ON THE COHOMOLOGICAL DIMENSION OF ARTIN-SCHREIER STRUCTURES

Dan Haran *

School of Mathematical Sciences

Raymond and Beverly Sackler

Faculty of Exact Sciences

Tel Aviv University

Tel Aviv, Israel

* Research partially supported by the Alexander-von-Humboldt Foundation.

Introduction

Let G be a pro-p-group and let G' be an open subgroup of G. Assume that G' is a free pro-p-group. If G is torsion free, then a celebrated theorem of Serre ([S], Corollaire 2) states that G itself is a free pro-p-group. This is especially useful in Galois theory, when G is the absolute Galois group $G(K)$ of a field K and $G' = G(L)$, where L is a finite extension of K. Indeed, if $p \neq 2$ then G is torsion free. However, if $p = 2$ then G may contain elements of order 2 (called *involutions*; henceforth $\mathrm{Inv}(G)$ will denote the set of involutions of G). Ershov ([E], Theorem 4) has shown, using a field theoretical characterization of such groups by quadratic forms due to R. Ware ([W], Corollary 3.3), that in this case G is what we call a *real free* pro-2-group, i.e., the free pro-2-product of copies of $\mathbb{Z}/2\mathbb{Z}$ with a free pro-2-group.

The purpose of this work is to generalize this result to arbitrary profinite (not necessarily absolute Galois) groups. To avoid new definitions at this stage, we mention here only the most significant case of pro-2-groups; the complete results and some applications are listed in section 2.

THEOREM A: *A pro-2-group G is a real free pro-2-group if and only if either G itself is a free pro-2-group or G contains an open free pro-2-subgroup G' of index 2 and the centralizer of every involution ε in G is $\{1, \varepsilon\}$.*

If G is the absolute Galois group $G(K)$ of a field K then Artin-Schreier theory guarantees the centralizer condition of Theorem A. Furthermore, if an open subgroup of $G(K)$ is a free pro-2-group then so is its intersection with the torsion free group $G' = G(K(\sqrt{-1}))$, and hence also G' is free, by the above mentioned Serre's theorem. Thus the above mentioned result of Ershov follows as a special case of Theorem A.

The proof of Theorem A is an analogue of our proof of Serre's theorem [H3] in the cohomology of groups and it requires several ingredients:

(i) Artin-Schreier structures (Definition 1.3) instead of profinite groups. The reader should consult [HJ1] for the basic properties of Artin-Schreier structures. The main reason for their use is that the real projectivity of a groups translates to the projectivity of a corresponding Artin-Schreier structure, which can be easier dealt with.

(ii) The cohomology theory of Artin-Schreier structures, developed in [H2]. We shall give its essentials below for the convenience of the reader.

(iii) Projective resolutions of profinite G-modules (see Section 1), as given in [H3].

Use of this machinery yields the following result in the theory of Artin-Schreier structures:

THEOREM B: *Let* $\mathbf{G} = \langle G, G', X \rangle$ *be an Artin-Schreier structure. If* $X = \mathrm{Inv}(G)$ *then* $\mathrm{cd}_p\mathbf{G} = \mathrm{cd}_p G'$ *for every prime* p*.*

In particular we have:

COROLLARY: *An Artin-Schreier structure* $\mathbf{G} = \langle G, G', X \rangle$ *is projective if and only if* G' *is a projective profinite group and* $X = \mathrm{Inv}(G)$*.*

This yields a new characterization (Proposition 2.2) of real projective groups, from which also Theorem A will be derived.

1. Cohomology of Artin-Schreier structures

We shall be concerned with structures of the form

$$\mathbf{G} = \langle G, G', X \rangle, \tag{1}$$

where G is a profinite group with a continuous left action on the Boolean space X (possibly empty) and G' is an open subgroup of G of index 1 or 2. Associate with $\mathbf{G}$ the disjoint union $\widetilde{X} = \{x^+ \mid x \in X\} \mathbin{\dot\cup} \{x^- \mid x \in X\}$ of two homeomorphic copies of X. Let G act on $\widetilde{X}$ by

$$gx^+ = \begin{cases} (gx)^+ & \text{if } g \in G' \\ (gx)^- & \text{if } g \in G \smallsetminus G' \end{cases} \qquad gx^- = \begin{cases} (gx)^- & \text{if } g \in G' \\ (gx)^+ & \text{if } g \in G \smallsetminus G' \end{cases}.$$

As G also acts on itself by multiplication from the left, we get a continuous action of G on the disjoint union $G \mathbin{\dot\cup} \widetilde{X}$.

Let p be a prime and put $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$. In the Galois cohomology one usually works with *discrete* G-modules (cf. [R], Definition II.1.1). We, however, shall be more interested in the category $\mathcal{C}_p(G)$ of inverse limits of finite (discrete) $\mathbb{F}_p[G]$-modules. One might call these objects profinite G-modules annihilated by p, or *profinite* $\mathbb{F}_p[\![G]\!]$-*modules.* More details on this category can be found in [H3], especially information about free and projective objects in $\mathcal{C}_p(G)$; nevertheless, a reader with some experience in the theory of profinite groups will have no difficulties in understanding the operations in $\mathcal{C}_p(G)$ used in this paper.

Definition 1.1: Assign to $\mathbf{G}$ the profinite $\mathbb{F}_p[\![G]\!]$-module $M_p(\mathbf{G}) = (\mathbb{F}_p \oplus \mathbb{F}_p\widetilde{X})/B_0$, where $\mathbb{F}_p\widetilde{X}$ is the free $\mathbb{F}_p$-module on $\widetilde{X}$ and B_0 is the closed G-submodule of $\mathbb{F}_p \oplus \mathbb{F}_p\widetilde{X}$ generated by $x^+ + x^- - 1$, for all $x \in X$.

To elucidate the definition, assume first that $\mathbf{G}$ is *finite*, i.e., G, G' and X are finite. The $\mathbb{F}_p$-vector spaces $\mathbb{F}_p$ and $\mathbb{F}_p\widetilde{X} = \bigoplus_{\tilde{x}\in\widetilde{X}} \mathbb{F}_p\tilde{x}$ are $\mathbb{F}_p[G]$-modules: the former with the trivial G-action and the latter via the action of G on $\widetilde{X}$. Then the definition reads

$$M_p(\mathbf{G}) = (\mathbb{F}_p \oplus \mathbb{F}_p\widetilde{X})/\sum_{x\in X} \mathbb{F}_p(x^+ + x^- - 1). \tag{2}$$

If $\mathbf{G}$ is not finite, then it is the inverse limit of finite structures $\mathbf{G}_i = \langle G_i, G'_i, X_i\rangle$, that is, $G = \varprojlim G_i$, $G' = \varprojlim G'_i$, $X = \varprojlim X_i$ and the G-action on X is induced from the G_i-actions on X_i (cf. [HJ1], Proposition 1.5). In this case $M_p(\mathbf{G}) = \varprojlim M_p(\mathbf{G}_i)$.

By abuse of notation, the elements of $\mathbb{F}_p \oplus \mathbb{F}_p\widetilde{X}$ will denote their images in $M_p(\mathbf{G})$ as well.

