Math. Ann. 253, 233–239 (1980)

Mathematische Annalen

Frattini Covers and Projective Groups Without the Extension Property

Y. Ershov[1]* and M. Fried[2]**

1 Department of Mathematics, Novosibirsk, USSR
2 Department of Mathematics, University of California, Irvine, CA 92717, USA

Let F be a field, $\bar{F}$ a fixed algebraic closure of F, and $G(\bar{F}/F)$ the Galois group of automorphisms of $\bar{F}$ fixed on F. The elementary theory of F is highly dependent on the group $G(\bar{F}/F)$. For example, let $\varphi(F)$ be the collection of finite quotient groups of $G(\bar{F}/F)$. Let $H_1, \ldots, H_t$, $G_1, \ldots, G_r$ be finite groups, and consider the statement $P(\mathbf{H};\mathbf{G};F)$:

$$H_i \in \varphi(F), \quad i=1,\ldots,t$$

and

$$G_j \notin \varphi(F), \quad j=1,\ldots,r.$$

Let S_n be the symmetric group on $\{1,2,\ldots,n\}$. For a given finite group $G \subseteq S_n$, methods of Kronecker [Wae, Sect. 61] interpret the existence of a finite Galois extension F_1/F having group G as a problem of finding, among an explicit collection of polynomials $m(z;x_1,\ldots,x_n)$ with coefficients in F, one that has an irreducible factor m_1 (over F) for which

$$\{\sigma \in S_n \mid m_1(z;x_{(1)\sigma},\ldots,x_{(n)\sigma}) \equiv m_1(z;x_1,\ldots,x_n)\} \simeq G.$$

From this observation it is an exercise to show that the statement $P(\mathbf{H};\mathbf{G};F)$ is an elementary statement over F.

There is a collection of fields F for which a primitive recursive (resp., recursive) procedure for deciding the statements $\{P(\mathbf{H};\mathbf{G};F)\}$ for all possible $\mathbf{H},\mathbf{G}$ gives a primitive recursive (resp., recursive) procedure for deciding the elementary theory of F. These fields are called *frobenius fields* (Sect. 3) and the axioms for F include two essential properties:

(i) F is a P.A.C. field (pseudo-algebraically closed; every absolutely irreducible nonempty algebraic set over F has a point with coordinates in F); and

(ii) $G(\bar{F}/F)$ has the *extension property* (Sect. 2).

* An outline of these results sent to Yale revealed that Macintyre and van den Dries have also produced projective groups lacking the extension property

** Supported by N.S.F. Grant MCS-78-02669

0025-5831/80/0253/0233/$01.40

It is part of folklore that the P.A.C. property for a field F has a simple relation to a property of $G(\bar{F}/F)$: if F is P.A.C., then $G(\bar{F}/F)$ is a *profinite projective* group (Sect. 1); and, conversely if G^* is a profinite projective group, there *exists* a field F for which $G(\bar{F}/F) \simeq G^*$. The first half appears in [A, FJH, DL] contain proofs of the second half. In Sect. 2 there is an example of a profinite projective group without the *extension property*, and Sect. 3 discusses the production and significance of P.A.C. fields which are not frobenius fields.

1. Frattini Covers and the Universal Frattini Cover of a Group

Let G be a group. The *frattini subgroup* of G, $\mathrm{Fr}(G)$, is the intersection of the maximal proper subgroups of G. If G has no maximal proper subgroups, define $\mathrm{Fr}(G) = G$. An element $g \in G$ is said to be a *nongenerator* of G if for *every* subset T of G for which $T \cup \{g\}$ generates G, T generates G.

Lemma 1.1 [H, p. 157]. *The nongenerators of G are exactly the elements of* $\mathrm{Fr}(G)$.

Let $\varphi: H \to G$ be a homomorphism of groups. Then H (or (φ, H)) is said to be a *frattini cover* (of G) if $\ker(\varphi) \subset \mathrm{Fr}(H)$ and φ is surjective.

