ADVANCES IN MATHEMATICS 51, 1–35 (1984)

Galois Stratification over Frobenius Fields

MICHAEL FRIED*

University of California, Irvine, California 92717

AND

DAN HARAN† AND MOSHE JARDEN‡

Tel-Aviv University, Tel-Aviv, Israel

INTRODUCTION

Let K be an infinite field finitely generated over its prime field. Denote by $G(K) = \mathcal{G}(K_s/K)$ the absolute Galois group of K. The set $G(K)^e$, for e a positive integer, is equipped with the normalized Haar measure, $\mu = \mu_e$, induced from the measure of $G(K)$ that assigns to $G(L)$ the value $1/[L:K]$, if L/K is a finite separable extension. If $\sigma = (\sigma_1, \ldots, \sigma_e) \in G(K)^e$, then we denote by $\tilde{K}(\sigma)$ the fixed field of $\sigma_1, \ldots, \sigma_e$ in $\tilde{K}$ (= the algebraic closure of K). Denote also by $\mathcal{L}(K)$ the first-order language of fields enriched with constant symbols for the elements of K. For every sentence θ of $\mathcal{L}(K)$ we define $A_e(\theta) = \{\sigma \in G(K)^e \mid \tilde{K}(\sigma) \models \theta\}$. Further we denote by $T_e(K)$ the theory of all sentences θ of $\mathcal{L}(K)$ with $\mu(A_e(\theta)) = 1$. In [13, Theorem 7.3] the following is shown.

A. A field F that contains K is a model of $T_e(K)$ if and only if it satisfies the following conditions:

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

(b) F is perfect (a perfect *PAC* field is also called an *Ax*-field); and

(c) F is *e-free*, i.e., $G(F) \cong \hat{F}_e$ = the free profinite group on e generators.

* Partially supported by NSF Grant MCA 76-07159 and BSF Grant 1546/78.

† Partially supported by a Minerva grant.

‡ Partially supported by a BSF Grant 1546/78, money from the University of California, Irvine, and a Minerva grant.

0001-8708/84 $7.50

In [11] the theory

$$T_\omega(K) = \bigcup_{e_0=1} \bigcap_{e=e_0} T_e(K)$$

is considered and in [11, Theorem 7.1] the following result appears:

B. A field F that contains K is a model of $T_\omega(K)$ if and only if:

(a) F is an Ax-field;

(b) F is ω-free, i.e., every embedding problem of finite groups over F is solvable.

In addition the following theorem is proved in [13] and [11].

C. (a) *If* θ is a sentence of $\mathscr{L}(K)$, then $\mu(A_e(\theta))$ is a rational number;

(b) there exists an $e_0 = e_0(\theta)$ such that $\theta \in T_\omega(K)$ if and only if $\theta \in T_e(K)$ for every $e \geqslant e_0$; and

(c) the theories $T_e(K)$ and $T_\omega(K)$ are decidable, and the functions $\mu(A_e(\theta))$ and $e_0(\theta)$ are computable.

The method of proof of Theorems A, B and C is model-theoretic and extensive use is made of ultra-products. The process of proof of Theorem C(c) associates to a given sentence θ of $\mathscr{L}(K)$ a boolean combination θ_1 of sentences of the form $(\exists x)[f(x) = 0]$, with $f \in K[x]$. Then, θ_1 is equivalent to θ modulo $T_e(K)$, and one can check directly whether or not $\theta_1 \in T_e(K)$. The transition from θ to θ_1 occurs, however, by virtue of Gödel's completeness theorem and its production therefore compels one to search for a proof of $\theta \to \theta_1$ among the sequence of sentences of $\mathscr{L}(K)$. In the context of actually deciding the truth of a sentence of $\mathscr{L}(K)$ the sequence of formal proofs, formed from a system of axioms of $T_e(K)$, is an abstract concept. In technical terms, this format suffices to show that $T_e(K)$ is a recursive theory: some process terminates with a yes or no answer to the truth of the original sentence. In practical terms, however, no sentence could be said to yield to the process, since, in particular, a priori there is no bound, even for the simplest sentences, on the number of steps of computation before the process terminates.

The above Theorems and their proofs are modelled after Ax' treatment [2] of the theory of finite fields. As for $T_e(K)$ and $T_\omega(K)$, Ax proves that the theory T of sentences of $\mathscr{L}(Z)$ true in $\mathbb{F}_p$ for all primes p is recursive. Fried and Sacerdote [5] improve this result and prove that T is even *primitive recursive*. Indeed, Fried and Sacerdote use explicit-geometric constructions in order to eliminate quantifiers from a given sentence θ given in a prenex normal form. This procedure does not take place within the language $\mathscr{L}(K)$.

It is necessary to consider more general sentences than those belonging to $\mathscr{L}(K)$. These generalized sentences are called *Galois sentences*, and the whole procedure is called *elimination of quantifiers through Galois stratification.*

In the present work we use the idea of Galois stratification in order to obtain a primitive recursive decision procedure for the theories $T_e(K)$ and $T_\omega(K)$. Moreover, the method itself has been considerably simplified and the results apply to a more general situation.

We consider therefore a perfect field M that contains the given field K. Denote by $\mathscr{C} = \mathscr{C}(M)$ the family of all finite groups that can be realized over M as Galois groups and assume that $\mathscr{C}$ is primitive recursive. By a *ring-cover, S/R, over K* we mean an integrally closed integral domain R which is finitely generated over K and an integral extension $S = R[z]$ of R such that the discriminant of z over R is a unit of R. If the quotient field F of S is Galois over the quotient field E of R, then we say that S/R is a *Galois-ring-cover.* In this case we denote $\mathscr{G}(S/R) = \mathscr{G}(F/E)$. The field M is now assumed to be a *Frobenius field*, i.e., M is assumed to satisfy the following condition:

If S/R is a Galois-ring-cover over M such that E is regular over M and $\mathscr{G}(S/R)$ belongs to $\mathscr{C}$, then there exists an M-homomorphism φ of S onto an extension N of M such that $\varphi(R) = M$ and $[F: E] = [N: M]$.

A *basic set* over K is a set of the form $A = V - V(g)$, where V is a K-irreducible algebraic set in an affine space $\mathbb{A}^n$ and $g \in K[X_1, ..., X_n]$ is a polynomial that does not vanish on V. If $x = (x_1, ..., x_n)$ is a generic point of V over K, then $K[A] = K[x, g(x)^{-1}]$ is said to be the *coordinate ring* of A. The set A is said to be *K-normal* if $K[A]$ is integrally closed. If this is the case and C is an additional K-normal basic set such that $K[C]/K[A]$ is a ring-cover, then C/A is called a *set-cover.* Let $A(M)$ be the M-rational points of A. Suppose that C/A is a Galois set-cover and let $a \in A(M)$. Then the specialization $x \to a$ can be extended to a K-homomorphism φ of $K[C]$ into $\tilde{M}$. The field $N = M \cdot \varphi K[C]$ is a Galois extension of M and there is an isomorphism φ^* of $\mathscr{G}(N/M)$ onto a subgroup $D_M(\varphi)$ of $\mathscr{G}(C/A)$, called the *decomposition group* of φ with respect to M. The conjugacy class of subgroups $\mathrm{Ar}_{A,M}(a) = \{D_M(\varphi)^\tau \mid \tau \in \mathscr{G}(C/A)\}$ is called the *Artin symbol* of a with respect to M.

A *Galois stratification* of $\mathbb{A}^n$ (with respect to K and $\mathscr{C}$) is a system

$$\mathscr{A} = \langle \mathbb{A}^n, C_i \to A_i, \mathrm{Con}(A_i) \rangle_{i \in I},$$

where $\mathbb{A}^n = \bigcup_{i \in I} A_i$ is a disjoint union of K-normal basic sets A_i, and for each $i \in I$, $C_i \to A_i$ are Galois set-covers equipped with a family of subgroups $\mathrm{Con}(A_i)$ of $\mathscr{G}(C_i/A_i)$ belonging to $\mathscr{C}$ and closed under conjugation. We very much allow the possibility that $\mathrm{Con}(A_i)$ might be empty for one or more

values of i. If $a \in \mathbb{A}^n(M)$, then we write $\mathrm{Ar}_{\mathscr{A},M}(a) \subseteq \mathrm{Con}(\mathscr{A})$ if for the unique $i \in I$ with $a \in A_i$ we have $\mathrm{Ar}_{A_i,M}(a) \subseteq \mathrm{Con}(A_i)$. The main result of this work is the following

THEOREM D. *Let $n \geqslant 0$ be an integer and denote by $\pi: \mathbb{A}^{n+1} \to \mathbb{A}^n$ the projection map on the first n coordinates. Suppose that $\mathscr{A}$ is a given Galois stratification of $\mathbb{A}^{n+1}$ with respect to K and $\mathscr{C}$. Then we can explicitly find a Galois stratification $\mathscr{B}$ of $\mathbb{A}^n$ (that does not depend on M) such that for each $b \in \mathbb{A}^n(M)$ we have: $\mathrm{Ar}_{\mathscr{B},M}(b) \subseteq \mathrm{Con}(\mathscr{B})$ if and only if there exists an $a \in \mathbb{A}^{n+1}(M)$ such that $\pi(a) = b$ and $\mathrm{Ar}_{\mathscr{A},M}(a) \subseteq \mathrm{Con}(\mathscr{A})$.*

Once we have this Theorem we may consider a Galois stratification $\mathscr{A}$ of $\mathbb{A}^n$ and n quantifiers $Q_1,\ldots,Q_n$ and define the expression θ_n,

$$(Q_1 X_1)\cdots(Q_n X_n)[\mathrm{Ar}(X_1,\ldots,X_n) \subseteq \mathrm{Con}(\mathscr{A})]$$

as a *Galois sentence*. We write $M \models \theta_n$ if $Q_1 a_1 \in M$, $Q_2 a_2 \in M,\ldots, Q_n a_n \in M$, we have $\mathrm{Ar}_{\mathscr{A},M}(a_1,\ldots,a_n) \subseteq \mathrm{Con}(\mathscr{A})$. It is not difficult to show that every sentence φ of $\mathscr{L}(K)$ written in a prenex normal form with n quantifiers is equivalent (over M) to a Galois sentence θ_n. The Main Theorem enables us to explicitly construct a Galois sentence θ_0 without quantifiers which is equivalent to θ_n. Thus we have the following

COROLLARY E. *Given a sentence φ of $\mathscr{L}(K)$ we can explicitly find a finite Galois extension L of K and a family* Con *of subgroups of $\mathscr{G}(L/K)$ belonging to $\mathscr{C}$ which is closed under conjugation such that $M \models \varphi$ if and only if $\mathscr{G}(L/L \cap M) \in$ Con.*

We deduce a decision procedure from Corollary E.

THEOREM F. *If the family $\mathscr{C}$ is primitive recursive, then the theory of sentences of $\mathscr{L}(K)$ that are true in every Frobenius field N that contains K and satisfies $\mathscr{C}(N) = \mathscr{C}$ is primitive recursive.*

In Section 1 of this work it is proved that if N is a PAC field and $G(N)$ is a free profinite group or a free pro-p-group, for a prime p, then N is a Frobenius field. As a result of Corollary E we obtain ultra-product-free proof of Theorems A, B and C, where now the terms "decidable" and "computable" are to be understood in the sense of primitive recursive.

In addition, if we denote by $T_e(K,p)$ (resp., $T_\omega(K,p)$) the theory of sentences in $\mathscr{L}(K)$ that are true in all Ax-fields N containing K such that $G(N)$ is the free pro-p-group with e (resp. $\aleph_0$) generators we have:

COROLLARY G. *The theories $T_e(K,p)$ and $T_\omega(K,p)$ are primitive recursive.*

1. Frobenius Fields

Let K be a field, let $R \subseteq S$ be integral domains which are finitely generated over K, and let $E \subseteq F$ be their respective quotient fields. Assume that F/E is finite and separable.

In this setup we define S/R to be a *ring-cover* over K, and we define F/E to be the *corresponding field-cover*, if R is integrally closed and if $S = R[z]$, where z is integral over R and the discriminant d of z over E is a unit of R.

In this case $d \cdot x \in R[z]$ for every element x of F which is integral over R (cf. Zariski–Samuel [29, p. 264]). Hence S is the integral closure of R in F. We say that z is a *primitive element for the cover* S/R.

If in addition F/E is a Galois extension, then S/R and F/E are said to be a Galois-ring-cover and a *Galois-field-cover*, respectively, over K. If E is a regular extension of K, then these covers are said to be *regular*.

Let φ be a K-homomorphism of S into $\tilde{K}$ and let M be an algebraic extension of φR. (We do not assume here that S/R is regular.) Then $N = M(\varphi S) = M(\varphi z)$ is a finite Galois extension of M (cf. Lang [17, p. 246]). The *decomposition group* of φ (with respect to M) is

$$D_M(\varphi) = \{\varepsilon \in \mathcal{G}(F/E) \mid (\forall x \in S)[\varphi x \in M \Rightarrow \varphi \varepsilon x = \varphi x]\}. \tag{1}$$

For every $\varepsilon \in D_M(\varphi)$ we can define an automorphism $\varepsilon' \in \mathcal{G}(N/M)$ by $\varepsilon' \varphi x = \varphi \varepsilon x$, where $x \in S$. Then the map $\varepsilon \mapsto \varepsilon'$ is an isomorphism of $D_M(\varphi)$ onto $\mathcal{G}(N/M)$ (as follows, e.g., from Proposition 15 of [17, p. 248]). We denote its inverse by φ^*.

In this section we are interested only in the case where $K = M$. We therefore write $D(\varphi)$ for $D_M(\varphi)$ and note that

$$D(\varphi) = \{\varepsilon \in \mathcal{G}(F/E) \mid (\forall x \in S)[\varphi x = 0 \Rightarrow \varphi \varepsilon x = 0]\}.$$

A finite group G is said to be *realizable* over M if M has a Galois extension N with a Galois group isomorphic to G. We denote the family of all finite groups which are realizable over M by $\mathscr{C}(M)$. Note that the decomposition groups $D_M(\varphi)$ above belong to $\mathscr{C}(M)$. Note also that $\mathscr{C}(M)$ is closed under the operation of taking quotient groups.

Definition. A field M is said to be a *Frobenius field* if it satisfies one (and hence all) of the following equivalent conditions:

(A) Suppose that S/R is a regular Galois-ring-cover over M with F/E the corresponding field-cover; N is the algebraic closure of M in F; and H is a subgroup of $\mathcal{G}(F/E)$ that belongs to $\mathscr{C}(M)$ and satisfies the condition $\mathrm{Res}_N H = \mathcal{G}(N/M)$. Then there exists an M-homomorphism $\varphi: S \to \tilde{M}$ such that $\varphi R = M$ and $D(\varphi) = H$.