Remark 1.2: Let $\mathbf{G}$ be finite. Suppose that X is the disjoint union of three subsets X_+, X_- and X_0, and let $x_0 \in X_0$. Then by (2) the following set

$$\{x^+ \mid x \in X_+\} \cup \{x^- \mid x \in X_-\} \cup \{x^+ \mid x_0 \neq x \in X_0\} \cup \{x_0^+\} \cup \{1\}$$

is a linear basis of $M_p(\mathbf{G})$ over $\mathbb{F}_p$. It will remain a basis after subtracting its element x_0^+ from some other elements. Thus also

$$\{x^+ \mid x \in X_+\} \cup \{x^- \mid x \in X_-\} \cup \{(x^+ - x_0^+) \mid x_0 \neq x \in X_0\} \cup \{x_0^+, x_0^-\}$$

is a linear basis of $M_p(\mathbf{G})$ over $\mathbb{F}_p$.

DEFINITION 1.3 (see [HJ1], section 3; also cf. [H2], section 1): The structure $\mathbf{G}$ is an *Artin-Schreier structure* if

(i) the stabilizer $G_x = \{\sigma \in G \mid \sigma x = x\}$ is of order 2 and $G_x \cap G' = 1$, for every $x \in X$; and

(ii) the *forgetful* map $d : X \to G$, where $d(x)$ is the generator of G_x, is continuous.

It follows from (i) and (ii) that

(iii) $d(\sigma x) = \sigma d(x) \sigma^{-1}$ for all $\sigma \in G$, $x \in X$, and $d(X) \cap G' = \emptyset$ (thus $X = \emptyset$ if $G' = G$).

Our aim is to define the cohomology functor of Artin-Schreier structures and to identify it with a certain Ext-functor. The presentation is not the same as in [H2], section 2, nevertheless it leads to the same definition in our context. Again, assume first that $\mathbf{G}$ is finite. Consider the following sequence of $\mathbb{F}_p[G]$-modules

$$F_* : \qquad \cdots \to F_n \xrightarrow[\partial_n]{} F_{n-1} \xrightarrow[\partial_{n-1}]{} \cdots \xrightarrow[\partial_2]{} F_1 \xrightarrow[\partial_1]{} F_0,$$

where

$F_0 = \mathbb{F}_p[G] \oplus \mathbb{F}_p \widetilde{X}$,

F_n, for $n \geq 1$, is the free $\mathbb{F}_p[G]$–module $\displaystyle\bigoplus_{\substack{g_1,\dots,g_{n-1}\in G\\ g_n \in G \cup X}} \mathbb{F}_p[G](g_1,\dots,g_n)$,

$$\partial_1\big((g_1)\big) = \begin{cases} g_1 - 1 & \text{if } g_1 \in G \\ x^+ + x^- - 1 & \text{if } g_1 = x \in X, \end{cases}$$

$$\partial_n(g_1,\dots,g_n) = g_1(g_2,\dots,g_n) + \\ + \sum_{i=1}^{n-1}(-1)^i(g_1,\dots,g_{i-1},g_ig_{i+1},g_{i+2},\dots,g_n) + (-1)^n(g_1,\dots,g_{n-1}),$$

for $n \geq 2$.

Observe that F_0 is also a free $\mathbb{F}_p[G]$-module: by 1.3(i), $g\tilde{x} = \tilde{x} \Leftrightarrow g = 1$, for every $\tilde{x} \in \widetilde{X}$. (Cf. also Lemma 3.1 (a).)

It is quite standard to check that F_* is a complex. To show that it is exact, notice that

$$\{g_0(g_1,\dots,g_n) \mid g_0,\dots,g_{n-1} \in G,\ g_n \in G \cup X\}$$

is a basis of F_n, for $n \geq 1$, as a vector space over $\mathbb{F}_p$ (do not confuse between $g_0(g_1)$ and $(g_0 g_1)$ in F_1), and $G \dot\cup \widetilde{X}$ is a basis of F_0. This enables us to define $\mathbb{F}_p$-linear maps $h_n : F_n \to F_{n+1}$ by

$$\begin{aligned}
&h_n\big(g_0(g_1,\ldots,g_n)\big) = (g_0, g_1, \ldots, g_n), \text{ for } n \geq 1,\\
&h_0(g_0) = (g_0), \text{ if } g_0 \in G,\\
&h_0(x^+) = (x), \quad \text{and} \quad h_0(x^-) = 0, \text{ if } x \in X.
\end{aligned}$$

These maps constitute a contracting homotopy of F_*, that is, they satisfy $\partial_{n+1} \circ h_n + h_{n-1} \circ \partial_n = \mathrm{id}$, for $n \geq 1$. Thus F_* is exact (cf. [P], Lemma 10.3.10).

Let $\overline{F}_n = F_n/D_n$, where D_n is the $\mathbb{F}_p[G]$-submodule of F_n generated by the elements $(g_1, \ldots, g_n)$ such that $g_i = 1$ for some i (and $D_0 = 0$). Clearly $\overline{F}_n$ is free for every $n \geq 0$. Since $\partial_n(D_n) \subseteq D_{n-1}$ for every $n \geq 1$, we obtain the quotient complex

$$\overline{F}_* : \qquad \cdots \to \overline{F}_n \xrightarrow[\bar\partial_n]{} \overline{F}_{n-1} \xrightarrow[\bar\partial_{n-1}]{} \cdots \xrightarrow[\bar\partial_2]{} \overline{F}_1 \xrightarrow[\bar\partial_1]{} \overline{F}_0.$$

The homotopy h_* defined above carries D_* into itself and hence induces a contracting homotopy of $\overline{F}_*$. Thus $\overline{F}_*$ is also an exact sequence of free $\mathbb{F}_p[G]$-modules.

If $\mathbf{G}$ is not finite, then it is the inverse limit of finite Artin-Schreier structures (cf. [HJ1], Lemma 4.4). The corresponding inverse limits of the sequences F_* and $\overline{F}_*$ are exact sequences (since $\varprojlim$ is an exact functor), in the category $\mathcal{C}_p(G)$.

Let A be a finite object in $\mathcal{C}_p(G)$, that is, a finite $\mathbb{F}_p[G]$-module. Then $\overline{F}_*$ induces the complex

$$\begin{aligned}
\mathrm{Hom}_G(\overline{F}_*, A) : \qquad &\cdots \leftarrow \mathrm{Hom}_G(\overline{F}_n, A) \xleftarrow[\delta_n]{} \mathrm{Hom}_G(\overline{F}_{n-1}, A) \xleftarrow[\delta_{n-1}]{} \cdots\\
&\cdots \xleftarrow[\delta_2]{} \mathrm{Hom}_G(\overline{F}_1, A) \xleftarrow[\delta_1]{} \mathrm{Hom}_G(\overline{F}_0, A)) \leftarrow 0
\end{aligned}$$

where $\mathrm{Hom}_G(F, A)$ denotes the group of $\mathcal{C}_p(G)$-morphisms from F to A, and $\delta_n(\varphi) = \varphi \circ \partial_n$ for every $\varphi \in \mathrm{Hom}_G(\overline{F}_n, A)$. One easily sees that:

(i) For $n \geq 1$, $\mathrm{Hom}_G(\overline{F}_n, A)$ can be identified with $C^n(\mathbf{G}, A)$, the set of continuous functions $f : G^{n-1} \times (G \dot\cup X) \to A$ satisfying $f(g_1, \ldots, g_{i-1}, 1, g_{i+1}, \ldots, g_n) = 0$ for every $1 \leq i \leq n$.