Lemma 1.2. *A surjective homomorphism $\varphi: H \to G$ is a frattini cover if and only if for every subset T of H, $\{\varphi(t) | t \in T\} \stackrel{\mathrm{def}}{=} \varphi(T)$ generates G if and only if T generates H.*

Proof. Suppose $\varphi: H \to G$ is a frattini cover, and T is a subset of H for which $\varphi(T)$ generates G. Then $\ker(\varphi) \cup T$ generates H. An induction using Lemma 1.1 shows that T generates H.

Conversely, suppose $\varphi: H \to G$ is surjective and each subset T of H generates H if $\varphi(T)$ generates G. Let $h \in \ker(\varphi)$, and let T be a subset of H for which $T \cup \{h\}$ generates H. Then $\varphi(T \cup \{h\})$ generates G, so $\varphi(T)$ generates G. By hypothesis, T generates H, and Lemma 1.1 implies that $h \in \mathrm{Fr}(H)$. □

Let $\varphi_i: H_i \to G$ be a homomorphism, $i = 1, 2$. Define the group $H_1 \underset{G}{\times} H_2$ to be the subgroup of $H_1 \times H_2$ consisting of the pairs $\{(h_1, h_2) | \varphi_1(h_1) = \varphi_2(h_2)\}$: the *fiber product of H_1 and H_2 over G*. Let $\mathrm{pr}_i : H_1 \underset{G}{\times} H_2 \to H_i$ be the natural projection (a homomorphism) onto the i-th factor. If φ_1 and φ_2 are surjective, then so are pr_1 and pr_2.

For the sake of simplicity, from this point on, G is a finite group. Consider the set $\mathscr{FC}(G)$ of frattini covers of G by finite groups. Let $\varphi_i: H_i \to H_0$ be a homomorphism, $i = 1, 2$.

Lemma 1.3. *Assume that $\varphi_i: H_i \to G$ is an element of $\mathscr{FC}(G)$, $i = 1, 2$, and that L is a minimal subgroup of $H_1 \underset{G}{\times} H_2$ that maps surjectively to G under $\varphi_1 \circ \mathrm{pr}_1$. Then pr_i restricted to L maps surjectively to H_i, $i = 1, 2$, and $L \xrightarrow{\varphi_1 \circ \mathrm{pr}_1} G$ is a frattini cover.*

Proof. Let T be a subset of L for which $\varphi_1 \circ \mathrm{pr}_1(T)$ generates G. Then, by Lemma 1.2, $\mathrm{pr}_i(T)$ generates H_i. Thus, if $\bar{L}$ is the subgroup of L generated by T, then the restriction of pr_i to $\bar{L}$ maps surjectively to H_i, $i = 1, 2$. Since L is minimal with

respect to this property, $\bar{L}=L$, and T generates L. From Lemma 1.2, $\varphi_1 \circ \mathrm{pr}_1 : L \to G$ is a frattini cover. □

An addition to the notation facilitates the construction of a *partial ordering* on $\mathscr{FC}(G)$. For $\alpha \in \mathscr{FC}(G)$ write $\alpha=(\varphi_\alpha, H_\alpha)$. Write $\alpha \to \beta$ if there exists $\gamma \in \mathscr{FC}(G)$ for which $H_\alpha \subset H_\beta \underset{G}{\times} H_\gamma$ and φ_α is given by $\varphi_\beta \circ \mathrm{pr}_\beta : H_\beta \underset{G}{\times} H_\gamma \to G$ restricted to H_α. Denote by $\mathrm{pr}_{\beta\alpha}$ the restriction of pr_β to H_α. From Lemma 1.3, this partial ordering on $\mathscr{FC}(G)$ is a *projective system* [N, p. 27] of surjective homomorphisms of frattini covers of G. Denote by G^{FC} the projective limit of this projective system. This (infinite) group, with the natural map $\varphi_{\mathrm{FC}} : G^{\mathrm{FC}} \to G$, is called *universal frattini cover of* G. The natural maps $\varphi_{\alpha,\mathrm{FC}} : G^{\mathrm{FC}} \to H_\alpha$ for $\alpha \in \mathscr{FC}(G)$ induce a profinite group structure on G^{FC}: a cofinal collection of neighborhoods of the origin is given by $\{\ker(\varphi_{\alpha,\mathrm{FC}})\}_{\alpha \in \mathscr{FC}(G)}$.

