ISRAEL JOURNAL OF MATHEMATICS, Vol. 41, No. 3, 1982

EMBEDDING COVERS AND THE THEORY OF FROBENIUS FIELDS

BY

DAN HARAN† AND ALEXANDER LUBOTZKY

ABSTRACT

We show that the theory of Frobenius fields is decidable. This is conjectured in [4], [8] and [13], and we prove it by solving a group theoretic problem to which this question is reduced there. To do this we present and develop the notion of embedding covers of finite and pro-finite groups. We also answer two other problems from [8], again by solving a corresponding group theoretic problem: A finite extension of a Frobenius field need not be Frobenius and there are PAC fields which are not Frobenius fields.

Introduction

A field K is called pseudo-algebraically closed (abbreviated: PAC) if every absolutely irreducible variety defined over K has a K-rational point. This notion, which generalizes the concept of algebraically closed fields, is originally due to Ax ([1], [2]), who has also given the first examples of PAC fields. Other interesting examples and most of the known PAC fields have been given by Jarden ([11], [12]). Contrary to the theory of algebraically closed fields, it has been recently shown by Cherlin–van den Dries–Macintyre ([3], [4]) and independently by Ershov ([6]), that the theory of PAC fields is undecidable. Thus attention is drawn to a subclass of PAC fields, which has been investigated in [8] — the Frobenius fields (= Iwasawa fields in [4]):

A PAC field K is called a Frobenius field if its absqlute Galois group $G = G(K)$ has the embedding property, i.e., whenever $\varphi : G \twoheadrightarrow B$ and $\Pi : A \twoheadrightarrow B$ are continuous epimorphisms, where A is a finite quotient of G, then there exists an epimorphism $\psi : G \twoheadrightarrow A$ such that $\Pi \circ \psi = \varphi$. (Actually, in [8] another, more natural definition is given; but this turns out — [8], theorem 1.2 — to be equivalent to the above definition.)

† Portions of this work will be incorporated in the doctoral dissertation of the first author done in Tel Aviv University under the supervision of Prof. Moshe Jarden.

Received July 25, 1981

The discussion on Frobenius fields in [8] has posed a few questions:

(A) Is this a proper subclass of the class of PAC fields? (See [8], problem 1.9.)

(B) Is a finite extension of a Frobenius field also a Frobenius field? (See [8], problem 1.8.)

(C) Is the theory of perfect Frobenius fields primitive recursively decidable, or, at least, decidable? (See Problem 4.10.)

The last question is also the main problem left in [4].

Problem (A) has been affirmatively answered by Ershov and Fried ([7]) and also in [4]. In this paper we extend and simplify their proofs and answer the problems (B) and (C) as well.

As noted in [14] the groups which appear as absolute Galois groups of PAC fields are exactly the projective profinite groups. Thus (A), (B) are equivalent to the following questions:

(A′) Is every projective profinite group also *superprojective* (i.e. projective with the embedding property)?

(B′) Is every open subgroup of a superprojective group also superprojective?

Less evident but also true is the fact that (C) is equivalent to a group-theoretic decision problem (see [4] for the case of decidability and [13] for the case of primitive recursive decidability):

(C′) Given finite groups $A_1, \cdots, A_m, B_1, \cdots, B_n$, decide whether there exists a superprojective group G such that $A_1, \cdots, A_m$ are quotients of G and $B_1, \cdots, B_n$ are not.

The answer to (A′) is negative, the answer to (B′) and hence also to (B) is negative. The problem (C′) is primitive recursively decidable, hence the answer to (C) is affirmative, in the stronger sense.

These results are based on two group-theoretic concepts.

First, we define the notion of the universal embedding cover $E(G)$ of a finite group G: this is the "smallest" cover of G which has the embedding property. In Section 1 we prove its existence and show that it is a finite group, which can be computed from G.

Secondly, we use the notion of the universal Frattini cover $\tilde{G}$ of a finite group G; this has been suggested by Ershov and Fried in [7] and by Cherlin, van den Dries and Macintyre in [3] (called there the minimal projective cover). The main result of Section 2 asserts that if G has the embedding property, then $\tilde{G}$ has it too.

The solutions to the problems (A′), (B′), (C′) are relatively easily derived in Sections 3 and 4 from the above-mentioned preparations.

Notation and conventions

This paper deals with the category of profinite groups. Hence "group" means "profinite group", "subgroup H of G" means "closed subgroup H of G" (denoted $H \leqq G$, and $H \lhd G$, if H is normal); homomorphism (epimorphism) is meant as *continuous*; it is denoted by $\to$ ($\twoheadrightarrow$). For example, we write "there is a $\varphi : H \twoheadrightarrow G$" to shorten the phrase "there is an epimorphism $\varphi : H \twoheadrightarrow G$".

$\mathrm{Im}(G)$ = the family of all finite homomorphic images of a group G.

$\langle T \rangle$ = the smallest (closed) subgroup generated by a subset T of a group G. If there exists a finite subset $T \subseteq G$ such that $\langle T \rangle = G$, then G is called finitely generated (f.g. group, for short) and the *rank* $\mathrm{rk}(G)$ of G is the minimal number of elements of such a subset.

The supernatural order of G (cf. [15], definition 4.3) is denoted by $|G|$.

$\Phi(H)$ = the Frattini subgroup of H = the intersection of all maximal open subgroups of H.

$A \lhd B$ denotes the semidirect product of a group B acting on a group A.

If $\varphi : H \twoheadrightarrow G$, we call the couple (H, φ) a *cover* of G. By abuse of language we use this term also for H or φ alone. Two covers $\varphi_1 : H_1 \twoheadrightarrow G_1$, $\varphi_2 : H_2 \twoheadrightarrow G$ are *isomorphic*, if there is an isomorphism $\theta : H_1 \xrightarrow{\sim} H_2$ such that $\varphi_1 = \varphi_2 \circ \theta$.

We tacitly use the fact that an epimorphism of a f.g. group onto itself is an automorphism (cf. [15], proposition 7.6).

1. Embedding property

The aim of this section is to show the existence of the universal embedding cover of a finite group (Theorem 1.12). We begin with some technical lemmas which will also be used in later sections.

LEMMA 1.1. *Consider a commutative diagram of groups with epimorphisms*

(1)
$$\begin{array}{ccc} B & \xrightarrow[p_2]{} & B_2 \\ \downarrow{\scriptstyle p_1} & & \downarrow{\scriptstyle \Pi_2} \\ B_1 & \xrightarrow[\Pi_1]{} & A \end{array}$$

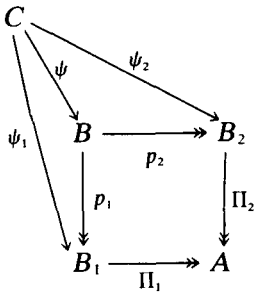
and put $p = \Pi_1 \circ p_1 = \Pi_2 \circ p_2$. *The following statements are equivalent*:

(a) *B is isomorphic to the* fibred product *of B_1, B_2 over A (w.r.t. the maps in* (1)*), i.e., there is an isomorphism*

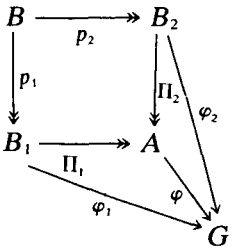
$$B \overset{\theta}{\twoheadrightarrow} B_1 \underset{A}{\times} B_2 = \{(b_1, b_2) \in B_1 \times B_2 \mid \Pi_1(b_1) = \Pi_2(b_2)\}$$

and $p_i \circ \theta^{-1}(b_1, b_2) = b_i$, *for* $i = 1, 2$ *and* $(b_1, b_2) \in B_1 \times_A B_2$.

(b) B *with* p_1, p_2 *is a* pullback *of the pair* (Π_1, Π_2), *i.e., given homomorphisms* $\psi_i : C \to B_i$, $i = 1, 2$, *such that* $\Pi_1 \circ \psi_1 = \Pi_2 \circ \psi_2$, *there is a unique homomorphism* $\psi : C \to B$ *such that* $p_i \circ \psi = \psi_i$, $i = 1, 2$.