(ii) $\mathrm{Hom}_G(\overline{F}_0, A)$ can be identified with the set of continuous functions $f' : G\cup\widetilde{X} \to A$ such that $f'(gz) = gf'(z)$ for every $g \in G$ and every $z \in G\cup\widetilde{X}$. The latter set may be identified with $C^0(\mathbf{G}, A) = A \oplus C_X(\mathbf{G}, A)$, where $C_X(\mathbf{G}, A)$ is the set of continuous functions $f : X \to A$ satisfying $f(gx) = gf(x)$ for every $g \in G'$ and every $x \in X$. (The element $a + f \in C^0(\mathbf{G}, A)$ that corresponds to f' is given by $a = f'(1)$ and $f(x) = f'(x^+)$.) (cf. [H2], section 2).

(iii) Under the above identifications $\delta_n : C^{n-1}(\mathbf{G}, A) \to C^n(\mathbf{G}, A)$ is given by

$$\begin{aligned} \big(\delta_1(a,f)\big)(g_1) &= g_1 a - a && \text{for every } g_1 \in G,\\ \big(\delta_1(a,f)\big)(x) &= f(x) + d(x)f(x) - a && \text{for every } x \in X, \end{aligned}$$

and for $n \geq 2$ by

$$\begin{aligned} (\delta_n f)(g_1, \dots, g_n) = {}& g_1 f(g_2, \dots, g_n) + \\ & + \sum_{i=1}^{n-1} (-1)^i f(g_1, \dots, g_{i-1}, g_i g_{i+1}, g_{i+2}, \dots, g_n) + (-1)^n f(g_1, \dots, g_{n-1}). \end{aligned}$$

We define the *cohomology group* $H^n(\mathbf{G}, A)$ as the n-th homology group of the above complex $C^*(\mathbf{G}, A)$.

REMARK 1.4: In [H2], section 2 we have defined $H^n(\mathbf{G}, A)$ for all *discrete* G-modules A. If A is a finite $\mathbb{F}_p[G]$-module, that definition coincides with the above definition.

Let M be a profinite $\mathbb{F}_p[\![G]\!]$-module and let A be a finite $\mathbb{F}_p[G]$-module. In [H3], section 3 we have defined $\mathrm{Ext}^n_G(M, A)$ to be the n-th homology group of the complex $\mathrm{Hom}_G(P_*, A)$, where P_* is any projective resolution of M in the category $\mathcal{C}_p(G)$.

LEMMA 1.5: *$H^n(\mathbf{G}, A) = \mathrm{Ext}^n_G(M_p(\mathbf{G}), A)$ for all $n \geq 0$. In fact,*

(a) *$M_p(\mathbf{G})$ is the cokernel of the map $\partial_1 : F_1 \to F_0$ in F_*;*

(b) *$M_p(\mathbf{G})$ is the cokernel of $\bar{\partial}_1 : \overline{F}_1 \to \overline{F}_0$ in $\overline{F}_*$;*

(c) *$\overline{F}_n$ is projective, for every $n \geq 0$.*

Proof: If (b) and (c) hold then $\overline{F}_*$ is a projective resolution of $M_p(\mathbf{G})$, and hence the first assertion follows.

(a) If $\mathbf{G}$ is finite, this is clear; the general case follows by a standard limit argument.

(b) As $F_0 = \overline{F}_0$ and $\bar{\partial}_1(\overline{F}_1) = \partial_1(F_1)$, the cokernels of ∂_1 and $\bar{\partial}_1$ are equal.

(c) We have $\mathbf{G} = \varprojlim \mathbf{G}_i$, where $\mathbf{G}_i = \langle G_i, G'_i, X_i \rangle$ are finite Artin-Schreier structures. By the definition, $\overline{F}_n = \varprojlim \overline{F}_{n,i}$, where $\overline{F}_{n,i}$ is a free, and hence a projective $\mathbb{F}_p[G_i]$-module. Thus the assertion follows from the following technical lemma. ∎

LEMMA 1.6: *Let P be a profinite $\mathbb{F}_p[\![G]\!]$-module. Assume that $G = \varprojlim G_i$ and $P = \varprojlim P_i$, where G_i is a finite group and P_i is a projective $\mathbb{F}_p[G_i]$-module, for every i. Then P is a projective profinite $\mathbb{F}_p[\![G]\!]$-module.*

Proof: By [H3], Lemma 3.2 we have to show that for every epimorphism of finite $\mathbb{F}_p[G]$-modules $\alpha : B \to A$ and every morphism $\varphi : P \to A$ there exists a morphism $\psi : P \to B$ such that $\alpha \circ \psi = \varphi$. For i sufficiently large, A and B are $\mathbb{F}_p[G_i]$-modules and the map $\varphi : P \to A$ factors through P_i (since A is finite), say into $\varphi' : P \to P_i$ and $\varphi_i : P_i \to A$. As P_i is a projective $\mathbb{F}_p[G_i]$-module, there is an $\mathbb{F}_p[G_i]$-morphism $\psi_i : P_i \to B$ such that $\alpha \circ \psi_i = \varphi_i$. Thus $\alpha \circ (\psi_i \circ \varphi') = \varphi$. ∎

Recall ([H2], Definition 6.1 and [H2], Proposition 6.2) that $\mathrm{cd}_p(\mathbf{G})$ is the smallest nonnegative integer n such that $H^{n+1}(\mathbf{G}, A) = 0$ for all finite $\mathbb{F}_p[G]$-modules (and if no such n exists then $\mathrm{cd}_p(\mathbf{G}) = \infty$).

Using this criterion we obtain:

PROPOSITION 1.7: $\mathrm{cd}_p(\mathbf{G}) < \infty$ *if and only if $M_p(\mathbf{G})$ has a projective resolution in $\mathcal{C}_p(G)$ of finite length.*

Proof: By the definition, $\mathrm{cd}_p(\mathbf{G}) < \infty$ if and only if there is n such that $H^n(\mathbf{G}, A) = 0$ for all finite $\mathbb{F}_p[G]$-modules A, i.e. (by Lemma 1.5), $\mathrm{Ext}^n_G(M_p(\mathbf{G}), A) = 0$ for all finite $\mathbb{F}_p[G]$-modules A. By [H3], Proposition 3.6 this is equivalent to the required condition.
∎

We remark that Proposition 1.7 is an analogue of

PROPOSITION 1.7' ([H3], Corollary 3.7): *Let G be a profinite group. Then $\mathrm{cd}_p G < \infty$ if and only if $\mathbb{F}_p$ has a projective resolution in $\mathcal{C}_p(G)$ of finite length.*

2. Main results.

In the preceding section we have explained all the notions that appear in the statement of Theorem B. We postpone the proof of Theorem B to section 4; our present aim is to draw some consequences from it, especially Theorem A mentioned in the introduction.

Notice, however, that for a prime $p \neq 2$ the assertion of Theorem B is not new. Indeed, $\mathrm{cd}_p\mathbf{G} = \mathrm{cd}_p G$ by [H2], Corollary 6.5. If G contains no elements of order p then by Serre's theorem $\mathrm{cd}_p G = \mathrm{cd}_p G'$; if G contains elements of order p then so does G', since $(G : G') \leq 2$, whence $\mathrm{cd}_p G = \infty = \mathrm{cd}_p G'$.

