# The Elementary Theory of Algebraic Fields of Finite Corank

Moshe Jarden (Tel Aviv) and Ursel Kiehne* (Saarbrücken)

## Contents



## Introduction

J. Ax proved in [2] that the theory of elementary statements true in all but a finite number of fields $\mathbb{F}_p$ of $p$ elements is decidable. In [6] it was proved that this theory coincides with the theory of elementary statements true in $\tilde{\mathbb{Q}}(\sigma)$ for almost all $\sigma \in \mathcal{G}(\tilde{\mathbb{Q}}/\mathbb{Q})$. Here "almost all" is used in the sense of the Haar measure $\mu$ of $\mathcal{G}(\tilde{\mathbb{Q}}/\mathbb{Q})$ defined with respect to its Krull topology and $\tilde{\mathbb{Q}}(\sigma)$ is the fixed field of $\sigma$ in $\tilde{\mathbb{Q}}$. Natural generalizations of the $\tilde{\mathbb{Q}}(\sigma)$ are the fixed fields $\tilde{\mathbb{Q}}(\underline{\sigma}) = \tilde{\mathbb{Q}}(\sigma_1, \ldots, \sigma_e)$ of $e$-tuples $(\sigma_1, \ldots, \sigma_e) \in \mathcal{G}(\tilde{\mathbb{Q}}/\mathbb{Q})^e$. Here $e$ is a positive integer which will remain fixed throughout this paper. It was proved in [6] and [7] that for almost all $(\underline{\sigma}) \in \mathcal{G}(\tilde{\mathbb{Q}}/\mathbb{Q})^e$ we have:

(*) Every non-void absolutely irreducible variety defined over $\tilde{\mathbb{Q}}(\underline{\sigma})$ has a $\tilde{\mathbb{Q}}(\underline{\sigma})$-rational point;

(**) The closed subgroup $\langle \underline{\sigma} \rangle$ generated by $\sigma_1, \ldots, \sigma_e$ is (topologically) isomorphic to the free pro-finite group, $\hat{F}_e$, generated by $e$ elements.

These two properties of the $\tilde{\mathbb{Q}}(\underline{\sigma})$ make it possible to prove that the theory of elementary statements true in $\tilde{\mathbb{Q}}(\underline{\sigma})$, for almost all $(\underline{\sigma}) \in \mathcal{G}(\tilde{\mathbb{Q}}/\mathbb{Q})^e$, is decidable. We note that our notations can be interpreted also for $e = 0$. In this case $\mathcal{G}(\tilde{\mathbb{Q}}/\mathbb{Q})^e = 1$, $\tilde{\mathbb{Q}}(\underline{\sigma}) = \tilde{\mathbb{Q}}$ and it is well known that the theory of $\tilde{\mathbb{Q}}$ is decidable (cf. Kreisel and Krivine [8, p. 59]). Thus our result can be considered as a generalization of this classical result as well as of Ax'.

* This work is partially a revised form of the doctoral dissertation of the second author done in Heidelberg University under the supervision of the first author.

In the proof we follow Ax' method and begin with a proof of an algebraic theorem.

If $E$ and $F$ are two fields of characteristic 0 which satisfy (*) and (**) and if $\tilde{\mathbb{Q}} \cap E \cong \mathbb{Q} \cap F$, then $E$ is elementary equivalent to $F$.

The proof of this theorem is, however, quite different from the corresponding theorem of Ax [6, Thm. 1]. Ax relies heavily on the fact that in the case $e=1$ the Galois groups involved are abelian, which is by no means the case for $e \geqq 2$. Our proof is a general one and its crucial point is the application of a theorem of Gaschütz which asserts that if $\theta\colon G \to H$ is an epimorphism of finite groups such that $G$ is generated by $e$ elements, then every system $y_1, \ldots, y_e$ of generators of $H$ can be lifted to a system of generators of $G$.

Ax uses non-principal ultraproducts of the $\mathbb{F}_p$ to bridge the gap between algebraic properties and logical properties of fields. We replace the non-principal ultraproducts by *regular* ultraproducts of the $\tilde{\mathbb{Q}}(\sigma)$. They are so constructed as to have the property that an elementary statement $\Theta$ is true in $\tilde{\mathbb{Q}}(\sigma)$ for almost all $(\sigma) \in \mathscr{G}(\tilde{\mathbb{Q}}/\mathbb{Q})^e$ if and only if it is true in all the regular ultraproducts of the $\tilde{\mathbb{Q}}(\sigma)$. Using the regular ultraproducts we prove that the theory of elementary statements true in $\tilde{\mathbb{Q}}(\sigma)$, for almost all $(\sigma) \in \mathscr{G}(\tilde{\mathbb{Q}}/\mathbb{Q})^e$, is the same as the theory of elementary statements true in all fields of characteristic 0 which satisfy (*) and (**). These properties in turn are shown to be equivalent to a conjunction $\Pi$ of $\aleph_0$ elementary statements. Again, using regular ultraproducts we show that every elementary statement is equivalent modulo $\Pi$ to a one-variable statement, *i.e.*, to a boolean expression in statements of the form $\exists X\, f(X)=0$, where $f \in \mathbb{Z}[X]$. For one-variable statements we establish a decision procedure which applies the fact that one can calculate the Galois group of a polynomial $f(X)$ over $\mathbb{Q}$. The general decision procedure is reduced to the former one by using Gödel's completeness theorem.

Finally, we note that all our results, apart from the decision procedure, are actually proved for an arbitrary denumerable hilbertian field $K$ rather than for $\mathbb{Q}$. The decision procedure is simultaneously established for $\mathbb{Q}$ and all the fields $\mathbb{F}_p(t)$.

The authors wish to acknowledge their indebtedness to P. Roquette for his interest, and especially for his crucial contribution in simplifying a former proof of the second author of the important Lemma 2.1. They thank also J. Janko for calling their attention to Gaschütz' theorem.

## 1. Ax Fields and Hyper Ax Fields

We start with some definitions which are similar to those which appear in Ax [2, §§ 2, 3, 4].

Let $F$ be a field and $A$ a (commutative) $F$-algebra. We say that $A$ is *absolutely entire* over $F$ if $\tilde{F} \otimes_F A$ is an integral domain. If $D$ is a field extension of $F$ then to say that $D$ is absolutely entire over $F$ is equivalent to saying that $D$ is a regular extension of $F$. Clearly, every subalgebra of an absolutely entire $F$-algebra is also absolutely entire. In particular, if $A$ is an $F$-algebra contained in a regular extension $D$ of $F$, then $A$ is absolutely entire. Note that this also applies to the case where $A$ is the coordinate ring of an affine absolutely irreducible variety $V$ which is defined over $F$, since in this case the quotient field of $A$ is regular over $F$ (cf. Lang [9, p. 71]).

We call a perfect field $F$ an *Ax* field, if every non-void absolutely irreducible variety $V$ which is defined over $F$ has an $F$-rational point. This is equivalent to

saying that for every *finitely* generated absolutely entire $F$-algebra $A$ there exists an $F$-algebra homomorphism of $A$ into $F$.

Following the second version in the definition of an Ax field one says that a perfect field $F$ is *hyper Ax* if for every *denumerably* generated absolutely entire $F$-algebra $A$ there exists an $F$-algebra homomorphism of $A$ into $F$.

Clearly every hyper Ax field is also an Ax field. The converse does not hold in general, but it does hold if the field in question is saturated. In order to explain what we mean we consider a field $K$ and denote by $\mathfrak{L}(K)$ the usual first order predicate calculus language of field theory $\mathfrak{L}$ enriched with new constants, one for every element of $K$. The variables of $\mathfrak{L}(K)$ are denoted by $X_1, X_2, X_3, \ldots$. As models of $\mathfrak{L}(K)$ we take only fields $F$ which contain $K$ and then we interpret the new constants as the corresponding elements of $K$. We call these fields $K$-fields. A mathematical statement $\Theta$ on $K$-fields is said to be *$K$-elementary*, if it is equivalent to a sentence in $\mathfrak{L}(K)$. We use the notation $F|=\Theta$ to denote that $\Theta$ holds over $F$. Two $K$-fields $F_1, F_2$ are said to be $K$-equivalent, if $F_1|=\Theta \Leftrightarrow F_2|=\Theta$ for every $K$-elementary statement $\Theta$; we denote this by $F_1 \equiv_K F_2$.

A field $F$ is said to be $\aleph_1$-saturated, if it has the following property. Let $\Phi_1, \Phi_2, \Phi_3, \ldots$ be a sequence of formulas of $\mathfrak{L}(K)$. If for every positive integer $n$ there exist elements $a_1, a_2, a_3, \ldots$ of $F$ such that

$$F|=\Phi_i(\underline{a}) \quad \text{for } i=1,\ldots,n,$$

then there exist elements $b_1, b_2, b_3, \ldots$ of $F$ such that

$$F|=\Phi_i(\underline{b}) \quad \text{for } i=1,2,3,\ldots.$$

Note that our definition of the saturation property is apparently stronger than the usual one which allows the formulas $\Phi_i$ to have only one free variable (cf. Bell and Slomson [3, p. 218]), but actually both can be proved to be equivalent (cf. Ax [2, p. 254]).

The same arguments used by Ax in proving Proposition 3 of [6] can be applied to the following lemma.

**Lemma 1.1.** *If $F$ is an $\aleph_1$-saturated Ax field, then $F$ is also a hyper Ax field.*

Also using Ax' arguments for proving his Lemma 8 of [11], one can prove the following slightly strengthened lemma.

**Lemma 1.2.** *Let $\mathfrak{D}$ be a non-principal ultra filter of a countable set $I$. Suppose that for every $i \in I$ we are given a field $F_i$. Then $F=\prod F_i/\mathfrak{D}$ is an $\aleph_1$-saturated field.*

Our aim now is to axiomatize the notion of an Ax field. Clearly, to say that a field is perfect is an elementary statement. As to the second condition we need the following lemma.

