ADVANCES IN MATHEMATICS 47, 74–87 (1983)

Elimination of Quantifiers in Algebraic Structures

ANGUS MACINTYRE, KENNETH MCKENNA,* LOU VAN DEN DRIES†

Department of Mathematics, Yale University, New Haven, Connecticut 06520

INTRODUCTION

One of the first techniques used in the study of the logical properties of algebraic objects was that of *elimination of quantifiers*. It was, for example, used by Tarski [16] to prove the decidability of the theory of any given algebraically closed field and the decidability of the theory of real closed ordered fields. The theories of various other algebraic structures (e.g., the p-adic numbers, divisible ordered abelian groups) may also be shown to eliminate quantifiers in appropriate languages. The choice of the language is especially important in these dealings. It must be chosen to lie close to natural algebraic phenomena. Any structure may be made to admit *elimination* of quantifiers by the choice of a sufficiently complex language: the structure may be Skolemized or Morleyized [15]. Clearly the resulting languages are too far from the natural relations on the objects to be of immediate algebraic interest.

In this paper we will show that for many natural languages those structures which have been shown in the past to admit elimination of quantifiers are, in fact, the *only* structures of their type to admit elimination of quantifiers in that language. In particular we will show that apart from the finite fields and the algebraically closed fields there are no other fields which admit elimination of quantifiers *in the language of rings with identity* (i.e., the language with primitives $+$, $\cdot$, $-$, 0, 1).[1] We will show that the only theory of ordered fields that admits elimination of quantifiers in the natural language of ordered domains is the theory of real closed ordered fields. We show that if K is a nontrivially valued field admitting elimination of quantifiers in the language of valued fields then K is algebraically closed. Now the theory of the p-adic numbers *does not* admit elimination of quantifiers in the pure language of valued fields (cf. [12]). However, if we include certain auxilary predicates $\{P_n(x)\}$ such that $P_n(x)$ holds if and only if x has an nth

* Present address: University of Chicago Law School, Chicago, Ill.

† Present address: Institute for Advanced Study, School of Mathematics, Princeton University, Princeton, N.J.

[1] This had been demonstrated previously by Macintyre [11] but by much more complicated arguments than we give here.

0001-8708/83/010074-14$07.50/0

root then $\mathbb{Q}_p$ does admit elimination of quantifiers [12]. We will prove a converse of this theorem, probably not best possible. (See discussion below.)

The notion of a ***model complete theory*** is related to elimination of quantifiers. A theory T is model complete if for every formula $\varphi(\bar{x})$ with free variables $\bar{x}$, there is a quantifier free formula $\psi(\bar{x}, \bar{y})$ so that $T \vdash \forall \bar{x}[\varphi(\bar{x}) \leftrightarrow \exists \bar{y}\psi(\bar{x}, \bar{y})]$. In his thesis McKenna shows that, although theories admitting elimination of quantifiers are rare, model complete theories are comparatively common in the following sense:

Let G be the Galois group of the algebraic closure $\tilde{\mathbb{Q}}$ over $\mathbb{Q}$. Then G is a compact group and hence possesses a unique translation invariant (Haar) measure, μ. It is a simple consequence of work of Jarden [8] that $\mu\{\sigma \in G | \mathrm{Th}(\mathrm{Fix}(\sigma))$ is model complete in the language of rings$\} = 1$. Let $\pi \in G$ be an involution, so $\pi^2 = \mathrm{id}_{\tilde{\mathbb{Q}}}$. Then $\mathrm{Fix}(\pi)$ is a real closure of $\mathbb{Q}$ and so $\mathrm{Th}(\mathrm{Fix}(\pi))$, which is, of course, the theory of real closed fields, is model complete as an ordered field. Moreover, $\mu\{\sigma \in G | \mathrm{Th}(\mathrm{Fix}(\pi) \cap \mathrm{Fix}(\sigma))$ is model complete as an ordered field$\} = 1$. This is proved by introducing a notion of *pseudo-real-closed* fields (prc fields), which is the real analogue of the notion of pseudo-algebraically closed field discussed by *Ax*, Jarden and others [1, 8]. Similarly he defines a notion of *pseudo-p-adically closed* field and uses it to prove that, if K_p is the relative algebraic closure of $\mathbb{Q}$ in $\mathbb{Q}_p$, then $\mu\{\sigma \in G | \mathrm{Th}(\mathrm{Fix}(\sigma) \cap K_p)$ is model complete$\} = 1$. It follows that there are $2^{\aleph_0}$ model complete theories of pseudo-real-closed fields (resp. pseudo-p-adically closed).

1. Preliminaries

Consider a theory T in a first order language L. T is said to admit QE (= quantifier elimination) if for every L-formula $\psi(\bar{x})$, $\bar{x}$ being a sequence of free variables, there is a quantifier free L-formula $\phi(\bar{x})$ such that $T \vdash \forall \bar{x}[\phi(\bar{x}) \leftrightarrow \psi(\bar{x})]$. Notice that we always work relative to the language L and as we vary L the nature of the formula $\psi(\bar{x})$ varies accordingly.

2. Algebraically Closed Fields

Theorem (Tarski). *Let L be the language of rings with identity. Let ACF be the theory of algebraically closed fields as formulated naturally in L. Then ACF admits elimination of quantifiers with respect to L.*

We will now prove the following converse of Tarski's Theorem:

Theorem 1. *Let K be an infinite field whose L-theory admits* QE. *Then K is algebraically closed.*

Toward this end we prove the following.

