A PROOF OF SERRE'S THEOREM

Dan Haran

School of Mathematical Sciences
Raymond and Beverly Sackler
Faculty of Exact Sciences
Tel Aviv University
Tel Aviv, Israel

Introduction

Serre ([9]) proved the following result:

THEOREM A: *Let G be a profinite group without elements of a prime order p, and let H be an open subgroup of G. Then* $\mathrm{cd}_p H = \mathrm{cd}_p G$.

Let G_p be a p-Sylow subgroup of G and let $H_p = H \cap G_p$ be a p-Sylow subgroup of H. By a theorem of Tate ([7], Proposition IV.2.1)

$$\mathrm{cd}_p H_p \le \mathrm{cd}_p H \le \mathrm{cd}_p G = \mathrm{cd}_p G_p \ ,$$

hence we may replace G by G_p and H by H_p. Furthermore, by [7], Proposition IV.2.1, $\mathrm{cd}_p H = \mathrm{cd}_p G$ if $\mathrm{cd}_p G < \infty$. Therefore Theorem A follows from the following result proved by Serre in [9]:

THEOREM A$'$: *Let G be a torsion free pro-p-group and let H be an open subgroup of G. If $\mathrm{cd}_p H < \infty$ then $\mathrm{cd}_p G < \infty$.*

The proof of Theorem A$'$ given in [9] is rather difficult. It uses the theory of Steenrod powers and Cartan's formula to show that for the Bockstein map β: $H^1(G, \mathbb{F}_p) \to H^2(G, \mathbb{F}_p)$ there are non-zero elements $z_1, \ldots, z_m \in H^1(G, \mathbb{F}_p)$ such that $u = \prod_{i=1}^m \beta(z_i) = 0$. On the other hand, if the kernel U of a homomorphism $z \in H^1(G, \mathbb{F}_p)$ satisfies $\mathrm{cd}_p U < \infty$, then the cup product by $\beta(z)$ is an isomorphism $H^q(G, A) \to H^{q+2}(G, A)$ for every G-module A annihilated by p and every $q > \mathrm{cd}_p U$. Thus if $\mathrm{cd}_p U < \infty$ for every open subgroup U of G then $\mathrm{cd}_p G < \infty$. The general assertion can be reduced to this particular case.

Later Serre proved the discrete analogue of Theorem A:

THEOREM B ([10], Theorem 9.2): *Let G be a group without elements of a prime order p and let H be a subgroup of finite index in G. Then* $\mathrm{cd}_p H = \mathrm{cd}_p G$.

The proof of the latter result is much simpler. Again, it is enough to show that $\mathrm{cd}_p G < \infty$ if $\mathrm{cd}_p H < \infty$. But this is done using the fact that $\mathrm{cd}_p G < \infty$ if and only if the trivial $\mathbb{Z}_p[G]$-module $\mathbb{Z}_p$ has a finite projective resolution.

To the best of our knowledge this proof has not been translated to the profinite case. The aim of this note is to fill up this gap. Notice that a straightforward analogue of the second proof does not immediately apply in our situation: In the Galois cohomology theory (as introduced in [8] or [7]) one uses only discrete modules, and there are not enough projective modules among them. We overcome this obstacle by using Brumer's development ([1]) of cohomology via profinite modules. This allows us to carry over Serre's simple proof of Theorem B to profinite groups.

It has been our intention to keep the exposition self-contained, assuming only basics of profinite groups and general cohomology theory (in an abelian category). We therefore repeat (and adapt) arguments given elsewhere, mostly from Brumer [1] and from the very clear exposition of the proof of Theorem B in Passman [6].

The author is grateful to Moshe Jarden for valuable remarks concerning the presentation of the material in this note.

1. Profinite G-modules

Recall that if G is a topological group then a *G-module* is a topological abelian group A on which G continuously acts such that $g(a+b) = ga + gb$ for all $a, b \in A$, $g \in G$. A *homomorphism* of G-modules is a continuous G-invariant homomorphism of their abelian groups.

Definition 1.1: Let $\mathcal{C}$ be a class of finite abelian groups. A *pro-$\mathcal{C}$-G-module* A is the inverse limit $\varprojlim A_i$ of some family $\{A_i\}$ of finite G-modules such that $A_i \in \mathcal{C}$ for every i.

We shall work only with a fixed family $\mathcal{C}$, which allows us to drop the prefix "pro-$\mathcal{C}$-".

> CONVENTION 1.2: Fix a prime p and denote $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$. In this paper G will always be a profinite group. Furthermore, "G-module" will mean "pro-$\mathcal{C}$-G-module", where $\mathcal{C}$ is the class of finite elementary abelian p-groups, i.e., finite vector spaces over $\mathbb{F}_p$.

Thus: finite G-modules are finite vector spaces over $\mathbb{F}_p$; inverse limits of G-modules are again G-modules. If $G = 1$, we write '$\mathbb{F}_p$-module' instead of '1-module'; thus $\mathbb{F}_p$-modules are inverse limits of finite vector spaces over $\mathbb{F}_p$.

Example 1.3. The following are examples of G-modules.

(a) $\mathbb{F}_p$ with the trivial G-action is a finite G-module.

(b) If G is finite then the group ring $\mathbb{F}_p[G] = \left\{ \sum_{g\in G} c_g g \mid c_g \in \mathbb{F}_p \right\}$ is a finite G-module.

(c) The complete group ring $\mathbb{F}_p[\![G]\!] = \varprojlim F[G/N]$, where N runs through the open normal subgroups of G. Observe that $\mathbb{F}_p[G]$ is dense in $\mathbb{F}_p[\![G]\!]$.

(d) If A, B are G-modules then so is $A \oplus B$ (with the product topology).

Let $\mathcal{B}$ be the family of open G-submodules of a G-module A; then $\cap_{B\in\mathcal{B}} B = 0$. Indeed, if $A = \varprojlim_i A_i$, where A_i are finite G-modules and B_i is the kernel of $A \to A_i$ then $B_i \in \mathcal{B}$ for every i, and $\cap_i B_i = 0$. Hence $A = \varprojlim_{B\in\mathcal{B}} A/B$. From this canonical presentation of A as an inverse limit one deduces that closed G-submodules of G-modules and quotients modulo closed G-submodules are G-modules.

It is easy to see that the category of G-modules is abelian. This provides a convenient framework for standard constructions, definitions and arguments. However, a reader less aquainted with abelian categories need not be discouraged, since the category of G-modules is a straightforward analogue of the more familiar category of modules over a ring. In fact, G-modules are topological modules over the topological ring $\mathbb{F}_p[\![G]\!]$.

Let H be a closed subgroup of G. Every G-module is also an H-module; in particular (taking $H = 1$), every G-module is an $\mathbb{F}_p$-module.

2. Free G-modules

Definition 2.1: Let X be a Boolean space. The *free G-module on X* is a G-module $F_G(X)$ and a continuous map $i\colon X \to F_G(X)$ such that for every G-module A and every continuous map $f\colon X \to A$ there exists a unique continuous G-homomorphism $\varphi\colon F_G(X) \to A$ such that $f = \varphi \circ i$.

Remark 2.2. Replacing the clause "a G-module A" by "a finite G-module A" does not alter the definition, since a G-module A is the inverse limit $\varprojlim A_j$ of finite G-modules, and $\varphi\colon F_G(X) \to A$ is uniquely determined by a compatible family of maps $\varphi_j\colon F_G(X) \to A_j$.

