THE ELEMENTARY THEORY OF NORMAL FROBENIUS FIELDS

Moshe Jarden

Introduction. The Galois stratification is introduced by Fried and Sacerdote [3] in order to establish an explicit primitive recursive decision procedure for the elementary theory of finite fields. This method is further developed in [2] and leads to a primitive recursive decision method for Frobenius fields. In order to be more explicit we consider a given Hilbertian field K with an elimination theory, in the sense of [2], and let M be a Frobenius field that contains K. If G is a profinite group, then we denote by $\operatorname{Im} G$ the set of all finite quotient groups of G. In particular, if we denote by $G(M)$ the absolute Galois group of M, then $\operatorname{Im} G(M)$ is the set of all finite groups that can be realized over M. It is proved in [2] that if $\operatorname{Im} G(M)$ is a primitive recursive set of groups, then the Galois stratification method leads to a primitive recursive decision procedure for the theory of perfect Frobenius fields M' that contain K and satisfy $\operatorname{Im} G(M) = \operatorname{Im} G(M')$.

This result is generalized in Section 1 of this work. We consider a class Π of profinite groups each of which appears as the absolute Galois group of a Frobenius field M. This class is supposed to be equipped with a primitive recursive algorithm to determine for given $m+n$ finite groups $G_1, \ldots, G_m, H_1, \ldots, H_n$ whether or not there exists a $P \in \Pi$ such that $G_1, \ldots, G_m \in \operatorname{Im} P$ and $H_1, \ldots, H_n \notin \operatorname{Im} P$. We denote by $\mathfrak{M}$ the class of all perfect Frobenius fields M that contain K and satisfy $G(M) \in \Pi$, and show how to modify the arguments in [2] in order to establish a primitive recursive procedure for the theory of $\mathfrak{M}$.

This procedure is applied in Section 2 to the set Π of all normal closed subgroups of the free profinite group $\hat{F}_\omega$ on $\aleph_0$ generators. It follows from the results of Melnikov [11] that each of these groups is indeed isomorphic to an absolute Galois group of a perfect Frobenius field. These fields are therefore called *normal Frobenius fields*. Moreover, Melnikov's characterization of these groups leads to an explicit algorithm for Π as in the preceding paragraph. It follows that the theory of normal Frobenius fields that contain K is primitive recursive via Galois stratification.

The decidability of the theory of all perfect Frobenius fields that contain K is hereby reduced to the above group theoretic decision problem for the class Π of all absolute Galois groups of Frobenius fields. An affirmative solution to this problem has been recently given by Haran and Lubotzky [6].

1. Galois stratification for a class of strongly projective groups. A profinite group P is said to be *projective* if for every epimorphism $\alpha: G \to H$ of profinite groups and every homomorphism $\gamma: P \to H$ there exists a homomorphism

Received June 1, 1982.

Partially supported by the fund for basic research administered by the Israel Academy of Sciences and Humanities.

$\beta: P \to G$ such that $\alpha \circ \beta = \gamma$. This is equivalent to saying that the cohomological dimension of P is $\leqslant 1$ (see Gruenberg [5: p. 164]). The profinite group G is said to have the *embedding property* if for every epimorphism $\alpha: G \to H$ of finite groups with $G \in \operatorname{Im} P$ and every epimorphism $\gamma: P \to H$ there exists an epimorphism $\beta: P \to G$ such that $\alpha \circ \beta = \gamma$. It is pointed out in Section 4 of [2] that $\mathbf{Z}_p \times \mathbf{Z}_p$ has the embedding property but is not projective. On the other hand there exist projective profinite groups that do not have the embedding property (see Eršov and Fried [1]). Therefore we call a profinite group *strongly projective* if it is projective and has the embedding property.

A field M is said to be PAC if every non-void absolutely irreducible variety V defined over M has an M-rational point. It is proved in [10: Proposition 4.8] that a profinite group P is projective if and only if there exists a PAC field M such that $G(M) \cong P$. Likewise a field M is said to be a *Frobenius-field* if M is PAC and $G(M)$ is a strongly projective group (see [2: Theorem 1.2]).