LEMMA 1. *Let $\Phi(\bar{x})$, $\bar{x} = \langle x_1, \ldots, x_n \rangle$, be a quantifier free formula in L. Then $\Phi(\bar{x})$ is equivalent with respect to field theory to a disjunction of formulas of type $p_1(\bar{x}) = p_2(\bar{x}) = \cdots = p_m(\bar{x}) = 0 \wedge q(\bar{x}) \neq 0$, where the p_i and q are in $\mathbb{Z}[\bar{x}]$. We will say that this is a disjunct of type (A).*

Proof. Trivial manipulations.

Proof of Theorem 1. We argue by contradiction. Let K have an algebraic extension $K(\alpha)$ of degree $n > 1$. Let $f(y, \bar{x}) = y^n + x_{n-1} y^{n-1} + \cdots x_0$. Then there is a quantifier free formula $\Phi(\bar{x})$, which we may take as a disjunction of formulas of type (A) which is equivalent in K to the formula $\forall y f(y, \bar{x}) \neq 0$. Assume first that α is separable over K.

Let $\alpha = \alpha_1, \ldots, \alpha_n$ be the distinct conjugates of α over K. Let $z_1, \ldots, z_n$ be n new variables. Finally put $F(\bar{z}, y)$ equal to $\Pi(y - (z_1 + z_2\alpha_j + \cdots + z_n\alpha_j^{n-1}))$. It is clear $F(\bar{z}, y) \in K[\bar{z}, y]$. Let $F(\bar{z}, y) = F_0(\bar{z}) + \cdots + F_{n-1}(\bar{z}) y^{n-1} + y^n$. We claim $\{F_i(\bar{z})\}_{0 \leqslant i \leqslant n-1}$ is algebraically independent over K. It is plainly enough to show that z_i is algebraic over $L = K(F_0(\bar{z}), \ldots, F_{n-1}(\bar{z}))$. Clearly the roots of $F(\bar{z}, y)$ are algebraic over L. These roots are $r_j = z_1 + z_2\alpha_j + \cdots + z_n\alpha_j^{n-1}$. Let M be the matrix

$$\begin{bmatrix} 1 & \alpha_1 & \cdots & \alpha_1^{n-1} \\ 1 & \alpha_2 & \cdots & \alpha_2^{n-1} \\ \vdots & \vdots & & \\ 1 & \alpha_n & \cdots & \alpha_n^{n-1} \end{bmatrix}$$

Then $M \cdot \bar{z} = \bar{r} = \langle r_1, \ldots, r_n \rangle$. Since the α's are distinct M is invertible in $M_n(K(\alpha_1, \ldots, \alpha_n))$. Thus $M^{-1} \cdot \bar{r} = \bar{z}$. This proves z_i is algebraic over L.

Now if $k_1, \ldots, k_n \in K$ and $k_i \neq 0$ for some $i > 1$ then $k_1 + k_2\alpha_j + \cdots + k_n\alpha_j^{n-1}$ is not in K. Hence under this condition $F(\bar{k}, y)$ has no root in K. Thus, under the assumption $k_i \neq 0$ for some $i > 1$ we have $K \models \Phi(F_0(\bar{k}) \cdots F_{n-1}(\bar{k}))$. Now $\{F_j(\bar{z})\}$ is algebraically independent over K and K is infinite. Thus there is no K-Zariski closed proper subset X of K^n such that $X \supset \{\langle F_0(\bar{k}), \ldots, F_{n-1}(\bar{k}) \rangle | \bar{k} \in K^n,\ k_i \neq 0$ for some $i > 1\}$. Thus if $\Phi(\bar{x}) = D_1(\bar{x}) \vee \cdots \vee D_r(\bar{x})$, where $D_m(\bar{x})$ is a disjunct of type (A) there is some $D_m(\bar{x})$, defining a nonempty set, which is just $q(\bar{x}) \neq 0$. Thus if $\bar{k} \in K^n$ and $q(\bar{k}) \neq 0$ then $f(y, \bar{k})$ has no root in K. But this is absurd since if we let $G(y, \bar{z}) = \prod^n (y - z_i)$ then $G(y, \bar{z}) = \sigma_1(\bar{z}) + \cdots + \sigma_n(\bar{z}) y^{n-1} + y^n$, where $\sigma_i(\bar{z})$ is the ith elementary symmetric polynomial. Since the $\sigma_i(\bar{z})$ are well known to be algebraically independent, $q(\sigma_1(\bar{z}), \ldots, \sigma_n(z)) \neq 0$. So, since K is infinite, there are $k_1, \ldots, k_n \in K$ with $q(\sigma_1(\bar{k}), \ldots, \sigma_n(\bar{k})) \neq 0$. But clearly $G(y, \bar{k})$ has all roots in K. This contradiction proves K is separably closed.

We now show K is perfect. If K has characteristic 0 we are done. Let K have characteristic p. Let $X = \{k \in K | x^p - k = 0$ has no root in $K.\}$ Then by

Lemma 1 $X = \{k \mid \Phi(k)\}$, where $\Phi(x)$ is a disjunction of formulas of type (A), and in this case all polynomials are one-variable polynomials. Clearly this implies X is finite or cofinite. But K is a vector space over its infinite subfield K^p so $K \backslash K^p = X$ cannot be finite or cofinite, unless $X = \varnothing$. So $K = K^p$. ▮

In a sense this proof will be a prototype for all our results in this direction. As pointed out above, Theorem 1 was first proved by Macintyre using techniques associated with $\aleph_1$-categoricity.