(B) Suppose that S/R is a regular Galois-ring-cover of M with F/E

the corresponding field-cover and $\mathcal{G}(F/E) \in \mathscr{C}(M)$. Then there exists an M-homomorphism $\varphi: S \to \tilde{M}$ such that $\varphi R = M$ and $D(\varphi) = \mathcal{G}(F/E)$.

(C) Suppose that F/E is a regular Galois field-cover over M such that $\mathcal{G}(F/E) \in \mathscr{C}(M)$, and $u_1, \ldots, u_m$ are elements of F. Then there exists an $\tilde{M}$-valued M-place φ of F which is finite at $u_1, \ldots, u_m$ such that $\varphi E = M$ and $D(\varphi) = \mathcal{G}(F/E)$.

Here φE is the residue field of E under φ and

$$D(\varphi) = \{\varepsilon \in \mathcal{G}(F/E) \mid (\forall x \in F)[\varphi x = 0 \Rightarrow \varphi \varepsilon x = 0]\}$$

is the *decomposition group* of φ.

We have to prove the equivalence of the conditions.

(A) $\Rightarrow$ (B): This follows from the fact that, in the situation of (B), the algebraic closure N of M in F is a finite Galois extension of M which is linearly disjoint from E over M. In particular the restriction map $\mathrm{Res}: \mathcal{G}(F/E) \to \mathcal{G}(N/M)$ is surjective.

(B) $\Rightarrow$ (C): By considering the irreducible polynomials of $u_1, \ldots, u_m$ over E we can find a ring $R = M[x_1, \ldots, x_n]$ with E as its quotient field such that each of the u_i is integral over R. By Lemma 2.15 we may assume that R is integrally closed and that if S is the integral closure of R in F, then S/R is a regular Galois-ring-cover. In particular we have that $x = (x_1, \ldots, x_n)$ is a generic point of an absolutely irreducible variety V defined over M. Replacing R by $R[j^{-1}]$, where $j \in R[x]$ is the Jacobian of V, if necessary, we can assume that V is non-singular.

By (B) there exists now an M-homomorphism $\varphi_0: S \to \tilde{M}$ such that $\varphi_0 R = M$ and $D(\varphi_0) = \mathcal{G}(F/E)$. By a well-known theorem in algebraic geometry, $\mathrm{Res}_R \varphi_0$ can be extended to an M-place φ_1 of E with M as the residue field (cf. Jarden–Roquette [14, p. 45]).

Let z be a primitive element for the ring-cover S/R and let $b = \varphi_0 z$. Then $F = E[z] \cong E \otimes_R S$. Hence there exists an $\tilde{M}$-valued M-place φ of F that extends both φ_0 and φ_1 such that $\varphi F = \varphi_0 S = M(b)$. We have only to prove that $D(\varphi) = \mathcal{G}(F/E)$. Indeed, denote by R' the valuation ring of φ in E and let $S' = R'[z]$. Then S' is the integral closure of R' in F and therefore the valuation ring of φ in F is the localization of S' with respect to the center of φ in S' (cf. Lang [16, p. 18]). It follows that

$$D(\varphi) = D(\mathrm{Res}_{S'} \varphi) \cong \mathcal{G}(M(b)/M) \cong D(\varphi_0).$$

The equality $D(\varphi) = D(\varphi_0)$ follows now from the obvious inclusion $D(\varphi) \subseteq D(\varphi_0)$.

(C) $\Rightarrow$ (A): In the situation of (A) denote by E' the fixed field of H in F. Then the condition $\mathrm{Res}_N H = \mathcal{G}(N/M)$ implies that N and E' are linearly disjoint over M and hence that E' is a regular extension of M. The ring S is finitely generated over M. Hence, by (C), there exists an $\tilde{M}$-valued

M – place φ of F which is finite on S and satisfying $\varphi E' = M$ and $D(\varphi) = \mathcal{G}(F/E') = H$. The restriction of φ to S is the desired homomorphism of Condition (A).

Remark. It follows from the arguments in the proof (B) $\Rightarrow$ (C) that in the situation of (C) the place φ can be chosen in such a way that $P = \varphi F$ is a Galois extension of M and that φ induces an isomorphism $\varphi^*: \mathcal{G}(P/M) \to \mathcal{G}(F/E)$, exactly as above, satisfying $\sigma(\varphi x) = \varphi((\varphi^* \sigma)\, x)$ for every $\sigma \in \mathcal{G}(P/M)$ and $x \in F$ with $\varphi x \neq \infty$.

We recall that a field M is said to be PAC if every absolutely irreducible non-empty variety V defined over M has an M-rational point. This is equivalent to saying that if R is a finitely generated integral domain over M with a quotient field regular over M, then there exists an M-homomorphism $\varphi: R \to M$. Using the same argument as in the proof of (B) $\Rightarrow$ (C) one sees that if M is a PAC field, E is a finitely generated regular field extension of M and $u_1, \ldots, u_m \in E$, then E has an M-place φ which is finite at $u_1, \ldots, u_m$ and has M as a residue field. Conversely, if M has this last property, then it is also PAC. It is clear that if M is a Frobenius field, then it is PAC. Indeed, take $E = F$ and apply C.

If G is a profinite group, then we denote by $\mathscr{C}(G)$ the family of all quotient groups of G by normal open subgroups. We say that G has the *embedding property* if for every normal open subgroup N and every epimorphism $\beta: B \to G/N$, with $B \in \mathscr{C}(G)$, there exists a continuous epimorphism $\theta: G \to B$ such that $\beta \circ \theta$ is the canonical restriction map.

The absolute Galois group of a field M is the Galois group of the maximal separable extension M_S of M over M. It is denoted by $G(M)$. Clearly $\mathscr{C}(G(M)) = \mathscr{C}(M)$. Thus, we say that M has the *embedding property* if $G(M)$ has it.

We now show that the Frobenius property of a field, which is a mixture of field properties and Galois-group properties, is equivalent to the conjunction of a pure field theoretic property, namely PAC, and a pure Galois group theoretic property, namely the embedding property. To do this we need the following:

LEMMA 1.1. *Let N be a finite Galois extension of a field M and let G be a finite group with an epimorphism $\pi: G \to \mathcal{G}(N/M)$. Then there exists a regular Galois field-cover F/E over M such that N is the algebraic closure of M in F and an isomorphism $\tau: G \simeq \mathcal{G}(F/E)$ such that the following diagram is commutative.*

$$\begin{array}{ccc} G & \xrightarrow{\tau} & \mathcal{G}(F/E) \\ & {\scriptstyle\pi}\searrow \quad \swarrow{\scriptstyle \mathrm{Res}} & \\ & \mathcal{G}(N/M) & \end{array}$$

Proof. Let $X = \{x^g | g \in G\}$ be a set of $|G|$ algebraically independent elements over M. The group G acts on X from the right in the obvious manner. It also acts on N through π by the formula $a^g = a^{\pi(g)}$. It follows that G acts on the field $F = N(X)$. Let E be the fixed field of G in F. Then $N \cap E = M$. Also NE, as a subfield of a rational function field over N, is a regular extension of N. It follows that E is a regular extension of M. Identifying G with $\mathcal{G}(F/E)$ in the obvious way we obtain the desired commutative diagram. ∎

THEOREM 1.2. *A field M is a Frobenius field if and only if it is* PAC *and has the embedding property.*

Proof. Suppose first that M is a Frobenius field. We have to show that M has the embedding property. Indeed, let N be a finite Galois extension of M and let $\pi: G \to \mathcal{G}(N/M)$ be an isomorphism, with $G \in \mathscr{C}(M)$. Let E, F, and τ be as in Lemma 1.1. From property C, there exists an $\tilde{M}$-valued M-place φ of F such that $\varphi E = M$ and the isomorphism $\varphi^*: \mathcal{G}(P/M) \to \mathcal{G}(F/E)$ is defined, where $P = \varphi F$. The restriction of φ to N is an M-automorphism. Without loss of generality we may assume that $\mathrm{Res}_N \varphi$ is the identity. Then $\tau^{-1} \circ \varphi^*: \mathcal{G}(P/M) \to G$ is an isomorphism and $\pi \circ \tau^{-1} \circ \varphi^*: \mathcal{G}(P/M) \to \mathcal{G}(N/M)$ is the restriction map.

Conversely,[1] suppose that M is a PAC field which has the embedding property. Let F/E be a regular Galois cover of fields over M such that $\mathcal{G}(F/E) \in \mathscr{C}(M)$ and let $u_1, \ldots, u_m \in F$. Denote by N the maximal algebraic extension of M contained in F. By the embedding property of M, there exists a Galois extension P of M that contains N and there exists an isomorphism $j: \mathcal{G}(P/M) \to \mathcal{G}(F/E)$ such that $\mathrm{Res}_N j(\sigma) = \mathrm{Res}_N \sigma$ for every $\sigma \in \mathcal{G}(P/M)$. Let $N' = NE$, $P' = PE$, and $Q = PF$. The fields P and E are linearly disjoint over M, hence the isomorphism $\mathrm{Res}: \mathcal{G}(P'/E) \to \mathcal{G}(P/M)$ composed with j gives an isomorphism $h: \mathcal{G}(P'/E) \to \mathcal{G}(F/E)$ such that the following diagram is commutative:

$$\begin{array}{ccc} \mathcal{G}(P'/E) & \xrightarrow{h} & \mathcal{G}(F/E) \\ & {\scriptstyle \mathrm{Res}} \searrow \quad \swarrow {\scriptstyle \mathrm{Res}} & \\ & \mathcal{G}(N'/E) & \end{array}$$

We use h to define a subgroup

$$\Delta = \{\delta \in \mathcal{G}(Q/E) | h(\mathrm{Res}_{P'} \delta) = \mathrm{Res}_F \delta\}$$

[1] The idea of the following argument is taken from the notes [23] of Peter Roquette on Hilbert's Irreducibility Theorem. The authors thank Roquette for his kind permission to use this material.

of $\mathcal{G}(Q/E)$. The definition immediately implies that

$$\Delta \cap \mathcal{G}(Q/P') = \Delta \cap \mathcal{G}(Q/F) = 1.$$

Further, it is also true that

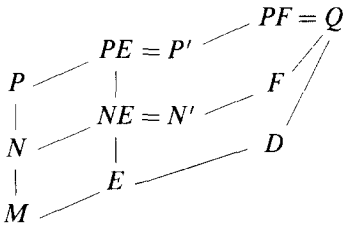
$$\Delta \cdot \mathcal{G}(Q/P') = \Delta \cdot \mathcal{G}(Q/F) = \mathcal{G}(Q/E).$$

Indeed, $Q = P' \otimes_{N'} F$. Hence, given an $\varepsilon \in \mathcal{G}(Q/E)$ there exists a $\delta \in \mathcal{G}(Q/E)$ such that $\mathrm{Res}_{P'}\delta = \mathrm{Res}_{P'}\varepsilon$ and $\mathrm{Res}_F \delta = h(\mathrm{Res}_{P'}\varepsilon)$. Then $\delta \in \Delta$ and $\delta^{-1}\varepsilon \in \mathcal{G}(Q/P')$.

The fixed field D of Δ in Q therefore satisfies the following relations:

$$P'D = FD = Q \qquad \text{and} \qquad P' \cap D = F \cap D = E.$$

In particular it follows that D is a regular extension of M, since $Q = PF$ is a regular extension of P.



Let z be a primitive element for the extension P/M. It can be written in the form $z = \sum_{i=1}^{n} d_i x_i$, where $d_i \in D$ and $x_i \in F$ for $i = 1,\ldots, n$. Since M is PAC, there exists an $M-$place ψ_0 such that $\psi_0 D = M$ and such that all the x_i, d_i, u_j are integral over the valuation ring of ψ_0. The place ψ_0 can be extended to a P-place ψ of Q such that $\psi Q = P$. Then $\varphi = \mathrm{Res}_F \psi$ is an M-place of F such that $\varphi E = M$ and $\varphi F = P$, since $z = \psi z = \sum_{i=1}^{n} \psi(d_i)\,\varphi(x_i) \in \varphi F$. Also $|P:M| = |F:E|$, hence $D(\varphi) = \mathcal{G}(F/E)$. ∎

Remark. Observe that the M-place φ constructed above has the property that $\varphi^* = j$, i.e., if $\tau \in \mathcal{G}(F/E)$, then

$$\varphi(\tau x) = (j^{-1}\tau)(\varphi x) \tag{2}$$

for every $x \in F$ such that $\varphi x \neq \infty$. Indeed, extend τ to an element δ of $\Delta = \mathcal{G}(Q/D)$. Then the relation

$$\psi(\delta x) = \delta(\psi x) \tag{3}$$

holds for every $x \in P$ and every $x \in D$, as follows immediately from the definitions. Hence (3) holds for every $x \in Q$ with $\psi x \neq 0$. In particular (3)

holds for every $x \in F$. Relation (2) follows from (3), since as $\delta \in \Delta$ we have $j^{-1}\tau = j^{-1}\,\mathrm{Res}_F \delta = \mathrm{Res}_{P'}\delta$. ∎

Let F be a profinite group generated by a set S converging to 1. We say that S is a *set of free generators* (with respect to the family $\mathscr{C}(F)$) if every continuous map $f: S \to G$, with $G \in \mathscr{C}(F)$ such that $f(S)$ generates G, can be extended to an epimorphism $f: F \to G$.

LEMMA 1.3. *If F admits a set of free generators, then F has the embedding property.*

Proof. If S is a finite set, then the Lemma follows from a Lemma of Gaschütz (see Jarden–Kiehne [13, Lemma 4.1]). If S is infinite, one can imitate an argument of Iwasawa in [22, p. 84] to derive the desired proof. ∎

COROLLARY 1.4. *If M is PAC field and $G(M)$ admits a set of free generators then M is a Frobenius field.*

Remark. Actually, if M is as in the Corollary, it satisfies a stronger property, called the *Čebotarev property*. We explain this:

Let F/E be a regular Galois cover over M with N as the algebraic closure of M in F. Suppose that $\mathscr{G}(F/E) \in \mathscr{C}(M)$ and that we are given a continuous map f of a set S of free generators of $G(M)$ into $\mathscr{G}(F/E)$ such that $\mathrm{Res}_N \sigma = \mathrm{Res}_N f(\sigma)$ for every $\sigma \in S$. Then there exists an M-place φ of F with $\varphi E = M$, $\varphi F = P$ for which φ^* is defined and satisfies $\varphi^*(\mathrm{Res}_P \sigma) = f(\sigma)$ for every $\sigma \in S$.

