The Elementary Theory of ω-Free Ax Fields

Moshe Jarden

Tel Aviv University, Department of Mathematics, Ramat-Aviv, Tel-Aviv, Israel

Contents

Introduction

We consider the field $\mathbb{Q}$ of rational numbers, its algebraic closure $\tilde{\mathbb{Q}}$, and for every positive integer e, the cartesian power $G_e=\mathcal{G}(\tilde{\mathbb{Q}}/\mathbb{Q})^e$ of the Galois group of $\tilde{\mathbb{Q}}$ over $\mathbb{Q}$. If $(\underline{\sigma})=(\sigma_1,\ldots,\sigma_e)\in G_e$, then we denote by $\tilde{\mathbb{Q}}(\underline{\sigma})$ the fixed field of $(\sigma_1,\ldots,\sigma_e)$ in $\tilde{\mathbb{Q}}$. It was proved in [7] that for a fixed positive integer e, the theory $T_e(Q)$ of all elementary statements of field theory that are true in $\tilde{\mathbb{Q}}(\underline{\sigma})$ for almost all $\tilde{\mathbb{Q}}(\underline{\sigma})\in G_e$, is decidable. Here "almost all" is used in the sense of the Haar measure μ_e defined for G_e with respect to the Krull topology. One of the main steps in establishing the decision procedure was the reduction modulo $T_e(\mathbb{Q})$ of an arbitrary elementary statement Θ to a, so called, one variable statement. A *one variable statement* is a statement that is equivalent to a boolean combination (i.e. one that uses disjunction, conjunction and negation) of sentences of the form $(\exists X)\, f(x)=0$, where $f\in\mathbb{Q}[x]$. It was proved that for a given elementary statement Θ one can find, in a finite number of steps, a one variable statement Φ such that $\Theta\leftrightarrow\Phi$ is true in $\tilde{\mathbb{Q}}(\underline{\sigma})$ for almost all $(\underline{\sigma})\in G_e$. A natural question which arises is to what extent does Φ depend on e? In order to understand the situation consider a typical example in which Θ is the statement "There exists a Galois extension with H as α Galois group", where H is a given finite group. Let $e_0=\operatorname{rank} H$.

If $e<e_0$, then Θ is false for every $(\underline{\sigma})\in G_e$, since the rank of every Galois group over $\tilde{\mathbb{Q}}(\sigma_1, \ldots, \sigma_e)$ is not greater then e. However, if $e\geqq e_0$, then Θ is true in $\tilde{\mathbb{Q}}(\underline{\sigma})$, for almost all $(\underline{\sigma})\in G_e$, since for almost all $(\underline{\sigma})\in G_e$, every finite group of order e is realizable over $\mathbb{Q}(\underline{\sigma})$ (see [7, Lemma 7.2]). This means that in the case $e<e_0$, Φ can be chosen as "$(\exists X)1=0$" and in the case $e\geqq e$. Φ can be chosen as "$(\exists X)0=0$". For an arbitrary elementary statement Θ we prove the following Theorem.

If Θ is an elementary statement, then one can find, in a finite number of steps, a one variable statement Φ and a positive integer e_0 such that $\tilde{\mathbb{Q}}(\underline{\sigma})\models\Theta\leftrightarrow\Phi$ for every $e\geqq e_0$ and almost all $(\underline{\sigma})\in G_e$.

In establishing this Theorem we develop methods and prove results similar to those that appear in [7]. We consider the theory $T_\omega(\mathbb{Q})$ of all elementary statements Θ for which there exists an e_0 such that $\tilde{\mathbb{Q}}(\underline{\sigma})\models\Theta$ for every $e\geqq e_0$ and almost all $(\underline{\sigma})\in G_e$. We prove that a field F is a model of $T_\omega(\mathbb{Q})$ if and only if it satisfies the following conditions:

(a) $\mathrm{char}(F)=0$,

(b) every non-void absolutely irreducible variety defined over F has an F-rational point,

(c) every finite embedding problem over F is solvable.

We show that conditions (a), (b) and (c) can be reformulated as a sequence, $\Pi(\mathbb{Q})$, of sentences in the first order predicate calculus language of the theory of fields; $\Pi(Q)$ is therefore a set of axioms for the theory $T_\omega(\mathbb{Q})$. Then we establish a recursive decision procedure for $T_\omega(\mathbb{Q})$ based on the elementary statements to one variable statements that was described above.

As in [7] we also develop an appropriate measure theory. Let $G=\bigcup_{e=1}^{\infty} G_e$ be the disjoint union of all the measure spaces G_e. Every subset A of G can be uniquely represented as a disjoint union, $A=\bigcup_{e=1}^{\infty} A_e$, where $A_e=A\cap G_e$. Let

$$\mu(A)=\sum_{e=1}^{\infty}\mu_e(A_e).$$

Then μ is a measure of G which is invariant under the action of G_1. A subset of G is said to be a *big set*, if there exists an e_0 such that $\mu_e(A_e)=1$ for every $e\geqq e_0$. For an elementary statement Θ we denote

$$A_e(\Theta)=\{(\underline{\sigma})\in G_e|\tilde{\mathbb{Q}}(\underline{\sigma})\models\Theta\},$$

$$A(\Theta)=\bigcup_{e=1}^{\infty} A_e(\Theta)=\{(\underline{\sigma})\in G|\tilde{\mathbb{Q}}(\underline{\sigma})\models\Theta\}.$$

Then $A(\Theta)$ is a big set if and only if Θ belongs to $T_\omega(\tilde{\mathbb{Q}})$. We prove that in any case, either $\mu(A(\Theta))=\infty$ or $\mu(A(\Theta))$ is a rational number. Moreover, we give a recursive procedure to compute $\mu(A(\Theta))$.

The proofs of the various decision procedures rely on the following fundamental algebraic-model theoretic result which is the analogue to Theorem 4.4 of [7].

Let E, F be fields that satisfy conditions (a), (b) and (c) above. If $\tilde{\mathbb{Q}}\cap E\cong\tilde{\mathbb{Q}}\cap F$, then E is elementarily equivalent to F.

The crucial points in the proof of this theorem is Lemma 3.1 of [7] together with the following result on an ultrapower of a field:

Let E be a perfect field such that $\mathcal{G}(\tilde{E}/E)$ is a free pro-finite group on a set T. Let $\mathcal{D}$ be an ultrafilter of a set I and let ${}^*E = E^I/\mathcal{D}$, ${}^*T = T^I/\mathcal{D}$. Then there exists a Galois extension N of ${}^*E$ that contains $\tilde{E}$, such that $\mathcal{G}(N/{}^*E)$ is a free pro-finite group on a set of the same cardinality as ${}^*T$.

Finally we note that the decision procedures are actually proved for every given infinite field which is finitely generated over its prime field. All other results hold even under assumption that K is countable and Hilbertion.

1. Free Pro-Finite Groups

A subset S of a pro-finite group G is said to be a *set of generators* for G, if the closed subgroup generated by S coincides with G. Every map ϕ_0 of S into a pro-finite group H has at most one extension to a continuous homomorphism $\phi: G \to H$.

A subset S of a pro-finite group G is said to *converge* to 1, if every open normal subgroup of G contains all but a finite number of elements of S.

Suppose that G has a set of generators S that converges to 1. The *rank* of G is then the smallest cardinality of such an S.

The condition rank $(G) \leqq \aleph_0$ is equivalent to the condition that G contains a decreasing sequence $G \supset G_1 \supset G_2 \supset \cdots$ of open normal subgroups that constitutes a basis for the neighbourhoods of 1 (see Ribes [10, p. 84]). Such a basis satisfies $\bigcap_{i=1}^{\infty} G_i = 1$.

Let S be an infinite set of generators of G that converges to 1, let $H = \{1, -1\}$ be the multiplicative group of two elements and let $\phi: G \to H$ be a continuous homomorphism. Then all but a finite number of elements of S are mapped to 1, by ϕ. Hence ϕ is fully characterized by that finite subset of S which is mapped onto -1. It follows that there exist at most $|S|$ continuous homomorphisms of G into H. Here $|S|$ means the cardinality of S.

A *free pro-finite group* is a couple (F, X), where F is a pro-finite group and X is a set of generators of F that converges to 1, such that every map ϕ_0 of X into a pro-finite group G for which $\phi_0(X)$ converges to 1 can be extended to a continuous homomorphism $\phi: F \to G$. X is said to be a *free set of generators for* F. We also say that F is a free pro-finite group *on* X.

Note that our definition of a free pro-finite group is essentially that of Ribes (cf. [10, p. 61]).

If F is free on an infinite set X, then every map ϕ_0 of X into $H = \{1, -1\}$ that maps all but a finite number of elements of X onto 1 can be extended to a continuous homomorphism of X into H. This implies that there are exactly $|X|$ continuous homomorphisms of F into H. Hence F can not be generated by a set S that converges to 1 and has a smaller cardinality than $|X|$. It follows that rank $(F) = |X|$. This conclusion holds also in the case where X is finite, as follows easily from Proposition 7.6 on page 68 of [10].