Consider now a class Π of strongly projective groups and let $\mathcal{G}$ be a finite collection of finite groups. For every subcollection $\mathcal{H}$ of $\mathcal{G}$ we denote: $\Pi_{\mathcal{G},\mathcal{H}} = \{P \in \Pi \mid \mathcal{H} = \mathcal{G} \cap \operatorname{Im} P\}$.

Let K be a countable Hilbertian field. We speak about the *explicit case* if

(a) the field K is given with an elimination theory (in the sense of [2: Section 2]) and

(b) given $m+n$ finite groups $G_1, \ldots, G_m, H_1, \ldots, H_n$ we can determine (in a primitive recursive way) whether or not there exists a group $P \in \Pi$ such that $G_1, \ldots, G_m \in \operatorname{Im} P$ and $H_1, \ldots, H_n \notin \operatorname{Im} P$.

The language of the theory of fields augmented by constants for the elements of K is denoted by $\mathcal{L}(K)$.

Next we consider the class $\mathfrak{M}$ of all perfect Frobenius-fields M that contain K and satisfy $G(M) \in \Pi$. For every subcollection $\mathcal{H}$ of $\mathcal{G}$ we denote by $\mathfrak{M}_{\mathcal{G},\mathcal{H}}$ the subclass of all $M \in \mathfrak{M}$ that satisfy $G(M) \in \Pi_{\mathcal{G},\mathcal{H}}$. We denote by $\operatorname{Th}(\mathfrak{M})$ the theory of all sentences θ of $\mathcal{L}(K)$ that are true in all $M \in \mathfrak{M}$. Our aim is this section is to prove that in the explicit case $\operatorname{Th}(\mathfrak{M})$ is a primitive recursive theory. By the Skolem–Löwenheim Theorem, every $M \in \mathfrak{M}$ contains a countable elementary subfield M_0 that contains K. In particular the profinite group $G(M_0)$ is countably generated (i.e. it is generated by a countable set converging to 1 (cf. Ribes [12: p. 84])), the field M is perfect and Frobenius and $\operatorname{Im} G(M) = \operatorname{Im} G(M_0)$. If we add the group $G(M_0)$ to Π and augment $\mathfrak{M}$ accordingly, we do not change $\operatorname{Th}(\mathfrak{M})$ but achieve that each of the classes Π_ω contains countably generated groups. Therefore we may assume that this is the case from the very beginning.

LEMMA 1.1. *Let θ be a sentence of $\mathcal{L}(K)$. Then there exists a finite collection $\mathcal{G}$ of finite groups and there exists a finite Galois extension L of K such that $\mathcal{G}$ contains all subgroups of $\mathcal{G}(L/K)$ and such that for every subcollection $\mathcal{H}$ of $\mathcal{G}$ there exists a conjugacy domain $\operatorname{Con}_{\mathcal{H}}$ of subgroups of $\mathcal{G}(L/K)$ which is contained in $\mathcal{H}$ such that for every $M \in \mathfrak{M}_{\mathcal{G},\mathcal{H}}$ we have: $M \vDash \theta$ if and only if $\mathcal{G}(L/L \cap M) \in \operatorname{Con}_{\mathcal{H}}$. In the explicit case, $\mathcal{G}$, L and the $\operatorname{Con}_{\mathcal{H}}$ can be effectively computed if θ is presented.*

Proof. Let M be a Frobenius field that contains K and let $\mathcal{C} = \operatorname{Im} G(M)$. It is shown in [2] how to construct a sequence of Galois stratifications

$$\mathfrak{A}_i = \langle A_i, C_{ij} \to A_{ij}, \operatorname{Con}_{\mathcal{C}}(A_{ij}) \rangle_{j \in J_i}, \quad i = 1, 2, \ldots, n,$$

which finally yields a finite Galois extension L/K and a conjugacy domain $\operatorname{Con}_{\mathcal{C}}$ of subgroups of $\mathcal{G}(L/K)$ which is contained in $\mathcal{C}$ such that for every Frobenius field M' containing K that satisfies $\operatorname{Im} G(M') = \mathcal{C}$ we have:

$$M' \vDash \theta \Leftrightarrow \mathcal{G}(L/L \cap M) \in \operatorname{Con}_{\mathcal{C}}.$$