Recently, considerable progress has been made on the classification of rings whose theory has QE. The work was begun by Rose for semiprime rings. Later Berline [3] extended Theorem 1 to all rings (with 1) of characteristic 0. Then joint work by Boffa, Macintyre and Point resolved the case of semisimple rings [4]. (There are some additional examples beyond fields). Together with Berline, they reduced the case of algebras over $\mathbb{F}_p$ to that of rings nilpotent of exponent 3. But there Cherlin (unpublished) has found quite a variety of interesting examples with QE.

3. Real Closed Fields

THEOREM (Tarski). *Let L_0 be the language of ordered domains. Let RCF be the theory of real closed fields as naturally formulated in L_0. Then RCF admits elimination of quantifiers relative to L_0.*

We will prove the following converse to Tarski's Theorem:

THEOREM 2. *Let K be an ordered field whose L_0-theory admits QE. Then K is real closed.*

We need the following:

LEMMA 2. *Let $\phi(\bar{x})$ be a quantifier free L_0-formula. Then over the theory of ordered fields $\phi(\bar{x})$ is equivalent to $D_1(\bar{x}) \vee \cdots \vee D_r(\bar{x})$, where each $D_j(\bar{x})$ is of the form $q_1(\bar{x}) > 0 \wedge \cdots \wedge q_m(\bar{x}) > 0$, or of the form, $p(\bar{x}) = 0 \wedge q_1(\bar{x}) > 0 \wedge \cdots \wedge q_m(\bar{x}) > 0$, where $p, q_1, \ldots, q_m \in \mathbb{Z}[\bar{x}]$, $p \neq 0$. We shall say each $D_j(\bar{x})$ is a disjunct of type (B).*

Proof. See [16]. Standard manipulations. ▮

The following general modeltheoretic fact will be very useful to us.

LEMMA 3. *Let T and T' be model complete theories in the same language and suppose A' is a model of T' which is a substructure of a model of T and also has a model of T as substructure.*
Then $A' \models T$.

Proof. Suppose $A_1 \subset A' \subset A_2$, where $A_i \models T$. Consider a sentence $(\forall\bar{x})(\exists\bar{y})\,\Phi(\bar{x},\bar{y})$ in T, with Φ quantifier free. Suppose $A' \models \neg(\forall\bar{x})(\exists\bar{y})\,\Phi(\bar{x},\bar{y})$. Select an existential $\psi(\bar{x})$ so that $T' \vdash (\forall\bar{x})[\neg(\exists\bar{y})\,\Phi(\bar{x},\bar{y}) \leftrightarrow \psi(\bar{x})]$. This is possible since T' is model complete. $A' \models (\exists\bar{x})\neg(\exists\bar{y})\,\Phi(\bar{x},\bar{y})$, so $A' \models (\exists\bar{x})\,\psi(\bar{x})$. Since ψ is existential, $A_2 \models (\exists\bar{x})\,\psi(\bar{x})$. So $A_1 \models (\exists\bar{x})\,\psi(\bar{x})$, since T is model complete. So there is $\bar{a}$ from A_1 such that $A_1 \models \psi(\bar{a})$. So $A' \models \psi(\bar{a})$. So $A' \models \neg(\exists\bar{y})\,\Phi(\bar{a},\bar{y})$. So $A_1 \models \neg(\exists\bar{y})\,\Phi(\bar{a},\bar{y})$. Contradiction, since $A_1 \models T$. So A' satisfies every $\forall\exists$ sentence from T. Since T is model complete, $A' \models T$. ▌

LEMMA 4. *Suppose K is an ordered field whose L_0-theory admits QE, and let A be its subfield of algebraic numbers. If A is real closed, then also K.*

Proof. Apply Lemma 3 to $T = \mathrm{RCF}$ and $T' = \mathrm{Th}(K)$. ▌

We may now proceed directly to the

Proof of Theorem 2. We again argue by contradiction.

Suppose K is not real closed.

Let A be the field of algebraic numbers of K. Then A is not real closed, by Lemma 3. Let $f(y,\bar{x}) = y^n + y^{n-1}x_{n-1} + \cdots + x_0$ and suppose there are $u_1,\dots,u_n \in A$ so that $f(y,\bar{u})$ has odd degree and no root in A. We may assume $f(y,\bar{u})$ irreducible over A. Let $\phi(\bar{x})$ be a quantifier free formula equivalent in K to $\forall y f(y,\bar{x}) \neq 0$. Let $F(\bar{z},y)$ be $\prod_j(y - (z_1 + \cdots + z_n\alpha_j^{n-1}))$, where $\alpha_1,\dots,\alpha_n$ are the distinct roots of $f(y,u)$. As in the proof of Theorem 1, if $F(\bar{z},y) = F_0(\bar{z}) + \cdots + F_{n-1}(\bar{z})\,y^{n-1} + y^n$ then the $F_j(\bar{z})$ are algebraically independent over A. This clearly implies, as in the proof of Theorem 1, that if $\phi(\bar{x}) = D_1(\bar{x}) \vee \cdots \vee D_k(\bar{x})$, where $D_i(\bar{x})$ is of type (B), that there is some $D_i(\bar{x})$ which is of the form $q_1(\bar{x}) > 0 \wedge \cdots \wedge q_k(\bar{x}) > 0$ and which is such that $K \models \exists\bar{x}D_i(\bar{x})$. Fix such an i. Let $X = \{\bar{b} \in A^n \mid A \models D_i(\bar{b})\}$. We see $\bar{K}$ (= real closure of K) satisfies $\exists\bar{x}D_i(\bar{x})$, so $\mathbb{R} \models \exists\bar{x}D_i(\bar{x})$, so $\mathbb{Q} \models \exists\bar{x}D_i(\bar{x})$, since X is given by inequalities with rational coefficients. So now select $a_1,\dots,a_n$ from $\mathbb{Q}$ with $\langle a_1,\dots,a_n\rangle \in X$. Let $f(y,\bar{a})$ have a real root ρ and write $f(y,\bar{a}) = (y-\rho)(b_{n-1}y^{n-1} + \cdots + b_0)$. Choose rational numbers μ and $b'_{n-1},\dots,b'_0$ close to ρ and $b_{n-1},\dots,b_0$, respectively, and let $g(y) = (y-\mu)(b'_{n-1}y^{n-1} + \cdots + b'_0)$. Then $g(y) \in \mathbb{Q}[y]$. Let $g(y) = s_1 + s_2y + \cdots + s_{n-1}y^{n-1} + y^n$. Then s_j is very close to a_j, thus eventually $\langle s_1,\dots,s_n\rangle \in X$. This contradiction proves that every odd degree polynomial of A has a root in A. We now show every positive element of A has a square root. Let Y be the set of all positive elements lacking square roots. By inspection of the form (B) the set Y is either finite or contains an open interval (a_1, a_2). The latter cannot happen since $\{a^2 \mid a \in A\}$ is dense in the positive part of A. But if $y \in Y$, then also $yn^2 \in Y$ for all $n \in \mathbb{N}$. Thus $Y = \varnothing$ and A is real closed. ▮

