Some simple biset functors

Serge Bouc

Abstract: Let p be a prime number, let H be a finite p-group, and let $\mathbb{F}$ be a field of characteristic 0, considered as a trivial $\mathbb{F}\mathrm{Out}(H)$-module. The main result of this paper gives the dimension of the evaluation $S_{H,\mathbb{F}}(G)$ of the simple biset functor $S_{H,\mathbb{F}}$ at an arbitrary finite group G. A closely related result is proved in the last section: for each prime number p, a Green biset functor E_p is introduced, as a specific quotient of the Burnside functor, and it is shown that the evaluation $E_p(G)$ is a free abelian group of rank equal to the number of conjugacy classes of p-elementary subgroups of G.

AMS subject classification: 18B99, 19A22, 20J15

Keywords: simple biset functors, Green biset functor, p-elementary

1. Introduction

Let R be a commutative ring. The *biset category* $R\mathcal{C}$ over R has finite groups as objects, with morphisms $\mathrm{Hom}_{R\mathcal{C}}(G,H) = R \otimes_{\mathbb{Z}} B(H,G)$, where $B(H,G)$ is the Burnside group of (H,G)-bisets. The composition of morphisms is induced by the usual tensor product of bisets. A *biset functor* over R is an R-linear functor from $R\mathcal{C}$ to the category R-Mod of R-modules. Biset functors over R form an abelian category, where morphisms are natural transformations of functors. They have proved a useful tool in various aspects of the representation theory of finite groups (see [12], [7], [8], [9]), and they are still the object of active research ([15], [1], [10], [16], [13], [14], [5], [4], [2], ...).

The simple biset functors over R are parametrized ([6], Proposition 2) by equivalence classes of pairs (H,W), where H is a finite group, and W is a simple $R\mathrm{Out}(H)$-module - the simple functor parametrized by (H,W) being denoted $S_{H,W}$. However for a finite group G, the computation of the evaluation $S_{H,W}(G)$ is generally quite hard: in Theorem 4.3.20 of [9], this evaluation is shown to be equal to the image of a complicated linear map. Assuming that R is a field - which is always possible when dealing with simple functors - the dimension of $S_{H,W}(G)$ is given by Theorem 7.1 of [11], as the rank of a yet complicated bilinear form with values in R.

Let $\mathbb{F}$ be a field of characteristic 0, let p be a prime number, and H be a finite p-group. The present paper is mainly devoted to the computation of the dimension of the evaluation $S_{H,\mathbb{F}}(G)$, where G is an arbitrary finite group, and $\mathbb{F}$ is the trivial $\mathbb{F}\mathrm{Out}(H)$-module. The result is as follows:

Theorem: *Let $\mathbb{F}$ be a field of characteristic 0, let p be a prime number, and H be a finite p-group. Let moreover G be a finite group.*

1. *If $H = \mathbf{1}$, the dimension of $S_{H,\mathbb{F}}(G)$ is equal to the number of conjugacy classes of cyclic subgroups of G.*
2. *If $H \cong C_p \times C_p$, the dimension of $S_{H,\mathbb{F}}(G)$ is equal to the number of conjugacy classes of non-cyclic p-elementary subgroups of G.*
3. *If H is any other finite p-group, the dimension of $S_{H,\mathbb{F}}(G)$ is equal to the number of conjugacy classes of sections (T, S) of G such that $T/S \cong H$ and T is p-elementary.*

In the last section of this paper, for each prime number p, we introduce a Green biset functor E_p, closely related to the two first assertions of the above theorem. Green biset functors have been defined in [9], Section 8.5. They are ring objects in the category of biset functors. For a finite group G, we denote by $F_p(G)$ the set of elements of the Burnside group $B(G)$ which vanish when restricted to all p-elementary subgroups of G, and we show that this actually defines a biset subfunctor F_p of B. The functor E_p is defined as the quotient B/F_p, and it then inherits from B a Green biset functor structure (over $\mathbb{Z}$). We show moreover that its evaluation $E_p(G)$ at a finite group G is a free abelian group of rank equal to the number of conjugacy classes of p-elementary subgroups of G. We also show that the biset functor $\mathbb{F}E_p = \mathbb{F} \otimes_{\mathbb{Z}} E_p$ fits in a non split short exact sequence

$$0 \to S_{(C_p)^2,\mathbb{F}} \to \mathbb{F}E_p \to S_{\mathbf{1},\mathbb{F}} \to 0$$

of biset functors over $\mathbb{F}$. In the case $\mathbb{F} = \mathbb{Q}$, the restriction of this sequence to p-groups is the short exact sequence of Theorem D of [12], involving the Dade functor $\mathbb{Q}D$, the Burnside functor $\mathbb{Q}B$, and the functor of rational representation $\mathbb{Q}R_{\mathbb{Q}}$.

2. Preliminary results

The basic definitions and notation on (double) Burnside algebras and their idempotents from Chapters 2.4 and 2.5 of [9] will be freely used throughout this paper.

Recall (Sections 5.3 and 5.4 of [9]) that for a normal subgroup N of a finite group G, the rational number $m_{G,N}$ is defined by

$$m_{G,N} = \frac{1}{|G|} \sum_{\substack{X \leq G \\ XN = G}} |X|\mu(X, G) ,$$

where μ is the Möbius function of the poset of subgroups of G. The group G is called a *B-group* if $m_{G,N} = 0$ for any non-trivial normal subgroup N of G. Any finite group G has a largest quotient B-group $\beta(G)$, unique up to isomorphism. If $N \trianglelefteq G$, then $m_{G,N} = 0$ if and only if $\beta(G) \cong \beta(G/N)$.

2.1. Lemma: [M. Baumann [3] - See also [6], 8), p 713] *Let L be a finite group, let p be a prime, and let E be an elementary abelian p-group on which L acts irreducibly, faithfully, and such that $H^1(L, E) = \{0\}$. Then the group $G = E \rtimes L$ is a B-group.*

Proof : First as E is L-simple, it follows that E is a minimal normal subgroup of G. Let N be any normal subgroup of G. Then $N \cap E$ is equal to E or $\mathbf{1}$. So if $N \not\geq E$, then $N \cap E = \mathbf{1}$, and N centralizes E. But $C_G(E) = E \cdot C_L(E) = E$, since L acts faithfully on E. Thus $N \leq E$, hence $N = \mathbf{1}$.

It follows that E is the unique minimal normal subgroup of G. By Proposition 5.6.4 of [9], since E is abelian,

$$m_{G,E} = 1 - \frac{|K_G(E)|}{|E|} \ , \tag{2.2}$$

where $K_G(E)$ is the set of complements of E in G. The group E acts by conjugation on $K_G(E)$, and the normalizer in E of $K \in K_G(E)$ is equal to the group E^K of fixed points of K on E. Since E is K-simple, and K-faithful, this is equal to $\mathbf{1}$. Thus E acts freely on $K_G(E)$. Since $H^1(L, E) = \{0\}$, the set $K_G(E)$ is a single conjugacy class, i.e. a single E-orbit. Thus $|K_G(E)| = |E|$, and $m_{G,E} = 0$. It follows that G is a B-group. □

2.3. Recall that a finite group G is called *cyclic modulo a prime number p* if $G/O_p(G)$ is cyclic, and that G is called *p-elementary* if $G \cong P \times C$, where P is a p-group and C is a cyclic group.

2.4. Lemma: *Let p be a prime number, and G be a finite group.*

1. [M. Baumann [3]] *The group $\beta(G)$ is cyclic modulo p if and only if G is cyclic modulo p.*
2. *The group $\beta(G)$ is a p-group if and only if G is p-elementary.*

Proof : For Assertion 1, use the fact that by a theorem of Conlon, the subspace $NC_p(G)$ of $\mathbb{Q}B(G)$ generated by the idempotents e_H^G, where H is *not* cyclic modulo p, is equal to the kernel of the morphism $\mathbb{Q}B(G) \to \mathbb{Q}pp_k(G)$, where $\mathbb{Q}pp_k(G)$ is the ring of p-permutation kG-modules. In particular, the correspondence $G \mapsto NC_p(G)$ is a biset subfunctor of $\mathbb{Q}B$. It follows that there exists a family $\mathcal{B}$ of B-groups such that for any group G, the space $NC_p(G)$ is the $\mathbb{Q}$-vector subspace of $\mathbb{Q}B(G)$ generated by the idempotents e_H^G, where $\beta(H) \in \mathcal{B}$. The family $\mathcal{B}$ consists of those B-groups H for which $e_H^H \in NC_p(H)$, i.e. the B-groups which are not cyclic modulo p. Now for any group G, and any subgroup H of G, the idempotent e_H^G is in $NC_p(G)$ if and only if $\beta(H) \in \mathcal{B}$, on the one hand, but also if and only if H is not cyclic modulo p. Hence $\beta(H)$ is not cyclic modulo p if and only if H is not cyclic modulo p. This proves Assertion 1.

For Assertion 2, clearly, if G-is p-elementary, one can assume $G \cong P \times C$, where P is a p-group, and C is a cyclic p'-group. By Proposition 5.6.6 of [9], this implies $\beta(G) \cong \beta(P) \times \beta(C) \cong \beta(P)$, since $\beta(C) = \mathbf{1}$. Hence $\beta(G)$ is a p-group.

Conversely, suppose that $\beta(G)$ is a p-group. In particular, it is cyclic modulo p, hence G is cyclic modulo p, by Assertion 1. The Frattini subgroup $\Phi(P)$ of P is a normal subgroup of G, and $G/\Phi(P) \cong \overline{P} \rtimes C$, where $\overline{P}$ is the elementary abelian group $P/\Phi(P)$. Suppose that the $\mathbb{F}_pC$-module $\overline{P}$ admits a simple quotient E with non-trivial C-action (that is, not isomorphic to $\mathbb{F}_p$). Then the action of C on E has a kernel $D < C$, and the group $E \rtimes (C/D)$ is a quotient of $\overline{P} \rtimes C$, hence a quotient of G. But $E \rtimes (C/D)$ is a B-group by Lemma 2.1: Indeed E is (C/D)-simple and faithful by construction, and $H^1(C/D, E) = \{0\}$, since C/D is a p'-group.

Now $E \rtimes (C/D)$ is a B-group, which is not a p-group, since $D \neq C$, and it is a quotient of G, hence of $\beta(G)$, which is a p-group. This is a contradiction.

