The Whitehead group of (almost) extra-special p-groups with p odd

Serge Bouc[1] and **Nadia Romero**[2]

Abstract: Let p be an odd prime number. We describe the Whitehead group of all extra-special and almost extra-special p-groups. For this we compute, for any finite p-group P, the subgroup $Cl_1(\mathbb{Z}P)$ of $SK_1(\mathbb{Z}P)$, in terms of a genetic basis of P. We also introduce a deflation map $Cl_1(\mathbb{Z}P) \to Cl_1\big(\mathbb{Z}(P/N)\big)$, for a normal subgroup N of P, and show that it is always surjective. Along the way, we give a new proof of the result describing the structure of $SK_1(\mathbb{Z}P)$, when P is an elementary abelian p-group.

Keywords: Whitehead group, almost extra-special p-groups, genetic basis.

MSC2010: 19B28, 20C05, 20D15.

Introduction

Whitehead groups were introduced by J.H.C. Whitehead in [23], as an algebraic continuation of his work on combinatorial homotopy. The computation of the Whitehead group $Wh(G)$ of a finite group G is in general very hard, and a compendium on the subject is the book by Bob Oliver ([17]) of 1988. Since then, it seems that not much progress has been made on this subject (see however [16], [15], [22], [21]).

Let p be an odd prime number. In this paper, we describe the Whitehead group of all extra-special and almost extra-special p-groups. The main reason for focusing on these p-groups is that, apart from elementary abelian p-groups, they are exactly the finite p-groups all proper factor groups of which are elementary abelian (see e.g. Lemma 3.1 of [10]). In particular these groups appear naturally in various areas as first crucial step in inductive procedures (see [10], [9], or the proof of Serre's Theorem in Section 4.7 of [3] for examples).

One of the main tools in our method is Theorem 9.5 of [17], which gives a first description, for a finite p-group P, of the subgroup $Cl_1(\mathbb{Z}P)$, an essential part of the torsion of $Wh(P)$. As this description requires the knowledge of the rational irreducible

[1]CNRS-LAMFA, UPJV, Amiens, France

[2]DEMAT, UGTO, Guanajuato, Mexico - Partially supported by SEP-PRODEP, project PTC-486

representations of P, it seems natural to try to translate it in terms of a *genetic basis* of P, which provides an explicit description of the rational irreducible representations of P, using only combinatorial informations on the poset of subgroups of P. The notions of genetic subgroup and genetic basis come from biset functor theory ([7]). They already have been used successfully for the computation of other groups related to representations of finite p-groups, e.g. the group of units of Burnside rings (see [6]), or the Dade group of endopermutation modules (see [5]).

Our first task is then to obtain a description of $Cl_1(\mathbb{Z}P)$ in terms of a genetic basis of P. The advantage of this description is that it only requires data of a combinatorial nature, and makes no use of linear representations. In particular this makes it much easier to implement for computational purposes, using e.g. GAP software ([13]). This also explains why in the proof of our main theorem (Theorem A below), we have to consider separately two special cases of "small" p-groups, for which the lattice of subgroups is in some sense too tight for the general argument to work.

We observe next on this description that for any normal subgroup N of P, there is an obvious *deflation operation* $\mathrm{Def}^P_{P/N} : Cl_1(\mathbb{Z}P) \to Cl_1\big(\mathbb{Z}(P/N)\big)$. Even if there seems to be no inflation operation in the other direction, which would provide a section of this map, we show that $\mathrm{Def}^P_{P/N}$ is always surjective. The existence of such a surjective deflation map already follows from Corollary 3.10 of [17], and it is shown in [4] that our deflation map is indeed the same as the map defined there.

As we will see in the next section, in the case of an extra-special or almost extra-special p-group P, the group $Cl_1(\mathbb{Z}P)$ is equal to the torsion part $SK_1(\mathbb{Z}P)$ of $Wh(P)$, so the computation of the Whitehead group of P comes down to the knowledge of $Cl_1\Big(\mathbb{Z}\big(P/\Phi(P)\big)\Big)$, where $\Phi(P)$ is the Frattini subgroup of P, and a detailed analysis of what happens with the unique faithful rational irreducible representation of P. Our main theorem is the following:

Theorem A. *Let p be an odd prime, and let P be an extra-special p-group of order at least p^5 or an almost extra-special p-group of order at least p^6. Set $N = \Phi(P) = P'$.*

1. *The group $Cl_1(\mathbb{Z}P)$ is isomorphic to $K \times (C_p)^M$, where $M = \frac{p^{k-1}-1}{p-1} - \binom{p+k-2}{p}$ if $|P| = p^k$, and K is the kernel of $\mathrm{Def}^P_{P/N} : Cl_1(\mathbb{Z}P) \to Cl_1\big(\mathbb{Z}(P/N)\big)$.*
2. *The group K is cyclic. More precisely, it is:*
   (a) *trivial if P is extra-special of order p^5 and exponent p^2.*
   (b) *of order p if P is almost extra-special of order p^6.*
   (c) *isomorphic to $Z(P)$ in all other cases.*

It should be noted that our methods not only give the algebraic structure of the

Whitehead group, but allow also for the determination of explicit generators of its torsion subgroup (see. Remark 3.18 for details).

The paper is organized as follows: Section 1 is a review of definitions and basic results on Whitehead groups, genetic bases of p-groups, extra-special and almost extra-special p-groups. In particular, the subgroups $Cl_1(\mathbb{Z}G)$ and $SK_1(\mathbb{Z}G)$ of the Whitehead group $Wh(G)$ of a group G are introduced. In Section 2, we give a procedure (Theorem 2.4) to compute $Cl_1(\mathbb{Z}P)$ for a finite p-group P (with p odd) in terms of a genetic basis of P. This procedure may be of independent interest, in particular from an algorithmic point of view. Finally, in Section 3, we begin by giving a new proof of the structure of $Wh(P)$ for an elementary abelian p-group P, for p odd, and then we come to our main theorems. The first of them is Theorem 3.16, which will give us point 1 of Theorem A, then Theorem 3.19 and Proposition 3.22 will deal with the description of the group K, giving us point 2. With these results we completely determine the structure of $Wh(P)$, when P is an extra-special or almost extra-special p-group, for p odd.

1. Preliminaries

Let G be a group. We will write $Z(G)$ for the center of G and G' for its commutator subgroup. The Frattini subgroup of G is denoted by $\Phi(G)$. If H is a subgroup of G, the normalizer of H in G will be denoted by $N_G(H)$, and its centralizer by $C_G(H)$. If $H = \langle h \rangle$ for an element $h \in G$, we may also write $C_G(H) = C_G(h)$.

1.1. About the Whitehead group.

Let R be an associative ring with unit. The infinite general linear group of R, denoted by $GL(R)$, is defined as the direct limit of the inclusions $GL_n(R) \to GL_{n+1}(R)$ as the upper left block matrix. If, for each $n > 0$, we denote by $E_n(R)$ the subgroup of $GL_n(R)$ generated by all elementary $n \times n$-matrices – i.e. all those which are the identity except for one non-zero off-diagonal entry – and we take the direct limit as before for the groups $E_n(R)$, we obtain a subgroup of $GL(R)$, denoted by $E(R)$. Whitehead's Lemma (Theorem 1.13 in [17], for instance) states that $E(R)$ is equal to the derived subgroup of $GL(R)$. The group $K_1(R)$ is defined as the abelianization of $GL(R)$, which is then equal to $GL(R)/E(R)$.

If G is a group and we take R as the group ring $\mathbb{Z}G$, then elements of the form $\pm g$ for $g \in G$ can be regarded as invertible 1×1-matrices over $\mathbb{Z}G$ and hence they represent elements in $K_1(\mathbb{Z}G)$. Let H be the subgroup of $K_1(\mathbb{Z}G)$ generated by classes of elements of the form $\pm g$ with $g \in G$. The *Whitehead group* of G is defined as $Wh(G) = K_1(\mathbb{Z}G)/H$.

If G is finite, the groups $K_1(\mathbb{Z}G)$ and $Wh(G)$ are finitely generated abelian groups (see Theorem 2.5 in [17]).

For the rest of this section, G denotes a finite group.

1.2. Definition. *Let D be an integral domain and K be its field of fractions, then $SK_1(DG)$ denotes the kernel of the morphism*

$$K_1(DG) \to K_1(KG).$$

By Theorem 7.4 in [17], $SK_1(\mathbb{Z}G)$ is isomorphic to the torsion subgroup of $Wh(G)$. Hence, $Wh(G)$ is completely determined by $SK_1(\mathbb{Z}G)$ and the rank of its free part (i.e. its *free rank*). According to Theorem 2.6 in [17], this free rank is equal to $r - q$, where r is the number of non-isomorphic irreducible $\mathbb{R}$-representations of G and q is the number of non-isomorphic irreducible $\mathbb{Q}$-representations of G.

1.3. Definition. *Consider the ring of p-adic integers $\hat{\mathbb{Z}}_p$. The group $Cl_1(\mathbb{Z}G)$ is defined as the kernel of the localization morphism*

$$l : SK_1(\mathbb{Z}G) \to \bigoplus_p SK_1(\hat{\mathbb{Z}}_p G).$$

By Theorem 3.9 in [17], $SK_1(\hat{\mathbb{Z}}_p G)$ is trivial whenever p does not divide $|G|$, and l is onto. In particular, $SK_1(\mathbb{Z}G)$ sits in an extension

$$0 \longrightarrow Cl_1(\mathbb{Z}G) \longrightarrow SK_1(\mathbb{Z}G) \longrightarrow \bigoplus_p SK_1(\hat{\mathbb{Z}}_p G) \longrightarrow 0.$$

This extension is used by Oliver in [17] to describe $SK_1(\mathbb{Z}G)$ in many cases. The important feature of the groups treated in this paper is that their derived subgroups are central and so by Theorem 8.10 in [17], the group $\bigoplus_p SK_1(\hat{\mathbb{Z}}_p G)$ is trivial, then describing $SK_1(\mathbb{Z}G)$ amounts to describing $Cl_1(\mathbb{Z}G)$.

1.4. About genetic bases.

A finite p-group Q is called a *Roquette p-group* if it has normal p-rank 1, i.e. if all its abelian normal subgroups are cyclic. The Roquette p-groups (see [19] or Theorem 4.10 of [14] for details) of order p^n are the cyclic groups C_{p^n}, if p is odd, and the cyclic groups C_{2^n}, the generalized quaternion groups Q_{2^n}, for $n \geqslant 3$, the dihedral groups D_{2^n}, for $n \geqslant 4$, and the semidihedral groups SD_{2^n}, for $n \geqslant 4$, if $p = 2$. A Roquette p-group Q admits a unique faithful rational irreducible representation Φ_Q (see e.g. Proposition 9.3.5 in [7]).

1.5. Definition. *Let P be a finite p-group. A subgroup S of P is called* genetic *if the section $S \trianglelefteq N_P(S) \leqslant P$ satisfies*

1. *The group $N_P(S)/S$ is a Roquette group.*
2. *Let $\Phi = \Phi_{N_P(S)/S}$ be the only faithful irreducible $\mathbb{Q}$-representation of $N_P(S)/S$ and $V = \mathrm{Ind}_{N_P(S)}^P \mathrm{Inf}_{N_P(S)/S}^{N_P(S)} \phi$, then the functor $\mathrm{Ind}_{N_P(S)}^P \mathrm{Inf}_{N_P(S)/S}^{N_P(S)}$ induces an isomorphism of $\mathbb{Q}$-algebras*

$$\mathrm{End}_{\mathbb{Q}P} V \cong \mathrm{End}_{\mathbb{Q}(N_P(S)/S)} \Phi.$$

Note that the right-hand side algebra is actually a skew field by Schur's lemma. So $\mathrm{End}_{\mathbb{Q}P} V$ is also a skew field, hence V is an indecomposable – that is, irreducible – $\mathbb{Q}P$-module.

