THE EPICENTER OF SPECIAL P-GROUPS OF RANK 2

MARCIN MAZUR

1. Introduction

A p-group P is called **special of rank** k if its center is elementary abelian of rank k and coincides with the commutator $[P, P]$. Special p-groups of rank 1 are called extraspecial. A group is called **capable** if it is isomorphic to a quotient of another group by its center. The **epicenter** of a group is the smallest subgroup of its center quotient by which is capable. The epicenter of extraspecial p-groups is well understood: it coincides with the center unless the group has exponenet p and order p^3 (see, for example, [2]). Capable special groups of rank 2 have been recently investigated by H. Heineken, L-C. Kappe, and R. Morse (unpublished), who obtained some partial results towards classifying them. An old result of Heineken [4] is that such p-groups have order p^5, p^6, or p^7. Heineken, Kappe, and Morse were able to classify such $p-$groups of order p^5 and stated some expectations about groups of order p^6 and p^7 supported by computations with GAP. However, their approach has been rather ad hoc and it has not seem to extend to settle the problem in general.

The goal of this work is to develope a more conceptual approach to the investigation of the epicenter of special groups in general, with main focus on special p-groups of rank 2 . In particular, we describe all capable special p-groups of rank 2 for odd primes p.

The main tools for our approach are developed in sections 2 and 3. In particular, of key importance are Proposition 3.9 and Theorem 3.10, which reduce questions about the epicenter to linear algebra problems. In section 4 we classify capable special p=groups of rank 2 which are powerful. Section 5 focuses on groups of exponent p. We show that grpoups of class 2 and exponent p are closely related to vector spaces equipped with an alternating bilinear map. This allows us to prove the following result (Theorem 5.7): *if G is a capable p-group of nilpotency class 2 with commutator* *elementary abelian of rank k, then the rank of $G/Z(G)$ is at most $2k+\binom{k}{2}$.* This result has been conjectured by Heineken and Nikolova, who proved it for groups of exponent p [5]. We show how to reduce the general case to the case of exponent p. Next we focus on the epicenter of special p-groups of rank 2 and exponenet p. We show that most of them are unicentral (i.e. have epicenter equal to the center) and classify those which are cabable and those which have epicenter of order p (see Theorem 5.1). This result is based on the very interesting work of R. Scharlau [8], who classified indecomposable objects in the category of finite dimensional vector spaces equipped with a pair of bilinear alternating forms. Even though some of our results (in particular, the description of capapble special p-groups of rank 2 and exponenet p) could have been obtained by a more ad-hoc methods, we believe that Scharlau's work is the right way to approach special p-groups of rank 2 and exponenet p (in a similarl way as the calssical theory of alternating forms is the right tool to undrstand extraspecial p-groups).

2. The epicenter

For elements a, b of a group G we write $[a, b] = a^{-1}b^{-1}ab$ and $a^b = b^{-1}ab$.

Recall that a group G is called *capable* if it is isomorphic to the group of inner automorphisms of some group H, i.e. $G \cong H/Z(H)$.

Definition 2.1. Let $G \cong F/R$ be a free presentation of G. The corresponding short exact sequence

$$1 \longrightarrow R/[F,R] \longrightarrow F/[F,R] \xrightarrow{\psi} G \longrightarrow 1$$

is a central extension. The image $\psi(Z(F/[F,R]))$ is a central subgroup of G called the *epicenter* and is denoted by $Z^*(G)$.

Note that the central extension in Definition 2.1 depends upon a choice of presentation and hence it is not unique. Nevertheless, the epicenter is a characteristic subgroup of G independent of any choice of presentation. A link between the epicenter and capability is established in the following result.

Theorem 2.2 ([1])**.** *The epicenter $Z^*(G)$ is the smallest central subgroup of G whose factor group is capable. In particular, G is capable if and only if $Z^*(G) = 1$.*

Another characterization of the epicenter is given by

Theorem 2.3 ([6], Cor. 2.5.8)**.** *$Z^*(G)$ is the intersection of all subgroups of the form $f(Z(E))$, where $f : E \longrightarrow G$ is a surjective homomorphism with $\ker f \subseteq Z(E)$.*

Consider now a free presentation $G = F/R$. Let T be the subgroup of F such that $Z(G) = T/R$. The map $F/R[F,F] \times T/R \longrightarrow (R \cap [F,F])/[F,R]$, given by $(xR[F,F], yR) \mapsto [x,y][F,R]$, is a well defined bilinear map. Since $G/[G,G] = F/R[F,F]$ and $Z(G) = T/R$, we get a homomorphism $\lambda : G/[G,G] \otimes Z(G) \longrightarrow (R \cap [F,F])/[F,R]$.