LEMMA 2.3: (a) *The free G-module on X exists and is unique up to a unique G-homomorphism.*

(b) *If $X = \varprojlim X_j$ and $G = \varprojlim G_j$ then $F_G(X) = \varprojlim F_{G_j}(X_j)$.*

(c) *If X is the disjoint union of X_1 and X_2 then $F_G(X) = F_G(X_1) \oplus F_G(X_2)$.*

(d) *Let $g_1, g_2 \in G$ and $x_1, x_2 \in X$. Then $g_1 i(x_1) = g_2 i(x_2)$ if and only if $g_1 = g_2$ and $x_1 = x_2$. In particular, $i\colon X \to F_G(X)$ is injective.*

Thus we shall consider X to be a closed subspace of $F_G(X)$, and i the inclusion map.

(e) $F_G(\{1\}) = \mathbb{F}_p[\![G]\!]$.

Proof: (b) Use the universal properties to construct the maps for which $\{F_{G_j}(X_j)\}$ is an inverse system, and then show that $\varprojlim F_{G_j}(X_j)$ has the universal property mentioned in Remark 2.2.

(c) Clearly $F_G(X_1) \oplus F_G(X_2)$ satisfies the universal property of $F_G(X)$.

(d) Consider $\mathbb{F}_p$ with the trivial G-action. If $x_1 \neq x_2$, there exists a continuous map $f\colon X \to \mathbb{F}_p$ such that $f(x_1) = 1$ and $f(x_2) = 0$. Let $\varphi\colon F_G(X) \to \mathbb{F}_p$ be the G-homomorphism such that $f = \varphi \circ i$, then $\varphi\big(g_1 i(x_1)\big) = g_1 f(x_1) = 1$ and $\varphi\big(g_2 i(x_2)\big) = g_2 f(x_2) = 0$, hence $g_1 i(x_1) \neq g_2 i(x_2)$.

If $x_1 = x_2$ and $g_1 \neq g_2$, there is an open $N \triangleleft G$ such that $g_1 N \neq g_2 N$. For the continuous map $f\colon X \to \mathbb{F}_p[G/N]$, given by $f(x) = 1$ for all $x \in X$, let $\varphi\colon F_G(X) \to \mathbb{F}_p[G/N]$ be the unique G-homomorphism such that $f = \varphi \circ i$. Now $\varphi\big(g_1 i(x_1)\big) = g_1 f(x_1) = g_1 N$ and similarly $\varphi\big(g_2 i(x_2)\big) = g_2 N$, hence $g_1 i(x_1) \neq g_2 i(x_2)$.

(e) If G is finite then clearly the group ring $\mathbb{F}_p[G]$ of Example 1.3(b) has the universal property of $F_G(\{1\})$. The general case follows from (b) and Example 1.3(c).

(a) The uniqueness if obvious. Existence: by (b) we may assume that X is finite, and by (c) we may assume that $|X| = 1$, say $X = \{1\}$, in which case $F_G(X)$ exists by (e).

∎

Lemma 2.4: *As an $\mathbb{F}_p$-module, $F_G(X)$ is the free $\mathbb{F}_p$-module $F_1(GX)$ on GX, where*

$$GX = \{gx \mid g \in G\ ,\ x \in X) \subseteq F_G(X)\ .$$

Proof: If $X = \varprojlim X_j$ then $GX = \varprojlim GX_j$, and by Lemma 2.3(b), $F_G(X) = \varprojlim F_G(X_j)$ and $F_1(GX) = \varprojlim F_1(GX_j)$. Thus we may assume that X is finite. Similarly we may assume that G is finite. In this case $F_G(X) = \bigoplus_{x \in X} \mathbb{F}_p[G]x = \bigoplus_{x \in X} \bigoplus_{g \in G} \mathbb{F}_p gx = F_1(GX)$. ∎

In the opposite direction we notice:

Lemma 2.5: *Let P be a G-module, and let W be a closed subset of P such that*

(i) *P is the free $\mathbb{F}_p$-module on W, i.e., $P = F_1(W)$;*

(ii) *$\mathbb{F}_p W = \{nw \mid n \in \mathbb{F}_p\ ,\ w \in W\}$ is G-invariant;*

(iii) *$\{g \in G \mid gw \in \mathbb{F}_p w\} = \{1\}$ for all $w \in W$.*

Then P is a free G-module.

Proof: The group $G' = \mathbb{F}_p^\times \times G$ acts continuously on P by $(n, g)z = ngz$. It follows from (i) that $0 \notin W$ (since there is a homomorphism $P \to \mathbb{F}_p$ mapping W into 1), and from (ii) and (iii) that

(ii') $\mathbb{F}_p^\times W = \{nw \mid n \in \mathbb{F}_p^\times,\ w \in W\} = \mathbb{F}_p W \smallsetminus \{0\}$ is G'-invariant; and

(iii') $\{(n, g) \in G' \mid (n, g)z = z\} = \{1\}$ for all $z \in \mathbb{F}_p^\times W$.

Furthermore, $\mathbb{F}_p^\times W$ is closed in P (it is the image of the compact set $\mathbb{F}_p^\times \times W$ in P). Let X be a closed system of representatives of the G'-orbits in $\mathbb{F}_p^\times W$ (cf. [3], Lemma 2.4). We proceed to show that $P = F_G(X)$.

A continuous map $f\colon X \to A$ into a G-module A can be uniquely extended to a G'-invariant continuous map $f'\colon \mathbb{F}_p^\times W \to A$ by $f'(ngx) = ngf(x)$. By (i) the restriction of f' to W can be uniquely extended to a continuous $\mathbb{F}_p$-linear map $\varphi\colon P \to A$; clearly φ extends f' as well. We claim that φ is a G-homomorphism; obviously it is then the unique G-homomorphism extending f, which will complete the proof.

Fix $g \in G$; both $z \mapsto \varphi(gz)$ and $z \mapsto g\varphi(z)$ are continuous $\mathbb{F}_p$-homomorphisms from P into A. They agree on W, since f' is G'-invariant, hence by (i) they are equal. Thus $\varphi(gz) = g\varphi(z)$ for all $z \in P$. ∎

We notice for the record the following weaker version of Lemma 2.5:

Corollary 2.6: *Let P be a G-module, and let W be a closed subset of P such that*

(i) *P is the free $\mathbb{F}_p$-module on W, i.e., $P = F_1(W)$;*

(ii) *W is G-invariant;*

(iii) *$\{g \in G \mid gw = w\} = \{1\}$ for all $w \in W$.*

Then P is a free G-module.

3. Projective G-modules

By the usual definition of a projective object in an abelian category, a G-module P is *projective* if for every epimorphism of G-modules $\alpha\colon B \to A$ and every morphism $\varphi\colon P \to A$ there exists a morphism $\psi\colon P \to B$ such that $\alpha \circ \psi = \varphi$. In order to present another – equivalent – definition we need a result on fibred products (cf. [4], Lemma 1.1 or [2], Proposition 20.6).

Lemma 3.1: *Consider a commutative diagram of G-modules*

$$\begin{tikzcd}
P \arrow[drr, "\varphi"] \arrow[ddr, "\varphi'"'] & & \\
& B \arrow[r, "\alpha"'] \arrow[d, "\alpha'"] & B/K \arrow[d, "\pi"] \\
& B/K' \arrow[r, "\pi'"'] & B/(K+K')
\end{tikzcd}$$

in which K and K' are G-submodules of B and $\alpha, \alpha', \pi, \pi'$ are the quotient maps. Assume that K' is open in B and $K \cap K' = \{0\}$. Then there exists a unique morphism $\psi\colon P \to B$ such that $\alpha \circ \psi = \varphi$ and $\alpha' \circ \psi = \varphi'$.