**Lemma 1.3.** *The following two statements on a perfect field $F$ are equivalent.*

1) *$F$ is an Ax field.*

2) *For every absolutely irreducible polynomial $f \in F[X_1, \ldots, X_n]$ of positive degree $\leqq n$, and for every $g \in F[X_1, \ldots, X_n]$ of degree $\leqq n$ which is not a multiple of $f$ there exist $a_1, \ldots, a_n \in F$ such that $f(a_1, \ldots, a_n)=0$ and $g(a_1, \ldots, a_n) \neq 0$.*

*Proof.* (1) $\Rightarrow$ (2). If $(\underline{x})$ is a generic point of the variety $f(\underline{X})=0$ then $g(\underline{x})\neq 0$. Writing $y=g(\underline{x})^{-1}$ we have that $F(\underline{x}, y)=F(\underline{x})$ is a regular extension of $F$; hence $(\underline{x}, y)$ has an $F$-specialization $(\underline{a}, b)$ with coordinates in $F$. It follows that $f(\underline{a})=0$ and $b\,g(\underline{a})=1$, whence $g(\underline{a})\neq 0$.

(2) $\Rightarrow$ (1). Let $V$ be a non-void absolutely irreducible variety of dimension $r$ defined over $F$. Then, as is well known, $V$ is birationally equivalent over $F$ to a hyper-surface $W$ in $S^{r+1}$, *i.e.* to a variety of the form $f(X_1, \ldots, X_{r+1})=0$, where $f\in F[X_1, \ldots, X_{r+1}]$ is an absolutely irreducible polynomial of positive degree. There exists a polynomial $g\in F[X_1, \ldots, X_{r+1}]$ which is not a multiple of $f$ such that the birational transformation $W\rightarrow V$ is biregular at every point $(\underline{a})$ of $W$ for which $g(\underline{a})\neq 0$. Every such point with coordinates in $F$ will supply an $F$-rational point of $V$. ‖

Our aim will be achieved if we show that for every polynomial $f(X_1, \ldots, X_n)$ of degree $\leqq n$ with general coefficients the statement "$f$ is absolutely irreducible" is elementary, *i.e.* is equivalent to a formula in $L$ with the coefficients of $f$ as the free variables.

Consider the Kronecker substitution $S_d$ which transforms $f(X_1, \ldots, X_n)$ into the polynomial $S_d f(Y)=f(Y, Y^d, \ldots, Y^{d^{n-1}})$ with one variable $Y$, where $d=n+1$ (cf. Lang [10, p. 150]). The degree of $S_d f$ is $\leqq d^n-1$; hence, if $S_d f$ factors over an extension $F'$ of $F$, then $[F': F]\leqq(d^n-1)!$.

If $f(\underline{X})=g_1(\underline{X})g_2(\underline{X})$, then $S_d f(Y)=S_d g_1(Y)\,S_d g_2(Y)$, and $S_d g_1, S_d g_2$ have the same coefficients as $g_1, g_2$ respectively. It follows that if $f(\underline{X})$ factors over an extension $F'$ of $F$, then $[F': F]\leqq(d^n-1)!$. If $F$ is perfect then $F'\cong_F F[Y]/h(Y)F[Y]$, where $h$ is an irreducible polynomial of degree $\leqq(d^n-1)!$. Thus, to say that $f(\underline{X})$ is absolutely irreducible over a perfect field $F$ is equivalent to the following elementary statement.

For every irreducible polynomial $h\in F[Y]$ of degree $\leqq(d^n-1)!$, there do not exist polynomials $g_1, g_2, g_3\in F[Y, X]$ such that (a) $\deg_Y g_i\leqq(d^n-1)!$ and $\deg_{\underline{X}} g_i<n$ for $i=1, 2$; (b) $\deg_Y g_3<2((d^n-1)!)$ and $\deg_{\underline{X}} g_3<n$; and (c)

$$f(\underline{X})=g_1(Y, \underline{X})\,g_2(Y, \underline{X})+g_3(Y, \underline{X})\,h(Y).$$

We sum up these results in the following lemma.

**Lemma 1.4.** *For every $p$ there is a sequence $\Theta_0, \Theta_1, \Theta_2, \ldots$ of sentences in the language $\mathfrak{L}$ of the theory of fields, which we can explicitely write down, such that a field $F$ of characteristic $p$ is an Ax field if and only if $F$ satisfies $\theta_i$ for every $i\geqq 0$.*

*Lemmas* 1.1, 1.2 *and* 1.4 *imply*

**Theorem 1.5.** *Every non-principal ultraproduct of $\aleph_0$ Ax fields is a hyper Ax field.*

## 2. The Elementary Equivalence Lemma for Hyper Ax Fields

The hyper Ax fields are of cardinality at least $\aleph_1$ (cf. Bell and Slomson [3, p. 218]); hence they are big enough to contain an ascending sequence of elementary subfields of cardinality $\aleph_0$. This property is used in this section to prove that every two

hyper Ax fields $F_1$, $F_2$ which contain isomorphic denumerable subfields $K_1$, $K_2$ such that $F_i/K_i$ $i=1,2$, are regular, and such that a certain group theoretical property is satisfied, are elementarily equivalent.

We begin with the following lemma, which is the main step toward the elementary equivalence theorem. All the maps in the category of pro-finite groups appearing in the sequel should be interpreted as continuous maps. In particular this applies to maps between Galois groups.

**Lemma 2.1** (The embedding lemma). *Let $E/L$, $F/M$ be two regular field extensions such that:*

a) *$E$ is a denumerable perfect field;*

b) *$F$ is hyper Ax field;*

c) *there exists an isomorphism $\Phi_0$ of $\tilde{L}$ onto $\tilde{M}$ such that $\Phi_0(L)=M$;*

d) *there exists a homomorphism $\varphi$ of $\mathcal{G}(\tilde{F}/F)$ into $\mathcal{G}(\tilde{E}/E)$ such that the diagram is commutative:*

$$\begin{array}{ccc} \mathcal{G}(\tilde{E}/E) & \xleftarrow{\varphi} & \mathcal{G}(\tilde{F}/F) \\ \downarrow & & \downarrow \\ \mathcal{G}(\tilde{L}/L) & \xleftarrow[\varphi_0]{} & \mathcal{G}(\tilde{M}/M) \end{array}$$

*where the vertical arrows are the natural restriction maps and $\varphi_0$ is the isomorphism induced by $\Phi_0$.*

*Then there exists an extension of $\Phi_0$ to a monomorphism $\Phi$ of $\tilde{E}$ into $\tilde{F}$ such that*

$$\Phi(E)\subseteq F, \quad \text{and} \quad \Phi(\varphi(\sigma)x)=\sigma\Phi(x) \quad \text{for every } \sigma\in\mathcal{G}(\tilde{F}/F) \text{ and } x\in\tilde{E}. \tag{1}$$

*If, in addition, $\varphi$ is surjective, then $F$ is regular over $\Phi(E)$.*

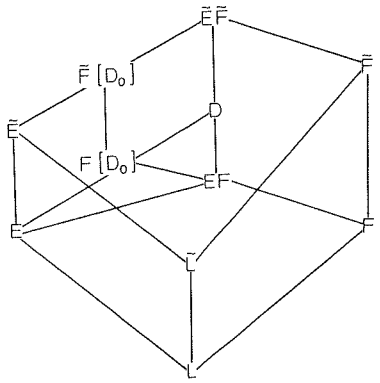
*Proof.* Without loss of generality we can assume that $L=M$ and that $\Phi_0$, $\varphi_0$ are the identity isomorphisms. Furthermore, we can assume that $E$ is free from $F$ over $L$. Hence $\tilde{E}$ is free from $\tilde{F}$ over $\tilde{L}$, so that they are linearly disjoint over $\tilde{L}$. This means that the map $x\otimes y\to xy$, $x\in\tilde{E}$, $y\in\tilde{F}$, defines an embedding of $\tilde{E}\otimes_{\tilde{L}}\tilde{F}$ onto $\tilde{E}[\tilde{F}]$. It follows that every $\sigma\in\mathcal{G}(\tilde{F}/F)$ can be uniquely extended to a $\tilde{\sigma}\in\mathcal{G}(\tilde{E}\tilde{F}/EF)$ which satisfies

$$\tilde{\sigma}x=\begin{cases}\varphi(\sigma)x & \text{if } x\in\tilde{E}\\ \sigma x & \text{if } x\in\tilde{F},\end{cases}$$

since $\varphi(\sigma)x=\sigma x$ for $x\in\tilde{L}$. The map $\sigma\to\tilde{\sigma}$ is an embedding of $\mathcal{G}(\tilde{F}/F)$ into $\mathcal{G}(\tilde{E}\tilde{F}/EF)$ whose inverse is the natural restriction map. Denote the fixed field of the image of $\mathcal{G}(\tilde{F}/F)$ by $D$. Then the restriction of the elements of $\mathcal{G}(\tilde{E}\tilde{F}/D)$ to $\tilde{F}$ gives rise to an isomorphism $\mathcal{G}(\tilde{E}\tilde{F}/D)\cong\mathcal{G}(\tilde{F}/F)$. It follows that $D\cap\tilde{F}=F$ and $D\tilde{F}=\tilde{E}\tilde{F}$.