Hence C acts trivially on $\overline{P}$. But for any p-group P, the kernel of the morphism $\mathrm{Aut}(P) \to \mathrm{Aut}\big(P/\Phi(P)\big)$ is a p-group. As C is a p'-group, and acts trivially on $\overline{P}$, it acts trivially on P. Thus $G \cong P \times C$, as was to be shown. □

2.5. Lemma: *Let p be a prime number, and P be a finite p-group.*

1. *Let Q be a normal subgroup of P. Then $Q \cap \Phi(P) = \mathbf{1}$ if and only if Q is elementary abelian and central in P, and admits a complement in P.*

2. *Let Q and R be normal subgroups of P, such that $|Q| = |R|$. Then $Q \cap \Phi(P) = \mathbf{1} = R \cap \Phi(P)$ if and only if Q and R are elementary abelian and central in P, and admit a common complement in P.*

   In this case, set $H = P/R \cong P/Q$, and denote by γ the rank of the group $H/\Phi(H)$. If Q and R have rank m, and if $Q \cap R\Phi(P)$ has rank $m - s$, the number of common complements of Q and R in P is equal *to*

$$(p^s-1)(p^{s-1}-1)\cdots(p-1)p^{\binom{s}{2}+s(m-s)+m(\gamma-s)}\ .$$

Proof : For Assertion 1, if Q is elementary abelian and central in P, and admits a complement L, then $P=Q\times L$. Thus $\Phi(P)=\mathbf{1}\times\Phi(L)$, hence $Q\cap\Phi(P)=\mathbf{1}$. Conversely, if $Q\cap\Phi(P)=\mathbf{1}$, then Q maps injectively into $P/\Phi(P)$, so Q is elementary abelian. Let $L\geq\Phi(P)$ be a subgroup of P such that $L/\Phi(P)$ is a complement of $Q\Phi(P)/\Phi(P)$ in the $\mathbb{F}_p$-vector space $P/\Phi(P)$. Then $Q\Phi(P)L=P$, thus $QL=P$, and $Q\Phi(P)\cap L=\Phi(P)$, i.e. $Q\cap L\leq Q\cap\Phi(P)=\mathbf{1}$. Since $L\geq\Phi(P)$, it follows that $L\trianglelefteq P$, thus $[L,Q]\leq L\cap Q=\mathbf{1}$, and Q is central in P.

For Assertion 2, let Q and R be normal subgroups of P with $|Q|=|R|$. If Q and R are elementary abelian central subgroups of P with a common complement in P, then $Q\cap\Phi(P)=R\cap\Phi(P)=\mathbf{1}$ by Assertion 1. Conversely, if $Q\cap\Phi(P)=\mathbf{1}$ and $R\cap\Phi(P)=\mathbf{1}$, then Q and R are elementary abelian and central in P by Assertion 1. If L is a complement of Q in P, then $P=Q\times L$ for Q is central in P, thus $L\trianglelefteq P$, and $P/L\cong Q$ is elementary abelian. Thus $L\geq\Phi(P)$, and $L/\Phi(P)$ is a complement of $Q\Phi(P)/\Phi(P)$ in $P/\Phi(P)$. Conversely if $L/\Phi(P)$ is a complement of $Q\Phi(P)/\Phi(P)$ in $P/\Phi(P)$, then L is a complement of Q in P, by the argument used in the proof of Assertion 1.

So finding a common complement to Q and R in P amounts to finding a common complement of $\widetilde{Q}=Q\Phi(P)/\Phi(P)$ and $\widetilde{R}=R\Phi(P)/\Phi(P)$ in $\widetilde{P}=P/\Phi(P)$. Moreover $|\widetilde{Q}|=|Q|=|R|=|\widetilde{R}|$. The $\mathbb{F}_p$-vector space $\widetilde{P}$ can be split as $\widetilde{P}=I\oplus E\oplus F\oplus V$, where $I=\widetilde{Q}\cap\widetilde{R}$, where E is a complement of I in $\widetilde{Q}$ and F is a complement of I in $\widetilde{R}$, and V is a complement of $\widetilde{Q}+\widetilde{R}$ in $\widetilde{P}$. Then $L=F\oplus V$ is a complement of $\widetilde{Q}$ in $\widetilde{P}$, and all the other complements of $\widetilde{Q}$ are of the form $\{\big(\varphi(x),x\big)\mid x\in L\}$, where $\varphi:L\to\widetilde{Q}$ is a group homomorphism. In other words, any complement L' of $\widetilde{Q}$ is of the form

$$L'=\{\big(a(f)+b(v),c(f)+d(v),f,v\big)\mid f\in F,\,v\in V\}\ ,$$

where $a:F\to I$, $b:V\to I$, $c:F\to E$ and $d:V\to E$ are group homomorphisms. The group L' is a complement of $\widetilde{R}$ if and only if its intersection with $\widetilde{R}$ is trivial, or equivalently if c is injective, hence an isomorphism, since $|E|=|F|$.

It follows that the number of common complements of $\widetilde{Q}$ and $\widetilde{R}$ in $\widetilde{P}$ is equal to the number of 4-tuples (a,b,c,d), where c is an isomorphism. Hence

$$\begin{aligned}|K_P(Q)\cap K_P(R)| &= |\mathrm{Aut}(E)||\mathrm{Hom}(F,I)||\mathrm{Hom}(V,I)||\mathrm{Hom}(V,E)|\\ &= |\mathrm{Aut}(E)||\mathrm{Hom}(F,I)||\mathrm{Hom}(V,\widetilde{Q})|\ .\end{aligned}$$

Moreover

$$I = \big(Q\Phi(P) \cap R\Phi(P)\big)/\Phi(P) = \big(Q \cap R\Phi(P)\big)\Phi(P)/\Phi(P) \cong Q \cap R\Phi(P)$$

has rank $m - s$, and $F \cong E \cong \widetilde{Q}/I$ has rank s. Finally

$$V \cong \widetilde{P}/(\widetilde{Q}\widetilde{R}) \cong \big(P/R\Phi(P)\big)/\big(QR\Phi(P)/R\Phi(P)\big)$$

has rank $\gamma - s$, since $P/R\Phi(P) \cong H/\Phi(H)$, as $\Phi(P/R) = R\Phi(P)/R$, and since $QR\Phi(P)/R\Phi(P) \cong Q/\big(Q \cap R\Phi(P)\big)$. This completes the proof. □

2.6. Corollary: *Let P be a finite p-group, and M be a normal subgroup of P. Then*

$$P/\big(M \cap \Phi(P)\big) \cong E \times (P/M) \ ,$$

where $E = M/\big(M \cap \Phi(P)\big)$ is elementary abelian.

Proof : The normal subgroup $\overline{M} = M/\big(M \cap \Phi(P)\big)$ of $\overline{P} = P/\big(M \cap \Phi(P)\big)$ intersects the Frattini subgroup $\Phi(\overline{P}) = \Phi(P)/\big(M \cap \Phi(P)\big)$ trivially, hence there exists a subgroup L of $\overline{P}$ such that $\overline{P} = \overline{M} \times L$. Moreover $L \cong \overline{P}/\overline{M} \cong P/M$. □

3. Simple biset functors and bilinear forms

Let $\mathbb{F}$ be any field. Recall (see [11]) that, given a finite group H, we defined, for any finite group G

$$\mathbb{F}\overline{B}(G,H) = \mathbb{F}B(G,H)/\sum_{|K|<|H|} \mathbb{F}B(G,K) \circ \mathbb{F}B(K,H) \ ,$$

and that the correspondence $G \mapsto \mathbb{F}\overline{B}(G,H)$ is a quotient biset functor of the Yoneda functor $G \mapsto \mathbb{F}B(G,H)$ at the group H.

When V is a $\mathbb{F}\mathrm{Out}(H)$-module, we defined an $\mathbb{F}$-valued bilinear form $\langle\ ,\ \rangle_{V,G}$ on $\mathbb{F}\overline{B}(G,H)$ by

$$\forall \alpha, \beta \in \mathbb{F}\overline{B}(G,H),\ \langle \alpha, \beta \rangle_{V,G} = \chi_V\big(\pi_H(\hat{\alpha}^{op} \circ \hat{\beta})\big) \ ,$$

where $\hat{\alpha}, \hat{\beta}$ are elements of $\mathbb{F}B(G,H)$ lifting $\alpha, \beta \in \mathbb{F}\overline{B}(G,H)$, respectively, where $\pi_H : \mathbb{F}B(H,H) \to \mathbb{F}\overline{B}(H,H) \cong \mathbb{F}\mathrm{Out}(H)$ is the projection map, and χ_V is the character of V, i.e. the trace function $\mathrm{End}_{\mathbb{F}}(V) \to \mathbb{F}$. The main property of these constructions is that

$$\mathbb{F}\overline{B}(G,H)/\mathrm{Rad}\langle\ ,\ \rangle_{V,G} \cong S_{H,V}(G)^{\dim_{\mathbb{F}} V} \ .$$

Moreover, if L is a finite group, then for any $\gamma \in B(L,G)$, any $\alpha \in \overline{B}(G,H)$, and any $\beta \in \overline{B}(L,H)$,

$$\langle \gamma(\alpha), \beta \rangle_{V,L} = \langle \alpha, \gamma^{op}(\beta) \rangle_{V,G} \; . \tag{3.1}$$

3.2. Suppose from now on that $\mathbb{F}$ is a field of characteristic 0. Observe that $\tilde{e}_K^G = (\tilde{e}_K^G)^{op}$ for any subgroup K of a finite group G. By (3.1), this implies that the decomposition

$$\mathbb{F}\overline{B}(G,H) = \bigoplus_{K \in [s_G]} \tilde{e}_K^G \mathbb{F}\overline{B}(G,H) \; ,$$

where $[s_G]$ is a set of representatives of conjugacy classes of subgroups of G, is an orthogonal decomposition with respect to the form $\langle \; , \; \rangle_{V,G}$. Moreover

$$\tilde{e}_G^G S_{H,V}(G)^{\dim_{\mathbb{F}} V} \cong \tilde{e}_G^G \mathbb{F}\overline{B}(G,H)/\mathrm{Rad}\langle \; , \; \rangle_{V,G} \; ,$$

and the isomorphism

$$\mathbb{F}\overline{B}(G,H) \cong \bigoplus_{K \in [s_G]} \big(\tilde{e}_K^K \mathbb{F}\overline{B}(K,H)\big)^{N_G(K)}$$

given by Proposition 6.5.5 of [9] induces an isomorphism

$$S_{H,V}(G)^{\dim_{\mathbb{F}} V} \cong \bigoplus_{K \in [s_G]} \big(\tilde{e}_K^K \mathbb{F}\overline{B}(K,H)/\mathrm{Rad}\langle \; , \; \rangle_{V,K}\big)^{N_G(K)} \; . \tag{3.3}$$

Now $\overline{B}(K,H)$ is generated by the images of the elements $(K \times H)/L$, where L is a subgroup of $K \times H$. If this image is non-zero, then L is of the form $L = \{\big(x, s(x)\big) \mid x \in X\}$, where X is a subgroup of K and $s : X \twoheadrightarrow H$ is a surjective group homomorphism.

The (K,G)-biset $U = (K \times H)/L$ factors as $U = \mathrm{Ind}_X^K \circ V$, for a suitable (X,H)-biset V ([9], Lemma 2.3.26), and by [9], Corollary 2.5.12

$$\tilde{e}_K^K \circ \mathrm{Ind}_X^K = \mathrm{Ind}_X^K \circ \widetilde{\mathrm{Res}_X^K e_K^K} \; .$$

Now $\mathrm{Res}_X^K e_K^K = 0$ if X is a proper subgroup of K. It follows that $\tilde{e}_K^K \mathbb{F}\overline{B}(K,H)$ is generated by the images $\bar{u}_s$ of the elements

$$u_s = \tilde{e}_K^K \times_K (K \times H)/\Delta_s^\diamond(K) \; ,$$

where $\Delta_s^\diamond(K) = \{\big(x, s(x)\big) \mid x \in K\}$, for a surjective group homomorphism $s : K \twoheadrightarrow H$.