Remark 2.4. When G is a finite group then $(R \cap [F,F])/[F,R]$ is isomorphic to the Schur multiplier $M(G)$. It is a result of Ganea that in this case the image $\lambda(G/[G,G] \otimes Z)$ coincides with the kernel of the natural map $M(G) \longrightarrow M(G/Z)$, for any central subgroup Z of G.

Theorem 2.5. *An element $z \in Z(G)$ belongs to the epicenter $Z^*(G)$ if and only if $G/[G,G] \otimes z$ is contained in the kernel of λ. The following elements of $G/[G,G] \otimes Z(G)$ belong to the kernel of λ:*

(i) *$g[G,G] \otimes g^k$, for any $g \in G$ and any integer k such that $g^k \in Z(G)$;*
(ii) *$a[G,G] \otimes b$, for any $a \in Z(G)$ and $b \in [G,G] \cap Z(G)$;*
(iii) *$a[G,G] \otimes [b,c] + b[G,G] \otimes [c,a] + c[G,G] \otimes [a,b]$, for any $a,b,c \in G$ such that the elements $[a,b],[b,c],[c,a]$ are in $Z(G)$.*

Proof. Note that $Z(F/[F,R]) \subseteq T/[F,R]$. For any $y \in T$, we have $y[F,R] \in Z(F/[F,R])$ if and only if $[x,y] \in [F,R]$ for all $x \in F$. In other words, $z \in Z(G)$ is of the form $z = yR$ for some $y[F,R] \in Z(F/[F,R])$ if and only if $G/[G,G] \otimes z$ is contained in the kernel of λ. This proves the first part of the theorem.

If $g = xR$ then $\lambda(g[G,G] \otimes g^k) = [x, x^k][F,R] = [F,R]$, which proves (i).

Under the assumptions of (ii), we have $a = xR$ and $b = yR$ for some $x \in T$ and $y \in [F,F] \cap T$. Since $[T,[F,F]] \subseteq [F,R]$, we have $\lambda(a[G,G] \otimes b) = [x,y][F,R] = [F,R]$. This proves (ii).

Finally, (iii) is a consequence of the Hall-Witt identity

$$[[x,y],z^x][[z,x],y^z][[y,z],x^y] = 1$$

applied to $a = xR$, $b = yR$, $c = zR$.

□

Corollary 2.6. *Let n, m be the exponents of $G/[G,G]$ and $G/Z(G)[G,G]$ respectively and let $a \in Z(G)$. Then $a^n \in Z^*(G)$ and if, in addition, $a \in [G,G]$ then $a^m \in Z^*(G)$.*

3. p-groups of nilpotency class 2

We start by recalling the following property of groups of nilpotency class 2.

Lemma 3.1. *Let G be a group of nilpotency class 2. Then for any a and b in G and any integer n we have*

$$(ab)^n = a^n b^n [b,a]^{\binom{n}{2}}; \tag{1}$$

$$[a^n, b] = [a, b^n] = [a,b]^n. \tag{2}$$

□

Proposition 3.2. *Let G be a p-group of nilpotency class 2. Suppose that for some $k \in \mathbb{N}$ the group G^{p^k} is nontrivial and cyclic, and either p is odd and $\exp([G,G])$ divides p^k, or $p = 2$ and $\exp([G,G])$ divides p^{k-1}. Then elements of order p in G^{p^k} belong to $Z^*(G)$. In particular, G is not capable.*

Proof. Increasing k if necessary, we may assume that G^{p^k} is cyclic of order p with a generator c. Clearly c is central and we claim that it belongs to the epicenter of G. Let $g \in G$ be any element such that $g^{p^k} \neq 1$. Then $g^n = c$ for some n divisible by p^k. Hence $g[G,G] \otimes c \in \ker\lambda$ by (i) of Theorem 2.5.

Fix now $g \in G$ such that $g^{p^k} \neq 1$. If $h^{p^k} = 1$ then $(gh)^{p^k} = g^{p^k}$ by (1). It follows that both $g[G,G] \otimes c$ and $(gh)[G,G] \otimes c$ are in $\ker\lambda$, and therefore so is $h[G,G] \otimes c$. This proves that $G/[G,G] \otimes c \subseteq \ker\lambda$. □

Remark 3.3. The above proof shows that Proposition 3.2 remains true for any finite p-group G for which there is k such that that G^{p^k} is cyclic of order p and $(gh)^{p^k} \neq 1$ for any g, h such that $g^{p^k} \neq 1$ and $h^{p^k} = 1$. In particular, this provides a new proof of Proposition 4.3.5 on page 62 of [7].

In this work we are mainly interested in the following class of groups.

Definition 3.4. A finite p group G of nilpotency class 2 is called *special* if $[G, G] = Z(G)$ and $Z(G)$ is elementary abelian. The *rank* of a special p-group is the rank of its center.

In particular, special p-groups of rank one are usually called extra-special.

