(32)

ON AX-FIELDS WHICH ARE C_i

By JAN DENEF, MOSHE JARDEN* *and* D. J. LEWIS†

[Received 20th July 1981]

Introduction

C. CHEVALLEY [**6**] proved in 1936 the following

THEOREM A. *Every form $f(X_0, \ldots, X_n)$ of degree $d \leq n$ with coefficients in a finite field K has a non-trivial zero in K^{n+1}.*

Fields K which are not finite may have a weaker property which is denoted by

C_i: If $f \in K[X_0, \ldots, X_n]$ is a form of degree d and $d^i \leq n$, then f has a non-trivial zero in K^{n+1}.

This property was introduced by S. Lang in [**15**], who, combining ideas of Tsen and Nagata, proved the following transition

THEOREM B. *If a field K is C_i and E is an extension field of K of transcendence degree j, then E is C_{i+j}.*

Thus algebraically closed fields are C_0, finite fields are C_1 and function fields of transcendence degree j over algebraically closed fields and over finite fields are C_j and C_{j+1}, respectively.

The investigation of the elementary theory of finite fields led J. Ax in [**2**] to consider the following possible property of a field K.

(1) Every absolutely irreducible variety defined over K has a K-rational point.

Note that the formulation of this property implies that we are using the convention not to consider the empty set as an absolutely irreducible variety.

Perfect fields K that have the property (1) have been called *Ax-fields;* see [**14**]. J. Ax observed in [**1**] that it is a consequence of Lang–Weil theorem [**18**] that every non-principal ultraproduct F of finite fields is an Ax-field. Of course, it follows from Chevalley's theorem that F is also C_1. In addition the absolute Galois group, $G(F)$, of F is abelian, more precisely it is isomorphic to $\hat{Z}$. This led Ax to prove in [**2**] that indeed the

* This paper was written while Jarden had a Minerva grant.
† This paper was written while Lewis had a Senior Humboldt award.

following general theorem holds:

THEOREM C. *If K is an Ax-field and $G(K)$ is abelian, then K is C_1.*

Ax went on to pose

PROBLEM D. *Is every Ax-field necessarily C_1?*

This problem makes sense because as was found later, there are many Ax-fields with a non-abelian absolute Galois group. An important family of such fields are given e.g. in [**14**] by

THEOREM E. *If K is a countable Hilbertian field, then for almost all e-tuples $\sigma=(\sigma_1,\ldots,\sigma_e)\in G(K)$, $\tilde{K}(\sigma)$ is an Ax-field with $\hat{F}_e$ as its absolute Galois group.*

We recall that a field K is said to be Hilbertian if for every m irreducible polynomials $f_1,\ldots,f_m\in K[T,X]$ there exist infinitely many elements $a\in K$ such that $f_1(a,X),\ldots,f_m(a,X)$ are irreducible in $K[X]$ (cf. Lang [**16**, Chap. VIII]).

The notation $\tilde{K}(\sigma)$ stands for the fixed field of the automorphisms $\sigma_1,\ldots,\sigma_e$ in the algebraic closure $\tilde{K}$ of K, the term 'almost all' is used in the sense of the Haar measure of $G(K)^e$ and $\hat{F}_e$ is the free profinite group on e generators. If $e\geq 2$, then $\hat{F}_e$ is not abelian. Other families of Ax-fields can be found in [**13**] and [**7**].

The main result of this paper gives a partial answer to the Ax Problem:

THEOREM F. a) *Every Ax-field that contains an algebraically closed field is C_1.*

b) *Every Ax-field of a positive characteristic is C_2.*

The main algebro-geometric tool used in proving this theorem is the well-known decomposition-intersection procedure of a Zariski K-closed set. We define a field K to be weakly-C_i if for every form $f\in K[X_0,\ldots,X_n]$ of degree d with $n\geq d^i$ there exists a K-closed subset W of $\mathbb{P}^n$ which is absolutely irreducible and which is contained in the zero set $V(f)$ of f. Recall that W is said to be *K-closed* if it is the zero set in $\mathbb{P}^n$ of homogeneous polynomials in $K[X_0,\ldots,X_n]$, while by saying 'W is an absolutely irreducible variety defined over K' we mean that the ideal of all polynomials in $\tilde{K}[X_0,\ldots,X_n]$ vanishing on W is prime and has a system of generators in $K[X_0,\ldots,X_n]$. Note that if a K-closed set W is absolutely irreducible, then it is defined over a finite purely inseparable extension of K (cf. Lang [**17**], especially p. 74). Using the decomposition–intersection procedure we prove:

LEMMA G. *A necessary and sufficient condition for a Hilbertian field K to be weakly-C_i is that every Ax-field that contains K is C_i.*

The proof of this lemma given in Section 2 uses Model-theoretic methods. In Section 3 we prove it in an algebraic way, by developing the properties of weakly C_i fields. In particular we prove the following transition principle:

THEOREM H. *If a Hilbertian field K is weakly C_i, then every extension of K is also weakly C_i.*

Thus we see that the Ax problem can be reformulated as follows,

PROBLEM D*. *Is every field weakly-C_1?*

In Section 4 we have tried to attack this problem by using algebro-geometric methods to examine forms of small degrees. The case of degree 4 is the first non-trivial one. Indeed, we prove:

THEOREM I. *If K is a field of characteristic $\neq 2$, then for every form $f \in K[X_0, X_1, X_2, X_3, X_4]$ of degree 4 there exists a K-closed subset $W \subseteq V(f) \subseteq \mathbb{P}^4$ which is absolutely irreducible.*

In Section 5, we apply the decomposition intersection procedure to prove:

THEOREM J. *The existential theory of Ax-fields is decidable.*

Finally it is our pleasure to express our indebtedness to Andrzej Schinzel for inspiring conversations on quartic forms.