1.6. Notation. *Let P be a finite p-group and S be a genetic subgroup of P. We write*

$$V(S) = \mathrm{Ind}_{N_P(S)}^P \mathrm{Inf}_{N_P(S)/S}^{N_P(S)} \Phi_{N_P(S)/S}.$$

Then $V(S)$ is an irreducible $\mathbb{Q}$-representation of P. Conversely, by Roquette's Theorem (Theorem 9.4.1 in [7]), for each irreducible $\mathbb{Q}$-representation V of P, there exists a genetic subgroup S of P such that $V \cong V(S)$.

The following theorem characterizes the genetic subgroups of a p-group. First some notation: for a subgroup S of a finite p-group P, let $Z_P(S) \geqslant S$ be the subgroup of $N_P(S)$ defined by $Z_P(S)/S = Z\big(N_P(S)/S\big)$. In particular $Z_P(S) = N_P(S)$ if $N_P(S)/S$ abelian, e.g. if $N_P(S)/S$ is a Roquette p-group for p odd.

1.7. Theorem. *[Theorem 9.5.6 in [7]] Let P be a finite p-group and S be a subgroup of P such that $N_P(S)/S$ is a Roquette group. Then the following conditions are equivalent:*

1. *The subgroup S is a genetic subgroup of P.*
2. *If $x \in P$ is such that ${}^xS \cap Z_P(S) \leqslant S$, then ${}^xS = S$.*
3. *If $x \in P$ is such that ${}^xS \cap Z_P(S) \leqslant S$ and $S^x \cap Z_P(S) \leqslant S$, then ${}^xS = S$.*

The next result is part of Theorem 9.6.1 in [7].

1.8. Theorem. *Let P be a finite p-group and S and T be genetic subgroups of P. The following conditions are equivalent:*

1. *The $\mathbb{Q}P$-modules $V(S)$ and $V(T)$ are isomorphic.*
2. *There exist $x, y \in P$ such that ${}^xT \cap Z_P(S) \leqslant S$ and ${}^yS \cap Z_P(T) \leqslant T$.*
3. *There exists $x \in P$ such that ${}^xT \cap Z_P(S) \leqslant S$ and $S^x \cap Z_P(T) \leqslant T$.*

If these conditions hold, then in particular the groups $N_P(S)/S$ and $N_P(T)/T$ are isomorphic.

The relation between groups appearing in point 2 is denoted by $S \frown_P T$. The theorem shows that this relation is an equivalence relation on the set of genetic subgroups of P, and we have the following definition.

1.9. Definition. *[Definition 9.6.11 in [7]] Let P be a finite p-group. A* genetic basis *of P is a set of representatives of the equivalence classes of $\frown_P$ in the set of genetic subgroups of P.*

1.10. Lemma. *Let P be a finite p-group and S be a genetic subgroup of P.*

1. *The kernel of $V(S)$ is equal to the intersection of the conjugates of S in P.*
2. *In particular $V(S)$ is faithful if and only S intersects $Z(P)$ trivially.*

Proof. Denote by Φ the unique rational irreducible representation of the Roquette group $N_P(S)/S$. Then

$$V(S) = \mathrm{Ind}_{N_P(S)}^P \mathrm{Inf}_{N_P(S)/S}^{N_P(S)} \Phi \cong \bigoplus_{x \in [P/N_P(S)]} x \otimes \Phi,$$

where $[P/N_P(S)]$ is a chosen set of representatives of $N_P(S)$-cosets in P. An element $g \in P$ acts trivially on $V(S)$ if and only if it permutes trivially the summands of this decomposition, that is if $g^x \in N_P(S)$ for any $x \in P$, and if moreover g^x acts trivially on Φ, which means that $g^x \in S$, since Φ is faithful. This proves Assertion 1.

Assertion 2 follows, since

$$\Big(\bigcap_{x \in P} {}^xS\Big) \cap Z(P) = \bigcap_{x \in P} \big({}^xS \cap Z(P)\big) = \bigcap_{x \in P} {}^x\big(S \cap Z(P)\big) = S \cap Z(P),$$

and since the normal subgroup $T = \bigcap_{x \in P} {}^xS$ of P is trivial if and only if $T \cap Z(P) = \mathbf{1}$, i.e. if $S \cap Z(P) = \mathbf{1}$. □

1.11. Remark. If P is abelian, then a subgroup S of P is genetic if and only if P/S is cyclic. Moreover the relation $\frown_P$ is the equality relation in this case, so there is a unique genetic basis of P, consisting of all the subgroups S of P such that P/S is cyclic.

1.12. Remark. Let P be a finite p-group, and S be a subgroup of P such that $N_P(S)$ is normal in P. If $N_P(S)/S$ is a Roquette group, then S is a genetic subgroup of P. Indeed if $N_P(S)$ is normal in P, then $N_P(S) = N_P({}^xS)$ for any $x \in P$. Hence ${}^xS \trianglelefteq N_P(S)$, and the group ${}^xS \cdot S/S$ is a normal subgroup of $N_P(S)/S$. It is trivial if and only if it intersects trivially the center $Z_P(S)/S$ of $N_P(S)/S$. Then

$$\begin{aligned} {}^xS = S \iff {}^xS \cdot S/S = \mathbf{1} \quad &\iff \quad {}^xS \cdot S \cap Z_P(S) = \big({}^xS \cap Z_P(S)\big)S = S \\ &\iff \quad {}^xS \cap Z_P(S) \leqslant S. \end{aligned}$$

1.13. About extra-special and almost extra-special p-groups.

1.14. Definition. *Let p be a prime and P be a finite p-group.*

1. *The group P is called extra-special if $Z(P) = P' = \Phi(P)$ has order p.*
2. *The group P is called almost extra-special if $P' = \Phi(P)$ has order p and $Z(P)$ is cyclic of order p^2.*

Extra-special and almost extra-special p-groups can be classified in the following way.

1.15. Notation. *Let H, K and M be groups such that $M \leqslant Z(H)$ and such that there exists an injective map $\theta : M \to Z(K)$. The central product of H and K with respect to θ will be denoted by $H *_\theta K$, and simply by $H * K$ if θ is clear from the context.*

For any integer $r \geqslant 1$, we will write H^{*r} for the central product of r copies of the group H, where $M = Z(H)$, with the convention $H^{*1} = H$.

For $p \neq 2$, set

$$M(p) = \langle x,\, y \mid x^p = y^p = 1,\, [x^{-1},\, y] = [y,\, x] = {}^y[y,\, x]\rangle$$

and

$$N(p) = \langle x,\, y \mid x^{p^2} = y^p = 1, {}^yx = x^{1+p}\rangle.$$

1.16. Theorem. *Let p be a prime and P be a finite p-group.*

1. *If P is extra-special, then there exists an integer $r \geqslant 1$ such that P has order p^{2r+1} and P is isomorphic to only one of the following groups: D_8^{*r} or $Q_8 * D_8^{*(r-1)}$ if $p = 2$, and $M(p)^{*r}$ or $N(p) * M(p)^{*(r-1)}$ if $p \neq 2$.*
2. *If P is almost extra-special, then there exists an integer $r \geqslant 1$ such that P has order p^{2r+2} and P is isomorphic to only one of the following groups: $D_8^{*r} * C_4$ if $p = 2$, and $M(p)^{*r} * C_{p^2}$ if $p \neq 2$.*

Proof. The proof of 1 can be found in Section 5.5 of [14]. As for point 2, one can refer to Sections 2 and 4 of [10]. □

Observe that if p is odd, the exponent of the group characterizes the isomorphism type of extra-special p-groups, one of them has exponent p and the other one has exponent p^2.

If P is an (almost) extra-special group, the quotient P/P' is elementary abelian, so it can be regarded as a (finite-dimensional) vector space E over the finite field $\mathbb{F}_p$. Moreover, if we take z a generator of P', then E is endowed with a bilinear form

$$b : E \times E \to \mathbb{F}_p,$$

that sends an element (u, v) to $b(u, v)$, the element of $\mathbb{F}_p$ satisfying $[\tilde{u}, \tilde{v}] = z^{b(u,v)}$ for all $\tilde{u} \in u$, $\tilde{v} \in v$ and $u, v \in E$. This bilinear form is alternating, i.e. $b(v, v) = 0$ for all $v \in E$, hence it is antisymmetric, i.e. $b(u, v) = -b(v, u)$ for all $u, v \in E$. Section 20 in [11] is concerned with this bilinear form for extra-special groups, but the property of being alternating is called *symplectic*.

Recall that if $f : V \times V \to K$ is a bilinear form on a finite dimensional vector space V over a field K, its *left radical* $V^{\perp}$ is defined by $V^{\perp} = \{v \in V \mid f(v, w) = 0\, \forall w \in V\}$, and its *right radical* by ${}^{\perp}V = \{v \in V \mid f(w, v) = 0\, \forall w \in V\}$. Clearly $V^{\perp} = {}^{\perp}V$ when f is antisymmetric. The *rank* of f is the codimension of $V^{\perp}$. The form f is called *non-degenerate* if $V^{\perp} = \{0\}$.

With the help of Lemma 20.4 in [11], we have the following observation.

1.17. Observation. *The bilinear form b is non-degenerate if and only if P is extra-special. If P is almost extra-special, then $E^{\perp} = \pi(Z(P))$ is a line in E, where $\pi : P \to P/P'$ is the projection morphism.*

In section 3.2 we will use the following result, which is part of Lemma 2.6 in [9]. For the proof we refer the reader to this reference.

1.18. Lemma. *Let P be an (almost) extra-special p-group, and let Q be a non-trivial subgroup of P. Then*

1. *$Q \trianglelefteq P \Leftrightarrow P' \leqslant Q$.*
2. *If Q is not normal in P, then $N_P(Q) = C_P(Q)$. In particular, it follows that in this case Q is elementary abelian of rank at most r, for the integer r defined as in Theorem 1.16, and we have $|Q||C_P(Q)| = |P|$. Moreover, $C_P(Q) = Q \times U$, where U is (almost) extra-special of order $|P|/|Q|^2$ or $U = Z(P)$.*

2. Cl_1 of finite p-group algebras for odd p

The goal of this section is to re-write Theorem 9.5 in [17] in terms of genetic bases, in the most possible succinct way. We take the statement of this theorem appearing in Section 1 of [18], which says the following: let p be an odd prime, let P be a finite p-group, and write $\mathbb{Q}P \cong \prod_{i=1}^{k} A_i$, where A_i is simple with irreducible module V_i and center $K_i = \mathrm{End}_{\mathbb{Q}P} V_i$. By Roquette's Theorem, for each $1 \leqslant i \leqslant k$, the field K_i is isomorphic to $\mathbb{Q}(\zeta_{r_i})$, where ζ_{r_i} is a primitive p^{r_i}-th root of unity for some non-negative r_i, and A_i is isomorphic to a matrix algebra over $\mathbb{Q}(\zeta_{r_i})$.

Consider the abelian group $T = \prod\limits_{i=1}^{k} \langle \zeta_{r_i} \rangle$. For each $h \in P$, define

$$\psi_h : C_P(h) \to T, \quad \psi_h(g) = (\det_{K_i}(g, V_i^h))_i$$

where $V_i^h = \{x \in V_i \mid hx = x\}$. Here V_i^h is viewed as a $K_i C_P(h)$-module, so $\det_{K_i}(g, V_i^h)$ is the determinant (in K_i) of the action of g in V_i^h. Since P is a p-group, this determinant is in $\langle \zeta_{r_i} \rangle$. Then Theorem 9.5 in [17] can be written in the following way.