Lemma 3.5. *Let G be a p-group of nilpotency class 2. Then the following conditions are equivalent.*

(i) $G^p \subseteq Z(G)$*;*
(ii) $[G, G]$ *is an elementary abelian p-group;*
(iii) $\phi(G) \subseteq Z(G)$*, where $\phi(G)$ is the Frattini subgroup.*

Proof. Assume (i). Then $[x, y]^p = [x^p, y] = 1$ for any $x, y \in G$, so $[G, G]$ has exponent p. Since $[G, G] \subseteq Z(G)$, (ii) follows. Now assume (ii). Then for any $x, y \in G$ we have $[x^p, y] = [x, y]^p = 1$. Hence $G^p \subseteq Z(G)$ and $\phi(G) = [G, G]G^p \subseteq Z(G)$. Finally, (i) is trivially a consequence of (iii). □

Corollary 3.6. *Let G be a special p-group of rank k and order p^n. Then $\phi(G) = Z(G)$ and $d(G) = n - k$, where $d(G)$ is the minimal number of generators of G.*

Lemma 3.7. *Let G be a finite, non-cyclic p-group with a central subgroup Z such that G/Z is elementary abelian. Then $Z^*(G) \subseteq Z$.*

Proof. Since G is not cyclic, G/Z is an elementary abelian p-group of rank at least 2, hence it is capable. The result follows now from Theorem 2.2. □

Proposition 3.8. *Let G be a finite p-group of nilpotency class 2 and such that $G/[G, G]$ is elementary abelian. Then*

(i) *If G is capable then $Z(G)$ is elementary abelian.*
(ii) *If $Z(G)$ is elementary abelian then $G = H \times A$, where A is elementary abelian and H is a special p-group. For any such H and A we have $Z^*(G) = Z^*(H)$.*

Proof. Part (i) is an immediate consequence of Corolarry 2.6. Assume now that the center of G is elementary abelian. Then $Z(G) = [G, G] \times A$ for some group A. Let $\pi : G \longrightarrow G/[G, G]$ be the quotient map. Since $G/[G, G]$ is elementary abelian, we have $G/[G, G] = H/[G, G] \times \pi(A)$ for some subgroup H of G. Clearly $G = HA$ and $H \cap A =$

$[G,G] \cap A = 1$. This shows that $G = H \times A$. It is clear that $[H,H] = [G,G] = Z(H)$, so H is special. Both the epicenters of G and H are contained in $[G,G]$ by Lemma 3.7. Let $a \in [G,G]$, $a \notin Z^*(H)$. There is a surjective homomorphism $f : E \longrightarrow H$ such that $\ker f \subseteq Z(E)$ and $a \notin f(Z(E))$. Then $\phi = f \times \mathrm{id} : E \times A \longrightarrow H \times A = G$ is a surjective homomorphism and $\phi(Z(E \times A)) = \phi(Z(E)) \times A$ does not contain a. Thus $a \notin Z^*(G)$. This proves that $Z^*(G) \subseteq Z^*(H)$.

Suppose now that $a \in [G,G]$, $a \notin Z^*(G)$. There is a surjective homomorphism $\phi : E \longrightarrow H \times A$ such that $\ker \phi \subseteq Z(E)$ and $a \notin \phi(Z(E))$. Let $F = \phi^{-1}(H)$, $B = \phi^{-1}(A)$. Note that $[F,B] \subseteq \ker \phi \subseteq Z(E)$. Thus $[[B,F],F] = 1 = [[F,B],F]$. By the Hall-Witt identity, $[[F,F],B] = 1$. Since $Z(F) \subseteq \phi^{-1}(Z(H)) = \phi^{-1}([H,H]) = \ker \phi \cdot [F,F]$, we have $[Z(F),B] = 1$. Thus $Z(F) \subseteq Z(E)$, since $E = FB$. Hence $a \notin \phi(Z(F))$ and consequently $a \notin Z^*(H)$. This completes the proof of (ii).

□

Proposition 3.9. *Let G be a p-group of nilpotency class 2 such that $[G,G]$ is elementary abelian. Let Y be the subgroup of $G/Z(G) \otimes [G,G]$ generated by elements of the form $aZ(G) \otimes [b,c] + bZ(G) \otimes [c,a] + cZ(G) \otimes [a,b]$ with $a,b,c \in G$. If $c \in [G,G]$ is such that $G/Z(G) \otimes c \subseteq Y$ then $c \in Z^*(G)$.*

Proof. We have an exact sequence

$$Z(G)/[G,G] \otimes [G,G] \xrightarrow{\ \epsilon\ } G/[G,G] \otimes [G,G] \xrightarrow{\ \pi\ } G/Z(G) \otimes [G,G] \longrightarrow 0$$