For each cardinal number α there exists exactly one (up to an isomorphism) free pro-finite group F of rank α (see [10, p. 61]). We follow our notation in [5] and denote by $\hat{F}_e$ the pro-finite free group on e generators. $\hat{F}_\omega$ will denote the pro-finite group of rank $\aleph_0$.

An embedding problem for pro finite group F is a diagram

$$\begin{array}{ccc} & & F \\ & & \downarrow \phi \\ G & \xrightarrow{\theta} & H \end{array}$$

where G, H are pro-finite groups and ϕ, θ are continuous epimorphisms. The *rank* of the embedding problem is defined to be the rank of G. The embedding problem is said to be *finite*, if G is finite. We say that the embedding problem is *solvable*, if there exists a continuous epimorphism $\psi: F \to G$ such that $\theta \circ \psi = \phi$.

For free pro-finite groups there is a large variety of embedding problems that can be solved. We start with $\hat{F}_e$.

(1.1) **Lemma.** *Every embedding problem of the form*

$$\begin{array}{ccc} & & \hat{F}_e \\ & & \downarrow \phi \\ G & \xrightarrow{\theta} & H \end{array}$$

in which G is generated by e elements is solvable.

Proof. Let $\{x_1, \ldots, x_e\}$ be a system of free generators for $\hat{F}_e$. Write $a_i = \phi(x_i)$, $i = 1, \ldots, e$. Then $a_1, \ldots, a_e$ generate H, since ϕ is surjective. By a consequence of a theorem of Gaschütz there exist $b_1, \ldots, b_e$ that generate G such that $\theta(b_i) = a_i$ for $i = 1, \ldots, e$ (see [7, Lemma 4.2]). The map $x_i \to b_i$, $i = 1, \ldots, e$ can therefore be extended to an epimorphism ψ of $\hat{F}_e$ onto G such that $\phi = \theta \circ \psi$. //

The free pro-finite group on a denumerable number of generators, $\hat{F}_\omega$ was characterized by Iwasawa, via embedding problems, as follows:

(1.2) **Lemma.** *Let F be a pro-finite group of rank $\leqq \aleph_0$. Then F is isomorphic to $\hat{F}_\omega$ if and only if every finite embedding problem for F is solvable.*

Proof. See Ribes [10, p. 84].

Problem. Is it true that every embedding problem for $\hat{F}_\omega$ of a countable rank is solvable?

The method of proof of Iwasawa's Theorem can be applied to free pro-finite groups on non-countable sets.

(1.3) **Lemma.** *Let F be a free pro-finite group on a non-countable set X. Then every embedding problem*

$$\begin{array}{ccc} & & F \\ & & \downarrow \phi \\ G & \xrightarrow{\theta} & H \end{array}$$

in which rank $(G) \leqq \aleph_0$ is solvable.

Proof. Let $N = \operatorname{Ker}\phi$. Then rank $F/N = \operatorname{rank} H \leqq \operatorname{rank} G \leqq \aleph_0$, hence there exists a decreasing sequence $F \supseteq F_1 \supseteq F_2 \supseteq \cdots \supseteq N$ of open normal subgroups such that $\bigcap_{i=1}^{\infty} F_i = N$. Each one of the sets $X \cap (F - F_i)$ is finite (since X converges to 1), hence $X_0 = X \cap (F - N) = \bigcup_{i=1}^{\infty} X \cap (F - F_i)$ is at most countable and it converges to 1. We order X_0 in a sequence $X_0 = \{x_1, x_2, x_3, \ldots\}$ and let $a_i = \phi(x_i)$ for $i = 1, 2, 3, \ldots$. Then $\{a_1, a_2, a_3, \ldots\}$ is a set of generators for H which converges to 1, since ϕ is continuous. Also, there exists a decreasing sequence $G \supseteq G_1 \supseteq G_2 \supseteq \cdots$ of open normal subgroups in G that constitutes a basis for the neighbourhoods of 1. Let $H_i = \theta G_i$ for $i = 1, 2, 3, \ldots$. Then each H_i is open and normal in H (by compactness), $H \supseteq H_1 \supseteq H_2 \supseteq \cdots$, and the H_i constitute a basis for the neighbourhoods of 1 in H. It follows that for every i there exists an n_i such that $a_n \in H_i$ for every $n > n_i$. We can therefore choose $b_1, b_2, b_3, \ldots$ in G such that $\theta b_n = a_n$ and $b_n \in G_i$ for every i and every $n > n_i$. In particular we have that the sequence $\{b_1, b_2, b_3, \ldots\}$ converges to 1.

Let now $J = \operatorname{Ker}\theta$. Then the $J \cap G_i$ are open and normal in J and they constitute a basis for the neighbourhoods of 1 in J. It follows that there exists a sequence $b_1', b_2', b_3', \ldots$ of generators of J that converges to 1.

The assumption that X is non-countable implies that $X - X_0$ contains an infinite sequence $X_1 = \{x_1', x_2', x_3', \ldots\}$. The map

$$\begin{aligned} x_i &\mapsto b_i \quad \text{for } i = 1, 2, 3, \ldots, \\ x_i' &\mapsto b_i' \quad \text{for } i = 1, 2, 3, \ldots, \\ x &\mapsto 1 \quad \text{for } x \in X - (X_0 \cup X_1) \end{aligned}$$

can now be extended to a continuous epimorphism ψ of F onto G (since $\{b_1, b_2, \ldots, b_1', b_2', \ldots,\}$ converges to 1 and generates G) and we have $\theta \circ \psi = \phi$. //

2. Free Pro-Finite Groups as Galois Groups

Let L be a perfect field and let $\tilde{L}$ be its algebraic closure. Suppose that $\mathcal{G}(\tilde{L}/L)$ is a free pro-finite group. Let $\mathcal{D}$ be a non-principle ultra-filter of a denumerable set I. Write ${}^*L = L^I/\mathcal{D}$. If $\mathcal{G}(\tilde{L}/L)$ is of a finite rank, then $\mathcal{G}(\widetilde{{}^*L}/{}^*L)$ can shown to be isomorphic to $\mathcal{G}(\tilde{L}/L)$; in particular $\mathcal{G}(\widetilde{{}^*L}/{}^*L)$ is free. We do not know whether or not $\mathcal{G}(\widetilde{{}^*L}/L)$ remains free when $\mathcal{G}(\tilde{L}/L)$ is of an infinite rank. Fortunately, for our purposes it suffices to prove a weaker theorem, namely that there exists a

Galois extension N of $^*L$ that contains $\tilde{L}$ such that $\mathcal{G}(N/^*L)$ is free. This is what we are going to do in this section. Furthermore we prove that, if rank $\mathcal{G}(\tilde{L}/L)=\aleph_0$, then rank $\mathcal{G}(N/^*L)=2^{\aleph_0}$. Thus we shall be in a position to apply the strong embedding property of free pro-finite groups of a non-countable rank which was proved in Lemma 1.3.

Let M be a Galois extension of a field L and let N be an extension of M. If S is a set of automorphisms of N over L, then by $M(S)$ we denote the fixed field of S in M, i.e. $M(S)=\{x\in M|\sigma x=x \text{ for every } \sigma\in S\}$.

(2.1) **Lemma.** *Let L' be a Galois extension of a field L such that $\mathcal{G}(L'/L)$ is a free pro-finite group on a set T. Let S be a subset of T and denote by N the maximal Galois extension of L which is contained in $L'(-S)$. Then $\mathcal{G}(N/L)$ is a free pro-finite group on $S|N$ and the restriction map $S\mapsto S|N$ is bijective.*

Proof. $\mathcal{G}(L'/N)$ is the smallest normal closed subgroup of $\mathcal{G}(L'/L)$ that contains $T-S$. The restriction map $\mathcal{G}(L'/L)\to\mathcal{G}(N/L)$ maps S onto $S|N$ and $T-S$ onto 1. $\mathcal{G}(L'/N)$ is its kernel. Our Lemma follows now from Ribes [10, p. 66]. //

(2.2) **Lemma.** *Let L be a field and let I be a set. Let m be a positive integer and suppose that for every $i\in I$ we have a Galois extension N_i of L such that $\mathcal{G}(N_i/L)$ is the free pro-finite group on a set S_i of m elements. Let $\mathcal{D}$ be an ultra-filter of I. Write $^*L=L'/\mathcal{D}$, $N'=\prod N_i/\mathcal{D}$, $N=^*\tilde{L}\cap N'$ and $S=\prod S_i/D$. Then N is a Galois extension of $^*L$, $S|N$ is a set of m elements and $G(N/^*L)$ is the free pro-finite group on $S|N$.*

Proof. Let H be a finite group generated by m elements. Then for every $i\in I$ there exists a Galois extension M_i that is contained in N_i such that $\mathcal{G}(M_i/L)\cong H$. Then $M=\prod M_i/\mathcal{D}$ is a Galois extension of $^*L$ contained in N', hence in N and we have $\mathcal{G}(M/^*L)=\prod\mathcal{G}(M_i/L)/\mathcal{D}\cong H$.