Proof: An easy diagram-chasing shows that for every $\bar{b} \in B/K$ and every $\bar{b}' \in B/K'$ such that $\pi(\bar{b}) = \pi'(\bar{b}')$ there exists a unique $b \in B$ such that $\alpha(b) = \bar{b}$ and $\alpha'(b) = \bar{b}'$. It follows that there exists a unique set-theoretic function $\psi \colon P \to B$ such that $\alpha \circ \psi = \varphi$ and $\alpha' \circ \psi = \varphi'$. We have

$$\psi(z_1 + z_2) = \psi(z_1) + \psi(z_2) \quad \text{for all} \quad z_1, z_2 \in P \ ,$$

$$\psi(gz) = g\psi(z) \quad \text{for all} \quad z \in P \quad \text{and all} \quad g \in G \ ,$$

as can be readily seen by applying p and p' to both sides of these equations. Finally, ψ is continuous, since its restriction to the open subgroup $U = \mathrm{Ker}\ \varphi'$ of P is continuous. Indeed, $\psi(U) \subseteq K'$, $\varphi(U) \subseteq (K + K')/K$, and the restriction of α to K' is an isomorphism $K' \to (K + K')/K$. As φ is continuous and $\alpha \circ \psi = \varphi$, the restriction of ψ to U is also continuous. ∎

LEMMA 3.2 (cf. [2], Lemma 20.8, Parts B, C): *A G-module P is projective if and only if for every epimorphism of finite G-modules $\alpha \colon B \to A$ and every morphism $\varphi \colon P \to A$ there exists a morphism $\psi \colon P \to B$ such that $\alpha \circ \psi = \varphi$.*

Proof: Assume that the condition holds and let $\alpha \colon B \to A$ be an epimorphism and $\varphi \colon P \to A$ a morphism of G-modules. Denote $K = \mathrm{Ker}\ \alpha$. Without loss of generality α is the quotient map $B \to B/K$.

(a) Assume first that K is finite. Then there exists an open G-submodule K' of B such that $K \cap K' = \{0\}$. Let $\alpha, \alpha', \pi, \pi'$ be as in Lemma 3.1 (see the diagram there). Since B/K' and $B/(K + K')$ are finite G-modules, by the assumption there exists a morphism $\varphi' \colon P \to B/K'$ such that the diagram commutes. By Lemma 3.1 there exists a morphism $\psi \colon P \to B$ such that $\alpha \circ \psi = \varphi$.

(b) In the general case let Γ be the collection of pairs (L, λ), where L is a G-submodule of K and $\lambda \colon P \to B/L$ is a morphism such that $\alpha_{L,K} \circ \lambda = \varphi$, where $\alpha_{L,K}$ is the quotient map $B/L \to B/K$. Partially order Γ by letting $(L', \lambda') \geq (L, \lambda)$ mean that $L' \subseteq L$ and $\alpha_{L',L} \circ \lambda' = \lambda$. Then Γ is inductive, and hence by Zorn's Lemma it has a maximal element (L, λ).

It remains to show that $L = 0$. If not, there is an open G-submodule N of G such that $L \not\subseteq N$; thus $L' = N \cap L$ is a proper open G-submodule of L. As $\mathrm{Ker}\ \alpha_{L',L}$ is finite, by (a) there exists a morphism $\lambda'\colon P \to B/L'$ such that $\alpha_{L',L} \circ \lambda' = \lambda$. Then $(L', \lambda') \in \Gamma$ and $(L', \lambda') > (L, \lambda)$, a contradiction. ∎

LEMMA 3.3: *Let P be a G-module.*

(a) *P is a quotient of a free G-module.*

(b) *If P is free then P is projective.*

(c) *P is projective if and only if it is a direct summand of a free G-module.*

(d) *If $P = \varprojlim P_i$, where P_i are projective G-modules then P is projective.*

(e) *P is projective in the category of $\mathbb{F}_p$-modules.*

Proof: (a) The identity $P \to P$ induces a G-epimorphism $F_G(P) \to P$.

(b) In the setup of Lemma 3.2 let $s\colon A \to B$ be a section of α, and let $\psi\colon P = F_G(X) \to B$ be the unique extension of $s \circ \mathrm{res}_X \varphi\colon X \to B$. Then $\alpha \circ \psi = \varphi$, since this is true on X.

(c) is a formal consequence of (a) and (b) in an abelian category: cf. [5], Proposition I.5.5.

(d) In the setup of Lemma 3.2 the map $\varphi\colon P \to A$ factors through some P_i (since A is finite), say into $\varphi'\colon P \to P_i$ and $\varphi_i\colon P_i \to A$. As P_i is projective, there is $\psi_i\colon P_i \to B$ such that $\alpha \circ \psi_i = \varphi_i$. Thus $\alpha \circ (\psi_i \circ \varphi') = \varphi$.

(e) If P is finite then it is a free $\mathbb{F}_p$-module, and hence projective. The general case follows by (d). ∎

In particular every G-module P is a quotient of a projective G-module P_0, and therefore, by induction, P has a *projective resolution*

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

(that is, P_* is an exact sequence and P_i are projective G-modules). If

$$\cdots \to P'_n \xrightarrow[\partial'_n]{} P'_{n-1} \xrightarrow[\partial'_{n-1}]{} \cdots \xrightarrow[\partial'_2]{} P'_1 \xrightarrow[\partial'_1]{} P'_0 \xrightarrow[\partial']{} P \to 0$$

is another projective resolution of P, there exists a chain transformation from the former projective resolution to the latter, that lifts the identity of P; such a chain transformation is unique up to a homotopy ([5], Theorem III.6.1).

Corollary 3.4 (cf. [6], Lemma 10.3.10): *A complex of $\mathbb{F}_p$-modules*

$$\cdots \to E_n \underset{\varepsilon_n}{\longrightarrow} E_{n-1} \longrightarrow \cdots \underset{\varepsilon_2}{\longrightarrow} E_1 \underset{\varepsilon_1}{\longrightarrow} E_0 \underset{\varepsilon}{\longrightarrow} E \to 0$$

is exact if and only if it splits, i.e., there exist continuous homomorphisms $s\colon E \to E_0$ and $s_n\colon E_n \to E_{n+1}$ for $n \geq 0$ such that

$$1 = \varepsilon s \ , \quad 1 = s\varepsilon + \varepsilon_1 s_0 \quad \text{and} \quad 1 = s_{n-1}\varepsilon_n + \varepsilon_{n+1}s_n \quad \text{for all} \quad n \geq 1 \ .$$

Proof: Put $E_{-1} = E$, $E_{-2} = 0$, $\varepsilon_0 = \varepsilon$, $\varepsilon_{-1} = 0$. Then we have to show that

$$E_* : \qquad \cdots \to E_n \underset{\varepsilon_n}{\longrightarrow} E_{n-1} \longrightarrow \cdots \underset{\varepsilon_2}{\longrightarrow} E_1 \underset{\varepsilon_1}{\longrightarrow} E_0 \underset{\varepsilon_0}{\longrightarrow} E_{-1} \underset{\varepsilon_{-1}}{\longrightarrow} E_{-2} \to 0$$

is exact if and only if there exist continuous homomorphisms $s_n\colon E_n \to E_{n+1}$, for $n \geq -1$, such that (letting $s_{-2}\colon E_{-2} \to E_{-1}$ be the zero map)

$$(*) \qquad 1 = s_{n-1}\varepsilon_n + \varepsilon_{n+1}s_n \quad \text{for all} \quad n \geq -1 \ .$$