(c) $\ker p_1 \cap \ker p_2 = 1$ *and* A *with* Π_1, Π_2 *is a* pushout *of the pair* (p_1, p_2), *i.e., given homomorphisms* $\varphi_i : B_i \to G$, $i = 1, 2$, *such that* $\varphi_1 \circ p_1 = \varphi_2 \circ p_2$, *there is a unique homomorphism* $\varphi : A \to G$ *such that* $\varphi \circ \Pi_i = \varphi_i$, $i = 1, 2$.



(d) $\ker p = \ker p_1 \times \ker p_2$.

PROOF. We only show (a) $\Leftrightarrow$ (b) $\Leftrightarrow$ (d); (c) will never be used in the sequel.

(a) $\Rightarrow$ (b): with no loss θ is identity; let ψ_1, ψ_2, C be as in (b). Clearly, if ψ exists, then necessarily $\psi(c) = (\psi_1(c), \psi_2(c))$; one verifies that this defines a continuous homorphism, hence (b).

(b) $\Rightarrow$ (a) follows from (a) $\Rightarrow$ (b) and the uniqueness of a pullback (up to an isomorphism).

(a) $\Rightarrow$ (d) follows from the definition of $B_1 \times_A B_2$.

(d) $\Rightarrow$ (a): define $\theta : B \to B_1 \times_A B_2$ by $\theta(b) = (p_1(b), p_2(b))$.

This is a well-defined homomorphism, and $\ker \theta = \ker p_1 \cap \ker p_2 = 1$. To an element $(b_1, b_2) \in B_1 \times_A B_2$ we may choose a $\hat{b}_i \in B$ such that $p_i(\hat{b}_i) = b_i$, $i = 1, 2$.

Now $p(\hat{b}_1) = p(\hat{b}_2)$, hence by (d), $\hat{b}_1 \equiv \hat{b}_2 \bmod(\ker p_1) \times (\ker p_2)$. Thus there are $a_1 \in \ker p_1$, $a_2 \in \ker p_2$ such that $\hat{b}_1 a_1 = \hat{b}_2 a_2$. We get

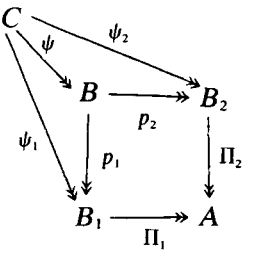
$$\theta(\hat{b}_1 a_1) = (p_1(\hat{b}_1 a_1), p_2(\hat{b}_2 a_2)) = (p_1(\hat{b}_1), p_2(\hat{b}_2)) = (b_1, b_2);$$

hence θ is surjective, whence (a). □

DEFINITION. A commutative diagram (1) satisfying one — and hence all — of the conditions of Lemma 1.1 is called a *cartesian diagram*, or a *cartesian square*.

LEMMA 1.2. *Let $\psi_i : C \twoheadrightarrow B_i$, $i = 1, 2$, be two epimorphisms. Then there is a commutative diagram, unique up to an isomorphism*;

(2)



where the square (1) *is cartesian and ψ is surjective.*

PROOF. If such a diagram exists, then with no loss $B_1 = C/K_1$, $B_2 = C/K_2$, $B = C/L$, $A = C/K$, where $K \subseteq K_1$, $K_2 \subseteq L$ are normal subgroups of C. By Lemma 1.1 (d)

$$L = K_1 \cap K_2, \qquad K = K_1 K_2, \tag{3}$$

hence the uniqueness of (2).

The equations (3) also suggest the definitions of groups B and A satisfying the conditions of the Lemma. □

We now concentrate on the *embedding property* (which is the *extension property* in [7]) of profinite groups.

Let us fix a group G. A pair of groups (A, B) may satisfy the following, so-called *embedding condition* $\mathrm{Emb}_G(A, B)$:

If A is a quotient group of G then for every pair of epimorphisms $\Pi : A \twoheadrightarrow B$, $\varphi : G \twoheadrightarrow B$ there exists an epimorphism $\psi : G \twoheadrightarrow A$ such that $\Pi \circ \psi = \varphi$.

DEFINITION. We say that G has the *embedding property* if $\mathrm{Emb}_G(A, B)$ is satisfied for all pairs (A, B) of finite groups.

A cover $p : H \twoheadrightarrow G$ is called an *embedding cover*, if H has the embedding property.

LEMMA 1.3. *A free profinite group has the embedding property.*

PROOF. See [8], lemma 1.3. □

LEMMA 1.4. *The following conditions on an f.g. group G are equivalent:*

(i) *G has the embedding property;*

(ii) $\mathrm{Emb}_G(A, B)$ *holds for every B finite and every A;*

(iii) $\mathrm{Emb}_G(G, B)$ *holds for every B finite;*

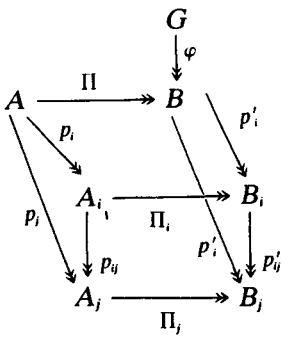
(iv) $\mathrm{Emb}_G(A, B)$ *holds for every A, B;*

(v) $\mathrm{Emb}_G(G, B)$ *holds for every B.*

PROOF. (i) $\Rightarrow$ (iv): Let A be a quotient group of G and let $\Pi: A \twoheadrightarrow B$, $\varphi: G \twoheadrightarrow B$ be epimorphisms. With no loss Π is the canonical map $A \twoheadrightarrow A/K$ with a $K \lhd A$. Let $\{N_i\}_{i\in I}$ be the directed family of all open normal subgroups in A and denote $A_i = A/N_i$, $B_i = A/N_iK$. Then

$$A = \varprojlim_{i\in I} A_i, \qquad B = \varprojlim_{i\in I} B_i$$

and we may define for every $i \in I$ and for every $i \geqq j$ canonical maps $p_i: A \twoheadrightarrow A_i$, $p_i': B \twoheadrightarrow B_i$, $\Pi_i: A_i \twoheadrightarrow B_i$, $p_{ij}: A_i \twoheadrightarrow A_j$, $p_{ij}': B_i \twoheadrightarrow B_j$, such that the following diagram is commutative



Let $\mathrm{rk}(G) = e$ and let $G = \langle g_1, \cdots, g_e \rangle$. For every $i \in I$ let

$$Y_i = \{\psi_i : G \twoheadrightarrow A_i \mid \Pi_i \circ \psi_i = p_i' \circ \varphi\}.$$

Then Y_i is a finite set (every $\psi_i: G \twoheadrightarrow A_i$ is determined by $\psi_i(g_1), \cdots, \psi_i(g_n)$); by (i) we have $Y_i \neq \varnothing$.

For $i \geqq j$ we define a map $Y_i \to Y_j$ by $\psi_i \mapsto p_{ij} \circ \psi_i$ and thus convert $\{Y_i\}$ into an inverse system of non-empty finite sets. Hence $Y = \varprojlim_{i\in I} Y_i$ is not empty and it

is easy to see that an element of Y defines a $\psi : G \twoheadrightarrow A$ such that $\Pi \circ \psi = \varphi$; hence (iv).

(iv) $\Rightarrow$ (v) $\Rightarrow$ (iii): are clear.

(iii) $\Rightarrow$ (ii): Let $\rho : G \twoheadrightarrow A$, $\Pi : A \twoheadrightarrow B$, $\varphi : G \twoheadrightarrow B$ be epimorphisms. By (iii) there is a $\psi' : G \twoheadrightarrow G$ such that $(\Pi \circ \rho) \circ \psi' = \varphi$. Thus $\psi = \rho \circ \psi'$ satisfies $\pi \circ \psi = \varphi$.