2.1. Theorem. *Let p be an odd prime and consider T and $\psi_h : C_P(h) \to T$, for each $h \in P$, as before. Then*

$$Cl_1(\mathbb{Z}P) \cong T/\langle \mathrm{Im}\psi_h \mid h \in P \rangle.$$

Now, since p is odd, if we let $\mathcal{S} = \{S_1, \ldots, S_k\}$ be a genetic basis of P, then $N_P(S_i)/S_i$ is cyclic for every $1 \leqslant i \leqslant k$ and each simple $\mathbb{Q}P$-module V_i is isomorphic to $V(S_i) = \mathrm{Indinf}_{N_P(S_i)/S_i}^{P} \Phi_{N_P(S_i)/S_i}$. Then the abelian group T defined before is isomorphic to $\Gamma(P) = \prod\limits_{i=1}^{k} \big(N_P(S_i)/S_i\big)$. This is because we can see the module $\Phi_{N_P(S_i)/S_i} \cong \mathbb{Q}(\zeta_{r_i})$, where $p^{r_i} = |N_P(S_i)/S_i|$ as actually being generated by a generator of $N_P(S_i)/S_i$ and thus the action of $N_P(S_i)/S_i$ on it can be seen as multiplication on the group. In particular, $\det_{K_i}(g, V_i^h)$, which is an element of the field K_i, can be regarded as an element in $N_P(S_i)/S_i$. The first step in re-writing Theorem 2.1 is to find this element, for every S_i, every element $h \in P$ and every $g \in C_P(h)$.

2.2. Notation. *Let p be and odd prime. If V is a simple $\mathbb{Q}P$-module and S is a genetic subgroup of P corresponding to V, we will write $\det_{N_P(S)/S}(g, V^h)$ for the element in $N_P(S)/S$ corresponding to $\det_K(g, V^h)$, where $K = \mathrm{End}_{\mathbb{Q}P}(V)$.*

2.3. Lemma. *Suppose p is an odd prime. Let V be a simple $\mathbb{Q}P$-module and S be a genetic subgroup of P corresponding to V. Take an element h in P and let $H = \langle h \rangle$. If g is in $C_P(H)$, let $[H\langle g \rangle \backslash P / N_P(S)]$ be a set of representatives of the double cosets of P on $H\langle g \rangle$ and $N_P(S)$. Then we have*

$$\det_{N_P(S)/S}\big(g,\, V^h\big) = \prod_{\substack{x \in [H\langle g \rangle \backslash P / N_P(S)] \\ s.t.\, H^x \cap N_P(S) \leqslant S}} \overline{l_{g,\,x}},$$

where $\overline{l_{g,x}}$ is determined as follows: the set $I_{g,x} = \langle g\rangle \cap \big(H\cdot{}^{x}N_P(S)\big)$ is actually a subgroup of $\langle g\rangle$. Let $m = |\langle g\rangle : I_{g,x}|$. Then g^m can be written as $g^m = h\cdot{}^{x}l_{g,x}$, for $h \in H$ and $l_{g,x} \in N_P(S)$; the element $l_{g,x}$ may not be unique, but its class $\overline{l_{g,x}}$ in $N_P(S)/S$ is, thanks to the conditions on x.

Proof. Set Φ for $\Phi_{N_P(S)/S}$. Let $[P/N_P(S)]$ be a set of representatives of the cosets of P in $N_P(S)$. Since $V \cong \mathrm{Indinf}_{N_P(S)/S}^{P}\Phi$, we can write it as $\bigoplus_{a\in[P/N_P(S)]} a\otimes\Phi$. The action of $y \in P$ is given by $y(a\otimes\omega) = ya\otimes\omega$, which is equal to $\tau_y(a)\otimes\overline{n_{y,a}}\omega$, if $ya = \tau_y(a)n_{y,a}$ for a corresponding $n_{y,a}$ in $N_P(S)$, with $\overline{n_{y,a}}$ being its class in $N_P(S)/S$.

If $y \in H$ fixes an element $u = \sum_{a\in[P/N_P(S)]} a\otimes\omega_a$ of V, we have

$$\sum_{a\in[P/N_P(S)]} \tau_y(a)\otimes\overline{n_{y,a}}\omega_a = \sum_{a\in[P/N_P(S)]} a\otimes\omega_a = \sum_{a\in[P/N_P(S)]} \tau_y(a)\otimes\omega_{\tau_y(a)}.$$

That is, for every $a \in [P/N_P(S)]$ we should have $\overline{n_{y,a}}\omega_a = \omega_{\tau_y(a)}$. If $\tau_y(a) = a$, then we should have that y is in $H\cap{}^{a}N_P(S)$ and that $H^a\cap N_P(S) \leqslant S$, if ω_a is different from zero. We consider then the set $[H\backslash P/N_P(S)]$ and we have that

$$u = \sum_{\substack{x\in[H\backslash P/N_P(S)]\\ s.t.\ H^x\cap N_P(S)\leqslant S}} \sum_{z\in[H/H\cap{}^{x}N_P(S)]} zx\otimes\omega_x.$$

This means that a $\mathbb{Q}$-basis for V^h is given by $\mu_{x,\omega} = \sum_{z\in[H/H\cap{}^{x}N_P(S)]} zx\otimes\omega$ with x running over $F = \{x \in [H\backslash P/N_P(S)] \mid H^x\cap N_P(S) \leqslant S\}$ and ω running over a $\mathbb{Q}$-basis of Φ. Since $\Phi \cong \mathbb{Q}(\zeta_r) \cong \mathrm{End}_{\mathbb{Q}P}(V)$, where ζ_r is a primitive p^r-th root of unity, if the order of $N_P(S)/S$ is p^r, then a $\mathbb{Q}(\zeta_r)$-basis of V^h is the set of $\mu_x = \mu_{x,1}$ with x running over F.

Now, for μ_x we have that $g\mu_x$ is equal to

$$\sum_{z\in[H/H\cap{}^{x}N_P(S)]} zh_{g,x}\sigma_g(x)\otimes\overline{n_{g,x}}\,1$$

if $gx = h_{g,x}\sigma_g(x)n_{g,x}$. That is

$$g\mu_{x,1} = h_{g,x}\mu_{\sigma_g(x),\overline{n_{g,x}}} = \mu_{\sigma_g(x),\overline{n_{g,x}}},$$

since $\mu_{\sigma_g(x),\overline{n_{g,x}}}$ is in V^h. So we can write $g\mu_x = \overline{n_{g,x}}\mu_{\sigma_g(x)}$, with $\overline{n_{g,x}}$ seen as an element in the field $\mathbb{Q}(\zeta_r)$. This implies that the action of g in V^h is given by a monomial matrix A, the coefficient in the non-zero entry of a row being $\overline{n_{g,x}}$. Then, the determinant of A is the product of the signature of the permutation σ_g by the product of the coefficients $\overline{n_{g,x}}$. Since p is odd, the signature is $+1$, and

$$\det(A) = \prod_{\substack{x\in[H\backslash P/N_P(S)] \\ s.t.\, H^x\cap N_P(S)\leqslant S}} \overline{n_{g,x}}.$$

Observe now that the group $H^x \cap N_P(S) \leqslant S$ does not change if we replace x by yx, for $y \in \langle g\rangle$, since g centralizes H. Moreover the intersection $I_{g,x} = \langle g\rangle \cap \big(H{\cdot}{}^x N_P(S)\big)$ is equal to $\langle g\rangle \cap \Big(H{\cdot}\big({}^x N_P(S) \cap C_P(H\langle g\rangle)\big)\Big)$, by Dedekind's modular law ([12], Hilfsatz 2.12.c), since g and H centralize H. Hence $I_{g,x}$ is a subgroup of $\langle g\rangle$. Now a set R of representatives of $H\backslash P/N_P(S)$ is the set of elements yx, where x is in a set of representatives of $H\langle g\rangle\backslash P/N_P(S)$, and y is in a set of representatives of $\langle g\rangle/I_{g,x}$. The set of elements y can be taken as $\{1, g, g^2, \ldots, g^{m-1}\}$. For $y = g^i$, with $0 \leqslant i \leqslant m-2$, we have $gyx = g^{i+1}x \in R$, so $n_{g,yx} = 1$. For $i = m-1$, we have $gyx = g^m x = h\cdot x\cdot l_{g,x}$.□

Our final version of Theorem 2.1 is the following.

2.4. Theorem. *Let p be an odd prime and P be a finite p-group. Take a set $\mathcal{C}$ of representatives of conjugacy classes of cyclic subgroups of P. For each $H \in \mathcal{C}$, let $\overline{E}_H$ be a generating set of the factor group $C_P(H)/H$ and $E_H \subseteq C_P(H)$ be a set of representatives of the classes $gH \in \overline{E}_H$. Let also $\mathcal{S}$ be a genetic basis of P and for each $S \in \mathcal{S}$, let $[H\langle g\rangle\backslash P/N_P(S)]$ be a set of representatives of the double cosets of P on $H\langle g\rangle$ and $N_P(S)$. Then*

$$Cl_1(\mathbb{Z}P) \cong \left(\prod_{S\in\mathcal{S}} \big(N_P(S)/S\big)\right)\Big/\mathcal{R},$$

where $\mathcal{R}$ is the subgroup generated by the elements $u_{H,g} = (u_{H,g,S})_{S\in\mathcal{S}}$, for $H \in \mathcal{C}$ and $g \in E_H$; for $S \in \mathcal{S}$, the component $u_{H,g,S}$ of $u_{H,g}$ is given by

$$u_{H,g,S} = \prod_{\substack{x\in[H\langle g\rangle\backslash P/N_P(S)] \\ s.t.\, H^x\cap N_P(S)\leqslant S}} \overline{l_{g,x}}, \qquad (\mathbf{2.5})$$

where $\overline{l_{g,x}}$ is the image in $N_P(S)/S$ of the element $l_{g,x} \in N_P(S)$ determined as follows: let m denote the index of $\langle g\rangle \cap \big(H{\cdot}{}^x N_P(S)\big)$ in $\langle g\rangle$. Then $g^m \in H{\cdot}{}^x N_P(S)$, so g^m can be written as $g^m = h.{}^x l_{g,x}$, for some $h \in H$ and $l_{g,x} \in N_P(S)$.

Proof. As we said at the beginning of the section, since p is odd, we have $Cl_1(\mathbb{Z}P) \cong \Gamma(P)/\mathcal{R}$, where

$$\Gamma(P) = \prod_{S \in \mathcal{S}} \big(N_P(S)/S\big)$$

and $\mathcal{R}$ is the subgroup generated by all the elements $u_{h,g} = (u_{h,g,S})_{S\in\mathcal{S}}$, with $g \in C_P(h)$ and $u_{h,g,S} = \det_{N_P(S)/S}\big(g, V(S)^h\big)$, where $V(S) = \mathrm{Indinf}_{N_P(S)/S}^P \Phi_{N_P(S)/S}$.

We first observe that $u_{h,g} = u_{{}^y h, {}^y g}$, for any $y \in G$. Indeed, setting $V = V(S)$, we have a commutative diagram

$$\begin{tikzcd} V^h \arrow[r, "g"] \arrow[d, "y"'] & V^h \arrow[d, "y"] \\ V^{{}^y h} \arrow[r, "{}^y g"] & V^{{}^y h} \end{tikzcd}$$

where the arrows are given by the actions of the labelling elements. It follows that the determinant of ${}^y g$ acting on $V^{{}^y h}$ is equal to the determinant of g acting on V^h. Hence to generate the subgroup $\mathcal{R}$ of $\Gamma(P)$, it suffices to take the elements $u_{h,g}$, where (h, g) runs through a set of representatives of conjugacy classes of pairs of commuting elements in P.

Now clearly for each $h \in H$, the map $g \mapsto u_{h,g}$ is a group homomorphism from $C_P(h)$ to $\Gamma(P)$, hence $\mathcal{R}$ is generated by the elements $u_{h,g}$, where $h \in P$ and g runs through a set of generators of $C_P(h)$. Moreover, as h acts as the identity on V^h, the group generated by h is contained in the kernel of this morphism.

Finally, by Lemma 2.3, setting $H = \langle h \rangle$, we have

$$u_{h,g,S} = \prod_{\substack{x \in [H\langle g\rangle \backslash P/N_P(S)] \\ s.t.\ H^x \cap N_P(S) \leqslant S}} \overline{l_{g,x}}$$

and this depends only on H, so we may denote it by $u_{H,g,S}$, and by $u_{H,g}$ the corresponding element of $\Gamma(P)$.