Also notice that the condition $X = \mathrm{Inv}(G)$ in Theorem B is essential: if the forgetful map $d : X \to \mathrm{Inv}(G)$ is not a bijection then $\mathrm{cd}_2\mathbf{G} = \infty$ (see [H2], Corollary 6.7).

Recall the definition of a projective Artin-Schreier structure. A morphism of Artin-Schreier structures

$$\alpha : \mathbf{B} = \langle B, B', Y \rangle \to \mathbf{A} = \langle A, A', Z \rangle$$

is a *cover* if $A = B/K$, $A' = B'/K$ and $Z = Y/K$, where K is a normal subgroup of B contained in B', and α is the quotient map ([HJ1], Definition 3.3 and 4.1). An Artin-Schreier structure $\mathbf{G}$ is *projective* if for every cover of Artin-Schreier structures $\alpha : \mathbf{B} \to \mathbf{A}$ and every morphism $\varphi : \mathbf{G} \to \mathbf{A}$ there exists a morphism $\psi : \mathbf{G} \to \mathbf{A}$ such that $\alpha \circ \psi = \varphi$ ([HJ1], Definition 7.1). We have shown ([H2], Corollary 3.4 and Proposition 6.2) that an Artin-Schreier structure $\mathbf{G}$ is projective if and only if $\mathrm{cd}_p\mathbf{G} \leq 1$ for every prime p. On the other hand, a profinite group G' is projective if and only if $\mathrm{cd}_p G' \leq 1$ for every prime p (cf. [G], Theorem 4). Thus Theorem B yields:

THEOREM 2.1: *An Artin-Schreier structure $\mathbf{G} = \langle G, G', X \rangle$ is projective if and only if G' is a projective profinite group and $X = \mathrm{Inv}(G)$.*

Recall ([HJ1], section 7) that a profinite group G is *real projective* if $\mathrm{Inv}(G)$ is closed in G and for every epimorphism of finite groups $\alpha : B \to A$ and every continuous homomorphism $\varphi : G \to A$ that satisfies $\varphi\big(\mathrm{Inv}(G)\big) \subseteq \alpha\big(\mathrm{Inv}(B)\big)$ there exists a continuous homomorphism $\psi : G \to B$ such that $\alpha \circ \psi = \varphi$. Equivalently ([HJ2], Theorem

3.6), G is a closed subgroup of a free profinite product of a free profinite group with copies of $\mathbb{Z}/2\mathbb{Z}$.

PROPOSITION 2.2: *A profinite group G is real projective if and only if either G is projective or G contains an open projective subgroup of index 2 and*

$$(1) \qquad \{\sigma \in G \mid \sigma\varepsilon\sigma^{-1} = \varepsilon\} = \langle\varepsilon\rangle \quad \text{for every } \varepsilon \in \mathrm{Inv}(G).$$

Proof: [HJ1], Proposition 7.7 states that G is real projective if and only if there is an open subgroup G' of G of index ≤ 2 such that the structure

$$\mathbf{G} = \langle G, G', \mathrm{Inv}(G)\rangle$$

is a projective Artin-Schreier structure. Let $G' \leq G$ be of index ≤ 2. Then $\mathbf{G}$ is an Artin-Schreier structure if and only if $G' \cap \mathrm{Inv}(G) = \emptyset$ and (1) holds. By Theorem 2.1, $\mathbf{G}$ is projective if and only if G' is projective. Finally notice that a projective group is torsion free, in particular contains no involutions. ∎

Theorem A of the Introduction is a corollary of Proposition 2.2. Indeed, a pro-2-group is projective if and only if it is free (see [R], Theorem IV.6.5), and on the other hand it is real projective if and only if it is real free (see [H1], Proposition 4.2).

COROLLARY 2.3: *Let a group $\{1,\delta\}$ of order 2 act on a free pro-2-group F. Then the corresponding semidirect product $G = F \rtimes \{1,\delta\}$ is a real free pro-2-group if and only if*

$$(2) \qquad \tau^\delta = \tau^{-1},\ \sigma^\tau = \sigma^\delta \quad \Longrightarrow \quad \sigma = 1, \qquad \text{for all } \sigma,\ \tau \in F\ .$$

Proof: Notice that $\mathrm{Inv}(G) \subseteq G \smallsetminus F$, since a projective profinite group is torsion free. Therefore (1) is equivalent to

$$(1') \qquad \{\sigma \in F \mid \sigma\varepsilon\sigma^{-1} = \varepsilon\} = \langle 1\rangle \quad \text{for every } \varepsilon \in \mathrm{Inv}(G).$$

Let $\sigma, \tau \in F$. Then clearly

$$\tau\delta \in \mathrm{Inv}(G) \iff \tau^\delta = \tau^{-1}$$

and

$$\sigma(\tau\delta)\sigma^{-1} = \tau\delta \iff (\sigma^{-1})^{\tau^{-1}} = (\sigma^{-1})^{\delta}.$$

Therefore (1') is equivalent to (2). ∎

Proposition 2.2 can also be interpreted in Galois theory. Let K be a field, and let $G = G(K)$ be its absolute Galois group. The involutions of G correspond via the Galois correspondence to the real closures of K. Condition (1) is satisfied: it is equivalent to the well known statement that every real closure of K admits no non-trivial K-automorphism. Furthermore, $K(\sqrt{-1})$ has no real closures, and hence $G' = G(K(\sqrt{-1}))$ contains no involutions; this implies that the structure

$$\mathbf{G}(K) = \langle G(K),\ G(K(\sqrt{-1})),\ \mathrm{Inv}(G(K))\rangle$$

is an Artin-Schreier structure (cf. [HJ1], Section 3). We call it the *absolute Artin-Schreier structure* of K.

Proposition 2.2 yields the following result, which answers in affirmative Problem 6.4 of [H1].

PROPOSITION 2.4: *Let K be a field such that $G(K(\sqrt{-1}))$ is projective. Then $G = G(K)$ is real projective.*

This has been shown in [H1], Theorem 6.1 only for an algebraic extension K of $\mathbb{Q}$. However, if one replaces the use of [H1], Theorem 4.4 in the proof by [E], Theorem 4, the assertion of Proposition 2.4 follows as well. The author would like to thank Efrat and Ershov for pointing out this to him.

Next we obtain information about the change of cohomological dimension of Artin-Schreier structures under transcendental extensions.

THEOREM 2.5: *Let $K(t)$ be the field of rational functions over a field K. Then $\mathrm{cd}_p\mathbf{G}(K(t)) \le \mathrm{cd}_p\mathbf{G}(K) + 1$ for every prime p. Moreover, equality holds if $\mathrm{cd}_p\mathbf{G}(K) < \infty$ and $p \neq \mathrm{char}\ K$.*

Proof: Put $K' = K(\sqrt{-1})$. By Theorem B

$$\mathrm{cd}_p\mathbf{G}(K)) = \mathrm{cd}_p G(K') \qquad \text{and} \qquad \mathrm{cd}_p\mathbf{G}(K(t)) = \mathrm{cd}_p G(K'(t)).$$

Therefore the assertion of the theorem is equivalent to [R], Proposition V.5.2. ∎

COROLLARY 2.6: *If R is a real closed field then the absolute Galois group of $R(t)$ is real projective.*

Proof: Let p be a prime. By [H2], Corollary 6.8 we have $\mathrm{cd}_p\mathbf{G}(R) = 0$. Therefore $\mathrm{cd}_p\mathbf{G}(R(t)) = 1$. By [HJ1], Proposition 7.7 the group G(R(t)) is real projective. ∎

We should remark that a stronger result is true: the group G(R(t)) is real free, i.e, a free profinite product of a free profinite group with copies of $\mathbb{Z}/2\mathbb{Z}$ (see [HJ2], 4.1). However, the proof of the latter result is based via the Riemann Existence Theorem on the analytic theory of Riemann surfaces. On the other hand, the proof of Corollary 2.6 above is purely algebraic.