Indeed, replacing E, if necessary, by the fixed field in F of $f(S)$, we can assume that $f(S)$ generates $\mathscr{G}(F/E)$. Extend f to an epimorphism, also called f, from $G(M)$ onto $G(F/E)$ and let P be the fixed field of the kernel of f. Denote by j the isomorphism of $\mathscr{G}(P/M)$ onto $\mathscr{G}(F/E)$ induced by f. Our assertion follows now from Theorem 1.2 and the Remark following that Theorem.

Two special cases of profinite groups with a set of free generators are known in the literature: let $\mathscr{C}$ be a family of finite groups of one of the two following types:

I. The family $\mathscr{C}$ is closed under the operations of taking subgroups, quotient groups and direct products;

II. The decomposition factors of every $G \in \mathscr{C}$ belong to a fixed set Δ of simple groups.

Then for every set S there exists a unique free *pro-$\mathscr{C}$-group* $\hat{F}_S(\mathscr{C})$ on *the set* S with S a set of free generators (see Ribes [22, p. 61] for type I and Mel'nikov [20, Section 2] for type II).

A field M is said to be $\mathscr{C}$, *S-free*, if $G(M) = \hat{F}_S(\mathscr{C})$. If $\mathscr{C}$ is the family of

all finite groups (resp. finite p-groups) we shorten this to the phrase *S-free* (resp. *p, S-free*) field. In particular, if S is a set of e elements or S is countable, we use the expressions e-free and ω-free (resp. p, e-free and p, ω-free).

We recall that a perfect PAC field is called an Ax-field. The following special case of Corollary 1.4 is important for the applications.

COROLLARY 1.5. *An Ax S-free field is a Frobenius field. Moreover, every set S of free generators of $G(M)$ has the Čebotarev property.*

If K is a countable Hilbertian field and e is a positive integer, then for almost all $\sigma \in G(K)^e$, the field $\tilde{K}(\sigma)$ is an Ax e-free field (see [13, Lemma 7.2]). Corollary 1.5 therefore implies:

COROLLARY 1.6. *Let K be a countable Hilbertian field. Then almost all e-tuples $\sigma \in \mathscr{G}(K)^e$ have the Čebotarev property.*

Remark. Corollary 1.6 is proved directly in [12, Theorem 2.2]. The superior proof given here solves the problem, left open in that paper, of whether the e-free and PAC properties together imply the Cebotarev property.

The above results give rise to some questions concerning the absolute Galois group of a Frobenius field. First, we note that the converse of Lemma 1.3. is not true. Indeed, the group $G = \hat{F}_2(2) \times \hat{F}_3(3)$ has the embedding property (since every homomorphic image of G is a product of images of $\hat{F}_2(2)$ and $\hat{F}_3(3)$), while no set $S = \{(\sigma_{2i}, \sigma_{3i})\}_{i \in I} \subseteq G$ is a set of free generators (since then $\{\sigma_{pi}\}_{i \in I}$ would be a set of free generators for $\hat{F}_p(p)$, $p = 2, 3$; however, as is easily verified, any set of free generators for $\hat{F}_e(p)$ has precisely e elements). However, open subgroups of free pro-C-groups of type II are again free pro-groups (see Mel'nikov [20, Proposition 2.1]) and hence have the embedding property. We therefore ask:

Problem 1.7. Do open subgroups of torsion-free profinite groups with embedding property also have this property?

The condition of being torsion free is essential, as there are subgroups of finite simple groups that do not have the embedding property.

It is known that an algebraic extension of a PAC field is again PAC (see *Ax* [2, p. 268] for the separable extension case and Roquette [23] for the purely inseparable extension case). A positive solution to Problem 1.7 will therefore also imply, by Theorem 1.2, a positive solution to the following problem:

Problem 1.8. Is a finite algebraic extension of a Frobenius field also a Frobenius field?

The connection between Frobenius fields and Hilbertian fields goes

beyond Corollary 1.6. Indeed, it follows immediately from the definitions, that every Frobenius field M with $G(M) \cong \hat{F}_\omega$ is Hilbertian. Having Theorem 1.2 in mind we ask:

Problem 1.9. Is every PAC Hilbertian field also a Frobenius field?

2. Explicit Computations

In this section we give meaning to the phrase "*presented* field." In particular we show how fields finitely generated over their prime fields (i.e., *finitely generated fields*) can be presented and how the usual algebraic and algebro-geometric operations may be performed "explicitly." We rely on well-known material accumulated by Van der Waerden in [26–28] and show how to link it with the theory of primitive recursive functions.

Consider the family $\mathcal{F}$ of all functions from $\mathbb{N}^n$ to $\mathbb{N}$, where $\mathbb{N}$ is the set of positive integers and n varies on $\mathbb{N}$. The set of primitive recursive functions (abbreviated PR-functions) is the smallest subfamily of $\mathcal{F}$ that contains the constant functions, the projection functions, and the successor function and is closed under composition and induction. Being closed under induction means that if f_1 and g are PR-functions, then the function f defined inductively by $f(x_1,\ldots,x_n,1)=f_1(x_1,\ldots,x_1)$ and $f(x,y+1)=g(x,y,f(x,y))$ is also PR. A subset of N^n is said to be PR if its characteristic function is PR. If $A \subseteq \mathbb{N}^n$ is a PR-set, then a function $f: A \to \mathbb{N}$ is said to be PR-*computable* if the extended function $\bar{f}: \mathbb{N}^n \to \mathbb{N}$ defined by $\bar{f}(x)=f(x)$ if $x \in A$ and $\bar{f}(x)=1$ if $x \notin A$ is PR. The addition and multiplication are simple examples of PR-functions. The inequality relation is PR. Establishing the PR-property for other functions is aided by using the *bounded* μ-*operator*, which is described as follows. Suppose that R is a PR-subset of $\mathbb{N}^{n+1}$ and $g: \mathbb{N}^n \to \mathbb{N}$ is a PR-function such that for every $x \in \mathbb{N}^n$ there exists $y \leqslant g(x)$ such that $(x,y) \in R$. Then the function $f(x)=$ the smallest y such that $(x,y) \in R$ is PR.

It is clear from the definition that any given PR-function can be computed, for given values of the argument, in finitely many steps. For example, in order to compute $f(x)$ defined above by the bounded μ-operator, one first computes $g(x)$ and then checks the validity of $(x,y) \in R$ for y starting from 1 to $g(x)$. Thus, one can even bound the number of steps necessary in order to compute $f(x)$ before actually computing $f(x)$.

This property of PR-functions makes them more attractive to algebraists and may be also more practical for computer scientists than the recursive functions. Indeed, for recursive functions one allows, in addition to the above operations, use of the (unbounded) μ-operator: For a recursive subset R of

$\mathbb{N}^{n+1}$ for which, corresponding to each $x \in \mathbb{N}^n$ there exists $y \in \mathbb{N}$ with $(x, y) \in R$, the function

$$f(x) = \text{the smallest } y \text{ such that } (x, y) \in R$$

is a recursive function.

Thus, recursive functions can also be computed in finitely many steps. But, in order to compute $f(x)$ in this case one has to check $R(x, y)$ for $y = 1$, $y = 2$,..., with no limiting bound in order to find the first y for which $(x, y) \in R$.

In this paper all of our algorithms and decision procedures are primitive recursive, not merely recursive: an important distinction since, as Ackermann proved, the family of recursive functions is strictly larger than the family of primitive recursive functions (cf. Hermes [9, p. 82]).

Next we consider rings and fields whose elements can be "recognized" and in which we can compute "effectively." In order to make these concepts precise we consider a sequence $(\xi_1, \xi_2, \xi_3, \ldots)$ of symbols and construct the set Λ of all formal quotients of *polynomial words* with coefficients in $\mathbb{Z}$ in these symbols. The definition of polynomial word is inductive: every element of $\mathbb{Z}$ and each of the ξ_i is considered as a polynomial word; and if t_1 and t_2 are two polynomial words, then $(t_1 + t_2)$ and $(t_1 t_2)$ are polynomial words. For example, $((\xi_1 + \xi_2) + \xi_3)$ and $(\xi_1 + (\xi_2 + \xi_3))$ are two distinct polynomial words and $((5\xi_1) + (\xi_2 \xi_3))/(\xi_2 + (-1 \cdot \xi_2))$ is an element of Λ.

Λ may be viewed as a subset of Λ_0, the set of all finite words in a finite alphabet

$$(\alpha_1, \ldots, \alpha_r) = (0, 1, \ldots, 9, \xi, /, +, \cdot, -, (,), |, \ldots).$$

A Gödel numbering—or a PR-indexing (cf. Rabin [21])—on Λ_0 (resp. Λ) may then be defined as the injective map $i_0 : \Lambda_0 \to \mathbb{N}$ (resp. its restriction i to Λ) given by

$$i_0(\alpha_{j_1}, \alpha_{j_2}, \ldots, \alpha_{j_n}) = p_1^{j_1} p_2^{j_2} \cdots p_n^{j_n},$$

where $2 = p_0 < p_1 < p_2 < \cdots$ is the prime numbers sequence. Clearly, $i(\Lambda)$ is a PR-subset of N.

Using i we define PR-functions and sets for Λ. It can be shown that the following sets and functions are PR: (a) The set $N = \{1, 2, 3, \ldots\}$ as well as all its PR-functions and sets; (b) the set $\mathbb{Z} = \{0, \pm 1, \pm 2, \ldots\}$; (c) the sequence $(\xi_1, \xi_2, \xi_3, \ldots)$ as well as all the sets $\{\xi_j | j \in S\}$, where S is a PR-subset of N; (d) the set Π of all polynomial words; (e) for each $n \in N$, the set Π_n of all polynomil words in $\xi_1, \ldots, \xi_n$; (f) the function from Π to N that assigns to each $\omega \in \Pi$ the smallest n such that $\omega \in \Pi_n$; (g) the subset Π_n' of Π_n of all words $\sum a_{\mathbf{k}} \xi_1^{k_1} \xi_2^{k_2} \cdots \xi_n^{k_n}$ having a canonical form, where $a_k \in \mathbb{Z}$, $k_1, k_2, \ldots, k_n$ are non-negative integers, and the monomials are ordered, say, by

lexicographical order; (h) the function from Π_n to Π'_n that assigns to each $\omega \in \Pi_n$ its canonical form in Π'_n; (i) the degree function on Π'_n; (j) the coefficient functions on Π'_n; (k) the addition and multiplication functions on $\bigcup_{n=0}^{\infty} \Pi'_n$. In short, all the "usual" information on polynomials should be "available" by means of PR-functions. All the above-mentioned functions and sets as well as the constant functions and the projections from Λ^n into Λ should be considered as *basic functions* and *sets*.

Of course, Λ together with its basic functions and sets is the minimal framework in which field-theoretical operations can be carried out. We thus make the following

DEFINITION. A ring R is said to be *presented* if there exists an injection $j: R \to \Lambda$ such that $j(R)$ is a PR-subset of Λ and addition and multiplication are PR-functions over R (via j). In addition the PR-construction of this PR-data from the basic functions should be "given."

A field F is said to be *presented* if, in addition to the presentation of F as a ring, the inverse function of $F^{\times}$ is a "given" PR-function, and the characteristic of F is also "given."

The use of the word "given" in this definition is done in the naive sense. Note that a presented ring must be countable.

It is clear that the ring $\mathbb{Z}$ is presented with j being the identity embedding. Likewise $\mathbb{Q}$ and $\mathbb{F}_p$ can be presented for every prime p.

In order to be able to work with polynomials over a presented ring we introduce the set $\sum$ of all polynomial-words in $X_1, X_2, X_3, \ldots$ with coefficients in Λ and define PR-functions as above. In particular Λ should be a PR-subset of $\sum$. If R is a presented ring and $j: R \to \Lambda$ is its presentation we extend j to an embedding of $S = R[X_1, X_2, X_3, \ldots]$ into $\sum$ by mapping every polynomial in S to its canonical form in $\sum$. We may therefore speak about PR-functions over S.

An *effective algorithm* over a presented ring R is a presented PR-computable map $\lambda: A \to B$, where A and B are presented PR-subsets of S^n and S^m, respectively.

We list some examples of effective algorithms:

(a) Division with a remainder in $\mathbb{N}$.

(b) The prime-decomposition in $\mathbb{N}$.

(c) Euclid's algorithm of polynomials over a given field.

(d) The prime-decomposition in $\mathbb{Z}[X]$ (cf. Van der Waerden [26, p. 77]).

(e) The prime-decomposition in $\mathbb{Q}[X]$ (follows from (*d*)).

(f) Decomposition of polynomials in several variables over a presented field K, if an effective algorithm for prime-decomposition in $K[X]$ is given (cf. [26, p. 135]).

In this case we say that K has the PR-*splitting algorithm*. We now wish to show that certain fields can be presented.

DEFINITION. Let Ω be a field extension of a presented field K. An element α of Ω is said to be *presented over* K if either α is algebraic over K and its monic irreducible polynomial, $\mathrm{irr}(\alpha, K)$, over K is presented or it is known that α is transcendental over K (and then we write $\mathrm{irr}(\alpha, K) = 0$).

By the Euclidean algorithm it is easy to show that if α is presented over K, then $K(\alpha)$ is also presented. Indeed, by changing the presentation $j: K \to \Lambda$, we may assume that there exists $\xi = \xi_i$, which does not appear in $j(K)$. For α of degree n over K, we assign to each element of $K(\alpha)$ the corresponding polynomial in ξ of degree $<n$ with coefficients in $j(K)$. If α is transcendental over K, then we assign to each element in $K(\alpha)$ the corresponding rational function $p(\xi)/q(\xi)$, where $gcd(p, q) = 1$ and q is monic.

In both cases the presentation of $K(\alpha)$ extends that of K and K is a PR-subset of $K(\alpha)$. We then say that $K(\alpha)$ is *presented over* K.

If α is a presented algebraic element over K and β is a presented element of $K(\alpha)$, then we can effectively find the norm $N_{K(\alpha)/K}\beta$ by computing the determinant of the matrix of the linear operator given by multiplication by β, relative to the basis $1, \alpha, \ldots, \alpha^{n-1}$. From this computation we easily see that the norm function $N_{K(\alpha)/K}$ is PR.

An n-tuple $(\alpha_1, \alpha_2, \ldots, \alpha_n)$ is said to be *presented over* K if α_i is presented over $K(\alpha_1, \ldots, \alpha_{i-1})$, for $i = 1, 2, \ldots, n$. A sequence $(\alpha_1, \alpha_2, \alpha_3, \ldots)$ of elements of Ω is said to be presented over K if the function $n \mapsto \mathrm{irr}(\alpha_n, K(\alpha_1, \ldots, \alpha_{n-1}))$ is PR. It is clear that in both cases $K(\alpha_1, \alpha_2, \ldots)$ is presented over $K(\alpha_1, \ldots, \alpha_m)$ for $m = 0, 1, 2, \ldots$. For the case of an infinite tuple one may have to change the presentation j of K in Λ in such a way that there exists a PR-subsequence $(\xi_{n_1}, \xi_{n_2}, \xi_{n_3}, \ldots)$ of $(\xi_1, \xi_2, \xi_3, \ldots)$ whose elements do not appear in $j(K)$.