1. The decomposition-interaction procedure

The decomposition-intersection procedure has already been used by several authors in connection with diophantine problems (see e.g. Greenleaf [**10**] and Fried-Sacerdote [**8**]). To fix notation we describe here our version of the procedure.

We consider a fixed field K and denote by $\tilde{K}$ and K_s the algebraic closure of K and its separable closure, respectively. To every non-empty Zariski K-closed set A in the affine space $\mathbb{A}^n$ or in the projective space $\mathbb{P}^n$ we make correspond a canonical K-closed subset A', defined in the following way. First we present A as a union, $A = \bigcup_i V_i$, of distinct K-closed irreducible sets. Each one of the V_i's we decompose into its $\tilde{K}$-components, $V_i = \bigcup_j W_{ij}$. The W_{ij} form, for a fixed i, a complete system of conjugate absolutely irreducible varieties, defined over $\tilde{K}$. This implies that the intersection $U_i = \bigcap_j W_{ij}$ is invariant under the action of the absolute Galois group $G(K)$ of K. Hence, U_i is a K-closed set (cf. Lang [**17**, p. 74]). Define now $A' = \bigcup_i U_i$.

We then iterate the procedure and obtain a descending sequence $A \supseteq A' \supseteq A'' \supseteq \cdots \supseteq A^{(m)} \supseteq A^{(m+1)} \supseteq \ldots$, where $A^{(m+1)} = (A^{(m)})'$. The sequence becomes stationary after finitely many steps, i.e. there exists an m such that $A^{(m)} = A^{(m+1)} = \ldots$, since both $\mathbb{A}^n$ and $\mathbb{P}^n$ are Noetherian topological spaces (cf. Hartshorne [**12**, page 5]). Let $A^* = A^{(m)}$ be the smallest set in the sequence.

Each of the K-sets $A^{(k)}$, for $k = 0, 1, \ldots, m$, has finitely many $\tilde{K}$-components. Therefore there exists a finite Galois extension L of K such that all these $\tilde{K}$-components are L-closed.

The fundamental property of the procedure can be expressed in

LEMMA 1.1. *Let M be a field extension of K such that $L \cap M = K$. Then A^* is not empty if and only if A has a non-empty M-closed subset which is absolutely irreducible.*

Proof. Suppose first that A^* is not empty. Then, in order to be able to use the above notation, we may assume that $A = A^*$, i.e. $A = A'$, and A is not empty. Let x be a generic point of V_i over K. Then, since $A = A'$, there exists an i' such that $x \in U_{i'}$. Hence $x \in V_{i'}$, so that $V_i \subseteq V_{i'}$ and therefore $i = i'$, from which we deduce that $V_i \subseteq U_i$. On the other hand, $U_i \subseteq V_i$, by construction, hence $U_i = V_i$. This implies that V_i is absolutely irreducible, since otherwise there would exist at least two W_{ij} and hence we would have the contradiction

$$\dim V_i = \dim \bigcap_j W_{ij} < \dim V_i,$$

by the dimension theorem (cf. Lang [**17**, p. 36]). Obviously V_i is an M-closed set.

Conversely, suppose that A contains an M-closed subset W which is absolutely irreducible (and understood to be non-empty). Let x be a generic point of W over M. Then there exist i and j such that $x \in W_{ij}$. Hence $W \subseteq W_{ij}$. Every automorphism of L/K can be extended to an automorphism over M. Taking into account that all the W_{ij}'s are conjugate under the action of $\mathcal{G}(L/K)$, we conclude that $W \subseteq \bigcap_{j} W_{ij'} = U_i \subseteq A'$. Proceeding by induction we prove that $W \subseteq A^*$, which implies that A^* is not empty.

2. The main results

We recall that a field K is said to be $C_{i,d}$ if every form $f \in K[X_0, \ldots, X_n]$ of degree d with $d^i \leq n$ has a non-trivial zero in K^{n+1}. A field K is said to be C_i if it is $C_{i,d}$ for every $d \in \mathbb{N}$.

In the following lemma we collect some classical results about C_i fields which are going to be used in the sequel.

LEMMA 2.1. a) *Every algebraically closed field is* C_0.

b) (*Chevalley*) *Every finite field is* C_1.

c) (*Lang*) *The maximal unramified extension of* $\mathbb{Q}_p \cap \tilde{\mathbb{Q}}$ *is* C_1.

d) (*Tsen–Nagata–Lang*) *If a field* K *is* C_i *and* E *is an extension of* K *of transcendental degree* j, *then* E *is* C_{i+j}.

Proof. Assertion a) is trivial. Assertions b), c) and d) can be found in Greenberg's book [**9**], pages 11, 94 (see also p. 100) and 22, respectively.

If $f_1, \dots, f_m$ are polynomials in $K[X_0, \dots, X_n]$, then we denote by $V(f_1, \dots, f_m)$ the K-set of the common zeros of $f_1, \dots, f_m$ in the affine space $\mathbb{A}^{n+1}$. If the polynomials are homogeneous, then we use the same notation in order to denote the corresponding K-subset of the projective space $\mathbb{P}^n$.

A field K is said to be weakly-$C_{i,d}$, if for every form $f \in K[X_0, \dots, X_n]$ of degree d, with $d^i \leq n$, the K-set $V(f)$ of $\mathbb{P}^n$ contains a K-set W which is absolutely irreducible. A field K is said to be weakly-C_i if it is weakly-$C_{i,d}$ for every $d \in \mathbb{N}$.

A perfect field K is called an *Ax-field* if every absolutely irreducible variety W defined over K has a K-rational point.

It is immediate from our definitions that every $C_{i,d}$ field is also weakly-$C_{i,d}$. On the other hand, every Ax-field K which is weakly-$C_{i,d}$ is also $C_{i,d}$. Note that one has to use the fact that if K is perfect, then every K-set W which is absolutely irreducible is also defined over K (cf, Lang [**17**, p. 74]).