3. Auxiliary results

We recall some elementary facts needed later. In this section let F be a field and G an abstract group (the reader may assume that they are finite). For an element x of a left $F[G]$-module M denote

$$G_x = \{\sigma \in G \mid \sigma(x) = x\}.$$

LEMMA 3.1: *Let M be an $F[G]$-module, and let $\mathcal{A}$ be a G-invariant linear basis of M over F.*

(a) *If G acts freely on $\mathcal{A}$ (that is, $G_x = 1$ for every $x \in \mathcal{A}$) then M is a free $F[G]$-module. In fact, $M = \oplus_{x\in\mathcal{A}_0} F[G]x$, where $\mathcal{A}_0 \subseteq \mathcal{A}$ is a system of representatives of the G-orbits in $\mathcal{A}$.*

(b) *Let N be the linear subspace of M generated by $\mathcal{A}' = \{x \in \mathcal{A} \mid G_x \neq 1\}$. Then N is an $F[G]$-submodule of M, and M/N is a free $F[G]$-module.*

Proof: (a) Clear.

(b) The first assertion follows as $\mathcal{A}'$ is G-invariant. The complement $\mathcal{A}'' = \{x \in \mathcal{A} \mid G_x = 1\}$ of $\mathcal{A}'$ in $\mathcal{A}$ is mapped injectively by the quotient map $M \to M/N$ onto a linear basis of M/N. Since G acts freely on this basis, M/N is free by (a). ∎

By '$\otimes$' we denote the tensor product over F. If M_1 and M_2 are (left) $F[G]$-modules then so is $M_1 \otimes M_2$, via the "diagonal" action of G on it: $\sigma(m_1 \otimes m_2) = \sigma m_1 \otimes \sigma m_2$ (cf. [Bro], p.55).

LEMMA 3.2: *Let M_1, M_2 be two vector spaces over a field F. Let $\mathcal{A}$ be a linear basis of M_1, and for every $x \in \mathcal{A}$ let $\mathcal{B}(x)$ be a basis of M_2. Then*

(a) $\{x \otimes y \mid x \in \mathcal{A},\ y \in \mathcal{B}(x)\}$ *is a basis of* $M_1 \otimes M_2$.

(b) *Its elements satisfy:* $x \otimes y = x' \otimes y' \iff x = x'$ and $y = y'$.

Assume that M_1, M_2 are $F[G]$-modules as well, and that $\mathcal{A}$ is G-invariant. Let $\mathcal{A}_0$ be a system of representatives of the G-orbits in $\mathcal{A}$, and assume that $\mathcal{B}(x)$ is G_x-invariant for every $x \in \mathcal{A}_0$. Then

(c) $\mathcal{B} = \{\sigma(x \otimes y) \mid \sigma \in G,\ x \in \mathcal{A}_0,\ y \in \mathcal{B}(x)\}$ *is a G-invariant basis of $M_1 \otimes M_2$ over F.*

(d) *Its elements satisfy* $G_{\sigma(x\otimes y)} = \sigma(G_x \cap G_y)\sigma^{-1}$.

(e) *Let N be the $F[G]$-submodule of $M_1 \otimes M_2$ generated by*

$$\{x \otimes y \mid x \in \mathcal{A}_0,\ y \in \mathcal{B}(x),\ G_y \cap G_x \neq 1\}.$$

Then $(M_1 \otimes M_2)/N$ is a free $F[G]$-module.

Proof: (a), (b) - elementary linear algebra.

(c) Define $\mathcal{B}'(\sigma x) = \sigma\mathcal{B}(x)$, for every $\sigma \in G, x \in \mathcal{A}_0$. The definition is good, since $\mathcal{B}(x)$ is G_x-invariant. Clearly $\mathcal{B}'(x)$ is a linear basis of M_2, for every $x \in \mathcal{A}$. It is easy to see that

$$\mathcal{B} = \{x \otimes y \mid x \in \mathcal{A},\ y \in \mathcal{B}'(x)\}.$$

By (a) this is a linear basis of $M_1 \otimes M_2$.

(d) Let $x \in \mathcal{A}_0, y \in \mathcal{B}(x), \tau \in G$. Then $\tau(x \otimes y) = \tau x \otimes \tau y$, hence by (b),

$$\tau(x \otimes y) = x \otimes y \iff \tau x = x \text{ and } \tau y = y \iff \tau \in G_x \cap G_y.$$

(e) By (d), N is the linear subspace of $M_1 \otimes M_2$ generated by the elements of $\mathcal{B}$ with nontrivial stabilizers. Therefore the assertion follows from Lemma 3.1(b). ∎

4. Proof of Theorem B.

Let $\mathbf{G}$ be as in Theorem B and let p be a prime. To be able to quote results from [H2], put $\mathbf{H} = \langle G', G', \emptyset\rangle$. This is an Artin-Schreier structure, and $\mathrm{cd}_p\mathbf{H} = \mathrm{cd}_p G'$ by [H2], Corollary 6.5. By [H2], Proposition 6.3 we have $\mathrm{cd}_p\mathbf{H} = \mathrm{cd}_p\mathbf{G}$ if either $\mathrm{cd}_p\mathbf{H} = \infty$ or $\mathrm{cd}_p\mathbf{G} < \infty$. Therefore to prove Theorem B it suffices to show that if $\mathrm{cd}_p G' < \infty$ then $\mathrm{cd}_p\mathbf{G} < \infty$.

Furthermore, we may assume that $p = 2$ and $\mathrm{Inv}(G) \neq \emptyset$. Otherwise $\mathrm{cd}_p\mathbf{G} = \mathrm{cd}_p G$ by [H2], Corollary 6.5, and G is torsion free, since G' is torsion free and $(G : G') \leq 2$. Therefore the assertion of the proposition follows from Serre's Théorème in [S]. This reduces Theorem B to the following assertion:

PROPOSITION 4.1: *Let $\mathbf{G} = \langle G, G', X\rangle$ be an Artin-Schreier structure such that $X = \mathrm{Inv}(G)$ is not empty. Assume that $\mathrm{cd}_2 G' < \infty$. Then $\mathrm{cd}_2\mathbf{G} < \infty$.*

Proof: (From now on $p = 2$ and thus 'profinite $\mathbb{F}_2[\![G]\!]$-module' is an object in $\mathcal{C}_2(G)$.)

By Proposition 1.7' there exists an exact sequence of profinite $\mathbb{F}_2[\![G']\!]$-modules

$$P_* : \qquad \cdots \to P_n \xrightarrow[\partial_n]{} P_{n-1} \xrightarrow[\partial_{n-1}]{} \cdots \xrightarrow[\partial_2]{} P_1 \xrightarrow[\partial_1]{} P_0 \xrightarrow[\partial]{} \mathbb{F}_2 \to 0$$

such that P_k is a projective profinite $\mathbb{F}_2[\![G']\!]$-module for every $k \geq 0$ and $P_k = 0$ for $k \gg 0$. We shall construct from P_* a projective resolution of finite length of $M_2(\mathbf{G})$ in the category of profinite $\mathbb{F}_2[\![G]\!]$-modules; this will give the desired result, by Proposition 1.7.