The construction of the Galois covers $C_{ij} \to A_{ij}$ and hence that of L does not depend on $\mathcal{C}$. We may therefore take $\mathcal{G}$ as the collection of all subgroups of $\mathcal{G}(C_{ij}/A_{ij})$, for $i = 1, \ldots, n$ and $j \in J_i$. A careful examination of the algorithm in [2] shows that the construction of the domains $\operatorname{Con}_{\mathcal{C}} A_{ij}$ and hence that of $\operatorname{Con}_{\mathcal{C}}$ depends only on $\mathcal{G} \cap \mathcal{C}$ but not on $\mathcal{C}$ itself. Therefore, given a subcollection $\mathcal{H}$ of $\mathcal{G}$ we define $\operatorname{Con}_{\mathcal{H}}$ in the following way: We check whether or not there exists a $P \in \Pi$ such that $\mathcal{H} = \mathcal{G} \cap \operatorname{Im} P$. In the negative case we put $\operatorname{Con}_{\mathcal{H}} = \varnothing$. In the positive case we may assume that P is countably generated and therefore we know, [2: Lemma 4.3], that there exists a Frobenius field M containing K such that $P = G(M)$. Then we define $\mathcal{C} = \operatorname{Im} P$, construct $\operatorname{Con}_{\mathcal{C}}$ as mentioned above and take $\operatorname{Con}_{\mathcal{H}} = \operatorname{Con}_{\mathcal{C}}$. If $M' \in \mathfrak{M}_{\mathcal{G}, \mathcal{H}}$ and $\mathcal{C}' = \operatorname{Im} G(M')$, then $\mathcal{H} = \mathcal{G} \cap \mathcal{C}'$; therefore $\operatorname{Con}_{\mathcal{C}'} = \operatorname{Con}_{\mathcal{C}} = \operatorname{Con}_{\mathcal{H}}$ and we have: $M' \vDash \theta \Leftrightarrow \mathcal{G}(L/L \cap M') \in \operatorname{Con}_{\mathcal{H}}$. □

If L/K is a Galois extension, we denote by $\mathcal{S}(L/K)$ the collection of all subgroups of $\mathcal{G}(L/K)$.

THEOREM 1.2. (a) *Suppose that we are in the explicit case and that θ is a given sentence of $\mathfrak{L}(K)$. Then we can primitive-recursively decide whether or not* $\theta \in \operatorname{Th}(\mathfrak{M})$.

(b) *If θ is true in all the fields $M \in \mathfrak{M}$ which are algebraic over K, then* $\theta \in \operatorname{Th}(\mathfrak{M})$.

Proof. Using the notation of Lemma 1.1 we claim that the following statements are equivalent:

(i) The sentence θ belongs to $\operatorname{Th}(\mathfrak{M})$.

(ii) If $\mathcal{H} \subseteq \mathcal{G}$ and $\Pi_{\mathcal{G}, \mathcal{H}}$ is not empty, then $\operatorname{Con}_{\mathcal{H}} = \mathcal{H} \cap \mathcal{S}(L/K)$.

Indeed, assume that (ii) is true and let $M \in \mathfrak{M}$. Taking $\mathcal{H} = \mathcal{G} \cap \operatorname{Im} G(M)$ we have $M \in \mathfrak{M}_{\mathcal{G}, \mathcal{H}}$ and $\mathcal{G}(L/L \cap M) \in \mathcal{S}(L/K) \cap \operatorname{Im} G(M) = \mathcal{H} = \operatorname{Con}_{\mathcal{H}}$. Therefore, by Lemma 1.1, $M \vDash \theta$.