Conversely, let M be a finite Galois extension of $^*L$ contained in N. Then one can write M in the form $M=\prod M_i/\mathcal{D}$ where M_i is a finite Galois extension of L of degree $[M:{}^*L]$ for almost all $i\in I$ (modulo $\mathcal{D}$). The group $\mathcal{G}(M_i/L)$ is generated by S/M_i, whence S/M generates $\mathcal{G}(M/^*L)$.

It follows that $\mathcal{G}(N/^*L)$ is generated by $S|N$, which is a set of not more than m elements, since S clearly contains exactly m elements. Furthermore, every finite group of rank $\leqq m$ is an epimorphic image of $\mathcal{G}(N/^*L)$. By [5, Thm. 2.4] $\mathcal{G}(N/^*L)\cong\hat{F}_m$. This also implies that $S|N$ contains exactly m elements (see Ribes [10, p. 68]). //

(2.3) **Lemma.** *Let L be a perfect field and suppose that $\mathcal{G}(\tilde{L}/L)$ is a free pro-finite group on a set T. Let $\mathcal{D}$ be an ultrafilter of a set I and let $^*L=L'/\mathcal{D}$, $^*T=T^I/\mathcal{D}$. Then there exists a Galois extension N of $^*L$ that contains L such that $\mathcal{G}(N/^*L)$ is a free pro-finite group of rank $|^*T|$.*

Proof. Let $^*\tilde{L}=\tilde{L}'/\mathcal{D}$ and embed $^*T$ in the obvious way in $\mathrm{Aut}(^*\tilde{L}/^*L)$. Let $S=\{\sigma_1,\ldots,\sigma_m\}$ be a finite subset of $^*T$. Every σ_j can be represented modulo $\mathcal{D}$ by a set $\{\sigma_{ji}|i\in I\}$ where $\sigma_{ji}\in T$. For every $i\in I$ let $S_i=\{\sigma_{1i},\ldots,\sigma_{mi}\}$. Then for almost all $i\in I$ (modulo $\mathcal{D}$), S_i contains exactly m elements and we have $S=\prod S_i/\mathcal{D}$.

Assertion. $^*\tilde{L}(^*T-S)=\prod\tilde{L}(T-S_i)/\mathcal{D}$. Let $x=\{x_i|i\in I\}_{\mathcal{D}}$ be an element of $^*\tilde{L}$. Suppose that $x\in\prod\tilde{L}(T-S_i)/\mathcal{D}$. Then $\{i\in I|x_i\in\tilde{L}(T-S_i)\}\in\mathcal{D}$. Let $\tau=\{\tau_i|i\in I\}_{\mathcal{D}}$ be

an element of $^*T-S$. Then $\{i\in I|\tau_i\in T-S\}\in\mathscr{D}$. Hence $\{i\in I|\tau_i x_i=x_i\}\in\mathscr{D}$, hence $\tau x=x$. It follows that $x\in{}^*\tilde{L}(^*T-S)$.

Suppose now that $x\notin\prod\tilde{L}(T-S_i)/\mathscr{D}$. Then

$$J=\{i\in I|x_i\notin\tilde{L}(T-S_i)\}\in\mathscr{D}.$$

For every $i\in j$ there exists a $\tau_i\in T-S_i$ such that $\tau x_i\neq x_i$. Let $\tau=\{\tau_i|i\in I\}_{\mathscr{D}}$. Then $\tau\in{}^*T-S$ and $\tau x\neq x$, hence $x\notin{}^*\tilde{L}(^*T-S)$.

For every $i\in I$ let N_i be the maximal Galois extension of L which is contained in $\tilde{L}(T-S_i)$. By Lemma 2.1, $S_i|N_i$ is a set of m elements on which $\mathscr{G}(N_i/L)$ is free. Hence, if we let $N_S={}^*\tilde{L}\cap\prod N_i/\mathscr{D}$, then we have, by Lemma 2.2, that N_S is a Galois extension of $^*L$, $S|N_S$ is a set of m elements and $\mathscr{G}(N_S/{}^*L)$ is a free pro-finite group on $S|N_S$.

Certainly N_S is contained in ${}^*\tilde{L}(^*T-S)$. Furthermore, N_S is the maximal Galois extension of $^*L$ having this property. Indeed, let $M={}^*L(x)$ be a finite Galois extension of $^*L$ which is contained in ${}^*L(^*T-S)$ and let $x=x_1,\ldots,x_n$ be all the conjugates of x over $^*L$. Present x_ν in the form $x_\nu=\{x_{\nu i}|i\in I\}_{\mathscr{D}}$, $\nu=1,\ldots,n$. Then, for almost all $i\in I\,\{x_{1i},\ldots,x_{ni}\}$ is contained in $\tilde{L}(T-S_i)$ and consists of a complete set of conjugates over L. Hence $\{x_{1i},\ldots,x_{ni}\}\subseteq N_i$. It follows that $x\in N_S$ and hence $M\subseteq N_S$.

If S' is a finite subset of $^*T$ that contains S, then $N_S\subseteq N_{S'}$ and the restriction map $\mathscr{G}(N_{S'}/{}^*L)\to\mathscr{G}(N_S/{}^*L)$ is obtained by mapping the elements of $(S'-S)|N_{S'}$ onto 1 and the elements of $S|N_{S'}$ onto $S|N_S$ respectively.

Let N be the Galois extension of $^*L$ generated by all the N_S's. Then $\mathscr{G}(N/{}^*L)$ is a free pro-finite group on $^*T/N$ (see Ribes [10, p. 67]). Furthermore, the map $^*T\to{}^*T|N$ is bijective. Indeed, if τ_1,τ_2 are two distinct elements of $^*T$ and $S=\{\tau_1,\tau_2\}$, then $\tau_1|N_S\neq\tau_2|N_S$, hence $\tau_1|N\neq\tau_2|N$. It follows that the cardinality of $^*T|N$ is equal to that of $^*T$.

Finally we prove that $\tilde{L}\subseteq N$. Let $L(x)$ be a finite Galois extension of L. Then there exists a finite subset S of T such that $\tau x=x$ for every $\tau\in T-S$, since T converges to 1. If we identify T with its image in $^*T$ by the natural embedding, then it follows that $\tau x=x$ for every $\tau\in{}^*T-S$, hence $x\in{}^*\tilde{L}(^*T-S)$. Moreover, $^*L(x)$ is a Galois extension of $^*L$, hence $x\in N_S$, hence $x\in N$. //

3. ω-Free Ax Fields

An embedding problem over a field L is a diagram of the form

$$\begin{array}{ccc} & & \mathscr{G}(M/L) \\ & & \big\downarrow\phi \\ G & \xrightarrow{\theta} & H \end{array} \tag{1}$$

in which M is a Galois extension of L, G and H are pro-finite groups, θ is a continuous epimorphism and ϕ is a continuous isomorphism. The problem is said to be *finite, of rank* α, if G is finite, of rank α, respectively. The problem is said to be *solvable* (res. *solvable in a given extension* L' *of* L), if there exists a Galois extension

N of L that contains M (res. and is contained in L') and there exists a continuous isomorphism ψ of $\mathcal{G}(N/L)$ onto G such that the diagram is commutative:

$$\begin{array}{ccc} \mathcal{G}(N/L) & \longrightarrow & \mathcal{G}(M/L) \\ \downarrow{\scriptstyle \psi} & & \downarrow{\scriptstyle \phi} \\ G & \xrightarrow{\theta} & H \end{array} \tag{2}$$

where the upper arrow is the natural restriction map.

It is not difficult to see that for a given G, H and θ, every embedding problem of the form (1) is solvable if and only if every embedding problem for $\mathcal{G}(L_s/L)$ (L_s is the separable closure of L) of the form

$$\begin{array}{ccc} & & \mathcal{G}(L_s/L) \\ & & \downarrow{\scriptstyle \lambda} \\ G & \xrightarrow{\theta} & H \end{array}$$

is solvable.

A field L is said to be *ω-free* if every finite embedding problem over L is solvable. This is equivalent to saying that every finite embedding problem for $\mathcal{G}(L_s/L)$ is solvable, if we assume further that rank $\mathcal{G}(L_s/L) \leqq \aleph_0$, then $\mathcal{G}(L_s/L) \cong \hat{F}_\omega$, by Lemma 1.2. The condition rank $\mathcal{G}(L_s/L) \leqq \aleph_0$ is always satisfied, if L is countable, since in this case $\mathcal{G}(L_s/L)$ has a countable basis for its topology. We formulate this results as a Lemma.