In particular, we get that $D$ is linearly disjoint from $\tilde{F}$ over $F$, *i.e.* $D$ is a regular extension of $F$. $\tilde{E}\tilde{F}$ is an algebraic extension of $D$; hence $\tilde{E}\subseteq D[\tilde{F}]=\tilde{F}[D]$. It follows that every element $x\in\tilde{E}$ can be written in the form

$$x=\sum y_i d_i \qquad y_i\in\tilde{F},\ d_i\in D. \tag{2}$$




Denote by $D_0$ the set of all the $d_i$ which appear in the expressions (2) for all $x \in \tilde{E}$. $D_0$ is denumerable, since $E$ is such, and we have that

$$\tilde{E} \subseteq \tilde{F}[D_0]. \tag{3}$$

If $x$ in (2) belongs to $E$, then, representing the $y_i$ as a linear combination of a basis $\{z_j\}$ of $\tilde{F}$ over $F$ which contains 1, and noting that $D$ is linearly disjoint from $\tilde{F}$ over $F$, we find a representation of the form (2) of $x$ in which the $y_i$ belong to $F$. Thus $E \subseteq F[D_0]$. $F[D_0]$ is a denumerably generated $F$-algebra which is contained in $D$, hence it is absolutely entire. It follows, by (b), that there exists an $F$-homomorphism $\Psi: F[D_0] \to F$. $\Psi$ can be extended to an $\tilde{F}$-homomorphism

$$\tilde{\Psi}: \tilde{F}[D_0] \to \tilde{F},$$

since $D$ is linearly disjoint from $\tilde{F}$ over $F$. Our definitions imply that

$$\tilde{\Psi}(\tilde{\sigma} x) = \sigma \Psi(x) \tag{4}$$

for every $\sigma \in \mathcal{G}(\tilde{F}/F)$ and for every $x$ which belongs to $\tilde{F}$ or to $D_0$, hence also for every $x \in \tilde{F}[D_0]$. In particular (4) holds for every $x \in \tilde{E}$, by (3). Hence, if we denote by $\Phi$ the restriction of $\tilde{\Psi}$ to $\tilde{E}$, we get that $\Phi$ is a monomorphism of $\tilde{E}$ into $\tilde{F}$ which fixes the elements of $L$ and satisfies (1).

Suppose now that the map $\varphi$ is surjective. Let $x \in \tilde{E}$ such that $\Phi(x) \in F$. Then, by (1), $\Phi(\varphi(\sigma) x) = \Phi(x)$, i.e. $\varphi(\sigma) x = x$, for every $\sigma \in \mathcal{G}(\tilde{F}/F)$; hence $x \in E$. It follows that $\Phi(\tilde{E}) \cap F = \Phi(E)$. This means that $F$ is a regular extension of $\Phi(E)$. ‖

*Remark.* If $\mathcal{G}(\tilde{F}/F) \cong \mathcal{G}(\tilde{E}/E) \cong \hat{\mathbb{Z}}$ then condition (d) of Lemma 2.1 is automatically fulfilled. (We shall prove later a generalization of this fact.) Our lemma reduces in this case to Proposition 2 of Ax [2]. Our proof appears to be simpler than that of Ax.

**Lemma 2.2.** *Let $K$ be a field, let $L$ and $M$ be extensions of $K$ and let $E$ and $F$ be regular extensions of $L$ and $M$ respectively. Suppose that*

(a) *$E$ and $F$ are hyper Ax fields;*

(b) *there exists a $K$-isomorphism $\Phi_0$ of $\tilde{L}$ onto $\tilde{M}$ such that $\Phi_0(L) = M$;*

(c) *there exists an isomorphism* $\varphi$ *of* $\mathcal{G}(\tilde{F}/F)$ *onto* $\mathcal{G}(\tilde{E}/E)$ *such that the diagram*

$$\begin{array}{ccc} \mathcal{G}(\tilde{E}/E) & \xleftarrow{\varphi} & \mathcal{G}(\tilde{F}/F) \\ \downarrow & & \downarrow \\ \mathcal{G}(\tilde{L}/L) & \xleftarrow[\varphi_0]{} & \mathcal{G}(\tilde{M}/M) \end{array}$$

*is commutative. Here* $\varphi_0$ *is induced by* $\Phi_0$.

*Then* $E$ *is* $K$*-elementarily equivalent to* $F$.

*Proof.* Suppose first that $L$ and $M$ are denumerable. By the Skolem-Löwenheim Theorem there exists a denumerable $K$-elementary subfield $M_1$ of $F$ which contains $M$ (cf. Bell and Slomson [3, p. 80]). Then $M_1$ is a perfect field which is algebraically closed in $F$. Hence, the map $\rho \circ \varphi^{-1}: \mathcal{G}(\tilde{E}/E) \to \mathcal{G}(\tilde{M}/M)$, where $\rho$ is the natural restriction map of $\mathcal{G}(\tilde{F}/F)$ onto $\mathcal{G}(\tilde{M}_1/M_1)$, is surjective. By Lemma 2.1 there exists a monomorphism $\Psi_1$ of $\tilde{M}_1$ into $\tilde{E}$ which extends $\Phi_0^{-1}$ such that $\Psi_1(M_1)$ is algebraically closed in $E$. Moreover, the isomorphism $\psi_1$ of

$$\mathcal{G}(\widetilde{\Psi_1(M_1)}/\Psi_1(M_1))$$

onto $\mathcal{G}(\tilde{M}_1/M_1)$ which is induced by $\Psi_1$ makes the diagram

$$\begin{array}{ccc} \mathcal{G}(\tilde{E}/E) & \xrightarrow{\varphi^{-1}} & \mathcal{G}(\tilde{F}/F) \\ \downarrow & & \downarrow \\ \mathcal{G}(\widetilde{\Psi_1(M_1)}/\Psi_1(M_1)) & \xrightarrow{\psi_1} & \mathcal{G}(\tilde{M}_1/M_1) \end{array}$$

commutative. Again we can find a denumerable $K$-elementary subfield $L_1$ of $E$ which contains $\Psi_1(M_1)$ and then a monomorphism $\Phi_1$ of $\tilde{L}_1$ into $\tilde{F}$ which extends $\Psi_1^{-1}$ such that $\Phi_1(L_1)$ is algebraically closed in $F$ and the corresponding group theoretical condition is fulfilled. In this way we can construct by induction two towers of denumerable fields,

$$L \subseteq L_1 \subseteq L_2 \subseteq \cdots \subseteq E; \qquad M \subseteq M_1 \subseteq M_2 \subseteq \cdots \subseteq F,$$

and monomorphisms $\Phi_i: L_i \to M_{i+1}$, $\Psi_i: M_i \to L_i$ such that $L_i$ is a $K$-elementary subfield of $E$, $M_i$ is a $K$-elementary subfield of $F$, $\Phi_i$ extends $\Psi_i^{-1}$ and $\Psi_i$ extends $\Phi_{i-1}^{-1}$. Let

$$L_\infty = \bigcup_{i=1}^{\infty} L_i, \qquad M_\infty = \bigcup_{i=1}^{\infty} M_i.$$

Then $L_\infty$ and $M_\infty$ are $K$-elementary subfields of $E$ and $F$ respectively, as can be easily proved (*e.g.* using Corollary 1.9 of Bell and Slomson [100, p. 76]). Moreover, the $\Phi_i$ and $\Psi_i$ can be combined to give a $K$-isomorphism $\Phi_\infty$ of $L_\infty$ onto $M_\infty$ and $\Psi_\infty$ of $M_\infty$ onto $L_\infty$ which are inverse to each other. It follows that $E \equiv_K F$.

Consider now the general case. Let $\Theta$ be a sentence of $\mathfrak{L}(K)$ which is true in $E$. There are only finitely many elements of $K$, say $x_1, \ldots, x_n$, which occur in $\Theta$.

Let $K_0$ be a denumerable subfield of $K$ which contains $x_1, \ldots, x_n$, let $L_0 = L \cap \tilde{K}_0$ and $M_0 = M \cap \tilde{K}_0$. Then $\Theta$ is also a sentence of $\mathfrak{L}(K_0)$, $L_0$ and $M_0$ are denumerable and $\Phi_0$ induces a $K$-isomorphism of $L_0$ onto $M_0$. It follows, by the first part of the proof that $E \equiv_{K_0} F$. Hence $F \models \Theta$. ‖

*Remark.* If $E$ and $F$ have cardinality $\aleph_1$, then one can extend the complete induction to a transfinite induction on all ordinals $\alpha < \aleph_1$ and eventually get a $K$-isomorphism between $E$ and $F$. However, we do not need this result, so we do not state it as a theorem.

## 3. The Elementary Equivalence Theorem for Ax Fields

We want now to obtain Lemma 2.2 for Ax fields rather than for hyper Ax fields. By Theorem 1.6 we can obtain hyper Ax fields from Ax fields by raising them to a non-principal ultrapower with an index set of cardinality $\aleph_0$. We can therefore achieve our result if we show that the group theoretic condition which appears in Lemma 2.2 is preserved in the passage to ultrapowers. This is done in the following lemma.