Conversely, assume that there exists a group $P \in \Pi$ such that for $\mathcal{H} = \mathcal{G} \cap \operatorname{Im} P$ there exists a group $H \in \mathcal{H} \cap \mathcal{S}(L/K) - \operatorname{Con}_{\mathcal{H}}$. By assumption $\Pi_{\mathcal{G}, \mathcal{H}}$ contains a countably generated group P'. Then $\mathcal{H} = \mathcal{G} \cap \operatorname{Im} P'$ and in particular $H \in \operatorname{Im} P'$. By Lemma 4.3 of [2] there exists a perfect Frobenius field M, algebraic over K, such that $G(M) \cong P$ and $H = \mathcal{G}(L/L \cap M)$. Lemma 1.1 implies that $M \nvDash \theta$.

The validity of Statement (ii) can be checked, since we are in the explicit case. Hence, we may decide whether or not $\theta \in \operatorname{Th}(\mathfrak{M})$. □

REMARK. Suppose that the group theoretic decision problem (b) for Π on page 156 can be solved in a recursive way. Then one can still use the methods of [9] and prove the 'recursive analogue' of Theorem 1.2.

2. Normal Frobenius fields. Let $G=G_0\rhd G_1\rhd\cdots\rhd G_{n-1}\rhd G_n=1$ be a normal sequence of a finite group G such that the factor groups G_i/G_{i+1} are simple for $i=0,\ldots,n-1$. These factor groups are called the *composition factors* of G. By the theorem of Jordan–Hölder [7: p. 63] they depend only on G. We denote by Σ the set of all finite simple groups and consider a subset Δ of Σ. A finite group G is said to be a Δ-*group* if all its composition factors belong to Δ. An inverse limit of Δ-groups is said to be a *pro-Δ-group*. For example, if $\Delta=\{\mathbf{Z}/p\mathbf{Z}\}$, then a pro-$\Delta$-group is a pro-$p$-group; for $\Delta=\{\mathbf{Z}/p\mathbf{Z}\mid p \text{ is a prime}\}$, we get the pro-solvable groups and $\Delta=\Sigma$ provides all pro-finite groups. Note that a closed normal subgroup and a factor group of a pro-Δ-group are again pro-Δ-groups. However an arbitrary closed subgroup of a pro-Δ-group is not necessarily a pro-Δ-group.

We denote by $\hat{F}_\omega(\Delta)$ the free pro-Δ-group on $\aleph_0$ generators. It can be obtained by starting from a free discrete group F_ω having $\aleph_0$ free generators $x_1,x_2,x_3,\ldots$. Then $\hat{F}_\omega(N)=\varprojlim F_\omega/N$, where N runs over all normal subgroups of F_ω that contain all but finitely many x_i's and such that F_ω/N is a Δ-group. In particular, if $\Delta=\Sigma$, then $\hat{F}_\omega=\hat{F}_\omega(\Delta)$ is the free profinite group on $\aleph_0$ generators.

If P is a profinite group and $S\in\Sigma$, then we denote by $\nu_P(S)$ the number of normal open subgroups N of P that satisfy $P/N\cong S$. Thus, ν_P is a function from Σ to the set of cardinal numbers $\leqslant|P|$. For primes p we write $\nu_P(p)$ instead of $\nu_P(\mathbf{Z}/p\mathbf{Z})$.

A function $g:\Sigma\to\{0,1,2,\ldots,\aleph_0\}$ is said to be Δ-*admissible* if $g(S)=0$ for every $S\in\Sigma-\Delta$ and if $g(p)\in\{0,\aleph_0\}$ for every prime p. Melnikov proved the following in Theorems 3.1, 3.2, 3.5 and in Proposition 3.1 of [11].