(ii) $\Rightarrow$ (i): is clear. □

REMARK. The condition that G be finitely generated is essential: the free profinite group $\hat{F}_\omega$ on $\omega = \{s_1, s_2, \cdots\}$ has by Lemma 1.3 the embedding property. However, as Ershov [6] has pointed out, the map $f : \omega \to \hat{F}_\omega$ defined by $f(s_1) = 1, f(s_{i+1}) = s_i$, $i = 1, 2, 3, \cdots$, extends to an epimorphism $\Pi : \hat{F}_\omega \twoheadrightarrow \hat{F}_\omega$ with $\ker \Pi \neq 1$. Clearly there is no $\psi : \hat{F}_\omega \twoheadrightarrow \hat{F}_\omega$ such that $\Pi \circ \psi = \mathrm{id}$, i.e., $\mathrm{Emb}_{\hat{F}_\omega}(\hat{F}_\omega, \hat{F}_\omega)$ fails to be satisfied.

Clearly the implications (i) $\Leftarrow$ (ii) $\Leftrightarrow$ (iii) $\Leftarrow$ (iv) $\Leftrightarrow$ (v) are valid for all groups. One can show that (i) $\Rightarrow$ (ii) is true for groups of countable rank (i.e. generated by a countable set converging to 1). However, we do not know whether (i) $\Rightarrow$ (ii) is true for all profinite groups.

LEMMA 1.5. *Let G be an f.g. group and N a characteristic subgroup of G. If G has the embedding property then so does G/N.*

PROOF. Let $\rho : G \twoheadrightarrow G/N$ be the canonical map and let $\Pi, \varphi : G/N \twoheadrightarrow B$ be two epimorphisms. By Lemma 1.4(v) there is a $\Psi' : G \twoheadrightarrow G$ such that $(\Pi \circ \rho) \circ \psi' = \varphi \circ \rho$. But $\psi' \in \mathrm{Aut}(G)$, hence $\psi'(N) = N$, whence Ψ' induces a $\psi \in \mathrm{Aut}(G/N)$ such that $\psi \circ \rho = \rho \circ \psi'$. Clearly $\Pi \circ \psi = \varphi$, which by Lemma 1.4(v) ends the proof. □

COROLLARY 1.6. *Let G be a finite group of rank e. Let N be the intersection of all open normal subgroups M of the free profinite group on e generators $\hat{F}_e$, which satisfy $\hat{F}_e/M \cong G$. Then $E_0 \overset{\text{def}}{=} \hat{F}_e/N$ is a finite group of rank e and it is an embedding cover of G.*

Moreover, $|E_0| \leqq |G|^{|G|^e}$.

PROOF. The embedding property of E_0 follows from Lemmas 1.3 and 1.5. Clearly $|E_0| \leqq |G|^n$, where n is the number of open $M \lhd \hat{F}_e$, for which $\hat{F}_e/M \cong G$. But there are at most $|G|^e$ epimorphisms of $\hat{F}_e$ onto G; hence $n \leqq |G|^e$. □

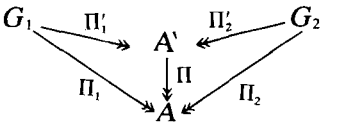
Besides the group E_0 of Cor. 16 there are other embedding covers of G. However, among all such covers there is a universal one; to show this we need the material developed below.

Let G_1, G_2 be two f.g. groups. Consider the class of pairs of epimorphisms with common images

$$\mathcal{P} = \mathcal{P}(G_1, G_2) = \{(\Pi_1, \Pi_2) \mid \Pi_1 : G_1 \twoheadrightarrow A \text{ and } \Pi_2 : G_2 \twoheadrightarrow A\}$$

and define a pre-order relation on $\mathcal{P}$: $(\Pi_1, \Pi_2) \leqq (\Pi_1', \Pi_2')$ iff there is an epimorphism Π such that the following diagram is commutative

(4)



Furthermore, write $(\Pi_1, \Pi_2) \sim (\Pi_1', \Pi_2')$ iff Π is an isomorphism: this is an equivalence relation on $\mathcal{P}$ and $\leqq$ defines a partial order relation on the quotient set $\mathcal{P}/\sim$. By abuse of notation we identity $\mathcal{P}/\sim$ with $\mathcal{P}$.

We also define the dual notion to $\mathcal{P}$.

Let $p_i : G_1 \times G_2 \twoheadrightarrow G_i$, $i = 1, 2$ be the canonical (coordinate) projections. Define

$$\mathcal{H} = \mathcal{H}(G_1, G_2) = \{H \mid H \leqq G_1 \times G_2 \text{ and } p_i(H) = G_i,\ i = 1, 2\};$$

$\mathcal{H}$ is partially ordered by inclusion.

For a pair $(\Pi_1, \Pi_2) \in \mathcal{P}$ with $A = \operatorname{Im}\Pi_1 = \operatorname{Im}\Pi_2$ let

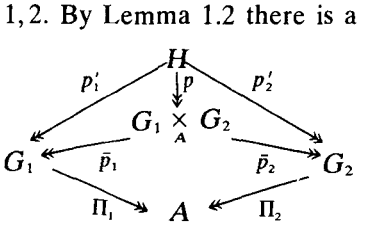
$$T(\Pi_1, \Pi_2) = G_1 \underset{A}{\times} G_2 = \{(g_1, g_2) \in G_1 \times G_2 \mid \Pi_1(g_1) = \Pi_2(g_2)\}. \tag{5}$$

Clearly $T(\Pi_1, \Pi_2) \in \mathcal{H}$.

LEMMA 1.7. *The map $T : \mathcal{P} \to \mathcal{H}$ is an order-reversing bijection between $\mathcal{P}$ and $\mathcal{H}$.*

PROOF. Let $(\Pi_1, \Pi_2), (\Pi_1', \Pi_2') \in \mathcal{P}$, $\operatorname{Im}\Pi_1 = \operatorname{Im}\Pi_2 = A$, $\operatorname{Im}\Pi_1' = \operatorname{Im}\Pi_2' = A'$. If $(\Pi_1', \Pi_2') \geqq (\Pi_1, \Pi_2)$, then $T(\Pi_1', \Pi_2') \subseteq T(\Pi_1, \Pi_2)$ by the definitions (4) and (5). Conversely, if $T(\Pi_1', \Pi_2') \subseteq T(\Pi_1, \Pi_2)$, define a $\Pi : A' \twoheadrightarrow A$ by $\Pi(\Pi_1' g_1) = \Pi_1(g_1)$, $g_1 \in G_1$. Then Π is well-defined and establishes the relation $(\Pi_1', \Pi_2') \geqq (\Pi_1, \Pi_2)$.

This also proves that T is injective. To show its surjectivity let $H \in \mathcal{H}$ and denote $p_i' = \operatorname{Res}_H p_i$, $i = 1, 2$. By Lemma 1.2 there is a commutative diagram



where $\bar{p}_i = \mathrm{Res}_{G_1 \times_A G_2} p_i$, $i = 1, 2$. But for every $(g_1, g_2) \in H$ we have

$$\bar{p}_i(p(g_1, g_2)) = p'_i(g_1, g_2) = g_i, \qquad i = 1, 2,$$

hence $p(g_1, g_2) = (g_1, g_2)$; hence $H = G_1 \times_A G_2 = T(\Pi_1, \Pi_2)$. □

LEMMA 1.8. *For every* $(\Pi_1, \Pi_2) \in \mathscr{P}$ *there is a maximal element* $(\Pi'_1, \Pi'_2) \in \mathscr{P}$ *such that* $(\Pi_1, \Pi_2) \leqq (\Pi'_1, \Pi'_2)$.