Recall the definition of a *projective* profinite group [N, p. 63]. A profinite group G^* is projective if, given a diagram

$$\begin{array}{ccccc} G_1 & \xrightarrow{\psi_{21}} & G_2 & \longrightarrow & 0 \\ & & \uparrow{\scriptstyle \psi_2} & & \\ & & G^* & & \end{array} \tag{1.1}$$

where the upper row is an exact sequence of finite groups and $\ker(\psi_2)$ is an open subgroup of G^*, then there exists $\psi_1 : G^* \to G_1$ such that $\psi_{21} \circ \psi_1 = \psi_2$.

Theorem 1.1. *The cover $\varphi_{\mathrm{FC}} : G^{\mathrm{FC}} \to G$ is a frattini cover of G, and G^{FC} with the collection of maps $\{\varphi_{\alpha,\mathrm{FC}}\}_{\alpha \in \mathscr{FC}(G)}$ is universal with respect to maps to the projective system $\mathscr{FC}(G)$. Also, G^{FC} is a projective group.*

Proof. All but the last sentence follows from the properties of projective systems. One may translate the statement that G^{FC} is projective into a statement about finite groups: for a diagram of finite groups

$$\begin{array}{ccccc} G_1 & \xrightarrow{\psi_{21}} & G_2 & \longrightarrow & 0 \\ & & \uparrow{\scriptstyle \psi_2} & & \\ & & H_2 & & \end{array} \tag{1.2a}$$

where $H_2 \xrightarrow{\varphi_2} G$ is a frattini cover of G and the upper row is exact, then there exists a frattini cover $H_1 \xrightarrow{\varphi_1} G$ and a homomorphism $\psi_1 : H_1 \to G_1$ for which the diagram

$$\begin{array}{ccccc} H_1 \underset{G}{*} H_2 & \xrightarrow{\psi_1 \circ \mathrm{pr}_1} & G_1 & \xrightarrow{\psi_{21}} & G_2 \\ & {\scriptstyle \mathrm{pr}_2}\searrow & & \nearrow{\scriptstyle \psi_2} & \\ & & H_2 & & \end{array} \tag{1.2b}$$

is commutative.

With no loss, by replacing G_2 by the image of ψ_2 and G_1 by ψ_{21}^{-1} of the image of ψ_2, one may assume that ψ_2 is surjective. Consider a group $\bar{H}$, minimal among the subgroups L of $G_1 \underset{G_2}{\times} H_2$ for which restriction of pr_2 to L is surjective. Lemma 1.2 is easily applied to see that $\varphi_2 \circ \mathrm{pr}_2 : \bar{H} \to G$ is a frattini cover: by the proof of Lemma 1.3, a subset T of $\bar{H}$ generates $\bar{H}$ if and only if $\mathrm{pr}_2(T)$ generates H_2, which, by Lemma 1.2 is equivalent to $\varphi_2 \circ \mathrm{pr}_2(T)$ generates G. Thus, the theorem is concluded by taking $\bar{H} = H_1$ and by taking ψ_1 equal to the restriction to $\bar{H}$ of $\mathrm{pr}_1 : G_1 \underset{G_2}{\times} H_2 \to G_1$.

Corollary 1.1. *Let*

$$\begin{array}{ccc} \varphi_{\mathrm{FC}} : G^{\mathrm{FC}} & \longrightarrow & G \\ & {\scriptstyle\psi}\searrow \quad \nearrow{\scriptstyle\gamma} & \\ & H & \end{array}$$

be a commutative diagram in which ψ is surjective. Then $H \xrightarrow{\gamma} G$ is a frattini cover of G.