LEMMA 2.1. *Let K be a field with a PR-splitting algorithm and let α be a presented separable (i.e., algebraic separable or transcendental) element over K. Then $K(\alpha)$ also has a PR-splitting algorithm.*

Proof. See Van der Waerden [26, p. 135]. ∎

LEMMA 2.2. *Let α be a presented separable element over a field K with a PR-splitting algorithm. Let β be a presented separable element over $L = K(\alpha)$. Then one may effectively present β over K and α over $K(\beta)$.*

Proof. If $\mathrm{irr}(\alpha, K) = 0$, then $\mathrm{irr}(\beta, K) = \mathrm{irr}(\beta, L)$ when $\mathrm{irr}(\beta, L) \in K[X]$, and $\mathrm{irr}(\beta, K) = 0$ otherwise. If $\mathrm{irr}(\alpha, K) \neq 0$, then $\mathrm{irr}(\beta, K)$ divides $N_{L/K}(\mathrm{irr}(\beta, L))$ and hence may be found. To present α over $K(\beta)$ apply Lemma 2.1. ∎

Lemmas 2.1 and 2.2 release us from the dependence on a presented n-tuple $\alpha = (\alpha_1,..., \alpha_n)$ in presenting $K(\alpha)$ over K, by induction.

The condition that $K(\alpha_1,..., \alpha_n)$ also possesses a PR-splitting algorithm is satisfied, by Lemma 2.1, in the case where for each $1 \leqslant i \leqslant n$, the element α_i is separable over $K(\alpha_1,..., \alpha_{i-1})$. However, even if $K(\alpha_1,..., \alpha_n)$ is separable over K, it may still happen that some α_i is not separable over $K(\alpha_1,..., \alpha_{i-1})$. Then we may use the PR-procedure suggested in the proof of "(2) implies (3)" of Theorem 1 of Lang [16, p. 53], and reorder $\alpha_1,..., \alpha_n$ such that α_i is separable over $K(\alpha_1,..., \alpha_{i-1})$ for $i = 1,..., n$. Thus, in discussing a field separably generated over K, we need not distinguish between the case where the n-tuple $(\alpha_1,..., \alpha_n)$ is presented over K and the case where each α_i is presented over $K(\alpha_1,..., \alpha_{i-1})$. Hence we may effectively composite presented separable field extensions. In particular we obtain:

THEOREM 2.3. *Let K be a perfect field with a PR-splitting algorithm. Let $\alpha = (\alpha_1,..., \alpha_n)$ be an n-tuple of elements presented over K. Then $L = K(\alpha)$ has a PR-splitting algorithm.*

Note. If K is a perfect field with a PR-splitting algorithm then every finitely generated extension L of K has a PR-splitting algorithm. We thus say that K is a field with *elimination theory* if every finitely generated extension of K has a PR-splitting algorithm. This name is justified by the observation that the classical elimination theory procedures of algebraic geometry may be effectively performed over a field K if and only if K satisfies this condition. By Theorem 2.3, every presented finitely generated field extension of a prime field or, more generally, of a perfect field with elimination theory is a field with elimination theory. There are, however, fields with a PR-splitting algorithm which are not fields with elimination theory. These fields have finite purely inseparable extensions that do not have a PR-splitting algorithm (see Fröhlich and Shepherdson [6, Theorem 7.27]). In addition a presented infinite algebraic extension of $\mathbb{Q}$ need not have a PR-splitting algorithm (see [6, Theorem 7.12]).

For ring presentation we have the following result: Let $R = K[\alpha]$, where $\alpha = (\alpha_1,..., \alpha_n)$ is presented over a presented field K. With no loss assume that for $r \leqslant n$, $\alpha_1,..., \alpha_r$ is a transcendence basis for $K(\alpha)/K$. For each $i > r$ we can write $\mathrm{irr}(\alpha_i, K(\alpha_1,..., \alpha_{i-1}))$ in the form $f_i(\alpha_1,..., \alpha_{i-1})/h(\alpha_1,..., \alpha_r)$, with $f_i \in K[X_1,..., X_i]$, $h \in K[X_1,..., X_r]$. Then the ring $R' = K[\alpha_1,..., \alpha_n, h(\alpha_1,..., \alpha_r)^{-1}]$ is clearly a presented ring: every element of R' has a unique representation as

$$\sum_{m_{r+1}=0}^{d_{r+1}-1} \cdots \sum_{m_n=0}^{d_n-1} \frac{g_m(\alpha_1,..., \alpha_r)}{h(\alpha_1,..., \alpha_r)^{k_m}} \alpha_{r+1}^{m_{r+1}} \cdots \alpha_n^{m_n},$$

where g_m/h^{k_m} is a reduced quotient of polynomials in $K[\alpha_1,..., \alpha_r]$,

$d_i = \deg \operatorname{irr}(\alpha_i, K(\alpha_1,..., \alpha_{i-1}))$ for $i = r+1,..., n$, and $m = (m_{r+1},..., m_n)$. Further we may effectively decide whether or not a given element of $K(\alpha)$ belongs to R'.

Thus we may present a suitable localization of a ring whose generators are presented. Using the machinery of Hermann (see [8, p. 753]) we could also present the ring R itself. But the above simple procedure suffices for our purposes.

LEMMA 2.4 (THE PRIMITIVE ELEMENT THEOREM). *Let $L = K(\alpha_1,..., \alpha_n)$ be a presented separable algebraic extension of a field K with a PR-splitting algorithm. Then one can effectively find $\beta \in L$ such that $K(\beta) = L$.*

Proof. Use, for example, the proof on page 84 of Zariski–Samuel [29]. Note that in the case where K is infinite one must find, for a given non-zero polynomial $g \in K[X_1,..., X_n]$, elements $b_1,..., b_n \in K$ such that $g(b) \neq 0$. This is easily effected by induction. ∎

LEMMA 2.5. *Let α be a presented algebraic separable element over a field K with a PR-splitting algorithm. Then one can effectively present the n-tuple $(\alpha_1, \alpha_2,..., \alpha_n)$ of conjugates of α and one can effectively compute the Galois group G of* $\operatorname{irr}(\alpha, K)$ *as a permutation group of $(\alpha_1, \alpha_2,..., \alpha_n)$ and hence also its action on $L = K(\alpha_1,..., \alpha_n)$. Moreover, if H is a presented subgroup of G, then one can present its fixed field in L over K.*

By an effective computation of the Galois group we mean that the corresponding algorithm from the set of all polynomials of degree n over K into the symmetric group S_n is PR. Obviously every subset of S_n is defined to be PR.

Proof. See Van der Waerden [26, p. 189] and Lang [17, p. 186].

THEOREM 2.6. *If K is a field with a PR-splitting algorithm, then its separable closure, K_s, can be given over K by a sequence $(\alpha_1, \alpha_2, \alpha_3,...)$ and has a PR-splitting algorithm. If K is a field with elimination theory, then, in addition, its algebraic closure, $\tilde{K}$, is a field with elimination theory.*

Proof. Order the set of all non-constant separable polynomials of $K[X]$ in a PR-sequence $(p_1, p_2, p_3,...)$. We construct, by induction, a sequence $(\alpha_1, \alpha_2, \alpha_3,...)$ of separable algebraic elements over K and an ascending sequence $K \subseteq K_1 \subseteq K_2 \subseteq \cdots$ of field extensions such that $K_k = K(\alpha_1,..., \alpha_{n_k})$ is the splitting field of $p_1 p_2 ... p_k$. Clearly $K(\alpha_1, \alpha_2, \alpha_3,...)$ is the separable closure of K and it is presented by the sequence $(\alpha_1, \alpha_2, \alpha_3,...)$. We must show how to decompose polynomials over K_s. Let $f \in K_s[X]$ be a non-constant polynomial. Then f has coefficients in $L = K(\alpha_1,..., \alpha_j)$ for some j. Compute $g(X) = N_{L/K} f(X)$. Without loss we may assume that g is separable

over K. Then we find $k \geqslant j$ such that $g \in \{p_1,..., p_k\}$. The decomposition of $f(X)$ over K_k is the desired decomposition of f over K_s.

If K is a field with elimination theory, an analogous construction proves that $\tilde{K}$ has a splitting algorithm. Hence $\tilde{K}$ is a field with elimination theory, since $\tilde{K}$ is perfect. ∎

Rabin proved the same result for recursively presented fields by presenting $\tilde{K}$ as a quotient of $K[X_1, X_2, X_3,...]$ by a certain, explicitly constructed, maximal ideal (see [21, Theorem 7]).

The following lemma is of use when dealing with Frobenius fields.

LEMMA 2.7. *Let K be a field with a splitting algorithm and let $F = K(\alpha_1,..., \alpha_n)$ be a presented separable extension of K. Then one can effectively find the separable algebraic closure L of K in F.*

Proof. We may rearrange $\alpha_1,..., \alpha_n$ such that $\alpha_1,..., \alpha_r$ is a separating transcendence base for the extension F/K. By the primitive element theorem we may assume that $r = n - 1$. Then we observe that $f(X) = \mathrm{irr}(\alpha_n, L(\alpha_1,..., \alpha_{n-1})) = \mathrm{irr}(\alpha_n, K_s(\alpha_1,..., \alpha_{n-1}))$. By Theorem 2.6, $f(X)$ can be computed effectively. Its coefficients are rational functions in $\alpha_1,..., \alpha_{n-1}$ over L. Let $\beta_1,..., \beta_m$ be all their coefficients. Then $L = K(\beta_1,..., \beta_m)$. ∎

Let R be a presented integral domain with a quotient field K. Let $\mathscr{L}(R)$ be the first-order predicate calculus language for the theory of rings enriched with constants for the elements of R. Using the given presentation of R we can equip $\mathscr{L}(R)$ with a Gödel numbering such that R is a PR-subset of $\mathscr{L}(R)$. Fields that contain a homomorphic image of R are models of $\mathscr{L}(R)$. The elements of R are interpreted in them as their corresponding images.

THEOREM 2.8. *Let R be a presented integral domain with a quotient field K. Then there is an effective algorithm that assigns to each formula $\varphi(X_1,..., X_n)$ a quantifier-free formula $\psi(X_1,..., X_n)$ such that for every algebraically closed model F of $\mathscr{L}(R)$ and for every $x_1,..., x_n \in F$ we have: $\varphi(x_1,..., x_n)$ is true in F if and only if $\psi(x_1, ..., x_n)$ is true in F.*

PROOF. The elimination of quantifiers algorithm we have in mind uses essentially only the division of polynomials with a remainder algorithm and is well known. Unfortunately the only reference known to us is [18]. ∎

This result is considerably generalized in Theorem 3.7.

In particular, when $n = 0$, i.e., when φ is a sentence, we can deduce the following

COROLLARY 2.9. *There is an effective algorithm that assigns to each sentence φ of $\mathscr{L}(R)$ a non-zero element $c \in R$ such that if F is an algebraically closed field containing a homomorphic image $\bar{R}$ of R and if c is*

mapped onto a non-zero element $\bar{c}$ of $\bar{R}$, then φ is true in $\tilde{K}$ if and only if φ is true in F.

We give two algebro-geometric applications of the last two results. Let K be a presented field and consider the affine n-dimensional space $\mathbb{A}^n$ over K. In particular $\mathbb{A}^0$ consists of one point, the origin. A *constructible* set A in $\mathbb{A}^n$ is a set of the form $A = P(V(h_1),..., V(h_m))$, where $h_1,..., h_m \in K[X_1,..., X_n]$ and P is a boolean polynomial in the symbols $\cup$, $\cap$ and $'$ (= taking the complement). Here $V(h_i)$ denotes the set of zeros of h_i in some universal extension of K (cf. Lang [16, p. 21]). If L is a field containing K, then we denote by $A(L)$ the set of points of A with coordinates in L. If K is a presented field, then A is said to be *presented* if $h_1,..., h_m$ and P are given. Note that A can be presented in many ways. In particular, if K is the quotient field of a presented integral domain R, then the h_i may be assumed to have coefficients in R.

LEMMA 2.10. *Let $f_1,...,f_m \in K[X_1,..., X_n]$. Define a morphism $\varphi: \mathbb{A}^n \to \mathbb{A}^m$ by $\varphi(x) = (f_1(x),...,f_m(x))$. Let $A \subseteq \mathbb{A}^n$ be a presented constructible set. Then $B = \varphi(A)$ is a constructible set which can be effectively presented.*

Proof. Let Ω be a universal domain containing K and let $B = \{(y_1,..., y_m) \in \Omega^m \mid \theta(y_1,..., y_m)$ is true in $\Omega\}$, where $\theta(Y_1,..., Y_m)$ is the formula

$$(\exists X_1) \cdots (\exists X_n)[f_1(X) = Y_1 \wedge \cdots \wedge f_m(X) = Y_m].$$

By Theorem 2.8 we can effectively find a quantifier-free formula $\theta'(Y_1,..., Y_m)$ equivalent to $\theta(Y_1,..., Y_m)$ over Ω. This formula gives B as a constructible subset of $\mathbb{A}^m$. ∎

G. Stolzenberg gives, in [25], a direct proof of Lemma 2.10 by using the results of G. Hermann in [8].

LEMMA 2.11. *Let $f \in R[X_1,..., X_n]$ be a presented absolutely irreducible polynomial. Then one can effectively compute a non-zero element $c \in R$ such that if $\mathfrak{p}$ is a prime ideal of R and $c \notin \mathfrak{p}$ then f remains absolutely irreducible over $R/\mathfrak{p}$.*

Proof. One can effectively write down a sentence in $\mathscr{L}(R)$ which is equivalent, modulo the theory of algebraically closed models of $\mathscr{L}(R)$, to the statement "f is absolutely irreducible", (cf. [13, p. 278]). ∎

A generic point of an irreducible algebraic set $V = V(h_1,..., h_m) \subseteq \mathbb{A}^n$ over K is a point $(x_1,..., x_n) \in V$ for which $K(x_1,..., x_n)$ is isomorphic to the quotient field of the ring $K[X_1,..., X_n]/\sqrt{\langle h_1,..., h_m \rangle}$.