Let X be be the subgroup of $G/[G,G] \otimes [G,G]$ generated by elements of the form $a[G,G] \otimes [b,c] + b[G,G] \otimes [c,a] + c[G,G] \otimes [a,b]$ with $a,b,c \in G$. Then $\pi(X) = Y$. It follows that $G/[G,G] \otimes c$ is contained in $X + \mathrm{im}(\epsilon)$. Let $j : G/[G,G] \otimes [G,G] \longrightarrow G/[G,G] \otimes Z(G)$ be the natural map. By (ii) and (iii) of Theorem 2.5 the group $j(X + \mathrm{im}(\epsilon))$ is contained in the kernel of the map λ of Theorem 2.5. It follows that $G/[G,G] \otimes c$ is contained in $\ker \lambda$ and therefore $c \in Z^*(G)$ again by Theorem 2.5. □

We can prove a stronger result when G is a p-group of nilpotency class 2 such that $G/[G,G]$ is elementary abelian. To this end, let $U_G = G/[G,G]$, $W_G = [G,G]$. Note that W_G is elementary abelian by Lemma 3.5. Thus we consider U_G, W_G as vector spaces over the field $\mathbb{F}_p$ of order p. Let $B_G : U_G \times U_G \longrightarrow W_G$ be defined by $B_G(a,b) = [g,h]$, where $a = g[G,G]$, $b = h[G,G]$. The identity $[gk,h] = [g,h]^k[k,h]$

implies that B_G is a well defined alternating bilinear map. We also define a map $f_G : U_G \longrightarrow W_G$ given by $f_G(a) = g^p$, where $a = g[G,G]$. This map is well defined and it is linear if $p \geq 3$. For $p = 2$, we have $f_G(a+b) = f_G(a) + f_G(b) + B_G(a,b)$. Now consider the space $U_G \otimes W_G$. Let X_B be the subspace spanned by the elements of the form $a \otimes B(b,c) + b \otimes B(c,a) + c \otimes B(a,b)$. Let X_f be the subspace spanned by all elements of the form $a \otimes f(a)$. Finally, let $X = X_B + X_f$.

Theorem 3.10. *Let G be a p-group of nilpotency class 2 such that $G^p \subseteq [G,G]$. An element $c \in Z(G)$ belongs to the epicenter $Z^*(G)$ if and only if $c \in [G,G]$ and $U_G \otimes c \subseteq X$.*

Proof. That $Z^*(G) \subseteq [G,G]$ follows by Lemma 3.7. That the condition $U_G \otimes c \subseteq X$ suffices to conclude that $c \in Z^*(G)$ follows by Theorem 2.5. The main part is to prove the sufficiency of this condition. In the notation of Theorem 2.5, it suffices to prove that X is the kernel of the map λ. This has been proved by Blackburn and Evans [3] and a detailed argument is given in [6, section 3.3]. □

Remark 3.11. As presented in [6, section 3.3], the result of Blackburn and Evans provides a nice way to compute the Schur multiplier of groups as in Theorem 3.10.

4. Capable powerful special p-groups of rank 2

The main result of this section is the following theorem, which classifies capable special p-groups G of rank 2 such that $[G,G] = G^p$ (which, for p odd, is equivalent to saying that G is powerful).

Theorem 4.1. *Let p be an odd prime, t a quadratic non-residue modulo p, and let G be a special $p-$group of rank 2 such that $G^p = [G,G]$. Then either $Z^*(G) = Z(G)$ or G is capable. Moreover, G is capable if and only if it is isomorphic to one of the following groups:*

(i) *Groups of order p^5:*

$$P_1 =< g,h,c : g^{p^2} = h^{p^2} = c^p = 1, [g,h] = h^p, [g,c] = 1, [h,c] = g^p >$$

$$P_2 =< g,h,c : g^{p^2} = h^{p^2} = c^p = 1, [g,h] = 1, [g,c] = h^p, [h,c] = g^p >$$

$$P_3 =< g,h,c : g^{p^2} = h^{p^2} = c^p = 1, [g,h] = 1, [g,c] = h^{tp}, [h,c] = g^p >$$

(ii) *Groups of order p^6:*

$$Q_1 =< g, h, c_1, c_2 : g^{p^2} = h^{p^2} = c_1^p = c_2^p = 1,$$

$$[g, h] = 1, [g, c_1] = g^p, [h, c_1] = h^{-p}, [g, c_2] = 1, [h, c_2] = g^p >$$

$$Q_2 =< g, h, c_1, c_2 : g^{p^2} = h^{p^2} = c_1^p = c_2^p = 1,$$

$$[g, h] = 1, [g, c_1] = g^p, [h, c_1] = h^{-p}, [g, c_2] = h^{-p}, [h, c_2] = g^p >$$

$$Q_3 =< g, h, c_1, c_2 : g^{p^2} = h^{p^2} = c_1^p = c_2^p = 1,$$

$$[g, h] = 1, [g, c_1] = g^p, [h, c_1] = h^{-p}, [g, c_2] = h^{-tp}, [h, c_2] = g^p >$$