It follows that $\mathcal{R}$ is generated by the elements $u_{H,g}$, where H is a cyclic subgroup of P up to conjugation, and for a given H, the element g runs through a subset of $C_P(H)$ which, together with H, generates $C_P(H)$. Together with Lemma 2.1, this completes the proof. □

To finish the section, we observe that if N is a normal subgroup of a finite p-group P with p odd, then there is surjective deflation morphism

$$\mathrm{Def}_{P/N}^P : Cl_1(\mathbb{Z}P) \to Cl_1\big(\mathbb{Z}(P/N)\big).$$

2.6. Proposition. *Let p be an odd prime and P be a finite p-group. Suppose N is a normal subgroup of P. Let $\mathcal{S}$ be a genetic basis of P and $\mathcal{S}_N = \{S \in \mathcal{S} \mid N \leqslant S\}$. Let $\tilde{B}$ be the set of subgroups $\tilde{S} = S/N$ of $\tilde{P} = P/N$, for $S \in \mathcal{S}_N$.*

1. *The set $\{\tilde{S} \mid S \in \mathcal{S}_N\}$ is a genetic basis of $\tilde{P}$, and for $S \in \mathcal{S}_N$, the projection $P \mapsto \tilde{P}$ induces an isomorphism $\pi_S : N_P(S)/S \to N_{\tilde{P}}(\tilde{S})/\tilde{S}$.*
2. *The composition*

$$s : \Gamma(P) = \prod_{S\in\mathcal{S}} \big(N_P(S)/S\big) \longrightarrow \prod_{S\in\mathcal{S}_N} \big(N_P(S)/S\big) \xrightarrow{\prod \pi_S} \prod_{\tilde{S}\in\tilde{\mathcal{S}}} \big(N_{\tilde{P}}(\tilde{S})/\tilde{S}\big) = \Gamma(\tilde{P})$$

induces a surjective deflation morphism $\mathrm{Def}^P_{P/N} : Cl_1(\mathbb{Z}P) \to Cl_1\big(\mathbb{Z}(P/N)\big)$. In particular $Cl_1\big(\mathbb{Z}(P/N)\big)$ is isomorphic to a quotient of $Cl_1(\mathbb{Z}P)$.

Proof. For Assertion 1, it is clear from the definitions that if S/N is a genetic subgroup of P/N, then S is a genetic subgroup of P. Moreover the irreducible representation of P associated to S is obtained by inflation from P/N to P of the irreducible representation of P/N associated to S/N, up to the obvious isomorphism $\pi_S : N_P(S)/S \cong N_{\tilde{P}}(\tilde{S})/\tilde{S}$.

For Assertion 2, as the map $s : \Gamma(P) \to \Gamma(\tilde{P})$ is surjective, all we have to check is that the subgroup $\mathcal{R}$ of defining relations for $Cl_1(\mathbb{Z}P) \cong \Gamma(P)/\mathcal{R}$ is mapped by s inside the corresponding subgroup $\tilde{\mathcal{R}}$ of defining relations for $Cl_1(\mathbb{Z}\tilde{P}) \cong \Gamma(\tilde{P})/\tilde{\mathcal{R}}$. So let H be a cyclic subgroup of P, let $g \in C_P(H)$, and let $S \in \mathcal{S}_N$. Then $\tilde{H} = HN/N$ is cyclic, and $\tilde{g} = gN \in C_{\tilde{P}}(\tilde{H})$. Moreover the map

$$H\backslash P/N_P(S) \ni HxN_P(S) \mapsto \tilde{H}\tilde{x}N_{\tilde{P}}(\tilde{S}) \in \tilde{H}\backslash\tilde{P}/N_{\tilde{P}}(\tilde{S}),$$

where $\tilde{x} = xN \in \tilde{P}$, is a bijection, since $HxN_P(S) = HxNN_P(S) = HNxN_P(S)$ as $N_P(S) \geqslant S \geqslant N$. Hence we may identify the sets of representatives $[H\backslash P/N_P(S)]$ and $[\tilde{H}\backslash\tilde{P}/N_{\tilde{P}}(\tilde{S})]$ via this map. Moreover

$$H^x \cap N_P(S) \leqslant S \iff (HN)^x \cap N_P(S) \leqslant S \iff \tilde{H}^{\tilde{x}} \cap N_{\tilde{P}}(\tilde{S}) \leqslant \tilde{S}.$$

Now, for $x \in [H\backslash P/N_P(S)]$ such that $H^x \cap N_P(S) \leqslant S$, the equality $gx = h_{g,x}\sigma_g(x)n_{g,x}$, where $h_{g,x} \in H$, $\sigma_g(x) \in [H\backslash P/N_P(S)]$, and $n_{g,x} \in N_P(S)$, implies $\tilde{g}\tilde{x} = \widetilde{h_{g,x}}\widetilde{\sigma_g(x)}\widetilde{n_{g,x}}$ in P/N. In other words $\pi_S\big(\overline{n_{g,x}}\big) = \overline{n_{\tilde{g},\tilde{x}}}$, that is $s(u_{H,g}) = u_{\tilde{H},\tilde{g}}$. This completes the proof. □

2.7. Remark. It is shown in [4] (where $\Gamma(P)$ is called the *genome* of P) that the map s is the deflation map in a structure of *biset functor* on Γ, but we will not need the corresponding additional operations of induction, restriction and inflation in this paper. It also follows from [4] that the deflation map $\mathrm{Def}^P_{P/N} : Cl_1(\mathbb{Z}P) \to Cl_1\big(\mathbb{Z}(P/N)\big)$ we obtain here is the same as the map given by Corollary 3.10 of [17].

3. Computing some Whitehead groups

As we noted in Section 1, the examples we will consider in this section are all finite p-groups with p odd that satisfy that the group $SK_1(\mathbb{Z}P)$ is equal to $Cl_1(\mathbb{Z}P)$. Hence, we will use Theorem 2.4 to calculate $Cl_1(\mathbb{Z}P)$. If P is abelian, Theorem 2.4 has a simpler expression, as it was already noted in Observation 1.13 of [18].

As we said in the introduction, to calculate the free rank of the Whitehead group of the groups in question, we will use Theorem 2.6 in [17]. We will also use Exercise 13.9 in Serre [20], which says that if G is a group of odd order and c is the number of irreducible non-isomorphic complex representations of G, then $(c+1)/2$ is the number of irreducible non-isomorphic real representations of G.

We introduce some notation that will be helpful in both of our examples.

3.1. Notation. *Let p be a prime. Suppose that W is a finite-dimensional vector space over the finite field $\mathbb{F}_p$. We denote by $S(W)$ the symmetric algebra of W and by $S^p(W)$ its homogeneous part of degree p. If $\psi : W \to \mathbb{F}_p$ is a linear functional, the map*

$$w_1 \otimes_{\mathbb{F}_p} \ldots \otimes_{\mathbb{F}_p} w_n \in W^{\otimes n} \mapsto \psi(w_1)\ldots\psi(w_n) \in \mathbb{F}_p$$

induces a well defined linear functional $S(W) \to \mathbb{F}_p$, that we denote by $A \mapsto A(\psi)$.

The choice of a basis $\{x_1, \ldots, x_k\}$ of W over $\mathbb{F}_p$ yields a standard identification of $S(W)$ with the polynomial ring $\mathbb{F}_p[x_1, \ldots, x_k]$.

With such an identification, if $A = A(x_1, \ldots, x_k) \in S(W)$ and ψ is a linear form on W, then $A(\psi) = A\big(\psi(x_1), \ldots, \psi(x_k)\big)$. In particular $A(\psi) = 0$ for all ψ if and only if the polynomial function associated to A is equal to zero, that is if $A(r_1, \ldots, r_k) = 0$ for any $(r_1, \ldots, r_k) \in \mathbb{F}_p^k$: indeed since $\{x_1, \ldots, x_k\}$ is a basis of W, for any such k-tuple $(r_1, \ldots, r_k) \in \mathbb{F}_p^k$, there is a unique linear form ψ on W such that $\psi(x_i) = r_i$ for $1 \leqslant i \leqslant k$.

3.2. Elementary abelian p-groups.

3.3. Lemma. *Let p be an odd prime and P be an elementary abelian p-group of rank k, the free rank of $Wh(P)$ is equal to*

$$\frac{(p^k-1)(p-3)}{2(p-1)}.$$

Proof. The number of non-isomorphic irreducible $\mathbb{R}$-representations of P is $(p^k+1)/2$. On the other hand, the number of non-isomorphic irreducible $\mathbb{Q}$-representations of P is equal to $(p^k+p-2)/(p-1)$, since the genetic basis for P is given by all its subgroups of index p plus P itself. The result follows from Theorem 2.6 in [17]. □

The description of SK_1 for elementary abelian groups appeared first in Alperin et al. [1]. We prove this result using our combinatorial approach with genetic bases. Our proof has some similarities with the one in [1], but makes no use of characters. It will also be useful when dealing with extra-special p-groups.

3.4. Lemma. *Let p be a prime and let W be a finite-dimensional vector space over $\mathbb{F}_p$. For x and y in W, we set $B_{x,y} = x^{p-1}y \in S^p(W)$. Then $S^p(W)$ is generated by the elements $B_{x,y}$ with x and y running over W.*

Proof. Recall that if $x_1, \ldots, x_m$ are m (not necessarily different) commuting variables, then for any n

$$(x_1 + \cdots + x_m)^n = \sum_{\substack{\alpha_1,\ldots,\alpha_m \text{ s.t.} \\ \alpha_1+\cdots+\alpha_m=n}} \frac{n!}{\alpha_1! \cdots \alpha_m!} x_1^{\alpha_1} \cdots x_m^{\alpha_m}.$$

This allows us to show that for any n

$$\sum_{\emptyset \neq A \subseteq \{1,\ldots,n\}} (-1)^{n-|A|} \left(\sum_{i \in A} x_i \right)^n = n!\, x_1 \cdots x_n, \tag{3.5}$$

and so if p is prime, then

$$\sum_{\emptyset \neq A \subseteq \{1,\ldots,p-1\}} (-1)^{p-1-|A|} \left(\sum_{i \in A} x_i \right)^{p-1} x_p = (p-1)!\, x_1 \cdots x_p,$$

which by Wilson's Lemma gives

$$\sum_{\emptyset \neq A \subseteq \{1,\ldots,p-1\}} (-1)^{p-|A|} \left(\sum_{i \in A} x_i \right)^{p-1} x_p = x_1 \cdots x_p,$$

that is

$$\sum_{\emptyset \neq A \subseteq \{1,\ldots,p-1\}} (-1)^{p-|A|} B_{\sum\limits_{i\in A} x_i, x_p} = x_1 \cdots x_p. \tag{3.6}$$

This completes the proof, by taking $x_1, \ldots, x_p \in W = S^1(W)$, which indeed commute in $S(W)$. $\square$

3.7. Theorem. *[Theorem 2.4 in [1]] Let p be an odd prime and P be an elementary abelian p-group of rank k, then $SK_1(\mathbb{Z}P)$ is isomorphic to $(C_p)^N$ where*

$$N = \frac{p^k - 1}{p - 1} - \binom{p + k - 1}{p}.$$

Proof. As we said before, the genetic basis of P consists of P itself and all its subgroups of index p, so $SK_1(\mathbb{Z}P)$ is isomorphic to the quotient of

$$\Gamma(P) = \prod_{[P:Q]=p} (P/Q)$$

by the subgroup generated by the elements $u_{x,y}$ for x, y in P, where

$$(u_{x,y})_Q = \begin{cases} yQ & \text{if } x \in Q \\ 1 & \text{otherwise.} \end{cases}$$

On the other hand, we can see P as a vector space over $\mathbb{F}_p$, and for each subgroup Q of index p, i.e. for each hyperplane Q of P, consider $\psi_Q : P \to \mathbb{F}_p$, a linear functional with kernel Q. The product of these ψ_Q induces an isomorphism from $\Gamma(P)$ to

$$V = \prod_{[P:Q]=p} \mathbb{F}_p,$$

and the elements $u_{x,y}$ can be seen as

$$(u_{x,y})_Q = \begin{cases} \psi_Q(y) & \text{if } x \in Q \\ 0 & \text{otherwise.} \end{cases}$$

We define a morphism $r : S^p(P) \to V$, sending $A \in S^p(P)$ to the vector whose Q-component is equal to $A(\psi_Q)$. We will show that $\mathrm{Im}(r)$ is equal to the subspace of V generated by the elements $u_{x,y}$, and that r is injective. This will give us the result.