LEMMA 2.1. *Let Δ be a set of finite simple groups.*

(a) *If N is a closed normal subgroup of $\hat{F}_\omega(\Delta)$, then ν_N is a Δ-admissible function.*

(b) *For every Δ-admissible function g there exists a closed normal subgroup N of $\hat{F}_\omega(\Delta)$ such that $g=\nu_N$.*

(c) *If N and M are two closed normal subgroups of $\hat{F}_\omega(\Delta)$ such that $\nu_N=\nu_M$, then $N\cong M$.*

(d) *If N is a closed normal subgroup of $\hat{F}_\omega(\Delta)$ and if G, H are Δ-groups such that $\nu_G(S)\leqslant\nu_N(S)$ for every $S\in\Sigma$, then for every pair $\alpha:N\to H$ and $\beta:G\to H$ of epimorphisms there exists an epimorphism $\gamma:N\to G$ such that $\alpha=\beta\circ\gamma$. In particular we have:*

(e) *If G is a Δ-group and if $\nu_G(S)\leqslant\nu_N(S)$ for every $S\in\Sigma$, then $G\in\operatorname{Im}N$.*

(f) *Every proper open normal subgroup of N is isomorphic to $\hat{F}_\omega(\Delta)$.*

COROLLARY 2.2. *Every closed normal subgroup N of $\hat{F}_\omega(\Delta)$ has the embedding property.*

Proof. Let G be a finite quotient of N and let $\alpha:N\to H$ and $\beta:G\to H$ be epimorphisms. Then H and G are Δ-groups and $\nu_G(S)\leqslant\nu_N(S)$ for every $S\in\Sigma$. It

follows from Lemma 2.1(d) that there exists an epimorphism $\gamma: N \to G$ such that $\alpha = \beta \circ \gamma$. □

LEMMA 2.3. *The following conditions on a subset Δ of Σ are equivalent:*
(a) *The profinite group $\hat{F}_\omega(\Delta)$ is projective.*
(b) *If a prime p divides the order of a group $S \in \Delta$, then $\mathbf{Z}/p\mathbf{Z} \in \Delta$.*

Proof. (a) ⇒ (b)

Let S be a group belonging to Δ and let p be a prime divisor of $|S|$. By a theorem of Gaschütz ([4: p. 275 and also Satz 6 p. 284]) there exists a short exact sequence

$$1 \to A \to H \xrightarrow{\pi} S \to 1$$

where A is a non-trivial elementary abelian p-group which is contained in the Frattini group $\phi(H)$ of H. Also, there exists an epimorphism $\sigma: \hat{F}_\omega(\Delta) \to S$. By the projectivity of $\hat{F}_\omega(\Delta)$ there exists a homomorphism $\eta: \hat{F}_\omega(\Delta) \to H$ such that $\pi \circ \eta = \sigma$. Then $A \cdot \pi(\hat{F}_\omega(\Delta)) = H$ and from the assumption $A \leqslant \phi(H)$ we deduce that $\pi(\hat{F}_\omega(\Delta)) = H$. Thus $\mathbf{Z}/p\mathbf{Z}$ is a composition factor of the Δ-group H and therefore $\mathbf{Z}/p\mathbf{Z} \in \Delta$.

(b) ⇒ (a)

It suffices to consider for every prime p the diagram

$$\begin{array}{ccccccc} & & & & \hat{F}_\omega(\Delta) & & \\ & & & & \downarrow \alpha & & \\ 1 & \to & A & \to & G & \to & H \to 1 \end{array} \tag{1}$$

where α is an epimorphism, the short exact sequence of finite groups is exact and A is an elementary abelian p-group, and to show that there exists an epimorphism $\beta: \hat{F}_\omega(\Delta) \to G$ that makes the diagram commutative (cf. Gruenberg [5: p. 157] or Ribes [12: p. 211]). If p does not divide $|H|$, then the short exact sequence splits, by Schur-Zassenhaus' Theorem and the existence of β is guaranteed. If p divides $|H|$, then p divides the order of one of the composition factors of H. This factor belongs to Δ, since H, being a quotient group of $\hat{F}_\omega(\Delta)$, is a Δ-group. It follows that $\mathbf{Z}/p\mathbf{Z} \in \Delta$. But this implies that all the composition factors of G belong to Δ, hence G is a Δ-group. Therefore, by Lemma 2.1(d), there exists an epimorphism $\beta: \hat{F}_\omega(\Delta) \to G$ that makes the diagram (1) commutative. □

Combining Corollary 2.2 and Lemma 2.3 we have:

LEMMA 2.4. *If a subset Δ of Σ satisfies the conditions of Lemma 2.3, then every closed normal subgroup of $\hat{F}_\omega(\Delta)$ is strongly projective.*

REMARK. The converse of Lemma 2.4 is not true. Indeed, $\hat{\mathbf{Z}}$ is obviously a strongly projective profinite group. On the other hand, $\nu_{S_3}(2) = 1$ and $\nu_{S_3}(S) = 0$ for every $S \in \Sigma$ different from $\mathbf{Z}/2\mathbf{Z}$. In addition there exist epimorphisms $\alpha: \hat{\mathbf{Z}} \to \mathbf{Z}/2\mathbf{Z}$ and $\beta: S_3 \to \mathbf{Z}/2\mathbf{Z}$ but there exists no epimorphism $\gamma: \hat{\mathbf{Z}} \to S_3$, since S_3 is not cyclic. It follows from Lemma 2.1(d) that there exists no subset Δ of Σ such that $\hat{\mathbf{Z}}$ is isomorphic to a closed normal subgroup of $\hat{F}_\omega(\Delta)$.

We return now to a fixed subset Δ of Σ and take Π to be the class of all profinite groups which are isomorphic to closed normal subgroups of $\hat{F}_\omega(\Delta)$. A Frobenius field M is said to be Δ-*normal* if $G(M)\in\Pi$.

LEMMA 2.5. *The following two conditions on $m+n$ Δ-groups $G_1,\dots,G_m$, $H_1,\dots,H_n$ are equivalent:*

(a) *There exists a group $P\in\Pi$ such that $G_1,\dots,G_m\notin \operatorname{Im} P$ and $H_1,\dots,H_n\in \operatorname{Im} P$.*

(b) *For every $1\leqslant j\leqslant n$ there exists a non-abelian group $S\in\Delta$ such that*

$$\max_{1\leqslant i\leqslant m} \nu_{G_i}(S)<\nu_{H_i}(S) \tag{2}$$

or there exists a prime p such that

$$\max_{1\leqslant i\leqslant m} \nu_{G_i}(p)=0<\nu_{H_j}(p). \tag{3}$$

Proof. (a)$\Rightarrow$(b)

The assumption $G_1,\dots,G_m\in\operatorname{Im} P$ implies that for every $S\in\Delta$ we have

$$\max_{1\leqslant i\leqslant m} \nu_{G_i}(S)\leqslant \nu_P(S). \tag{4}$$

Let $1\leqslant j\leqslant n$ and assume that (2) is false for every non-abelian $S\in\Sigma$ and that (3) is false for every prime p. Then by (4)

$$\nu_{H_j}(S)\leqslant \nu_P(S) \tag{5}$$

for every non-abelian $S\in\Sigma$, and for every prime p either $\nu_{H_j}(p)=0$ or

$$0<\nu_{H_j}(p)\leqslant \max_{1\leqslant i\leqslant m} \nu_{G_i}(p).$$

In either case we conclude that (5) is valid also for $S=\mathbf{Z}/p\mathbf{Z}$. By Lemma 2.1(e) the group H_j belongs to $\operatorname{Im} P$, a contradiction.

(b)$\Rightarrow$(a)

By Lemma 2.1(b) there exists a group $P\in\Pi$ such that $\nu_P(S)=\max_{1\leqslant i\leqslant m}\nu_{G_i}(S)$ for every non-abelian $S\in\Sigma$, and $\nu_P(p)=0$ if $\max_{1\leqslant i\leqslant m}\nu_{G_i}(p)=0$ and $\nu_P(p)=\aleph_0$ if $\max_{1\leqslant i\leqslant m}\nu_{G_i}(p)>0$, for every prime p. In particular $\nu_{G_i}(S)\leqslant\nu_P(S)$ for every $S\in\Sigma$, hence $G_i\in\operatorname{Im} P$, by Lemma 2.1(e), for $i=1,\dots,m$. If $1\leqslant j\leqslant n$, then there exists a non-abelian group $S\in\Sigma$ such that (2) is satisfied and hence $\nu_P(S)<\nu_{H_j}(S)$, or there exists a prime p such that (3) is satisfied; but then $\nu_P(p)=0<\nu_{H_j}(p)$. In both cases we conclude that $H_j\notin\operatorname{Im} P$. Thus (a) has been completely verified. □