Let $\varpi_H : \mathrm{Aut}(H) \to \mathrm{Out}(H)$ denote the projection map. Then:

3.4. Proposition: *Let $s, t : K \twoheadrightarrow H$ be two surjective group homomorphisms. Let $M = \mathrm{Ker}\, s$, and $N = \mathrm{Ker}\, t$. Then*

$$\begin{aligned}\langle \bar{u}_s, \bar{u}_t\rangle_{V,K} &= m_{K,M\cap N}\, \frac{\mu_{\trianglelefteq K}(M\cap N, M)}{|M:M\cap N|}\, \chi_V\Big(\sum_{Y\in\overline{\mathcal{K}}(K,M,N)} \varpi_H([s,Y,t])\Big)\\ &= m_{K,M\cap N}\, \frac{\mu_{\trianglelefteq K}(M\cap N, M)}{|M:M\cap N|}\, \chi_V\Big(\sum_{\substack{\theta\in\mathrm{Aut}(H)\\ \Delta_\theta(H)\leq (s\times t)(K)}} \varpi_H(\theta)\Big)\ ,\end{aligned}$$

where $\mu_{\trianglelefteq K}$ is the Mbius function of the poset of normal subgroups of K, and

$$\overline{\mathcal{K}}(K, M, N) = \{Y \leq K \mid YN = YM = K,\ Y\cap N = Y\cap M = M\cap N\}$$

is the set of subgroups Y of K, containing $M\cap N$, such that $Y/(M\cap N)$ is a common complement of $M/(M\cap N)$ and $N/(M\cap N)$ in $K/(M\cap N)$. Moreover for $Y \in \overline{\mathcal{K}}(K, M, N)$, the symbol $[s, Y, t]$ denotes the automorphism of H defined by $[s, Y, t]\big(t(y)\big) = s(y)$, $\forall y \in Y$.

Proof : By definition, and since $\tilde{e}_K^K$ is an idempotent

$$\begin{aligned}\langle \bar{u}_s, \bar{u}_t\rangle_{V,K} &= \chi_V\big(\pi_H(u_s^{op}\circ u_t)\big)\\ &= \chi_V\Big(\pi_H\big((H\times K)/\Delta_s(K)\times_K \tilde{e}_K^K \times_K (K\times H)/\Delta_t^\diamond(K)\big)\Big)\ ,\end{aligned}$$

where $\Delta_s(K) = \{\big(s(x), x\big) \mid x \in K\}$. Set

$$a_{s,t} = (H\times K)/\Delta_s(K)\times_K \tilde{e}_K^K \times_K (K\times H)/\Delta_t^\diamond(K)\ .$$

Then

$$a_{s,t} = \frac{1}{|K|}\sum_{L\leq K} |L|\mu(L, K)(H\times H)/\Delta_{s,t}(L)\ ,$$

where $\Delta_{s,t}(L) = \{\big(s(l), t(l)\big) \mid l \in L\}$.

This subgroup of $H\times H$ is equal to $\Delta_\theta(H)$, for some automorphism θ of H, if and only if

$$\textbf{(3.5)}\qquad L\cap M = L\cap N \ \text{ and }\ LM = K = LN\ ,$$

where $M = \mathrm{Ker}\, s$ and $N = \mathrm{Ker}\, t$. In this case the automorphism θ is defined by $\theta\big(t(l)\big) = s(l)$, for any $l \in L$. The two conditions 3.5 and the automorphism θ remain unchanged when L is replaced by $L(M\cap N)$. Moreover the conditions 3.5 are equivalent to saying that the group $Y = L(M\cap N)$

is in $\overline{\mathcal{K}}(K,M,N)$, and in this case $\theta=[s,Y,t]$. Conversely, fix some $Y\in\overline{\mathcal{K}}(K,M,N)$, and consider all the subgroups L of K such that $L(M\cap N)=Y$. Recall that

$$\sum_{\substack{L\leq Y\\ L(M\cap N)=Y}}|L|\mu(L,K)=m_{K,M\cap N}|Y|\mu(Y,K)\ .$$

This gives:

$$\pi_H(a_{s,t})=m_{K,M\cap N}\sum_{Y\in\overline{\mathcal{K}}(K,M,N)}\frac{|Y|}{|K|}\mu(Y,K)\varpi([s,Y,t])\ .$$

Now if $Y/(M\cap N)$ is a complement of $M/(M\cap N)$ in $K/(M\cap N)$, and if $K/M\cong H$, it follows that $|Y|=|M\cap N||H|$. Moreover the poset $]Y,K[$ is isomorphic to the poset $]M\cap N,M[^Y$. But since M and N are normal subgroups of K, the commutator group $[M,N]$ is contained in $M\cap N$. It follows that $]M\cap N,M[^Y=]M\cap N,M[^{YN}=]M\cap N,M[^K$, and that $\mu(Y,K)=\mu_{\trianglelefteq K}(M\cap N,M)$. This completes the proof of the first equality of the proposition. The second one follows from the observation that the correspondences

$$Y\mapsto[s,Y,t]\ \text{ and }\ \theta\mapsto\{k\in K\mid\theta\big(t(k)\big)=s(k)\}$$

are mutual inverse bijections between $\overline{\mathcal{K}}(K,M,N)$ and the set of automorphisms θ of H such that $\Delta_\theta(H)\leq(s\times t)(K)$ (see Section 8.3 of [6]). □

3.6. Corollary:

1. *If $\tilde{e}_K^K S_{H,V}(K)\neq\{0\}$, the group $\beta(K)$ is isomorphic to $\beta(L)$, where L is a subgroup of $H\times H$ with the following properties:*
   - *(a) $p_1(L)=p_2(L)=H$.*
   - *(b) $k_1(L)$ and $k_2(L)$ are direct products of minimal normal subgroups of H.*
   - *(c) There exist an automorphism θ of H such that $\theta\big(k_2(L)\big)=k_1(L)$.*
2. *In particular, if H is a p-group for some prime p, then K is p-elementary. If $K=P\times C$, where P is a p-group and C is a cyclic p'-group, then*

   $$\tilde{e}_K^K S_{H,V}(K)\cong\tilde{e}_P^P S_{H,V}(P)\ ,$$

   and this isomorphism is compatible with the action of $\mathrm{Aut}(K)$.

Proof : Indeed, if $\tilde{e}_K^K S_{H,V}(K)\neq\{0\}$, then the bilinear form $\langle\ ,\ \rangle_{V,K}$ is not identically zero on $\tilde{e}_K^K\mathbb{F}\overline{B}(K,H)$. It follows that there exist surjective group homomorphisms $s,t:K\twoheadrightarrow H$ such that $\langle\bar{u}_s,\bar{u}_t\rangle_{V,K}\neq 0$.

Then $m_{K,M\cap N}\neq 0$, $\mu_{\trianglelefteq K}(M\cap N,M)\neq 0$, and $\overline{\mathcal{K}}(K,M,N)\neq\emptyset$, where $M=\mathrm{Ker}\,s$ and $N=\mathrm{Ker}\,t$. Hence $\beta(K)\cong\beta\big(K/(M\cap N)\big)$. Now $K/(M\cap N)$ is isomorphic to $L=(s\times t)(K)$, which is a subgroup of $H\times H$ such that $p_1(L)=p_2(L)=H$. Moreover $k_1(L)=s(\mathrm{Ker}\,t)\cong N/(M\cap N)$ and $k_2(L)=t(\mathrm{Ker}\,s)\cong M/(M\cap N)$. Then $\mu_{\trianglelefteq K}(M\cap N,M)=\mu_{\trianglelefteq H}\big(\mathbf{1},t(\mathrm{Ker}\,s)\big)$, and this is non zero if and only if the lattice $[\mathbf{1},t(\mathrm{Ker}\,s)]^H$ of normal subgroups of H contained in $t(\mathrm{Ker}\,s)$ is complemented, i.e. if $t(\mathrm{Ker}\,s)$ is a direct product of minimal normal subgroups of H. Finally, let $Y\in\overline{\mathcal{K}}(K,M,N)$ and $\theta=[s,Y,t]$. If $u\in k_2(L)=t(\mathrm{Ker}\,s)$, then there exist $v\in\mathrm{Ker}\,s$ and $y\in Y$ such that $u=t(v)=t(y)$. Then $v^{-1}y\in\mathrm{Ker}\,t$, and $\theta(u)=s(y)=s(v^{-1}y)\in s(\mathrm{Ker}\,t)=k_1(L)$. In other words $\theta\big(k_2(L)\big)=k_1(L)$, which completes the proof of Assertion 1.

The first part of Assertion 2 follows from Assertion 2 of Lemma 2.4. Now if H is a p-group, if $K=P\times C$, where P is a p-group and C is a p'-group, and if $s:K\twoheadrightarrow H$ is a surjective group homomorphism, then $C\leq\mathrm{Ker}\,s$. In other words, there is a surjective homomorphism $\bar{s}:P\twoheadrightarrow H$ such that $s=\bar{s}\circ\pi$, where $\pi:K\to P$ is the projection map. Moreover $\mathrm{Ker}\,s=\mathrm{Ker}\,\bar{s}\times C$.

So with the notation of Proposition 3.4, $M=\overline{M}\times C$, where $\overline{M}=\mathrm{Ker}\,\bar{s}$. Similarly $N=\overline{N}\times C$, where $N=\mathrm{Ker}\,\bar{t}$, and $\bar{t}:P\twoheadrightarrow H$ is such that $t=\bar{t}\circ\pi$. Clearly $|M:M\cap N|=|\overline{M}:\overline{M}\cap\overline{N}|$. Moreover, one checks easily that

$$m_{K,M\cap N}=m_{P\times C,(\overline{M}\cap\overline{N})\times C}=m_{P,\overline{M}\cap\overline{N}}m_{C,C}=m_{P,\overline{M}\cap\overline{N}}\frac{\phi(|C|)}{|C|}\ ,$$

since P and C have coprime orders, and C is cyclic.

Also

$$\mu_{\trianglelefteq K}(M\cap N,M)=\mu_{\trianglelefteq P}(\overline{M}\cap\overline{N},\overline{M})\ .$$

Finally, the maps $Q\mapsto Q\times\mathbf{1}$ and $Y\mapsto(Y\cap P)$ induce inverse bijections from $\overline{\mathcal{K}}(P,\overline{M},\overline{N})$ to $\overline{\mathcal{K}}(K,M,N)$, and for any $Y\in\overline{\mathcal{K}}(K,M,N)$,

$$[s,Y,t]=[\,\bar{s},Y\cap P,\bar{t}\,]\ .$$

It follows that the matrix of the form $\langle\ ,\ \rangle_{V,K}$ on $\tilde{e}_K^K\mathbb{F}\overline{B}(K,H)$ is equal to the matrix of the form $\langle\ ,\ \rangle_{V,P}$ on $\tilde{e}_P^P\mathbb{F}\overline{B}(P,H)$, multiplied by the non-zero scalar $\frac{\phi(|C|)}{|C|}$. Hence the two forms define isomorphic quadratic spaces. As all the above bijections are obviously compatible with the action of $\mathrm{Aut}(K)$ and the canonical group homomorphism $\mathrm{Aut}(K)\to\mathrm{Aut}(P)$, the induced isomorphism

$$\tilde{e}_K^K S_{H,V}(K)\cong\tilde{e}_P^P S_{H,V}(P)$$

is compatible with the action of $\mathrm{Aut}(K)$. $\square$

3.7. Notation: *Let H and P be finite p-groups.*

1. *Let $\mathcal{Q}_H(P)$ denote the $\mathbb{F}$-vector space with basis the set*

$$\Sigma_H(P) = \{s \mid s : P \twoheadrightarrow H\}$$

of surjective group homomorphisms from P to H, endowed with the $\mathbb{F}$-valued bilinear form $\langle\ ,\ \rangle_{V,P}$ defined as follows: For $s, t \in \Sigma_H(P)$, set $M = \mathrm{Ker}\, s$ and $N = \mathrm{Ker}\, t$. If $M \cap \Phi(P) \neq N \cap \Phi(P)$, set $\langle s, t\rangle_{V,P} = 0$. And if $M \cap \Phi(P) = N \cap \Phi(P)$, then the groups $M/(M \cap N)$ and $N/(M \cap N)$ are central elementary abelian subgroups of the same rank of $P/M \cap N$. In this case, set

$$\langle s, t\rangle_{V,P} = m_{P,M\cap N} \frac{\mu(M\cap N, M)}{|M:M\cap N|} \chi_V\Big(\sum_{Y \in \overline{\mathcal{K}}(P,M,N)} \varpi_H([s, Y, t])\Big) \ .$$

2. *Let $\mathcal{Q}_H^\sharp(P)$ be the subspace of $\mathcal{Q}_H(P)$ with basis the subset*

$$\Sigma_H^\sharp(P) = \{s \mid s : P \twoheadrightarrow H,\ \ \mathrm{Ker}\, s \cap \Phi(P) = \mathbf{1}\}$$

of $\Sigma_H(P)$.