Proof. Use Lemma 1.2. For T a subset of H for which $\gamma(T)$ generates G, let T' be a subset of G^{FC} that maps one-one and onto T under ψ. Then $\gamma \circ \psi(T') = \gamma(T) = \varphi_{\mathrm{FC}}(T')$ generates G, so T' generates G^{FC}. Thus $\psi(T') = T$ generates H, and Lemma 1.2 implies that $\gamma : H \to G$ is a frattini cover. □

2. A Projective Profinite Group Without the Extension Property

Recall the *extension property* for a profinite group G^*. Let $\varphi(G^*)$ be the collection of finite groups that are quotients of G^* by normal open subgroups of G^*. Then G^* is said to have the extension property if for K a normal open subgroup of G^* and $G_1 \in \varphi(G^*)$ with $\beta : G_1 \to G^*/K \to 1$ exact, there exists a surjective homomorphism $\theta : G^* \to G_1$ for which $\beta \circ \theta$ is the canonical map.

Let a, b, c be generators of a group $G(a, b, c)$ where the orders of a and c are 2, the order of b is 3, $a^{-1} \cdot b \cdot a = b^{-1}$, and c commutes with a and b. Let $G(a, b, c)^{\mathrm{FC}}$ be the universal frattini cover of $G(a, b, c)$. *Note that $G(a, b, c)$ is generated by 2 elements: a and $b \cdot c$.*

Theorem 2.1. *The group $G(a, b, c)^{\mathrm{FC}}$ is projective, but it does not have the extension property.*

Proof. From Theorem 1.1, one must only show that $G(a, b, c)^{\mathrm{FC}}$ does not have the extension property. Consider the diagram

$$\begin{array}{ccccc} G(a,b,c)^{\mathrm{FC}} & \xrightarrow{\varphi_{\mathrm{FC}}} & G(a,b,c) & \xrightarrow{\beta_a} & Z/(2) \\ & & & & \uparrow{\scriptstyle\beta_c} \\ & & & & G(a,b,c) \end{array} \tag{2.1}$$

where the map β_a is the surjective map that sends b and c to the identity in $Z/(2)$ and β_c is the surjective map that sends a and b to the identity in $Z/(2)$. If $G(a, b, c)^{\mathrm{FC}}$

has the extension property, then there exists $\varphi^*: G(a,b,c)^{FC} \to G(a,b,c)$ with $\beta_c \circ \varphi^* = \beta_a \circ \varphi_{FC}$ and φ^* is surjective.

Denote by $G(a,b,c) \underset{Z/(2)}{\times} G(a,b,c)$ the fiber product (Sect. 1) computed from the diagram

$$\begin{array}{ccc} G(a,b,c) & & G(a,b,c) \\ & {\scriptstyle \beta_a}\searrow \quad \swarrow{\scriptstyle \beta_c} & \\ & Z/(2) & \end{array} \tag{2.2}$$

Then the map

$$G(a,b,c)^{FC} \xrightarrow{(\varphi_{FC}, \varphi^*)} G(a,b,c) \underset{Z/(2)}{\times} G(a,b,c)$$

(given by $g \in G(a,b,c)^{FC} \to (\varphi_{FC}(g), \varphi^*(g))$) has image equal to a subgroup L of $G(a,b,c) \underset{Z/(2)}{\times} G(a,b,c)$ with the following property:

L is mapped surjectively onto $G(a,b,c)$ by the restriction of pr_i to L, $i=1,2$. (2.3a)

Let a', b', and $c' \in G(a,b,c)^{FC}$ be elements that map (resp.) to a, b, c under φ^{FC}. Since $\varphi^{FC}: G(a,b,c)^{FC} \to G(a,b,c)$ is a frattini cover, $\{a', b' \cdot c'\}$ generates $G(a,b,c)^{FC}$ (Lemma 1.2). Thus, L is generated by the image of $\{a', b' \cdot c'\}$:

L is generated by 2 elements, and (Corollary 1.1) $\mathrm{pr}_1: L \to G(a,b,c)$ is a frattini cover. (2.3b)

The remainder of the proof consists of showing that there is *no* subgroup L of $G(a,b,c) \underset{Z/(2)}{\times} G(a,b,c)$ having properties (2.3a) and (2.3b): therefore, the surjective map φ^* does not exist. This is divided into steps.