If E_* is exact then it is a projective resolution of $E_{-2} = 0$ by Lemma 3.3(e), and both 0 and 1 are chain transformations of E_* to itself that lift the identity of $E_{-2} = 0$. By the preceding remark they are homotopic, which gives $(*)$. Conversely, $(*)$ implies the exactness of E_*: if $a \in \operatorname{Ker} \varepsilon_n$, for $n \geq -1$, then

$$a = s_{n-1}\varepsilon_n(a) + \varepsilon_{n+1}s_n(a) = \varepsilon_{n+1}s_n(a) \in \operatorname{im}(\varepsilon_{n+1}) \ . \qquad \blacksquare$$

Let P be a G-module, and let

$$P_* : \qquad \cdots \to P_n \underset{\partial_n}{\longrightarrow} P_{n-1} \underset{\partial_{n-1}}{\longrightarrow} \cdots \underset{\partial_2}{\longrightarrow} P_1 \underset{\partial_1}{\longrightarrow} P_0 \underset{\partial}{\longrightarrow} P \to 0$$

be a projective resolution of P. Let A be a G-module. Then P_* yields the complex $\operatorname{Hom}_G(P_*, A)$ of abelian groups

$$0 \to \operatorname{Hom}_G(P_0, A) \to \operatorname{Hom}_G(P_1, A) \to \cdots \to \operatorname{Hom}_G(P_{n-1}, A) \to \operatorname{Hom}_G(P_n, A) \to \cdots \ ,$$

where $\operatorname{Hom}_G(P_n, A)$ is the group of G-homomorphisms from P_n into A. The homology groups

$$\operatorname{Ext}^n_G(P, A) = H^n\big(\operatorname{Hom}(P_*, A)\big)$$

of this complex do not depend on the choice of the projective resolution P_* of P ([5], Corollary III.6.3).

For example, consider $\mathbb{F}_p$ as a G-module with the trivial G-action. To compute $\mathrm{Ext}^n_G(\mathbb{F}_p, A)$ we shall use the so-called *standard free resolution* P_*, defined as follows:

P_0 is the free G-module $F_G(\{1\}) = \mathbb{F}_p[\![G]\!]$ (see Lemma 2.3(e));

P_n is the free G-module $F_G(G^n)$; here $G^n = G \times \cdots \times G$ (n times);

$\partial\colon P_0 \to \mathbb{F}_p$ is the unique extension of the map $\{1\} \to \mathbb{F}_p$ given by $1 \mapsto 1$;

(thus if G is finite then $\partial(\sum_{g\in G} a_g g) = \sum_{g\in G} a_g$); and

$\partial_n\colon P_n \to P_{n-1}$ is the unique extension of the map $\partial_n\colon G^n \to P_{n-1}$ given by

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

We leave it to the reader to check that P_* is indeed an exact sequence. If G is finite, this is done exactly as in [5], Theorem IV.5.1; the general case follows, since an inverse limit of exact sequences is exact ([7], Proposition I.3.6).

By the universal property of free G-modules, $\mathrm{Hom}_G(P_n, A)$ may be identified with the set $C^n(G,A)$ of continuous functions $f\colon G^n \to A$, and $\partial^*\colon C^{n-1}(G,A) \to C^n(G,A)$ is then clearly given by

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

Thus $\mathrm{Hom}_G(P_*, A)$ is the complex $C^*(G,A)$ from which one derives the cohomology groups $H^n(G,A)$ of G with coefficients in A (see [7], p. 94). Hence:

COROLLARY 3.5: *If A is a finite G-module then*

$$\mathrm{Ext}^n_G(\mathbb{F}_p, A) = H^n(G,A)\ .$$

The following result provides the link between projective resolutions and the cohomological dimension.

PROPOSITION 3.6: *Let P be a G-module.*

(a) *If there is a projective resolution P_* of P with $P_n = 0$ then $\mathrm{Ext}^n_G(P, A) = 0$ for all G-modules A.*

(b) *If $\mathrm{Ext}^n_G(P, A) = 0$ for all finite G-modules A then there is a projective resolution P_* of P with $P_{n+1} = 0$.*

Proof: (a) clear.

(b) Let P_* be a projective resolution. Let $P_n \xrightarrow[\mu]{} \partial(P_n) \xrightarrow[i]{} P_{n-1}$ be the decomposition of $\partial_n\colon P_n \to P_{n-1}$ into an epimorphism μ and a monomorphism i. It suffices to show that $\partial_n(P_n)$ is projective, since then

$$0 \to \partial_n(P_n) \xrightarrow[i]{} P_{n-1} \xrightarrow[\partial_{n-1}]{} \cdots \xrightarrow[\partial_1]{} P_0 \xrightarrow[\partial]{} P \longrightarrow 0$$

is a projective resolution of P.

We shall use Lemma 3.2 to prove this. Consider the diagram

$$\begin{tikzcd} P_{n-1} & \partial_n(P_n) \arrow[l, "i"'] \arrow[d, "\varphi"'] & P_n \arrow[l, "\mu"'] & P_{n+1} \arrow[l, "\partial_{n+1}"'] \\ B \arrow[r, "\alpha"'] & A & & \end{tikzcd}$$

in which α is an epimorphism of finite G-modules. Since $H^n(G, A) = 0$, the sequence

$$\mathrm{Hom}_G(P_{n-1}, A) \to \mathrm{Hom}_G(P_n, A) \to \mathrm{Hom}_G(P_{n+1}, A)$$

is exact. Notice that $\mu\partial_{n+1} = 0$, hence $\varphi\mu$ is in the kernel of $\mathrm{Hom}_G(P_n, A) \to \mathrm{Hom}_G(P_{n+1}, A)$. Therefore there exists a G-homomorphism $\varphi'\colon P_{n-1} \to A$ such that $\varphi\mu = \varphi'\partial_n = \varphi' i\mu$, in particular, $\varphi' i = \varphi$. Since P_{n-1} is projective, there is $\psi\colon P_{n-1} \to B$ such that $\alpha\psi = \varphi'$. Thus $\alpha(\psi i) = \varphi$, which shows that $\partial_n(P_n)$ is projective. ∎

Actually, one can achieve even $P_n = 0$ in (b), but the proof is much more subtle (see [1], Corollary 3.2). We shall not need this refinement.

COROLLARY 3.7: $\mathrm{cd}_p G < \infty$ *if and only if* $\mathbb{F}_p$ *has a projective resolution of finite length.*

Proof: By [7], Proposition IV.1.5 and its proof, $\mathrm{cd}_p G < \infty$ if and only if there is n such that $H^{n+1}(G, A) = 0$ for all finite G-modules A. (Recall that by Convention 1.2

finite G-modules are finite elementary abelian p-groups.) Now apply Corollary 3.5 and Proposition 3.6. ∎

4. The Complete Tensor Product

Let A, B, C be $\mathbb{F}_p$-modules. A continuous map $f\colon A \times B \to C$ is $\mathbb{F}_p$-*bilinear* if

$$f(a+a', b) = f(a,b) + f(a', b) \quad \text{and} \quad f(a, b+b') = f(a,b) + f(a,b')$$

for all $a, a' \in A$, $b, b' \in B$. This, of course, also implies that

$$f(na, b) = nf(a,b) = f(a, nb)$$

for all $n \in \mathbb{F}_p$, $a \in A$, $b \in B$.