We denote by $G(K) = \mathcal{G}(K_s/K)$ the absolute Galois group of the field K. It is equipped with a Haar measure μ, as is introduced, e.g., in [**14**, p. 287]. For an e-tuple $\sigma = (\sigma_1, \dots, \sigma_e) \in G(K)^e$, we denote by $\tilde{K}(\sigma)$ and by $K_s(\sigma)$ the fixed field in $\tilde{K}$ and in K_s, respectively, of $\sigma_1, \dots, \sigma_e$. The absolute Galois group of $\tilde{K}(\sigma)$ is generated by $\sigma_1, \dots, \sigma_e$. If it is isomorphic to the free profinite group on e generators, then $\tilde{K}(\sigma)$ is said to be *e-free.*

LEMMA 2.2. *Let* K *be a countable Hilbertian field. Then:*

a) *For every* $e \in \mathbb{N}$ *and for almost all* $\sigma \in G(K)^e$, *the field* $\tilde{K}(\sigma)$ *is an e-free Ax-field.*

b) *Let* θ *be an elementary statement with coefficients in* K, *and let* $e \in \mathbb{N}$. *Then* θ *is true in* $\tilde{K}(\sigma)$ *for almost all* $\sigma \in G(K)^e$ *if and only if* θ *is true in every e-free Ax-field that contains* K.

Proof. See [**14**, Lemmas 7.2 and 7.3].

COROLLARY 2.3. *If* K *is a countable Hilbertian field, then* $\tilde{K}(\sigma)$ *is* C_1 *for almost all* $\sigma \in G(K)$.

Proof. By Lemma 2.2, for almost all $\sigma \in G(K)$, $\tilde{K}(\sigma)$ is a 1-free Ax-field. Hence $\tilde{K}(\sigma)$ is also C_1, by Theorem C.

The key lemma to the main results links all notions introduced in this section.

LEMMA 2.4. *Let K be a countable Hilbertian field. Then the following statements are equivalent:*

a) *Every finite algebraic extension of K is weakly-*$C_{i,d}$

b) *Every algebraic extension of K is weakly-*$C_{i,d}$.

c) *Every Ax-field which is algebraic over K is* $C_{i,d}$.

d) *For every* $e \in \mathbb{N}$ *and for almost all* $\sigma \in G(K)^e$ *the field* $\tilde{K}(\sigma)$ *is* $C_{i,d}$.

Proof. The implications a)$\Rightarrow$b)$\Rightarrow$c) are obvious. The implication c)$\Rightarrow$d) follows from Lemma 2.2a). In order to prove d)$\Rightarrow$a) we consider a finite extension K' of K and a form $f \in K'[X_0, \ldots, X_{d^i}]$ of degree d. Apply the decomposition–intersection procedure to $A = V(f)$ and attain a finite Galois extension L of K' as in the discussion preceding Lemma 1.1. Let $\sigma_1', \ldots, \sigma_e'$ be generators of $G(L/K')$. Then, there exist $\sigma_1, \ldots, \sigma_e \in G(K)$ that extend $\sigma_1', \ldots, \sigma_e'$, respectively, such that $\tilde{K}(\sigma)$ is $C_{i,d}$. In particular A has a $\tilde{K}(\sigma)$-rational point. In addition $L \cap \tilde{K}(\sigma) = K'$, hence A^* is not empty, by Lemma 1.1. Another use of Lemma 1.1, this time for $M = K'$, implies that A has a K'-closed subset which is absolutely irreducible. Thus K' is weakly-$C_{i,d}$.

LEMMA 2.5. *If K is a countable Hilbertian field and every finite extension of K is weakly* $C_{i,d}$, *then every Ax-field F that contains K is* $C_{i,d}$.

Proof. By the Skolem–Löwenheim theorem we may assume, without loss, that F is also countable. Then we find a purely transcendental extension K' of K such that F is algebraic over K'. The field K' is also Hilbertian (cf. Lang [**16**, p. 55]). By Lemma 2.2 and 2.4 the field $\tilde{K}(\sigma)$ is $C_{i,d}$, for every $e \in \mathbb{N}$ and for almost all $\sigma \in G(K)^e$. Hence, by Lemma 2.2, the field $\tilde{K}'(\sigma)$ is $C_{i,d}$, for every $e \in \mathbb{N}$ and for almost all $\sigma \in G(K')^e$. It follows from Lemma 2.4, that F is $C_{i,d}$.

THEOREM 2.6. a) *Every Ax-field F of characteristic* $p > 0$ *is* C_2. *(This result was also independently obtained by U. Kiehne, A. Macintyre and L. van den Dries.)*

b) *Every Ax-field that contains an algebraically closed field is* C_1.

c) *Every Ax-field that contains the maximal unramified extension U of* $\mathbb{Q}_p \cap \tilde{\mathbb{Q}}$ *is* C_2.

Proof. a) If F is algebraic over $\mathbb{F}_p$, then F is even C_1, by Lemma 2.1. Otherwise F contains the Hilbertian field $\mathbb{F}_p(t)$, where t is transcendental over $\mathbb{F}_p$. By Lemma 2.1, every finite extension of $\mathbb{F}_p(t)$ is C_2. Hence, by Lemma 2.5, F is also C_2. Assertion b) and c) are proved in the same way.

3. Weakly-C_i fields

Weakly-C_i fields play an important role in the proof of Theorem 2.6. It is therefore not without interest to study the properties of weakly-C_i fields for their own sake. In particular this study leads to an alternative, 'algebraic' proof of Theorem 2.6. However, since the proofs of the basic properties of the weakly-C_i fields are, more or less, a repetition of the proofs for the C_i-fields, we do not bring them in full detail and emphasize only the new ingredients.

Our first step is to reformulate the concept of quasi-C_i fields in terms of points. We recall that an extension F of a field K is said to be *primary* if $K_s \cap F = K$.

