$ realizes q_n. Let V the variety over k_1 of which p_{n-1} is the generic type. Then, as in the formalism in the proof of Theorem 2.1, we may identify p_n with the generic type of a subvariety W (defined over k_1) of $\tau(V)$ which projects generically onto V. Then $f(W)$ is a subvariety, defined over k_2 of $\tau(f(V))$ which projects generically onto $f(V)$. Applying axiom (ii) to K_2 and using saturation, we may find in K_2 a generic point of $f(W)$ over k_2 of the form $(c, D_2(c))$. Writing c as $(c_0, \ldots, c_{n-1})$ we see that $(c_0, D(c_0), \ldots, D^n(c_0))$ realizes q_n, as required.

The axioms (i) and (ii) can, with a little more work, be used to obtain an *effective* quantifier elimination, again avoiding classical differential algebra.

Finally we will point out briefly how some basic facts about differentially closed fields (ω-stability and the DCC on differential varieties) can be deduced quite easily, without going through classical differential algebra.

LEMMA 2.4. *DCF_0 is ω-stable.*

Proof. Let (K, D) be a model of DCF_0 and k a differential subfield. Let a be a finite tuple from K. Now $d_n = \text{tr.degree}(k(a, \ldots, D^{(n)}(a))/ k(a, \ldots, D^{(n-1)}(a)))$ is clearly nonincreasing in n. Let m be chosen where this stabilizes. Let V be the irreducible k-variety of which

$(a, D(a), \ldots, D^{(m)}(a))$ is a k-generic point. Then one shows easily that the quantifier-free type of a over k (and thus, by Remark 2.3, $tp(a/k)$) is determined by V and d_m. (Moreover, once one has defined forking, it follows that the nonforking extensions of $tp(a/k)$ correspond to the absolutely irreducible components of V.)

LEMMA 2.5. *Let (k, D) be a differentially closed field. Let Π be a family of differential polynomials over k in the differential indeterminates $X_1, \ldots, X_n$. Then there is a finite subset Π_0 of Π such that the common zero set of Π in k equals the common zero set of Π_0 in k.*

Proof. We will prove the lemma in the case where $n = 1$. It easily generalizes. So let Π be a set of differential polynomials over k in the single differential indeterminate X. Let (K, D) be a saturated elementary extension of (k, D). Let V be the common zero set of Π in K. It will be sufficient to show that V is definable by a single formula in (K, D) (for then we can apply compactness to conclude that V is defined as the zero set of a finite subset of Π). So we want to prove:

SUBLEMMA. *V is definable.*

We proceed by induction on the complexity of the simplest differential polynomial in Π. (The complexity of $f(X)$ is (m, r), where m is the order of f and r is the degree of f in $D^{(m)}$; the complexities are ordered lexicographically.) Let this be f. Let $s(X)$ be the separant of f, that is, $s(X) = \partial f / \partial X^{(m)}$, where m is the order of f. Since s is of lower complexity than f, we conclude by induction that $\{x \in V\colon s(x) = 0\}$ is definable. We have to establish the definability of the set

$$V_0 = \{x \in V\colon s(x) \neq 0\}.$$

Suppose $x \in V_0$. Then by applying D repeatedly to $f(x)$ we see that $D^{(m+j)}(x)$ is a well-defined rational function of x, $D(x), \ldots, D^{(m)}(x)$ for all j. Let Π' be the result of replacing $D^{(m+j)}(X)$ by this function in each element of Π and multiplying out by denominators. Then

$$V_0 = \{x \in K\colon s(x) \neq 0, g(x) = 0, \forall g(X) \in \Pi'\}.$$

All elements of Π' have order at most m, so we can apply the Hilbert Basis Theorem and replace Π' by a finite set. Thus V_0 is definable.

This proves the sublemma (and hence the lemma for the case $n = 1$).

REFERENCES

1. L. Blum, Differentially closed fields: A model-theoretic tour, *in* ''Contributions to Algebra'' (H. Bass, P. Cassidy, and J. Kovacic, Eds.), Academic Press, San Diego, 1977.
2. E. Hrushovski and A. Pillay, Effective bounds for number of generic points on curves in semiabelian varieties, preprint, 1997.
3. S. Lang, ''Algebra,'' Addison−Wesley, Reading, MA, 1965.
4. A. Robinson, ''Introduction to Model Theory and to the Metamathematics of Algebra,'' North-Holland, Amsterdam, 1974.
5. I. Shafarevich, ''Basic Algebraic Geometry 1,'' 2nd ed., Springer-Verlag, New York/Berlin, 1994.