PROOF. By Zorn's Lemma it suffices to show that a chain $\{(\Pi_{1\alpha}, \Pi_{2\alpha})\}_{\alpha \in I}$ in $\mathscr{P}$ has a supremum. For $\beta \leqq \alpha \in I$ there is a unique $\Pi_{\alpha\beta} : \mathrm{Im}\, \Pi_{1\alpha} \twoheadrightarrow \mathrm{Im}\, \Pi_{1\beta}$ such that $\Pi_{\alpha\beta} \circ \Pi_{i\alpha} = \Pi_{i\beta}$, $i = 1, 2$. Thus $\{(\mathrm{Im}\, \Pi_{1\alpha})\}_{\alpha \in I}$ is an inverse system and its limit defines the supremum. (One may also carry out the dual proof in $\mathscr{H}$, using the intersection property of compact subsets of $G_1 \times G_2$.) □

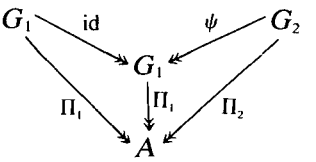
An element $(\Pi_1, \Pi_2) \in \mathscr{P}$ is called *trivial*, if Π_1 is an isomorphism. This is equivalent to: $\mathrm{Res}_{T(\Pi_1, \Pi_2)} p_2$ is an isomorphism.

Note that a trivial element is always maximal.

The elements of $\mathscr{P}$ may be seen as embedding problems. In fact we have:

LEMMA 1.9. *Let* $(\Pi_1, \Pi_2) \in \mathscr{P}(G_1, G_2)$. *Then there is a* $\psi : G_2 \twoheadrightarrow G_1$ *such that* $\Pi_1 \circ \psi = \Pi_2$ *iff there is a trivial* $(\Pi'_1, \Pi'_2) \in \mathscr{P}$ *such that* $(\Pi_1, \Pi_2) \leqq (\Pi'_1, \Pi'_2)$.

PROOF. If such a ψ exists, then $(\Pi_1, \Pi_2) \leqq (\mathrm{id}, \psi)$, as follows from the diagram:



Conversely, if there is a commutative diagram (4) with Π'_1 an isomorphism, let $\psi = (\Pi'_1)^{-1} \circ \Pi'_2$. □

COROLLARY 1.10. *An f.g. group* G *has the embedding property iff every maximal element in* $\mathscr{P}(G, G)$ *is trivial.*

To simplify the formulation let us make a definition:

DEFINITION. A cover $p : H \twoheadrightarrow G$ of an f.g. group G is called a *quasi-embedding cover, q.e.c.*, for short, if for every embedding cover $\varphi : E \to G$ the group H is a quotient of E, i.e., there is a $\psi : E \to H$ such that $p \circ \psi = \varphi$.

LEMMA 1.11. *Let G and A be two f.g. groups.*

(i) *If $p : H \twoheadrightarrow G$ is a q.e.c., then* $\mathrm{rk}(H) = \mathrm{rk}(G)$.

(ii) *Let $p : H \twoheadrightarrow G$, $\Pi : G \twoheadrightarrow A$ be two epimorphisms, then $\Pi \circ p$ is a q.e.c. iff both p and Π are q.e.c.'s.*

(iii) *Let $\Pi_1 : G_1 \twoheadrightarrow A$ and $\Pi_2 : G_2 \twoheadrightarrow A$ be two q.e.c.'s. Then there are q.e.c.'s $p : H \twoheadrightarrow A$, $p_1 : H \twoheadrightarrow G_1$, $p_2 : H \twoheadrightarrow G_2$ such that $\Pi_1 \circ p_1 = p = \Pi_2 \circ p_2$.*

(iv) *If G does not have the embedding property, there exits a q.e.c. $p_1 : H \twoheadrightarrow G$ with a non-trivial kernel.*

PROOF. (i) Let $e = \mathrm{rk}(G)$; clearly $\mathrm{rk}(H) \geqq e$. By Lemma 1.3 the group $\hat{F}_e$ is an embedding cover of G, hence H is a quotient of $\hat{F}_e$, whence $\mathrm{rk}(H) \leqq e$.

(ii) Clear.

(iii) By (ii) and by Lemma 1.8 we may assume that (Π_1, Π_2) is maximal in $\mathcal{P}(G_1, G_2)$. We form a cartesian square

(6)
$$\begin{array}{ccc} H & \xrightarrow{p_2} & G_2 \\ \downarrow{\scriptstyle p_1} & & \downarrow{\scriptstyle \Pi_2} \\ G_1 & \xrightarrow[\Pi_1]{} & A \end{array}$$

with $H = G_1 \times_A G_2$ and put $p = \Pi_1 \circ p_1 = \Pi_2 \circ p_2$. By symmetry and by (ii) it suffices to show that p_1 is a q.e.c. Now let $\psi_1 : E \twoheadrightarrow G_1$ be an embedding cover. Then so is $\Pi_1 \circ \psi_1$; hence G_2 is a quotient of E, since Π_2 is a q.e.c. By the embedding property of E there is a $\psi_2 : E \twoheadrightarrow G_2$ such that $\Pi_1 \circ \psi_1 = \Pi_2 \circ \psi_2$. By Lemma 1.1 (b) there is a homomorphism $\psi : E \to H$ satisfying $p_1 \circ \psi = \psi_1$, $p_2 \circ \psi = \psi_2$. Thus $\psi(E) \in \mathcal{H}(G_1, G_2)$ and $\psi(E) \subseteq H$; but it follows from Lemma 1.7 that H is minimal in $\mathcal{H}(G_1, G_2)$, hence $H = \psi(E)$ is a quotient of E.

(iv) By Corollary 1.10 there exists a non-trivial maximal pair (Π_1, Π_2) in $\mathcal{P}(G, G)$. Thus in the cartesian square (6), where now $G_1 = G_2 = G$, we have $\ker p_1 \neq 1$. We show that p_1 is a q.e.c. as in the proof of (iii) (omitting the sentence: "Then... q.e.c.").

THEOREM 1.12. *Let G be an f.g. group. Then there is a cover $p : E(G) \twoheadrightarrow G$, unique up to an isomorphism, satisfying*

(a) *p is an embedding cover, i.e., $E(G)$ has the embedding property.*

(b) *p is a q.e.c.*

Moreover,

(c) $\mathrm{rk}(E(G)) = \mathrm{rk}(G)$.

(d) *When G is a given finite group, then $E(G)$ is also finite and $E(G)$ and p may be effectively* (= *primitive recursively*) *computed.*

PROOF. Let $\{G_0 = 1, G_2, G_3, \cdots\}$ be the set of the finite quotients of the q.e.c.'s of G. Then we may form a sequence

$$H_0 = G \xleftarrow[\theta_1]{} H_1 \xleftarrow[\theta_2]{} H_3 \xleftarrow[\theta_3]{} \cdots$$

of q.e.c.'s such that for every $n \geqq 0$ the groups $G_0, G_1, \cdots, G_n$ are quotients of H_n. Indeed, suppose we have constructed $\theta_1, \cdots, \theta_{n-1}$ with these properties; then $\Pi_1 = \theta_{n-1} \circ \cdots \circ \theta_1$ is by Lemma 1.11 (ii) a q.e.c. There is a q.e.c. $\Pi_2 : H' \twoheadrightarrow G$ such that G_n is a quotient of H'. Hence by Lemma 1.11 (iii) there are q.e.c.'s $p_1 = \theta_n : H_n \twoheadrightarrow H_{n-1}$ and $p_2 : H_n \twoheadrightarrow H'$. In particular, G_n is a quotient of H_n.

Now let $E(G) = \varprojlim_i H_i$ and let $p : E(G) \twoheadrightarrow G$ be the induced map. We claim that p is a q.e.c. For let $\varphi_0 : E \twoheadrightarrow G$ be an embedding cover. Then we may inductively choose $\varphi_i : E \twoheadrightarrow H_i$ such that $\theta_i \circ \varphi_i = \varphi_{i-1}$, $i = 1, 2, \cdots$ (since φ_{i-1} is an embedding cover and θ_i is a q.e.c.). These define the desired map $\varphi : E \twoheadrightarrow E(G)$; hence (b). By Lemma 1.11 (i) follows also (c).