(3.1) **Lemma.** *If L is a countable ω-free field, then $\mathcal{G}(L_s/L) \cong \hat{F}_\omega$.*

Note that the concept of an ω-free field is not the proper analogue to the concept of an e-free field which was defined in [7, Section 4] for every positive integer e. We recall that a field L is said to be an e-free field if $\mathcal{G}(L_s/L) \cong \hat{F}_e$. This condition is preserved by ultra-product, whereas the condition $\mathcal{G}(L_s/L) \cong \hat{F}_\omega$ is not. Since the use of ultra-products is essential in our method we had to abandon the rank condition and remain only with the finite embedding problem condition.

We recall that for every positive integer e there exist e-free Ax subfields of $\tilde{\mathbb{Q}}$. Indeed, the $\tilde{\mathbb{Q}}(\underline{\sigma})$'s are e-free Ax fields for almost all $(\underline{\sigma}) \in \mathcal{G}(\tilde{\mathbb{Q}}/\mathbb{Q})^e$ (see [7, Lemma 7.2]). We therefore pose the following

Problem. Does there exist an ω-free Ax subfield of $\tilde{\mathbb{Q}}$?

We proceed now to express the concept of an ω-free field by a sequence of sentences in the first order predicate calculus language $\mathfrak{L}$ of the theory of fields. In order to do it we add to $\mathfrak{L}$ a one variable predicate symbol P and denote the new language by $(\mathfrak{L}, P)$. Models for this language are to be denoted by (L', L), where L' is the domain of the nodel and L is the subset of L' that corresponds to P.

(3.2) **Lemma.** *For a given epimorphism $\theta\colon G \to H$ of finite groups we can write a sentence $\Delta'(\theta, G, H)$ in $(\mathfrak{L}, P)$ such that for every pair of fields $L' \supseteq L$ we have:*

$$(L', L) \models \Delta'(\sigma, G, H)$$

if and only every embedding problem of the form (1) *is solvable in L'.*

Proof. Let $H=\{1=\pi_1, \pi_2, \ldots, \pi_m\}$, $G=\{1=\tau_1, \tau_2, \ldots, \tau_m\}$ and let $(\underline{\alpha})=(\alpha_1, \ldots, \alpha_m)$, $(\underline{\beta})=(\beta_2, \ldots, \beta_n)$ be two sets of symbols. We let H and G operate on $(\underline{\alpha})$ and $(\underline{\beta})$ respectively by

$$\pi_i \alpha_j=\alpha_k \Leftrightarrow \pi_i \pi_j=\pi_k \quad \text{for } i,j,k=1,\ldots,m,$$
$$\tau_i \beta_j=\beta_k \Leftrightarrow \tau_i \tau_j=\tau_k \quad \text{for } i,j,k=1,\ldots,n.$$

Thus we have embedded H and G in the symmetric groups $S(\underline{\alpha})$ and $S(\underline{\beta})$ of all permutations of $(\underline{\alpha})$ and $(\underline{\beta})$, respectively. One can now write down a sentence $\Delta'(\sigma, G, H)$ in $(\mathfrak{L}, P)$ which is equivalent to the following statement:

For every $a_1, \ldots, a_m \in L$ and $\alpha_1, \ldots, \alpha_m \in L'$ that satisfy:

(a) $f(X)=X^m+a_1 X^{m-1}+\cdots+a_m$ is irreducible over L;

(b) $\alpha_i \neq \alpha_j$ for $i,j=1,\ldots,m$;

(c) $f(X)=(X-\alpha_1)\ldots(X-\alpha_m)$;

(d) there exist polynomials $p_i \in L[X]$ of degree $\leqq m-1$ such that $\alpha_i=p_j(\alpha_1)$ for $j=1,\ldots,m$ and

(e) $\pi_i \alpha_i=p_j(\pi_i \alpha_1)$ for $i,j=1,\ldots,m$ and

(f) $\pi \alpha_i \neq p_j(\pi \alpha_1)$ for $j=1,\ldots,m$ and all $\pi \in S(\underline{\alpha})-H$,

there exist $b_1, \ldots, b_n \in L$ and $\beta_1, \ldots, \beta_n \in L'$ that satisfy

(g) $g(X)=X^n+b_1 X^{n-1}+\cdots+b_n$ is irreducible over L,

(h) $\beta_i \neq \beta_j$ for $i,j=1,\ldots,n$;

(i) $g(X)=(X-\beta_1)\ldots(X-\beta_n)$;

(j) there exist polynomials $q_i \in L[X]$ of degree $\leqq n-1$ such that $\beta_j=q_j(\beta_1)$ for $j=1,\ldots,n$ and

(k) $\tau_i \beta_j=q_j(\tau_i \beta_1)$ for $i,j=1,\ldots,n$ and

(l) $\tau \beta_j \neq q_j(\tau \beta_1)$ for $i=1,\ldots,n$ and $\tau \in S(\underline{\beta})-G$;

(m) there exist $h_i \in L[X]$ of degree $\leqq n-1$ such that $\alpha_j=h_j(\beta_1)$ and $\theta(\tau_i)\alpha_i=h_j(\tau_i \beta_1)$ for $j=1,\ldots,m$ and $i=1,\ldots,n$.

Suppose therefore that $(L', L) \models \Delta'(\theta, G, H)$ and consider the embedding problem (1). Let α_1' be an element of M for which $M=L(\alpha_1')$. Let $f(X)=X^m+a_1' X^{m-1}+\cdots+a_m'$ be an irreducible polynomial over L such that $f(\alpha_1')=0$. If we denote

$$\alpha_j'=\phi^{-1}(\pi_j)\alpha_1' \quad \text{for } j=1,\ldots,m,$$

then ϕ is an isomorphism of permutation groups and we can identify a_j, α_j and $\phi^{-1}(\pi_j)$ with a_j', α_j' and π_j, respectively, for $j=1,\ldots,m$. Then $a_1, \ldots, a_m, \alpha_1, \ldots, \alpha_m$ satisfy (a)–(f). In particular (e) and (f) are satisfied, since an element $\pi \in S(\underline{\alpha})$ belongs to H if and only $\pi \alpha_j=p_j(\pi \alpha_1)$ for $j=1,\ldots,m$. It follows that there exist $b_1, \ldots, b_n \in L$ and $\beta_1, \ldots, \beta_n \in L'$ that satisfy (g)–(m). If we let $N=L(\beta_1)$ and define $\psi: \mathfrak{G}(N/L) \to G$ appropriately we obtain a solution to the embedding problem (1) in L.

A similar argument shows that if for the given θ, G, H every embedding problem (1) is solvable in L', then $(L', L) \models \Delta'(\theta, G, H)$. //

By Theorem 2 of [6] one can find, in a finite number of steps, a sentence $\Delta(\theta, G, H)$ in the language $\mathfrak{L}$ such that for every field L and every infinite algebra-

ically closed extension L' of L.

$$(L', L) \models \Delta'(\theta, G, H) \Leftrightarrow L \models \Delta(\theta, G, H).$$

Denote by Π_1 the set of all sentences of the form $\Delta(\theta, G, H)$, and the sentence in $\mathfrak{L}$ that asserts that there exists an irreducible polynomial of degree 3 over the field L in question (if this sentence is valid, then, by Artin-Schreier Theorem, $[\tilde{L}: L] = \infty$). Clearly Π_1 is countable and it follows from Lemma 3.2 that a field L is ω-free if and only if $L \models \Pi_1$.

We recall that a field L is said to be an Ax *field* if it is perfect and if every absolutely irreducible variety defined over L has an L-rational point. The condition that L is perfect is clearly equivalent to the conditions: The derivatives of all irreducible polynomials $f \in L[X]$ of degree n are not zero, for $n = 1, 2, 3, \ldots$. These conditions can be explicitely written down as sentences in $\mathfrak{L}$. Thus it follows from [7, Section 1], that there exists a sequence Π_2 of sentences in $\mathfrak{L}$, which one can explicitely write down, such that L is an Ax field if and only if $L \models \Pi_2$.

We consider now a field K and extend the language $\mathfrak{L}$ to a language $\mathfrak{L}(K)$ by adding new constants, one for every element of K. We take as models of $\mathfrak{L}(K)$ only fields L that contain K and then we interpret the new constants as the corresponding elements of K. These fields are called *K-fields*. A mathematical statement on K-fields is said to be *K-elementary*, if it is equivalent to a sentence of $\mathfrak{L}(K)$. Two K-fields L_1, L_2 are said to be *K-equivalent*, if $L_1 \models \Theta \Leftrightarrow L_2 \models \Theta$, for every K-elementary statement Θ; we denote this by $L_1 \equiv_K L_2$.