Theorem 2 has recently been extended to:
Each linearly ordered ring (associative with $1 \neq 0$) whose theory admits QE is a real closed field. See [7].

4. p-ADIC FIELDS AND FIELDS OF LAURENT SERIES

We will work in a language $L_{V,P}$ for valued fields. This contains the usual language for fields, with a 1-ary predicate symbol V for the valuation ring, and 1-ary predicates P_n ($n = 2,...,$) (ultimately to be interpreted by the nonzero nth powers).

A p-adically closed field is a valued field such that

(i) the value group Γ is a $\mathbb{Z}$-group with least positive element 1;

(ii) $v(p) = 1$;

(iii) the residue class field is $\mathbb{F}_p$;

(iv) Hensel's Lemma holds.

We will construe p-adically closed fields as $L_{V,P}$ structures by interpreting V as the valuation ring, and P_n as the group of nonzero nth powers. Obviously, the class of p-adically closed fields is an EC_Δ class in this formulation.

The relevance of the P_n's comes from the result that p-adically closed fields admit QE, but *do not* if the P_n are not used. See [2, 10, 12]. Of course, p-adically closed fields are model complete in the language not using the P_n.

Now we define a p-field to be an $L_{V,P}$ structure K which has a field as its underlying domain and is a substructure of a p-adically closed field L; in particular P_n defines in K the set:

$$\{x \in K : x \text{ is an } n\text{th power in } L\}.$$

Obviously, a p-field is a valued field with discrete group, $v(p) = 1$, and residue class field $\mathbb{F}_p$. The following lemma is crucial.

LEMMA 5. (a) *Suppose K is a p-field, and $n \geqslant 2$. Then there is an integer r_n such that for all x in K: $v(1-x) > r_n \Rightarrow P_n(x)$.*

(b) *If K is a p-field, $\{x : K \vDash P_n(x)\}$ is a clopen subgroup of K^*.*

Proof. (a) Embed K in a p-adically closed K_1. Since P_n in K_1 is interpreted by the nonzero nth powers, the conclusion holds for K_1 by Hensel–Rychlik [12]. Since P_n is interpreted in K by $\{x \in K_1 : P_n(x)\} \cap K$, the result follows.

(b) Immediate from (a), since $\{x \in K : P_n(x)\}$ is a group under multiplication. ▮

Now we can easily obtain a converse to Macintyre's quantifier elimination for $\mathbb{Q}_p$.

THEOREM 4. *Suppose K is a p-field which admits QE in $L_{V,P}$. Then K is p-adically closed.*

The proof follows closely that for real closed fields, so we feel justified in giving fewer details.

Step 1. First we describe a normal form for quantifier-free formulas, along the lines of Lemma 2. Because $V(x) \leftrightarrow P_2(1+p^3x^2)$ holds in all p-fields, we have only to consider disjunctions of formulas which are conjunctions of the form (C):

$$\begin{aligned} & p_1(\bar{x})=0 \wedge \cdots \wedge p_k(\bar{x})=0 \\ \wedge \quad & q(\bar{x}) \neq 0 \\ \wedge \quad & P_{n_1}(s_1(\bar{x})) \wedge \cdots \wedge P_{n_u}(s_u(\bar{x})) \\ \wedge \quad & \neg P_{n_{u+1}}(t_1(\bar{x})) \wedge t_1(\bar{x}) \neq 0 \wedge \cdots \wedge \neg P_{n_{u+v}}(t_v(\bar{x})) \wedge t_v(\bar{x}) \neq 0. \end{aligned}$$

Note that all conjuncts except the equations define *open* sets in the (products of the) valuation topology.

Step 2. Let A be the field of algebraic numbers of K. A is a p-field. Most importantly, A is *dense* in its Henselization $\bar{A}$, which is a p-adically closed field. By Lemma 3, K is p-adically closed if and only if A is p-adically closed.

Suppose A is not p-adically closed. Then A is not Henselian. We select $\alpha \in \bar{A}$ of minimal degree $n > 1$ over A, with minimal polynomial $f(y)$. By standard transformations we can assume that f is a counterexample to the following version of Hensel's Lemma [6]:

If $f \in V[y]$, and $\beta \in V$ with $v(f(\beta)/(f'(\beta))^2) > 0$, then f has a root in V.