**Lemma 3.1.** *Let $E, F$ be two perfect fields such that there exists an isomorphism $\varphi$ of $\mathcal{G}(\tilde{F}/F)$ onto $\mathcal{G}(\tilde{E}/E)$. Let $\mathcal{D}$ be an ultrafilter of a set $I$, and write ${}^*E = E^I/\mathcal{D}$, ${}^*F = F^I/\mathcal{D}$. Then there exists an isomorphism $\tilde{\varphi}$ of $\mathcal{G}({}^{\widetilde{*}}F, {}^*F)$ onto $\mathcal{G}({}^{\widetilde{*}}E/{}^*E)$ such that the diagram*

$$\begin{array}{ccc} \mathcal{G}({}^{\widetilde{*}}E/{}^*E) & \xleftarrow{\tilde{\varphi}} & \mathcal{G}({}^{\widetilde{*}}F/{}^*F) \\ \downarrow & & \downarrow \\ \mathcal{G}(\tilde{E}/E) & \xleftarrow[\varphi]{} & \mathcal{G}(\tilde{F}/F) \end{array} \qquad (*)$$

*is commutative.*

*Proof.* Let $M$ be a Galois extension of ${}^*F$ of degree $n$. Then there exists a $y \in {}^*\tilde{F} = \tilde{F}^I/\mathcal{D}$ such that ${}^*M = {}^*F(y)$. Let $g \in {}^*F[Y]$ be an irreducible polynomial such that $g(y) = 0$. Then $g$ is normal over ${}^*F$ (*i.e.* all the roots of $g$ are contained in ${}^*F(y)$). These are elementary statements, hence, for almost all $i \in I$ (*i.e.* for a set of $i \in I$ which belongs to $\mathcal{D}$) we have: $g_i \in F[Y]$ is an irreducible normal polynomial over $F$ of degree $n$ such that $g_i(y_i) = 0$. Here $\{g_i \mid i \in I\}$ and $\{y_i \mid i \in I\}$ are representative sets for $g$ and $y$ respectively. Write $M_i = F(y_i)$. Then $M_i$ is a Galois extension of $F$ of degree $n$, for almost all $i$, and $M = \prod M_i/\mathcal{D}$. If we denote by $L_i$ the fixed field of $\varphi \mathcal{G}(\tilde{F}/M_i)$, then we get the following commutative diagram of exact short sequences

$$\begin{array}{ccccccccc} 1 & \longrightarrow & \mathcal{G}(\tilde{F}/M_i) & \longrightarrow & \mathcal{G}(\tilde{F}/F) & \longrightarrow & \mathcal{G}(M_i/F) & \longrightarrow & 1 \\ & & \downarrow{\scriptstyle \varphi} & & \downarrow{\scriptstyle \varphi} & & \downarrow{\scriptstyle \varphi_{M_i}} & & \\ 1 & \longrightarrow & \mathcal{G}(\tilde{E}/L_i) & \longrightarrow & \mathcal{G}(\tilde{E}/E) & \longrightarrow & \mathcal{G}(L_i/E) & \longrightarrow & 1. \end{array}$$

Here $\varphi_{M_i}$ is the isomorphism induced by $\varphi$. Then $L_i$ is a Galois extension of $E$ of degree $n$, for almost all $i$. Write $L=\prod L_i/\mathcal{D}$ and $\varphi_M=\prod\varphi_{M_i}/\mathcal{D}$. Then $L$ is a Galois extension of $^*E$ of degree $n$ and $\varphi_M$ is an isomorphism of $\mathcal{G}(M/^*F)$ onto $\mathcal{G}(L/^*E)$. It is easy to see that $L$ is uniquely defined by $M$, *i.e.* it does not depend on the choice of $y$ or on the choice of the representative of $y$. Moreover, if we exchange the roles of $E$ and $F$ and start with $L$, then $M$ will be the corresponding field and $\psi_L=\varphi_M^{-1}$ will be the corresponding isomorphism.

If $M'$ is another finite Galois extension of $^*F$ which contains $M$, then $L'$ contains $L$ and the diagram

$$\begin{array}{ccc} \mathcal{G}(L'/^*E) & \xleftarrow{\varphi_{M'}} & \mathcal{G}(M'/^*F) \\ \downarrow & & \downarrow \\ \mathcal{G}(L/^*E) & \xleftarrow{\varphi_M} & \mathcal{G}(M/^*F) \end{array}$$

is commutative. It follows that the $\varphi_M$'s can be combined to form an isomorphism $\tilde{\varphi}$ of $\mathcal{G}(\widetilde{^*F}/^*F)$ onto $\mathcal{G}(\widetilde{^*E}/E)$.

It remains now to show that the diagram $(*)$ is commutative. Let $M_0$ be a finite Galois extension of $F$ and let $y\in\tilde{F}$ be such that $M_0=F(y)$. Let $L_0$ be the fixed field of $\varphi\mathcal{G}(\tilde{F}/M_0)$ and write $L_0=E(x)$, with $x\in\tilde{E}$. Put $M=^*F(y)$. Then $y_i=y$, $M_i=M_0$ and $L_i=L_0$ for every $i\in I$. Hence $L=\prod L_i/\mathcal{D}=^*E(x)$ and it is clear that if $\sigma\in\mathcal{G}(\widetilde{^*F}/^*F)$ then $\varphi(\sigma|\tilde{F})\,x=\tilde{\varphi}(\sigma)\,x$. Hence $(*)$ is indeed commutative.

**Theorem 3.2.** *Let $K$ be a field, let $L$ and $M$ be extensions of $K$ and let $E$ and $F$ be regular extensions of $L$ and $M$ respectively. Suppose that:*

(a) *$E$ and $F$ are* Ax *fields;*

(b) *there exists a $K$-isomorphism $\Phi_0$ of $\tilde{L}$ onto $\tilde{M}$ such that $\Phi_0(L)=M$;*

(c) *there exists an isomorphism $\varphi$ of $\mathcal{G}(\tilde{F}/F)$ onto $\mathcal{G}(\tilde{E}/E)$ such that the diagram*

$$\begin{array}{ccc} \mathcal{G}(\tilde{E}/E) & \xleftarrow{\varphi} & \mathcal{G}(\tilde{F}/F) \\ \downarrow & & \downarrow \\ \mathcal{G}(\tilde{L}/L) & \xleftarrow{\varphi_0} & \mathcal{G}(\tilde{M}/M) \end{array}$$

*is commutative. Here $\varphi_0$ is induced by $\Phi_0$.*

*Then $E$ is $K$-elementarily equivalent to $F$.*

*Proof.* Let $I$ be a denumerable set and let $\mathcal{D}$ be a non-principal ultrafilter of $I$. In the notations of Lemma 3.1 we have, by Theorem 1.5, that $^*E$ and $^*F$ are hyper Ax fields and we have the commutative diagram $(*)$ of Lemma 3.1. If we combine it with the diagram of Lemma 2.2 we get the following commutative diagram

$$\begin{array}{ccc} \mathcal{G}(\widetilde{^*E}/^*E) & \xleftarrow{\tilde{\varphi}} & \mathcal{G}(\widetilde{^*F}/^*F) \\ \downarrow & & \downarrow \\ \mathcal{G}(\tilde{L}/L) & \xleftarrow{\varphi_0} & \mathcal{G}(\tilde{M}/M). \end{array}$$

Moreover, $^*E/E$ and $^*F/F$ are regular extensions, hence $^*E/L$ and $^*F/M$ are regular extensions. It follows from Lemma 2.2 that $^*E$ is $K$-elementarily equivalent to $^*F$. Hence $E$ is $K$-elementarily equivalent to $F$, since $^*E$ and $^*F$ are $K$-elementary extensions of $E$ and $F$ respectively. ‖

## 4. A Consequence of a Theorem of Gaschütz

There are some cases in which the group theoretic condition which appears in Theorem 3.2 is automatically fulfilled. This happens when the groups involved are finitely generated free pro-finite groups.

For each positive integer $e$ we denote by $\hat{F}_e$ the free pro-finite group generated by $e$ elements. (For the definition of $\hat{F}_e$ and its properties, consult, for example, Ribes [12, Chap. I, § 7].)

The following lemma is a special case of an astonishing lemma of Gaschütz [4, Satz 1].

**Lemma 4.1.** *Let $\vartheta: G \to H$ be an epimorphism of finite groups. If $G$ is generated by $e$ elements, then for every system $y_1, \ldots, y_e$ of generators of $H$ there exists a system $x_1, \ldots, x_e$ of generators of $G$ such that $\vartheta x_i = y_i$ for $i = 1, \ldots, e$.*

The pro-finite equivalent to Lemma 4.1 is the following lemma.

**Lemma 4.2.** *Let $\vartheta: G \to H$ be an epimorphism of pro-finite groups. If $G$ is (topologically) generated by $e$ elements, then for every system $y_1, \ldots, y_e$ of generators of $H$ there exists a system $x_1, \ldots, x_e$ of generators of $G$ such that $\vartheta x_i = y_i$ for $i = 1, \ldots, e$.*

*Proof.* Consider first the case where $H$ is finite. Then the kernel $N$ of $\vartheta$ is a closed normal subgroup of $G$ of finite index. For every closed normal subgroup $M$ of $G$ of finite index which is contained in $N$ we write $\mathscr{G}(M) = \{(x_1, \ldots, x_e) \in G^e \mid (\underline{x})$ generates $G$ modulo $M$ and $\vartheta(\underline{x}) = (\underline{y})\}$. Then $\mathscr{G}(M)$ is a closed subset of $G^e$ and it is not empty, by Lemma 4.1. Since $\mathscr{G}(M_1) \cap \mathscr{G}(M_2) \supseteq \mathscr{G}(M_1 \cap M_2)$ and $G^e$ is compact, there exists an $e$-tuple $(\underline{x})$ which belongs to all the $\mathscr{G}(M)$. This $e$-tuple generates $G$ and satisfies the condition $\vartheta x_i = y_i$ for $i = 1, \ldots, e$.