Let Π_0 be a set of axioms in $\mathfrak{L}$ for the theory of fields and let $\Pi_3(K)$ be the *diagram* of K, i.e. the set of all sentences of the form.

$$a+b=c, \quad ab=c, \quad a, b, c \in K,$$
$$a'+b' \neq c', \quad a'b' \neq c', \quad a', b', c' \in K,$$

that are valid in K. Then $\Pi_0 \cup \Pi_3(K)$ is a set of axioms for the theory of K-fields. This is not an explicit set of axioms, unless K is "explicitly given". We shall define this concept later on.

We sum up this section with the following Lemma:

(3.3) **Lemma.** *A model L of $\mathfrak{L}(K)$ is an ω-free Ax K-field if and only if $L \models \Pi(K)$. Here $\Pi(K) = \Pi_0 \cup \Pi_1 \cup \Pi_2 \cup \Pi_3(K)$, where Π_0, Π_1, Π_2 are explicitly given sequences of sentences in $\mathfrak{L}$ and $\Pi_3(K)$ is the diagram of K.*

4. The Elementary Equivalence Theorem

We prove in the section the fundamental result about ω-free Ax K-fields, namely that an ω-free Ax K-field F is characterized by its K-algebraic part, $\tilde{K} \cap F$, up to a K-elementary equivalence.

We recall that a commutative algebra A over a field F is said to be *absolutely entire*, if $\tilde{F} \otimes_F A$ is an integral domain. A perfect field F is *hyper-Ax* if for every countably generated absolutely entire F-algebra A there exists an F-algebra homomorphism of A into F. Every hyper-Ax field is an Ax field. Conversely, every non-principal ultra-power of an Ax field with a countable exponent is a hyper-Ax field (see, [7, Thm. 1.5]).

(4.1) **Lemma.** *Let F be an ω-free Ax K-field and let F' be a countable K-elementary subfield of F. Then there exists an ω-free hyper-Ax K-field F_1 such that:* (a) *F_1 is an elementary extension of F,* (b) *F_1 has a Galois extension P_1 that contains F such that $\mathcal{G}(P_1/F_1)$ is a free pro-finite group of non-countable rank.*

Proof. By a lemma of Scott there exists an ultra-filter $\mathcal{D}_1$ of a set I_1 such that $F_1'=F'^{I_1}/\mathcal{D}_1$ is an elementary extension of F (see Bell and Slomson [3, p. 163]). By Lemma 3.3 F_1' is an ω-free K field, by [7, Thm. 1.5], F_1 is an hyper-Ax field and by [3, p. 92], F_1 is an elementary extension of F_1', hence also of F. The cardinality of F' is $\aleph_0$, hence, by [3, p. 116, Lemma 1.16 and p. 132, Thm. 3.21]

$$|F_1|=|F_1'|^{\aleph_0}\geqq\aleph_0^{\aleph_0}=2^{\aleph_0}. \tag{$*$}$$

As every ultra-power of an ultra-power, F_1 can be expressed in the form $F_1=F'^I/\mathcal{D}$, where $\mathcal{D}$ is an ultra-filter of a set I (see [3, p. 125]). Again, by Lemma 3.3, F' is a ω-free and perfect, hence, by Lemma 3.1 $\mathcal{G}(\tilde{F}'/F')$ is a free pro-finite group on a set T of cardinality $\aleph_0$. By [3, p. 125] and by ($*$), $|T^I/\mathcal{D}|=|F_1'^I/\mathcal{D}|\geqq 2^{\aleph_0}$, hence, by Lemma 2.3, there exist a Galois extension P_1 of F_1 that contains $\tilde{F}'$ such that $\mathcal{G}(P_1/F_1)$ is a free pro-finite group on a set of cardinality $|T^I/\mathcal{D}|$, i.e. on a non-countable set. //

(4.2) **Theorem.** *If E and F are two ω-free Ax K-fields such that $\tilde{K}\cap E\cong_K\tilde{K}\cap F$, then $E\equiv_K F$.*

Proof. Assume first that $|K|\leqq\aleph_0$. Let $L=\tilde{K}\cap E$ and $M=\tilde{K}\cap F$, then there exists an automorphism ϕ_0 of $\tilde{K}$ over K such that $\phi_0(L)=M$. Let Φ_0 be the isomorphism of $\mathcal{G}(\tilde{M}/M)$ onto $\mathcal{G}(\tilde{L}/L)$ induced by ϕ_0.

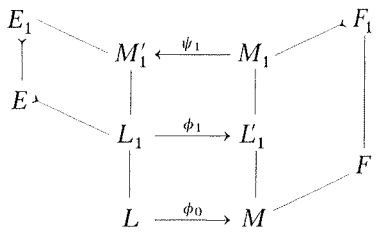
By Skolem-Löwenheim Theorem there exist countable elementary subfields L_1 of E and F' of F that contain L and M respectively (see [3, p. 80]). Let F_1 and P_1 be as in Lemma 4.1. The rank of $\mathcal{G}(\tilde{L}_1/L_1)$ is $\leqq\aleph_0$, hence, by Lemma 1.3, there exists a continuous epimorphism Φ_1' such that the following diagram is commutative,

$$\begin{array}{ccc} & & \mathcal{G}(\tilde{F}_1/F_1) \\ & \overset{\phi_1}{\swarrow} & \downarrow r \\ \mathcal{G}(\tilde{L}_1/L_1) & \xleftarrow{\Phi_1'} & \mathcal{G}(P_1/F_1) \\ \downarrow & & \downarrow \\ \mathcal{G}(\tilde{L}/L) & \xleftarrow{\Phi_0} & \mathcal{G}(\tilde{M}/M) \end{array}$$

here r is the restriction map. Then $\phi_1=r\circ\Phi_1'$ is a continuous epimorphism of $\mathcal{G}(\tilde{F}_1/F_1)$ onto $\mathcal{G}(\tilde{L}_1/L_1)$. L is algebraically closed in L_1, since L is algebraically closed in E, hence, by [7, Lemma 2.1], there exists a monomorphism ϕ_1 of $\tilde{L}_1$ into $\tilde{F}_1$ that extends ϕ_0 such that $L_1=\phi_1(L_1)$ is algebraically closed in F_1.

Note that L_1 is also algebraically closed in E, since it is an elementary subfield. Hence, if we replace E, F, ϕ_0, L and M by F_1, E, ϕ_1^{-1}, L_1 and L_1 we obtain a situation that is similar to the initial one. The same argument implies therefore that F_1 contains a countable elementary subfield M_1 that contains L_1, E has an elementary extension E_1 which is necessarily an ω-free Ax K-field, and there

exists a monomorphism ψ_1 of $\tilde{M}_1$ into $\tilde{E}_1$ that extends ϕ_1^{-1} such that $M_1' = \psi_1(M_1)$ is algebraically closed in E_1.



Continuing inductively one can construct four towers of fields

$$E = E_0 \prec E_1 \prec E_2 \prec \cdots,$$
$$L = L_0 \subseteq L_1 \subseteq L_2 \subseteq \cdots,$$
$$M = M_0 \subseteq M_1 \subseteq M_2 \subseteq \cdots,$$
$$F = F_0 \prec F_1 \prec F_2 \prec \cdots$$

and monomorphisms

$$\phi_i \colon \tilde{L}_i \to \tilde{M}_i \qquad i = 0, 1, 2, \ldots.$$
$$\psi_i \colon \tilde{M}_i \to \tilde{L}_{i+1} \qquad i = 1, 2, 3, \ldots.$$

such that $L_i \prec E_{i-1}$, $M_i \prec F_i$, ϕ_i extends ψ_{i-1}^{-1} and ψ_i extends ϕ_i^{-1} for $i = 1, 2, 3, \ldots$ ("$L_i \prec E_{i-1}$" means that L_i is an elementary subfield of E_{i-1}). Let $E_\infty = \bigcup_{i=0}^{\infty} E_i$ and $F_\infty = \bigcup_{i=0}^{\infty} F_i$. Then $E_i \prec E_\infty$ and $F_i \prec F_\infty$, by [3, p. 79]. In particular

$$E_\infty \equiv_K E \quad \text{and} \quad F_\infty \equiv_K F. \tag{1}$$

Moreover we get that $L_i \prec E_\infty$ and $M_i \prec F_\infty$ for $i = 1, 2, 3, \ldots$, hence, if we let $L_\infty = \bigcup_{i=1}^{\infty} L_i$ and $M_\infty = \bigcup_{i=1}^{\infty} M_i$, we get that $L_\infty \prec E_\infty$ and $M_\infty \prec F_\infty$ as one can easily deduce by applying, for example, Vaught's Test for elementary extensions (see [3, p. 76, Cor. 1.9]). In particular

$$L_\infty \equiv_K E_\infty \quad \text{and} \quad M_\infty \equiv_K E_\infty. \tag{2}$$

Further, the ϕ_i and ψ_i can be combined to give a K-isomorphism ϕ_∞ of L_∞ onto M_∞ and ψ_∞ of M_∞ onto L_∞ which are inverse to each other. If we combine this fact with (1) and (2) we get that $E \equiv_K F$.