3. *Set*

$$\mathcal{N}_H(P) = \{N \mid N \trianglelefteq P,\ \ N \cap \Phi(P) = \mathbf{1}\} \ .$$

4. *Denote by $\mathcal{E}_H(P)$ the set of normal subgroups R of P, contained in $\Phi(P)$, and such that $P/R \cong E \times H$, for some elementary abelian p-group E.*

3.8. Proposition: *Let H be a p-group, and K be a p-elementary group. Set $P = O_p(K)$. Then:*

1. *There is an isomorphism of $\mathbb{F}\mathrm{Aut}(K)$-modules*

$$\tilde{e}_K^K S_{H,V}(K) \cong \mathcal{Q}_H(P)/\mathrm{Rad}\langle\ ,\ \rangle_{V,P} \ .$$

2. *Let Γ be a finite group acting on the group K. Then Γ acts on the set $\mathcal{E}_H(P)$, and there is an isomorphism of $\mathbb{F}\Gamma$-modules*

$$\tilde{e}_K^K S_{H,V}(K) \cong \bigoplus_{R \in [\Gamma \backslash \mathcal{E}_H(P)]} \mathrm{Ind}_{\Gamma_R}^{\Gamma}\big(\mathcal{Q}_H^\sharp(P/R)/\mathrm{Rad}\langle\ ,\ \rangle_{V,P/R}\big) \ ,$$

where $[\Gamma\backslash\mathcal{E}_H(P)]$ is a set of representatives of Γ-orbits on $\mathcal{E}_H(P)$, and Γ_R denotes the stabilizer of R in Γ.

Proof : The map $s\in\Sigma_H(P)\mapsto \bar{u}_s\in\tilde{e}_P^P\mathbb{F}\overline{B}(P,H)$ induces a surjective linear map $\mathcal{Q}_H(P)\to\tilde{e}_P^P\mathbb{F}\overline{B}(P,H)$. Let $s,t\in\Sigma_H(P)$, and set $M=\mathrm{Ker}\, s$ and $N=\mathrm{Ker}\, t$. Then $|M|=|N|$. It follows from Lemma 2.5 that $\overline{\mathcal{K}}(P,M,N)\neq\emptyset$ if and only if $M/(M\cap N)$ and $N/(M\cap N)$ are central elementary abelian subgroups of $P/(M\cap N)$, which intersect trivially the Frattini subgroup of $P/(M\cap N)$. But

$$\Phi\big(P/(M\cap N)\big)=\Phi(P)(M\cap N)/(M\cap N)\ .$$

Hence $M/(M\cap N)\cap\Phi\big(P/(M\cap N)\big)=\big(M\cap\Phi(P)\big)(M\cap N)/(M\cap N)$. This group is trivial if and only if $M\cap\Phi(P)\leq M\cap N$, i.e. if $M\cap\Phi(P)\leq N\cap\Phi(P)$. Hence $\overline{\mathcal{K}}(P,M,N)\neq\emptyset$ if and only if $M\cap\Phi(P)=N\cap\Phi(P)$.

This holds in particular if $\langle\bar{u}_s,\bar{u}_t\rangle\neq 0$. In this case, by Proposition 3.4

$$\langle\bar{u}_s,\bar{u}_t\rangle_{V,P}=m_{P,M\cap N}\,\frac{\mu_{\trianglelefteq P}(M\cap N,M)}{|M:M\cap N|}\,\chi_V\Big(\sum_{Y\in\overline{\mathcal{K}}(P,M,N)}\varpi_H([s,Y,t])\Big)\ .$$

But $\mu_{\trianglelefteq P}(M\cap N,M)=\mu(M\cap N,M)$, since $P/(M\cap N)$ centralizes both $M/(M\cap N)$ and $N/(M\cap N)$. Hence

$$\langle\bar{u}_s,\bar{u}_t\rangle_{V,P}=\langle s,t\rangle_{V,P}$$

in this case, and Assertion 1 follows.

Since $\langle s,t\rangle_{V,P}=0$ if $M\cap\Phi(P)\neq N\cap\Phi(P)$, the quadratic space $\mathcal{Q}=\big(\mathcal{Q}_H(P),\langle\ |\ \rangle_{V,P}\big)$ splits as the orthogonal sum of the subspaces $\mathcal{Q}_R$ generated by the elements $s\in\Sigma_H(P)$ such that $\mathrm{Ker}\, s\cap\Phi(P)=R$. These subspaces are permuted by the action of $\mathrm{Aut}(K)$, and the space $\mathcal{Q}_R$ is invariant by $\mathrm{Aut}(K)_R$.

Let $\pi_R:P\to P/R$ be the canonical projection. The map

$$\theta_R:\bar{s}\in\Sigma_H^\sharp(P/R)\mapsto\bar{s}\circ\pi_R$$

is a bijection from $\Sigma_H^\sharp(P/R)$ to the set $\{s\in\Sigma_H(P)\mid\mathrm{Ker}\, s\cap\Phi(P)=R\}$, and the map $Y\mapsto Y/R$ is a bijection from $\overline{\mathcal{K}}(P,M,N)$ to $\overline{\mathcal{K}}(P/R,M/R,N/R)$, such that

$$[\bar{s},Y/R,\bar{t}\,]=[\theta_R(\bar{s}),Y,\theta_R(\bar{t}\,)]\ ,$$

for any $\bar{s},\bar{t}\in\Sigma_H^\sharp(P/R)$.

Moreover, if $M\cap\Phi(P)=N\cap\Phi(P)=R$, then

$$m_{P,M\cap N}=m_{P,R}m_{P/R,(M\cap N)/R}=m_{P/R,(M\cap N)/R}\ ,$$

as $R \leq \Phi(P)$. Also

$$M/(M \cap N) \cong (M/R)/\big((M/R) \cap (N/R)\big) \ .$$

It follows that

$$\forall \bar{s}, \bar{t} \in \Sigma_H^\sharp(P/R), \ \ \langle \theta_R(\bar{s}), \theta_R(\bar{t}\,)\rangle_{V,P} = \langle \bar{s}, \bar{t}\,\rangle_{V,P/R} \ .$$

Hence there is an isomorphism

$$\mathcal{Q}_R/\mathrm{Rad}\langle\ ,\ \rangle_{V,P} \cong \mathcal{Q}_H^\sharp(P/R)/\mathrm{Rad}\langle\ ,\ \rangle_{V,P/R} \ ,$$

of $\mathbb{F}\Gamma_R$-modules.

To complete the proof of Assertion 2, it remains to observe that if Q is a p-group, the set $\Sigma_H^\sharp(Q)$ is non-empty if and only if the group Q is isomorphic to $E \times H$, for some elementary abelian p-group E: Indeed, if $Q = E \times H$, where E is elementary abelian, then $\Phi(Q) = \mathbf{1} \times \Phi(H)$, and the projection map $s : Q \to H = Q/E$ is an element of $\Sigma_H^\sharp(Q)$. Conversely, if $s \in \Sigma_H^\sharp(Q)$, then $E = \mathrm{Ker}\, s$ is an elementary abelian central subgroup of Q, which admits a complement L in Q, by Lemma 2.5. Thus $Q = E \times L$, and $L \cong Q/E \cong H$. Hence $Q \cong E \times H$. □

3.9. Theorem: *Let G be a finite group, let H be a finite p-group, and let V be a simple $\mathbb{F}\mathrm{Out}(H)$-module. Then*

$$S_{H,V}(G)^{\dim_{\mathbb{F}} V} \cong \bigoplus_{(K,R)} \Big(\mathcal{Q}_H^\sharp(K_p/R)/\mathrm{Rad}\langle\ ,\ \rangle_{V,K_p/R}\Big)^{N_G(K,R)} \ .$$

where (K, R) runs through a set of G-conjugacy classes of pairs consisting of a p-elementary subgroup K of G, and a p-subgroup R in $\mathcal{E}_H(K_p)$, where $K_p = O_p(K)$, and $N_G(K, R) = N_G(K) \cap N_G(R)$.

Proof : This follows from Equation 3.3, Corollary 3.6 and Proposition 3.8. □

4. Proof of the theorem

This section is devoted to the proof of the following theorem, announced in the introduction:

4.1. Theorem: *Let $\mathbb{F}$ be a field of characteristic 0, let p be a prime number, and H be a finite p-group. Let moreover G be a finite group.*

1. If $H = \mathbf{1}$, the dimension of $S_{H,\mathbb{F}}(G)$ is equal to the number of conjugacy *classes of cyclic subgroups of G.*

2. *If $H \cong C_p \times C_p$, the dimension of $S_{H,\mathbb{F}}(G)$ is equal to the number of conjugacy classes of non-cyclic p-elementary subgroups of G.*

3. *If H is any other finite p-group, the dimension of $S_{H,\mathbb{F}}(G)$ is equal to the number of conjugacy classes of sections (T, S) of G such that $T/S \cong H$ and T is p-elementary.*

Proof : Step 1: Let K be a subgroup of G. Then $\tilde{e}_K^K S_{H,\mathbb{F}}(K) = \{0\}$, by Corollary 3.6, unless $K \cong P \times C$, where P is a p-group and C is a cyclic p'-group, and in this case $\tilde{e}_K^K S_{H,\mathbb{F}}(K) \cong \tilde{e}_P^P S_{H,\mathbb{F}}(P)$ as $\mathbb{F}\mathrm{Aut}(K)$-modules.