Recall ([1], Section 2) that the *complete tensor product* of A and B is an $\mathbb{F}_p$-module $A\widehat{\otimes}B$ and an $\mathbb{F}_p$-bilinear map $\theta\colon A \times B \to A\widehat{\otimes}B$ (we write $a\widehat{\otimes}b$ for $\theta(a,b)$) with the following universal property: given an $\mathbb{F}_p$-module C and an $\mathbb{F}_p$-bilinear map $f\colon A \times B \to C$, there exists a unique continuous $\mathbb{F}_p$-linear map $g\colon A\widehat{\otimes}B \to C$ such that $g \circ \theta = f$.

Remark 4.1.

(a) Replacing the clause "an $\mathbb{F}_p$-module C" above by "a finite $\mathbb{F}_p$-module C" does not alter the definition of the complete tensor product (cf. Remark 2.2).

(b) The complete tensor product of A and B is obviously unique up to a unique isomorphism, if it exists. Now $\varprojlim A/U \otimes B/V$, where U (resp. V) runs through the open $\mathbb{F}_p$-submodules of A (resp. B), satisfies the universal property mentioned in (a). Therefore $A\widehat{\otimes}B = \varprojlim A/U \otimes B/V$; notice that the $\mathbb{F}_p$-modules $A/U \otimes B/V$ are finite. Thus $A\widehat{\otimes}B$ is the completion of $A \otimes B$ in the topology induced by the kernels of the maps $A \otimes B \to A/U \otimes B/V$.

(c) If $\alpha\colon A \to A'$ and $\beta\colon B \to B'$ are morphisms of $\mathbb{F}_p$-modules then, by the definition of $A\widehat{\otimes}B$, there exists a unique homomorphism $\alpha\widehat{\otimes}\beta\colon A\widehat{\otimes}B \to A'\widehat{\otimes}B'$ such that $(\alpha\widehat{\otimes}\beta)(a\widehat{\otimes}b) = \alpha(a)\widehat{\otimes}\beta(b)$ for all $a \in A$, $b \in B$.

(d) It follows immediately from the universal property of the complete tensor product or form (b) above that $(A\widehat{\otimes}B)\widehat{\otimes}C = A\widehat{\otimes}(B\widehat{\otimes}C)$, and hence we denote it by $A\widehat{\otimes}B\widehat{\otimes}C$.

More generally, if $A_0, \dots, A_m$ are $\mathbb{F}_p$-modules then $A_0\widehat{\otimes}\cdots\widehat{\otimes}A_m$ can be inductively defined by inserting parentheses in any meaningful way.

LEMMA 4.2: *Let $F_1(X)$ and $F_1(Y)$ be free $\mathbb{F}_p$-modules. Then $F_1(X)\widehat{\otimes}F_1(Y)$ is the free $\mathbb{F}_p$-module on its subset $\{x\widehat{\otimes}y \mid x \in X\ ,\ y \in Y\}$.*

Proof: It is enough to show that the $\mathbb{F}_p$-linear map $F_1(X \times Y) \to F_1(X)\widehat{\otimes}F_1(Y)$, extending $(x, y) \mapsto x\widehat{\otimes}y$, is an isomorphism. This is well known if X and Y are finite, since then $F_1(X)\widehat{\otimes}F_1(Y) = F_1(X) \otimes F_1(Y)$. In the general case $X = \varprojlim X_i$ and $Y = \varprojlim Y_i$, where X_i and Y_1 are finite. Therefore $X \times Y = \varprojlim X_i \times Y_i$, and so by Lemma 2.3(b), $F_1(X) = \varprojlim F_1(X_i)$, $F_1(Y) = \varprojlim F_1(Y_i)$ and $F_1(X \times Y) = \varprojlim F_1(X_i \times Y_i)$. Thus $F_1(X \times Y) \to F_1(X)\widehat{\otimes}F_1(Y)$ is the inverse limit of the isomorphisms $F_1(X_i \times Y_i) \to F_1(X_i)\widehat{\otimes}F_1(Y_i)$, and hence an isomorphism. ∎

The *complete tensor product* $A_*\widehat{\otimes}B_*$ of two sequences of $\mathbb{F}_p$-modules

$$A_* : \qquad \cdots \to A_n \xrightarrow[\alpha_n]{} A_{n-1} \longrightarrow \cdots \longrightarrow A_1 \xrightarrow[\alpha_1]{} A_0 \xrightarrow[\alpha]{} A \to 0$$

$$B_* : \qquad \cdots \to B_n \xrightarrow[\beta_n]{} B_{n-1} \longrightarrow \cdots \longrightarrow B_1 \xrightarrow[\beta_1]{} B_0 \xrightarrow[\beta]{} B \to 0$$

is the sequence of $\mathbb{F}_p$-modules

$$C_* : \qquad \cdots \to C_n \xrightarrow[\gamma_n]{} C_{n-1} \longrightarrow \cdots \longrightarrow C_1 \xrightarrow[\gamma_1]{} C_0 \xrightarrow[\gamma]{} C \to 0$$

defined as follows. First, to simplify the notation, for $n < 0$ put $A_n = B_n = 0$, and for $n \leq 0$ let $\alpha_n\colon A_n \to A_{n-1}$ and $\beta_n\colon B_n \to B_{n-1}$ be the zero maps. Then define

$$C = A\widehat{\otimes}B \quad \text{and} \quad C_n = \oplus_{i=0}^{n}(A_i\widehat{\otimes}B_{n-i}) = \oplus_{i+j=n}(A_i\widehat{\otimes}B_j)\ ,$$

$$\gamma = \alpha\widehat{\otimes}\beta \quad \text{and} \quad \gamma_n = \oplus_{i+j=n}\left[(\alpha_i\widehat{\otimes}1) + (-1)^i(1\widehat{\otimes}\beta_j)\right]\ , \quad \text{for every} \quad n \in \mathbb{Z}$$

(this is where α_0, β_0 come in). The last equation simply means that

$$\gamma_n(v_i\widehat{\otimes}v_j) = \alpha_i(v_i)\widehat{\otimes}v_j + (-1)^i v_i\widehat{\otimes}\beta_j(v_j)\ , \quad \text{for} \quad v_i \in A_i \quad \text{and} \quad v_j \in B_j\ .$$

LEMMA 4.3 (cf. [6], Lemma 10.3.11): *The complete tensor product of exact sequences of $\mathbb{F}_p$-modules is also an exact sequence.*

Proof: Assume that A_* and B_* are exact. Using Remark 4.1(c) it is straightforward to check that $\gamma_n\gamma_{n+1} = 0$ and $\gamma\gamma_1 = 0$. Since A_* is exact, by Corollary 3.4 there exist $\mathbb{F}_p$-homomorphisms $s\colon A \to A_0$ and $s_n\colon A_n \to A_{n+1}$, for $n \geq 0$ that split A_*, i.e.,

$$\alpha s = 1 \ , \quad 1 = s\alpha + \alpha_1 s_0 \quad \text{and} \quad 1 = s_{n-1}\alpha_n + \alpha_{n+1}s_n \ , \quad \text{for all} \quad n \geq 1 \ .$$

Similarly there exist $t\colon B \to B_0$ and $t_n\colon B_n \to B_{n+1}$, for $n \geq 0$ that split B_*. Check (again using Remark 4.1(c)) that $u = s\widehat{\otimes}t\colon C \to C_0$ and $u_n\colon C_n \to C_{n+1}$, given by

$$u = s\widehat{\otimes}t \quad \text{and} \quad u_n = \big[(s\alpha\widehat{\otimes}t_n) + (s_0\widehat{\otimes}1)\big] \oplus \big(\oplus_{i=1}^n (s_i\widehat{\otimes}1)\big) \ , \quad \text{for} \quad n \geq 0 \ ,$$

split C_*. Thus by Corollary 3.4 sequence C_* is exact. ∎

5. Serre's Theorem

This section is based on Passman [6], Section 10.3 that deals with discrete groups.