We show first that the elements $u_{x,y}$ are in $\mathrm{Im}(r)$. For x, $y \in P$, let $B_{x,y} = x^{p-1}y \in S^p(P)$. Then

$$B_{x,y}(\psi_Q) = \psi_Q(x)^{p-1}\psi_Q(y) = \begin{cases} 0 & \text{if } x \in Q \\ \psi_Q(y) & \text{otherwise} \end{cases}$$

since $\lambda^{p-1} = 1$ if λ is in $\mathbb{F}_p - \{0\}$ and $0^{p-1} = 0$. In particular $B_{y,y}(\psi_Q) = \psi_Q(y)$ for all $y \in P$, thus $r(B_{y,y} - B_{x,y}) = u_{x,y}$.

On the other hand, by Lemma 3.4, $S^p(P)$ is generated by the elements $B_{x,y}$ where x and y run through P, so we have that $\mathrm{Im}(r)$ is contained in (hence equal to) the subspace of V generated by the elements $u_{x,y}$.

Finally, we prove that r is injective. Let A be in the kernel of r, then $A(\psi_Q) = 0$ for every Q of index p in P. If ψ is any other linear functional of P with kernel Q, then there exists $\lambda \in \mathbb{F}_p$ such that $\psi = \lambda\psi_Q$, and so $A(\psi) = \lambda^p A(\psi_Q) = 0$, since A is homogeneous of degree p. Choosing a basis of P over $\mathbb{F}_p$ as in Notation 3.1, we can view A as a homogeneous polynomial of degree p, and the polynomial function A is zero. It remains to see that A is actually the zero polynomial, but this follows from Lemma 2.1 of [1]. □

3.8. Corollary. *Let p be an odd prime, and P be a finite p-group. If $|P/\Phi(P)| = p^k$, then $SK_1(\mathbb{Z}P)$ has a subquotient isomorphic to $(C_p)^N$, where*

$$N = \frac{p^k - 1}{p - 1} - \binom{p + k - 1}{p},$$

and in particular $SK_1(\mathbb{Z}P) \neq 0$ if $k \geqslant 3$.

Proof. Indeed $Cl_1\big(\mathbb{Z}\big(P/\Phi(P)\big)\big) \cong (C_p)^N$, for $N = \frac{p^k-1}{p-1} - \binom{p+k-1}{p}$, by Theorem 3.7. Moreover, this group is a quotient of $Cl_1(\mathbb{Z}P)$, by Proposition 2.6. Finally $Cl_1(\mathbb{Z}P)$ is a subgroup of $SK_1(\mathbb{Z}P)$, and $N > 0$ if $k \geqslant 3$. □

3.9. Extra-special and almost extra-special p-groups.

We begin by finding a genetic basis of an (almost) extra-special p-group.

3.10. Proposition. *Let p be a prime and P be an (almost) extra-special p-group. A genetic basis of P is given by all its subgroups of index p, together with P and a subgroup Y of maximal order such that $Y \cap Z(P) = \mathbf{1}$. In particular P has a unique faithful rational irreducible representation, up to isomorphism.*

Proof. We abbreviate $Z(P)$ by Z.

By theorems 1.7 and 1.8, the subgroups of P of index 1 or p are genetic and are not linked modulo $\frown_P$. They clearly intersect Z non-trivially. On the other hand, any genetic subgroup $S \neq P$ which intersects Z non-trivially must have index p, since $P' \leqslant S$ and so the cyclic group $P/S \cong (P/P')/(S/P')$, should have order p. This implies that if there is another group in $\mathcal{S}$, it must intersect Z trivially.

Let $Y \leqslant P$ be of maximal order with the property $Y \cap Z = \mathbf{1}$. By Lemma 1.18, we have that $C_P(Y) = N_P(Y) = YZ$. In particular $N_P(Y) \trianglelefteq P$ and $N_P(Y)/Y \cong Z$ is a

Roquette group. Then Y is genetic, by Remark 1.12. Also, by Lemma 1.18, we have that if $Y_1 \leqslant P$ is a group such that $Y_1 \cap Z = \mathbf{1}$, but it is not maximal order with this property, then $C_P(Y_1) = N_P(Y_1)$, but $N_P(Y_1)/Y_1$ is not cyclic. Thus Y_1 is not a genetic subgroup of P.

Finally, if Y is a subgroup of P of maximal order such that $Y \cap Z = \mathbf{1}$, then Y has $|P/YZ| = |Y|$ distinct conjugates in P, by Lemma 1.18. These conjugates are subgroups of index p in the elementary abelian group YP', and they all intersect trivially (that is, they don't contain) the group P'. Since there are exactly $|Y|$ subgroups of YP' not containing P', these subgroups are exactly the conjugates of Y in P.

Now if Y_0 is another subgroup of P such that $Y_0 \cap Z = \mathbf{1}$, then $Y_0 \cap YP'$ is a subgroup of YP' which does not contain P'. Hence it is contained in some conjugate of Y, and there exists $x \in P$ such that $Y_0 \cap YP' \leqslant Y^x$. It follows that $Y_0 \cap YZ \leqslant Y^x$, for YP' is the subgroup of YZ consisting of elements of order at most p. In other words

$$ {}^xY_0 \cap Z_P(Y) = {}^xY_0 \cap YZ = {}^x(Y_0 \cap YZ) \leqslant Y. $$

Now if Y_0 is another subgroup of maximal order such that $Y_0 \cap Z = \mathbf{1}$, exchanging the roles of Y and Y_0 in the previous argument shows that there also exists an element $y \in P$ such that ${}^yY \cap Y_0Z \leqslant Y_0$. By Theorem 1.8, it follows that $Y_0 \frown_P Y$. The last assertion now follows from Lemma 1.10. □

As a first consequence of this result we have.

3.11. Lemma. *Let p be an odd prime, and n be a positive integer.*

1. *Let P be an extra-special p-group of order p^{2n+1}. Then the free rank of $Wh(P)$ is equal to*
$$ \frac{(p^{2n} + p - 2)(p - 3)}{2(p - 1)}. $$
2. *Let P be an almost extra-special group of order p^{2n+2}. Then the free rank of $Wh(P)$ is equal to*
$$ \frac{(p^{2n+1} + p^2 + p + 1)(p - 3) + 8}{2(p - 1)}. $$

Proof. The free rank of $Wh(P)$ is equal to $r - q$, where r (resp. q) is the number of irreducible real (resp. rational) representations of P, up to isomorphism. In general, for a finite p-group P and a field K of characteristic 0, the irreducible representations of P over K can be recovered from the knowledge of a genetic basis $\mathcal{B}$ of P (see [2]): this is because the functor R_K of representations of p-groups over K is *rational* in the sense of Definition 10.1.3 of [7], as can be easily deduced from Theorem 10.6.1 of [7]. A proof of this fact can also be found in [8]. In particular, the number $l_K(P)$ of such representations, up to isomorphism, is equal to

$$l_K(P) = \sum_{S \in \mathcal{B}} \partial l_K\big(N_P(S)/S\big),$$

where $\partial l_K(Q)$ denotes the number of *faithful* irreducible representations of a p-group Q over K, up to isomorphism. For a Roquette p-group Q, we have moreover $\partial l_K(Q) = 1$ if $Q = \mathbf{1}$, and $\partial l_K(Q) = l_K(Q) - l_K(Q/Z)$ otherwise, where Z is the unique central subgroup of order p of Q.

If p is odd, all the groups $N_P(S)/S$, for $S \in \mathcal{B}$, are cyclic. Now for $Q = C_{p^m}$, with $m \geqslant 0$, we have

$$l_{\mathbb{R}}(Q) = \frac{p^m + 1}{2} \;\text{ and }\; l_{\mathbb{Q}}(Q) = m + 1.$$

It follows that $\partial l_{\mathbb{R}}(Q) = \frac{p^m - p^{m-1}}{2}$ if $m > 0$, and $\partial l_{\mathbb{R}}(Q) = 1$ if $m = 0$. On the other hand $\partial l_{\mathbb{Q}}(Q) = 1$ for any m.

In case P is extra-special of order p^{2n+1}, the genetic basis obtained in Proposition 3.10 consists of the group $S = P$, for which $N_P(S)/S$ is trivial, of $\frac{p^{2n}-1}{p-1}$ subgroups S of index p in P, for which $N_P(S)/S \cong C_p$, and the subgroup $S = Y$, for which $N_P(S)/S \cong Z(P) \cong C_p$. This gives

$$r = l_{\mathbb{R}}(P) = 1 + \frac{p^{2n} - 1}{p-1}\frac{p-1}{2} + \frac{p-1}{2} = \frac{p^{2n} + p}{2},$$

and

$$q = l_{\mathbb{Q}}(P) = 1 + \frac{p^{2n} - 1}{p-1} + 1 = \frac{p^{2n} + 2p - 3}{p-1}.$$

In case P is almost extra-special of order p^{2n+2}, the genetic basis obtained in Proposition 3.10 consists of the group $S = P$, for which $N_P(S)/S$ is trivial, of $\frac{p^{2n+1}-1}{p-1}$ subgroups S of index p in P, for which $N_P(S)/S \cong C_p$, and the subgroup $S = Y$, for which $N_P(S)/S \cong Z(P) \cong C_{p^2}$. This gives

$$r = l_{\mathbb{R}}(P) = 1 + \frac{p^{2n+1} - 1}{p-1}\frac{p-1}{2} + \frac{p^2 - p}{2} = \frac{p^{2n+1} + p^2 - p + 1}{2},$$

and

$$q = l_{\mathbb{Q}}(P) = 1 + \frac{p^{2n+1} - 1}{p-1} + 1 = \frac{p^{2n+1} + 2p - 3}{p-1}.$$

This completes the proof. $\square$

To calculate $Cl_1(\mathbb{Z}P)$ we will need the following result.

3.12. Lemma. *Let p be an odd prime. Let W be a vector space over $\mathbb{F}_p$ of finite dimension k, which is endowed with a bilinear, alternating form $b : W \times W \to \mathbb{F}_p$. Suppose that the rank of b is not equal to 2.*

For x and y in W, we still set $B_{x,y} = x^{p-1}y \in S^p(W)$. Then we have

$$S^p(W) = \langle B_{x,y} \mid x,\, y \in W \text{ s.t. } b(x,\, y) = 0\rangle.$$

Proof. We will write $\mathcal{O}$ for $\langle B_{x,y} \mid x,\, y \in W \text{ s.t. } b(x,\, y) = 0\rangle$. We will prove that $B_{x,y} \in \mathcal{O}$ for *any* $x, y \in W$, and by Lemma 3.4, it will follow that $S^p(W) = \mathcal{O}$.

Observe that, since $B_{x,y} \in \mathcal{O}$ for an $x, y \in W$ with $b(x, y) = 0$, it follows from formula 3.6 that $x_1x_2 \ldots x_{p-1}y \in \mathcal{O}$ for any elements $x_1, \ldots, x_{p-1}$ of W such that $b(x_i, y) = 0$ for $1 \leqslant i \leqslant p-1$.