But $E(G)$ also satisfies (a). Otherwise there is, by Lemma 1.11 (iv), a q.e.c. $\theta : H \twoheadrightarrow E(G)$ with $\ker \theta \neq 1$. By construction of $E(G)$ we have $\mathrm{Im}(H) = \mathrm{Im}(E(G)) = \{G_0, G_1, \cdots\}$; by Lemma 1.11 (i) both groups are f.g., hence $H \cong E(G)$. Thus θ is, a fortiori, an isomorphism; a contradiction.

The uniqueness of p is trivial. When G is finite, then $E(G)$ is by (b) a quotient of the group E_0 from Corollary 1.6, hence finite.

In fact $E(G)$ has the smallest order among all quotients of E_0 which cover G and have the embedding property, and thus may be computed. □

DEFINITION. The cover $p : E(G) \twoheadrightarrow G$ of Theorem 1.12 is called the *universal embedding cover.*

2. Frattini covers

Frattini cover is the concept which links the embedding property with projective groups. Some recent papers ([5], [7], [3]) deal with this notion from different points of view. To be self-contained we develop this theory from the beginning; however, proofs which have already appeared will be only referred to.

DEFINITION. A group homomorphism $\varphi : H \to G$ is a *Frattini cover* of G if it satisfies one of the following equivalent conditions:

(i) φ is surjective and $\ker\varphi \subseteq \Phi(H)$;
(ii) if $H' \leqq H$ then: $H' = H \Leftrightarrow \varphi(H') = G$;
(iii) if $T \subseteq H$ is a set then: $\langle T\rangle = H \Leftrightarrow \langle \varphi T\rangle = G$.

The equivalence is a profinite analogue of [7], lemma 1.2.
Note that by (iii) a group G and its Frattini cover H have the same rank.

Some immediate properties of Frattini covers are summed-up in

LEMMA 2.1. *Let $H_1 \overset{\psi}{\to} H_2 \overset{\varphi}{\to} G$ be two homomorphisms. We have:*

(i) *if φ, ψ are Fr. covers, then $\varphi\circ\psi$ is a Fr. cover;*
(ii) *If φ is a Fr. cover and $\varphi\circ\psi$ is surjective, then ψ is surjective;*
(iii) *if $\varphi\circ\psi$ is a Fr. cover, then*

$$\psi \text{ is surjective} \Leftrightarrow \psi \text{ is a Fr. cover} \Leftrightarrow \varphi \text{ is a Fr. cover.}$$

PROOF. An exercise (cf. also [5] 3.2, 3.3). □

LEMMA 2.2. *Let $p : A \twoheadrightarrow B$ be a group epimorphism. Then:*
(a) $p\Phi(A) \subseteq \Phi(B)$, *i.e.*, $\phi(A) \subseteq p^{-1}\Phi(B)$;
(b) *if p is a Fr. cover, then $\Phi(A) = p^{-1}\Phi(B)$.*

PROOF. Let $\mathcal{M}$, $\mathcal{N}$ be the families of open maximal subgroups of A, B, respectively. There is a 1–1 map $\mathcal{N} \to \mathcal{M}$ defined by

$$N \mapsto p^{-1}N;$$

if p is a Fr. cover, this map is obviously surjective. Hence

$$\Phi(A) = \bigcap_{M\in\mathcal{M}} M \subseteq \bigcap_{N\in\mathcal{N}} p^{-1}N = p^{-1}\Big(\bigcap_{N\in\mathcal{N}} N\Big) = p^{-1}\Phi(B),$$

and if p is a Fr. cover, the inclusion is equality, hence (a) and (b).

LEMMA 2.3. *Consider a cartesian square* (see Lemma 1.1)

$$\begin{array}{ccc} B & \xrightarrow[p_2]{} & B_2 \\ {\scriptstyle p_1}\downarrow & & \downarrow{\scriptstyle \Pi_2} \\ B_1 & \xrightarrow[\Pi_1]{} & A \end{array}$$

If p_1 is a Fr. cover, then so is Π_2.

PROOF. By 1.1 (d) we have

$$p_2(\ker p_1) = p_2(\ker p_1 \cdot \ker p_2) = p_2(\ker \Pi_2 \circ p_2) = \ker \Pi_2.$$

Now p_1 is a Fr. cover, thus $\ker p_1 \subseteq \Phi(B)$, and by Lemma 2.2(a)

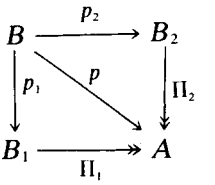
$$\ker \Pi_2 = p_2(\ker p_1) \subseteq p_2\Phi(B) \subseteq \Phi(B_2). \qquad \square$$

LEMMA 2.4. *Let $\varphi : H \to G$ be an epimorphism. Then there is an $H' \leqq H$ such that the restriction $\mathrm{Res}_{H'} \varphi : H' \to G$ is a Frattini cover.*

PROOF. H' is a minimal closed subgroup of H such that $\varphi(H') = G$. Its existence is proved in [5], 4.1. $\square$

LEMMA 2.5. (a) *Let $\Pi_i : B_i \twoheadrightarrow A$, $i = 1, 2$ be two epimorphisms. Then there exists a commutative diagram*

(1)



in which p is a Frattini cover;

(b) *under the same assumption there exists a commutative diagram* (1) *in which p_1 is a Fr. cover;*

(c) *if $\Pi_i : B_i \twoheadrightarrow A_i$, $i = 1, 2$ are Fr. cover, there exists a commutative diagram* (1) *in which p_1, p_2, p are Fr. covers.*

PROOF. By Lemma 1.1(a) we construct a diagram (1) in which p_1, p_2, p are epimorphisms. If B is replaced by a suitable subgroup and p_1, p_2, p by their restrictions, we obtain (a) (or (b)) by Lemma 2.4. But if Π_1, Π_2, p are Fr. covers, then so are p_1, p_2 by Lemma 2.1. $\square$

We now fix some terminology.

We recall that a group P is *projective* iff for every pair of epimorphisms $\varphi : P \twoheadrightarrow B$, $\Pi : A \twoheadrightarrow B$ there exists a homomorphism $\psi : P \to A$ such that $\Pi \circ \psi = \varphi$. An epimorphism $P \twoheadrightarrow G$ is called a *projective* cover of G iff P is projective.

Let G be an f.g. group. For two epimorphisms $\varphi_i : H_i \twoheadrightarrow G$, $i = 1, 2$ we shall write $\varphi_1 \geqq \varphi_2$ iff there is an epimorphism $\theta : H_1 \twoheadrightarrow H_2$ such that $\varphi_1 = \varphi_2 \circ \theta$. One readily sees that this pre-order relation defines a partial order on the family of all isomorphism classes of covers of G; however, by abuse of language we employ this notation rather for the covers of G. In this sense we use the words "largest" and "smallest".

Finally, a projective group which has the embedding property is called *superprojective.*

THEOREM 2.6. *Let G be an f.g. group. Then there exists a cover $\tilde{\varphi}: \tilde{G} \twoheadrightarrow G$, unique up to an isomorphism, satisfying the following equivalent conditions:*

(i) *$\tilde{\varphi}$ is a projective Frattini cover of G;*

(ii) *$\tilde{\varphi}$ is the largest Frattini cover of G;*

(iii) *$\tilde{\varphi}$ is the smallest projective cover of G.*

Such a cover $\tilde{\varphi}$ is called the *universal Frattini cover* of G.

The condition (ii) is taken as the definition of $\tilde{\varphi}$ in [7], while the condition (i) is taken as the definition of $\tilde{\varphi}$ in [3].

PROOF. Assume $\mathrm{rk}(G) = e$; then there is an epimorphism $\tilde{\rho}: \hat{F}_e \twoheadrightarrow G$. By Lemma 2.4 there is an $H \leqq \hat{F}_e$ such that $\rho = \mathrm{Res}_H \tilde{\rho}$ is a Frattini cover. Now $\hat{F}_e$ is projective, hence H is projective (see [5], theorem 2.5). Thus ρ is a projective Frattini cover.

We now show the equivalence of the conditions.