(iii) *Groups of order p^7:*

$$R =< g, h, c_1, c_2, c_3 : g^{p^2} = h^{p^2} = c_1^p = c_2^p = c_3^p = 1,$$

$$[g, h] = 1, [g, c_1] = g^p, [h, c_1] = h^{-p}, [g, c_2] = 1, [h, c_2] = g^p, [g, c_3] = h^p, [h, c_3] = 1 > .$$

In order to prove the theorem we need several preparatory steps. Let then G be a special p-group of rank 2 such that $G^p = [G, G]$ (p an odd prime). As at the end of Section 3, set $U = G/[G, G]$, $W = [G, G] = Z(G) = G^p$. Thus U and W are vector spaces over $\mathbb{F}_p$ and W has dimension 2. Let $B : U \times U \longrightarrow W$ be given by $B(a, b) = [g, h]$, where $a = g[G, G]$, $b = h[G, G]$. Then B is a non-degenerate alternating bilinear map whose image spans W. This, in particular, implies that $\dim U \geq 3$. Finally, let $f : U \longrightarrow W$ be given by $f(a) = g^p$, where $a = g[G, G]$. Thus f is a surjective linear map. Recall that X_f is the subspace of $U \otimes W$ spanned by elements of the form $a \otimes f(a)$, where $a \in U$. The subspace X_B of $U \otimes W$ is spanned by all elements of the form $a \otimes B(b, c) + b \otimes B(c, a) + c \otimes B(a, b)$, and $X = X_f + X_B$.

The following lemma is straightforward.

Lemma 4.2. *Let $x, y, z \in U$ be linearly dependent. Then $x \otimes B(y, z) + y \otimes B(z, x) + z \otimes B(x, y) = 0$.*

Since f is surjective, we may choose $v, w \in U$ such that $a = f(v), b = f(w)$ is a basis of W.

Lemma 4.3. *The subspace X_f of $U \otimes W$ has codimension 1 and it is spanned by $\ker f \otimes W$ and the elements $v \otimes a$, $w \otimes b$, and $v \otimes b + w \otimes a$.*

Proof. Clearly, $v \otimes a$ and $w \otimes b$ are contained in X_f. Note that if $u \in \ker f$ then $(v+u) \otimes a$ and $(w+u) \otimes b$ are in X_f. It follows that $u \otimes a$, $u \otimes b$ are contained in X_f. This means that $\ker f \otimes W \subseteq X_f$. Any element $x \in U$ can be expressed as $rv + sw + u$ for some $r, s \in \mathbb{F}_p$ and $u \in \ker f$. Thus $x \otimes f(x) = r^2 v \otimes a + s^2 w \otimes b + rs(v \otimes b + w \otimes a) + u \otimes f(x)$. This shows that X_f is spanned by $\ker f \otimes W$ and the elements $v \otimes a$, $w \otimes b$, and $v \otimes b + w \otimes a$. In particular, X_f has codimension 1 in $U \otimes W$ □

Proposition 4.4. *Either $Z^*(G) = Z(G)$ or G is capable. Furthermore, G is capable if and only if the following conditions hold:*

(i) *B is trivial on* $\ker f \times \ker f$*;*
(ii) *$v \otimes B(u, w) + w \otimes B(v, u) \in X_f$ for every $u \in \ker f$.*

Proof. By Lemma 4.3, there is no $c \in W$ such that $U \otimes c \subseteq X_f$. If $X_B \subseteq X_f$ then $X = X_f$ and G is capable by Theorem 3.10. If X_B is not contained in X_f then $X = U \otimes W$ and $Z^*(F) = Z(F)$, again by Theorem 3.10. This proves the first part of the proposition. For the second part, note that we have just proved that capability of G is equivalent to the condition $X_B \subseteq X_f$.

Suppose first that $X_B \subseteq X_f$. Consider $x, y \in \ker f$ and let $B(x, y) = ra + sb$ for some $r, s \in \mathbb{F}_p$. Then $v \otimes (ra + sb) + x \otimes B(y, v) + y \otimes B(v, x)$ is in X_B. As $\ker f \otimes W \subseteq X_f$ and $v \otimes a \in X_f$, we see that $sv \otimes b \in X_f$. Thus $s = 0$ by Lemma 4.3. Similarly, we show that $r = 0$. It follows that B is trivial on $\ker f \times \ker f$. Since for any $u \in \ker f$ we have $v \otimes B(u, w) + w \otimes B(v, u) + u \otimes B(w, v) \in X_B$ and $u \otimes W \subseteq X_f$, we see that (ii) holds.