Consider now the general case. Let Θ be a sentence of $\mathfrak{Q}(K)$ that is true in E. There are only finitely many elements of K, say $x_1, \ldots, x_n$, that occur in Θ. Let K_0 be a countable subfield of K that contains $x_1, \ldots, x_n$. Then Θ is also a sentence of $\mathfrak{Q}(K_0)$ and $\tilde{K}_0 \cap E \cong_{K_0} \tilde{K}_0 \cap F$. It follows, by the first part of the proof, that $E \equiv_{K_0} F$. Hence $F \vDash \Theta$. //

5. The Measure Space G

Let K be a field. For every positive integer e let $G_e=\mathcal{G}(K_s/K)^e$ and let μ_e be the completed Haar measure of G_e with respect to its Krull topology (see [7, Section 6]). Let $G=\bigcup_{e=1}^{\infty} G_e$. Every subset A of G can be uniquely represented as a disjoint union, $A=\dot{\bigcup}_{e=1}^{\infty} A_e$, where $A_e=A\cap G_e$. We topologize G by defining a subset A as *open*, if A_e is open in G_e for all e. Then a subset B of G is colsed if and only if B_e is colsed for all e. The topological space G thus obtained is Hausdorff, locally compact and totally disconnected. A colsed subset C is compact if and only if it is *bounded*, i.e. if C_e is empty for all e greater than some e_0. The group G_1 acts continuously on G from left and from right.

A subset A is said to be *measurable* if A_e is measurable for all e. The collection of all the measurable subsets of G form a σ-field of sets. For every measurable subset A we define

$$\mu(A)=\sum_{e=1}^{\infty}\mu_e(A_e).$$

Then μ is a complete regular Borel measure of G and it is invariant under the action of G_1. The restriction of μ to G_e coincides with μ_e and we clearly have

$$\mu(A)<\infty\Rightarrow\lim_{e\to\infty}\mu(A_e)=0.$$

A subset A of G is said to be *big*, if $\mu(A_e)=1$ for all but finitely many e. The intersection of finitely many big sets is clearly also a big set. A subset A is said to be *very big*, if $\mu(A_e)=1$ for all e. A countable intersection of very big sets is also a very big set. A subset B is said to be *small*, if $G-B$ is big, i.e. if $\mu(B_e)=0$ for all but finitely many e. A subset B of G is a *zero set* if and only if $G-B$ is a very big set.

An ultra-filter $\mathcal{D}$ of G is said to be *μ-regular*, if it contains all the big sets of G (cf. [7, Section 6]).

(5.1) **Lemma.** *Let $\mathcal{D}_0$ be a family of subsets of G. If for every $D_1,\ldots,D_n\in\mathcal{D}_0$ the set $D_1\cap\cdots\cap D_n$ is not a small set, then there exists a μ-regular ultra-filter $\mathcal{D}$ of G that contains $\mathcal{D}_0$.*

Proof. Clearly, the intersection of every big set with finitely many elements of $\mathcal{D}_0$ is not empty. Hence, there exists an ultrafilter $\mathcal{D}$ of G that contains $\mathcal{D}_0$ and all the big sets. $\mathcal{D}$ is a μ-regular ultra-filter. //

6. Regular Ultraproducts

We consider, for every positive integer e and for every $(\underline{\sigma})=(\sigma_1,\ldots,\sigma_e)\in G_e$, the field $\tilde{K}(\underline{\sigma})$, which is, by definition, the fixed field in K of the unique extension of $\sigma_1,\ldots,\sigma_e$ to $\tilde{K}$. $\tilde{K}(\underline{\sigma})$ is a perfect field. A *μ-regular* ultraproduct of the $\tilde{K}(\underline{\sigma})$'s is an ultraproduct of the form $\prod_{(\underline{\sigma})\in G}\tilde{K}(\underline{\sigma})/\mathcal{D}$, where $\mathcal{D}$ is a μ-regular ultrafilter of G.

Note the analogy with non-principal ultraproducts $\prod F_p/\mathscr{D}$ of the finite prime fields. In these ultraproducts one ignores what happens in finitely many F_p's, whereas in the μ-regular ultrafilters, $\prod \tilde{K}(\underline{\sigma})/\mathscr{D}$, one ignores families of $\tilde{K}(\underline{\sigma})$ in which the $(\underline{\sigma})$'s belong to a small set.

If E is an extension of K, then we denote by $[E/K]$ the set of all polynomials $f \in K[X]$ having a root in E.

For every $f \in K[X]$ and every positive integer e we denote

$$A_e(f) = \{(\underline{\sigma}) \in G_e \mid f \text{ has a root in } \tilde{K}(\underline{\sigma})\}$$

$$B_e(f) = G_e - A_e(f)$$

$$A(f) = \bigcup_{e=1}^{\infty} A_e(f), \qquad B(f) = \bigcup_{e=1}^{\infty} B_e(f).$$

The analogue of Lemma 6.2 of [7] is the following Lemma. Note that this Lemma makes it possible to "dig" arbitrary deep holes in $\tilde{K}$ via the μ-regular ultraproducts of the $\tilde{K}(\underline{\sigma})$.

(6.1) **Lemma.** *If L is an algebraic extension of K and if L is perfect, then there exists a μ-regular ultraproduct F of the $\tilde{K}(\underline{\sigma})$'s such that $\tilde{K} \cap F \cong_K L$.*

Proof. 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 that contains all the roots of $f_1, \ldots, f_m, g_1, \ldots, g_n$, let $L_0 = K' \cap L$ and let

$$e_0 = \operatorname{rank} \mathscr{G}(K'/L_0).$$

For every $e \geqq e_0$ choose $\sigma_1', \ldots, \sigma_e'$ that generate $\mathscr{G}(K'/L_0)$. If $\sigma_1, \ldots, \sigma_e$ are extensions of $\sigma_1', \ldots, \sigma_e'$ respectively to K_s, then $K' \cap \tilde{K}(\underline{\sigma}) = L_0$; hence each one of the polynomials $f_1, \ldots, f_m$ has a root in $\tilde{K}(\underline{\sigma})$, and no one of the polynomials $g_1, \ldots, g_n$ has a root in $\tilde{K}(\underline{\sigma})$. Let

$$D_e = \{(\underline{\sigma}) \in G_e \mid \sigma_i | K' = \sigma_i' \text{ for } i = 1, \ldots, e\}.$$

Then $\mu(D_e) > 0$ (see [7, Section 6, (1)]). Hence $D = \bigcup_{e=e_0}^{\infty} D_e$ is not a small set and we have

$$D \subseteq A(f_1) \cap \cdots \cap A(f_m) \cap B(g_1) \cap \cdots \cap B(g_n).$$

By Lemma 5.1 there exists a μ-regular ultrafilter $\mathscr{D}$ of G that contains all the $A(f)$'s and the $B(g)$'s for which $f \in [L/K]$, $g \in K[X] - [L/K]$ and f, g are separable over K. Then every separable polynomial $h \in K[X]$ has a root in L if and only if it has a root in $F = \prod \tilde{K}(\underline{\sigma})/\mathscr{D}$. It follows that $[L/K] = [F/K]$, since L and F are both perfect. Hence, by a Lemma of Ax [1, p. 172], $\tilde{K} \cap F \cong_K L$. //

For every sentence Θ in $\mathfrak{L}(K)$ and every positive integer e we let

$$A_e(\Theta) = \{(\underline{\sigma}) \in G_e \mid \tilde{K}(\underline{\sigma}) \models \Theta\},$$

$$A(\Theta) = \bigcup_{e=1}^{\infty} A_e(\Theta).$$

(6.2) **Lemma.** *Let Θ be a sentence in $\mathfrak{L}(K)$. Then $\tilde{K}(\underline{\sigma}) \models \Theta$ for a big set of $(\underline{\sigma})$'s in G if and only if $F \models \Theta$ for every regular ultraproduct F of the $\tilde{K}(\underline{\sigma})$'s.*

Proof. If $A(\Theta)$ is a big set and $\mathscr{D}$ is a regular ultrafilter of G, then $A(\Theta)\in\mathscr{D}$; hence $\prod \tilde{K}(\underline{\sigma})/\mathscr{D}\models\Theta$.

If $A(\Theta)$ is not a big set, then its complement $A(\sim\Theta)$ is not a small set; hence, by Lemma 5.1, there exists a regular ultrafilter $\mathscr{D}$ that contains $A(\sim\Theta)$. Hence $\prod \tilde{K}(\underline{\sigma})/\mathscr{D}\not\models\Theta$. //

We assume that the reader is familier with the concept of a hilbertian field (see [7, Section 7]).