Return now to the general case. For every closed normal subgroup $I$ of $H$ of finite index we write

$$\mathscr{H}(I) = \{(x_1, \ldots, x_e) \in G^e \mid (\underline{x}) \text{ generates } G \text{ and } \vartheta(\underline{x}) \equiv (\underline{y}) \pmod{I}\}.$$

Then, by the first part of the proof, $\mathscr{H}(I)$ is a non-empty closed subset of $G^e$. As before, we find that there exists an $e$-tuple $(\underline{x})$ which belongs to all the $\mathscr{H}(I)$. This $e$-tuple generates $G$ and satisfies the condition $\vartheta(\underline{x}) = (\underline{y})$. ‖

As a result of 4.2 we get

**Lemma 4.3.** *Let $\vartheta_1$ and $\vartheta_2$ be two epimorphisms of $\hat{F}_e$ onto a pro-finite group $G$. Then there exists a continuous automorphism $\varphi$ of $\hat{F}_e$ such that $\vartheta_1 \circ \varphi = \vartheta_2$.*

*Proof.* Let $x_1, \ldots, x_e$ be a system of generators for $\hat{F}_e$. Write $y_i = \vartheta_2 x_i$ for $i = 1, \ldots, e$. Then $y_1, \ldots, y_e$ generate $G$. By Lemma 4.2, there exists a system

$z_1, \ldots, z_e$ of generators of $\hat{F}_e$ such that $\vartheta_1 z_i = x_i$, for $i = 1, \ldots, e$. The map $x_i \mapsto z_i$, $i = 1, \ldots, e$, can now be extended to a continuous epimorphism $\varphi$ of $\hat{F}_e$ onto itself, which obviously satisfies $\vartheta_1 \varphi = \vartheta_2$. It follows from Ribes [12, p. 69], that $\varphi$ is indeed an automorphism. ‖

A field $F$ is said to be $e$-free if $\mathcal{G}(F_s/F) \cong \hat{F}_e$; here $F_s$ is the separable closure of $F$. If a field $F$ of characteristic $p$ is $e$-free then $F^{1/p^\infty}$ is a perfect $e$-free field, since $\mathcal{G}(\tilde{F}/F^{1/p^\infty}) \cong \mathcal{G}(F_s/F)$.

**Theorem 4.4.** *Let $E$, $F$ be $e$-free Ax fields which contain a common field $K$. If $\tilde{K} \cap E \cong_K \tilde{K} \cap F$, then $E \equiv_K F$.*

*Proof.* Write $L = \tilde{K} \cap E$, $M = \tilde{K} \cap F$ and let $\Phi_0$ be an automorphism of $\tilde{K}$ such that $\Phi_0(L) = M$. $L$ and $M$ are perfect fields and $E/L$, $F/M$ are regular extensions, since $E$, $F$ are perfect. Let $\varphi_0$ be the isomorphism of $\mathcal{G}(\tilde{K}/M)$ onto $\mathcal{G}(\tilde{K}/L)$ induced by $\Phi_0$ and let $\rho$: $\mathcal{G}(\tilde{E}/E) \to \mathcal{G}(\tilde{K}/L)$, $\rho'$: $\mathcal{G}(\tilde{F}/F) \to \mathcal{G}(\tilde{K}/M)$ be the natural epimorphisms induced by restriction. Then, by Lemma 4.3, there exists an isomorphism $\varphi$: $\mathcal{G}(\tilde{F}/F) \to \mathcal{G}(\tilde{E}/E)$ such that $\rho \circ \varphi = \varphi \circ \rho'$, since $\mathcal{G}(\tilde{F}/F) \cong \mathcal{G}(\tilde{E}/E) \cong \hat{F}_e$. Theorem 3.2 asserts now that $E \equiv_K F$. ‖

**Corollary 4.5.** *Let $E$, $F$ be $e$-free Ax fields such that $E$ is contained in $F$. If $\tilde{E} \cap F = E$, then $F$ is an elementary extension of $E$.*

*Remark.* Corollary 4.5 means that the theory of $e$-free Ax fields possesses a weak form of model completeness.

## 5. Axiomatization of the Concept of an $e$-Free Field

The concept of an $e$-free field can, like the concept of an Ax field, be characterized by $\aleph_0$ elementary statements. In order to prove this claim, we first cite the following lemma from [7, Thm. 2.4].

**Lemma 5.1.** *Let $G$ be a pro-finite group which is generated by $e$ elements. Then $G$ is isomorphic to $\hat{F}_e$ if and only if every finite group with $e$ generators is a homomorphic image of $G$.*

Using a standard compactness argument one can see that the condition "$G$ is generated by $e$ elements" is equivalent to "Every finite homomorphic image of $G$ is generated by $e$ elements". Lemma 5.1 therefore applies.

**Lemma 5.2.** *A pro-finite group $G$ is isomorphic to $\hat{F}_e$ if and only if it satisfies the following conditions:*

a) *Every finite group generated by $e$ elements is a homomorphic image of $G$.*

b) *Every finite homomorphic image of $G$ is generated by $e$ elements.*

If we translate Lemma 5.2 to the (non-formal) language of fields, we get the following lemma.

**Lemma 5.3.** *A field $F$ is $e$-free if and only if it satisfies the following conditions:*

a) *The Galois group, $\mathcal{G}(f, F)$ over $F$ of every monic polynomial $f \in F[X]$ without multiple roots is generated by e elements.*

b) *For every finite group $H$ generated by e elements, there exists a monic $f \in F[X]$, without multiple roots, such that $\mathcal{G}(f, F) \cong H$.*

Our task now is to show that each of the conditions (a) and (b) can be rewritten as a conjunction of $\aleph_0$ elementary statements. For this purpose, consider a polynomial

$$f(X) = X^n + c_1 X^{n-1} + \cdots + c_n$$

with coefficients $c_i$ in $F$ and with $n$ distinct roots $a_1, \ldots, a_n$ in $F_s$. Let $U_1, \ldots, U_n$ be $n$ variables and write $W = a_1 U_1 + \cdots + a_n U_n$. Let $S(\underline{U})$ be the full permutation group of $\{U_1, \ldots, U_n\}$. For every $\pi \in S(\underline{U})$ write

$$\pi W = a_1 \pi U_1 + \cdots + a_n \pi U_n.$$

Consider the polynomial

$$g(\underline{a}, \underline{U}, Z) = \prod_{\pi \in S(\underline{U})} (Z - \pi W)$$

in the variables $\underline{U}, Z$ and with $a_1, \ldots, a_n$ as parameters. Clearly $g$ is invariant under permutations of the $a_i$; hence its coefficients are symmetric polynomials in the $a_i$ with integral coefficients. Thus they are polynomials in the $c_i$ with integral coefficients. We can therefore write

$$g(\underline{a}, \underline{U}, Z) = \sum_{(\nu)} g_\nu(\underline{c})\, U_1^{\nu_1} \ldots U_n^{\nu_n} Z^{\nu_{n+1}}. \qquad (*)$$

The degree of $g$ is $n!$. Note that the $g_\nu$ depend only on $n$ and we can effectively calculate them. Their coefficients must always be interpreted modulo the characteristic of $F$. We abbreviate the right hand side of $(*)$ by $h(\underline{c}, \underline{U}, Z)$. Let

$$h(\underline{c}, \underline{U}, Z) = h_1(\underline{U}, Z) \ldots h_r(\underline{U}, Z)$$

be a factorisation of $h$ in $F[\underline{U}, Z]$ into irreducible factors. Every one of the $h_i$ has in $F(\underline{a})$ the form

$$h_i(\underline{U}, Z) = \prod_{\pi \in S_i} (Z - \pi W),$$

where $S_i$ is a subset of $S(\underline{U})$. The elements of $S(\underline{U})$ operate on the $h_i$ according to the formula

$$\tau h_i(\underline{U}, Z) = h_i(\tau \underline{U}, Z) = \prod_{\pi \in S_i} (Z - \tau \pi W),$$

and the set $\{h_1, \ldots, h_r\}$ is permuted by this operation. Let now $\tau_1 \in S_1$. Then $S(\underline{U})$ is isomorphic to $S(\tau_1 \underline{a})$, as a permutation group, by the map $\pi \mapsto \pi'$, where $\pi'$ is defined by

$$\pi'(a_i) = a_j \Leftrightarrow \pi(\tau_1 U_i) = \tau_1 U_j.$$

It is well known that the subgroup $G = \{\pi \in S(\underline{U}) \mid \pi h_1 = h_1\}$ of $S(\underline{U})$, is mapped under this isomorphism onto $\mathcal{G}(f, F)$ (cf. Van der Waerden [13, § 61]).

Using this description of $\mathcal{G}(f, F)$, we denote by $\Lambda'_a(n)$ the following statement:

For every $c_1, \ldots, c_n$ such that $f(X)=X^n+c_1 X^{n-1}+\cdots+c_n$ has no multiple roots, there exist irreducible polynomials $h_1(\underline{U}, Z), \ldots, h_r(\underline{U}, Z)$ such that

$$h(\underline{c}, \underline{U}, Z)=\prod_{i=1}^{r} h_i(\underline{U}, Z)$$

and such that for at least one of the $e$-tuples $(\pi_1, \ldots, \pi_e)\in S(\underline{U})^e$ the following statement holds: $\bigwedge_{i=1}^{e} \pi_i h_1 = h_1$ and for all $\pi\in S(\underline{U})$, $\pi h_1 = h_1$ implies that $\bigwedge_{j=1}^{n} \pi U_j = \omega U_j$ for at least one $\omega\in\langle \pi_1, \ldots, \pi_e\rangle$.

Note that for a given $\pi_1, \ldots, \pi_e$ one can explicitely write the subgroup $\langle \pi_1, \ldots, \pi_e\rangle$, and this can be done in a finite number of steps, a bound for which can be calculated in advance.

By the above reasoning $F$ satisfies condition (a) of Lemma 5.3 if and only if $\Lambda'_a(n)$ holds over $F$ for every $n\geqq 1$.

Let $G$ be a group of $n$ elements. Then $G$ can be identified with a subsgroup of $S(U_1, \ldots, U_n)$. We denote by $\Lambda'_b(G)$ the following statement:

There exist $c_1, \ldots, c_n$ such that $f(X)=X^n+c_1 X^{n-1}+\cdots+c_n$ has no multiple roots, and there exist irreducible polynomials $h_1(\underline{U}, Z), \ldots, h_r(\underline{U}, Z)$ such that $h(\underline{c}, \underline{U}, Z)=\prod_{i=1}^{r} h_i(\underline{U}, Z)$, $\pi h_1 = h_1$ for all $\pi\in G$, and $\pi h_1 \neq h_1$ for all $\pi\in S(\underline{U})-G$.

Again, $F$ satisfies condition (b) of Lemma 5.3 if and only if $\Lambda'_b(G)$ holds over $F$ for every finite group $G$ generated by $e$ elements.