We now proceed as in the proof of Theorem 1 to form $F(\bar{z}, y)$ whose coefficients are algebraically independent over K. Let $\bar{z}_0 = (0, 1, 0, 0, \ldots)$. Then $F(\bar{z}_0, y) = f(y)$. There is a neighborhood U of $\bar{z}_0$ in the product topology on A^n, so that if $\bar{z}_1 \in U$ then

$$v\left(F(\bar{z}_1, \beta) \Big/ \left(\frac{\partial F}{\partial y}(\bar{z}_1, \beta)\right)^2\right) > 0$$

(by continuity).

The neighborhood U is not contained in any proper Zariski closed subset of A^n.

Now consider the condition:

$x_0, \dots, x_{n-1} \in V$, and there is a $\beta \in V$ so that

$$v(g(\beta)/(g'(\beta))^2) > 0$$

and g has no zero in V, where $g(y) = f(y, \bar{x})$

$$= y^n + x_{n-1} y^{n-1} + \cdots + x_0$$

(i.e., $f(y, \bar{x})$ is a counterexample to Hensel's Lemma of degree n).

Let $\Phi(\bar{x})$ be a quantifier-free formula equivalent over K to the above. Φ can be taken as disjunction of formulas of type (C). By the argument about U, one of the disjuncts lacks equational conditions, and so defines a nonvoid open set in A^n.

Step 3. One can now proceed exactly as in the real case, factoring f over $\bar{A}$ and approximating. This concludes the proof. ▮

Notes (i) The above result may not be best possible. Our definition of p-field forces the interpretation of each P_n to be a clopen subgroup. It should be obvious that this fact was crucial to our proof. It is an interesting, and apparently difficult problem to extend our result to the class of valued fields where P_n is simply interpreted as the group of invertible nth powers. The field $\mathbb{Q}$ under the p-adic valuation is not a p-field, under the latter interpretation.

(ii) It is routine to establish an analogous result for the class of valued fields of characteristic zero with algebraically closed residue class field, value group a $\mathbb{Z}$-group, and a distinguished element t with $v(t) = 1$. Now we would consider quantifier elimination in terms of V, P_n, and t. We regard this result as essentially weaker than the p-adic case, since we know many examples where the use of a constant like t changes a non-model-complete field into a model-complete field. For example, this happens with $\mathbb{C}((t))$.

4. General Valued Fields

4.1. Example. Let $D = \mathbb{Q}[x, y]$, and let $V = D$. Let F be the quotient field of D. Consider the two natural embeddings

$$\begin{tikzcd} & D \arrow[dl, "\sigma_1"'] \arrow[dr, "\sigma_2"] & \\ \mathbb{Q}((x))((y)) & & \mathbb{Q}((y))((x)) \end{tikzcd}$$

These induce valuations v_1, v_2 on F, with valuation-rings V_1, V_2, so that $V \subset V_1$, $V \subset V_2$. But

$$v_1(y) > v_1(x),$$
$$v_2(x) > v_2(y).$$

So the relation

$$v_i(x) > v_i(y)$$

is not quantifier-free definable in terms of V_i.

4.2. The following seems to be the best way of formalizing

$$v(x) \geqslant v(y).$$

DEFINITION.. Let D be a domain. Then a linear divisibility relation (l.d. relation) on D is a binary relation div on D such that for all a, b, $c \in D$:

(i) (a div b and b div c) $\Rightarrow$ a div c,

(ii) a div b or b div a,

(iii) (a div b and a div c) $\Rightarrow$ a div $(b+c)$,

(iv) if $c \neq 0$, then (a div $b \Leftrightarrow ac$ div bc),

(v) not 0 div 1.

An l.d. relation div on the domain D induces a valuation ring V_{div} of the quotient field $Q(D)$ of D: $V_{\text{div}} = \{a/b \mid a, b \in D,\ b \neq 0,\ b \text{ div } a\}$, and for the corresponding valuation v_{div} on $Q(D)$ we have (with a, $b \in D$):

$$v_{\text{div}}(a) \leqslant v_{\text{div}}(b) \Leftrightarrow a \text{ div } b.$$

div $\mapsto V_{\text{div}}$ is easily seen to be a bijection of the set of l.d. relations on D onto the set of valuation rings of $Q(D)$, whose inverse is given by:

$$V \mapsto \text{div}_V \overset{\text{def.}}{=} \{(a, b) \in D^2 \mid v(a) \leqslant v(b)\},$$

where v is the valuation on $Q(D)$ associated with V. Clearly an l.d. relation div on D can be extended uniquely to an l.d. relation Q(div) on $Q(D)$ such that

$$(D, \text{div}) \subset (Q(D), Q(\text{div})).$$

So let us redefine a valued field as a field with an l.d. relation on it, and define a valued domain as a substructure of a valued field, i.e., as a domain with an l.d. relation.

Clearly the notion of extension for valued fields does not change by this convention.

Let L_{val} be the language of valued domains with a predicate div. Let $\mathrm{ACF}_{\text{val}}$ be the theory of non-trivially valued algebraically closed fields, formulated in this language.