(i) $\Rightarrow$ (ii): Let $\varphi: H \twoheadrightarrow G$ be a Frattini cover; since $\tilde{G}$ is projective, there is a homomorphism $\psi: \tilde{G} \to H$ such that $\varphi \circ \psi = \tilde{\varphi}$. By Lemma 2.1(iii) ψ is surjective, hence $\tilde{\varphi} \geqq \varphi$.

(ii) $\Rightarrow$ (i): Let $\Pi_1: A \twoheadrightarrow B$, $\Pi_2: \tilde{G} \twoheadrightarrow B$ be two epimorphisms. By Lemma 2.5(b) there exists a commutative diagram

$$\begin{array}{ccccc} H & \xrightarrow{p_2} & \tilde{G} & \xrightarrow{\tilde{\varphi}} & G \\ \downarrow{\scriptstyle p_1} & & \downarrow{\scriptstyle \Pi_2} & & \\ A & \xrightarrow[\Pi_1]{} & B & & \end{array}$$

where p_2 is a Frattini cover. By Lemma 2.1(i) so is $\tilde{\varphi} \circ p_2$; hence $\tilde{\varphi} \geqq \tilde{\varphi} \circ p_2$, i.e., H is a quotient group of the finitely generated group $\tilde{G}$ ($\mathrm{rk}(\tilde{G}) = \mathrm{rk}(G)$). This implies that p_2 is an isomorphism, hence $\Pi_1 \circ p_1 \circ p_2^{-1} = \Pi_2$, which shows that $\tilde{G}$ is projective.

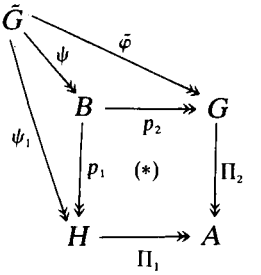
(i) $\Rightarrow$ (iii): Let $\varphi: P \twoheadrightarrow G$ be a projective cover of G. Then there is a homomorphism $\psi: P \to \tilde{G}$ such that $\tilde{\varphi} \circ \psi = \varphi$. By Lemma 2.1(ii) ψ is surjective, hence $\varphi \geqq \tilde{\varphi}$.

(iii) $\Rightarrow$ (i): Let $\rho: H \twoheadrightarrow G$ be a projective Frattini cover. Since $\tilde{\varphi} \leqq \rho$, there is an epimorphism $\psi: H \twoheadrightarrow \tilde{G}$ such that $\tilde{\varphi} \circ \psi = \rho$. By Lemma 2.1(iii) $\tilde{\varphi}$ is a Frattini cover.

The uniqueness of $\tilde{\varphi}$ is clear from (ii) or (iii). □

COROLLARY 2.7. *Let $\tilde{\varphi}: \tilde{G} \twoheadrightarrow G$ be the universal Frattini cover. Then H is a quotient group of $\tilde{G}$ iff H is a Frattini cover of a quotient group of G.*

PROOF. Assume that there exists an epimorphism $\psi_1 : \tilde{G} \twoheadrightarrow H$; by Lemma 1.2 there is a commutative diagram of epimorphisms



where the square (*) is cartesian; by Lemma 2.3, H is a Frattini cover of the quotient group A of G.

Conversely, assume that H is a Fr. cover of a quotient A of G, i.e., there are epimorphisms $\Pi : G \twoheadrightarrow A$, $\varphi : H \twoheadrightarrow A$. By the projectivity of $\tilde{G}$ there is a homomorphism $\psi : \tilde{G} \to H$ such that $\varphi \circ \psi = \Pi \circ \tilde{\varphi}$; by Lemma 2.1(ii), ψ is surjective, hence H is a quotient of $\tilde{G}$. □

Some other properties of the universal Fr. cover are contained in the next

PROPOSITION 2.8. (i) *The group $K = \ker \tilde{\varphi}$ is pro-nilpotent. Its p-Sylow subgroups S_p are free pro-p-groups and $K = \Pi_p S_p$. Moreover, K is superprojective.*

(ii) $p \,||\, G| \Leftrightarrow p \,||\, \tilde{G}|$, *for every prime p.*

(iii) $\tilde{G} \cong (G/\Phi(G))\tilde{}$.

PROOF. (i) From the finite analogue it is easily seen that the Frattini subgroup of a profinite group is pro-nilpotent. But $K \subseteq \Phi(\tilde{G})$, hence K is also pro-nilpotent. Therefore $K = \Pi_p S_p$. Now $\tilde{G}$ is a projective, hence (cf. [5], 2.5) every S_p is projective and thus even a free pro-p-group (cf. [10], theorem 4 and [15], theorem 6.5). By Lemma 1.3, S_p is even superprojective. It is now a straightforward exercise to show from this fact that $\Pi_p S_p$ is also superprojective.

(ii) $\Rightarrow$ clear; $\Leftarrow$: Assume that $p \nmid |G|$. Then S_p is the unique p-Sylow subgroup of $\tilde{G}$. Clearly S_p is a characteristic subgroup of K and K is normal in $\tilde{G}$; hence S_p is normal in $\tilde{G}$. By the Schur–Zassenhaus Theorem S_p has a complement H in $\tilde{G}$. Clearly $\tilde{\varphi}(H) = G$, and as $\tilde{\varphi}$ is a Frattini cover, $H = \tilde{G}$. Hence $S_p = 1$, whence $p \nmid |\tilde{G}|$.

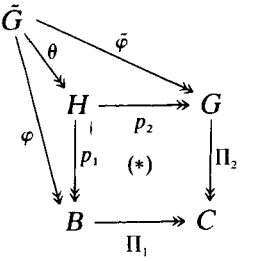
(iii) By Lemma 2.1(i) the composed map $\tilde{G} \overset{\tilde{\varphi}}{\twoheadrightarrow} G \twoheadrightarrow G/\Phi(G)$ is a Fr. cover; $\tilde{G}$ is projective hence this cover satisfies condition (i) of Theorem 2.6.

We now come to the main result of this section.

THEOREM 2.10. *Let G be an f.g. profinite group. If G has the embedding property, so does $\tilde{G}$, i.e., $\tilde{G}$ is superprojective.*

PROOF. Let A and B be quotient groups of $\tilde{G}$ and let $\varphi : \tilde{G} \twoheadrightarrow B$, $\Pi : A \twoheadrightarrow B$, be two epimorphisms; we have to show that there is a $\psi : \tilde{G} \twoheadrightarrow A$ such that $\Pi \circ \psi = \varphi$.

I. Assume first that $A = G$. By Lemma 1.2 the maps φ and $\tilde{\varphi}$ define a commutative diagram

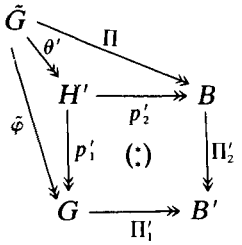


in which (*) is a cartesian square. By Lemma 2.1(iii) p_2 is a Fr. cover, hence for every $H' \leqq H : p_2(H') = G \Rightarrow H' = H$. This means that H is a minimal element in $\mathcal{H}(B, G)$. Thus by Lemma 1.7, (Π_1, Π_2) is a maximal pair in $\mathcal{P}(B, G)$. But G has the embedding property, hence by Lemma 1.10, (Π_1, Π_2) is trivial. Therefore Π_1, p_2 are isomorphisms.

By assumption there is an $\alpha \in \mathrm{Aut}(G)$ such that $p_1 \circ p_2^{-1} = \Pi \circ \alpha$. Put $\psi = \alpha \circ \tilde{\varphi}$; then

$$\Pi \circ \psi = (\Pi \circ \alpha) \circ \tilde{\varphi} = (p_1 \circ p_2^{-1}) \circ (p_2 \circ \theta) = p_1 \circ \theta = \varphi.$$

II. Assume that $A = \tilde{G}$. By Lemma 1.2 the maps $\tilde{\varphi}$ and Π define a commutative diagram



in which the square (:) is cartesian. By 1.1(iii) p_1' and θ' are Fr. covers.