It is not difficult to see that $\Lambda'_a(n)$ and $\Lambda'_b(G)$ are equivalent to sentences $\Lambda_a(n)$, $\Lambda_b(G)$ in the formal language $\mathfrak{L}$. Altogether, there are $\aleph_0$ sentences. Taking into account Lemma 5.3, we have proved the following lemma.

**Lemma 5.4.** *There is a sequence $\Lambda_1, \Lambda_2, \Lambda_3, \ldots$ of sentences in $\mathfrak{L}$, which can be explicitely written down, such that a field $F$ is e-free, if and only if it satisfies $\Lambda_i$ for every $i\geqq 1$.*

## 6. Regular Ultraproducts

If $L$ is an $e$-free field, then $\mathcal{G}(L_s/L)$ is generated by $e$ elements; any field $L$ whose Galois group, $\mathcal{G}(L_s/L)$, is generated be $e$ elements, is said to have *corank* $\leqq e$ (cf. [7, § 1]). In this section we consider a fixed field $K$ and study, via measure theory, the set of all fields of corank $\leqq e$ which are algebraic over $K$. It turns out that, if $K$ is denumerable and hilbertian, then "almost all" of these fields are $e$-free Ax fields. The assumption that a field is hilbertian will, however, be made only in Section 7. Here we shall study relations between these fields and their "regular" ultraproducts which are valid without this assumption. We begin by introducing the Haar measure.

It is well known that the Galois group $\mathcal{G}(K_s/K)$ is compact with respect to its Krull topology. There is, therefore, a unique way to define a Haar measure $\mu$ on the Borel field of $\mathcal{G}(K_s/K)$ such that $\mu(\mathcal{G}(K_s/K))=1$. If $L$ is a finite separable extension of $K$, then $\mu(\mathcal{G}(K_s/L))=[L:K]^{-1}$; if $L$ is an infinite extension then

$\mu(\mathcal{G}(K_s/L))=0$. We complete $\mu$ by adjoining to the Borel field all the subsets of zero sets and denote the completion also by $\mu$. More generally, for a positive integer $e$, we consider the product space $\mathcal{G}(K_s/K)^e$ and again denote by $\mu$ the appropriate completion of the power measure. It coincides with the completion of the Haar measure of $\mathcal{G}(K_s/K)^e$. In particular, this implies that if $L$ is a finite Galois extension of $K$ and $C$ is a subset of $\mathcal{G}(L/K)^e$, then

$$\mu(\{(\underline{\sigma})\in\mathcal{G}(K_s/K)^e \mid (\underline{\sigma}|L)\in C\})=\frac{|C|}{[L:K]^e}. \tag{1}$$

An ultrafilter $\mathcal{D}$ of $\mathcal{G}(K_s/K)^e$ is said to be *regular*, if it contains all the subsets of $\mathcal{G}(K_s/K)^e$ of measure 1. It follows that if $K_s/K$ is an infinite extension, then every regular ultrafilter is non-principal. The following lemma shows how to construct regular ultrafilters; it is analogous to the corresponding lemma for non-principal ultrafilters.

**Lemma 6.1.** *Let $\mathcal{D}_0$ be a family of subsets of $\mathcal{G}(K_s/K)^e$ such that for every $A_1,\dots,A_n\in\mathcal{D}_0$, $A_1\cap\cdots\cap A_n$ is not a zero set. Then there exists a regular ultrafilter of $\mathcal{G}(K_s/K)^e$ which contains $\mathcal{D}_0$.*

*Proof.* Let $\mathcal{D}_1$ be the family of all subsets of $\mathcal{G}(K_s/K)^e$ of measure 1. Then $B_1\cap\cdots\cap B_n$ is not empty for every $B_1,\dots,B_n\in\mathcal{D}_1\cup\mathcal{D}_2$. It follows that there exists an ultrafilter of $\mathcal{G}(K_s/K)^e$ which contains $\mathcal{D}_1\cup\mathcal{D}_2$. This ultrafilter is regular. ‖

For every $(\underline{\sigma})=(\sigma_1,\dots,\sigma_e)\in\mathcal{G}(K_s/K)^e$, let $K_s(\underline{\sigma})$ be the fixed field in $K_s$ of $\sigma_1,\dots,\sigma_e$. If $p=\mathrm{char}(K)$, let $\tilde{K}(\underline{\sigma})=K_s(\underline{\sigma})^{1/p^\infty}$; it is the fixed field in $\tilde{K}$ of the unique extension of $\sigma_1,\dots,\sigma_e$ to $\tilde{K}$. To every regular ultrafilter $\mathcal{D}$ of $\mathcal{G}(K_s/K)^e$ there corresponds an ultraproduct $\prod\tilde{K}(\underline{\sigma})/\mathcal{D}$, which will be referred to as a *regular* ultraproduct. This corresponds to the non-principal ultraproducts of the finite fields in Ax theory (cf. [1, part II] and [6]). Analogously to Proposition 7 of [6], we prove the following lemma.

**Lemma 6.2.** (a) *If $F$ is an ultraproduct of the fields $\tilde{K}(\underline{\sigma})$, then $\tilde{K}\cap F$ is perfect and of corank $\leqq e$.*

(b) *For every perfect subfields $L$ of $\tilde{K}$ of corank $\leqq e$ which contains $K$, there exists a regular ultraproduct $F$ of the $\tilde{K}(\underline{\sigma})$ such that $\tilde{K}\cap F\cong_K L$.*

*Proof.* a) It was proved in Section 5 that the property of a field of having corank $\leqq e$ is equivalent to a conjunction of sentences in $\mathfrak{L}$. Each one of them holds for every $\tilde{K}(\underline{\sigma})$, hence also for $F$. It follows that $\mathrm{corank}(F)\leqq e$. Clearly $F$ is also perfect, hence $\tilde{K}\cap F$ is perfect. The group $\mathcal{G}(\tilde{K}/\tilde{K}\cap F)$ is a homomorphic image of $\mathcal{G}(\tilde{F}/F)$, hence $\mathcal{G}(\tilde{K}/\tilde{K}\cap F)$ is also generated by $e$ elements.

b) We begin the proof of (b) by introducing some notations. For every perfect extension $E$ of $K$ we denote by $[E/K]$ the set of all polynomials $f\in K[X]$ which have a root in $E$. Ax proved in [11, p. 172] that if $E'$ is another perfect extension of $K$, then

$$[E/K]=[E'/K]\Leftrightarrow\tilde{K}\cap E\cong_K\tilde{K}\cap E'. \tag{2}$$

For every $f \in K[X]$ we define

$$A(f) = \{(\underline{\sigma}) \in \mathcal{G}(K_s/K)^e \mid f \text{ has a root in } \tilde{K}(\underline{\sigma})\}.$$

We also write $B(f) = \mathcal{G}(K_s/K)^e - A(f)$. These notations will also be used in the sequel.

By our assumption, there exist $\tau_1, \ldots, \tau_e \in \mathcal{G}(K_s/K)^e$ such that $\tilde{K}(\underline{\tau}) = L$. Let $f_1, \ldots, f_m, g_1, \ldots, g_n \in K[X]$ be separable polynomials such that $f_1, \ldots, f_m \in [L/K]$ and $g_1, \ldots, g_n \notin [L/K]$. Let $K'$ be a finite Galois extension of $K$ which contains all the roots of $f_1, \ldots, f_m, g_1, \ldots, g_n$. Then $\{(\underline{\sigma}) \in \mathcal{G}(K_s/K)^e \mid \sigma_i | K' = \tau_i | K' \text{ for } i = 1, \ldots, e\}$ is a set of positive measure which is contained in $A(f_1) \cap \cdots \cap A(f_m) \cap B(g_1) \cap \cdots \cap B(g_n)$. By Lemma 6.1, there exists a regular ultrafilter $\mathcal{D}$ of $\mathcal{G}(K_s/K)^e$ which contains all the $A(f)$ and $B(g)$ such that $f \in [L/K]$, $g \in K[X] - [L/K]$ and $f, g$ are separable over $K$. Denote $F = \prod \tilde{K}(\underline{\sigma})/\mathcal{D}$, then for every separable $h \in K[X]$, $h$ has a root in $\tilde{K} \cap F$ if and only if it has a root in $L$. This implies that $[F/K] = [L/K]$, since $F$ and $L$ are perfect. Hence $\tilde{K} \cap F \cong_K L$, by (2). ‖

## 7. Elementary Statements over Regular Ultraproducts

For a $K$-elementary statement $\Theta$ we write

$$A(\Theta) = A_K(\Theta) = \{(\underline{\sigma}) \in \mathcal{G}(K_s/K)^e \mid \tilde{K}(\underline{\sigma}) | = \Theta\}.$$

In particular, note that $A(f) = A(\exists X[f(X) = 0])$. Clearly, $A(\Theta_1 \vee \Theta_2) = A(\Theta_1) \cup A(\Theta_2)$ and $-A(\Theta) = A(\sim \Theta)$.

**Proposition 7.1.** *Let $K$ be a denumerable field and let $\Theta$ be a $K$-elementary statement. Then $\tilde{K}(\underline{\sigma}) | = \Theta$ for almost all $(\underline{\sigma}) \in \mathcal{G}(K_s/K)^e$, if and only if $F | = \Theta$ for every regular ultraproduct $F$ of the $\tilde{K}(\underline{\sigma})$.*

*Proof.* If $\mu(A(\Theta)) = 1$, then $A(\Theta) \in \mathcal{D}$, for every regular ultrafilter $\mathcal{D}$ of $\mathcal{G}(K_s/K)^e$; hence $\prod \tilde{K}(\underline{\sigma})/\mathcal{D} | = \Theta$. If $A(\Theta)$ is not a set of measure 1, then, by Lemma 6.1, there exists a regular ultrafilter $\mathcal{D}$ of $\mathcal{G}(K_s/K)^e$ which contains $A(\sim \Theta)$, hence

$$\prod \tilde{K}(\underline{\sigma})/\mathcal{D} | = \sim \Theta. \quad \|$$

A field $K$ is said to be *hilbertian* if for every irreducible polynomial $f \in K[T, X]$ there exist infinitely many $t \in K$ such that $f(t, X)$ is irreducible in $K[X]$. We note that every finite algebraic extension of a hilbertian field is hilbertian. If $K_0$ is any field and $x$ is a transcendental element over $K$ then $K_0(x)$ is hilbertian. Moreover, $\mathbb{Q}$ is hilbertian (cf. Lang [10, Chap. VIII]).