THEOREM (Robinson [13]). $\mathrm{ACF}_{\text{val}}$ *admits QE. It is the model completion of the theory of valued domains.*

Actually Robinson shows only that $\mathrm{ACF}_{\text{val}}$ is model complete, because this is what he needs to derive the decidability of $\mathrm{ACF}_{\text{val}}$. But one easily sees that a valued field (K, div_K) has an up to isomorphism unique prime extension $(\tilde{K}, \mathrm{div}_{\tilde{K}})$ to a model of $\mathrm{ACF}_{\text{val}}$. If div_K is nontrivial, then this prime extension is $(\tilde{K}, \mathrm{div}_{\tilde{K}})$, where $\tilde{K}$ is the algebraic closure of K and $\mathrm{div}_{\tilde{K}}$ is any extension of div_K to $\tilde{K}$. If div_K is trivial, first extend div_K to a nontrivial $\mathrm{div}_{K(x)}$ on a pure transcendental extension of K, and then use the first case. Model completeness of $\mathrm{ACF}_{\text{val}}$ together with the existence of prime extensions for substructures implies that $\mathrm{ACF}_{\text{val}}$ admits QE, by [15].

We prove a converse to this theorem:

THEOREM 5. *Let $K = (K, \mathrm{div}_K)$ be a non-trivially valued field such that* $\mathrm{Th}(K)$ *admits QE. Then K is algebraically closed.*

4.3. We assume (K, div_K) is a nontrivially valued field such that $\mathrm{Th}(K)$ admits QE.

We first pass to a subfield A of K which will play the role of the field of algebraic numbers of K. If div_K is nontrivial on the prime field $\mathbb{F}$ of K, let A be the field of algebraic numbers of K, and div_A the l.d. relation on A induced by div_K. If div_K is trivial on $\mathbb{F}$, select t with $v(t) \neq 0$, and let A be the relative algebraic closure of $\mathbb{F}(t)$ in K, and div_A the l.d. relation on A induced by div_K.

The esential facts about A are:

LEMMA 6. (a) *The valuation on A is a rank* 1 *valuation, and so A is dense in its Henselization.*

(b) *If A is algebraically closed, then so is K.*

Proof (a) Standard.

(b) Lemma 3 and Robinson's Theorem. ∎

4.4. Let us establish notation. Given (K, div_K), we put:

(a) $\Gamma_K =$ value group;

(b) $\mathrm{Res}(K)$ = residue class field;

(c) $(\bar{K}, \mathrm{div}_{\bar{K}})$ = henselization of (K, div_K);

We are going to exploit the following lemma.

LEMMA 7. *Let $K = (K, div)$ be a perfect, henselian field such that*

(a) Res (K) *is algebraically closed*;

(b) Γ_K *is divisible*;

(c) *if* char $(K) = 0$ *and* char $(\mathrm{Res}(K)) = p > 0$, *then K^* is p-divisible*;

(d) *if* char $(K) = p > 0$, *then K is closed under Artin–Schreier extensions.*

Then K is algebraically closed.

Proof. If char (Res (K)) = 0, then a proper algebraic extension of K has a unique valuation extending the valuation on K, and this valuation either enlarges the value group, or the residue field of K, which contradicts the assumptions. So suppose char $(\mathrm{Res}(K)) = p > 0$ and that K is not algebraically closed. Then, because K is perfect, it has a proper finite Galois extension L. Let $G = \mathrm{Gal}\,(L|K)$ and H be a p-Sylow subgroup of G. If $H \neq G$, then the fixed field of H is a separable extension M of K with $[M:K] > 1$, and $p \nmid [M:K]$. Extend the valuation v (uniquely) to a valuation v_M on M. Then the formula $[M:K] = [\mathrm{Res}(M):\mathrm{Res}(K)] \cdot [\Gamma_M:\Gamma_K] = 1.1 = 1$ holds [14, p. 237], contradiction. So $G = H$ and G is a p-group. As a nontrivial p-group G has a cyclic quotient of order p which implies that K has a cyclic extension of degree p; but this is impossible by the conditions (c) and (d), except that in the case of char $K = 0$, char $\mathrm{Res}(K) = p > 0$ we still have to check that K has a primitive pth root of unity. So let char $K = 0$, char $\mathrm{Res}(K) = p > 0$ and let ζ be a primitive pth root of unity. Then $K(\zeta)/K$ is separable of degree $\leqslant p - 1$, and hence $[K(\zeta):K] = [\mathrm{Res}(K(\zeta)):\mathrm{Res}(K)][\Gamma_{K(\zeta)}:\Gamma_K] = 1.1 = 1$ which shows that $\zeta \in K$. ▮

We now prove the theorem. To begin we note that any quantifier-free formula in the current language is a boolean combination of atoms $p(\bar{x}) = 0$, $r(\bar{x})$ div $s(\bar{x})$.

If $X \subset K$, K any valued field, is defined by such an atom, then $K \backslash B \subset X$ or $K \backslash B \subset K \backslash X$ for some bounded neighborhood B of 0. This property of sets $X \subset K$ is clearly preserved under taking boolean combinations.

From this we deduce the following.

LEMMA 8. *Let A be as in* 4.3. *Then the multiplicative group of A is divisible. Hence A is perfect and Γ_A is divisible. A is closed under Artin-Schreier extensions if* $\mathrm{ch}(A) \neq 0$. $\mathrm{Res}(A)$ *is not finite.*

It remains to show: $\operatorname{Res}(A)$ is algebraically closed.