Let H be an open subgroup of G, say $m = (G : H)$, and choose $1 = g_1, g_2, \ldots, g_m \in G$ such that $G = \bigcup_{i=1}^m Hg_i$. To fix the notation, write for all $\sigma \in G$ and all $i = 1, \ldots, m$

$$g_i\sigma = h_i(\sigma)g_{i\sigma} \ , \tag{1}$$

where $i \mapsto i\sigma$ is a permutation of $\{1, 2, \ldots, m\}$ and $h_i(\sigma) \in H$. Clearly $(i, \sigma) \mapsto i\sigma$ and $h_i\colon G \to H$, $i = 1, \ldots, m$, are continuous functions. For $\sigma, \tau \in G$ we have

$$h_i(\sigma\tau)g_{i(\sigma\tau)} = g_i(\sigma\tau) = (g_i\sigma)\tau = h_i(\sigma)g_{i\sigma}\tau = h_i(\sigma)h_{i\sigma}(\tau)g_{(i\sigma)\tau} \ ,$$

hence

$$i(\sigma\tau) = (i\sigma)\tau \ , \tag{2}$$

$$h_i(\sigma\tau) = h_i(\sigma)h_{i\sigma}(\tau) \ . \tag{3}$$

Given a sequence $\mathbf{P} = (P_0, P_1, P_2, \ldots)$ of H-modules, define a G-module structure on the $\mathbb{F}_p$-module

$$Q_n(\mathbf{P}) = Q_n(P_0, P_1, P_2, \ldots, P_n) = \bigoplus_{i_1+\cdots+i_m=n} P_{i_1} \widehat{\otimes} P_{i_2} \widehat{\otimes} \cdots \widehat{\otimes} P_{i_m}$$

in the following way. Write $d(v) = j$ if $v \in P_j$. Every $\tau \in G$ induces an $\mathbb{F}_p$-linear map $P_{i_1} \widehat{\otimes} \cdots \widehat{\otimes} P_{i_m} \to P_{i_{1\tau}} \widehat{\otimes} \cdots \widehat{\otimes} P_{i_{m\tau}}$ by

$$\tau(v_1 \widehat{\otimes} \cdots \widehat{\otimes} v_m) = (-1)^a v_1' \widehat{\otimes} \cdots \widehat{\otimes} v_m' \ , \tag{4}$$

where

$$v_i' = h_i(\tau) v_{i\tau} \tag{4'}$$

and

$$a = \sum_{\substack{i<j \\ i\tau^{-1} > j\tau^{-1}}} d(v_i) d(v_j) \ . \tag{4''}$$

This map uniquely extends to an $\mathbb{F}_p$-linear map $\tau\colon Q_n(\mathbf{P}) \to Q_n(\mathbf{P})$.

Notice that

$$d(v_i') = d(v_{i\tau}) \ . \tag{5}$$

Lemma 5.1: *$Q_n(\mathbf{P})$ is a G-module.*

Proof: Clearly the map $(\tau, v) \mapsto \tau(v)$ from $G \times Q_n(\mathbf{P}) \to Q_n(\mathbf{P})$ is continuous. Also $1(v) = v$, since the right handed side of (4") is an empty sum, if $\tau = 1$. We have to show that

$$\sigma\big(\tau(v_1 \widehat{\otimes} v_2 \widehat{\otimes} \cdots \widehat{\otimes} v_m)\big) = (\sigma\tau)(v_1 \widehat{\otimes} v_2 \widehat{\otimes} \cdots \widehat{\otimes} v_m) \ ,$$

for all $\sigma, \tau \in G$. By definition (4)

$$\sigma\big(\tau(v_1 \widehat{\otimes} v_2 \widehat{\otimes} \cdots \widehat{\otimes} v_m)\big) = (-1)^a \sigma(v_1' \widehat{\otimes} v_2' \widehat{\otimes} \cdots \widehat{\otimes} v_m') = (-1)^{a+b} v_1'' \widehat{\otimes} v_2'' \widehat{\otimes} \cdots \widehat{\otimes} v_m'' \ ,$$

where v_i' and a' are given by equations ($4'$) and ($4''$), and

$$v_i'' = h_i(\sigma) v_{i\sigma}' \quad \text{and} \quad b = \sum_{\substack{i<j \\ i\sigma^{-1} > j\sigma^{-1}}} d(v_i') d(v_j') \ .$$

Hence by ($4'$) and (3)

$$v_i'' = h_i(\sigma) h_{i\sigma}(\tau) v_{i\sigma\tau} = h_i(\sigma\tau) v_{i\sigma\tau} \ ,$$

and thus it remains to be shown that

$$a + b \equiv \sum_{\substack{i<j \\ i\tau^{-1}\sigma^{-1} > j\tau^{-1}\sigma^{-1}}} d(v_i) d(v_j) \bmod 2 \ .$$

Now $a = a_1 + a_2$, where

$$\begin{aligned} a_1 &= \sum d(v_i) d(v_j) \quad \text{with} \quad i<j \quad i\tau^{-1} > j\tau^{-1} \quad i\tau^{-1}\sigma^{-1} > j\tau^{-1}\sigma^{-1} \ , \\ a_2 &= \sum d(v_i) d(v_j) \quad \text{with} \quad i<j \quad i\tau^{-1} > j\tau^{-1} \quad i\tau^{-1}\sigma^{-1} < j\tau^{-1}\sigma^{-1} \ . \end{aligned}$$

By (5) and a change of the summation indices,

$$b = \sum_{\substack{i<j \\ i\sigma^{-1} > j\sigma^{-1}}} d(v_{i\tau}) d(v_{j\tau}) = \sum_{\substack{i\tau^{-1} < j\tau^{-1} \\ i\tau^{-1}\sigma^{-1} > j\tau^{-1}\sigma^{-1}}} d(v_i) d(v_j) = b_1 + b_2 \ ,$$

where

$$\begin{aligned} b_1 &= \sum d(v_i) d(v_j) \quad \text{with} \quad i<j \quad i\tau^{-1} < j\tau^{-1} \quad i\tau^{-1}\sigma^{-1} > j\tau^{-1}\sigma^{-1} \ , \\ b_2 &= \sum d(v_i) d(v_j) \quad \text{with} \quad i>j \quad i\tau^{-1} < j\tau^{-1} \quad i\tau^{-1}\sigma^{-1} > j\tau^{-1}\sigma^{-1} \ . \end{aligned}$$

By interchanging i and j notice that $a_2 = b_2$. Thus

$$a + b = a_1 + b_1 + 2a_2 \equiv a_1 + b_1 = \sum_{\substack{i<j \\ i\tau^{-1}\sigma^{-1} > j\tau^{-1}\sigma^{-1}}} d(v_i) d(v_j) \quad \bmod 2 \ . \qquad \blacksquare$$

More can be said about $Q_n(\mathbf{P})$ if the P_i are free or, at least, projective.