We need to recall the notion of the complete tensor product and some constructions from [H3]. Let $A_1, \ldots, A_n$ be inverse limits of finite vector spaces over $\mathbb{F}_2$ (i.e., objects in $\mathcal{C}_2(1)$), say $A_j = \varprojlim_{i\in I} A_{ji}$. Their *complete tensor product* $A_1\widehat{\otimes}\cdots\widehat{\otimes}A_n \in \mathcal{C}_2(1)$ is defined as $A_1\widehat{\otimes}\cdots\widehat{\otimes}A_n = \varprojlim A_{1i}\otimes\cdots\otimes A_{ni}$, where '$\otimes$' denotes the tensor product over $\mathbb{F}_2$ (cf. [Bru], section 2 and [H3], section 4).

Choose and fix an element $\delta \in \mathrm{Inv}(G)$; as in [H3], Section 5, the representatives $1, \delta$ of G/G' define functions $h_1, h_2 \colon G \to G'$ by the equations

$$h_1(\sigma) = \sigma, \qquad h_2(\sigma) = \delta\sigma\delta, \qquad \text{for} \quad \sigma \in G',$$
$$h_1(\sigma) = \sigma\delta, \qquad h_2(\sigma) = \delta\sigma, \qquad \text{for} \quad \sigma \in G\smallsetminus G'.$$

Given a sequence $P_0, P_1, P_2, \dots$ of profinite $\mathbb{F}_2[\![G']\!]$-modules, this defines a profinite $\mathbb{F}_2[\![G]\!]$-module structure on

$$(1) \qquad Q_n = Q_n(P_0, \dots, P_n) = \bigoplus_{i+j=n} P_i \widehat{\otimes} P_j \in \mathcal{C}_2(1)$$

in the following way. If $v_i \in P_i$ and $v_j \in P_j$ (such that $i+j=n$), let

$$(2) \qquad \sigma(v_i \widehat{\otimes} v_j) = \begin{cases} h_1(\sigma)v_i \widehat{\otimes} h_2(\sigma)v_j = \sigma v_i \widehat{\otimes} (\delta\sigma\delta)v_j \in P_i \widehat{\otimes} P_j & \text{if } \sigma \in G', \\ h_1(\sigma)v_j \widehat{\otimes} h_2(\sigma)v_i = \sigma\delta v_j \widehat{\otimes} \delta\sigma v_i \quad \in P_j \widehat{\otimes} P_i & \text{if } \sigma \in G \smallsetminus G' \end{cases}$$

(see [H3], Lemma 5.1; here we omit the sign, since we are in characteristic 2).

Then the sequence

$$Q_* : \qquad \cdots \to Q_n \xrightarrow[\gamma_n]{} Q_{n-1} \xrightarrow[\gamma_{n-1}]{} \cdots \xrightarrow[\gamma_2]{} Q_1 \xrightarrow[\gamma_1]{} Q_0 \xrightarrow[\gamma]{} \mathbb{F}_2 \to 0,$$

where

$$\gamma(v_i \widehat{\otimes} v_j) = \partial(v_i)\partial(v_j),$$

$$\gamma_n(v_i \widehat{\otimes} v_j) = \partial_i(v_i) \widehat{\otimes} v_j + v_i \widehat{\otimes} \partial_j(v_j) \in P_{i-1} \widehat{\otimes} P_j \ \oplus \ P_i \widehat{\otimes} P_{j-1},$$

is exact (see [H3], Lemma 4.3). It is easy to see that $\gamma, gam_1, gam_2, \dots,$ are homomorphisms of profinite $\mathbb{F}_2[\![G]\!]$-modules. Clearly $Q_n = 0$ for $n \gg 0$, since $P_i = 0$ for $i \gg 0$.

Notice that if A and B are profinite $\mathbb{F}_2[\![G]\!]$-modules then $A \widehat{\otimes} B$ also carries a structure of a profinite $\mathbb{F}_2[\![G]\!]$-module via the diagonal G-action: $g(a \widehat{\otimes} b) = ga \widehat{\otimes} gb$. Thus tensoring Q_* with the profinite $\mathbb{F}_2[\![G]\!]$-module $M_2(\mathbf{G})$ we get the following sequence of profinite $\mathbb{F}_2[\![G]\!]$-modules

$$\cdots \to Q_n \widehat{\otimes} M_2(\mathbf{G}) \to Q_{n-1} \widehat{\otimes} M_2(\mathbf{G}) \to \cdots$$
$$\cdots \to Q_0 \widehat{\otimes} M_2(\mathbf{G}) \to \mathbb{F}_2 \widehat{\otimes} M_2(\mathbf{G}) = M_2(\mathbf{G}) \to 0,$$

which is of finite length. This sequence is exact by [H3], Lemma 4.3, since it is the tensor product of Q_* with the exact sequence $0 \to M_2(\mathbf{G}) \to M_2(\mathbf{G}) \to 0$.

We have therefore reduced Proposition 4.1 to the following:

PROPOSITION 4.2: *Let* $\mathbf{G} = \langle G, G', X\rangle$ *be an Artin-Schreier structure and let* $P_0, P_1, \dots, P_n$ *be profinite* $\mathbb{F}_2[\![G']\!]$*-modules. If*

$$(*) \qquad X = \mathrm{Inv}(G)$$

and $\mathrm{Inv}(G) \neq \emptyset$ *then* $Q_n(P_0, \dots, P_n) \widehat{\otimes} M_2(\mathbf{G})$ *is a projective profinite* $\mathbb{F}_2[\![G]\!]$*-module.*

Proof of Proposition 4.2: We may assume that $P_0, P_0, \dots, P_n$ are free profinite $\mathbb{F}_2[\![G']\!]$-modules. Indeed, each P_j is a direct summand of a free profinite $\mathbb{F}_2[\![G']\!]$-module F_j ([H3], Lemma 3.3(c)). Now $Q_n(P_0, \dots, P_n)$ is a direct summand of $Q_n(F_0, \dots, F_n)$ ([H3], Lemma 5.3), and hence by the defining universal property of the complete tensor product $Q_n(P_0, \dots, P_n) \widehat{\otimes} M_2(\mathbf{G})$ is a direct summand of $Q_n(F_0, \dots, F_n) \widehat{\otimes} M_2(\mathbf{G})$. Therefore ([H3], Lemma 3.3(c)) the projectivity of $Q_n(F_0, \dots, F_n) \widehat{\otimes} M_2(\mathbf{G})$ implies the projectivity of $Q_n(P_0, \dots, P_n) \widehat{\otimes} M_2(\mathbf{G})$.