If $b = 0$, there is nothing to prove. Otherwise let $x, y \in W$ such that $b(x, y) \neq 0$. Since $B_{x,\lambda y} = \lambda B_{x,y}$ for $\lambda \in \mathbb{F}_p$, to prove that $B_{x,y} \in \mathcal{O}$, we can assume without loss of generality that $b(x, y) = 1$, up to replacing y by a suitable scalar multiple. If the restriction of b to $\langle x, y\rangle^\perp$ was identically 0, then $\langle x, y\rangle^\perp$ would be precisely the radical of b, so b would have rank 2, contradicting our assumption. Hence we can find $z, t \in \langle x, y\rangle^\perp$ such that $b(z, t) \neq 0$, and up to replacing t by some scalar multiple, we can assume that $b(z, t) = 1$.

Now let $\alpha \in \mathbb{F}_p$, and set $u = \alpha x + t$ and $v = y + \alpha z$. Then

$$b(u, v) = \alpha b(x, y) + \alpha^2 b(x, z) + b(t, y) + \alpha b(t, z) = 0,$$

since $b(x, y) = 1 = -b(t, z)$ and $b(x, z) = 0 = b(t, y)$.

It follows that $B_{u,v} \in \mathcal{O}$. But $B_{u,v}$ is equal to

$$(\mathbf{3.13}) \quad (\alpha x + t)^{p-1}(y + \alpha z) = \sum_{i=0}^{p-1} \binom{p-1}{i} \alpha^i x^i y t^{p-1-i} + \sum_{i=0}^{p-1} \binom{p-1}{i} \alpha^{i+1} t^{p-1-i} z x^i.$$

By the observation at the beginning of the proof, the element $x^i y t^{p-1-i}$ is in $\mathcal{O}$ whenever $p-1-i > 0$, since $b(x, t) = b(y, t) = b(t, t) = 0$. Similarly $t^{p-1-i}zx^i \in \mathcal{O}$ if $i > 0$, since $b(t, x) = b(z, x) = b(x, x) = 0$. It follows that in (3.13), the only elements possibly not in $\mathcal{O}$ correspond to $p - 1 - i = 0$ in the first summation and to $i = 0$ in the second. Hence

$$\alpha^{p-1}x^{p-1}y + \alpha t^{p-1}z \in \mathcal{O},$$

and this holds for any $\alpha \in \mathbb{F}_p$. For $\alpha = 1$, this gives $x^{p-1}y + t^{p-1}z \in \mathcal{O}$, and for $\alpha = -1$, this gives $x^{p-1}y - t^{p-1}z \in \mathcal{O}$. It follows that $x^{p-1}y \in \mathcal{O}$, as was to be shown. □

3.14. Remark. If the rank of b is equal to 2, then the result of Lemma 3.12 is no longer true: for example in the non-degenerate case, that is when W has dimension 2, saying that $b(x, y) = 0$ for $x \neq 0$ is equivalent to saying that y is a scalar multiple of x. In this case $\mathcal{O}$ is the subspace of $S^p(W)$ generated by the elements x^p, for $x \in W$. So $\mathcal{O}$ has dimension 2, whereas $S^p(W)$ has dimension $p+1$.

We now come to our main theorem, describing the structure of $Cl_1(\mathbb{Z}P)$ when P is an extra-special or almost extra-special p-group for p odd. We first recall that Oliver ([17] Example 7 page 16) showed that if P is extra-special of order p^3, then $Cl_1(\mathbb{Z}P) \cong (C_p)^{p-1}$, and that if P is almost extra-special of order p^4, then $Cl_1(\mathbb{Z}P) \cong (C_p)^{(p^2+p-2)/2}$. Hence in what follows, we may assume that P is an extra-special group of order at least p^5, or an almost extra-special p-group of order at least p^6.

3.15. Notation. Let p be an odd prime and n be a positive integer. Let P be an extra-special p-group of order p^{2n+1} or an almost extra-special p-group of order p^{2n+2}. Let Z denote the center of P, and $N = P' \leqslant Z$ be the Frattini subgroup of P. Let Y be a subgroup of P of maximal order such that $Y \cap Z = \mathbf{1}$, as in Proposition 3.10. Recall that Y is elementary abelian. In any case, the group P can be written as a semidirect product $P = X \cdot Y$, where $X \geqslant Z$ is an abelian normal subgroup of P with $C_P(X) = X$ and $Y \cap X = \mathbf{1}$:

- If P is extra-special of exponent p, the group X is equal to $C \times X_0$, for some subgroup $X_0 \cong (C_p)^n$ and $C = N = Z$.
- If P is extra-special of exponent p^2, the group X is equal to $C \times X_0$, for some subgroup $X_0 \cong (C_p)^{n-1}$, some subgroup $C \cong C_{p^2}$, and $N = Z < C$.
- If P is almost extra-special, then $X = C \times X_0$, for some subgroup $X_0 \cong (C_p)^n$, and $N < Z = C \cong C_{p^2}$.

So in all cases we have $X = C \times X_0$, for some cyclic subgroup $C \geqslant Z \geqslant N$.

Moreover the subgroup Y is elementary abelian of order p^n. It is maximal subject to the condition $Y \cap Z = \mathbf{1}$, so by Proposition 3.10, we have a genetic basis of P consisting of P itself, its subgroups of index p, and Y. The normalizer $N_P(Y)$ is equal to $Z \cdot Y$, so

$$\Gamma(P) \cong \Big(\prod_{[P:Q]=p} (P/Q) \Big) \times Z.$$

3.16. Theorem. *Let p be an odd prime, and let P be an extra-special p-group of order at least p^5, or an almost extra-special p-group of order at least p^6. Let $N = P'$ be the Frattini subgroup of P, and Z be the center of P. Then there is a split sequence of* *abelian groups*

$$0 \longrightarrow K \longrightarrow Cl_1(\mathbb{Z}P) \xrightarrow{\mathrm{Def}^P_{P/N}} Cl_1\big(\mathbb{Z}(P/N)\big) \longrightarrow 0,$$

where K is cyclic, isomorphic to a quotient of Z. In particular $Cl_1(\mathbb{Z}P)$ is isomorphic to $K \times (C_p)^M$, where K is cyclic of order dividing p^2, and $M = \frac{p^{k-1}-1}{p-1} - \binom{p+k-2}{p}$ if $|P| = p^k$.

Proof. The product $\prod\limits_{[P:Q]=p} (P/Q)$ identifies with $\Gamma(P/N)$, and we have a surjective projection map $\mathrm{Def}^P_{P/N} : \Gamma(P) \to \Gamma(P/N)$, with kernel isomorphic to Z. By Proposition 2.6, this map induces a surjective deflation map

$$\mathrm{Def}^P_{P/N} : Cl_1(\mathbb{Z}P) = \Gamma(P)/\mathcal{R} \to Cl_1\big(\mathbb{Z}(P/N)\big) = \Gamma(P/N)/\overline{\mathcal{R}},$$

where $\mathcal{R}$ is the subgroup of $\Gamma(P)$ generated by the elements $u_{H,g}$ introduced in Theorem 2.4, and H is a cyclic subgroup of P with $g \in C_P(H)$. Similarly $\overline{\mathcal{R}}$ is the corresponding subgroup of $\Gamma(P/N)$ generated by the elements $u_{F,c}$, where F is a cyclic subgroup of P/N and $c \in P/N$ (we always have $c \in C_{P/N}(F)$, as P/N is abelian).

The proof of Theorem 2.6 shows that $\mathrm{Def}^P_{P/N}(u_{H,g}) = u_{HN/N,gN}$. Conversely, if F is a cyclic subgroup of P/N, generated by f, and if $c \in P/N$, then there exists a pair (H, g) of a cyclic subgroup H of P and an element $g \in C_P(H)$ such that $HN/N = F$ and $gN = c$ if and only if $b(f, c) = 0$, where b is the bilinear alternating form on P/N with values in $\mathbb{F}_p$ induced by taking commutators in P. Our assumptions on P imply that the rank of b is not 2, so we can apply Lemma 3.12. This shows that the subspace of $\Gamma(P/N)$ generated by the elements $u_{F,c}$, where $F = \langle f\rangle$ for $f \in P/N$, and $c \in P/N$ such that $b(f, c) = 0$, generate $S^p(P/N) = \overline{\mathcal{R}}$, by Lemma 3.4. It follows that $\mathrm{Def}^P_{P/N}$ induces a *surjective* map $e : \mathcal{R} \to \overline{\mathcal{R}}$. Let L denote the kernel of this map. We have a commutative diagram with exact rows

$$\begin{tikzcd}
0 \arrow[r] & L \arrow[r] \arrow[d, "l"] & \mathcal{R} \arrow[r, "e"] \arrow[d, "i"] & \overline{\mathcal{R}} \arrow[r] \arrow[d, "j"] & 0 \\
0 \arrow[r] & Z \arrow[r] & \Gamma(P) \arrow[r, "\mathrm{Def}^P_{P/N}"] & \Gamma(P/N) \arrow[r] & 0
\end{tikzcd}$$

where the vertical maps i and j are the inclusion maps. The Snake's Lemma now shows that the map l is injective, and moreover we have an exact sequence of cokernels

$$0 \longrightarrow K \longrightarrow Cl_1(\mathbb{Z}P) \xrightarrow{\mathrm{Def}^P_{P/N}} Cl_1\big(\mathbb{Z}(P/N)\big) \longrightarrow 0, \tag{3.17}$$

where $K = Z/l(L)$. Since the kernel Z of $\mathrm{Def}^P_{P/N}$ corresponds to the component of $\Gamma(P)$ indexed by Y, the image $l(L)$ is generated by the components $w_Y \in N_P(Y)/Y \cong Z$ of vectors w in the kernel of the deflation map $e : \mathcal{R} \to \overline{\mathcal{R}}$. Hence $l(L)$ is a subgroup of the group generated by all the elements $u_{H,g,Y}$, where H is a cyclic subgroup of P and $g \in C_P(H)$.

It remains to see that the exact sequence 3.17 splits. To see this, consider the completed diagram

$$\begin{tikzcd}
 & 0 \arrow[d] & 0 \arrow[d] & 0 \arrow[d] & \\
0 \arrow[r] & L \arrow[r] \arrow[d, "l"] & \mathcal{R} \arrow[rr, "e"] \arrow[d, "i"] & & \overline{\mathcal{R}} \arrow[r] \arrow[d, "j"] & 0 \\
0 \arrow[r] & Z \arrow[r] \arrow[d] & \Gamma(P) \arrow[rr, "c"] \arrow[d, "a"] & & \Gamma(P/N) \arrow[r] \arrow[d, shift left, "b"] \arrow[ll, dashed, bend left, "t"] & 0 \\
0 \arrow[r] & K \arrow[r] \arrow[d] & Cl_1(\mathbb{Z}P) \arrow[rr, "d"] \arrow[d] & & Cl_1\big(\mathbb{Z}(P/N)\big) \arrow[r] \arrow[d] \arrow[u, dashed, shift left, "s"] & 0, \\
 & 0 & 0 & & 0 &
\end{tikzcd}$$

where a and b are the projection maps, and c, d are the respective deflation maps, and e is the restriction of c to $\mathcal{R}$. The map b is split surjective, because $\Gamma(P/N)$ and $Cl_1\big(\mathbb{Z}(P/N)\big)$ are both elementary abelian. Similarly, the map c is split surjective by construction. Let s be a section of b and let $t : \Gamma(P/N) \to \Gamma(P)$ be a section of c. Then

$$d \circ a \circ t \circ s = b \circ c \circ t \circ s = b \circ s = \mathrm{Id},$$

so the map $a \circ t \circ s$ is a section of d. To complete the proof, observe that K is a isomorphic to a quotient of Z, and that Z is cyclic of order p or p^2. □

3.18. Remark. It follows from this proof that to obtain a minimal set $\mathcal{M}$ of generators of $Cl_1(\mathbb{Z}P)$, we can take a subset $(v_S)_{S\in\mathcal{S}}$ of the canonical basis of $\Gamma(P/N)$ (as $\mathbb{F}_p$-vector space), corresponding to a set $\mathcal{S}$ of subgroups of index p of P, which maps by b to a basis of $Cl_1\big(\mathbb{Z}(P/N)\big)$. Then v_S is a generator of the component $P/S \cong (P/N)\big/(S/N)$ of $\Gamma(P)$, for $S \in \mathcal{S}$. If K is trivial[3], we set $\mathcal{T} = \mathcal{S}$. Otherwise, we also choose a generator v_Y of $Z \cong N_P(Y)/Y$, and we set $\mathcal{T} = \mathcal{S} \sqcup \{Y\}$. Then we take for $\mathcal{M}$ the image in $Cl_1(\mathbb{Z}P)$ by the projection map a of the set $\{v_S \mid S \in \mathcal{T}\}$.