LEMMA 3.1. *A field K is weakly-$C_{i,d}$ if and only if every form $f \in K[X_0, \ldots, X_n]$ of degree d with $d^i \leq n$ has a zero $x = (x_0, \ldots, x_n) \neq (0, \ldots, 0)$ such that the rational function field $K(x)$ is a primary extension of K.*

Proof. Suppose that K is weakly-$C_{i,d}$ and let f be a form as above. Then the K-set $V(f)$ in $\mathbb{P}^n$ has a K-closed subset W which is absolutely irreducible. Then W is defined over a purely inseparable extension K' of K. Let x be a generic point of W over K'. Then x is a non-trivial zero of f and $K(x)/K$ is a primary extension.

Conversely suppose that f and x are as stated in the lemma and that $K(x)$ is a primary extension of K. Denote by W the K-closed set generated by x in $\mathbb{P}^n$. Then W is irreducible over K_s, since $k(x)$ is linearly disjoint from K_s over K (cf. [**17**, p. 67]). Hence W is absolutely irreducible, since its $\tilde{K}$-components must be conjugate over K_s (cf. [**17**, p. 34]).

The next lemma is the analog of Lemma 3.1 and 3.2 of [**9**].

LEMMA 3.2. *Let K be a field which is not separably closed and let k_0 be an integer. Then there exists a form $\varphi \in K[X_1, \ldots, X_k]$ of degree $k > k_0$ such that if $K(x_1, \ldots, x_k)$ is a primary extension of K, then*

$$\varphi(x_1, \ldots, x_k) = 0 \Rightarrow x_1 = \cdots = x_k = 0. \tag{1}$$

Proof. By assumption K has a Galois extension L of degree $l > 1$ with, say, a Galois group G. Let $\omega_1, \ldots, \omega_l$ be a basis for L/K and consider the form

$$\psi = \prod_{\sigma \in G} (\omega_1^\sigma X_1 + \cdots \omega_l^\sigma X_l)$$

of degree l and with coefficients in K. If $\psi(x) = 0$, then there exists a $\sigma \in G$ such that

$$\omega_1^\sigma x_1 + \cdots + \omega_l^\sigma x_l = 0. \tag{2}$$

Furthermore, if $K(x_1, \ldots, x_l)/K$ is a primary extension, then $K(x_1, \ldots, x_l)$ is linearly disjoint from L over K and hence $x_1 = \cdots = x_l = 0$.

Next construct the form

$$\psi_2 = \psi(\psi(X_1, \ldots, X_l), \psi(X_{l+1}, \ldots, X_{2l}), \ldots, \psi(X_{(l-1)l+1}, \ldots, X_{l^2}))$$

It is of degree l^2 and has the property (1). Iterating this procedure, we obtain the desired form φ.

Based on Lemma 3.2 one can next prove the analog to Theorem 3.4 of [**9**].

PROPOSITION 3.3. *Let K be a weakly-C_i field and let $f_1, f_2, \ldots, f_r$ be forms over K of degree d with n variables. If $n > rd^i$, then $f_1, f_2, \ldots, f_r$ have a common non-trivial zero in some primary extension of K.*

Then one proceeds to attain the analog of Theorem 3.6 of [**9**].

PROPOSITION 3.4. *If a field K is weakly-C_i and E is an extension of K of transcendence degree j, then E is weakly-C_{i+j}.*

An entirely new property of weakly-C_i fields appears if the basic field is Hilbertian.

PROPOSITION 3.5. *If a Hilbertian field K is weakly-C_i, then every extension of K is also weakly-C_i.*

Proof. Using Proposition 3.4, it suffices to prove that $K(t)$ is weakly-C_i, when t is transcendental over K. This has been essentially done in Section 2 by model-theoretic methods. Here we shall only sketch an algebraic proof for this statement.

We have to take a form $f \in K(t)[X_0, \ldots, X_{d^i}]$ of degree d, consider the projective $K(t)$-closed set $A = V(f)$, apply the decomposition-intersection procedure to A and prove that the corresponding set A^* is not empty. In this procedure we produce finitely many $K(t)$-irreducible subsets V of A and consider their $\widetilde{K(t)}$-components W_j. All of these sets are defined over a finite normal extension F of $K(t)$. We then specialize t to an element $\bar{t}$ of K and reduce all the corresponding objects. The specialization $t \to \bar{t}$ has to be done such that, (among others) the degree of F over $K(t)$ is unchanged, the V's remain irreducible and the W_j remain absolutely irreducible. The first two conditions are guaranteed by the Hilbertian property and the last one by, say, the Bertini–Noether theorem (cf. Lang [**16**, p. 157]).

The reduced algebraic sets obtained are exactly those which appear in the decomposition-intersection procedure applied to the reduced set $\bar{A}$. In particular $\bar{A}^*$ is not empty, since K is assumed to be quasi-C_i. Hence A^* is not empty.

COROLLARY 3.6. a) *Every field of a positive characteristic is weakly-C_2.*
b) *Every field that contains an algebraically closed field is weakly-C_2.*
c) *etc.*

In particular this corollary supplies an algebraic proof to Theorem 2.6.

A primary extension of a primary extension of a field K is again a primary extension of K. Using Lemma 3.1 we have a kind of a 'going-down' property of weakly-C_i fields.

LEMMA 3.7. *If L is a primary extension of a field K and if L is weakly-C_i, then K is also weakly-C_i.*

COROLLARY 3.8. *Let K be a global field. Then $K_s(\sigma)$ is a weakly-C_i field for every $\sigma \in G(K)$. It follows that every Ax-field that contains $K_s(\sigma)$ is C_2.*

Proof. By a theorem of Ax, there exists a non-principal ultra-product F of finite fields such that $K_s \cap F = K_s(\sigma)$ (see [**1**, p. 175]). The field F is C_1, since the finite fields are. Hence $K_s(\sigma)$ is weakly-C_1, by Lemma 3.7.