Proof. We first claim that if n is an integer > 1 then there is a polynomial $Q(x_0,\dots,x_{n-1}) = Q(\bar{x}) \in \mathbb{F}[\bar{x}]$ with all coefficients of non-negative value and such that the image of $Q(\bar{x})$ in $\operatorname{Res}(A)[\bar{x}]$, $\bar{Q}(\bar{x})$, is not zero and furthermore if $\bar{Q}(\bar{a}) \neq 0$, a from A, then $y^n + a_{n-1}y^{n-1} + \cdots a_0$ has a root in A. We now construct Q. Let $f(y,\bar{x}) = y^n + x_{n-1}y^{n-1} + \cdots + x_0$ and $\psi(\bar{x}) = \psi(x_0,\dots,x_{n-1})$ be an open L_{val}-formula under $\operatorname{Th}(K)$ equivalent to $\exists y f(y,\bar{x}) = 0$. We may assume that $\psi(\bar{x})$ is a finite disjunction of formulas of the following type:

$$p_1(\bar{x}) = \cdots = p_k(\bar{x}) = 0 \wedge q_1(\bar{x}) \operatorname{div} r_1(\bar{x}) \wedge \cdots \wedge q_l(\bar{x}) \operatorname{div} r_l(\bar{x})$$
$$\wedge \neg(s_1(\bar{x}) \operatorname{div} t_1(\bar{x})) \wedge \cdots \wedge \neg(s_m(\bar{x}) \operatorname{div} t_m(\bar{x})), \qquad (*)$$

where all appearing polynomials have their coefficients in $V_{\mathbb{F}}$ such that for all i with $1 \leqslant i \leqslant k$: $p_i(\bar{x})$ has image $\overline{p_i}(\bar{x}) \in \operatorname{Res}(A)[\bar{x}]\backslash\{0\}$ and for each atom $q_j(\bar{x})$ div $r_j(\bar{x})$ at least one of $q_j(\bar{x})$, $r_j(\bar{x})$ has image $\neq 0$ in $\operatorname{Res}(A)[\bar{x}]$, and, finally, for each negated atom $\neg(s_h(\bar{x}) \operatorname{div} t_h(\bar{x}))$ at least one of $s_h(\bar{x})$, $t_h(\bar{x})$ has image $\neq 0$ in $\operatorname{Res}(A)[\bar{x}]$. All this can be reached by multiplication with suitable elements of $\mathbb{F}$.

Claim. There is at least one disjunct $(*)$ in which no $p_i(\bar{x})$ appears and no conjunct $q_j(\bar{x})$ div $r_j(\bar{x})$ with $\bar{q}_j(\bar{x}) = 0$ in $\operatorname{Res}(A)$ $[\bar{x}]$ and no conjunct $(s_h(\bar{x})$ div $t_h(\bar{x}))$ with $\overline{s_h}(\bar{x}) \neq 0$ in $\operatorname{Res}(A)[\bar{x}]$. Let us first assume that the claim is true; so we have a disjunct $(*)$ in which $k = 0$ and for all $1 \leqslant j \leqslant l$, $1 \leqslant h \leqslant m$: $\overline{q_j}(\bar{x}) \neq 0$, $\overline{s_h}(\bar{x}) = 0$ (hence $\overline{t_h}(\bar{x}) \neq 0$). Then let $Q(\bar{x})$ be the product of all q_j and t_h; so $Q(\bar{x}) \in V_{\mathbb{F}}[\bar{x}]$ and $\bar{Q}(\bar{x}) \in \mathbb{F}[\bar{x}]\backslash\{0\}$ and for all $a = (a_0,\dots,a_{n-1}) \in V^n$ with $\bar{Q}(\bar{a}_0,\dots,\bar{a}_{n-1}) \neq 0$: $y^n + a_{n-1}y^{n-1} + \cdots + a_0$ has a root in A. This is because $\bar{Q}(\bar{a}) \neq 0$ implies easily that the disjunct $(*)$ becomes true in A upon substituting a for $\bar{x}$. Suppose the claim does not hold. Then we form a product $P(\bar{x}) \in V_{\mathbb{F}}[\bar{x}]$ by taking from each disjunct $(*)$ factors as follows: all $p_i(\bar{x})$ are factors; for each atom $q_j(\bar{x})$ div $r_j(\bar{x})$ with $\overline{q_j}(\bar{x}) = 0$ $r_j(\bar{x})$ should be a factor; for each negated atom $\neg(s_h(\bar{x})$ div $t_h(\bar{x}))$ with $\overline{s_h}(\bar{x}) \neq 0$ $s_h(\bar{x})$ should be a factor. So because the claim is supposed to be not true $P(\bar{x})$ has a factor from each disjunct; also $\bar{P}(\bar{x}) \neq 0$ in $\operatorname{Res}(A)[\bar{x}]$. We now show:

$$\text{for all } a = (a_0,\dots,a_{n-1}) \in V_A^n \text{ such that } y^n + a_{n-1}y^{n-1} + \cdots + a_0$$
$$\text{has a root in } A,\ \bar{P}(\bar{a}_0,\dots,\bar{a}_{n-1}) = 0 \text{ holds.} \qquad (**)$$

For at least one of the disjuncts $(*)$ must hold in K upon substituting a for $\bar{x}$; now if this particular disjunct has given us a factor $p_i(\bar{x})$ of $P(\bar{x})$, then $p_i(a) = 0$, so certainly $\bar{P}(\bar{a}) = 0$; if the disjunct gives a factor $r_j(\bar{x})$, then this is because $\bar{q}_j(\bar{x}) = 0$, so $v(q_j(a)) > 0$; but also $q_j(a) \operatorname{div} r_j(a)$ holds, so

$v(r_j(a)) > 0$, i.e., $\bar{r}_j(\bar{a}) = 0$, hence $\bar{P}(\bar{a}) = 0$; similarly one shows that if the disjunct gives a factor $s_h(\bar{x})$, then also $\bar{P}(\bar{a}) = 0$. So the statement (**) above is proved. This statement implies that $\bar{P}(\sigma_0(\bar{b}),\ldots, \sigma_{n-1}(\bar{b})) = 0$ for all $b \in V^n$, so as Res(A) is infinite by Lemma 7, $\bar{P}(\sigma_0(\bar{z}),\ldots, \sigma_{n-1}(\bar{z}) = 0$ in Res$(A)[\bar{z}]$ which however contradicts the algebraic independence of the elementary symmetric functions $\sigma_0(\bar{z}),\ldots, \sigma_{n-1}(\bar{z})$ over Res(A).