Step 1: A presentation of $G(a,b,c) \underset{Z/(2)}{\times} G(a,b,c)$

It is best to denote the left hand copy by $G(a,b,c)_a$, the right hand copy by $G(a,b,c)_c$; both are isomorphic to $S_3 \times Z/(2)$. An element of $G(a,b,c) \underset{Z/(2)}{\times} G(a,b,c)$ is represented by a 4-tuple (g_a, g'_a, g_c, g'_c): $g_a, g_c \in S_3$ and $g'_a, g'_c \in Z/(2)$; in representing $Z/(2)$ as the two element set $\bar{0}, \bar{1}$, the elements a, b, c in $G(a,b,c)_a$ may be taken as (resp.) $((12)_a, \bar{0}_a)$, $((123)_a, \bar{0}_a)$, $(\overline{1d}_a, \bar{1}_a)$, and the elements a, b, c in $G(a,b,c)_c$ may be taken as (resp.) $((12)_c, \bar{0}_c)$, $((123)_c, \bar{0}_c)$, $(\overline{1d}_c, \bar{1}_c)$; and g_a is of order exactly 2 if and only if $g'_c = \bar{1}_c$.

Step 2: A description of generators for L satisfying (2.3a) *and* (2.3b)

Assume there is a group L satisfying (2.3a) and (2.3b), and let $g(i) = (g_a(i), g_a(i)', g_c(i), g_c(i)')$, $i=1, 2$ be generators of L. To assure that

$$\mathrm{pr}_a: G(a,b,c)_a \underset{Z/(2)}{\times} G(a,b,c)_c \to G(a,b,c)_a$$

restricted to L is surjective, with no loss one may assume that $g_a(1)$ is of order 2, $g_a(2)$ is of order 3, and $g_a(2)' = \bar{1}_a$. From Step 1, $g_c(1)' = \bar{1}_c$, $g_c(2)' = \bar{0}_c$. To assure that

$$\mathrm{pr}_c : G(a,b,c)_a \underset{Z/(2)}{\times} G(a,b,c)_c \to G(a,b,c)_c$$

restricted to L is surjective, one may assume that $g_c(1)$ is of order 3 and $g_c(2)$ is of order 2. For example, here are two such generators:

$$g(1) = ((12)_a, g_a(1)', (123)_c, \bar{1}_c)$$

and

$$g(2) = ((123)_a, \bar{1}_a, (12)_c, \bar{0}_c).$$

Step 3. $\mathrm{pr}_a : L \to G(a,b,c)_a$ *is not a frattini cover*

Consider the subset $T = \{g(1)^3, g(2)\}$ of L. Clearly $\mathrm{pr}_a(T)$ generates G. However, T does not generate L: there is no element of the group generated by T whose 3rd coordinate is of order 3.

This concludes the proof of the theorem. □

A group G is said to be *frattini trivial* if G has only a trivial frattini subgroup. Among the frattini trivial groups are those which have no nontrivial nilpotent normal subgroups [H, p. 158]. The universal frattini cover of a frattini trivial group should recieve special investigatory efforts.