Conversely, suppose that the conditions (i) and (ii) hold. We need to prove that $L(z_1, z_2, z_3) = z_1 \otimes B(z_2, z_3) + z_2 \otimes B(z_3, z_1) + z_3 \otimes B(z_1, z_2) \in X_f$ for any three elements z_1, z_2, z_3 in U. Since L is trilinear, it suffices to prove this when each z_i is from the set $\{v, w\} \cup \ker f$. By Lemma 4.2 we may assume that the z_1, z_2, z_3 are distinct. If at least two of the z_i are in $\ker f$, then $L(z_1, z_2, z_3) \in X_f$ follows from the vanishing of B on $\ker f$ and the fact that $\ker f \otimes W \subseteq X_f$. When only one of the z_i is in $\ker f$, the same conclusion follows from (ii). □

Proposition 4.5. *Consider the action of $GL_2(\mathbb{F}_p)$ by conjugation of $sl_2(F_p)$. Let $t \in \mathbb{F}_p$ be a non-square. The induced action of $GL_2(\mathbb{F}_p)$ on s-dimensional subspaces of $sl_2(F_p)$ has the following orbits:*

(i) *when $s = 1$, there are three orbits, represented by the subspaces $Y_1 =< \left(\begin{smallmatrix} 0 & 1 \\ 0 & 0 \end{smallmatrix}\right) >$, $Y_2 =< \left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right) >$, $Y_3 =< \left(\begin{smallmatrix} 0 & 1 \\ t & 0 \end{smallmatrix}\right) >$.*

(ii) *when $s = 2$, there are 3 orbits represented by the subspaces $Y_1^{\perp} =< \left(\begin{smallmatrix} 1 & 0 \\ 0 & -1 \end{smallmatrix}\right), \left(\begin{smallmatrix} 0 & 1 \\ 0 & 0 \end{smallmatrix}\right) >$, $Y_2^{\perp} =< \left(\begin{smallmatrix} 1 & 0 \\ 0 & -1 \end{smallmatrix}\right), \left(\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right) >$, $Y_3^{\perp} =< \left(\begin{smallmatrix} 1 & 0 \\ 0 & -1 \end{smallmatrix}\right), \left(\begin{smallmatrix} 0 & 1 \\ -t & 0 \end{smallmatrix}\right) >$.*

(iii) *when $s = 3$, there is 1 orbit.*

Proof. Let us start with $s = 1$. Note that the set of determinants of non-zero elements in a given one dimensional subspace of $sl_2(\mathbb{F}_p)$ consists either of all squares in $\mathbb{F}_p$, or of all non-squares in $\mathbb{F}_p$, or of 0 only. Since any two non zero 2×2 matrices with trace 0 and the same determinant are conjugate, part (i) follows.

For (ii), note that the function $(A, B) \mapsto \mathrm{tr}(AB)$ is a non-degenerate bilinear form on $sl_2(\mathbb{F}_p)$ which is invariant under the action of $GL_2(\mathbb{F}_p)$. Taking orthogonal complements with respect to this form gives a bijection between one dimensional subspaces and two dimensional subspaces and takes orbits of $GL_2(\mathbb{F}_p)$ on one dimensional subspaces onto orbits on two dimensional subspaces. This proves (ii), since $Y_i^{\perp}$ is the space orthogonal to Y_i.

Finally, (iii) is clear. □

We are now ready to prove Theorem 4.1.

Proof of Theorem 4.1: The first part of the theorem has been established in Proposition 4.4. Suppose now that G is capable. Choose a basis a, b of W and $v, w \in U$ such that $f(v) = a$ and $f(w) = b$. Furthermore, choose a basis $u_1, \ldots, u_s$ of $\ker f$. We may write $B(v, u_i) = s_i a + t_i b$ and $B(w, u_i) = p_i a + q_i b$ for $s_i, t_i, p_i, q_i \in \mathbb{F}_p$. By Proposition 4.4 (i), we have $B(u_i, u_j) = 0$ for all $1 \le i, j \le s$. By Lemma 4.3, part (ii) Proposition 4.4 is equivalent to the condition $s_i + q_i = 0$, $i = 1, 2, \ldots, s$.