By Proposition 3.8, there is an isomorphism of $\mathbb{F}\mathrm{Aut}(P)$-modules

$$\tilde{e}_P^P S_{H,\mathbb{F}}(P) \cong \bigoplus_R \mathrm{Ind}_{\mathrm{Aut}(P)_R}^{\mathrm{Aut}(P)} \big(\mathcal{Q}_H^\sharp(P/R)/\mathrm{Rad}\langle\ ,\ \rangle_{\mathbb{F},P/R}\big) ,$$

where R runs through a set of representatives of $\mathrm{Aut}(P)$-orbits of normal subgroups of P contained in $\Phi(P)$, such that $P/R \cong E \times H$, for some elementary abelian p-group E. So the computation of $\tilde{e}_P^P S_{H,\mathbb{F}}(P)$ comes down to the computation of the $\mathbb{F}\mathrm{Aut}(Q)$-module

$$\mathcal{V}_H(Q) = \mathcal{Q}_H^\sharp(Q)/\mathrm{Rad}\langle\ ,\ \rangle_{\mathbb{F},Q} ,$$

for a p-group $Q = P/R$ of the form $E \times H$, where R is some normal subgroup of P contained in $\Phi(P)$. Recall that $\mathcal{Q}_H^\sharp(Q)$ is the $\mathbb{F}$-vector space with basis

$$\Sigma_H^\sharp(Q) = \{s \mid s : Q \twoheadrightarrow H,\ \ \mathrm{Ker}\, s \cap \Phi(Q) = \mathbf{1}\} ,$$

and that the bilinear form $\langle\ ,\ \rangle_{\mathbb{F},Q}$ is defined for $s, t \in \Sigma_H^\sharp(Q)$ by

$$\langle s, t\rangle_{\mathbb{F},Q} = m_{Q,M\cap N} \frac{\mu(M\cap N, M)}{|M : M\cap N|} |\overline{\mathcal{K}}(Q, M, N)| ,$$

where $M = \mathrm{Ker}\, s$ and $N = \mathrm{Ker}\, t$.

This shows that $\langle s, t\rangle_{\mathbb{F},Q}$ depends only on M and N. It follows that $\mathcal{Q}_H^\sharp(Q)/\mathrm{Rad}\langle\ ,\ \rangle_{\mathbb{F},Q}$ is also isomorphic to the quotient of the $\mathbb{F}$-vector space with basis the set $\mathcal{N}_H(Q) = \{N \trianglelefteq Q \mid P/N \cong H,\ \ N \cap \Phi(Q) = \mathbf{1}\}$ introduced in Notation 3.7, by the radical of the bilinear form $\langle\ ,\ \rangle_{\mathbb{F},Q}^\natural$ defined by

$$\langle M, N\rangle_{\mathbb{F},Q}^\natural = m_{Q,M\cap N} \frac{\mu(M\cap N, M)}{|M : M\cap N|} |\overline{\mathcal{K}}(Q, M, N)| ,$$

for $M, N \in \mathcal{N}_H(Q)$.

Step 2: Now Assertion 1 is well known (see e.g. Proposition 4.4.8 [9]), but it can also be recovered from the argument of Step 1: Indeed, if $H = \mathbf{1}$, there is a unique normal subgroup N of Q such that $Q/N \cong H$, namely Q itself. If moreover $N \cap \Phi(Q) = 1$, then $\Phi(Q) = \mathbf{1}$, and Q is elementary abelian. But as $Q = P/R$, for some $R \leq \Phi(P)$, it follows that $R = \Phi(P)$, and $Q = P/\Phi(P)$. Moreover $\mathcal{N}_H(Q) = \{Q\}$, and

$$\langle Q, Q\rangle^{\natural}_{\mathbb{F},Q} = m_{Q,Q} ,$$

which is equal to 0 if Q is non-cyclic, and to $1 - 1/p$ otherwise. Hence $\mathcal{V}_H(Q) = \{0\}$ if Q is non-cyclic, and $\mathcal{V}_H(Q)$ is one dimensional if $Q = P/\Phi(P)$ is cyclic, i.e. if P is cyclic. But $P = O_p(K)$ for some p-elementary subgroup K of G. Hence P is cyclic if and only if K itself is cyclic, and this leads to Assertion 1.

We can now assume that H is a non-trivial p-group, of order p^h, and make a series of observations:

- Let P be a p-group, and Q be a normal subgroup of P. Example 5.2.3 of [9] shows that $m_{P,Q} = m_{P,\Phi(P)Q}$. By Proposition 5.3.1 of [9], it follows that

  $$\textbf{(4.2)} \qquad m_{P,Q} = m_{P,\Phi(P)} m_{P/\Phi(P),Q\Phi(P)/\Phi(P)} = m_{E,F} ,$$

  where E is the elementary abelian p-group $P/\Phi(P)$, and F its subgroup $Q\Phi(P)/\Phi(P)$. If E has rank $n \geq 2$ and F has rank k, then

  $$\textbf{(4.3)} \qquad m_{E,F} = (1 - p^{n-2})(1 - p^{n-3}) \cdots (1 - p^{n-k-1}) ,$$

  (which is equal to 0 if $k \geq n-1$, and non-zero otherwise). This follows from an easy induction argument on k, using Proposition 5.3.1 of [9], and starting with the case $k = 1$, which is a special case of Equation 2.2.

  If E has rank 1 and $F = \mathbf{1}$, then $m_{E,F} = 1$. In this case $m_{E,E} = 1 - \frac{1}{p}$. This is the only case where $m_{E,F}$ is not an integer.

- Let $M, N \in \mathcal{N}_H(Q)$. Then in particular M and N have the same order. Recall that $m_{Q,M\cap N}$ is non-zero if and only if $\beta(Q) \cong \beta\big(Q/(M \cap N)\big)$. So either Q and $Q/(M \cap N)$ are both cyclic, or they are both non-cyclic. Equivalently, either Q is cyclic, or $Q/(M \cap N)$ is non-cyclic. If H is non-cyclic, then $Q/(M \cap N)$ is non-cyclic, as it maps surjectively on $Q/M \cong H$.

  So if $m_{Q,M\cap N} = 0$, then H is cyclic, Q is non-cyclic, and $Q/(M \cap N)$ is cyclic. But then $M/(M \cap N) = N/(M \cap N)$, since the cyclic group $Q/(M \cap N)$ admits a unique subgroup of a given order. Thus $M = N$. Conversely, if H is cyclic, if Q is non-cyclic, and if $M = N$, then $m_{Q,M\cap N} = 0$ since $Q/(M \cap N) \cong H$ is cyclic.

- If $M, N \in \mathcal{N}_H(Q)$, then the subgroups $\overline{M} = M/(M \cap N)$ and $\overline{N} = N/(M \cap N)$ are central elementary abelian subgroups of the same order of $\overline{Q} = Q/(M \cap N)$. If $\overline{M}$ has rank m, then

$$\mu(M \cap N, M) = (-1)^m p^{\binom{m}{2}} .$$

Now by Lemma 2.5, the product

$$\alpha_{M,N} = \mu(M \cap N, M)|\overline{K}(Q, M, N)| \tag{4.4}$$

is equal to

$$\begin{aligned}\alpha_{M,N} &= (-1)^m(p^s-1)(p^{s-1}-1)\cdots(p-1)p^{\binom{m}{2}+\binom{s}{2}+s(m-s)+m(\gamma-s)} \\ &= (-1)^{m+s}(1-p^s)(1-p^{s-1})\cdots(1-p)p^{\binom{m}{2}+\binom{s}{2}+s(m-s)+m(\gamma-s)} ,\end{aligned}$$

where γ is the rank of $H/\Phi(H)$, and s is the rank of $\overline{M}/\big(\overline{M}\cap\overline{N}\Phi(\overline{Q})\big) \cong M/\big(M \cap N\Phi(Q)\big)$.

Step 3: Finally $\langle M, N\rangle^\natural_{\mathbb{F},Q} = 0$ if and only if $m_{Q,M\cap N} = 0$, i.e. H is cyclic, $M = N$, and Q is not cyclic. In all other cases, the groups $\overline{M} = M/(M\cap N)$ and $\overline{N} = N/(M\cap N)$ are elementary abelian, and central in $\overline{Q} = Q/(M\cap N)$. Moreover $\overline{M} \cap \overline{N} = \mathbf{1}$. Let m be the rank of $\overline{M}$, let s denote the rank of $\overline{M}/\big(\overline{M} \cap \overline{N}\Phi(\overline{Q})\big)$, and let γ denote the rank of $H/\Phi(H)$. Then

$$\begin{aligned}\langle M, N\rangle^\natural_{\mathbb{F},Q} &= m_{Q,M\cap N}\frac{\alpha_{M,N}}{|M{:}M\cap N|} \\ &= m_{Q,M\cap N}\,\frac{\alpha_{M,N}}{|\overline{M}|} \\ &= (-1)^m m_{Q,M\cap N}(p^s-1)(p^{s-1}-1)\cdots(p-1)p^{\binom{m}{2}-m+\binom{s}{2}+s(m-s)+m(\gamma-s)} ,\end{aligned}$$

i.e. finally

$$\langle M, N\rangle^\natural_{\mathbb{F},Q} = (-1)^m m_{Q,M\cap N}(p^s-1)(p^{s-1}-1)\cdots(p-1)p^{\frac{1}{2}(m-s)(m+s+1)+m(\gamma-2)} . \tag{4.5}$$

Let n denote the rank of $Q/\Phi(Q)$. By Equation 4.3

$$m_{Q,M\cap N} = (1-p^{n-2})(1-p^{n-3})\cdots(1-p^{n-k-1}) ,$$

where k is the rank of $(M\cap N)\Phi(Q)/\Phi(Q) \cong M\cap N$. Since $Q/M\Phi(Q) \cong H/\Phi(H)$ has rank γ, it follows that $M\Phi(Q)/\Phi(Q) \cong M$ has rank $n-\gamma$. Since $M/(M\cap N)$ has rank m, it follows that $k = n-m-\gamma$. Thus

$$m_{Q,M\cap N} = (1-p^{n-2})(1-p^{n-3})\cdots(1-p^{m+\gamma-1}) .$$

It follows that

$$(\mathbf{4.6})\qquad \langle M,N\rangle_{\mathbb{F},Q}^{\natural}=A_{M,N}(-1)^{m+s}p^{\frac{1}{2}(m-s)(m+s+1)+m(\gamma-2)}\ ,$$

where

$$A_{M,N}=(1-p^{n-2})(1-p^{n-3})\cdots(1-p^{m+\gamma-1})(1-p^{s})(1-p^{s-1})\cdots(1-p)$$

is an integer congruent to 1 modulo p.

Step 4: Assume first that H is non-cyclic, i.e. that $\gamma\geq 2$. In this case $\langle M,N\rangle_{\mathbb{F},Q}^{\natural}$ is non-zero. If $M=N$, then $m=s=0$, and $\langle M,N\rangle_{\mathbb{F},P}^{\natural}=A_{M,M}$ is congruent to 1 modulo p. And if $M\neq N$, then $m\geq 1$. As $\gamma\geq 2$ and $m\geq s$, the exponent

$$\frac{1}{2}(m-s)(m+s+1)+m(\gamma-2)$$

of p in the right hand side of 4.6 is non-negative. It is equal to 0 if and only if $m=s$ and $\gamma=2$. In this case $\overline{M}\cap\overline{N}\Phi(\overline{Q})=\mathbf{1}$, so $\overline{M}$ maps into $\overline{Q}/\overline{N}\Phi(\overline{Q})\cong H/\Phi(H)$, which has rank $\gamma=2$. It follows that $m\leq 2$.