3. P.A.C. Fields that are not Frobenius Fields

Let F be a field, $R_1 \subset R_2$ integral domains which are finitely generated over F, and $E_1 \subsetneq E_2$ the respective quotient fields of R_1 and R_2. Assume that E_2/E_1 is finite and separable. Call R_2/R_1 a *ring cover* over F if R_1 is *integrally closed* and $R_2 = R_1[z]$ for z an element integral over R_1 whose discrimant $d(z)$ is a unit of R_1[ZS, Vol. I, p. 264]. If, in addition, E_2/E_1 is a Galois extension, then R_2/R_1 is said to be a *Galois ring cover*. The cover is *regular* if E_1 is a regular extension of F (i.e., the algebraic closure of F in E_1 is just F). One further concept is required for the definition of *frobenius field*. Let $\mathfrak{p}$ be a maximal prime ideal of R_1 for which the residue field $R_1/\mathfrak{p}$ is isomorphic to F. For $\mathfrak{P}$, a prime ideal of R_2 for which $\mathfrak{P} \cap R_1 \equiv \mathfrak{p}$ (i.e., $\mathfrak{P}$ *lies over* $\mathfrak{p}$), $D(\mathfrak{P}) \overset{\mathrm{def}}{=} \{\sigma \in G(E_2/E_1) \mid \sigma(\mathfrak{P}) \equiv \mathfrak{P}\}$ is the *decomposition group* of $\mathfrak{P}$. If $\mathfrak{P}_1$ and $\mathfrak{P}_2$ are two primes lying over $\mathfrak{p}$, then $D(\mathfrak{P}_1)$ is conjugate in $G(E_2/E_1)$ to $D(\mathfrak{P}_2)$. Thus for $\mathfrak{p}$ maximal in R_1, one associates a conjugacy class, $D(\mathfrak{p})$, of subgroups of $G(E_2/E_1)$ [ZS, Vol. II, pp. 67–82].

A field F is a frobenius field if for *each* galois regular ring cover R_2/R_1 the following holds: for M the algebraic closure of F in E_2, and H a subgroup of $G(E_2/E_1)$ for which $H \in \mathcal{G}(G(\bar{F}/F))$ (Sect. 2) and restriction of H to M is equal to $G(M/F)$, there exists a prime $\mathfrak{p}$ of R_1 for which $H \in D(\mathfrak{p})$.

There are two related results from [FJH]:

(i) F is a frobenius field if and only if F is P.A.C. and $G(\bar{F}/F)$ has the extension property (Sect. 2); and

(ii) there is an explicit (e.g., primitive recursive) elimination of quantifiers (through Galois stratifications) for any frobenius field.

Among the many consequences of these results is this: for F a frobenius field with a primitive recursive *splitting algorithm* and a primitive recursive theory for deciding a statement from the collection $\{P(\mathbf{H}, \mathbf{G}; F)\}$ (as in the introduction) there is a primitive recursive elimination of quantifiers for the elementary theory of F.

More generally, let $\mathscr{L} = \{F_\alpha\}_{\alpha \in I}$ be a collection of frobenius fields containing a given field K, finitely generated over its prime field. Then there is a primitive recursive theory for deciding the statements of K that are true in *each* of the fields F_α, $\alpha \in I$, if there is a primitive recursive theory for deciding statements from the following collection: for each $\mathbf{H}$, $\mathbf{G}$, there exists $\alpha \in I$ such that $P(\mathbf{H}, \mathbf{G}; \mathbf{F}_\alpha)$ is true.

These results make very precise the distinctions between general P.A.C. fields and the important subset of frobenius fields. Therefore, it is significant that *the example of Sect. 2 allows one to produce* a P.A.C. *field which is not a frobenius field* [FJH].

References

[A] Ax, J.: Solving diophantine problems modulo every prime. Ann. Math. **85**, 161–183 (1967)

[DL] Dries, L. van den, Lubotzky, L.: Normal subgroups of free profinite groups (preprint)

[FJH] Fried, M., Jarden, M., Haran, D.: Galois stratifications over frobenius fields (preprint)

[FS] Fried, M., Sacerdote, G.: Solving diophantine problems over all residue class fields of a number field and all finite fields. Ann. Math. **104**, 203–233 (1976)

[H] Hall, M., Jr.: The theory of groups. New York: McMillan 1963

[N] Northcott, D.G.: An introduction to homological algebra. Cambridge: Cambridge University Press 1962

[WAE] Waerden, B.L. van der: Modern algebra. New York: Unger 1950

[ZS] Zariski, O., Samuel, P.: Commutative algebra. Vols. I, II. Princeton: Van Nostrand 1960

Received July 18, 1980