(6.3) **Lemma.** *If K is a countable Hilbertian field, then every μ-regular ultraproduct F of the $\tilde{K}(\underline{\sigma})$'s is an ω-free Ax K-field.*

Proof. By Lemma 3.3 we must prove that the set of axioms $\Pi(K)$ holds in F. Clearly $F\models\Pi_0\cup\Pi_3(K)$. Also, Lemma 6.2 implies that $F\models\Pi_2$, since $\tilde{K}(\underline{\sigma})$ is an Ax field for every e and almost all $(\underline{\sigma})\in G_e$ (see [7, Lemma 7.2]). Every sentence of Π_1 has the form $\Delta(\theta, G, H)$, where $\theta: G\to H$ is an epimorphism of finite groups. We know that $\mathscr{G}(\tilde{K}/\tilde{K}(\underline{\sigma}))\cong\hat{F}_e$, for every e and almost all $(\underline{\sigma})\in G_e$ (see [7, Lemma 7.2]). Hence, if $e\geqq\operatorname{rank} G$, then by Lemma 1.1, the embedding problem

$$\begin{array}{ccc} & & \mathscr{G}(\tilde{K}/\tilde{K}(\underline{\sigma})) \\ & & \big\downarrow{\scriptstyle\phi} \\ G & \xrightarrow{\theta} & H \end{array}$$

is solvable for every continuous epimorphism ϕ and for almost all $(\underline{\sigma})\in G_e$. Hence by Lemma 3.2 and the discussion that follows the Lemma, $\tilde{K}(\underline{\sigma})\models\Delta$ for almost all $(\underline{\sigma})\in G_e$. It follows that $A(\Delta(\theta, G, H))$ is a big set in G and hence $F\models\Delta(\theta, G, H)$. //

7. Elementary Statements over ω-Free Ax Fields

The following theorem says that if K is a countable Hilbertian field, then $\Pi(K)$ is a set of axioms for the theory of all sentences Θ of $\mathfrak{L}(K)$ that hold in $\tilde{K}(\underline{\sigma})$ for a big set of $(\underline{\sigma})$ in G.

(7.1) **Theorem.** *For a countable Hilbertian field K and a sentence Θ of $\mathfrak{L}(K)$ the following two statements are equivalent.*

(a) $\tilde{K}(\underline{\sigma})\models\Theta$ *for a big set of* $(\underline{\sigma})$ *in* G.

(b) $F\models\Theta$ *for every ω-free Ax K-field.*

Proof. (a) $\Rightarrow$ (b): Let F be an ω-free Ax K-field. Then $\tilde{K}\cap F$ is a perfect field. By Lemma 6.1 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 6.3 E is an ω-free Ax K-field and Θ holds in E (by (a)). By Theorem 4.2 $E\equiv_K F$, hence $F\models\Theta$.

(b) $\Rightarrow$ (a): Follows from Lemmas 6.2 and 6.3. //

A *one variable statement* is a K-elementary statement which is equivalent to a sentence of the form

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

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

The following Lemma gives us the complete information about $A(\Phi)$. Note that no assumption is made here on the field K.

(7.2) **Lemma.** *Let Φ be a K-elementary statement of one variable*

(a) *There exist positive integers n, r and integers $n_1, \ldots, n_r$ of absolute values $\leqq n$ such that*

$$\mu(A_e(\Phi)) = \sum_{i=1}^{r} \left(\frac{n_i}{n}\right)^e$$

for every positive integer e.

(b) *If $K \nvDash \Phi$, then $|n_i| < n$ for $i = 1, \ldots, r$; hence $\lim_{e \to \infty} \mu(A_e(\Phi)) = 0$ and $\mu(A(\Phi))$ is a rational number.*

(c) *If $K \vDash \Phi$, then $\lim_{e \to \infty} \mu(A_e(\Phi)) = 1$ and $\mu(A(\Phi)) = \infty$.*

Proof. We suppose that Φ is given by (1). Let L be the splitting field of $f_1, \ldots, f_m$ and let $n = [L:K]$. Then, for every positive integer e and every $(\underline{\sigma}) \in G_e$,

$$\tilde{K}(\underline{\sigma}) \vDash \Phi \Leftrightarrow L(\underline{\sigma}) \vDash \Phi$$

(see [4, Lemma 3.11]). There are only finitely many fields between K and L (cf. [9, p. 185]). It suffices therefore to prove that for every intermediate field $K \subseteq K' \subseteq L$ there exists a positive integer r' and integers $n'_1, \ldots, n'_{r'}$ of absolute value $\leqq n$ that depend only on K' and Φ but not on e, such that

$$\mu\{(\underline{\sigma}) \in G_e | L(\underline{\sigma}) = K'\} = \sum_{i=1}^{r'} \left(\frac{n_i}{n}\right)^e. \tag{2}$$

$\mu(A_e(\Phi))$ is then the sum of all the right hand sides of the (2), where K' runs over all the fields between K and L in which Φ holds.

Let $K = K_0, K_1, \ldots, K_{r'} = L$ be all the intermediate fields between K' and L. Then

$$\{(\underline{\sigma}) \in G_e | L(\underline{\sigma}) = K'\} = \mathcal{G}(K_s/K')^e - \bigcup_{i=1}^{r'} \mathcal{G}(K_s/K_i)^e. \tag{3}$$

Furthermore, for an intermediate field $K \subseteq K'' \subseteq L$ we have

$$\mu(\mathcal{G}(K_s/K'')^e) = \frac{1}{[L:K'']} = \frac{[L:K'']}{n}$$

and $[L:K''] \leqq n$. Hence

$$\mu\{(\underline{\sigma}) \in G_e | L(\underline{\sigma}) = K'\} = \frac{[L:K_0]^e}{n} + \sum_{t=1}^{r'} (-1)^t \sum_{(i)} \frac{[L:K_{i_1} \ldots K_{i_t}]^e}{n} \tag{4}$$

where $(\underline{i})=(i_1, \ldots, i_t)$ runs over all the t-tuples of positive integers between 1 and r'. The proof of (a) is thus completed.

(b) If $K \models \Phi$, then all the K_i appearing on the right hand side of (3) (including K_0) are proper extensions of K. It follows that the corresponding degrees

$$[L:K_{i_1 \ldots i_t}]$$

on the right hand side of (4) are smaller than n. This means that $|n_i|<n$, hence $\lim_{e\to\infty} \mu(A_e(\Phi))=0$. *Also*

$$\mu(A(\Phi))=\sum_{e=1}^{\infty} \mu(A_e(\Phi))=\sum_{i=1}^{r} \frac{n_i}{n-n_i}$$

is a rational number.

(c) If $K \models \Phi$, then $\{(\underline{\sigma}) \in G_e | L(\underline{\sigma})=K\} \subseteq A_e(\Phi)$. Arguing as in (b) on can prove that

$$\lim_{e\to\infty} \mu\{(\underline{\sigma}) \in G_e | L(\underline{\sigma}) \neq K\}=0.$$

Also

$$\mu\{(\underline{\sigma}) \in G_e | L(\underline{\sigma})=K\}=1-\mu\{(\underline{\sigma}) \in G_e | L(\underline{\sigma}) \neq K\},$$

hence $\lim_{e\to\infty} \mu(A_e(\Phi))=1$. It follows that $\mu(A(\Phi))=\infty$. //

Denote by $\mathscr{A}$ the boolean algebra of subsets of G generated by all the sets of the form $A(f)$, where f is a separable polynomial, and all the small sets. By definition $A(f)=A((\exists X) f(X)=0)$, hence every set $A \in \mathscr{A}$ differs from some $A(\Phi)$, where Φ is a one variable statement, only by a small set.

If A and B are two subsets of G that differ only by a zero set, then we write $A \approx B$.

The following Theorem shows that every K-elementary statement is equivalent modulo small sets to a one variable statement.

(7.3) **Theorem.** *If K is a Hilbertian countable field and Θ is a K-elementary statement then:*

(a) $A(\Theta) \in \mathscr{A}$, *i.e. there exists a one variable statement Φ such that:*

(i) $A(\Theta) \approx A(\Phi)$,

(ii) $\tilde{K}(\underline{\sigma}) \models \Theta \leftrightarrow \Phi$, *for a big set of $(\underline{\sigma})$'s in G,*

(iii) $F \models \Theta \leftrightarrow \Phi$, *for ever ω-free Ax K-field F,*

(iv) $\Pi(K) \models \Theta \leftrightarrow \Phi$ (i.e. *$\Theta \leftrightarrow \Phi$ holds in every nodel of $\Pi(K)$*),

(v) $\Pi(K) \vdash \Theta \leftrightarrow \Phi$ (i.e. *there is a formal proof of $\Theta \leftrightarrow \Phi$ from $\Pi(K)$*);

(b) $\mu(A(\Theta))$ *is either infinity or a rational number.*

Remark. Note that (a), (ii) means that there exists an e_0 such that for all $e \geqq e_0$ $A_e(\Theta)$ differs from $A_e(\Phi)$ only by a zero set. This was exactly the initial problem of this work.