If $m=2$, then $\overline{M}\,\overline{N}\Phi(\overline{Q})=\overline{Q}$, thus $\overline{M}\,\overline{N}=\overline{Q}$, and $H\cong\overline{Q}/\overline{N}\cong\overline{M}$ (since $\overline{M}\cap\overline{N}=\mathbf{1}$), so H is elementary abelian of rank 2.

If $m=1$, then as $\overline{M}\cong C_p$ maps into $\overline{Q}/\overline{N}\Phi(\overline{Q})\cong C_p\times C_p$, the group $\overline{Q}/\big(\overline{M}\,\overline{N}\Phi(\overline{Q})\big)$ is cyclic, so $\overline{Q}/\overline{M}\,\overline{N}$ is cyclic. But $\overline{M}\,\overline{N}$ is a central subgroup of $\overline{Q}$. It follows that $\overline{Q}$ is abelian, so $H\cong\overline{Q}/\overline{M}$ is abelian. Hence $\overline{Q}/\overline{M}$ is non-cyclic, and it has a subgroup $\overline{M}\,\overline{N}/\overline{M}$ of order p such that the corresponding quotient $\overline{Q}/\overline{M}\,\overline{N}$ is cyclic. It follows that $\overline{Q}/\overline{M}\cong H\cong C_p\times C_{p^{h-1}}$, for some $h\geq 2$.

Step 5: Assume that H is neither cyclic nor isomorphic to $C_p\times C_{p^{h-1}}$, for some $h\geq 2$. Then the matrix of the bilinear form $\langle\ ,\ \rangle_{\mathbb{F},Q}^{\natural}$ is congruent to the identity matrix modulo p. In particular, it is non-singular, and the $\mathbb{F}\mathrm{Aut}(Q)$-module $\mathcal{V}_H(Q)=\mathcal{Q}_H^{\sharp}(Q)$ is isomorphic to the permutation module on the set $\mathcal{N}_H(Q)$.

It follows that the $\mathrm{Aut}(P)$-module $\tilde{e}_P^P S_{H,\mathbb{F}}(P)$ is isomorphic to the permutation module on the set of normal subgroups M of P such that $P/M\cong H$. Going back to Step 1 and to the p-elementary subgroup $K=P\times C$ of G, it follows that the space $\tilde{e}_K^K S_{H,\mathbb{F}}(K)^{N_G(K)}$ has a basis in one to one correspondence with the $N_G(K)$-orbits of normal subgroups M of K such that $K/M\cong H$. Now the isomorphism (3.3) shows that $S_{H,\mathbb{F}}(G)$ has a basis in one to one correspondence with the G-conjugacy classes of sections (K,M) of G such that K is p-elementary and $K/M\cong H$. This proves the theorem, in the case where H is neither cyclic nor isomorphic to $C_p \times C_{p^{h-1}}$, for some $h \geq 2$.

Step 6: Suppose now that H is cyclic, of order $p^h > 1$. Assume first that Q is cyclic. Then since $Q \cong E \times H$ for some elementary abelian p-group E, it follows that $E = \mathbf{1}$, i.e. $Q \cong H$. In this case $\mathcal{N}_H(Q) = \{\mathbf{1}\}$, and $\langle \mathbf{1}, \mathbf{1} \rangle^\natural_{H,\mathbb{F}} = 1$. Hence $\mathcal{V}_H(Q)$ is isomorphic to the trivial $\mathbb{F}\mathrm{Aut}(Q)$-module in this case.

If Q is non-cyclic, let $M, N \in \mathcal{N}_H(Q)$. Recall that

$$\langle M, N \rangle^\natural_{\mathbb{F},Q} = m_{Q,M\cap N} \, \frac{\alpha_{M,N}}{|M{:}M\cap N|} \ ,$$

where $\alpha_{M,N}$ is defined in (4.4).

The groups $\overline{M} = M/(M \cap N)$ and $\overline{N} = N/(M \cap N)$ are non-trivial elementary abelian central subgroups of $\overline{Q} = Q/(M \cap N)$, and have a common complement in $\overline{Q}$. As $\overline{M}$ is isomorphic to the subgroup MN/N of the cyclic group $Q/N \cong H$, it follows that $\overline{M} \cong C_p$. Moreover $\overline{M}$ has a complement in $\overline{Q}$, so $\overline{Q} \cong C_p \times C_{p^h}$. Hence if $Q/\Phi(Q)$ has rank n, then $\Phi(Q)(M \cap N)/\Phi(Q)$ has rank $n-2$ since

$$Q/\big(\Phi(Q)(M \cap N)\big) \cong \overline{Q}/\Phi(\overline{Q}) \cong C_p \times C_p \ .$$

By Equations 4.3 and 4.2, it follows that

$$m_{Q,M\cap N} = (1-p^{n-2})(1-p^{n-3}) \cdots (1-p) \ .$$

Moreover since $m = 1$ and $\gamma = 1$, Equation 4.5 gives

$$\langle M, N \rangle^\natural_{\mathbb{F},Q} = -m_{Q,M\cap N}(p^s-1)(p^{s-1}-1) \cdots (p-1) p^{\frac{1}{2}(1-s)(2+s)-1} \ .$$

Since $0 \leq s \leq m = 1$, there are two cases:

- If $s = 1$, then $\overline{M}$ maps into $\overline{Q}/\overline{N}\Phi(\overline{Q}) \cong H/\Phi(H) \cong C_p$, hence $MN = Q$ as above, and $Q/N \cong C_{p^h} \cong \overline{M} \cong C_p$, so $h = 1$. In this case

$$\begin{aligned} \langle M, N \rangle^\natural_{\mathbb{F},Q} &= -(1-p^{n-2})(1-p^{n-3}) \cdots (1-p)(p-1)/p \\ &= (1-p^{n-2})(1-p^{n-3}) \cdots (1-p^2)(1-p)^2/p \ . \end{aligned}$$

- If $s = 0$. Then $\overline{M} \leq \overline{N}\Phi(\overline{Q})$, so $\overline{M}\Phi(\overline{Q}) = \overline{N}\Phi(\overline{Q})$. If $h = 1$, then $\overline{Q}/\overline{M} \cong C_p$, so $\overline{M} \geq \Phi(\overline{Q})$, and it follows that $\overline{M} = \overline{N}$, a contradiction. Thus $h > 1$ in this case. Moreover

$$\langle M, N \rangle^\natural_{\mathbb{F},Q} = -(1-p^{n-2})(1-p^{n-3}) \cdots (1-p) \ .$$

So in any case, there is a non-zero rational number ρ, depending only on Q (and H), such that $\langle M,N\rangle^\natural_{\mathbb{F},Q} = \rho$ when $\langle M,N\rangle^\natural_{\mathbb{F},Q} \neq 0$. Moreover $\langle M,N\rangle^\natural_{\mathbb{F},Q} \neq 0$ if and only if $M \neq N$.

So the matrix of the form $\langle\ ,\ \rangle^\natural_{\mathbb{F},P}$ is equal to ρJ, where J is a matrix of size $|\mathcal{N}_H(Q)|$, with zero diagonal, and non-diagonal coefficients equal to 1. Hence this matrix is non-singular if and only if $|\mathcal{N}_H(Q)| > 1$.

But $Q = E \times L$, where $L \cong H$ and E is a non-trivial elementary abelian p-group. The elements of $\mathcal{N}_H(Q)$ are exactly the groups

$$E_\varphi = \{\big(e,\varphi(e)\big) \mid e \in E\}\ ,$$

where φ is a group homomorphism from E to L. There are $|E|$ such homomorphisms, hence $|\mathcal{N}_H(Q)| = |E| > 1$.

It follows that the matrix of the form $\langle\ ,\ \rangle^\natural_{\mathbb{F},Q}$ is non-singular, hence the form $\langle\ ,\ \rangle^\natural_{\mathbb{F},Q}$ is non-degenerate.

So either when Q is cyclic, or when it is not, the form $\langle\ ,\ \rangle^\natural_{\mathbb{F},Q}$ is non-degenerate. By the same argument as at the end of Step 4, this proves that $S_{H,\mathbb{F}}(G)$ has a basis in one to one correspondence with the G-conjugacy classes of sections (K,M) of G for which K is p-elementary and $K/M \cong H$. This proves the theorem in the case where H is cyclic.

Step 7: Suppose now that $H \cong C_p \times C_{p^{h-1}}$, for some $h \geq 2$. Note that if $h = 2$, then H is elementary abelian, so $Q = P/R \cong E \times H$ is elementary abelian. Since $R \leq \Phi(P)$, this forces $R = \Phi(P)$.

Now if $M,N \in \mathcal{N}_H(Q)$, since $\gamma = 2$ in this case,

$$\langle M,N\rangle^\natural_{\mathbb{F},Q} = (-1)^m m_{Q,M\cap N}(p^s-1)(p^{s-1}-1)\cdots(p-1)p^{\frac{1}{2}(m-s)(m+s+1)}\ ,$$

and moreover

$$m_{Q,M\cap N} = (1-p^{n-2})(1-p^{n-3})\cdots(1-p^{m+1})\ ,$$

where n is the rank of $Q/\Phi(Q)$, where m is the rank of the elementary abelian subgroups $\overline{M} = M/(M\cap N)$ and $\overline{N} = N/(M\cap N)$ of $\overline{Q} = Q/(M\cap N)$, and s is the rank of $M/\big(M\cap N\Phi(Q)\big) \cong \overline{M}/\big(\overline{M}\cap\overline{N}\Phi(\overline{Q})\big)$. Since the exponent $\frac{1}{2}(m-s)(m+s+1)$ of p is non-negative, it follows that $\langle M,N\rangle^\natural_{\mathbb{F},Q}$ is an integer. Moreover, if $m > s$, this integer is a multiple of p. On the other hand $m = s$ if and only if $\overline{M}\cap\overline{N}\Phi(\overline{Q}) = \mathbf{1}$, or equivalently if $M\cap N\Phi(Q) = M\cap N$. Since $M\cap\Phi(Q) = N\cap\Phi(Q) = \mathbf{1}$, this is equivalent to $MN\cap\Phi(Q) = \mathbf{1}$. In this case

$$\langle M,N\rangle^\natural_{\mathbb{F},Q} = (1-p^{n-2})(1-p^{n-3})\cdots(1-p) \qquad (\mathbf{4.7})$$

is congruent to 1 modulo p. It follows that the matrix of the form $\langle\ ,\ \rangle^\natural_{\mathbb{F},Q}$ is congruent modulo p to the incidence matrix of the relation $\sim$ on $\mathcal{N}_H(Q)$ defined by $M \sim N$ if and only if $MN \cap \Phi(Q) = \mathbf{1}$. There are now two cases:

• **Case 1:** Assume first that $h \geq 3$, i.e. that H is not elementary abelian of rank 2.

4.8. Lemma: *Let $H = C_p \times C_{p^{h-1}}$, for $h \geq 3$, and $Q = E \times H$, where E is an elementary abelian p-group of rank e. Let S denote the incidence matrix of the relation $\sim$ on $\mathcal{N}_H(Q)$ defined by*

$$M \sim N \Leftrightarrow MN \cap \Phi(Q) = \mathbf{1} \ .$$

Then:

1. *if $e = 0$, the matrix S is the matrix (1).*
2. *if $e \geq 1$, the eigenvalues of S are $p^{e+1} - p + 1$, $p^e - p + 1$, and $1 - p$, with respective multiplicities 1, $p^{e+1} - p$, and $p^{2e} - p^{e+1} + p - 1$.*

In both cases M is invertible modulo p.