LEMMA 2.12. *Let K be a field with elimination theory.*

(a) *Let $h_1,...,h_m$ be presented polynomials in $K[X_1,...,X_n]$ and let $V = V(h_1,...,h_m)$ be the algebraic set defined by them. Then one can effectively compute generic points $(x_{i1},...,x_{in})$ over K of the K-components V_i of V.*

(b) *Let $x = (x_1,...,x_n)$ be a presented point over K. Then one can effectively compute polynomials $g_1,...,g_k \in K[\mathbf{X}]$ such that x is a generic point of the K-irreducible set $V(g_1,...,g_k)$.*

(c) *If $V = V(h_1,...,h_m)$ is a presented algebraic set, then one can effectively compute the K-components $V_i = V(g_{i1},...,g_{ik_i})$ of V.*

(d) *One can effectively compute the dimension of every given irreducible set.*

Proof. See Van der Waerden [28, Section 31]. ∎

A constructible set A over a field K is said to be a *basic set* if it is of the form $A = V - V(g)$, where $V = V(f_1,...,f_m)$, and $f_1,...,f_m$, $g \in K[X_1,...,X_n]$ and where V is a K-irreducible set on which g does not vanish. If x is a generic point of V, then $K[A] = K[x, g(x)^{-1}]$ is said to be the *coordinate ring* of A and $K(A) = K(x)$ is said to be the *function field* of A. We also define $\dim A$ as the transcendence degree of $K(A)$ over K. The basic set A is said to be *normal* if $K[A]$ is an integrally closed domain. The basic set A is *presented* if the polynomials $f_1,...,f_m$ and the ring $K[A]$ are presented.

Let $\mathscr{P}$ be a property of constructible sets (e.g., normal, basic, nonsingular, etc.). A $\mathscr{P}$-stratification of a constructible set A is a finite family $\{A_i | i \in I\}$ of disjoint constructible sets having the property $\mathscr{P}$ and for which $A = \bigcup_{i \in I} A_i$.

Let A be a basic set with $K[A] = K[x, g(x)^{-1}]$ and let B be a basic subset of A with $K[B] = K[x', h(x')^{-1}]$. Then $g(x') \neq 0$ and $K[x', g(x')^{-1}] \subseteq K[x', h(x')^{-1}]$ (cf. Lang [16, p. 31]). The subset B is a Zariski-open subset of A if and only if $K[A] \subseteq K[B]$.

LEMMA 2.13 (THE STRATIFICATION LEMMA). *Let K be a field with elimination theory and let $\mathscr{P}$ be a property of constructible sets. Suppose that to every presented basic set A we can effectively compute a basic $\mathscr{P}$-set B with B open in A. Then we can effectively produce a $\mathscr{P}$-stratification of every presented constructible set.*

Proof. Let A be a presented constructible set. Applying several boolean-algebra operations to the algebraic sets that define A and using an induction hypothesis on the dimension we can assume that A is a basic set. The effectiveness of these operations follows from Lemma 2.12. We have also to use the dimension theorem (cf. [16, p. 36]): If V_1 and V_2 are irreducible algebraic sets and $V_1 \not\subseteq V_2$, then $\dim V_1 \cap V_2 < \dim V_1$.

For a basic set A we can, by hypothesis, effectively find a basic $\mathscr{P}$-set B, open in A. Then $\dim A - B < \dim A$ and we can again apply the induction hypothesis to produce a $\mathscr{P}$-stratification of $A - B$. ∎

In particular we have:

LEMMA 2.14. *There is an effective procedure for producing a basic and normal stratification of a presented constructible set.*

Proof. This Lemma follows from the stratification Lemma and from the following:

LEMMA 2.15. *Let K be a field with elimination theory. Let $(x_1,..., x_n, z)$ be a presented $(n+1)$-tuple over K for which z is a separable algebraic element over $K(x)$. Then we can effectively find a polynomial $g \in K[X]$ such that:*

(a) $g(x) \neq 0$,

(b) *the ring $K[x, g(x)^{-1}]$ is integrally closed,*

(c) *the ring $K[x, g(x)^{-1}, z]$ is a cover of the ring $K[x, g(x)^{-1}]$ (in the sense of Section 1), and*

(d) *the rings $K[x, g(x)^{-1}]$ and $K[x, g(x)^{-1}, z]$ are presented.*

Proof. It suffices to find a $g \in K[X]$ that satisfies conditions (a) and (b). Indeed, if we multiply g by a product of the denominator and the discriminant of $\mathrm{irr}(z, K(x))$ and another suitable polynomial according to the remark preceding Lemma 2.4, we can change g to also satisfy (c) and (d).

In order to find a $g \in K[X]$ that satisfies (a) and (b) we consider first the case where $K(x)$ is a separable extension of K. After reordering $x_1,..., x_n$ we may assume that x_i is separable over $K(x_1,..., x_{i-1})$ for $i = 1,..., n$. We proceed by induction on n.

By the induction hypothesis we can effectively find a polynomial $g_1 \in K[X_1,..., X_{n-1}]$ such that $g_1(x) \neq 0$ and $K[x_1,..., x_{n-1}, g_1(x)^{-1}]$ is integrally closed. If x_n is transcendental over $K(x_1,..., x_{n-1})$, then $K[x_1,..., x_n, g_1(x)^{-1}]$ is also integrally closed (cf. Zariski–Samuel [30, p. 126]). If x_n is separable algebraic over $K(x_1,..., x_{n-1})$, then, by the first part of the proof, we can effectively find $g \in K[X_1,..., X_{n-1}]$ such that $K[x, g(x)^{-1}]$ is a ring cover of $K[x_1,..., x_{n-1}, g(x)^{-1}]$. In particular $K[x, g(x)^{-1}]$ is integrally closed.

In the general general case we can again follow the proof "(2) implies (3)" of Theorem 1 of Lang [16, p. 53], and find a finite purely inseparable extension K' of K such that $K'(x)/K'$ is separable. We can also find a basis $\alpha_1,..., \alpha_m$ for K'/K, a basis $\alpha_1,..., \alpha_k$ for $K'(x)/K(x)$ out of it, and a power q of the characteristic such that $\alpha^q \in K$ for every $\alpha \in K'$. We then find, by the

procedure for the separable case, a polynomial $h \in K'[X]$ such that $h(x) \neq 0$ and $K'[x, h(x)^{-1}]$ is integrally closed. For every $1 \leqslant i \leqslant m$ we find $g_i, h_{ij} \in K[X]$ such that $g_i(x) \neq 0$ and

$$\alpha_i = (h_{i1}(x)\,\alpha_1 + \cdots + h_{ik}(x)\,\alpha_k)\,g_i(x)^{-1}.$$

Then we define $g(X) = g_1(X) \cdots g_k(X)\,h(X)^q$. It follows that $K(x) \cap K^1[x, g(x)^{-1}] = K[x, g(x)^{-1}]$, which is therefore integrally closed. ∎

3. The Galois Stratification

In this section we consider a presented field K and a perfect Frobenius field M that contains K. Let $\mathscr{C} = \mathscr{C}(M)$ be the family of finite groups that can be realized over M. The case where K is a field with elimination theory and $\mathscr{C}$ is a PR-*family* of finite groups is referred to as the *explicit case*. The results achieved in this section hold for the general case. In the explicit case, however, they become effective in the sense of Section 2. Thus instead of only proving the existence of a set A with explicit properties as in the general case, in the explicit case we effectively find A.

A (*Galois*) *set-cover*, $C \to A$, *over* K is a pair (A, C) of K-normal basic sets such that $K[C]/K[A]$ is a (Galois) ring-cover (see Section 1). In the explicit case, if A is a presented K-normal basic set and if F is a presented finite Galois extension of $K(A)$, then, by Lemma 2.15, we can effectively find a K-normal basic set C' that covers a presented K-basic set A', which is open in A, such that $K(C') = F$.

Let $C \to A$ be a Galois set-cover over K with $K[A] = K[x_1, \ldots, x_n, g(x)^{-1}]$ and let z be a primitive element for the ring-cover $K[C]/K[A]$. Put also $\mathscr{G}(C/A) = \mathscr{G}(K(C)/K(A))$. Suppose that $(a_1, \ldots, a_n)$ is a point of $A(M)$. Then the map $x_i \mapsto a_i$, for $i = 1, \ldots, n$, can be uniquely extended to a homomorphism φ_0 of $K[A]$ into M. The homomorphism φ_0 can be further extended to a homomorphism φ of $K[C]$ into a Galois extension $N = M(\varphi z)$ of M. As in Section 1, φ gives rise to an isomorphism φ^* of $\mathscr{G}(N/M)$ onto the decomposition group $D_M(\varphi)$. As φ ranges over all possible extensions of φ_0 to $K[C]$, the group $D_M(\varphi)$ ranges over a conjugacy class of subgroups of $\mathscr{G}(C/A)$. We call this class the *Artin symbol* of a and denote it by $\mathrm{Ar}_{C \to A}(a)$.

If $D \to A$ is another Galois set-cover such that $K[C] \subseteq K[D]$ and $a \in A(M)$, then $\mathrm{Ar}_{C \to A, M}(a) = \mathrm{Res}_{K(C)}\,\mathrm{Ar}_{D \to A}(a)$. Thus, whenever no confusion arises, we omit the reference to the cover from the Artin symbol and write it as $\mathrm{Ar}_{A,M}(a)$. If $H \in \mathrm{Ar}_{A,M}(a)$, then $\mathrm{Ar}_{A,M}(a) = \{H^\sigma \mid \sigma \in \mathscr{G}(C/A)\}$.

If $n = 0$, then $K(A) = K$, $K(C) = L$ and $\mathrm{Ar}_{A,M}(a) = \{\mathscr{G}(L/L \cap M)^\sigma \mid \sigma \in \mathscr{G}(L/K)\}$.

Replacing A by an open subset does not affect the Artin symbol. Indeed, if $h \in K[X_1,\dots,X_n]$ is a polynomial that does not vanish on A and if we let $A' = A - V(h)$ and $C' = C - V(h)$, then $C' \to A'$ is also a Galois set-cover. If $a \in A'(M)$, then $\mathrm{Ar}_{A',M}(a) = \mathrm{Ar}_{A,M}(a)$.

More generally, if A' is a K-normal basic set contained in A with a generic point x', then the specialization $x \to x'$ uniquely extends to a K-homomorphism τ_0 of $K[A]$ into $K[A']$. Let z be a primitive element for $K[C]/K[A]$, let $p(X)$ be the image by τ_0 in $K[A'][X]$ of $\mathrm{irr}(z, K(A))$, and let z' be a root of $p(X)$. Then z' is a primitive element for a cover $C' \to A'$ and τ_0 can be extended to a homomorphism $\tau: K[C] \to K[C']$ such that $\tau(z) = z'$. The cover $C' \to A'$ is said to be *induced* by $C \to A$. If $a \in A'(M)$, then $\tau^* \mathrm{Ar}_{A',M}(a) \subseteq \mathrm{Ar}_{A,M}(a)$. Indeed, if φ is a homomorphism of $K[C']$ into $\tilde{M}$ that extends the specialization $x' \to a$, then $\tau^* D_M(\varphi) \subseteq D_M(\varphi\tau)$, hence $\tau^* D_M(\varphi) = D_M(\varphi\tau)$, since both groups are isomorphic.

We introduce the notation $\mathrm{Con}(A)$ to denote a *conjugacy domain* (i.e., a union of conjugacy classes) of subgroups of $\mathscr{G}(C/A)$ that belong to $\mathscr{C}$. Note that if $\mathrm{Ar}_{A,M}(a) \cap \mathrm{Con}(A) \neq \emptyset$, then $\mathrm{Ar}_{A,M}(a) \subseteq \mathrm{Con}(A)$.

Having the cover $C' \to A'$ in mind we define

$$\mathrm{Con}(A') = \{H \leqslant \mathscr{G}(C'/A') \mid H \in \mathscr{C} \text{ and } \tau^* H \in \mathrm{Con}(A)\}.$$

Here we are using the notation "$H \leqslant G$" to mean "H is a subgroup of the group G." The conjugacy domain $\mathrm{Con}(A')$ of $\mathscr{G}(C'/A')$ thus defined is said to be *induced* by $\mathrm{Con}(A)$. If $a \in A'(M)$, then $\mathrm{Ar}_{A',M}(a) \subseteq \mathrm{Con}(A')$ if and only if $\mathrm{Ar}_{A,M}(a) \subseteq \mathrm{Con}(A)$.

Let $n \geqslant 0$ and let $\pi: \mathbb{A}^{n+1} \to \mathbb{A}^n$ be the projection on the first n coordinates. If $n = 0$, then π maps every point of $\mathbb{A}^1$ onto the only point, the origin, of $\mathbb{A}^0$.

If $A \subseteq \mathbb{A}^{n+1}$ and $B \subseteq \mathbb{A}^n$ are two basic sets such that $\pi(A) = B$, then either $\dim A = \dim B + 1$ or $\dim A = \dim B$. The first case is treated in Lemma 3.1, the second in Lemma 3.2.

LEMMA 3.1. *Let $C \to A$ and $D \to B$ be Galois set-covers over K, the former equipped with a conjugacy domain $\mathrm{Con}(A)$ of subgroups of $\mathscr{G}(C/A)$ belonging to $\mathscr{C}$. Suppose that $A \subseteq \mathbb{A}^{n+1}$, $B = \pi(A)$, $\dim A = \dim B + 1$ and $K(D)$ contains the algebraic closure L of $K(B)$ in $K(C)$. Define*

$$\mathrm{Con}(B) = \{G \leqslant \mathscr{G}(D/B) \mid G \in \mathscr{C} \ \&\ \mathrm{Res}_L G \in \mathrm{Res}_L \mathrm{Con}(A)\}.$$

Then there exists an $h = h_{A,C,B,D} \in K[X_1,\dots,X_n]$, not vanishing on B such that for $B' = B - V(h)$, $A' = A - V(h)$, $C' = C - V(h)$, $D' = D - V(h)$ and for every $b \in B'(M)$ we have:

(1) $\mathrm{Ar}_{B',M}(b) \subseteq \mathrm{Con}(B)$ *if and only if there exists an $a \in A'(M)$ such that $\pi(a) = b$ and $\mathrm{Ar}_{A,M}(a) \subseteq \mathrm{Con}(A)$.*

Moreover, h does not depend on M and $\mathscr{C}$ and can be effectively found in the explicit case, if A, B, C and D are presented.