Let therefore P_j be $F_{G'}(S_j)$, the free profinite $\mathbb{F}_2[\![G']\!]$-module on a Boolean space S_j, for $0 \le j \le n$ (see [H3], Definition 2.1). Then we may assume that $S_0, \dots, S_n$ are finite. Indeed, writing S_j as $\varprojlim_{i \in I} S_{ji}$, where S_{ji} is a finite space, we get $P_j = \varprojlim_i F_{G'}(S_{ji})$, and from this clearly

$$Q_n = Q_n(P_0, \dots, P_n) = \varprojlim_{i \in I} Q_n\big(F_{G'}(S_{0i}), \dots, F_{G'}(S_{ni})\big).$$

Hence

$$Q_n \widehat{\otimes} M_2(\mathbf{G}) = \varprojlim_{i \in I} Q_n\big(F_{G'}(S_{0i}), \dots, F_{G'}(S_{ni})\big) \widehat{\otimes} M_2(\mathbf{G}).$$

Thus $Q_n \widehat{\otimes} M_2(\mathbf{G})$ is projective by [H3], Lemma 3.3(d).

The next step should be a reduction to a finite Artin-Schreier structure. However, although $\mathbf{G}$ is an inverse limit of finite Artin-Schreier structures, the latter need not satisfy $(*)$. To circumvent this crucial obstacle we use below two tricks. First, we generalize the so-far reduced problem from Artin-Schreier structures to arbitrary (i.e., not necessarily Artin-Schreier) structures, that have been introduced in section 1 precisely for this purpose. Secondly, we replace $Q_n \widehat{\otimes} M_2(\mathbf{G})$ by a certain quotient profinite $\mathbb{F}_2[\![G]\!]$-module, which turns out to be $Q_n \widehat{\otimes} M_2(\mathbf{G})$ itself if $\mathbf{G}$ is an Artin-Schreier structure.

From now on let $\mathbf{G} = \langle G, G', X\rangle$ be a structure with a continuous bijection $d : X \to \mathrm{Inv}(G)$ satisfying

$$d(\sigma x) = \sigma d(x)\sigma^{-1} \qquad \text{for every } \sigma \in G,\ x \in X. \tag{3}$$

(Thus X can be identified with $\mathrm{Inv}(G)$ via d, whence $\mathbf{G}$ is simply $\mathbf{G} = \langle G, G', \mathrm{Inv}(G)\rangle$, where G acts on $\mathrm{Inv}(G)$ via conjugation. We have not put it this way merely to avoid ambiguity in notation: if $g \in G,\ x \in X = \mathrm{Inv}(G)$, then gx could be either the product of g and x in G or the result of acting with g on x in X, that is, $gxg^{-1} \in G$.)

Let $S_0, \dots, S_n$ be finite disjoint sets, and for every $0 \le j \le n$ let P_j be the free profinite $\mathbb{F}_2[\![G']\!]$-module on S_j. Assume that there is an involution $\delta \in G \smallsetminus G'$, fix it, and define $Q_n = Q_n(P_0, \dots, P_n)$ as above (with respect to δ).

For every $\varepsilon \in \mathrm{Inv}(G)$ let $X(\varepsilon) = \{x \in X \mid \varepsilon x = x\}$, and denote by x_ε the unique element of X such that $d(x_\varepsilon) = \varepsilon$. Then $x_\varepsilon \in X(\varepsilon)$ by (3). Furthermore, the group $\langle\varepsilon\rangle$ acts regularly on $X \smallsetminus X(\varepsilon)$, hence it is possible to choose subsets $X_+(\varepsilon)$ and $X_-(\varepsilon)$ of X such that $\varepsilon X_+(\varepsilon) = X_-(\varepsilon)$ and X is the disjoint union of $X(\varepsilon), X_+(\varepsilon), X_-(\varepsilon)$.

Let

$$\mathcal{B} = \left\{ s_i \widehat{\otimes} \delta\varepsilon s_j \widehat{\otimes} (x^+ - x_\varepsilon^+) \in Q_n \widehat{\otimes} M_2(\mathbf{G}) \,\middle|\, \begin{array}{c} s_i \in S_i, s_j \in S_j, \varepsilon \in \mathrm{Inv}(G), x_\varepsilon \ne x \in X(\varepsilon) \\ \text{such that } i + j = n \text{ and } s_i = s_j \end{array} \right\} \tag{4}$$

(Thus $\mathcal{B} = \emptyset$ if n is odd.) Let $N(\mathbf{G})$ be the closed G-submodule of $Q_n \widehat{\otimes} M_2(\mathbf{G})$ generated by $\mathcal{B}$. If $\mathbf{G}$ is an Artin-Schreier structure then $\mathcal{B} = \emptyset$, and hence $N(\mathbf{G}) = 0$. This reduces Proposition 4.2 to the first assertion of the following lemma:

LEMMA 4.3: *$R(\mathbf{G}) = \big(Q_n \widehat{\otimes} M_2(\mathbf{G})\big)/N(\mathbf{G})$ is a projective profinite $\mathbb{F}_2[\![G]\!]$-module. Moreover, if $\mathbf{G}$ is a finite structure then $R(\mathbf{G})$ is a free $\mathbb{F}_2[G]$-module.*

Proof of Lemma 4.3: - divides into two parts.

PART I: *Reduction to a finite structure.* Let $\{K_i\}$ be the directed set of open normal subgroups of G contained in G'. Put $G_i = G/K_i$, $G'_i = G'/K_i$ and $X_i = \mathrm{Inv}(G_i)$. Then $\mathbf{G}_i = \langle G_i, G'_i, X_i\rangle$ is a finite structure, for every i, and $\mathbf{G} = \varprojlim_i \mathbf{G}_i$. It follows that

$$M_2(\mathbf{G}) = \varprojlim_i M_2(\mathbf{G}_i) \quad \text{and} \quad P_j = F_{G'}(S_j) = \varprojlim_i F_{G'_i}(S_j), \text{ for every } 0 \le j = 0 \le n.$$

Futhermore let δ_i be the image of δ in G_i. Taking only sufficiently big i we may assume that $\delta_i \in G_i \smallsetminus G'_i$. Define $Q_n\bigl(F_{G'_i}(S_0), \dots, F_{G'_i}(S_n)\bigr)$ using δ_i. It follows that

$$\begin{aligned}
&Q_n = \varprojlim_i Q_n\bigl(F_{G'_i}(S_0), \dots, F_{G'_i}(S_n)\bigr),\\
&Q_n \widehat{\otimes} M_2(\mathbf{G}) = \varprojlim_i Q_n(F_{G'_i}(S_0), \dots, F_{G'_i}(S_n)) \widehat{\otimes} M_2(\mathbf{G}_i),\\
&N(\mathbf{G}) = \varprojlim_i N(\mathbf{G}_i), \qquad \text{and hence} \qquad R(\mathbf{G}) = \varprojlim_i R(\mathbf{G}_i).
\end{aligned}$$

Therefore by Lemma 1.6 it suffices to show that $R(\mathbf{G}_i)$ is projective for every i.

Part II: *A linear basis of* $Q_n \otimes M_2(\mathbf{G})$. We may assume that $\mathbf{G}$ is a finite structure. In this case, of course, $P_j = \bigoplus_{s \in S_j} \mathbb{F}_2[G']s$, the complete tensor product '$\widehat{\otimes}$' is just '$\otimes$', the tensor product over $\mathbb{F}_2$, and finite (free) profinite $\mathbb{F}_2[\![G]\!]$-modules are precisely finite (free) $\mathbb{F}_2[G]$-modules. Since free profinite $\mathbb{F}_2[\![G]\!]$-modules are projective (cf. [H3, Lemma 3.3]), it suffices to prove the second assertion of the lemma.