LEMMA 5.2: *Assume that P_i is a free H-module, $P_i = F_H(X_i)$, for $i \geq 0$. Then*

(a) *$Q_n(\mathbf{P})$ is the free $\mathbb{F}_p$-module on the subset*

$$\begin{aligned} W = &\{h_1 v_1 \widehat{\otimes} \cdots \widehat{\otimes} h_m v_m \mid \\ &\quad h_1, \ldots, h_m \in H,\ v_1 \in X_{i_1}, \ldots, v_m \in X_{i_m},\ i_1 + \cdots + i_m = n\} \end{aligned}$$

(b) *$\mathbb{F}_p W = \{nw \mid n \in \mathbb{F}_p\ ,\ w \in W\}$ is G-invariant.*

(c) *Let $0 \neq w = h_1 v_1 \widehat{\otimes} \cdots \widehat{\otimes} h_m v_m \in W$ and let $\tau \in G$. Then $\tau(w) \in \mathbb{F}_p w$ if and only if*

$$v_{j\tau} = v_j \qquad \text{and} \qquad g_j \tau g_{j\tau}^{-1} = h_j h_{j\tau}^{-1}\ , \qquad \text{for } 1 \leq j \leq m$$

(d) *$\{\tau \in G \mid \tau(w) \in \mathbb{F}_p w\} \cap H = \{1\}$ for every $0 \neq w \in W$.*

Proof: (a) By Lemma 2.4, P_i is the free $\mathbb{F}_p$-module on $\{hv \mid h \in H,\ v \in X_i\}$, and by Lemma 4.2, $P_{i_1} \widehat{\otimes} P_{i_2} \widehat{\otimes} \cdots \widehat{\otimes} P_{i_m}$ is the free $\mathbb{F}_p$-module on

$$\{h_1 v_1 \widehat{\otimes} \cdots \widehat{\otimes} h_m v_m \mid h_1, \ldots, h_m \in H,\ v_1 \in X_{i_1}, \ldots, v_m \in X_{i_m}\}$$

As $Q_n(\mathbf{P})$ is the direct sum of such free $\mathbb{F}_p$-modules, (a) follows.

(b) By (4), $\tau(w) = \pm w'$, where

$$w' = h_1(\tau) h_{1\tau} v_{1\tau} \widehat{\otimes} \cdots \widehat{\otimes} h_m(\tau) h_{m\tau} v_{m\tau}\ . \tag{6}$$

We see that $w' \in W$. Hence $\tau(w) \in \mathbb{F}_p W$.

(c) Define w' by (6). Then

$$\tau(w) \in \mathbb{F}_p w \Leftrightarrow w' \in \mathbb{F}_p w \Leftrightarrow w = w'\ ,$$

since w, w' belong to the free $\mathbb{F}_p$-basis W of $Q_n(\mathbf{P})$. But

$$w = w' \Leftrightarrow h_j(\tau) h_{j\tau} v_{j\tau} = h_j v_j \Leftrightarrow h_j(\tau) h_{j\tau} = h_j \quad \text{and} \quad v_{j\tau} = v_j\ , \quad \text{for} \quad 1 \leq j \leq m\ .$$

By (1), $h_j(\tau) = g_j \tau g_{j\tau}^{-1}$, hence the assertion follows.

(d) Let $\tau \in H$ such that $\tau(w) \in \mathbb{F}_p w$. By (c) we have $g_1 \tau g_{1\tau}^{-1} = h_1 h_{1\tau}^{-1}$. Recall that $g_1 = 1$, and notice that $1\tau = 1$, by (1). Thus $\tau = 1$. ∎

Lemma 5.3: *Let $\mathbf{P} = (P_0, P_1, P_2, \ldots)$ and $\mathbf{F} = (F_0, F_1, F_2, \ldots)$ be sequences of H-modules. If P_i is a direct summand of F_i, for every $i \geq 0$, then the G-module $Q_n(\mathbf{P})$ is a direct summand of $Q_n(\mathbf{F})$, for every $n \geq 0$.*

Proof: For every $i \geq 0$ there exists an H-module P_i' such that $F_i = P_i \oplus P_i'$. Write $P_{i,0} = P_i$ and $P_{i,1} = P_i'$. It is easy to see that

$$Q_n(F_0, F_1, \ldots, F_n) = \bigoplus_{i_0, i_1, \ldots, i_n \in \{0,1\}} Q_n(P_{0,i_0}, P_{1,i_1}, \ldots, P_{n,i_n})$$

(not only as $\mathbb{F}_p$-modules, but also as G-modules). Thus $Q_n(\mathbf{P}) = Q_n(P_0, P_1, \ldots, P_n)$ is a direct summand of $Q_n(\mathbf{F}) = Q_n(F_0, F_1, \ldots, F_n)$. ∎

The preceding lemmas give a nice characterization in one case:

Corollary 5.4: *Assume that G is torsion free. Let $\mathbf{P} = (P_0, P_1, P_2, \ldots)$ be a sequence of projective H-modules. Then $Q_n(\mathbf{P})$ is a projective G-module for every $n \geq 0$.*

Proof: Since projective modules are precisely the direct summands of free modules (Lemma 3.3(c)), by Lemma 5.3 it is enough to show that $Q_n(\mathbf{P})$ is a free G-module for every $n \geq 0$, if the P_i are free H-modules.

By Lemma 5.2, $Q_n(\mathbf{P})$ is the free $\mathbb{F}_p$-module on a certain subset W, for which $\mathbb{F}_p W$ is G-invariant, and, denoting $G(w) = \{\tau \in G \mid \tau(w) \in \mathbb{F}_p w\}$, we have $G(w) \cap H = \{1\}$ for every $0 \neq w \in W$. But $G(w) \cap H$ is open in $G(w)$, since H is open in G. Therefore $G(w)$ is a finite subgroup of G, and hence $G(w) = 1$. By the criterion of Lemma 2.5, $Q_n(\mathbf{P})$ is a free G-module. ∎

Our next objective are projective resolutions.

Lemma 5.5: *Let*

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

be an exact sequence of H-modules. Write $d(v) = j$ if $v \in P_j$, and denote

$$\partial_{ik}(v) = \begin{cases} \partial_{d(v)}(v) & \text{if } i = k \\ v & \text{if } i \neq k \end{cases}. \tag{7}$$

Then

$$Q_* : \qquad \cdots \to Q_n \underset{\gamma_n}{\longrightarrow} Q_{n-1} \underset{\gamma_{n-1}}{\longrightarrow} \cdots \underset{\gamma_2}{\longrightarrow} Q_1 \underset{\gamma_1}{\longrightarrow} Q_0 \underset{\gamma}{\longrightarrow} \mathbb{F}_p \to 0 \ ,$$

where

$$Q_n = Q_n(\mathbf{P}) = \bigoplus_{i_1+\cdots+i_m=n} P_{i_1}\widehat{\otimes}P_{i_2}\widehat{\otimes}\cdots\widehat{\otimes}P_{i_m} \ ,$$

$$\gamma(v_1\widehat{\otimes}\cdots\widehat{\otimes}v_m) = \partial(v_1)\cdots\partial(v_m) \ , \tag{8}$$

$$\gamma_n(v_1\widehat{\otimes}\cdots\widehat{\otimes}v_m) = \sum_{k=1}^{m}(-1)^{d(v_1)+\cdots+d(v_{k-1})}\partial_{1k}(v_1)\widehat{\otimes}\cdots\widehat{\otimes}\partial_{mk}(v_m) \ , \tag{9}$$

is an exact sequence of G-modules.