Proof. Suppose that $K[B]=K[x, g_1(x)^{-1}]$ and $K[A]=K[x, y, g_2(x, y)^{-1}]$, where $x=(x_1,..., x_n)$. Then $K[B]\subseteq K[A]$ and y is transcendental over $K(B)$. Let z be a primitive element for the cover $C\to A$ and let $S=K[D]\cap L$. Find a polynomial $f\in S[Y, Z]$ irreducible over L such that $f(y, z)=0$. Then $f(Y, Z)$ is absolutely irreducible. By Lemma 2.11 we can compute a non-zero element $u\in S$ such that if φ is a homomorphism of S into a field and $\varphi(u)\neq 0$, then with $f'=\varphi f$, the polynomial $f'(Y, Z)$ is absolutely irreducible and its degree in Z is equal to that of $f(Y, Z)$. Let $h\in K[X_1,..., X_n]$ be a polynomial such that $h(x)=g_1(x)^k\cdot N_{L/K(B)}(u)$ for some $k\geqslant 0$. Then statement (1) is true. Indeed, by multiplying h by an appropriate polynomial we may assume that $K[D']\cap L/K[B']$ is a ring cover. Thus with no loss we may assume that $K(D)=L$. Let $b\in B'(M)$ be such that $\mathrm{Ar}_{B',M}(b)\subseteq \mathrm{Con}(B)$. Extend the K-specialization $x\to b$ to a homomorphism φ of $K[C']$ into $\widetilde{M(y')}$ such that $\varphi(y)=y'$ and y' is a transcendental element over M. Then $g_2(b, y')\neq 0$, since $\pi(A)=B$. Let $z'=\varphi(z)$ and denote $N=M\cdot\varphi(K[D'])$, $R=M[y', g_2(b, y')^{-1}]=M[\varphi(K[A'])]$, $E=M(y')$ and $F=E(z')$. Then $R[z']/R$ is a ring cover over M with F/E the corresponding field cover. Also, $[F: NE]=\deg_Z f'(y', Z)=\deg_Z f(y, Z)=[K(C): P]$, where $P=K(A)K(D)$, since $h(b)\neq 0$, hence $\varphi(u)\neq 0$, hence $f'(y', Z)$ is irreducible over NE. This implies that in the following commutative diagram the left vertical arrow is an isomorphism:

$$\begin{array}{ccccccc} 1 & \to & \mathscr{G}(K(C)/P) & \to & \mathscr{G}(C/A) & \to & \mathscr{G}(D/B) \to 1 \\ & & \uparrow{\scriptstyle \varphi^*} & & \uparrow{\scriptstyle \varphi^*} & & \uparrow{\scriptstyle \varphi^*} \\ 1 & \to & \mathscr{G}(F/NE) & \to & \mathscr{G}(F/E) & \to & \mathscr{G}(N/M) \to 1. \end{array}$$

The conjugacy class $\mathrm{Ar}_{B',M}(b)$ is generated by $\varphi^*\mathscr{G}(N/M)$. Hence, by the definition of $\mathrm{Con}(B)$, there exists a group $H\in \mathrm{Con}(A)$ (hence $H\in\mathscr{C}$) such that $\mathrm{Res}_{K(D)}H=\varphi^*\mathscr{G}(N/M)$. A diagram-chasing shows that there is a subgroup H' of $\mathscr{G}(F/E)$ such that $\varphi^*H'=H$. Hence $H'\in\mathscr{C}$ and $\mathrm{Res}_N H'=\mathscr{G}(N/M)$. Also N is the algebraic closure of M in F, since $f'(Y, Z)$ is absolutely irreducible. We have assumed that M is a Frobenius field, hence there exists an M-epimorphism $\psi: R[z']\to F'$ such that $\psi(y')=c\in M$ and $\psi^*\mathscr{G}(F'/M)=H'$. It follows from the definitions that $\varphi^*D_M(\psi)\subseteq D_M(\psi\varphi)$. Thus $H=\varphi^*D_M(\psi)=D_M(\psi\varphi)$, since both sides are isomorphic to $\mathscr{G}(F'/M)$. Thus, the point $a=(b, c)=\psi\varphi(x, y)$ belongs to $A'(M)$ and it satisfies $\pi(a)=b$ and $\mathrm{Ar}_{A,M}(a)\subseteq \mathrm{Con}(A)$ since $H\in\mathrm{Con}(A)$.

The converse implication in (1) follows from

$$\mathrm{Res}_{K(D)}\,\mathrm{Ar}_{A',M}(a)=\mathrm{Ar}_{B',M}(b). \quad \blacksquare$$

LEMMA 3.2. *Let $C \to A$ and $D \to B$ be Galois set-covers over K such that $B = \pi(A)$ and $K[A]$ is integral over $K[B]$. Let E and F be the maximal separable extensions of $K(B)$ in $K(A)$ and $K(C)$, respectively. Then F/E is a Galois extension and* $\mathrm{Res}: \mathcal{G}(C/A) \to \mathcal{G}(F/E)$ *is an isomorphism. Assume also that $F \subseteq K(D)$.*

Let $\mathrm{Con}(A)$ *be a conjugacy domain of subgroups of $\mathcal{G}(C/A)$ belonging to $\mathscr{C}$. Define* $\mathrm{Con}(B)$ *as the set of all H^σ, where H is a subgroup of $\mathcal{G}(K(D)/E)$ which belongs to $\mathscr{C}$ such that $\mathrm{Res}_F H \in \mathrm{Res}_F \mathrm{Con}(A)$ and $\sigma \in \mathcal{G}(D/B)$.*

Let $b \in B(M)$. Then $\mathrm{Ar}_{B,M}(b) \subseteq \mathrm{Con}(B)$ if and only if there exists an $a \in A(M)$ such that $\pi(a) = b$ and $\mathrm{Ar}_{A,M}(a) \subseteq \mathrm{Con}(A)$.

Proof. Both extensions $K(A)/E$ and $K(C)/F$ are purely inseparable. Hence $K(A)$ and F are linearly disjoint over E and $K(A) \cdot F = K(C)$. If $\mathrm{char}(K) = p \neq 0$, let q be a power of p such that $K(A)^q \subseteq E$ and $K(C)^q \subseteq F$. Then $K(C)^q/K(A)^q$ is a Galois extension and $E \cdot K(C)^q = F$. Hence F/E is also a Galois extension.

Denote by R and S the integral closures of $K[B]$ in E and F, respectively. Then $R \subseteq K[A]$ and $S \subseteq K[C] \cap K[D]$. Let x and y be generic points of A and B such that $\pi(x) = y$.

Suppose now that $\mathrm{Ar}_{B,M}(b) \subseteq \mathrm{Con}(B)$. Then there exists an $H \leqslant \mathcal{G}(K(D)/E)$ that belongs to $\mathrm{Ar}_{B,M}(b)$ and there exists a group $G \in \mathrm{Con}(A)$ such that $\mathrm{Res}_F H = \mathrm{Res}_F G$. The condition $H \in \mathrm{Ar}_{B,M}(b)$ means that there exists a K-homomorphism φ of $K[D]$ into a Galois extension N of M such that $\varphi(y) = b$ and $\varphi^* \mathcal{G}(N/M) = H$. We have assumed that M is a perfect field. Hence there exists a unique K-homomorphism ψ of $K[C]$ into N such that $\mathrm{Res}_S \psi = \mathrm{Res}_S \varphi$. In particular $a = \psi(x)$ belongs to $A(M)$ and $\pi(a) = b$. Also, if we denote $M \cdot \psi(K[C])$ by N_0, then $\mathrm{Res}_F \psi^* \mathcal{G}(N_0/M) = \mathrm{Res}_F H$. Thus $\psi^* \mathcal{G}(N_0/M) = G$. It follows that $G \in \mathrm{Ar}_{A,M}(a)$ and $\mathrm{Ar}_{A,M}(a) \subseteq \mathrm{Con}(A)$.

The converse follows similarly from the definitions by reversing the arguments. ∎

Let $n \geqslant 0$ and let A be a constructible set in $\mathbb{A}^n$. A Galois stratification

$$\mathscr{A} = \langle A, C_i \to A_i, \mathrm{Con}(A_i) \rangle_{i \in I}$$

of A with respect to K and $\mathscr{C}$ is a decomposition $A = \bigcup_{i \in I} A_i$ of A as a finite union of disjoint basic sets A_i, each one equipped with a Galois cover $C_i \to A_i$ of basic sets and a conjugacy domain $\mathrm{Con}(A_i)$ of subgroups of $\mathcal{G}(C_i/A_i)$ that belong to $\mathscr{C}$.

If $a \in A(M)$, then we write $\mathrm{Ar}_{\mathscr{A},M}(a) \subseteq \mathrm{Con}(\mathscr{A})$, if $\mathrm{Ar}_{A_i,M}(a) \subseteq \mathrm{Con}(A_i)$, for the unique $i \in I$ such that $a \in A_i$.

Suppose that $\mathscr{A}' = \langle A, C_j' \to A_j', \mathrm{Con}(A_j') \rangle_{j \in J}$ is an additional Galois stratification of A. Then $\mathscr{A}'$ is said to be a *refinement* of $\mathscr{A}$ if for each $j \in J$ there exists a unique $i \in I$ such that $A_j' \subseteq A_i$ and the domain $\mathrm{Con}(A_j')$ is

induced by the domain $\mathrm{Con}(A_t)$. It is then clear that if $a \in A(M)$, then $\mathrm{Ar}_{\mathscr{A},M}(a) \subseteq \mathrm{Con}(\mathscr{A})$ if and only if $\mathrm{Ar}_{\mathscr{A}',M}(a) \subseteq \mathrm{Con}(\mathscr{A}')$

The following Lemma will be needed in the refinement and stratification procedure of Lemma 3.4.

LEMMA 3.3. *Let $n \geqslant 0$ and let $\{C_t \to A_t \mid t \in T\}$ be a finite collection of Galois set-covers over K, where each $A_t \subseteq \mathbb{A}^{n+1}$. Let $B \subseteq \mathbb{A}^n$ be a K-normal basic set such that $B \subseteq \pi(A_t)$ for every $t \in T$. Then there exist Galois set-covers $D \to B'$ and $C'_{ti} \to A'_{ti}$, for $i \in I(t)$, over K such that:*

(a) *B' is a K-open subset of B.*

(b) *The sets A'_{ti} are contained in A_t and they are mutually disjoint.*

(c) *The covers $C'_{ti} \to A'_{ti}$ are induced by the cover $C_t \to A_t$.*

(d) *We have $\pi^{-1}(B') \cap A_t = \bigcup_{i \in I(t)} A'_{ti}$ and $\pi(A'_{ti}) = B'$.*

(e) *If $\dim A'_{ti} = \dim B'$, then $K[A'_{ti}]$ is integral over $K[B']$ and $K(D)$ contains the maximal separable extension of $K(B')$ in $K(C'_{ti})$.*

(f) *If $\dim A'_{ti} = \dim B' + 1$, then $K(D)$ contains the algebraic closure of $K(B')$ in $K(C'_{ti})$ and the polynomial $h_{A'_{ti}C'_{ti},B',D}$ defined as in Lemma 3.1 does not vanish at any point of B'.*

Moreover, if in the explicit case $C_t \to A_t$ and B are presented, then $C'_{ti} \to A'_{ti}$ and $D \to B'$ can be effectively computed.

Proof. By the stratification Lemma we can stratify $A_t \cap \pi^{-1}(B) = \bigcup_{j \in J(t)} A_{tj}$ into K-normal basic sets. Let $I(t) = \{j \in J(t) \mid \dim \pi(A_{tj}) = \dim B\}$ and let $I'(t) = J(t) - I(t)$. Then $B_0 = \bigcup_{j \in I(t)} (B - \pi(A_{tj})) \cup \bigcup_{j \in I'(t)} \pi(A_{tj})$ has a smaller dimension than that of B. Hence there exists a polynomial $f \in K[X_1, \ldots, X_n]$ that vanishes on B_0 but not on B.

For $i \in I(t)$ we denote by F_{ti} the separable closure (resp. the algebraic closure) of $K(B)$ in $K(C_{ti})$ if $\dim A_{ti} = \dim B$ (resp., if $\dim A_{ti} = \dim B + 1$). Let P be a finite Galois extension of $K(B)$ that contains all the F_{ti}'s. Then we can find a multiple $g \in K[X_1, \ldots, X_n]$ of f that does not vanish on B such that

(i) $B' = B - V(g)$ has a Galois cover D with $K(D) = P$,

(ii) if $\dim A_{ti} = \dim B + 1$, then the appropriate polynomial $h_{A_{ti},C_{ti},B,D}$ defined in Lemma 3.1 divides g,

(iii) if $\dim A_{ti} = \dim B$, then $K[A'_{ti}]$ is an integral extension of $K[B']$, where $A'_{ti} = A_{ti} - V(g)$.

The sets B' and A'_{ti}, for $t \in T$ and $i \in I(t)$, have the desired properties. ∎

LEMMA 3.4 (THE ELIMINATION LEMMA). *Let $n \geqslant 0$ and let $\mathscr{A} = \langle \mathbb{A}^{n+1}, C_i \to A_i, \mathrm{Con}(A_i) \rangle_{i \in I}$ be a Galois stratification of $\mathbb{A}^{n+1}$ over K. Then there*

exists a Galois stratification $\mathscr{B} = \langle \mathbb{A}^n, D_j \to B_j, \mathrm{Con}(B_j)\rangle_{j\in J}$ *such that for every* $b \in \mathbb{A}^n(M)$ *we have:* $\mathrm{Ar}_{\mathscr{B},M}(b) \subseteq \mathrm{Con}(\mathscr{B})$ *if and only if there exists an* $a \in \mathbb{A}^{n+1}(M)$ *that satisfies* $\pi(a) = b$ *and* $\mathrm{Ar}_{\mathscr{A},M}(a) \subseteq \mathrm{Con}(\mathscr{A})$.

In the explicit case, if $\mathscr{A}$ is presented, then $\mathscr{B}$ can be effectively computed.

Proof. By considering the intersections of the sets $\pi(A_i)$ and using the stratification Lemma we can stratify $\mathbb{A}^n$ into a union of disjoint K-normal basic sets U_s, for $s \in S$, such that for every $i \in I$ and $s \in S$ either $U_s \subseteq \pi(A_i)$ or $U_s \cap \pi(A_i) = \phi$. By the Lemma 3.3 and by the stratification Lemma we can stratify each of the U_s separately and then combine the separate stratifications into basic normal stratifications $\mathbb{A}^n = \dot{\bigcup}_{j\in J} B_j$ and $\mathbb{A}^{n+1} = \dot{\bigcup}_{j\in J} \dot{\bigcup}_{k\in K(j)} A_{jk}$ with the following properties:

(a) Every A_{jk} is contained in a unique A_i and has a Galois cover C_{jk} which is induced by $C_i \to A_i$. We denote by $\mathrm{Con}(A_{jk})$ the conjugacy domain of subgroups of $\mathscr{G}(C_{jk}/A_{jk})$ which is induced by $\mathrm{Con}(A_i)$.

(b) We have $\pi(A_{jk}) = B_j$ for every $j \in J$ and every $k \in K(j)$ and we have $\pi^{-1}(B_j) = \dot{\bigcup}_{k\in K(j)} A_{jk}$.