By part I of this proof there exists a $\tilde{\psi} : \tilde{G} \twoheadrightarrow G$ such that $\Pi_1' \circ \tilde{\psi} = (\Pi_2' \circ \varphi)$. Therefore by Lemma 1.1 (b) there is a homomorphism $\psi' : \tilde{G} \to H'$ such that (i)

$p_1' \circ \psi' = \tilde{\psi}$ and (ii) $p_2' \circ \psi' = \varphi$. From (i) it follows by Lemma 2.1(ii) that ψ' is surjective. Since $\tilde{G}$ is a projective group, there is a homomorphism $\psi : \tilde{G} \to \tilde{G}$ such that $\theta' \circ \psi = \psi'$. Again by Lemma 2.1(ii) ψ is surjective. Finally by (ii)

$$\Pi \circ \psi = p_2' \circ \theta' \circ \psi = p_2' \circ \psi' = \varphi.$$

This ends the proof by Lemma 1.4. □

COROLLARY 2.11. *Let G be an f.g. group with a trivial Frattini subgroup. Then $\tilde{G}$ has the embedding property iff G has it.*

PROOF. By Lemma 2.2(b) it follows that $\Phi(\tilde{G}) = \tilde{\varphi}^{-1}\Phi(G) = \ker \varphi$, hence $G \cong \tilde{G}/\Phi(\tilde{G})$. Thus one implication follows by Lemma 1.5 and the other one by Theorem 2.10. □

REMARK. The condition $\Phi(G) = 1$ in the Corollary is essential: if G is the direct product of the cyclic groups C_p and C_{p^2} of orders p, p^2, respectively, G does not have the embedding property, as one readily sees. But $G/\Phi(G) = C_p \times C_p$ has the embedding property and so by Proposition 2.8(iii) and Theorem 2.10 $\tilde{G}$ has it as well. (In fact $\tilde{G}$ is the free pro-p-group on 2 elements $\hat{F}_2(p)$.)

Combining the universal properties of the universal embedding cover and of the universal Frattini cover one easily obtains

COROLLARY 2.12. *Let G be an f.g. group. Then $\widetilde{E(G)} = E(\tilde{G})$.*

3. Applications to Frobenius fields

Frobenius fields have been defined and studied in [8]; a decision procedure for certain subclasses of Frobenius fields has been given there. For our purposes it is convenient to take instead of the definition of a Frobenius field (see [8], section 1) the following equivalent characterization ([8], theorem 1.2):

PROPOSITION 3.1. *A field M is a Frobenius field iff*

(i) *M is* PAC, *i.e., every (non-empty) absolutely irreducible variety defined over M has an M-rational point; and*

(ii) *the absolute Galois group $G(M)$ of M has the embedding property.*

REMARK. In [4] this characterization serves as a definition of an Iwasawa field.

For some time it was not known whether every PAC field is a Frobenius field or not. As observed in [14], (4.8) the class $\{G(K) \mid K \text{ is a PAC field}\}$ and the class

of projective (profinite) groups coincide. Thus the above-mentioned problem is equivalent to the question, whether every projective group is *superprojective* (i.e., projective with the embedding property). First counter-examples were given by Ershov and Fried ([7], section 2) and by Cherlin, van den Dries and Macintyre ([4], 6.2). Our Corollary 2.11 generalizes (and simplifies the proof of validity of) these examples:

Take a finite group G which does not have the embedding property and for which $\Phi(G) = 1$. Then $\tilde{G}$ is projective but not superprojective. (Note that we do not use Theorem 2.10 here!) Construction of such a group G may be facilitated by the following Lemma.

LEMMA 3.2. (i) *Let G be a finite group, with $N_1, N_2 \lhd G$ such that $N_1 \not\cong N_2$ and $G/N_1 \cong G/N_2$, then G does not have the embedding property.*

(ii) *Let $A \lhd B$ be a semidirect product of finite groups A, B, not isomorphic to $A \times B$. Then $G = (A \lhd B) \times B$ does not have the embedding property.*

PROOF. (i) Otherwise there is a $\psi \in \mathrm{Aut}(G)$ such that $(\theta \circ \rho) \circ \psi = \varphi$ where $\rho : G \twoheadrightarrow G/N_1$, $\varphi : G \to G/N_2$ are the canonical maps and $\theta : G/N_1 \xrightarrow{\sim} G/N_2$; hence $N_2 = \ker \varphi = \ker(\theta \circ \rho) \circ \psi = \psi^{-1} N_1$, a contradiction to $N_1 \not\cong N_2$.

(ii) Let $N_1 = A \lhd B$, $N_2 = A \times B$ and apply (i). □

EXAMPLES. I. The example of [7], theorem 2.1 is just $G = S_3 \times C_2 = (C_3 \lhd C_2) \times C_2$, where C_n denotes the cyclic group of order n.

II. The example in [4], (6.2) is actually $G = D_q \times C_2 = (C_q \lhd C_2) \times C_2$, where q is an odd prime.

III. Let S be a finite simple non-abelian group, and let $n \geqq 5$. Denote

$$A = S^n = \underbrace{S \times \cdots \times S}_{n}.$$

The alternating group $B = A_n$ of degree $n \geqq 5$ acts on A, permuting the coordinates. One easily sees that a semidirect product of two groups with no non-trivial normal nilpotent subgroups has again no non-trivial normal nilpotent subgroups. Thus $N = A \lhd B$ has this property too.

For n sufficiently large (say, such that $|A_n| \nmid |S|^n$) $N \not\cong A \times B$. Indeed, otherwise there is a $B' \lhd N$ such that $B' \cong B$. Let $\Pi : N \twoheadrightarrow B$ be the canonical projection; then $\Pi(B') \lhd B$, B is simple, hence $\Pi(B') = 1$ or $\Pi(B') = B$. The first possibility yields $B' \subseteq \ker \Pi = A$, hence $|B| \mid |A|$, a contradiction. The other possibility implies $B' \cap A = 1$, hence $N = A \times B'$. But then $B' \subseteq C_N(A)$, whence $B = \Pi(N) = \Pi(B') \subseteq \Pi(C_N(A)) = \{b \in B \mid b$ acts as an inner au-

tomorphism on A}. This is a contradiction, since every $b \neq 1$ in B acts as an outer automorphism.

Thus by Lemma 3.2(ii) $C = N \times B$ does not have the embedding property; also, C has no non-trivial normal nilpotent subgroups; in particular $\Phi(C) = 1$.

Ax ([2], p. 268) and Roquette (unpublished) have shown that a finite extension of a PAC field is PAC. The material developed in Section 2 and the last example enable us to show that this property is not true for Frobenius fields, thereby answering problem 1.8 in [8].

PROPOSITION 3.3. (i) *There exists a tower of finite field extensions $K \subset L \subset M$ such that K and M are Frobenius fields and L is not.*

(ii) *There exists a projective group $\tilde{G}$ with open subgroups $I \subset H \subset \tilde{G}$ such that $\tilde{G}$ and I have the embedding property while H does not have it.*

PROOF. In view of the observations preceding Lemma 3.2, (i) follows from (ii).

To show (ii), let C be the group of Example III above. Embed C in a finite simple group G. (By Cayley's Theorem C can be embedded in a symmetric group S_m; now define an embedding $f: S_m \to A_{m+2}$ by

$$f(\tau) = \begin{cases} \begin{pmatrix} 1 & 2 & \cdots & m & m+1 & m+2 \\ \tau(1) & \tau(2) & \cdots & \tau(m) & m+1 & m+2 \end{pmatrix} & \operatorname{sg}\tau = 1 \\ \begin{pmatrix} 1 & 2 & \cdots & m & m+1 & m+2 \\ \tau(1) & \tau(2) & \cdots & \tau(m) & m+2 & m+1 \end{pmatrix} & \operatorname{sg}\tau = -1 \end{cases}, \quad \tau \in S_m. \qquad .)$$

Now let $\tilde{\varphi}: \tilde{G} \twoheadrightarrow G$ be the universal Frattini cover of G and let $I = \ker \tilde{\varphi}$, $H = \tilde{\varphi}^{-1}C$. By Corollary 2.11 $\tilde{G}$ has the embedding property, since the simple group G has it; so does I, by Proposition 2.8(i). Moreover, by this Proposition I is a normal pro-nilpotent subgroup of H. But since $H/I \cong C$ and C has no normal nilpotent subgroups (except 1), I is the largest normal pro-nilpotent subgroup of H (i.e., the Fitting subgroup), hence I is a characteristic subgroup of H. By Lemma 1.5 H does not have the embedding property, since C does not have it. □

Proposition 3.3 also shows that a finite extension of a non-Frobenius PAC field may be Frobenius. Moreover, problem 1.7 in [8] is answered by this, negatively, of course. The most important open problem of [8], as well as of [4] and [13], is solved in the next section.