[3]This will occur only in Assertion 1 of Proposition 3.22 below, i.e. when P is extra-special of order p^5 and exponent p^2

As we can see from this procedure, the splitting of the exact sequence of Theorem 3.16 is *not* canonical: first we have made a choice for the genetic subgroup Y, and then we also make a choice of a set $\mathcal{S}$ and of generators v_S, for $S \in \mathcal{T}$.

We now come to the proof of Theorem A, which we split in two parts: first the "generic" case, when the group P is large enough, and then two special cases of "small" groups of order p^5 and p^6. The generic case is the following one.

3.19. Theorem. *Let p be an odd prime, and let P be a p-group of order p^k which is either:*

1. *extra-special of exponent p with $k \geqslant 5$, or*
2. *extra-special of exponent p^2 with $k \geqslant 7$, or*
3. *almost extra-special with $k \geqslant 8$.*

Then $Cl_1(\mathbb{Z}P)$ is (non-canonically) isomorphic to $Z \times (C_p)^M$, where Z is the center of P (so $Z \cong C_p$ in cases 1 and 2, and $Z \cong C_{p^2}$ in case 3), and $M = \frac{p^{k-1}-1}{p-1} - \binom{p+k-2}{p}$.

Proof. We keep Notation 3.15 throughout. We know from Theorem 3.16 that $Cl_1(\mathbb{Z}P) \cong K \times (C_p)^M$, where $M = \frac{p^{k-1}-1}{p-1} - \binom{p+k-2}{p}$.

Moreover the group K is isomorphic to the quotient of Z by the subgroup generated by the elements w_Y, where w is an element in the kernel of the deflation map $e : \mathcal{R} \to \overline{\mathcal{R}}$. Such an element w_Y is a product of elements $u_{H,g,Y}$, for some pairs (H, g) of a cyclic subgroup H of P, and an element $g \in C_P(H)$. We start by computing $u_{H,g,Y}$ for such a pair (H, g), using formula 2.5. We will show that $u_{H,g,Y} = 1$ in the cases of the statement of the theorem, and it will follow that $K \cong Z$. We have

$$u_{H,g,Y} = \prod_{x \in D} \overline{l_{g,\,x}}$$

where D is a chosen set of representatives of those double cosets $H\langle g\rangle x N_P(Y)$ in P for which $H^x \cap N_P(Y) \leqslant Y$. For each $x \in D$, if m_x is the index of $\langle g\rangle \cap \big(H \cdot {}^{x}N_P(Y)\big)$ in $\langle g\rangle$, the element g^{m_x} can be written $g^{m_x} = h_x \cdot {}^{x}l_{g,x}$, for $h_x \in H$ and $l_{g,x} \in N_P(Y)$. Since $N_P(Y) = ZY$ is a normal subgroup of p, by Lemma 1.18, the group $H \cdot {}^{x}N_P(Y)$ and the integer m_x do not depend on x. Let m denote this integer. Since $g^p \in Z$ for any $g \in P$, we have $m = 1$ if $g \in HZY$, and $m = p$ otherwise.

Since $H\langle g\rangle ZY$ is also a normal subgroup of P, we have $H\langle g\rangle tZY = H\langle g\rangle ZYt = tH\langle g\rangle ZY$, for any $t \in P$. Hence D is a subset of a set of representatives of $P/H\langle g\rangle ZY$. If D is empty, we have $u_{H,g,Y} = 1$, so we can assume $D \neq \emptyset$. If $H^t \cap ZY \leqslant Y$, then $H^t \cap Z \leqslant Y \cap Z = \mathbf{1}$. Then $H \cap Z = \mathbf{1}$, so H has order 1 or p, since $h^p \in Z$ for any $h \in P$.

- If $H \cap ZY = \mathbf{1}$ then $H^t \cap ZY = (H \cap ZY)^t = \mathbf{1}$ for any $t \in P$, so our set D is a set of representatives of $P/H\langle g\rangle ZY$.
- If $H \cap ZY \neq \mathbf{1}$, then $H \leqslant ZY$. If there exists $t_0 \in P$ with $H^{t_0} \cap ZY \leqslant Y$, we have $H^{t_0} \leqslant Y$, and up to replacing H by H^{t_0}, we can assume $H \leqslant Y$. Then for $t \in P$, we have $H^t \cap ZY = H^t$, and $H^t \leqslant Y$ implies $[H, H^t] \leqslant Z \cap Y = \mathbf{1}$. In other words $H^t \cap ZY \leqslant Y$ if and only if $t \in C_P(H)$. Here D is a set of representatives of $C_P(H)/H\langle g\rangle ZY = C_P(H)/\langle g\rangle ZY$.

So in each case, there are subgroups M and Q of P with $ZY \leqslant M \leqslant Q$ such that D is a set of representatives of Q/M.

We have $g^m = h{\cdot}z{\cdot}y$, for some $h \in H$, $z \in Z$ and $y \in Y$. Observe that $z = g^p$ and $h = y = 1$ if $m = p$. Then for $x \in D$, we have $g^m = h{\cdot}z{\cdot}{}^x(y^x) = h{\cdot}{}^x(z[y,x]y)$, so with the identification $N_P(Y)/Y \cong Z$, we have $l_{g,x} = z[y,x]$. It follows that $u_{H,g,Y} = \prod\limits_{x\in D}\big(z[y,x]\big) = z^{|D|}[y, \prod\limits_{x\in D} x]$. Now the commutator $[y, \prod\limits_{x\in D} x]$ only depends of the images of y and $\prod\limits_{x\in D} x$ in the elementary abelian group P/N. As $M \geqslant N$, the map $x \mapsto \overline{x} = xN$ is a bijection from Q/M to $\overline{Q}/\overline{M}$, where $\overline{Q} = Q/N$ and $\overline{M} = M/N$. The subgroup $\overline{M}$ admits a supplement W in the elementary abelian group $\overline{Q}$, and W is a set of representatives of $\overline{Q}/\overline{M}$. Since $\sum\limits_{w\in W} w = 0$ as p is odd, it follows that $\prod\limits_{x\in D} x$ maps to 0 in P/N, that is $\prod\limits_{x\in D} x \in N \leqslant Z$, and $[y, \prod\limits_{x\in D} x] = 1$. This gives finally

$$(\mathbf{3.20}) \qquad u_{H,g,Y} = \begin{cases} z^{|D|} & \text{if } g \in HzY \text{ for some } z \in Z, \\ g^{p|D|} & \text{otherwise.} \end{cases}$$

- If P is extra-special of order p^{2l+1}, with $l \geqslant 2$, then Y has order p^l and Z has order p.
  - As we said, if $g \in HzY$, for $z \in Z$, we have $u_{H,g,Y} = z^{|D|}$. If $H \nleqslant ZY$, then

    $$|D| = |P : H\langle g\rangle ZY| = |P : HZY| \geqslant p^{2l+1}/(p{\cdot}p{\cdot}p^l) = p^{l-1}.$$

    Now if we assume $H \leqslant Y$, then $g \in HZY = ZY$, and

    $$|D| = |C_P(H) : \langle g\rangle ZY| = [C_P(H) : ZY| \geqslant p^{2l}/p^{l+1} = p^{l-1}$$

    again. For $l \geqslant 2$, this is a multiple of $p = |Z|$, and $u_{H,g,Y} = 1$.
  - If $g \notin HZY$, then $u_{H,g,Y} = g^{p|D|}$. So $u_{H,g,Y} = 1$ unless g has order p^2, and then g^p generates Z. If $H \nleqslant ZY$, then

    $$|D| = |P : H\langle g\rangle ZY| = |P : H\langle g\rangle Y| \geqslant p^{2l+1}/p{\cdot}p^2{\cdot}p^l = p^{l-2}.$$

On the other hand, if $H \leqslant Y$, then

$$|D| = |C_P(H) : \langle g\rangle ZY| = |C_P(H) : \langle g\rangle Y| \geqslant p^{2l}/p^2{\cdot}p^l = p^{l-2}$$

again. Hence $|D|$ is a multiple of p if $l \geqslant 3$, so $u_{H,g,Y} = 1$.

So $u_{H,g,Y} = 1$ if P is extra-special, unless possibly if P has exponent p^2 and order p^5.

• If P is almost extra-special of order p^{2l+2}, with $l \geqslant 2$, then Y has order p^l and Z is cyclic of order p^2.

- If $g \in HzY$, for $z \in Z$, then $u_{H,g,Y} = z^{|D|}$. If $H \nleqslant ZY$, we have

$$|D| = |P : H\langle g\rangle ZY| = |P : HZY| \geqslant p^{2l+2}/(p{\cdot}p^2{\cdot}p^l) = p^{l-1}.$$

  If we now assume $H \leqslant Y$, then $g \in HZY = ZY$, and

$$|D| = |C_P(H) : \langle g\rangle ZY| = |C_P(H) : ZY| \geqslant p^{2l+1}/p^2{\cdot}p^l = p^{l-1}$$

  again. Hence then $|D|$ is a multiple of p^2 if $l \geqslant 3$, so $u_{H,g,Y} = 1$.

- If $g \notin HZY$, then $u_{H,g,Y} = g^{p|D|}$. If $H \nleqslant ZY$, since $\langle g\rangle Z$ has order at most p^3 as $g^p \in Z$, we have

$$|D| = |P : H\langle g\rangle ZY| \geqslant p^{2l+2}/p{\cdot}p^3{\cdot}p^l = p^{l-2},$$

  If we now assume $H \leqslant Y$, then

$$|D| = |C_P(H) : \langle g\rangle ZY| \geqslant p^{2l+1}/p^3{\cdot}p^l = p^{l-2}$$

  again. Hence then $|D|$ is a multiple of p if $l \geqslant 3$, and $u_{H,g,Y} = g^{p|D|} = 1$.

So $u_{H,g,Y} = 1$ if P is almost extra-special, unless possibly if P has order p^6. □

So we are left with the special cases where P is either extra-special of order p^5 and exponent p^2, or almost extra-special of order p^6. In both cases, we will use the next lemma, where the notation is again as in 3.15.

3.21. Lemma. *Let P be extra-special of order p^5 and exponent p^2, or almost extra-special of order p^6. Then there exist $a \in X_0$ and $b \in Y$ with the following properties:*

1. *The elements a and b both have order p, and centralize C.*
2. *The group $U = \langle a, b\rangle$ is extra-special of order p^3 and exponent p. Its center is equal to N.*

3. *For $\alpha \in \{0, \ldots, p-1\}$, set $H_\alpha = \langle ab^\alpha \rangle$. Also set $H_\infty = \langle b \rangle$, and denote by $\mathbb{L}$ the set $\{0, \ldots, p-1, \infty\}$. Then $\langle H_\alpha, H_\beta \rangle = U$ for any pair (α, β) of distinct elements of $\mathbb{L}$, and the map $\alpha \in \mathbb{L} \mapsto H_\alpha N$ is a bijection from $\mathbb{L}$ to the set of subgroups of order p^2 of U.*

Proof. In both cases $Y \cong (C_p)^2$. Since $[C, Y] \leqslant Z \leqslant C$, the group Y normalizes C, and $C_Y(C) \neq \mathbf{1}$ since the automorphism group of C is cyclic. We choose a non trivial element b of $C_Y(C)$. Then b does not centralize X_0, for otherwise b centralizes $CX_0 = X$, contradicting $C_P(X) = X$. Hence we can choose $a \in X_0$ such that $[a, b] \neq 1$. Then the group $U = \langle a, b \rangle$ is extra-special of order p^3 and exponent p, as a and b have order p and $[a, b]$ generates N. In particular N is equal to the center of U.