(c) Every B_j is equipped with a Galois cover D_j.

(d) If $\dim A_{jk} = \dim B_j$, then $K[A_{jk}]$ is an integral extension of $K[B_j]$ and $K(D_j)$ contains the maximal separable extension of $K(B_j)$ in $K(C_{jk})$. We define a conjugacy domain $\mathrm{Con}_k(B_j)$ of $\mathscr{G}(D_j/B_j)$ by $\mathrm{Con}(A_{jk})$ as in Lemma 3.2

(e) If $\dim A_{jk} = \dim B_j + 1$, then $K(D_j)$ contains the maximal algebraic extension of $K(B_j)$ in $K(C_{jk})$. Also, the polynomial $h_{A_{jk},C_{jk},B_j,D_j}$ defined as in Lemma 3.1 does not vanish at any point of B_j.

We define a conjugacy domain $\mathrm{Con}_k(B_j)$ of $\mathscr{G}(D_j/B_j)$ by $\mathrm{Con}(A_{jk})$ as in Lemma 3.1.

The stratification $\mathscr{A}' = \langle \mathbb{A}^{n+1}, C_{jk} \to A_{jk}, \mathrm{Con}(A_{jk})\rangle_{j\in J, k\in K(j)}$ is a refinement of $\mathscr{A}$. For each $j \in J$ we define $\mathrm{Con}(B_j) = \bigcup_{k\in K(j)} \mathrm{Con}_k B_j$. Then $\mathscr{B} = \langle \mathbb{A}^n, D_j \to B_j, \mathrm{Con}(B_j)\rangle_{j\in J}$ is a Galois stratification of $\mathbb{A}^n$ and if $b \in \mathbb{A}^n(M)$, then $\mathrm{Ar}_{\mathscr{B},M}(b) \subseteq \mathrm{Con}(\mathscr{B})$ if and only if there exists an $a \in \mathbb{A}^{n+1}(M)$ such that $\pi(a) = b$ and $\mathrm{Ar}_{\mathscr{A}',M}(a) \subseteq \mathrm{Con}(\mathscr{A}')$, i.e., $\mathrm{Ar}_{\mathscr{A},M}(a) \subseteq \mathrm{Con}(\mathscr{A})$. ∎

Lemma 3.4 is used to "eliminate" an existential quantifier. Analogously, Lemma 3.5 is used to "eliminate" a universal quantifier.

LEMMA 3.5. *Let* $\mathscr{A} = \langle \mathbb{A}^{n+1}, C_i \to A_i, \mathrm{Con}(A_i)\rangle_{i\in I}$ *be a Galois stratification of* $\mathbb{A}^{n+1}$ *over* K. *Then there exists a Galois stratification* $\mathscr{B} = \langle \mathbb{A}^n, D_j \to B_j, \mathrm{Con}(B_j)\rangle_{j\in J}$ *such that for every* $b \in \mathbb{A}^n(M)$ *we have:* $\mathrm{Ar}_{\mathscr{B},M}(b) \subseteq \mathrm{Con}(\mathscr{B})$ *if and only if every* $a \in \mathbb{A}^{n+1}(M)$ *with* $\pi(a) = b$ *satisfies* $\mathrm{Ar}_{\mathscr{A},M}(a) \subseteq \mathrm{Con}(\mathscr{A})$.

In the explicit case $\mathscr{B}$ can be effectively computed if $\mathscr{A}$ is presented.

Proof. Let $\mathscr{A}^c = \langle \mathbb{A}^{n+1}, C_i \to A_i, \operatorname{Con}^c A_i \rangle_{i \in I}$ be the *complementary Galois stratification* to $\mathscr{A}$ of $\mathbb{A}^{n+1}$, where

$$\operatorname{Con}^c A_i = \{H \leqslant \mathscr{G}(C_i/A_i) \mid H \in \mathscr{C} \text{ and } H \notin \operatorname{Con}(A_i)\}.$$

By Lemma 3.4, we can find a Galois stratification $\mathscr{B}^c = \langle \mathbb{A}^n, D_j \to B_j, \operatorname{Con}^c B_j \rangle_{j \in J}$ of $\mathbb{A}^n$ over K such that for every $b \in \mathbb{A}^n(M)$ we have: $\operatorname{Ar}_{\mathscr{B}^c, M}(b) \subseteq \operatorname{Con}(\mathscr{B}^c)$ if and only there exists an $a \in \mathbb{A}^{n+1}(M)$ such that $\pi(a) = b$ and $\operatorname{Ar}_{\mathscr{A}^c, M}(a) \subseteq \operatorname{Con}(\mathscr{A}^c)$. The complementary Galois stratification to $\mathscr{B}^c$ of $\mathbb{A}^n$ is the Galois stratification we are looking for. ∎

Let $m, n \geqslant 0$ be integers, let $Q_1, \ldots, Q_m$ be quantifiers and let

$$\mathscr{A} = \langle \mathbb{A}^{m+n}, C_i \to A_i, \operatorname{Con}(A_i) \rangle_{i \in I}$$

be a Galois stratification of $\mathbb{A}^{m+n}$ over K. The expression

$$(Q_1 X_1) \cdots (Q_m X_m)[\operatorname{Ar}(X, Y) \subseteq \operatorname{Con}(\mathscr{A})], \tag{1}$$

with $X = (X_1, \ldots, X_m)$ and $Y = (Y_1, \ldots, Y_n)$ is said to be a *Galois formula (with respect to K and $\mathbf{C}$) in the free variables* $Y_1, \ldots, Y_n$. We denote it by $\theta = \theta(Y_1, \ldots, Y_n)$. For $b_1, \ldots, b_n \in M$ we write $M \models \theta(b)$ if $Q_1 a_1 \in M, \ldots, Q_m a_m \in M$ we have $\operatorname{Ar}_{\mathscr{A}, M}(a, b) \subseteq \operatorname{Con}(\mathscr{A})$. Here "$Q_i a_i \in M$" is to be read as "there exists an a_i in M" if Q_i is $\exists$, and as "for every a_i in M" if Q_i is $\forall$. If $n = 0$, then θ is said to be a *Galois sentence.*

Remark 3.6. Denote by $\mathscr{L}(K)$ the language of fields enriched with constant symbols for the elements of K. Every formula $\varphi(Y_1, \ldots, Y_n)$ of $\mathscr{L}(K)$ can be written (effectively, in the explicit case) in a prenex normal form:

$$(Q_1 X_1) \cdots (Q_m X_m) \left[\bigvee_{i=1}^{k} \bigwedge_{j=1}^{l} f_{ij}(X, Y) = 0 \wedge g_{ij}(X, Y) \neq 0 \right],$$

where $f_{ij}, g_{ij} \in K[X, Y]$. The formula in the brackets defines a K-constructible set $A \subseteq \mathbb{A}^{m+n}$. We can construct a K-normal basic stratification $\mathbb{A}^{m+n} = \dot{\bigcup}_{i \in I} A_i$ such that for every $i \in I$ either $A_i \subseteq A$ or $A_i \subseteq \mathbb{A}^{m+n} - A$. In the first case define $C_i = A_i$ and $\operatorname{Con}(A_i) = \{\langle id \rangle\}$, in the second case define $C_i = A_i$ and $\operatorname{Con}(A_i) =$ the empty family. Let $\mathscr{A}$ be the corresponding Galois stratification and define θ as in (1). Obviously, if $b_1, \ldots, b_n \in M$, then $M \models \theta(b)$ if and only if $M \models \varphi(b)$.

Applying Lemmas 3.4 and 3.5 on $\theta(Y_1, \ldots, Y_n)$ m times we eliminate its quantifiers one by one. Thus:

THEOREM 3.7. *Every Galois formula $\theta(Y_1, \ldots, Y_n)$ is equivalent to a Galois formula $\tau(Y_1, \ldots, Y_n)$ without quantifiers, i.e., for $b_1, \ldots, b_n \in M$ we have $M \models \theta(b)$ if and only if $M \models \tau(b)$.*

Moreover, τ depends only on θ, K and $\mathscr{C}$ but not on M and, in the explicit case, it can be effectively computed if θ is presented.

In particular, if $n = 0$, then θ is a Galois sentence and τ has the form $\mathrm{Ar}\, 0 \subseteq \mathrm{Con}$, where Con is a conjugacy domain of subgroups of $\mathscr{G}(L/K)$ belonging to $\mathscr{C}$, and L is a finite Galois extension of K. We therefore have the following

THEOREM 3.8. *Let θ be a Galois sentence. Then we can find (effectively, in the explicit case) a finite Galois extension L of K (that depends only on θ but not on $\mathscr{C}$) and a conjugacy domain* Con *of subgroups of $\mathscr{G}(L/K)$ belonging to $\mathscr{C}$ such that if M' is a Frobenius field containing K and $\mathrm{C}(M') = \mathscr{C}$, then $M' \models \theta$ if and only if $\mathscr{G}(L/L \cap M') \in \mathrm{Con}$.*

Interestingly enough we now find the converse to Remark 3.6 to be also true:

COROLLARY 3.9. *Let θ be a Galois sentence. Then one can find a sentence φ in $\mathscr{C}(K)$ such that*

$$M' \models \theta \Leftrightarrow M' \models \varphi$$

for any Frobenius field M' extending K with $\mathscr{C}(M') = \mathscr{C}$.

Proof. Let L and Con be as in Theorem 3.8. With no loss we may assume that Con is a conjugacy class, generated by some $H \in \mathscr{C}$. Find $\alpha_0, \alpha_1, \ldots, \alpha_m \in L$, such that $K(\alpha_0) = L(H)$, $K(\alpha_1), \ldots, K(\alpha_m) = L$ are all the distinct intermediate fields in $L/L(H)$, and find their respective irreducible polynomials $f_0, \ldots, f_m$ over K. The sentence

$$(\exists X)[f_0(X) = 0] \wedge \bigwedge_{i=1}^{m} (\forall Y)[f_i(Y) \neq 0]$$

is obviously the desired sentence φ. ∎

4. Model-Theoretic Applications

As in Section 3 we consider a fixed basic field K. We start with applications to general Frobenius fields containing K and the specialize to the case where the absolute Galois groups are free.

THEOREM 4.1. *Let M_1 and M_2 be two perfect Frobenius fields containing K. Then M_1 is elementarily equivalent to M_2 with respect to the language $\mathscr{L}(K)$ if and only if $\mathscr{C}(M_1) = \mathscr{C}(M_2)$ and $K_s \cap M_1 \cong_K K_s \cap M_2$. In particular, if M_1 is algebraically closed in M_2 and $\mathscr{C}(M_2) = \mathscr{C}(M_2)$, then M_1 is an elementary subfield of M_2.*

Proof. The "if" part is an immediate corollary of Theorem 3.8 and Remark 3.6. the "only if" part is a special case of Lemma 5 of Ax [1]. ∎

Let $\mathscr{C}$ be a family of finite groups and denote by $T(K, \mathscr{C})$ the theory of all sentences θ in $\mathscr{L}(K)$ that are true in every perfect Frobenius field M' that contains K and satisfies $\mathscr{C}(M') = \mathscr{C}$.

The following Lemma is needed to establish a decision procedure for $T(K, \mathscr{C})$.

LEMMA 4.2. *Let G be a countably generated profinite group that has the embedding property and such that $cd(G) \leqslant 1$. Let L be a finite Galois extension of a countable Hilbertian field K and let H be a subgroup of $\mathscr{G}(L/K)$. If $H \in \mathscr{C}(G)$, then there exists a perfect Frobenius field M, algebraic over K, with $G(M) \cong G$ such that $L \cap M$ is the fixed field of H in L.*

Proof. Denote by K_0 the fixed field of H in L. We first show that there exists a PAC algebraic extension E of K_0 and a Galois extension F of E with G as the Galois group such that $L \subseteq F$ and the map Res_L: $\mathscr{G}(F/E) \to \mathscr{G}(L/K_0)$ is surjective. To do this we consider a sequence $\{(f_i(T_1, \ldots, T_{r_i}, X), g_i(T_1, \ldots, T_{r_i}))\}_{i=1}^{\infty}$ of all pairs of polynomials with coefficients in K_0 such that f_i is absolutely irreducible and $g_i \neq 0$. We may view G as a projective limit of a sequence

$$H = G_0 \xleftarrow{\pi_0} G_1 \xleftarrow{\pi_1} G_2 \xleftarrow{\pi_2} \cdots$$

of finite groups G_i with epimorphisms π_i. Then we construct, by induction, increasing sequences $K_0 \subseteq K_1 \subseteq K_2 \subseteq \cdots$ and $L = L_0 \subseteq L_1 \subseteq L_2 \subseteq \cdots$ of finite separable extensions of K_0 such that for every $i \geqslant 0$:

(a) there exist $a_1, \ldots, a_{r_i}, b$ in K_i such that $f_i(a, b) = 0$ and $g_i(a) \neq 0$ (if $i \geqslant 1$);

(b) the field L_i is a Galois extension of K_i and there is an isomorphism $\psi_i: \mathscr{G}(L_i/K_i) \xrightarrow{\sim} G_i$;

(c) the following diagram is commutative:

$$\begin{array}{ccc} \mathscr{G}(L_{i+1}/K_{i+1}) & \xrightarrow{\mathrm{Res}} & \mathscr{G}(L_i/K_i) \\ \downarrow{\scriptstyle \psi_{i+1}} & & \downarrow{\scriptstyle \psi_i} \\ G_{i+1} & \xrightarrow{\pi_i} & G_i \end{array}$$

Indeed, the transition from K_i to K_{i+1} can be done by first adjoining a root (a, b) of f_{i+1} such that $K_i(a, b)$ is linearly disjoint from L_i over K_i and $g_{i+1}(a) \neq 0$. Then one applies Theorem 3 of Kuyk [15] to construct K_{i+1}

and L_{i+1}. The desired fields E and F can now be taken as $E = \bigcup_{i=1}^{\infty} K_i, F = \bigcup_{i=1}^{\infty} L_i$. That E is PAC follows by Weil's "descent" theory (see also the proof of Lemma 4.1 of [4]).

Thus we obtain an exact sequence

$$1 \to G(F) \to G(E) \to G \to 1$$

that splits, since $cd(G) \leqslant 1$ (see Gruenberg [7, p. 164]). Hence there exists a perfect algebraic extension M of E with $G(M) \cong G$ such that $F \cap M = E$, which implies $L \cap M = K_0$. Again, M is an Ax-field, since E is an Ax-field. By assumption $G(M)$ has the embedding property, hence M is a Frobenius field by Theorem 1.2. ∎

COROLLARY 4.3. *Let G be a countably generated profinite group. Then there exists a countable Frobenius field M with $G(M) \cong G$ if and only if G has the embedding property and $cd(G) \leqslant 1$.*

Proof. By virtue of Lemma 4.2 it suffices to remind that if M is an Ax-field, then $cd(G(M)) \leqslant 1$ (see [2, p. 269]). ∎

Remarks. (a) Using Lemmas 6.1, 6.3 and 2.3 of [11], one can prove Lemma 4.2 and hence its corollary for the case in which the restriction on G to be countably generated is omitted. However, the field M obtained in this case is no longer algebraic over K nor is it countable. This method is used by Lubotzky and van den Dries in [19] to prove that for every profinite group G with $cd(G) \leqslant 1$ there exists a PAC field M such that $G(M) \cong G$.