Proof. (a) Assume that $A(\Theta) \notin \mathscr{A}$. Then, by considering the boolean algebra $\mathscr{A}$ modulo the small sets, one can prove that there exist two regular ultrafilters $\mathscr{D}_1$

and $\mathscr{D}_2$ of G such that

$$\mathscr{D}_1 \cap \mathscr{A} = \mathscr{D}_2 \cap \mathscr{A}, \tag{5}$$

$$A(\Theta) \in \mathscr{D}_1 - \mathscr{D}_2 \tag{6}$$

(see Ax [2, p. 265]. Let $F_i = \prod \tilde{K}(\underline{\sigma})/\mathscr{D}_i$, $i = 1, 2$. Then $[F_1/K] = [F_2/K]$, by (5) and since F_1, F_2 are perfect fields. Hence, by a lemma of Ax [1, p. 172], $\tilde{K} \cap F_2 \cong_K \tilde{K} \cap F_2$. By Lemma 6.3 F_1 and F_2 are ω-free Ax-fields. Hence, by Theorem 4.2 $F_1 \equiv_K F_2$. This contradicts (6).

It follows that $A(\Theta) \in \mathscr{A}$. Hence there exists a one variable statement Φ such that $A(\Theta) \approx A(\Phi)$. This is (i) by the definitions. Statement (iii) follows from (ii) by Theorem 7.1. Statement (iv) follows from (iii) by Lemma 3.3. Statement (v) follows from (iv) by Godel's completeness Theorem (see [3, p. 102].

(b) By (a), (ii) there exists an e_0 such that $\mu(A_e(\Theta)) = \mu(A_e(\Phi))$ for every $e \geqq e_0$. If $\mu(A(\Theta)) < \infty$, then, by Lemma 7.2 and in the notations of this Lemma $|n_i| < n$ for $i = 1, \ldots, r$. Hence

$$\begin{aligned}\mu(A(\Theta)) &= \sum_{e \leqq e_0} \mu(A_e(\Theta)) + \sum_{e = e_0}^{\infty} \mu(A_e(\Phi)) \\ &= \sum_{e \leqq e_0} \mu(A_e(\Theta)) + \sum_{i=1}^{r} \frac{n_i^{e_0}}{n^{e_0 - 1}(n - n_i)}.\end{aligned}$$

By [7, Thm. 7.5], each one of the numbers $\mu(A_e(\Theta)$ is rational; hence $\mu(A(\Theta))$ is a rational number too. //

8. The Decision Procedure

In this section we establish a decision procedure for the theory of ω-free Ax K-fields provided K is "given" in a sense which is to be defined here. We also prove the possibility of deciding other relevant questions and in particular determining for a given sentence Θ of $\mathfrak{L}(K)$, a one variable sentence Φ such that $A(\Phi \leftrightarrow \Theta)$ is a big set.

A field K is said to be of a *finite type*, if it is finitely generated over its prime field K_0. Every such field can be obtained from K_0 in two steps: first by a purley transcendental extension, $K_1 = K_0(t_1, \ldots, t_r)$, and then by a finite separable extension, $K = K_1(x)$. K_0 is said to be *given*, if its characteristic is given; K_1 is said to be *given*, if K_0 and r are given; finally K is said to be *given*, if K_0, K_1 and a separable irreducible polynomial, a root of which generates K over K_1, are given. The elements of a given field K can be explicitely written down and one can calculate the sum and the product of any two elements of K. It follows that for a given field K the set of axioms $\Pi(K)$ that was defined in Section 3 can be explicitely written down. Moreover one can factor any given polynomial $g \in K[X_1, \ldots, X_n]$ into irreducible factors (see van der Waerden [11, § 42, p. 135]). Finally we note that every infinite field of a finite type is Hilbertian (see Lang [8, p. 155]).

(8.1) **Theorem.** *Let K be a given infinite field, of a finite type. Then there exists a recursive decision procedure such that if Θ is a given sentence of $\mathfrak{L}(K)$, then*

(a) *one can find a one variable statement* Φ *and a positive integer* e_0 *such that for every* $e \geqq e_0$ *the set* $A_e(\Theta)$ *differs from* $A_e(\Phi)$ *only by a zero set;*

(b) *one can decide whether or not* $A(\Theta)$ *is a big set (i.e. whether or not* Θ *belongs to the theory of* ω*-free Ax K-fields);*

(c) *one can decide whether or not* $A(\Theta)$ *is a very big set;*

(d) *one can calculate* $\mu(A(\Theta))$.

Proof. One orders all the formal proofs from $\Pi(K)$ in a sequence and checks them one by one. After a finite number of steps one arrives at a formal proof of a sentence of the form $\Theta \leftrightarrow \Phi$, where Φ is a one variable sentence (by Thm. 7.3). Let

$$\Delta(\theta_1, G_1, H_1), \ldots, \Delta(\theta_m, G_m, H_m)$$

be all the axioms of the form $\Delta(\theta, G, H)$ appearing in this proof and let $e_0 = \max_{1 \leqq i \leqq m} \operatorname{rank} G_i$. Then for every $e \geqq e_0$ and for almost all $(\underline{\sigma}) \in G_e$ we have that $\tilde{K}(\underline{\sigma}) | = \Delta(\theta_i, G_i, H_i)$, $i = 1, \ldots, r$ (by Lemma 7.2 of [7], Lemma 1.1 and Lemma 3.2 along with the proceeding discussion). All the other axioms that appear in the proof are satisfied by $\tilde{K}(\underline{\sigma})$ for every $e \geqq 1$ and almost all $(\underline{\sigma}) \in G_e$ (by [7, Lemma 7.2 and Section 3]). It follows that $\tilde{K}(\underline{\sigma}) \models \Theta \leftrightarrow \Phi$ for every $e \geqq e_0$ and almost all $(\underline{\sigma}) \in G_e$.

Denote by L the splitting field of the set of polynomials appearing in Φ. Let $K = K_0, K_1, \ldots, K_r = L$ be all the fields between K and L. One computes, by the method of [7, Section 8] the numbers r and $n = [L:K]$ and checks whether or not $K_i \models \Phi$ for every $0 \leqq i \leqq r$. If this is the case, then $\tilde{K}(\underline{\sigma}) \models \Phi$, for every $e \geqq 1$ and all $(\underline{\sigma}) \in G_e$ (see the proof of Lemma 7.2); hence $\tilde{K}(\underline{\sigma}) \models \Theta$, for every $e \geqq e_0$ and almost all $(\underline{\sigma}) \in G_e$, i.e. $A(\Theta)$ is a big set. Otherwise $A(\Theta)$ is not a big set. If $A(\Theta)$ is found to be a big set, then one decides, by the decision procedure of [7, Section 9], seperately for each $1 \leqq e \leqq e_0$, whether or not $\mu(A_e(\Theta)) = 1$. If $\mu(A_e(\Theta)) = 1$ for every $1 \leqq e < e_0$, then $A(\Theta)$ is a very big set, otherwise it is not. Finally one computes the integers $n_1, \ldots, n_r$ of Lemma 7.2 relating to Φ, by following the proof of this Lemma. Then one has,

$$\mu(A_e(\Phi)) = \sum_{i=1}^{r} \left(\frac{n_i}{n}\right)^e \quad \text{for } e = 1, 2, \ldots.$$

If $K \models \Phi$, then $\mu(A(\Theta)) = \mu(A(\Phi)) = \infty$ (by Lemma 7.2). Otherwise $|n_i| < |n|$ for $i = 1, \ldots, r$ and then

$$\mu(A(\Theta)) = \sum_{e < e_0} \mu(A_e(\Theta)) + \sum_{i=1}^{r} \frac{n_i^{e_0}}{n^{e_0 - 1}(n - n_i)}.$$

Each one of the measures $\mu(A_e(\Theta))$, $1 \leqq e < e_0$, can be computed by [7, Thm. 8.2].

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. Jarden, M.: Elementary statements over large algebraic fields. Trans. of AMS **164**, 67–91 (1972)

5. Jarden, M.: Algebraic extensions of finite corank of hilbertian fields. Israel J. of Math. **18**, 279–307 (1974)
6. Jarden. M.: Algebraically closed fields with distinguished subfields. To be published in Arch. Math.
7. Jarden, M., Kiehne, U.: The elementary theory of algebraic fields of finite corank. Inventiones math. **30**, 275–294 (1975)
8. Lang, S.: Diophantine Geometry. New York: Interscience 1962
9. Lang, S.: Algebra. Reading: Addison-Wesley 1965
10. Ribes, L.: Introduction to profinite groups and Galois cohomology, Queens papers in pure and applied Mathematics, No. 24 (1970)
11. van der Waerden, B. L.: Modern algebra, Vol. I. Berlin-Heidelberg-New York: Springer

Received March 4, 1976