As $\{hs \mid h \in G',\ s \in S_i\}$ is a basis of P_i, by Lemma 3.2(a) the following set is a basis of Q_n:

$$\mathcal{A} = \{h_1 s_i \otimes h_2 s_j \mid h_1, h_2 \in G',\ s_i \in S_i,\ s_j \in S_j,\ i+j=n\}.$$

Its elements satisfy, by Lemma 3.2(b),

$$h_1 s_i \otimes h_2 s_j = h'_1 s'_i \otimes h'_2 s'_j \iff h_1 = h'_1,\ h_2 = h'_2,\ s_i = s'_i,\ s_j = s'_j. \tag{5}$$

Notice that $\mathcal{A}$ is G-invariant. In fact, by (2), G acts on $\mathcal{A}$ in the following way:

$$\sigma(h_1 s_i \otimes h_2 s_j) = \begin{cases} \sigma h_1 s_i \otimes \delta\sigma\delta h_2 s_j & \text{if } \sigma \in G', \\ \sigma\delta h_2 s_j \otimes \delta\sigma h_1 s_i & \text{if } \sigma \in G \smallsetminus G'. \end{cases} \tag{6}$$

It follows from (6) and (5) that the set

$$\begin{aligned}
\mathcal{A}'_0 &= \{h_1 s_i \otimes h_2 s_j \in \mathcal{A} \mid h_1 = 1\}\\
&= \{s_i \otimes \delta\varepsilon s_j \mid s_i \in S_i,\ s_j \in S_j,\ i+j=n,\ \varepsilon \in G \smallsetminus G'\}
\end{aligned}$$

is a system of representatives of the G'-orbits in $\mathcal{A}$. Let $\mathcal{A}_0 \subseteq \mathcal{A}'_0$ be a system of representatives of the G-orbits in $\mathcal{A}$. Denote

$$\mathcal{A}_1 = \{s_i \otimes \delta\varepsilon s_j \in \mathcal{A}'_0 \mid s_i = s_j,\ \varepsilon \in \mathrm{Inv}(G)\}.$$

Looking at (5) and (6) we see that

$$G_w = \begin{cases} \{1,\varepsilon\} & \text{if } w = s_i \otimes \delta\varepsilon s_j \in \mathcal{A}_1 \\ 1 & \text{if } w \in \mathcal{A}'_0 \smallsetminus \mathcal{A}_1. \end{cases} \tag{7}$$

Observe that $\mathcal{A}_1 \subseteq \mathcal{A}_0$. Indeed,

$$\mathcal{A}_1 = \{w \in \mathcal{A}'_0 \mid G'G_w = G\} = \{w \in \mathcal{A}'_0 \mid G'w = Gw\},$$

and hence every $w \in \mathcal{A}_1$ is the unique element of $\mathcal{A}'_0$ in the G-orbit $G'w$ of w.

For every $w \in \mathcal{A}_0$ choose a basis $\mathcal{B}(w)$ of $M_2(\mathbf{G})$: for $w \in \mathcal{A}_0 \smallsetminus \mathcal{A}_1$ in an arbitrary way, and for $w = s \otimes \delta\varepsilon s \in \mathcal{A}_1$ let $\mathcal{B}(w)$ be the disjoint union $\mathcal{B}(w) = \mathcal{B}_+(w) \cup \mathcal{B}_-(w) \cup \mathcal{B}_0(w)$, where

$$\mathcal{B}_+(w) = \{x^+ \mid x \in X_+(\varepsilon)\} \cup \{x_\varepsilon^+\}$$

$$\mathcal{B}_-(w) = \{x^- \mid x \in X_-(\varepsilon)\} \cup \{x_\varepsilon^-\}$$

$$\mathcal{B}_0(w) = \{x^+ - x_\varepsilon^+ \mid x_\varepsilon \neq x \in X(\varepsilon)\}.$$

This is a basis by Remark 1.2. Notice that the set $\mathcal{B}$ of generators of $N(\mathbf{G})$ defined by (4) can be written in this notation as

$$\mathcal{B} = \{w \otimes y \mid w \in \mathcal{A}_1,\ y \in \mathcal{B}_0(w)\}.$$

If $w = s \otimes \delta\varepsilon s \in \mathcal{A}_1$ then $\varepsilon\mathcal{B}_+(w) = \mathcal{B}_-(w)$ and $\varepsilon\mathcal{B}_-(w) = \mathcal{B}_+(w)$. Also, as $-1 = 1$ in $\mathbb{F}_2$, every $x \in X(\varepsilon)$ satisfies

$$\varepsilon(x^+ - x_\varepsilon^+) = x^- - x_\varepsilon^- = (1 - x^+) - (1 - x_\varepsilon^+) = x^+ - x_\varepsilon^+.$$

Therefore, by (7), $\mathcal{B}(w)$ is G_w-invariant and for every $y \in \mathcal{B}(w)$

$$G_w \cap G_y = \{1,\varepsilon\} \cap G_y = \begin{cases} \{1,\varepsilon\} & \text{if } y \in \mathcal{B}_0(w) \\ 1 & \text{if } y \in \mathcal{B}_+(w) \cup \mathcal{B}_-(w). \end{cases}$$

Thus

$$\mathcal{B} = \{w \otimes y \mid w \in \mathcal{A}_0,\ y \in \mathcal{B}(w),\ G_w \cap G_y \neq 1\}.$$

By Lemma 3.2(e), the $\mathbb{F}_2[G]$-module $Q_n \otimes M_2(\mathbf{G})/N(\mathbf{G})$ is free. ∎

References

[Bro] K. Brown, *Cohomology of groups, GTM 87*, Springer-Verlag 1982.

[Bru] A. Brumer, *Pseudocompact algebras, profinite groups and class formations,* Journal of Algebra **4** (1966), 442-470.

[E] Yu.L. Ershov, *Galois groups of maximal 2-extensions,* Matematicheski Zametki **36** (1984), 956–961.

[G] K.W. Gruenberg, *Projective profinite groups,* Journal London Mathematical Society **42** (1967), 155–165.

[H1] D. Haran, *Closed subgroups of $G(Q)$ with involutions,* Journal of Algebra **129**, 393-411.

[H2] D. Haran, *Cohomology theory of Artin-Schreier structures,* Journal of Pure and Applied Algebra **69**, 141–160 (1990).

[H3] D. Haran, *A proof of Serre's theorem,* Indian Journal of Mathematics **55**, 213–234 (1990).

[HJ1] D. Haran and M. Jarden, *The absolute Galois group of a pseudo real closed field,* Annali della Scuola Normale Superiore di Pisa **12** (1985), 449–489.

[HJ2] D. Haran and M. Jarden, *Real free groups and the absolute Galois group of* $\mathbb{R}(t)$, Journal of pure and applied algebra **37** (1985), 155–165.

[M] S. Mac Lane, *Homology, 3rd corrected edition,* Springer-Verlag 1975.

[P] D.S. Passman, *The algebraic structure of group rings,* Wiley 1977.

[R] L. Ribes, *Introduction to profinite groups and Galois cohomology,* Queen's papers in pure and applied mathematics **24**, Kingston 1970.

[S] J.-P. Serre, *Sur la dimension cohomologique des groupes profinis,* Topology **3** (1965), 413–420.

[W] R. Ware, *Quadratic forms and profinite 2-groups,* Journal of Algebra **58** (1979), 227–237.