COROLLARY 3.9. *The field $\mathbb{R}$ of the real numbers is weakly-C_1.*

Proof. The field $\mathbb{R}_{\text{alg}} = \tilde{\mathbb{Q}} \cap \mathbb{R}$ is of the form $\tilde{\mathbb{Q}}(\sigma)$, where σ is the complex conjugation. Hence, as in the proof of Corollary 3.8, there exists an ultraproduct F of finite fields such that $\mathbb{R}_{\text{alg}} = \tilde{\mathbb{Q}} \cap F$. As is well-known, $\mathbb{R}_{\text{alg}}$ is an elementary subfield of R. By Scott's Lemma, (cf. Bell and Slomson [**3**, p. 163]) $\mathbb{R}$ can be elementarily embedded in an ultrapower $^*\mathbb{R} = \mathbb{R}_{\text{alg}}^I/\mathcal{D}$ of $\mathbb{R}_{\text{alg}}$. Then $\mathbb{R}$ can be considered as an algebraically closed subfield of $^*F = F^I/\mathcal{D}$. The field $^*F$ is C_1, since F is. It follows from Lemma 3.7 that $\mathbb{R}$ is weakly-C_1.

Note that we have used here model-theoretic methods to derive a result for $\mathbb{R}$ from properties of finite fields.

We are not in a position to decide whether or not $\mathbb{Q}$ is weakly-C_1. The following proposition is a partial result in that direction.

PROPOSITION 3.10. *For every field K and for every positive integer d there exists a finite extension K_d of K which is weakly-$C_{1,d}$.*

Proof. By Theorem 2.6 every Ax-field containing $\tilde{K}$ is C_1. Let T be a set of axioms for Ax-fields that contain K (cf. [**14**, p. 278]) and let Δ be the diagram of $\tilde{K}$ (cf. Chang–Keisler [**4**, p. 78]). Then every model of $T \cup \Delta$ is a C_1-field. By Gödel completeness theorem $C_{1,d}$ is provable from $T \cup \Delta$. Hence $C_{1,d}$ is provable from a set $T \cup \Delta_0$, where Δ_0 is a finite subset of Δ. Let K_d be a finite extension of K that contains all the elements of $\tilde{K}$ appearing in Δ_0. Then every Ax-field that contains K_d is $C_{1,d}$. If K is Hilbertian and countable, then we deduce from Lemma 2.4

that K_d is weakly-$C_{1,d}$. In the general case K contains a countable Hilbertian field E (unless K is algebraic over a finite field, in which case K is already C_1). Hence E has a finite extension E_d, which is weakly-$C_{1,d}$ and such that every Ax-field containing E_d is $C_{1,d}$. We claim that the field $K_d = KE_d$ is weakly-$C_{1,d}$. Indeed, if $f \in K_d[X_0, \ldots, X_d]$ is a form of degree d, then its coefficients belong to a countable Hilbertian field L that contains E_d. By Lemma 2.4, L is weakly-$C_{1,d}$, hence $V(f)$ contains an L-closed set W which is absolutely irreducible. The set W is obviously also K_d-closed, consequently K_d is weakly-$C_{1,d}$.

4. Quartics

This section presents an attempt to attack problem D^* the hard way, i.e. by carrying out the decomposition–intersection procedure directly, using diophantine methods. We have not gone very far in this direction and have essentially treated only forms of degree 4. It turns out that already in this case the procedure is quite involved. To handle forms of degree 6 by these methods appears to be very difficult.

Throughout this section we are working over a field K of characteristic not 2.

LEMMA 4.1. *If d is a prime and $f \in K[X_0, \ldots, X_d]$ is an irreducible form of degree d, then $V(f)$ contains a non-empty K-closed set W of $\mathbb{P}^d$ which is absolutely irreducible.*

Proof. If f is irreducible over K_s, take $W = V(f)$. Otherwise f decomposes over K_s, $f = \varphi_1 \varphi_2 \cdots \varphi_c$, where $c > 1$ and the φ_i are irreducible over K_s. All the φ_i are conjugate over K. In particular they have the same degree. Thus $d = c \cdot \deg \varphi_i$ implies that $c = d$ and that $\deg \varphi_i = 1$. The linear subvariety $W = V(\varphi_1, \varphi_2, \ldots, \varphi_d)$ of $V(f)$ is K-closed and non-zero, since there are more variables than forms. Obviously W is also absolutely irreducible.

COROLLARY 4.2. *If $f \in K[X_0, \ldots, X_d]$ is a form of degree d and $d =$ 1, 2, 3, 5, 7 or 11, then $V(f)$ contains a non-empty K-closed set W of $\mathbb{P}^d$ which is absolutely irreducible.*

Proof. If $d = 2$ or 3, then either f is irreducible over K and Lemma 4.1 applies or f is reducible over K and hence has a linear factor φ with coefficients in K. In the later case $V(\varphi) \subseteq V(f)$. If $d = 5$, then either f is irreducible over K and Lemma 4.1 applies or f has a factor g which is irreducible over K and of degree at most 2. Then $V(g) \subseteq V(f)$ and as noted, $V(g)$ contains a non-zero K-closed set W which is absolutely irreducible.

If $d = 7$, then either f is irreducible and Lemma 4.1 applies or f has a factor g of degree <3 and we can use the preceding paragraph.

Suppose finally that $d=11$. If f is irreducible over K, then Lemma 4.1 applies, otherwise f has a K-factor g of degree ≤ 5. If $\deg g \neq 4$, then the first paragraph applies, if $\deg g=4$, then f has also a factor h of degree 7 and we can use the preceding paragraph.