Employing arguments similar to those used in previous cases we now can show easily that Res(A) is algebraically closed.

Since A is dense in its Henselization (Lemma 6), arguments similar to those used in the p-adic case show that A is in fact Henselian. Thus the theorem is proved.

5. Postscript

Consider the field $L = \bigcup_{n \geqslant 1} K((t^{1/n}))$ of formal Puiseux series (fractional power series) over an algebraically closed field K of characteristic $p \neq 0$. L is *not* algebraically closed ([5, p. 64]. (The algebraic closure of L is obtained by iterated Artin-Schreier extensions.) It follows from Section 4 that Th(L) does not admit elimination of quantifiers as a valued field. This is not altogether too pathological in as much as $\mathbb{C}((t))$ does not admit elimination of quantifiers as a valued field either. However, in the language of Section 3 (with t distinguished) $\mathbb{C}((t))$ does admit elimination of quantifiers.

However, L is much more perverse than $\mathbb{C}((t))$. Anyone familiar with the Kaplansky Hypothesis-A [9] may well wonder why, since L clearly satisfies Hypothesis–A, the Ax–Kochen analysis does not apply to K. The answer to this is that L admits algebraic immediate extensions (namely $\tilde{L}$). Another point of view on this might be that L does not satisfy the very strong form of Hensel's lemma Kaplansky uses, a version which takes into consideration all p^jth formal derivatives of a polynomial instead of just the first derivative. We might say that L is not *sufficiently* Henselian.

A famous theorem of Ax and Kochen states that if K_1 and K_2 are Henselian valued fields with ch(Res(K_i)) = 0, $\Gamma_{K_i} \equiv \Gamma_{K_2}$, and Res($K_1$) $\equiv$ Res(K_2), then $K_1 \equiv K_2$. If L is as in the preceding paragraph we see L furnishes a counterexample to this theorem for characteristic $p \neq 0$. If M is an algebraically closed field, $ch(M) = p \neq 0$ and $M((t^{\mathbb{Q}}))$ is the field of formal power series with well-founded support in the rational group $\mathbb{Q}$ (i.e., $\{f: \mathbb{Q} \to M \mid \{q \in \mathbb{Q} \mid f(q) \neq 0\}$ is well founded$\}$) then $M((t^{\mathbb{Q}}))$ is algebraically closed (so Henselian), Res$(M((t^{\mathbb{Q}}))) = M \equiv$ Res(L) and $\Gamma_{M((t^{\mathbb{Q}})} = \mathbb{Q} = \Gamma_L$ but $M((t^{\mathbb{Q}})) \not\equiv L$.

It might be possible to gain control over the Artin–Schreier extensions of L (and so prove decidability) by introducing new predicates for this purpose. However, we do not see how this might be accomplished at this time.

REFERENCES

1. J. AX, The elementary theory of finite fields, *Ann. of Math.* **88** (1968), 239–271.
2. J. AX AND S. KOCHEN, Diophantine problems over local fields I and II, *Amer. J. Math.* (1965), 605–648.
3. C. BERLINE, Rings which admit elimination of quantifiers, *J. Symbol. Logic* **46**, 56–58.
4. M. BOFFA, A. MACINTYRE, AND F. POINT, *in* "Proceedings of Karpacz 1979" (L. Pacholski and A. Wilkie, Eds), Springer-Verlag, Berlin/New York/Heidelberg, 1980.
5. C. CHEVALLEY,"Introduction to the Theory of Algebraic Functions of One Variable," American Mathematical Society Surveys No. VI, Amer. Math. Soc., Providence, R. I., 1951.
6. P. COHEN, Decision procedures for real and p-adic fields, *Comm. Pure Appl. Math.* **22** (1969), 131–153.
7. L. VAN DEN DRIES, A linearly ordered ring whose theory admits quantifier elimination is a real closed field, *Proc. Amer. Math. Soc.* **79** (1980), 97–100.
8. M. JARDEN, Elementary statements over large algebraic fields, *Trans. Amer. Math. Soc.* **164** (1972), 67–91.
9. I. KAPLANSKY, Maximal fields with valuation, *Duke Math. J.* **9** (1942), 313–321.
10. S. KOCHEN, Integer valued rational functions over the p-adic numbers: A p-adic Analogue of the theory of real fields, *Proc. Symp. Pure Math.* **12** (1969), 57–73.
11. A. MACINTYRE, On ω_1-categorical fields, *Fund. Math.* **7** (1971), 1–25.
12. A. MACINTYRE, On definable sets of p-adic numbers, *J. Symbol. Logic* **41** (1976), 605–610.
13. A. ROBINSON,"Complete Theories," North-Holland, Amsterdam, 1956.
14. P. RIBENBOIM, "Theorie des valuations," Les Presses de L'Université de Montréal, Montreal, 1967.
15. G. SACKS,"Saturated Model Theory," Benjamin, New York, 1972.
16. A. TARSKI AND J. MCKINSEY, "A Decision Method for Elementary Algebra and Geometry," Univ. of California Press, Berkeley, 1951.