Let V be the 2 dimensional subspace of $U/\ker f$ and set $\overline{u} = u + \ker f$ for any $u \in U$. Note that f gives an isomorphism from V to W. Let T be the space of all linear transformations from V to W. This is a 4 dimensional $\mathbb{F}_p$-vector space. Using bases a, b of W and $\overline{v}, \overline{w}$ of V we may represent any element of T as a 2×2 matrix over $\mathbb{F}_p$. Note that changing a basis of W results in conjugation of the representing matrix by the change of basis matrix. Let T_1 be the subspace of T consisting of those transformations whose matrix has trace 0 (this subspace does not depend on the choice of basis of W). Clearly T_1 has dimension 3. As B vanishes on $\ker f \times \ker f$, the map $B(-,u)$ can be considered as an element of T for any $u \in \ker f$. As we have noticed above, part (ii) Proposition 4.4 implies that $B(-,u)$ belongs to T_1. The assignment $u \mapsto B(-,u)$ is therefore a linear map from $\ker f$ to T_1. Since B is non-degenerate, this map is injective. This shows that $s = \dim \ker f \leq 3$. In other words, we have $p^5 \leq G \leq p^7$ (this also follows from [4]).

Let T_2 be the image of $\ker f$ in T_1. As we have seen above, choosing a basis of W allows to identify T_2 with an s-dimensional subspace of $sl_2(\mathbb{F}_p)$ (matrices of trace 0). Note that $GL_2(\mathbb{F}_p)$ acts on $sl_2(\mathbb{F}_p)$ by conjugation. A different choice of a basis results in conjugate subspace. We will use Proposition 4.5 to choose a suitable basis of W.

case 1 $s = 1$, i.e. $|G| = p^5$. By Proposition 4.5, there is a basis a, b of W and a basis u of $\ker f$ such that $B(-,u)$ is represented by one of the matrices $\left(\begin{smallmatrix} 0 & 1 \\ 0 & 0 \end{smallmatrix}\right)$, $\left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)$, $\left(\begin{smallmatrix} 0 & 1 \\ t & 0 \end{smallmatrix}\right)$. Thus we consider the following three subcases:

(1) There is a basis a, b of W and a basis v, w, u of U such that $a = f(v), b = f(w), 0 = f(u)$ and $B(v,u) = 0$, $B(w,u) = a$. Suppose that $B(v,w) = pa + qb$. Then $B(v + pu, w) = qb$. If we had $q = 0$, then $B(v + pu, -)$ would vanish on U, which is not possible as B is non-degenerate. Hence $q \neq 0$. Replacing v by $v + pu$ allows us to assume that $p = 0$. Setting $v' = q^{-1}v, a' = q^{-1}a$, $w' = w$, $b' = b$, $u' = q^{-1}u$, we have $a' = f(v'), b' = f(w'), 0 = f(u')$, $B(v', u') = 0$, $B(w', u') = a'$, and $B(v', w') = b'$. Choosing $g, h, c \in G$ such that $g[G,G] = v'$, $h[G,G] = w'$, $c[G,G] = u'$, we see that

$$< g, h, c : g^{p^2} = h^{p^2} = c^p = 1, [g,h] = h^p, [g,c] = 1, [h,c] = g^p >$$

is a presentation of G. Thus G is isomorphic to P_1.

(2) There is a basis a, b of W and a basis v, w, u of U such that $a = f(v), b = f(w), 0 = f(u)$ and $B(v,u) = b$, $B(w,u) = a$. Suppose that $B(v,w) = pa + qb$. Then $B(v + pu, w - qu) = 0$. Replacing v, w by $v + pu$, $w - qu$ respectively, we may assume that $B(v,w) = 0$. Choosing $g, h, c \in G$ such that $g[G,G] = v$, $h[G,G] = w$, $c[G,G] = u$, we

see that

$$< g, h, c : g^{p^2} = h^{p^2} = c^p = 1, [g, h] = 1, [g, c] = h^p, [h, c] = g^p >$$

is a presentation of G. Thus G is isomorphic to P_2.

(3) There is a basis a, b of W and a basis v, w, u of U such that $a = f(v), b = f(w), 0 = f(u)$ and $B(v, u) = tb$, $B(w, u) = a$ (recall that t is a fixed non-square in $\mathbb{F}_p$). Suppose that $B(v, w) = pa + qb$. Then $B(v + pu, w - t^{-1}qu) = 0$. Replacing v, w by $v + pu$, $w - t^{-1}qu$ respectively, we may assume that $B(v, w) = 0$. Choosing $g, h, c \in G$ such that $g[G, G] = v$, $h[G, G] = w$, $c[G, G] = u$, we see that

$$< g, h, c : g^{p^2} = h^{p^2} = c^p = 1, [g, h] = 1, [g, c] = h^{tp}, [h, c] = g^p >$$

is a presentation of G. Thus G is isomorphic to P_3.