LEMMA 4.3. *Let $\tilde{K}$ be an algebraically closed field and let q_1, q_2 be quadratic forms over $\tilde{K}$ in the variables X_0, X_1, X_2, X_3, X_4 such that the projective set $V(q_1, q_2)$ has dimension 2. Suppose that $V(q_1, q_2) = \bigcup_{i=1}^{4} V(\lambda_{i1}, \lambda_{i2})$, where the λ_{ij} are linear forms over $\tilde{K}$. Then no five forms λ_{ij} are linearly independent over $\tilde{K}$.*

Proof. Assume that there are five λ_{ij} which are linearly independent. There are two cases.

Case I. There are i and j such that $\lambda_{i1}, \lambda_{i2}, \lambda_{j1}, \lambda_{j2}$ are linearly independent. Thus, after a linear change of coordinates we may suppose that $V(X_1, X_2)$, $V(X_3, X_4)$, $V(X_0, \lambda)$ are components of $V(q_1, q_2)$, where λ is a linear form not containing X_0. For $k=1,2$ we write q_k in the form

$$q_k = aX_0^2 + (b_1X_1 + b_2X_2 + b_3X_3 + b_4X_4)X_0 + p(X_1, X_2, X_3, X_4), \quad (1)$$

where $a, b_1, b_2, b_3, b_4 \in \tilde{K}$ and p is a quadratic form over $\tilde{K}$. Using the fact that q_k vanishes on $V(X_1, X_2)$ and on $V(X_3, X_4)$, we deduce that $a=b_1=b_2=b_3=b_4=0$, which means that X_0 does not appear in q_k. Moreover, q_k vanishes on $V(X_0, \lambda)$, hence, $q_k = f_kX_0 + g_k\lambda$, with f_k and g_k polynomials, and g_k not containing X_0. It follows now that $f_k=0$, since q_k, g_k and λ do not contain X_0. Thus $q_1 = g_1\lambda$ and $q_2 = g_2\lambda$. Therefore $V(\lambda) \subseteq V(q_1, q_2)$, contrary to $\dim V(q_1, q_2) = 2$.

Case II. We suppose Case I does not occur. Since $V(q_1, q_2) = 2$, for each $i=1,2,3,4$, the pair $\lambda_{i1}, \lambda_{i2}$ is a linearly independent set. Hence, if some five of the λ_{ij} form a linearly independent set, we may, after a change of variables, assume

$$\lambda_{11} = X_1, \lambda_{21} = X_2, \lambda_{31} = X_3, \lambda_{41} = X_4, \lambda_{12} = X_0.$$

Being in Case II implies that $\lambda_{01}, \lambda_{02}, \lambda_{i1}, \lambda_{i2}$ are linearly dependent, and since we can remove X_i from λ_{i2}, we may assume that $\lambda_i = a_iX_0 + b_iX_i$, for $i=2,3,4$. Similarly, if $2 \leq i < j \leq 4$, then $X_i, X_j, \lambda_{i2}, \lambda_{j2}$ are linearly dependent and hence $\lambda_{22} = \lambda_{32} = \lambda_{42}$ $(= aX_0 + bX_1 = \lambda$, say). If, say, $a \neq 0$, then we may replace X_0 by λ and finally make another change of variables to assume that $\lambda = X_0$. Thus q_1 and q_2 both vanish on $V(X_i, X_0)$ for $i=1,2,3,4$. This implies, in the notation (1), that $p=0$. Therefore $V(X_0) \subseteq V(q_1, q_2)$ which is again a contradiction to the assumption $\dim V(q_1, q_2) = 2$.

LEMMA 4.4. *If $q_1, q_2 \in K[X_0, X_1, X_2, X_3, X_4]$ are quadratic forms, then*

$V(q_1, q_2)$ contains a non-empty K-closed subset $W \subseteq \mathbb{P}^4$ which is absolutely irreducible.

Proof. If K' is a purely inseparable extension of K, then every K'-closed subset of $\mathbb{P}^4$ is also K-closed. Therefore, replacing K by its maximal purely inseparable extension, we may assume that K is a perfect field.

If some form in the rational pencil

$$\{a_1q_1 + a_2q_2 \mid a_1, a_2 \in K, \text{ not both } 0\} \tag{2}$$

vanishes on a K-closed linear variety Λ of dimension $m \geq 2$, then $V(q_1, q_2) \supseteq V(q_i) \cap \Lambda = B$, for $i = 1$ or $i = 2$, where B is K-closed and is either equal to Λ or is projectively equivalent over K to a quadratic hypersurface in $\mathbb{P}^m$. By Corollary 4.2, B contains a K-closed set which is absolutely irreducible. Thus we can assume

No form in the rational pencil (2) vanishes on a K-closed linear variety of dimension ≥ 2. (3)

In particular (3) implies

No form in the rational pencil (2) splits over $\tilde{K}$. (4)

Indeed, if a form q of (2) splits, $q = \lambda\mu$, then either λ has coefficients in K, or λ has coefficients in a quadratic extension of K and is conjugate to μ. In the former case q vanishes on the K-closed hyperplane $V(\lambda)$ and in the latter q vanishes on $V(\lambda, \mu)$ a contradiction to (3).

If $V(q_1, q_2) = V(q_k)$ for $k = 1$ or $k = 2$, then our conclusion follows from Corollary 4.2. Hence we can assume that $V(q_1, q_2) \neq V(q_k)$ and therefore that $\dim V(q_1, q_2) = 2$. Obviously we may also assume that $V(q_1, q_2)$ is not absolutely irreducible.