THEOREM 2.6. *Let K be a given countable Hilbertian field with an elimination theory. Let Δ be a primitive recursive set of finite groups that satisfies the following condition:*

(*) *If $S\in\Delta$ and if p is a prime divisor of $|S|$, then $\mathbf{Z}/p\mathbf{Z}\in\Delta$.*

Then the theory $T(K,\Delta)$ of all sentences in $\mathfrak{L}(K)$ that are true in every perfect Δ-normal Frobenius field that contains K is primitive recursive via Galois stratification. Moreover, a sentence θ of $\mathfrak{L}(K)$ belongs to $T(K,\Delta)$ if and only if it is true in all models of $T(K,\Delta)$ which are algebraic over K.

Proof. By Corollary 2.4 every group in Π is strongly projective. Moreover, given $m+n$ finite groups $G_1, \ldots, G_m, H_1, \ldots, H_n$ we can effectively check whether they are Δ-groups and whether they satisfy condition (b) of Lemma 2.5. We are therefore in the explicit case. Our theorem is a special case of Theorem 1. □

As a complement to Theorem 2.6 we point out an explicit system of axioms for the theory $T(K, \Delta)$.

LEMMA 2.7. *Let E be a perfect countable field and let Δ be a subset of Σ that satisfies condition (*) of Theorem* 2.6. *Then E is a Δ-normal Frobenius field that contains K if and only if the following conditions are satisfied:*

(a) *E is an* Ax (= *perfect* PAC) *field that contains K.*

(b) *The group $G(E)$ has the embedding property; in other words, if E' and F are Galois extensions of E, and $\pi: \mathcal{G}(E'/E) \to \mathcal{G}(F/E)$ is an epimorphism, then there exists a Galois extension F' of E that contains F and there exists an isomorphism $\varphi: \mathcal{G}(F'/E) \to \mathcal{G}(E'/E)$ such that $\pi \circ \varphi = \mathrm{res}$.*

(c) *For every positive integer m and a prime p we have: if $\mathbf{Z}/p\mathbf{Z}$ is realizable over E, then $(\mathbf{Z}/p\mathbf{Z})^m$ is realizable over E.*

(d) *For every Δ-group H we have: H is realizable over E if and only if every quotient of H of the form S^m, where $S \in \Delta$ is not abelian, is realizable over E.*

(e) *A finite group H which is not a Δ-group is not realizable over E.*

Proof. Lemma 2.1 and Corollary 2.2 imply that every perfect Δ-normal Frobenius field that contains K satisfies conditions (a)–(e).

Conversely, suppose that E satisfies these conditions. Then (a) and (b) imply that E is a perfect Frobenius field that contains K. Conditions (c) and (e) imply that the function $\nu_{G(E)}$ is Δ-admissible. Hence, by Lemma 2.1(b) there exists a closed normal subgroup N of $\hat{F}_\omega(\Delta)$ such that $\nu_N = \nu_{G(E)}$. Therefore, conditions (c) and (d) imply that $\mathrm{Im}\, G(E) = \mathrm{Im}\, N$. In addition, $G(E)$ and N are countably generated profinite groups with the embedding property. Using compactness arguments we are able to deduce that $G(E) \cong N$. This means that E is a Δ-normal field. □

Conditions (a)–(e) on the field E can be explicitly written as a sequence of sentences $A(K, \Delta)$ in the language $\mathcal{L}(K)$. In particular we can use Lemma 1.4 of [9] for condition (a) and we can use Lemma 3.2 of [8] for condition (b). It is proved in this last lemma that every embedding problem over E is equivalent to an elementary statement on the pair $(\tilde{E}, E)$, where $\tilde{E}$ is the algebraic closure of E. If one examines the elementary statement that appears there, one sees that it is not difficult to eliminate the quantifiers on elements of $\tilde{E}$. For example, if $f \in E[X]$ is a polynomial of degree m and one speaks about the existence of elements $\alpha_1, \ldots, \alpha_m$ of $\tilde{E}$ such that $f(X) = (X-\alpha_1)\cdots(X-\alpha_m)$, then one can speak instead about the existence of an irreducible polynomial $p \in E[X]$ of degree $m!$ and about the existence of polynomials $q_1, \ldots, q_m$ of degree $(m!)-1$ such that $f(X) \equiv (X-q_1(Z))\cdots(X-q_m(Z)) \bmod p(Z)$.