The groups H_α, for $\alpha \in \mathbb{L}$, all have order p, and are different from N. So the groups $H_\alpha N$ are subgroups of order p^2 of U. Clearly $\langle H_\alpha, H_\beta \rangle = U$ for any distinct element α, β of $\mathbb{L}$, hence the subgroups $H_\alpha N$, for $\alpha \in \mathbb{L}$, are all distinct. This completes the proof, as U has exactly $p + 1 = |\mathbb{L}|$ subgroups of order p^2. □

We now proceed with the proof of the above mentioned two special cases.

3.22. Proposition.

1. *Let P be extra-special of order p^5 and exponent p^2. Then the group K of Theorem 3.16 is trivial.*
2. *Let P be almost extra-special of order at least p^6. Then the group K of Theorem 3.16 has order p.*

Proof. We keep the notation of Lemma 3.21.
1) Suppose first that P is extra-special of order p^5 and exponent p^2. Then we have $X = C \times X_0$, where $C \cong C_{p^2}$ contains the center $Z = N$ of order p of P, and $X_0 \cong C_p$. On the other hand $Y \cong (C_p)^2$ in this case. We will build an element w in the kernel of $e : \mathcal{R} \to \overline{\mathcal{R}}$ with non trivial component $w_Y \in Z$. Then w_Y will generate Z, so K will be trivial in this case, as stated.

In order to build w, we first fix a generator g of C. Next we consider the set $\mathbb{L}$ and the subgroups H_α of $C_P(C) = C_P(g)$, for $\alpha \in \mathbb{L}$, introduced in Lemma 3.21. We now set

$$w = (u_{\mathbf{1},g})^{-1} \prod_{\alpha \in \mathbb{L}} u_{H_\alpha, g}.$$

For an arbitrary cyclic subgroup H of $C_P(g)$, the component $u_{H,g,S}$ of $u_{H,g}$ at a genetic subgroup S of P is given by Formula 2.5. When $|P : S| = p$, this formula comes down to

$$u_{H,g,S} = \begin{cases} 1 & \text{if } H \not\leqslant S, \\ \overline{g} & \text{otherwise,} \end{cases}$$

where $\overline{g}$ is the image of g in P/S. It follows that the component w_S of w at S is equal to $(\overline{g})^{-1+n_S}$, where $n_S = |\{\alpha \in \mathbb{L} \mid H_\alpha \leqslant S\}|$. Then either $S \geqslant U = \langle a, b\rangle$, and $S \geqslant H_\alpha$ for all $\alpha \in \mathbb{L}$, so $n_S = p+1$, and $w_S = (\overline{g})^p = 1$, since P/S has order p; or $S \ngeqslant U$, and then $S \cap U$ is a subgroup of index p of U. So $|S \cap U| = p^2$, and $S \cap U = H_\alpha Z$ for a unique $\alpha \in \mathbb{L}$. Hence $H_\alpha \leqslant S$, and $H_\beta \nleqslant S$ for $\beta \in \mathbb{L} - \{\alpha\}$. It follows that $n_S = 1$ in this case, so $w_S = (\overline{g})^{-1+1} = 1$ again. This shows that w is in the kernel of the map $e : \mathcal{R} \to \overline{\mathcal{R}}$.

We now compute the component w_Y of w indexed by Y, using 3.20: we consider a cyclic subgroup H of order at most p of $C_P(g)$. Then $g \notin HZY$, because HZY has exponent p. Then $u_{H,g,Y} = g^{p|D|}$, where D is a set of representatives of those double cosets $H\langle g\rangle tZY$ such that $H^t \cap ZY \leqslant Y$.

We know moreover that $|D| = |P : H\langle g\rangle ZY| = |P : HCY|$ if $H \nleqslant ZY$, since $Z \leqslant C = \langle g\rangle$, and that $|D| = |C_P(H) : \langle g\rangle ZY| = |C_P(H) : CY|$ if $H \leqslant Y$.

If $H = \mathbf{1}$, then $|D| = |P|/(|C||Y|) = p^5/(p^2{\cdot}p^2) = p$, so $u_{H,g,Y} = g^{p^2} = 1$. If $H = H_\alpha$, for $\alpha \in \mathbb{L} - \{\infty\}$, then $|D| = |P : H_\alpha CY| = p^5/(p{\cdot}p^2{\cdot}p^2) = 1$, for $H_\alpha \nleqslant CY$. Then $u_{H_\alpha,g,Y} = g^p$. Finally, if $H = H_\infty$, we have $|D| = |C_P(H_\infty) : CY| = p^4/(p^2{\cdot}p^2) = 1$, so $u_{H_\alpha,g,Y} = g^p$ again.

This gives $w_Y = 1^{-1} \prod_{\alpha\in\mathbb{L}} g^p = g^{p(p+1)} = g^p$, and g^p is a generator of Z. So we have indeed built an element w in the kernel of $e : \mathcal{R} \to \overline{\mathcal{R}}$ such that the component w_Y generates Z. It follows that the group K is trivial in this case, as claimed.

2) Suppose now that P is almost extra-special of order p^6. Then we have $C = Z \cong C_{p^2} > P' = N$. In this case, let $g \in P$ and H be a subgroup of order 1 or p of $C_P(H)$, Equation 3.20 shows that $u_{H,g,Y}$ is equal to $(v_{H,g})^{|D|}$ for some $v_{H,g} \in Z$, where D is a set of representatives of double cosets $H\langle g\rangle tZY$ such that $H^t \cap ZY \leqslant Y$. We claim that $u_{H,g,Y} \in N$. Indeed, if $g \notin HZY$, then $v_{H,g} = g^p \in N$. So we can assume that $g \in HZY$. Then if $H \nleqslant ZY$, we have $|D| = |P : H\langle g\rangle ZY| = |P : HZY| \geqslant p^6/(p{\cdot}p^2{\cdot}p^2) = p$. If $H \leqslant Y$, then $g \in HZY = ZY$, and $|D| = |C_P(H) : ZY| \geqslant p^5/(p^2{\cdot}p^2) = p$. In both cases $|D|$ is a multiple of p, so $u_{H,g,Y} = (v_{H,g})^{|D|} \in N$ again, as claimed.

As in the proof of Assertion 1, we will build an element w in the kernel of $e : \mathcal{R} \to \overline{\mathcal{R}}$ such that w_Y generates N. This will show that $K \cong Z/N \cong C_p$, as claimed. We first choose a generator g of $Z = C$. The formal definition of w is then the same as in the proof of Assertion 1:

$$w = (u_{\mathbf{1},g})^{-1} \prod_{\alpha\in\mathbb{L}} u_{H_\alpha,g}.$$

The computation of the component w_S for a subgroup S of index p of P is also very similar to what we did for Assertion 1: for a subgroup S of index p of P, we have $w_S = (\overline{g})^{-1+n_S}$, where $n_S = |\{\alpha \in \mathbb{L} \mid H_\alpha \leqslant S\}|$. We have $n_S = 1$ or $n_S = p+1$, thus

$w_S = 1$, and w lies in the kernel of $e : \mathcal{R} \to \overline{\mathcal{R}}$.

As for the component w_Y of w, we observe that $u_{H,g,Y} = g^{|D|}$ since $g \in Z$, where D is as above. If $H = \mathbf{1}$, then $|D| = |P : ZY| = p^2$, and $u_{\mathbf{1},g,Y} = g^{|P:ZY|} = g^{p^2} = 1$. For $\alpha \in \mathbb{L} - \{\infty\}$, we have $|D| = |P : H_\alpha\langle g\rangle ZY| = |P/H_\alpha ZY| = p^6/p{\cdot}p^2{\cdot}p^2 = p$, so $u_{H_\alpha,g,Y} = g^p$. Finally, for $H = H_\infty \leqslant Y$, we have $|D| = |C_P(H_\infty) : \langle g\rangle ZY| = |C_P(H_\infty) : ZY| = p^5/(p^2{\cdot}p^2) = p$, so $u_{H_\infty,g,Y} = g^p$ again.

It follows that $w_Y = 1^{-1}(g^p)^{p+1} = g^{p^2+p} = g^p$, so w_Y generates N, as was to be shown. □

References

[1] R. C. Alperin, R. K. Dennis, R. Oliver, and M. R. Stein. SK_1 of finite abelian groups, II. *Invent. Math.*, 87:253–302, 1987.

[2] L. Barker. Genotypes of irreducible representations of finite p-groups. *Journal of Algebra*, 306:655–681, 2007.

[3] D. J. Benson. *Representations and cohomology II*, volume 31 of *Cambridge studies in advanced mathematics*. Cambridge University Press, 1991.

[4] S. Bouc. K-theory, genotypes, and p-biset functors. In preparation.

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

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

[7] S. Bouc. *Biset functors for finite groups*. Springer, Berlin, 2010.

[8] S. Bouc. Fast decomposition of p-groups in the Roquette category, for $p > 2$. In *RIMS Kôkyûroku*, volume 1872, pages 113–121, 2014. arXiv:1403.6092.

[9] S. Bouc and N. Mazza. The Dade group of (almost) extraspecial p-groups. *Journal of Pure and Applied Algebra*, 192:21–51, 2004.

[10] J. F. Carlson and J. Thévenaz. Torsion endo-trivial modules. *Algebras and Representation Theory*, 3:303–335, 2000.

[11] K. Doerk and T. Hawkes. *Finite soluble groups*. Walter de Gruyter, Berlin, 1992.

[12] B. Huppert, *Endliche Gruppen I*, Springer-Verlag Berlin Heidelberg New York, Die Grundlehren der mathematischen Wissenschaften, vol. 134, 1967.

[13] The GAP Group. *GAP – Groups, Algorithms, and Programming, Version 4.8.5*, 2016. (`http://www.gap-system.org`).

[14] D. Gorenstein. *Finite groups.* Chelsea Publishing, New York, 1968.

[15] J. Guaschi, D. Juan-Pineda, and S. Millán López. The lower algebraic K-theory of the braid groups of the sphere. Preprint, arXiv:1209.4791, 2012.

[16] J.-F. Lafont, B. A. Magurn, and I. J. Ortiz. Lower algebraic K-theory of certain reflection groups. *Proceedings of the Cambridge Philosophical Society*, 148:193–226, 2010.

[17] R. Oliver. *Whitehead groups of finite groups.* Cambridge University Press, U.K., 1988.

[18] N. Romero. Computing Whitehead groups using genetic bases. *Journal of algebra*, 450:646–666, 2016.

[19] P. Roquette. Realisierung von Darstellungen endlicher nilpotenter Gruppen. *Arch. Math.*, 9:241–250, 1958.

[20] J.-P. Serre. *Linear representations of finite groups.* Springer-Verlag, New York, 1977.

[21] F. Ushitaki. $SK_1(\mathbb{Z}[G])$ of finite solvable groups which act linearly and freely on spheres. *Osaka Journal of Mathematics*, 28(1):117–127, 1991.

[22] F. Ushitaki. A generalization of a theorem of Milnor. *Osaka Journal of Mathematics*, 31:430–415, 1994.

[23] J. H. C. Whitehead. Simple homotopy types. *American Journal of Mathematics*, 72:1–57, 1950.

Serge Bouc, CNRS-LAMFA, 33 rue St Leu, 80039, Amiens, France.
`serge.bouc@u-picardie.fr`

Nadia Romero, DEMAT, UGTO, Jalisco s/n, Mineral de Valenciana, 36240, Guanajuato, Gto., Mexico.
`nadia.romero@ugto.mx`