**Lemma 7.2.** *Let $K$ be a hilbertian field. Then*

(a) *$\tilde{K}(\underline{\sigma})$ is an e-free field for almost all $(\underline{\sigma}) \in \mathcal{G}(K_s/K)^e$. If, in addition, $K$ is denumerable, then*

(b) *$\tilde{K}(\underline{\sigma})$ is an Ax field for almost all $(\underline{\sigma}) \in \mathcal{G}(K_s/K)^e$, and*

(c) *every regular ultraproduct of the $\tilde{K}(\underline{\sigma})$ is an e-free Ax field.*

*Proof.* Statement (a) is a part of Theorem 5.1 of [7]; statement (b) is Theorem 2.5 of [6]; statement (c) follows from (a) and (b) by Lemmas 1.4, 5.4 and Proposition 7.1. ‖

We are now in a position to prove

**Theorem 7.3.** *Let $K$ be a denumerable hilbertian field and let $\Theta$ be a $K$-elementary statement. Then the following two statements are equivalent:*

(a) $\tilde{K}(\underline{\sigma})|=\Theta$ *for almost all* $(\underline{\sigma})\in\mathscr{G}(K_s/K)^e$.

(b) $F|=\Theta$ *for every e-free Ax field $F$ which contains $K$.*

*Proof.* (b) $\Rightarrow$ (a) follows from Lemma 7.2.

(a) $\Rightarrow$ (b). Let $F$ be an $e$-free Ax field which contains $K$. Then one shows, as in the proof of Lemma 6.2(a), that $\tilde{K}\cap F$ is a perfect field of corank $\leqq e$. By Lemma 6.2(b), there exists a regular ultraproduct $E$ of the $\tilde{K}(\underline{\sigma})$ such that $\tilde{K}\cap E\cong_K\tilde{K}\cap F$. By Lemma 7.2 and Proposition 7.1, $E$ is an $e$-free Ax field and $E|=\Theta$. By Theorem 4.4 $E\equiv_K F$, hence $F|=\Theta$. ‖

Let $\mathscr{A}=\mathscr{A}_K$ be the boolean algebra of $\mathscr{G}(K_s/K)^e$ generated by all of the $A(f)$ for which $f$ is separable, and all of the zero sets. Clearly, $A(f)\in\mathscr{A}$ for all $f\in K[X]$.

**Theorem 7.4.** *Let $K$ be a denumerable hilbertian field and let $\Theta$ be a $K$-elementary statement. Then $A(\Theta)\in\mathscr{A}$.*

*Proof.* Assume that $A(\Theta)\notin\mathscr{A}$. Consider the boolean algebra $J$ of all subsets of $\mathscr{G}(K_s/K)^e$ modulo zero sets. Let $\bar{\mathscr{A}}$, $\overline{A(\Theta)}$ be the boolean subalgebra and the element of $J$ which correspond to $\mathscr{A}$ and $A(\Theta)$ respectively. Then $\overline{A(\Theta)}\notin\bar{\mathscr{A}}$, since $\mathscr{A}$ contains all the zero sets. By a proposition of Ax [6, p. 265], there exist two ultrafilters $D_1$, $D_2$ of $J$ such that $D_1\cap\bar{\mathscr{A}}=D_2\cap\bar{\mathscr{A}}$, $\overline{A(\Theta)}\in D_1$ and $\overline{A(\Theta)}\notin D_2$. Note that the ultrafilters of $J$ are in a bijective correspondence with the regular ultrafilters of $\mathscr{G}(K_s/K)^e$. It follows that there exist regular ultrafilters, $\mathscr{D}_1,\mathscr{D}_2$, of $\mathscr{G}(K_s/K)^e$ such that

$$\mathscr{D}_1\cap\mathscr{A}=\mathscr{D}_2\cap\mathscr{A},\quad A(\Theta)\in\mathscr{D}_1 \text{ and } A(\Theta)\notin\mathscr{D}_2. \tag{$*$}$$

Let $F_i=\prod\tilde{K}(\underline{\sigma})/\mathscr{D}_i$. Then, by Lemma 7.2, the $F_i$ are $e$-free Ax fields. Moreover, if $f\in K[X]$, then $f$ has a root in $F_1$ if and only if $f$ has a root in $F_2$, since $\mathscr{D}_1\cap\mathscr{A}=\mathscr{D}_2\cap\mathscr{A}$. It follows, by Ax [1, p. 172], that $\tilde{K}\cap F_1\cong_K\tilde{K}\cap F_2$. Hence, by Theorem 4.4, $F_1\equiv_K F_2$. This contradicts $(*)$. ‖

A $K$-elementary statement is said to be a *one-variable statement*, if it is equivalent to a sentence of the form

$$\Phi=\Phi([\exists X\, f_1(X)=0],\ldots,[\exists X\, f_m(X)=0]),$$

where $\Phi(Z_1,\ldots,Z_m)$ is a boolean polynomial in the variables $Z_1,\ldots,Z_m$; the union, intersection and the complement operations are to be interpreted as disjunction, conjunction and negation, respectively, and $f_1,\ldots,f_m$ are separable polynomials.

*Notation.* If $A,B$ are two subsets of $\mathscr{G}(K_s/K)^e$ which differ only by a zero set, then we write $A\approx B$.

**Theorem 7.5.** *Let $K$ be a denumerable hilbertian field and let $\Theta$ be a $K$-elementary statement. Then there exists a one-variable statement $\Phi$ such that*

(a) $A(\Theta)\approx A(\Phi)$.

(b) $\tilde{K}(\underline{\sigma})| = \Theta \leftrightarrow \Phi$ *for almost all* $(\underline{\sigma}) \in \mathcal{G}(K_s/K)^e$.

(c) $F| = \Theta \leftrightarrow \Phi$ *for every e-free Ax field* $F$ *which contains* $K$.

(d) $\mu(A(\Theta)) = \mu(A(\Phi))$ *is a rational number.*

*Proof.* Every element of $\mathscr{A}$ can be written in the form $A(\Phi) \cup \mathcal{O}$ where $\mathcal{O}$ is a zero set. Hence (a) is a corollary of Theorem 7.4.

Statement (b) follows from (a).

Statement (c) follows from (b) and Theorem 7.3.

To prove (d) we first show that $A(\Phi)$ is measurable and $\mu(A(\Phi))$ is a rational number, where $\Phi$ is as in (*). Indeed, let $L$ be the splitting field of the polynomial $f_1, \ldots, f_m$. Denote by $C$ the set of all $(\underline{\sigma}') \in \mathcal{G}(L/K)^e$ such that $L(\underline{\sigma}')| = \Phi$. It is clear that

$$A(\Phi) = \{(\underline{\sigma}) \in \mathcal{G}(K_s/K)^e \mid (\underline{\sigma}/L) \in C\}$$

(cf. [6, Lemma 3.11]). Hence, by formula (1) of Section 6,

$$\mu(A(\Phi)) = \frac{|C|}{[L:K]^e}.$$

The equality in (d) follows now from (a). ‖

We conclude this section by considering a change in the basis field. Let $K'$ be a regular extension of $K$. Denote by $\rho: \mathcal{G}(K_s'/K')^e \to \mathcal{G}(K_s/K)^e$ the epimorphism induced by restriction. Then $\tilde{K} \cap \tilde{K}'(\underline{\sigma}) = \tilde{K}(\rho(\underline{\sigma}))$ for every $(\underline{\sigma}) \in \mathcal{G}(K_s'/K')^e$. Denote by $\mu'$ the completion of the Haar measure of $\mathcal{G}(K_s'/K')^e$. Then $\rho$ is a measurable map, *i.e.* $\mu'(\rho^{-1} A) = \mu(A)$ for every measurable subset $A$ of $\mathcal{G}(K_s/K)^e$ (cf. Halmos [5, p. 279]).

**Theorem 7.6.** *Let* $K, K'$ *be denumerable hilbertian fields such that* $K'$ *is a regular extension of* $K$. *Then*

(a) $\tilde{K}'(\underline{\sigma}) \equiv_K \tilde{K}(\rho(\underline{\sigma}))$ *for almost all* $(\underline{\sigma}) \in \mathcal{G}(K_s'/K')^e$.

(b) $A_{K'}(\Theta) \approx \rho^{-1} A_K(\Theta)$ *for every* $K$*-elementary statement* $\Theta$.

(c) $\mu(A_K(\Theta)) = \mu'(A_{K'}(\Theta))$ *for every* $K$*-elementary statement* $\Theta$.

*Proof.* Denote by $S$ (resp. $S'$) the set of all $(\underline{\sigma}) \in \mathcal{G}(K_s/K)^e$ (resp. $\mathcal{G}(K_s'/K')^e$) such that $\tilde{K}(\underline{\sigma})$ (resp. $\tilde{K}'(\underline{\sigma})$) is an $e$-free Ax field. Then $\mu_K(S) = 1$ and $\mu_{K'}(S') = 1$, by Lemma 7.2. It follows that $\mu_{K'}(\rho^{-1}(S) \cap S') = 1$. By Theorem 4.4 $\tilde{K}'(\underline{\sigma}) \equiv_K \tilde{K}(\rho(\underline{\sigma}))$ for every $(\underline{\sigma}) \in \rho^{-1}(S) \cap S'$.