Let $V(q_1, q_2) = \bigcup_{i=1}^{n} Z_i$ be a decomposition into $\tilde{K}_0$-components. Then $4 = (\deg q_1)(\deg q_2) = \sum_{i=1}^{n} k_i \cdot \deg Z_i$, where k_i is the intersection multiplicity of $V(q_1)$ and $V(q_2)$ along Z_i (cf. [**12**, p. 53]). It follows that $2 \leq n \leq 4$. If any Z_i is defined over K, we have the desired conclusion. Hence we may suppose that no Z_i is defined over K. If all the Z_i's are linear, then they have the form $Z_i = V(\lambda_{i1}, \lambda_{i2})$, where $\lambda_{i1}, \lambda_{i2}$ are linear forms over $\tilde{K}$, since $\dim Z_i = 2$. The set $\{Z_1, \ldots, Z_n\}$ is closed under conjugation. Hence, its intersection is a K-closed linear variety which is contained in $V(q_1, q_2)$ and, by Lemma 4.3, is not empty. We may therefore assume that one of the Z_i's is non-linear. Then its conjugate over K is also non-linear. Thus

$V(q_1, q_2) = Z \cup \bar{Z}$, where $Z, \bar{Z}$ are absolutely irreducible L-closed conjugate quadratic surfaces and L is a quadratic extension of K. (5)

Our proof will be complete if we show that (4) and (5) lead to a contradiction. Indeed, Hodge and Pedoe show in [**11**, p. 202 and 204] that it is possible to change variables over $\tilde{K}$ such that Z attains the form $V(X_0, p'(X_1, X_2, X_3, X_4))$, where p' is a quadratic form over $\tilde{K}$. Making the inverse change we find that $Z = V(\lambda, p)$, where λ is a linear form and
3 p is a quadratic form over $\tilde{K}$. We claim:

$$\text{The ideal } \langle \lambda, p\rangle \text{ of } \tilde{K}[X_0, X_1, X_2, X_3, X_4] \text{ is prime.} \tag{6}$$

Indeed, we may again suppose that λ is X_0 and that p does not contain X_0. Then

$$\tilde{K}[X_0, X_1, X_2, X_3, X_4]/\langle \lambda, p\rangle \cong K[X_1, X_2, X_3, X_4]/\langle p\rangle.$$

If $\langle \lambda, p\rangle$ is not prime, then the above ring is not an integral domain, hence p is not irreducible. Thus $p = \pi_1\pi_2$, where π_1 and π_2 are linear forms. Thus $Z = V(\lambda, \pi_1) \cup V(\lambda, \pi_2)$ is a union of two linear varieties, a contradiction to (5).

It follows from (6) that $q_1, q_2 \in \langle \lambda, p\rangle$. Hence there exist $c_1, c_2 \in \tilde{K}$ and linear forms γ_1, γ_2 over $\tilde{K}$ such that $q_1 = c_1 p + \gamma_1\lambda$ and $q_2 = c_2 p + \gamma_2 \lambda$. Moreover, by (4) $c_1 \neq 0$ and $c_2 \neq 0$. Hence $cq_1 - q_2 = (c\gamma_1 - \gamma_2)\lambda$, where $c = c_2 c_1^{-1}$ and (4) implies that $c \notin K$. Let $c^\sigma \neq c$ be a conjugate to c over K. Then the linear form λ^σ divides $c^\sigma q_1 - q_2$ and therefore $V(\lambda, \lambda^\sigma) \subseteq V(q_1, q_2)$. This is a contradiction to the assumption that no $\tilde{K}$-component of $V(q_1, q_2)$ is linear.

LEMMA 4.5. *If $f \in K[X_0, X_1, X_2, X_3, X_4]$ is a quartic form, then $V(f)$ contains a K-closed subset W of $\mathbb{P}^4$ which is absolutely irreducible.* (*L. van den Dries informed the authors that he had also obtained this result.*)

Proof. We may assume again that K is a perfect field. If f is reducible over K, it has a factor g of degree 1 or 2 with coefficients in K and we may use Corollary 4.2 to obtain W. Thus we may suppose that f is irreducible over K. In this case f factors over $\tilde{K}$ as $f = g_1 \cdots g_m$, where m equals 1, 2 or 4 and the g_i are conjugate over K. If $m = 4$, then the g_i are linear and $V(f)$ contains the K-closed non-empty linear variety $V(g_1, g_2, g_3, g_4)$. If $m = 1$ then $V(f)$ is absolutely irreducible. If $m = 2$, then the g_i are quadratic and $V(f)$ contains the variety $V(g_1, g_2)$. The g_i may be chosen to be defined over a quadratic extension L of K with a basis e_1, e_2. Thus $g_1 = e_1 q_1 + e_2 q_2$, where q_1, q_2 are quadratic forms with coefficients in K. Hence $V(g_1, g_2) = V(q_1, q_2)$ and, by Lemma 4.4, the last variety contains W.

COROLLARY 4.6. *If $f \in K[X_0, \ldots, X_{13}]$ is a form of degree* 13, *then $V(f)$ contains a K-closed set W which is absolutely irreducible.*

Proof. If f is reducible over K, then it must have a factor of degree

$1, 2, 3, 4, 5$ or 7 and the conclusion follows from Corollary 4.2 and Lemma 4.4. If f is irreducible over K, then we use Lemma 4.1.

Combining all the lemmas together, we arrive at the following result.

THEOREM 4.7. *Every field K of characteristic not 2 is weakly-$C_{1,d}$ for $d = 1, 2, 3, 4, 5, 7, 11$ and 13.*

COROLLARY 4.5. *Every Ax-field K of characteristic not 2 is $C_{1,d}$ for $d = 1, 2, 3, 4, 5, 7, 11$ and 13.*

5. The existential theory of Ax-fields

The elementary theory of Ax-fields has been proved to be undecidable (see [**5**]). It is therefore not without interest to observe here that the decomposition–intersection procedure leads to a decision procedure for the existential theory of Ax-fields.