THEOREM 2.8. *If K and Δ are as in Theorem* 2.6, *then $A(K, \Delta)$ is a system of axioms for the theory $T(K, \Delta)$.*

Proof. Let F be a field satisfying the axioms $A(K,\Delta)$ and let E be a countable elementary subfield of F that contains K. Lemma 2.7 implies that E is a perfect Δ-normal Frobenius field. It follows that E and therefore also F satisfy $T(K,E)$. □

Conditions (b)–(e) of Lemma 2.7 can be written in terms of groups and thus provide an internal characterization of normal subgroups of $\hat{F}_\omega(\Delta)$. This is a completion to Melnikov's results:

PROPOSITION 2.9. *Let Δ be a set of simple groups and let G be a countably generated pro-Δ-group. Then G is isomorphic to a closed normal subgroup of $\hat{F}_\omega(\Delta)$ if and only if the following conditions are satisfied:*

(a) *The group G has the embedding property.*

(b) *For every positive integer m and every prime p we have: $\mathbf{Z}/p\mathbf{Z} \in \operatorname{Im} G \Rightarrow (\mathbf{Z}/p\mathbf{Z})^m \in \operatorname{Im} G$.*

(c) *For every Δ-group H we have: $H \in \operatorname{Im} G$ if and only if every quotient of H of the form S^m, where $S \in \Delta$ is non-abelian, belongs to* Im G.

As a peculiarity we note the following:

COROLLARY 2.10. *If a countably generated pro-Δ-group G satisfies conditions* (a), (b) *and* (c) *of Proposition* 2.9, *then every proper open normal subgroup of G is isomorphic to $\hat{F}_\omega(\Delta)$.*

REFERENCES

1. Yu. L. Eršov and M. Fried, *Frattini covers and projective groups without the extension property,* Math. Ann. 253 (1980), 233–239.
2. M. Fried, D. Haran and M. Jarden, *Galois stratification over Frobenius fields,* Adv. in Math., to appear.
3. M. Fried and G. Sacerdote, *Solving diophantine problems over all residue class fields of a number field and all finite fields,* Ann. of Math. (2) 104 (1976), 203–233.
4. W. Gaschütz, *Über modulare Darstellungen endlicher Gruppen, die von freien Gruppen induziert werden,* Math. Z. 60 (1954), 274–286.
5. K. W. Gruenberg, *Projective profinite groups,* J. London Math. Soc. 42 (1967), 155–165.
6. D. Haran and A. Lubotzky, *Embedding covers and the theory of Frobenius fields,* Israel J. Math. 41 (1982), 181–202.
7. B. Huppert, *Endliche Gruppen I,* Springer, Berlin, 1967.
8. M. Jarden, *The elementary theory of ω-free* Ax *fields,* Invent. Math. 38 (1976), 187–206.
9. M. Jarden and U. Kiehne, *The elementary theory of algebraic fields of finite corank,* Invent. Math. 30 (1975), 275–294.
10. A. Lubotzky and L. van den Dries, *Subgroups of free profinite groups and large subfields of* **Q**, Israel J. Math. 39 (1981), 25–45.

11. O. V. Melnikov, *Normal subgroups of free profinite groups,* Math. USSR-Izv. 12 (1978), 1–20. (1979).
12. L. Ribes, *Introduction to profinite groups and Galois cohomology,* Queen's University, Kingston, Ontario, 1970.

School of Mathematical Sciences
Tel Aviv University
Ramat Aviv, Tel Aviv 69978