(b) There exist profinite groups G that have the embedding property and for which $cd(G) \geqslant 2$. For example, if $G = \mathbb{Z}_p \times \mathbb{Z}_p$, then $cd(G) = 2$, by Proposition 4.4 [22, p. 221], while it has a pair of free generators and hence it has the embedding property.

Problem 4.4. Does there exist a profinite group G with $cd(G) \leqslant 1$ that does not have the embedding property?

The existence of such a group would provide an example of a PAC field which is not a Frobenius field.

THEOREM 4.5. *Let K be a Hilbertian field with elimination theory. If M is a Frobenius field containing K, and $\mathscr{C} = \mathscr{C}(M)$ is a primitive recursive family of finite groups, then the theory $T(K, \mathscr{C})$ is primitive recursive.*

Proof. Using the Skolem–Löwenheim theorem one can assume, without loss of generality, that M is countable. Hence $G(M)$ is countably generated and it has the embedding property.

Starting now with a given sentence θ of $\mathscr{L}(K)$ we find a finite Galois extension L of K and a conjugacy class Con as in Theorem 3.8. Applying

Lemma 4.2 for $G = G(M)$ we find that $\theta \in T(K, \mathscr{C})$ if and only if $\mathrm{Con} = \{H \leqslant \mathscr{G}(L/K) \mid H \in \mathscr{C}\}$. The validity of the last equality can be effectively checked, since we are in the explicit case. ∎

Let now $\mathscr{D}$ be a family of finite groups closed under the operation of taking subgroups, homomorphic images and extensions (we then say that $\mathscr{D}$ is a *full family*), and let $e \geqslant 0$ be an integer. Consider the subfamily $\mathscr{D}_e = \{G \in \mathscr{D} \mid \mathrm{rank}(G) \leqslant e\}$. If M is a field, then $\mathscr{C}(M) = \mathscr{D}_e$ if and only if $G(M) \cong \hat{F}_e(\mathscr{D}) =$ the free pro-$\mathscr{D}$-group on e generators (cf. [10, Theorem 2.4] and Schuppar [24, Satz 2.1]). If M is a Frobenius countable field, then $\mathscr{C}(M) = \mathscr{D}$ if and only if $G(M) \cong \hat{F}_\omega(\mathscr{D}) =$ the free pro-$\mathscr{D}$-group on $\aleph_0$ generators. We also recall that a $\mathscr{D}$-free PAC field M is a Frobenius field.

LEMMA 4.6. *Under the above assumptions* $cd(\hat{F}_e(\mathscr{D})) \leqslant 1$ *for every* $0 \leqslant e \leqslant \omega$.

Proof. Consider the (non-proper) embedding problem

$$\begin{array}{ccccccccc} & & & & & & \hat{F}_e(\mathscr{D}) & & \\ & & & & & & \downarrow \pi & & \\ 1 & \longrightarrow & C & \longrightarrow & B & \xrightarrow{\beta} & A & \longrightarrow & 1 \end{array}$$

where the short sequence of finite groups is exact, π if surjective and C is an elementary abelian p-group. We have to show that there exists a homomorphism $\gamma: \hat{F}_e(\mathscr{D}) \to B$ such that $\beta \circ \gamma = \pi$ (cf. Ribes [22, p. 211]). We consider the case where $e < \omega$. The case $e = \omega$ may be treated similarly. Observe that $A \in \mathscr{D}$. If $\mathbb{Z}/p\mathbb{Z} \in \mathscr{D}$, then $B \in \mathscr{D}$ and hence γ can be defined by considering generators $x_1, \ldots, x_e$ for $\hat{F}_e(\ )$, taking elements $b_1, \ldots, b_e$ such that $\beta b_i = \pi x_i$ for $i = 1, \ldots, e$, and defining $\gamma x_i = b_i$ for $i = 1, \ldots, e$. If $Z/pZ \notin \mathscr{D}$, then the order of A is relatively prime to p. In this case the short sequence splits, by Schur–Zassenhaus' Theorem and the existence of γ is obvious. ∎

It follows from Lemmas 4.2 and 4.6 that for every $0 \leqslant e \leqslant \omega$ there exists a Frobenius field with $\hat{F}_e(\mathscr{D})$ as its absolute Galois group. The following Theorem uses this fact and shows that, in a certain sense, the theory $T(K, \mathscr{D})$ is a limit of the theories $T(K, \mathscr{D}_e)$ as e approaches ω.

THEOREM 4.7. *Let* $\mathscr{D}$ *be a full family of finite groups, suppose that* K *is a countable Hilbertian field and let* θ *be a sentence of* $\mathscr{L}(K)$. *Then* $\theta \in T(K, \mathscr{D})$ *if and only if there exists an* e_0 *such that* $\theta \in T(K, \mathscr{D}_e)$ *for every* $e_0 \leqslant e < \omega$.

In the explicit case the theories $T(K, \mathscr{D}_e)$ and $T(K, \mathscr{D})$ are primitive recursive. Moreover, the function "$e_0(\theta) =$ the smallest e_0 which $\theta \in T(K, \mathscr{D}_e)$ for every $e \geqslant e_0$" is primitive recursive. Hence the intersection $\bigcap_{e=1}^{\infty} T(K, \mathscr{D}_e)$ is also a primitive recursive theory.

Proof. Only the existence of e_0 has to be proved. The rest is a special case of Theorem 4.5. Indeed, let θ be a sentence of $\mathscr{L}(K)$ and consider the elimination of quantifiers procedure via Galois stratification of θ, as described in Section 3. Denote by e_0 the maximal rank of the (finitely many) subgroups of the Galois groups of the Galois covers that occur in the procedure. If $e \geqslant e_0$, then the conjugacy domain Con of subgroups of $\mathscr{G}(L/K)$ (we are using the notation of Theorem 4.6) obtained with respect to the family is equal to the corresponding domain Con_e obtained with respect to $\mathscr{D}_e$. Hence $\theta \in T(K, \mathscr{D}_e)$ for every $\omega > e \geqslant e_0$ if and only if $\theta \in T(K, \mathscr{D})$. ∎

Consider now the special case where $\mathscr{D}$ is the family of all finite groups. Write $T_e(K)$ and $T_\omega(K)$ for $T(K, \mathscr{D}_e)$ and $T(K, \mathscr{D})$. For every $\sigma_1, \ldots, \sigma_e \in G(K)$ we denote by $\tilde{K}(\sigma)$ the fixed field of $\sigma_1, \ldots, \sigma_e$ in $\tilde{K}$. Then $\tilde{K}(\sigma)$ is an e-free Ax-field for almost all $\sigma \in G(K)^e$ (cf. Lemma 7.2 of [13]). Here "almost all" is used in the sense of the normalized Haar measure μ of the compact group $G(K)$. For every sentence θ of $\mathscr{L}(K)$ we denote $A_e(\theta) = \{\sigma \in G(K)^e \mid \tilde{K}(\sigma) \models \theta\}$. Then Theorems 3.8 and 4.7 yield the following strengthening of the results of [13] and [11].

THEOREM 4.8. *Let K be a countable Hilbertian field and let θ be a sentence of $\mathscr{L}(K)$. Then:*

(a) *The set $A_e(\theta)$ is measurable and $\mu(A_e(\theta))$ is a rational number.*

(b) *We have $\mu(A_e(\theta)) = 1$ if and only if $\theta \in T_e(K)$, i.e., θ is true in every e-free Ax-field that contains K.*

(c) *We have $\theta \in T_\omega(K)$ if and only if there exists an e_0 such that $\theta \in T_e(K)$ for every $e_0 \leqslant e < \omega$.*

(d) *If K has elimination theory, then the theories $T_e(K)$, $T_\omega(K)$ and $\bigcap_{e=1}^{\infty} T_e(K)$ as well as the functions $\mu(A_e(\theta))$ and $e_0(\theta)$ are primitive recursive.*

Proof. (a) Let L and Con be as in Theorem 3.8. Then $\mu(A_e(\theta))$ is equal to the number of e-tuples $(\bar{\sigma}_1, \ldots, \bar{\sigma}_e)$ in $\mathscr{G}(L/K)^e$ that generate groups belonging to Con, divided by $|L:K|^e$.

(b) If $\mu(A_e(\theta)) = 1$ and if F is an e-free Ax-field, then there exists a $\sigma \in A_e(\theta)$ such that $L \cap \tilde{K}(\sigma) = L \cap F$. It follows by Theorem 3.8 that θ is true in F.

The rest of the Theorem is a special case of Theorem 4.7. ∎

Another case of interest is where $\mathscr{D}$ is the family of all finite p-groups. In this case $\mathscr{D}$ is primitive recursive and Theorem 4.7 applies.

More generally, let S be a non-empty set of prime numbers and consider the family of all finite nilpotent groups whose orders are divisible only by primes belonging to S. This is a primitive recursive family but it is not closed under extensions. However, the free pro-$\mathscr{D}$-group on e generators is $\hat{F}_e(\mathscr{D}) = \prod_{p\in S} \hat{F}_e(p)$, for every $0 \leqslant e \leqslant \omega$. It has a system of e free generators and has therefore the embedding property. Moreover $cd(\hat{F}_e(\mathscr{D})) = \max_{p\in S} cd_p(\hat{F}_e(p)) = 1$. Thus, the proof of Theorem 4.7 remains valid in this case and therefore the same applies for its consequences.

We end up this work by asking:

Problem 4.9. Is the theory of all perfect Frobenius fields decidable?

Note added in proof. Most of the problems raised in this work have been resolved since this paper was submitted for publication. Problems 1.7, 1.8, and 4.5 got negative answers by Haran and Lubotzky's Proposition 3.3 [Embedding covers and the theory of Frobenius fields, *Israel J. Math.* **41** (1982), 181–201]. Ershov and Fried [Frattini covers and projective groups without the extension property, *Math. Anal.* **253** (1980), 233–239] were the first to give a negative answer to Problem 4.5. Finally, Haran and Lubotzky [*ibid.*, Theorem 4.4] proved that the theory of perfect Frobenius fields is primitive recursive. This is a positive solution to Problem 4.10. The recursiveness of the theory of Frobenius fields is also proved by Cherlin, van den Dries, and Macintyre [The elementary theory of regularly closed fields, *Crelle J.*, in press].

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.* **88** (1968), 239–271.
3. M. FRIED, Toward a general theory of diophantine problems with applications to P-adic fields and fields of finite corank, unpublished.
4. M. FRIED AND M. JARDEN, Diophantine properties of subfields of $\tilde{\mathbb{Q}}$, *Amer. J. Math.* **100** (1978), 653–666.
5. M. FRIED AND G. SACERDOTE, Solving diophantine problems over all residue class fields of a number field and all finite fields, *Ann. of Math.* **104** (1976), 203–233.
6. A. FRÖHLICH AND J. C. SHEPHERDSON, Effective procedures in field theory, *Philos. Trans. Roy. Soc. London Ser. A* **248** (1955), 407–432.
7. K. W. GRUENBERG, Projective profinite groups, *J. London Math. Soc.* **42** (1967), 155–165.
8. G. HERMANN, Die Frage der endlich vielen Schritte in der Theorie der Polynomideals, *Math. Ann.* **95** (1926), 736–788.
9. H. HERMES, "Enumerability, Decidability, Computability," Springer-Verlag, Berlin/Heidelberg/New York, 1965.
10. M. JARDEN, Algebraic extensions of finite corank of Hilbertian fields, *Israel J. Math.* **18** (1974), 279–307.
11. M. JARDEN, The elementary theory of ω-free Ax fields, *Inven. Math.* **38** (1976), 187–206.

12. M. JARDEN, An analogue of Čebotarev density theorem for fields of finite corank, *J. Math. Kyoto Univ.* **20** (1980), 141–147.
13. M. JARDEN AND U. KIEHNE, The elementary theory of algebraic fields of finite corank, *Invent. Math.* **30** (1975), 275–294.
14. M. JARDEN AND P. ROQUETTE, The Nullstellensatz over p-adically closed fields, *J. Math. Soc. Japan* **32** (1980), 425–460.
15. W. KUYK, Generic approach to the Galois embedding and extension problem, *J. Algebra* **9** (1968), 393–407.
16. S. LANG, "Algebraic Geometry," Interscience, New York, 1958.
17. S. LANG, "Algebra," Addison–Wesley, Reading, Mass., 1965.
18. A. LEVI, Notes of a seminar on decision procedures given at the Hebrew University, Jerusalem, 1965.
19. A. LUBOTZKY AND L. VAN DEN DRIES, Normal subgroups of free profinite groups, *Israel J. Math.* **39** (1981), 25–45.
20. O. V. MEL'NIKOV, Normal subgroups of free profinite groups, *Math. USSR-Izv.* **12**(1)(1978), 1–20.
21. M. O. RABIN, Computable algebra, general theory and theory of computable fields, *Trans. Amer. Math. Soc.* **95** (1960), 341–360.
22. L. RIBES, Introduction to profinite groups and Galois cohomology, Queen papers in pure and applied Mathematics 24, Queen's University, Kingston, Ontario, 1970.
23. P. ROQUETTE, Notes on Hilbert's Irreducibility Theorem, Heidelberg, 1978.
24. B. SCHUPPAR, Modelltheoretische Untersuchungen zur Galois-theorie von Funktionenkörpern, *Crelle J.*, in press.
25. G. STOLZENBERG, Constructive normalization of an algebraic variety, *Bull. Amer. Math. Soc.* **74** (1968), 595–599.
26. B. L. VAN DER WAERDEN, "Modern Algebra I," Ungar, New York, 1953.
27. B. L. VAN DER WAERDEN, "Modern Algebra II," Ungar, New York, 1950.
28. B. L. VAN DER WAERDEN, "Einführung in die algebraische Geometrie," Springer-Verlag, Berlin/Heidelberg/New York, 1973.
29. O. ZARISKI AND P. SAMUEL, "Commutative Algebra I," Springer-Verlag, New York/Heidelberg/Berlin, 1975.
30. O. ZARISKI AND P. SAMUEL, "Commutative Algebra II," Springer-Verlag, New York/Heidelberg/Berlin, 1975.