Proof: To prove the exactness of Q_*, it suffices to consider P_* and Q_* as sequences of $\mathbb{F}_p$-modules, forgetting the respective group actions. It is easy to see, by induction on m, that Q_* is precisely the m-fold tensor product $P_*\widehat{\otimes}P_*\widehat{\otimes}\cdots\widehat{\otimes}P_*$ of m (equal) sequences (of course, here we identify $\mathbb{F}_p\widehat{\otimes}\cdots\widehat{\otimes}\mathbb{F}_p$ with $\mathbb{F}_p$ by $v_1\widehat{\otimes}\cdots\widehat{\otimes}v_m \mapsto v_1\cdots v_m$). Thus Q_* is exact by Lemma 4.3.

It remains to be shown that γ_n are G-homomorphisms. Let $\tau \in G$. By (9) and by (4)

$$\tau\big(\gamma_n(v_1\widehat{\otimes}\cdots\widehat{\otimes}v_m)\big) = \sum_{k=1}^{m}(-1)^{\sum_{i<k} d(v_i)}(-1)^{c_k} w_{1k}\widehat{\otimes}\cdots\widehat{\otimes}w_{mk} \ ,$$

where $w_{ik} = h_i(\tau)\partial_{i\tau,k}(v_{i\tau})$ and

$$c_k = \sum_{\substack{i<j \\ i\tau^{-1}>j\tau^{-1}}} d\big(\partial_{ik}(v_i)\big)d\big(\partial_{jk}(v_j)\big).$$

Now

$$w_{ik} = \partial_{i\tau,k}\big(h_i(\tau)v_{i\tau}\big) = \partial_{i\tau,k}(v_i') = \partial_{i,k\tau^{-1}}(v_i') \ ,$$

in the notation of (4'). By (6) we have

$$d\big(\partial_{ik}(v_i)\big) = d(v_i) - \delta_{ik} \ ,$$

where $\delta_{ik} = 1$ if $i = k$, and $\delta_{ik} = 0$ if $i \neq k$. Therefore

$$\begin{aligned} c_k &= \sum_{\substack{i<j \\ i\tau^{-1} > j\tau^{-1}}} \big(d(v_i) - \delta_{ik}\big)\big(d(v_j) - \delta_{jk}\big) \\ &= \sum_{\substack{i<j \\ i\tau^{-1} > j\tau^{-1}}} d(v_i)d(v_j) - \sum_{\substack{k<j \\ k\tau^{-1} > j\tau^{-1}}} d(v_j) - \sum_{\substack{i<k \\ i\tau^{-1} > k\tau^{-1}}} d(v_i) \\ &= a - \sum_{\substack{k<i \\ k\tau^{-1} > i\tau^{-1}}} d(v_i) - \sum_{\substack{i<k \\ i\tau^{-1} > k\tau^{-1}}} d(v_i) \ , \end{aligned}$$

and hence

$$\begin{aligned} & c_k + \sum_{i<k} d(v_i) \\ &= a - \sum_{\substack{k<i \\ k\tau^{-1} > i\tau^{-1}}} d(v_i) - \sum_{\substack{i<k \\ i\tau^{-1} > k\tau^{-1}}} d(v_i) + \sum_{\substack{i<k \\ i\tau^{-1} < k\tau^{-1}}} d(v_i) + \sum_{\substack{i<k \\ i\tau^{-1} > k\tau^{-1}}} d(v_i) \\ &= a - \sum_{\substack{k<i \\ k\tau^{-1} > i\tau^{-1}}} d(v_i) + \sum_{\substack{i<k \\ i\tau^{-1} < k\tau^{-1}}} d(v_i) = a + \sum_{i\tau^{-1} < k\tau^{-1}} d(v_i) \\ &= a + \sum_{i<k\tau^{-1}} d(v_{i\tau}) = a + \sum_{i<k\tau^{-1}} d(v_i') \ , \end{aligned}$$

by (5). Therefore

$$\begin{aligned} & \tau\big(\gamma_n(v_1 \widehat{\otimes} \cdots \widehat{\otimes} v_m)\big) = \sum_{k=1}^{m} (-1)^{a + \sum_{i<k\tau^{-1}} d(v_i')} \partial_{1,k\tau^{-1}}(v_1') \widehat{\otimes} \cdots \widehat{\otimes} \partial_{m,k\tau^{-1}}(v_m') \\ &= \sum_{k=1}^{m} (-1)^{a + \sum_{i<k} d(v_i')} \partial_{1,k}(v_1') \widehat{\otimes} \cdots \widehat{\otimes} \partial_{m,k}(v_m') = \gamma_n\big((-1)^a v_1' \widehat{\otimes} \cdots \widehat{\otimes} v_m'\big) \\ &= \gamma_n\big(\tau(v_1 \widehat{\otimes} \cdots \widehat{\otimes} v_m)\big) \ . \quad \blacksquare \end{aligned}$$

We are now in position to prove Serre's Theorem. As mentioned in the Introduction, it follows from Theorem A$'$.

Proof of Theorem A$'$: By Corollary 3.7 there is a projective resolution of finite length

$$P_* : \qquad \cdots \to P_n \longrightarrow P_{n-1} \longrightarrow \cdots \longrightarrow P_0 \longrightarrow \mathbb{F}_p \to 0$$

in the category of H-modules. Let $Q_n = Q_n(\mathbf{P})$, for $n \geq 0$. The exact sequence of Lemma 5.5

$$Q_* : \qquad \cdots \to Q_n \longrightarrow Q_{n-1} \longrightarrow \cdots \longrightarrow Q_0 \longrightarrow \mathbb{F}_p \to 0$$

is a projective resolution of $\mathbb{F}_p$ in the category of G-modules, by Corollary 5.4. Moreover, it is clearly of finite length. Thus $\mathrm{cd}_p G < \infty$ by Corollary 3.7. ∎

References

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

[2] M. D. Fried and M. Jarden, *Field Arithmetic,* Ergebnisse der Mathematik III **11**, Springer Verlag, Heidelberg, 1986.

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

[4] D. Haran, A. Lubotzky, *Embedding covers and the theory of Frobenius fields*, Israel Journal of Mathematics **41** (1982), 181-202.

[5] S. Maclane, *Homology*, 3rd corrected edition, Springer Verlag 1975.

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

[7] L. Ribes, *Introduction to profinite groups and Galois cohomology*, Queen's Papers in Pure Mathematics **24**, Kingston 1970.

[8] J.-P. Serre, *Cohomologie galoisienne*, 4th edition, LNM 5, Springer Verlag 1986.

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

[10] R.G. Swan, *Groups of cohomological dimension one*, Journal of Algebra **12** (1969), 585-601.

School of Mathematical Sciences
Raymond and Beverly Sackler
Faculty of Exact Sciences
Tel Aviv University
TEL AVIV 69978
Israel