Proof : If $e = 0$, then $E = \mathbf{1}$ and $Q \cong H$, so $\mathcal{N}_H(Q)$ consists of the trivial subgroup E of Q. Since $E \sim E$, Assertion 1 follows.

If $e \geq 1$, then $\mathcal{N}_H(Q)$ consists of the subgroups

$$E_\varphi = \{\big(x, \varphi(x)\big) \mid x \in E\} \ ,$$

where $\varphi : E \to H$ is a group homomorphism. Since E is elementary abelian, the image of φ is contained in the subgroup $C_p \times C_p$ of $H = C_p \times C_{p^{h-1}}$. So there are group homomorphisms $a, b : E \to C_p$ such that $\varphi = (a, b)$, i.e. $\varphi(x) = \big(a(x), b(x)\big)$ for any $x \in E$.

Let $\varphi = (a, b)$ and $\varphi' = (a', b')$ be two group homomorphisms from E to H. Then, with an additive notation

$$E_\varphi E_{\varphi'} = \{\big(x - x', a(x) - a'(x'), b(x) - b'(x')\big) \mid x, x' \in E\} \leq E \times C_p \times C_p \ .$$

The element $\big(x - x', a(x) - a'(x'), b(x) - b'(x')\big)$ is in $\Phi(Q) = \mathbf{1} \times \mathbf{1} \times C_{p^{h-2}}$ if and only if $x = x'$ and $a(x) = a'(x')$. Thus

$$E_\varphi \sim E_{\varphi'} \Leftrightarrow \mathrm{Ker}(a - a') \leq \mathrm{Ker}(b - b') \ .$$

Identifying E with the vector space $(\mathbb{F}_p)^e$, and C_p with $\mathbb{F}_p$, the homomorphisms a, b, a', b' become elements of the dual vector space E^*, and the condition $\mathrm{Ker}(a - a') \leq \mathrm{Ker}(b - b')$ means that there is a scalar $\lambda \in \mathbb{F}_p$ such that

$b-b'=\lambda(a-a')$. Hence the incidence matrix S is the matrix indexed by pairs $\big((a,b),(a',b')\big)$ of pairs of elements of E^*, defined by

$$S\big((a,b),(a',b')\big)=\begin{cases}1 & \text{if } \exists\lambda\in\mathbb{F}_p,\ b-b'=\lambda(a-a')\\ 0 & \text{otherwise}\end{cases}\quad.$$

Let T be the rectangular matrix indexed by the set of pairs $\big((a,b),(c,\lambda)\big)$, where $a,b,c\in E^*$, and $\lambda\in\mathbb{F}_p$, defined by

$$T\big((a,b),(c,\lambda)\big)=\begin{cases}1 & \text{if } c=b-\lambda a\\ 0 & \text{otherwise}\end{cases}\quad.$$

Then for $a,b,a',b'\in E^*$, consider the sum

$$s=\sum_{\substack{c\in E^*\\ \lambda\in\mathbb{F}_p}} T\big((a,b),(c,\lambda)\big)T\big((a',b'),(c,\lambda)\big)\ .$$

The non-zero terms in this summation correspond to pairs (c,λ) such that $c=b-\lambda a=b'-\lambda a'$. Hence s is equal to the number of $\lambda\in\mathbb{F}_p$ such that $b-\lambda a=b'-\lambda a'$. This is equal to 1 if $a'\neq a$ and if $b'-b$ is a scalar multiple of $a'-a$, to p if $a=a'$ and $b=b'$, and to 0 if $a=a'$ and $b\neq b'$. In other words

$$T\cdot {}^tT=S+(p-1)\mathrm{Id}\ .$$

Since $T\cdot {}^tT$ is symmetric, it is diagonalizable over $\mathbb{C}$, with real eigenvalues. Let μ be an eigenvalue of $T\cdot {}^tT$, and u be a corresponding eigenvector. Then $T\cdot {}^tTu=\mu u$, thus ${}^tT\cdot T\cdot {}^tTu=\mu {}^tTu$. So either ${}^tTu=0$, and then $\mu=0$. And if $\mu\neq 0$, then ${}^tTu$ is an eigenvector of ${}^tT\cdot T$ for the eigenvalue μ. Moreover, the map $u\mapsto {}^tTu$ is an injection of the μ-eigenspace of $T\cdot {}^tT$ into the μ-eigenspace of ${}^tT\cdot T$. The same argument applied to ${}^tT\cdot T$ instead of $T\cdot {}^tT$ shows that these two matrices have the same non-zero eigenvalues, and the same multiplicities.

Now for $c,c'\in E^*$ and $\lambda,\lambda'\in\mathbb{F}_p$

$${}^tT\cdot T\big((c,\lambda),(c',\lambda')\big)=\sum_{a,b\in E^*} T\big((a,b),(c,\lambda)\big)T\big((a,b),(c',\lambda')\big)\ .$$

The right hand side is the number of pairs (a,b) of elements of E^* such that $c=b-\lambda a$ and $c'=b-\lambda' a$, i.e. the number of elements $a\in E^*$ such that $c+\lambda a=c'+\lambda' a$, or $c-c'=(\lambda-\lambda')a$. This is equal to 1 if $\lambda\neq\lambda'$, to $|E|$ if $\lambda=\lambda'$ and $c=c'$, and to 0 if $\lambda=\lambda'$ and $c\neq c'$. Hence the matrix ${}^tT\cdot T$ is a block matrix of the following form

$$ {}^tT\cdot T = \begin{pmatrix} |E|\mathrm{Id} & \Omega & \cdots & \Omega \\ \Omega & |E|\mathrm{Id} & \cdots & \Omega \\ \vdots & \vdots & \ddots & \vdots \\ \Omega & \Omega & \dots & |E|\mathrm{Id} \end{pmatrix}\ , $$

where all the p^2-blocks are square matrices of size $|E|$, and Ω is a matrix with all entries equal to 1. Let μ be an eigenvalue of this matrix, and

$$ v = \begin{pmatrix} X_1 \\ X_2 \\ \vdots \\ X_p \end{pmatrix} $$

be a corresponding eigenvector, where $X_1, \dots, X_p$ are column vectors of size $|E|$. Equivalently, for each $i \in \{1, \dots, p\}$

$$ |E|X_i + \sum_{j\neq i} \Omega X_j = \mu X_i\ . $$

But $\Omega X = s(X)\omega$ for any column vector X of size $|E|$, where $s(X)$ denotes the sum of the entries of X, and ω is a column vector of size $|E|$ with all entries equal to 1. Setting $\sigma = \sum_{j=1}^p s(X_j)$, this gives, since $|E| = p^e$

$$ p^e X_i + \big(\sigma - s(X_i)\big)\omega = \mu X_i\ . $$

Hence if $\mu \neq p^e$, the vector X_i is a multiple of ω, i.e. $X_i = \alpha_i\omega$ for some scalar α_i. Then $s(X_i) = \alpha_i p^e$, thus $\sigma = \tau p^e$, where $\tau = \sum_{j=1}^p \alpha_j$. Finally

$$ p^e\alpha_i + \big(\tau - \alpha_i\big)p^e = \tau p^e = \mu\alpha_i\ . $$

Thus if $\mu \neq 0$, all the α_i's are equal to α, say, and then $\tau = p\alpha$, thus $\mu = p^{e+1}$. Conversely, if $X_i = \omega$ for all i, then v is an eigenvector of ${}^tT\cdot T$ with eigenvalue p^{e+1}. So p^{e+1} is an eigenvalue of ${}^tT\cdot T$, with multiplicity 1.

If $\mu = 0$, then the vector v corresponding to $X_i = \alpha_i\omega$ for $i \in \{1, \dots p\}$ is in the kernel of ${}^tT\cdot T$ if and only if $\sum_{j=1}^p \alpha_i = 0$. Hence 0 is an eigenvalue of ${}^tT\cdot T$ with multiplicity $p-1$.

Finally, if $\mu = p^e$, then $s(X_i) = \sigma$ for $i \in \{1, \dots p\}$, hence $\sigma = p\sigma = 0$. The vector v is in the p^e-eigenspace of ${}^tT\cdot T$ if and only if $s(X_i) = 0$ for all i. Thus p^e is an eigenvalue of ${}^tT\cdot T$, with multiplicity $p(p^e - 1)$.

It follows that $T \cdot {}^tT$ has eigenvalues p^{e+1}, p^e, and 0, with respective multiplicities 1, $p^{e+1} - p$, and $p^{2e} - p^{e+1} + p - 1$. This completes the proof, since $S = T \cdot {}^tT - (p-1)\mathrm{Id}$. □

Lemma 4.8 shows that the form $\langle\ ,\ \rangle^\natural_{\mathbb{F},Q}$ is non-degenerate whenever H is a quotient of Q. By the argument of the end of Step 4, or the end of Step 6, this shows that $S_{H,\mathbb{F}}(G)$ has a basis in bijection with the G-conjugacy classes of sections (T,S) of G such that T is p-elementary and $T/S \cong H$.

• **Case 2:** Suppose finally that $H = C_p \times C_p$. As observed earlier, in this case, if R is a normal subgroup of P contained in $\Phi(P)$ such that $P/R \cong E \times H$ for some elementary abelian p-group E, then in fact $R = \Phi(P)$. The group $Q = P/R$ is elementary abelian, and decomposes as $Q = E \times L$, where $L \cong H$ is elementary abelian of rank 2. The set $\mathcal{N}_H(Q)$ is the set of complements M of L in Q, and $MN \cap \Phi(Q) = \mathbf{1}$ for any $M,N \in \mathcal{N}_H(Q)$. Equation 4.7 shows that

$$\langle M,N\rangle^\natural_{\mathbb{F},Q} = (1-p^{n-2})(1-p^{n-3})\cdots(1-p)\ ,$$

where n is the rank of $P/\Phi(P)$. *This is non-zero, and does not depend on* $M,N \in \mathcal{N}_H(Q)$. Hence the form $\langle\ ,\ \rangle^\natural_{\mathbb{F},Q}$ has rank 1 in this case. Thus $\tilde{e}^P_P S_{H,\mathbb{F}}(P)$ is one dimensional if P is non-cyclic, and it is zero otherwise. Saying that P is non-cyclic is equivalent to saying that the p-elementary group $K = P \times C$ of Step 1 is non-cyclic. Hence $S_{H,\mathbb{F}}(G)$ has a basis in bijection with the conjugacy classes of non-cyclic p-elementary subgroups of G. This completes the proof of Theorem 4.1. □

4.9. Remark: As $C_p \times C_p$ is a B-group, Case 2 above also follows from Proposition 11 of [6]: for a B-group H and a finite group G, the dimension of $S_{H,\mathbb{F}}(G)$ is equal to the number of conjugacy classes of subgroups K of G such that $\beta(K) \cong H$. Now by Lemma 2.4, if $\beta(K) \cong C_p \times C_p$, then K is p-elementary, and non cyclic (for otherwise $\beta(K) = \mathbf{1}$). Conversely, if K is p-elementary and non cyclic, then $\beta(K)$ is a non trivial p-group, and also a B-group, hence $\beta(K) \cong C_p \times C_p$.