A sentence in the elementary language of the theory of fields is said to be *existential* if it has the form

$$\exists X_1 \cdots \exists X_n \Big[\bigvee_i \bigwedge_j f_{ij}(X) = 0 \wedge g_{ij}(X) \neq 0 \Big], \tag{1}$$

where f_{ij} and g_{ij} are polynomials with integral coefficients. We may replace each inequality $g_{ij}(X) \neq 0$ by the equivalent formula $\exists Y_{ij}[Y_{ij} g_{ij}(X) - 1 = 0]$. Thus we may assume that the sentence has the form

$$\exists X_1 \cdots \exists X_n \Big[\bigvee_i \bigwedge_j f_{ij}(X) = 0 \Big]. \tag{2}$$

The formula in the square brackets of (2) defines a $\mathbb{Q}$-closed algebraic set A of the affine space $\mathbb{A}^n$. Thus (2) can be rewritten in the form

$$\exists X_1 \cdots \exists X_n [X \in A]. \tag{3}$$

In order to test whether (3) is true in every Ax-field of characteristic 0 one applies the decomposition–intersection procedure for A over $\mathbb{Q}$. This can effectively be done by elimination theory (cf. Van der Waerden [**20**, p. 116] and [**19**, § 37] or Ax [**1**, § 2]).

If A^* is empty, then we consider an Ax-field M that contains $\mathbb{Q}$ such that $L \cap M = \mathbb{Q}$. Here L is the finite Galois extension of $\mathbb{Q}$ over which all the absolutely irreducible varieties that occur in the procedure are defined. Indeed, we may take M as $\tilde{\mathbb{Q}}(\sigma_1, \ldots, \sigma_e)$ with suitable $e \in \mathbb{N}$ and $\sigma_1, \ldots, \sigma_e \in G(\mathbb{Q})$, as has already been shown in the proof of Lemma 2.4. By Lemma 1.1, A has no M-rational point. Hence if A^* is empty, then (3) fails to be true in some Ax-field that contains $\mathbb{Q}$.

If A^* is not empty, then, by Lemma 1.1, A has a $\mathbb{Q}$-closed subset W which is absolutely irreducible and one can effectively find W. The variety

W has an M-rational point in every Ax-field M that contains $\mathbb{Q}$. In this case (3) is true in every such M.

Now we find a finite set of primes, S, such that W is defined and absolutely irreducible when considered as an $\mathbb{F}_p$-closed set for every prime p not in S (cf. Ax [**2**, p. 253] and [**1**, p. 169]). Then we repeat the decomposition-intersection procedure for A over $\mathbb{F}_p$, for each $p \in S$. If A^* is not empty in each of these cases, then (3) is true in every Ax-field. Otherwise (3) is false in some Ax-field. Indeed if L is a finite extension of $\mathbb{F}_p$, then there exists an infinite algebraic extension M of $\mathbb{F}_p$ such that $gcd([L:\mathbb{F}_p], [M:\mathbb{F}_p]) = 1$. The field M is an Ax-field, by Lang–Weil's theorem [**18**] and $L \cap M = \mathbb{F}_p$. One applies Lemma 1.1 once more.

We have thus proved:

THEOREM 5.1. a) *The existential theory of Ax-fields of a given characteristic is decidable.*

b) *The existential theory of Ax-field is decidable.*

REFERENCES

1. J. Ax, 'Solving diophantine problems modulo every prime', *Annals of Mathematics* 85 (1967), 161–183.

2. J. Ax, 'The elementary theory of finite fields', *Annals of Mathematics* 88 (1968), 239–271.

3. J. L. Bell and A. B. Slomson, *Models and ultraproducts*, North-Holland, Amsterdam, 1974.

4. C. C. Chang and H. J. Keisler, *Model theory*, North-Holland, Amsterdam, 1973.

5. G. Cherlin, L. v. d. Dries and A. Macintyre. 'Decidability and undecidability theorems for PAC-fields', *Bulletin of the AMS* 4 (1981), 101–104.

6. C. Chevalley, (*Demonstration d'une hypothèse de M. Artin*), Abb. Math. Seminar Univ. Hamburg 11 (1936), 73–75.

7. M. Fried and M. Jarden, 'Diophantine properties of subfields of $\tilde{\mathbb{Q}}$', *American Journal of Math.* 100 (1978), 653–666.

8. M. Fried and G. Sacerdote, 'Solving diophantine problems over all residue class fields of a number field and all finite fields', *Annals of Mathematics* 104 (1976), 203–233.

9. M. J. Greenberg, *Lectures on forms in many variables*, Benjamin, New-York, 1969.

10. M. Greenleaf, 'Irreducible subvarieties and rational points', *American Journal of Math.* 87 (1965), 25–31.

11. W. V. D. Hodge and D. Pedoe, *Methods of algebraic geometry II*, Cambridge, At the University Press, 1952.

12. R. Hartshorne, *Algebraic geometry*, Springer-Verlag, New-York, 1977.

13. M. Jarden, 'The elementary theory of ω-free Ax-fields', *Inventiones math.* 38 (1976), 187–206.

14. M. Jarden and U. Kiehne, 'The elementary theory of algebraic fields of finite corank', *Inventiones math.* 30 (1975), 275–294.

15. S. Lang, 'On quasi algebraic closure', *Annals. of Math.* 55 (1952), 373–390.

16. S. Lang, *Diophantine geometry*, Interscience Publishers, New-York, 1962.

17. S. Lang, *Introduction to algebraic geometry*, Interscience Publishers, New-York, 1964.

18. S. Lang and A. Weil, 'Number of points of varieties in finite fields', *American Journal of Math.*, 76 (1954), 819–827.
19. B. L. Van der Waerden, *Modern algebra I*, Frederick Unger, New York, 1953.
20. B. L. Van der Waerden, *Einführung in die algebraische Geometrie*, Springer Verlag, Berlin, 1973.

(*JD*) *Department of Mathematics*
Katholieke Universiteit
Leuven
3000 Louvain
Belgium

(*MJ*) *School of Mathematical Sciences*
Tel-Aviv University
Ramat-Aviv
Israel

(*DJL*) *Mathematics Department*
Michigan University
Ann Arbor MI 48104 USA