This completes the proof of statement (a).

Statement (b) follows from (a); (c) follows from (b). ‖

## 8. The Decision Procedure

In this section we restrict ourselves to the case where the ground field $K$ is either the field of the rational numbers $\mathbb{Q}$ or one of the fields $\mathbb{F}_p(t)$, where $\mathbb{F}_p$ is the field with $p$ elements and $t$ is transcendental over $\mathbb{F}_p$. In each of these cases, one is able to make an explicit list of the sentences of the language $\mathfrak{L}(K)$; from here on, $\mathfrak{L}(K)$ will be denoted by $\mathfrak{L}_p$, where $p = \mathrm{char}(K)$. For every $p$ we denote by $\mathfrak{T}_p$ the *theory* (*i.e.* the set) of all the sentences of $\mathfrak{L}_p$ that hold in every $e$-free Ax $K$-

field with characteristic $p$ or, equivalently, that hold in $\tilde{K}(\underline{\sigma})$ for almost all $(\underline{\sigma})\in\mathscr{G}(K_s/K)^e$, where $p=\mathrm{char}(K)$. Our aim is to give a scheme of instructions which will enable us to decide in a finite number of steps, whether or not a given sentence of $\mathfrak{L}_p$ belongs to $\mathfrak{T}_p$. In other words, we are going to give a *decision procedure* for $\mathfrak{T}_p$. In doing so we use the fact that every given polynomial $f\in K[X_1,\dots,X_n]$ can be effectively decomposed in a product of irreducible factors.

We follow Ax' decision procedure for the theory of finite fields (cf. [2, §§ 9, 11]) and begin with the procedure for one-variable statement. Let

$$\Phi=\Phi([\exists X\, f_1(X)=0],\dots,[\exists X\, f_m(X)=0]), \tag{1}$$

be a one-variable statement. Then one can effectively transfer it into one in which the $f_i$ are monic, are irreducible and have no common roots. Thus, let us suppose that we begin such a statement. The $f_i$ have the form

$$f_i(X)=X^{n_i}+c_{i1}X^{n_i-1}+\cdots+c_{in_i}$$

with given $c_{ij}$ in $K$. Let $a_{i1},\dots,a_{in_i}$ be $n_i$ symbols which stand for the roots of $f_i$; let $U_{i1},\dots,U_{in_i}$ be $n_i$ variables. Write $W=\sum_{i=1}^{m}(a_{i1}U_{i1}+\cdots+a_{in_i}U_{in_i})$ and let $g(\underline{a},\underline{U},Z)=\prod_{\pi\in S}(Z-\pi W)$, where $S$ is the cartesian product of the permutation groups $S(\underline{U}_i)$ and $\pi W=\sum_{i=1}^{n}(a_{i1}\pi U_{i1}+\cdots+a_{in_i}\pi U_{in_i})$. The coefficients of $g$ are symmetric polynomials in each of the sets of symbols $(\underline{a}_i)$ with integral coefficients (which are to be calculated modulo $p$). Therefore, we can effectively rewrite them as polynomials in the given $c_{ij}$. We do this, and rewrite $g$ in the form

$$g(\underline{a},\underline{U},Z)=\sum_{(\nu)}g_\nu(\underline{c})\,Z^{\nu_0}\prod_{i=1}^{m}U_{i1}^{\nu_{i1}}\dots U_{in_i}^{\nu_{in_i}}. \tag{2}$$

We denote the right hand side of (2) by $h(\underline{c},\underline{U},Z)$ and decompose it into a product of irreducible polynomials over $K$

$$h(\underline{c},\underline{U},Z)=h_1(\underline{U},Z)\dots h_r(\underline{U},Z).$$

Then we determine the subgroup $G$ of $S$ which fixes $h_1$. As in Section 5, one can prove that there exists a $\tau\in S$ such that $G$ is isomorphic to $\mathscr{G}(f_1\dots f_m,K)$ under the map $\pi\mapsto\pi'$, where $\pi'$ is defined by

$$\pi'(a_{ij})=a_{kl}\Leftrightarrow\pi(\tau U_{ij})=\tau U_{kl}.$$

It follows that if $L$ is the splitting field of $f_1\dots f_m$ over $K$, then an $e$-tuple $(\pi_1,\dots,\pi_e)\in G^e$ satisfies

$$\Phi\left(\bigvee_{j=1}^{n_1}\bigwedge_{k=1}^{e}\pi_k U_{1j}=U_{1j},\dots,\bigvee_{j=1}^{n_m}\bigwedge_{k=1}^{e}\pi_k U_{mj}=U_{mj}\right) \tag{3}$$

if and only if

$$L(\underline{\pi}')|=\Phi([\exists X\, f_1(X)=0],\dots,[\exists X\, f_m(X)=0]), \tag{4}$$

where $L(\underline{\pi}')$ is the fixed field of $(\underline{\pi}')$ in $L$.

We calculate the order of $G$ and the number $c$ of the $e$-tuples $(\underline{\pi}) \in G^e$ satisfying (3). Then, by an argument similar to that used in the proof of Theorem 7.5, we get $\mu(A(\Phi)) = \frac{c}{|G|^e}$.

We have therefore proved the following lemma:

**Lemma 8.1.** *Let $K$ be either $\mathbb{Q}$ or one of the $\mathbb{F}_p(t)$. Then for every given one-variable statement $\Phi$ we can effectively calculate $\mu(A(\Phi))$. It is a rational number.*

We come now to the main result of this work.

**Theorem 8.2.** *Let $K$ be either $\mathbb{Q}$ or one of the $\mathbb{F}_p(t)$. Then for every given $K$-elementary statement $\Theta$ we can find a one-variable statement $\Phi$ such that $A(\Theta) \approx A(\Phi)$ and we can compute $\mu(A(\Theta))$. In particular, we can decide in a finite number of steps whether or not $\Theta \in \mathfrak{T}_p$.*

*Proof.* By Lemma 1.4 and Lemma 5.4 we can explicitly write down a list of sentences $\Psi_1, \Psi_2, \Psi_3, \ldots$ in the language $\mathfrak{L}$ such that a $K$-field $F$ is an $e$-free Ax field if and only if $F \models \Psi_n$ for every $n \geqq 1$. Write $\mathfrak{W} = \{\Psi_1, \Psi_2, \Psi_3, \ldots\}$. Theorem 7.5 asserts that there exists a one-variable statement $\Phi'$ such that $\mathfrak{W} \models \Theta \leftrightarrow \Phi'$. By Gödels completeness theorem there exists a formal proof of $\Theta \leftrightarrow \Phi'$ from $\mathfrak{W}$ (cf. Bell and Slomson, [3, p. 234]). Thus we proceed as follows. We order the formal proofs from $\mathfrak{W}$ in a sequence and check them one by one. After a finite number of steps we must hit a proof of a sentence of the form $\Theta \leftrightarrow \Phi$, where $\Phi$ is a one-variable statement. Then $F \models \Theta \leftrightarrow \Phi$ for every $e$-free Ax $K$-field $F$, hence $A(\Theta) \approx A(\Phi)$, by Theorem 7.3. Thus by Lemma 8.1 we can compute $\mu(A(\Theta))$. $A(\Theta)$ belongs to $\mathfrak{T}_p$ if and only if $\mu(A(\Theta)) = 1$. ‖

*Remark.* Technically speaking, our proofs imply that the set of Gödel numbers of $\mathfrak{T}_p$ is recursive, whereas the set of Gödel numbers of the set of all one-variable statements is primitive recursive. The difference is that, given a one-variable statement $\Phi$ one can give in advance a bound for the number of steps necessary for computing $\mu(A(\Phi))$ and deciding whether or not $\Phi \in \mathfrak{T}_p$, whereas this is not possible with an arbitrary $K$-elementary statement $\Theta$. The only thing we know is that we have to proceed with a certain sequence of operations and calculations with $\Theta$ and that we are ensured that after a finite number of steps we will arrive at the desired conclusion. It would, therefore, be reasonable to look for another decision procedure which cures this defect.

## References


1. Ax, J.: Solving diophantine problems modulo every prime. Annals of Math. **85**, 161–183 (1967)
2. Ax, J.: The elementary theory of finite fields. Annals of Math. **88**, 239–271 (1968)
3. Bell, J. L., Slomson, A. B.: Models and ultraproducts. Amsterdam: North-Holland 1969
4. Gaschütz, W.: Zu einem von B. H. und H. Neumann gestellten Problem. Math. Nachrichten **14**, 249–252 (1956)
5. Halmos, P. R.: Measure theory. Princeton: Van Nostrand 1950
6. Jarden, M.: Elementary statements over large algebraic fields. Trans. of A.M.S. **164**, 67–91 (1972)
7. Jarden, M.: Algebraic extensions of hilbertian fields of finite corank. Israel J. of Math. **18**, 279–307 (1974)

8. Kreisel, G., Krivine, J. L.: Elements of mathematical logic. Amsterdam: North-Holland 1967
9. Lang, S.: Introduction to algebraic geometry. New York: Interscience Publishers 1958
10. Lang, S.: Diophantine geometry. New York: Interscience Publishers 1962
11. Mendelson, E.: Introduction to mathematical logic. Princeton: Van Nostrand 1964
12. Ribes, L.: Introduction to profinite groups and Galois cohomology. Queen papers in pure and applied Math. **24**, Kingston 1970
13. Van der Waerden, B. L.: Moderne Algebra I. Berlin-Heidelberg-New York: Springer 1940

Moshe Jarden
Department of Math. Sciences
Tel Aviv University
Ramat Aviv, Tel Aviv
Israel

Ursel Kiehne
Math. Institut der Univ. des Saarlandes
D-6600 Saarbrücken
Bau 27
Federal Republic of Germany

*Received April 10, 1975*