5. A Green biset functor for p-elementary groups

The following theorem is closely related to Theorem 4.1. In particular, it yields an alternative proof of its Assertions 1 and 2. We refer to Section 8.5 of [9] for the basic definitions on Green biset functors.

5.1. Theorem: *Let p be a prime number.*

1. *For a finite group G, let $\mathcal{E}l_p(G)$ denote the set of p-elementary sub-*

groups of G. Set

$$F_p(G) = \{u \in B(G) \mid \forall H \in \mathcal{E}l_p(G),\ \mathrm{Res}^G_H u = 0\}\ .$$

Then the assignment $G \mapsto F_p(G)$ is a biset subfuntor of the Burnside functor B, and the quotient functor

$$E_p = B/F_p$$

is a Green biset functor (over $\mathbb{Z}$).

2. *For a finite group G, the evaluation $E_p(G)$ is a free abelian group of rank equal to the number of conjugacy classes of p-elementary subgroups of G.*
3. *Let $\mathbb{F}$ be a field of characteristic 0. Then the biset functor $\mathbb{F}E_p = \mathbb{F} \otimes_{\mathbb{Z}} E_p$ has a unique non zero proper subfunctor I, isomorphic to $S_{(C_p)^2,\mathbb{F}}$, and the quotient $\mathbb{F}E_p/I$ is isomorphic to $S_{\mathbf{1},\mathbb{F}} \cong \mathbb{F}R_{\mathbb{Q}}$. In other words there is a non split short exact sequence*

$$(\mathbf{5.2}) \qquad 0 \to S_{(C_p)^2,\mathbb{F}} \to \mathbb{F}E_p \to S_{\mathbf{1},\mathbb{F}} \to 0$$

of biset functors over $\mathbb{F}$.

Proof : Let $\mathbb{F}B = \mathbb{F} \otimes_{\mathbb{Z}} B$ be the Burnside functor over $\mathbb{F}$. If we forget the $\mathbb{F}$-structure on $\mathbb{F}B$, we get an inclusion $B \to \mathbb{F}B$ of biset functors over $\mathbb{Z}$. In particular, for each finite group G, we get an inclusion

$$f_p : F_p(G) \to \mathbb{F}B(G)\ .$$

Now saying that $u \in B(G)$ lies in $F_p(G)$ amounts to saying that the restriction of $f_p(u)$ to any p-elementary subgroup of G is equal to 0. Since any subgroup of a p-elementary group is again p-elementary, this amounts to saying that $|f_p(u)^H| = 0$ for any $H \in \mathcal{E}l_p(G)$. In other words $f_p(u)$ is a linear combination of idempotents e^G_K of $\mathbb{F}B(G)$, where K is a subgroup of G which is *not* p-elementary. By Lemma 2.4, we get that $u \in \mathbb{F}_p(G)$ if and only if $f_p(u)$ is a linear combination of idempotents e^G_K, for subgroups K such that $\beta(K)$ is not a p-group, that is $\beta(K)$ is non trivial and not isomorphic to $(C_p)^2$.

Let $\mathcal{G}_p$ be the class of B-groups which are non trivial, and not isomorphic to $(C_p)^2$. Then $\mathcal{G}_p$ is a *closed* class of B-groups ([9], Definition 5.4.13), that is, if a B-group L admits a quotient in $\mathcal{G}_p$, then actually $L \in \mathcal{G}_p$ (this is because the only quotient B-groups of $(C_p)^2$ are the trivial group and $(C_p)^2$, up to isomorphism). By Theorem 5.4.14 of [9], this closed class $\mathcal{G}_p$ is associated to a subfunctor N_p of the Burnside functor $\mathbb{F}B$, defined for a finite group G by

$$N_p(G) = \sum_{\substack{K \le G \\ \beta(K) \in \mathcal{G}_p}} \mathbb{F}e_K^G \;.$$

This shows that $f_p\big(F_p(G)\big) = f_p\big(B(G)\big) \cap N_p(G)$, and since N_p is a biset subfunctor of $\mathbb{F}B$, it follows that F_p is a biset subfunctor of B. As biset subfunctors of B are also ideals of the Green biset functor B (see Lemma 2.5.8, Assertion 4 in [9]), we get that F_p is an ideal of B. It follows that the quotient $E_p = B/F_p$ is a Green biset functor. This completes the proof of Assertion 1.

Moreover, the ghost map

$$\Phi_G : B(G) \to \prod_{\substack{K \le G \\ \mathrm{mod.}\, G}} \mathbb{Z}$$

sending $u \in B(G)$ to the sequence $|u^K|$, is injective by Burnside's theorem. The above discussion shows that Φ induces an injective map

$$E_p(G) = B(G)/F_p(G) \to \prod_{\substack{K \in \mathcal{E}l_p(G) \\ \mathrm{mod.}\, G}} \mathbb{Z} \;,$$

which becomes an isomorphism after tensoring with $\mathbb{F}$. Assertion 2 follows.

Finally, it follows from Theorem 5.4.14 of [9] that the lattice $[0, \mathbb{F}E_p]$ of biset subfunctors of $\mathbb{F}E_p$ is isomorphic to the set of closed classes of B-groups which contain $\mathcal{G}_p$. There are exactly three such classes: the class $\mathcal{G}_p$, the class of non-trivial B-groups, and the class of all B-groups. So $[0, \mathbb{F}E_p]$ is a totally ordered set of cardinality 3. Hence $\mathbb{F}E_p$ admits a unique non zero proper subfunctor I. The quotient $\mathbb{F}E_p/I$ is the unique simple quotient of $\mathbb{F}B$, hence it is isomorphic to $S_{\mathbf{1},\mathbb{F}} \cong \mathbb{F}R_{\mathbb{Q}}$. Now I is a simple biset functor, which is a subquotient of $\mathbb{F}B$. By Proposition 5.5.1 of [9], it follows that $I \cong S_{H,\mathbb{F}}$ for some B-group H. Since the group $K = (C_p)^2$ has a unique non cyclic subgroup, it follows that $I(K)$ is one dimensional, and a trivial $\mathbb{F}\mathrm{Out}(K)$-module. Moreover K is a group of minimal order such that $I(K) \neq \{0\}$. Hence $H \cong K$, and $I \cong S_{(C_p)^2,\mathbb{F}}$. This completes the proof of Assertion 3, and the proof of Theorem 5.1. □

5.3. Remark: One can show that the exact sequence (5.2) is essentially unique as a non split exact sequence in the category $\mathcal{F}_{\mathbb{F}}$ of biset functors over $\mathbb{F}$: more precisely, one can show that $\mathrm{Ext}^1_{\mathcal{F}_{\mathbb{F}}}(S_{\mathbf{1},\mathbb{F}}, S_{(C_p)^2,\mathbb{F}}) \cong \mathbb{F}$.

5.4. Remark: If G is a p-group (or even if G is p-elementary), then $F_p(G) = \{0\}$, so $E_p(G) \cong B(G)$. So if we restrict the exact sequence (5.2) to finite

p-groups, we get an exact sequence

$$0 \to S_{(C_p)^2,\mathbb{F}} \to \mathbb{F}B \to \mathbb{F}R_{\mathbb{Q}} \to 0$$

of p-biset functors over $\mathbb{F}$. This (restricted) exact sequence was introduced in [12], where is was shown that for a finite p-group P, the evaluation $S_{(C_p)^2,\mathbb{F}}(P)$ is isomorphic to $\mathbb{F}D(P)$, where $D(P)$ is the Dade group of endopermutation modules. It was also shown that the dimension of $S_{(C_p)^2,\mathbb{F}}(P)$ is equal to the number of conjugacy classes of non cyclic subgroups of P, which is also the number of conjugacy classes of non-cyclic p-elementary subgroups of P. So this agrees with Assertion 2 of Theorem 4.1.

5.5. Remark: For a finite group G, let $M_p(G)$ be the $\mathbb{Z}$-submodule of $B(G)$ generated by the classes of the transitive G-sets G/H, where H is a p-elementary subgroup of G. One can check easily that $M_p(G) \cap F_p(G) = \{0\}$, so comparing ranks, one might hope that $B(G) = M_p(G) \oplus F_p(G)$. This is false in general: for $p = 2$, when G is the symmetric group S_3, there are three p-elementary subgroups in G, up to conjugation, namely the proper subgroups of G (that is the trivial group, the alternating subgroup $A = A_3$, and the subgroup C of order 2). Hence if $B(G) = M_p(G) \oplus F_p(G)$, then in particular $G/G \in M_p(G) \oplus F_p(G)$ so there exist integers a, b, c such that the element $u = G/G - (b\,G/\mathbf{1} + a\,G/A + c\,G/C)$ is in $F_p(G)$. Taking fixed points by A then gives $|u^A| = 0 = 1 - 2a$, a contradiction. One can show more precisely that $M_p(G) \oplus F_p(G)$ has index 2 in $B(G)$ in this case.

References

[1] L. Barker and I. A. Öğüt. Some deformations of the fibred biset category. *Turkish J. Math.*, 44(6):2062–2072, 2020.

[2] J. Barsotti. On the unit group of the Burnside ring as a biset functor for some solvable groups. *J. Algebra*, 508, 05 2018.

[3] M. Baumann. The composition factors of the functor of permutation modules. *J. Algebra*, 344:284–295, 2011.

[4] R. Boltje and O. Coşkun. Fibered biset functors. *Adv. Math.*, 339:540–598, 2018.

[5] R. Boltje, G. Raggi-Cárdenas, and L. Valero-Elizondo. The $-_+$ and $-^+$ constructions for biset functors. *J. Algebra*, 523:241–273, 2019.

[6] S. Bouc. Foncteurs d'ensembles munis d'une double action. *J. Algebra*, 183(0238):664–736, 1996.

[7] S. Bouc. The Dade group of a p-group. *Invent. Math.*, 164:189–231, 2006.

[8] S. Bouc. The functor of units of Burnside rings for p-groups. *Comment. Math. Helv.*, 82:583–615, 2007.

[9] S. Bouc. *Biset functors for finite groups*, volume 1990 of *Lecture Notes in Mathematics*. Springer-Verlag, Berlin, 2010.

[10] S. Bouc and N. Romero. The center of a Green biset functor. *Pacific Journal of Mathematics*, 303:459–490, 2019.

[11] S. Bouc, R. Stancu, and J. Thévenaz. Simple biset functors and double Burnside ring. *Journal of Pure and Applied Algebra*, 217:546–566, 2013.

[12] S. Bouc and J. Thévenaz. The group of endo-permutation modules. *Invent. Math.*, 139:275–349, 2000.

[13] O. Coşkun and E. Yalçın. Obstructions for gluing biset functors. *J. Algebra*, 532:268–310, 2019.

[14] O. Coşkun and D. Yılmaz. Fibered p-biset functor structure of the fibered Burnside rings. *Algebr. Represent. Theory*, 22(1):21–41, 2019.

[15] B. García. Essential support of Green biset functors via morphisms. *Arch. Math. (Basel)*, 116(1):23–32, 2021.

[16] B. Rognerud. Around evaluations of biset functors. *Ann. Inst. Fourier (Grenoble)*, 69(2):805–843, 2019.

Serge Bouc
LAMFA-CNRS UMR 7352
Université de Picardie-Jules Verne
33, rue St Leu, 80039 Amiens Cedex 01
France
`serge.bouc@u-picardie.fr`
`http://www.lamfa.u-picardie.fr/bouc/`