4. Decidability of Frobenius fields

In this section we obtain primitive recursive procedures for theories of some classes of Frobenius fields, especially the theory of all perfect Frobenius fields (see problem 4.10 in [8 and section 7 in [4]).

Let $A_1, \cdots, A_m$, $B_1, \cdots, B_n$ be finite groups, $1 \leqq m$, $0 \leqq n$. Let

$$\mathscr{A} = \{A \leqq A_1 \times \cdots \times A_m \mid p_i(A) = A_i,\ i = 1, \cdots, m\},$$

where $p_1, \cdots, p_m$ are the coordinate projections. Recall that $E(A)$ denotes the universal embedding cover of A defined in Section 1.

LEMMA 4.1. *The following conditions are equivalent*:

(i) *there exists a superprojective group* Γ *such that*

$$A_1, \cdots, A_m \in \mathrm{Im}(\Gamma) \quad \textit{and} \quad B_1, \cdots, B_n \notin \mathrm{Im}(\Gamma);$$

(ii) *there exists an f.g. superprojective group* Γ *such that*

$$A_1, \cdots, A_m \in \mathrm{Im}(\Gamma) \quad \textit{and} \quad B_1, \cdots, B_n \notin \mathrm{Im}(\Gamma);$$

(iii) *there is an* $A \in \mathscr{A}$ *such that none of* $B_1, \cdots, B_n$ *is a Frattini cover of a quotient group of* $E(\mathscr{A})$.

PROOF. (i) $\Rightarrow$ (iii): By assumption there are maps $\psi_i : \Gamma \twoheadrightarrow A_i$, $i = 1, \cdots, m$. These define a $\psi : \Gamma \to A_1 \times \cdots \times A_m$ such that $p_i \circ \psi = \psi_i$, $i = 1, \cdots, m$. Thus $A = \mathrm{Im}\,\psi$ belongs to $\mathscr{A}$. By Theorem 1.12(b), $E(A) \in \mathrm{Im}(\Gamma)$; hence by Theorem 2.6(iii), $\tilde{E}(A)$ is a quotient of Γ. Therefore $B_1, \cdots, B_n \notin \mathrm{Im}(\tilde{E}(A))$, hence by Corollary 2.7 they are not Fr. covers of quotients of $E(A)$.

(iii) $\Rightarrow$ (ii): By Corollary 2.7 $B_1, \cdots, B_n \notin \mathrm{Im}(\Gamma)$, where $\Gamma = \tilde{E}(A)$, while $A_1, \cdots, A_m \in \mathrm{Im}(\Gamma)$, since they are quotients of A. The group $E(A)$ has the embedding property, hence by Theorem 2.10 Γ is superprojective. □

By Theorem 1.12 there clearly exists a primitive recursive algorithm to check the validity of condition (iii) in Lemma 4.1 for given groups $A_1, \cdots, A_m$, $B_1, \cdots, B_n$.

THEOREM 4.2. *Let* K *be a Hilbertian field with elimination theory. There is a primitive recursive decision procedure for the theory* $T(K)$ *of all perfect Frobenius fields containing* K.

[K is a field with elimination theory if the procedures of classical elimination theory may be effectively performed over K (see [8], a note following theorem 2.3). All finitely generated extensions of prime fields fall within this class.]

PROOF. Jarden ([13], theorem 1.2) has improved the decision procedure of [8] and reduced thereby the problem to Problem (C') in the Introduction. Thus our Theorem is now a Corollary of Lemma 4.1 and the remark following it. □

COROLLARY 4.3. *For every $p \geqq 0$ there is a primitive recursive decision procedure for the theory T_p of all perfect Frobenius fields of characteristic p.*

PROOF. For $p = 0$ apply Theorem 4.2 to $K = \mathbf{Q}$. For $p > 0$ let $K = \mathbf{F}_p(t)$ be the field of rational functions over the prime field $\mathbf{F}_p$. We claim that T_p is the set of all elementary sentences which are in $T(K)$. Indeed, if M is a perfect Frobenius field of characteristic p, then M is clearly infinite. Hence a sufficiently large ultrapower $^*M$ of M will be uncountable. In particular, $^*M$ contains a transcendental element over $\mathbf{F}_p$, hence we may assume that $^*M \supseteq K$. Thus $^*M$ is elementarily equivalent to M and it is a model of $T(K)$. □

THEOREM 4.4. *There is a primitive recursive decision procedure for the elementary theory of perfect Frobenius fields.*

A proof of Theorem 4.4 runs along the line of the decision procedures in [8] and [13], replacing the Galois covers over fields by Galois covers over rings (as they have been originally introduced in [9]). We intend to work out the details, which are essentially of an algebro-geometric nature, in a subsequent work.

Cherlin, van den Dries and Macintyre [4] have shown that the theory of all Frobenius fields is (recursively) decidable, if Problem (C') in our Introduction is decidable. Thus by Lemma 4.1 we have

COROLLARY 4.5. *The elementary theory of Frobenius fields is decidable.*

ACKNOWLEDGEMENT

The authors wish to express their gratitude to Moshe Jarden for many valuable discussions and for his constant interest and encouragement.

REFERENCES

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

2. J. Ax, *The elementary theory of finite fields*, Ann. of Math. **86** (1968), 239–271.

3. G. Cherlin, A. Macintyre and L. van den Dries, *Decidability and undecidability theorems for PAC fields*, Bull. Amer. Math. Soc. **4** (1981), 101–104.

4. G. Cherlin, A. Macintyre and L. van den Dries, *The elementary theory of p.a.c. fields*, a preprint.

5. J. Cossey, O. H. Kegel and L. G. Kovács, *Maximal Frattini extensions*, Arch. Math. **35** (1980), 210–217.

6. Yu. L. Ershov, *Regularly closed fields*, Doklady **251**, No. 4 (1980), 783–785.

7. Yu. Ershov and M. Fried, *Frattini covers and projective groups without the extension property*, Math. Ann. **253** (1980), 233–239.

8. M. Fried, D. Haran and M. Jarden, *Galois stratification over Frobenius fields*, Advances in Math., to appear.

9. M. Fried and G. Sacerdote, *Solving diophantine problems over all residue class fields and all finite fields*, Ann. of Math. **104** (1976), 203–233.

10. K. Gruenberg, *Projective profinite groups*, J. London Math. Soc. **42** (1967), 155–165.

11. M. Jarden, *Elementary statements over large algebraic fields*, Trans. Amer. Math. Soc. **164** (1972), 67–91.

12. M. Jarden, *The elementary theory of ω-free Ax fields*, Invent. Math. **38** (1976), 187–206.

13. M. Jarden, *Normal Frobenius fields*, a preprint.

14. A. Lubotzky and L. van den Dries, *Subgroups of free profinite groups and large subfields of $\tilde{\mathbf{Q}}$*, Israel J. Math. **39** (1981), 25–45.

15. P. Ribes, *Introduction of profinite groups and Galois cohomology*, Queen Papers in Pure and Applied Mathematics **24**, Queen's University, Kingston, Ontario, 1970.

TEL AVIV UNIVERSITY
TEL AVIV, ISRAEL

BAR ILAN UNIVERSITY
RAMAT GAN, ISRAEL