By Proposition 4.5, the groups P_1, P_2, P_3 are pairwise non-isomorphic. A straightforward verification, using Proposition 4.4, shows that all three groups are indeed capable.

case 2 $s = 2$, i.e. $|G| = p^6$. By Proposition 4.5, we have the following three subcases:

(1) There is a basis a, b of W and a basis v, w, u_1, u_2 of U such that $a = f(v), b = f(w), 0 = f(u_1) = f(u_2)$, $B(v, u_1) = a$, $B(w, u_1) = -b$, $B(v, u_2) = 0$, $B(w, u_2) = a$. Suppose that $B(v, w) = pa + qb$. Then $B(v + qu_1, w - pu_1) = 0$. Replacing v, w by $v+qu_1$, $w-pu_1$ respectively, we may assume that $B(v, w) = 0$. Choosing $g, h, c_1, c_2 \in G$ such that $g[G, G] = v$, $h[G, G] = w$, $c_1[G, G] = u_1$, $c_2[G, G] = u_2$ we see that

$$< g, h, c_1, c_2 : g^{p^2} = h^{p^2} = c_1^p = c_2^p = 1,$$

$$[g, h] = 1, [g, c_1] = g^p, [h, c_1] = h^{-p}, [g, c_2] = 1, [h, c_2] = g^p >$$

is a presentation of G. Thus G is isomorphic to Q_1.

(2) There is a basis a, b of W and a basis v, w, u_1, u_2 of U such that $a = f(v), b = f(w), 0 = f(u_1) = f(u_2)$, $B(v, u_1) = a$, $B(w, u_1) = -b$, $B(v, u_2) = -b$, $B(w, u_2) = a$. Suppose that $B(v, w) = pa + qb$. Then $B(v + qu_1, w - pu_1) = 0$. Replacing v, w by $v+qu_1$, $w-pu_1$ respectively, we may assume that $B(v, w) = 0$. Choosing $g, h, c_1, c_2 \in G$

such that $g[G,G] = v$, $h[G,G] = w$, $c_1[G,G] = u_1$, $c_2[G,G] = u_2$ we see that

$$< g, h, c_1, c_2 : g^{p^2} = h^{p^2} = c_1^p = c_2^p = 1,$$

$$[g, h] = 1, [g, c_1] = g^p, [h, c_1] = h^{-p}, [g, c_2] = h^{-p}, [h, c_2] = g^p >$$

is a presentation of G. Thus G is isomorphic to Q_2.

(3) There is a basis a, b of W and a basis v, w, u_1, u_2 of U such that $a = f(v), b = f(w), 0 = f(u_1) = f(u_2)$, $B(v, u_1) = a$, $B(w, u_1) = -b$, $B(v, u_2) = -tb$, $B(w, u_2) = a$. Suppose that $B(v, w) = pa + qb$. Then $B(v + qu_1, w - pu_1) = 0$. Replacing v, w by $v+qu_1$, $w-pu_1$ respectively, we may assume that $B(v, w) = 0$. Choosing $g, h, c_1, c_2 \in G$ such that $g[G,G] = v$, $h[G,G] = w$, $c_1[G,G] = u_1$, $c_2[G,G] = u_2$ we see that

$$< g, h, c_1, c_2 : g^{p^2} = h^{p^2} = c_1^p = c_2^p = 1, [g, h] = 1, [g, c_1] = g^p, [h, c_1] = h^{-p}, [g, c_2] = h^{-tp}, [h, c_2] = g^p >$$

is a presentation of G. Thus G is isomorphic to Q_3.

By Proposition 4.5, the groups Q_1, Q_2, Q_3 are pairwise non-isomorphic. A straightforward verification, using Proposition 4.4, shows that all three groups are indeed capable.

case 3 $s = 3$, i.e. $|G| = p^7$. There is a basis a, b of W and a basis v, w, u_1, u_2, u_3 of U such that $a = f(v), b = f(w), 0 = f(u_1) = f(u_2) = f(u_3)$, $B(v, u_1) = a$, $B(w, u_1) = -b$, $B(v, u_2) = 0$, $B(w, u_2) = a$, $B(v, u_3) = b$, $B(w, u_3) = 0$. Suppose that $B(v, w) = pa + qb$. Then $B(v+qu_1, w-pu_1) = 0$. Replacing v, w by $v+qu_1$, $w-pu_1$ respectively, we may assume that $B(v, w) = 0$. Choosing $g, h, c_1, c_2 \in G$ such that $g[G,G] = v$, $h[G,G] = w$, $c_1[G,G] = u_1$, $c_2[G,G] = u_2$, $c_3[G,G] = u_3$ we see that

$$< g, h, c_1, c_2, c_3 : g^{p^2} = h^{p^2} = c_1^p = c_2^p = c_3^p = 1,$$

$$[g, h] = 1, [g, c_1] = g^p, [h, c_1] = h^{-p}, [g, c_2] = 1, [h, c_2] = g^p, [g, c_3] = h^p, [h, c_3] = 1 >$$

is a presentation of G. Thus G is isomorphic to R. A straightforward verification, using Proposition 4.4, shows that R is indeed capable. This completes the proof of Theorem 4.1. □

5. p-groups of nilpotency class 2 and exponent p

The main result of this section is the following theorem.

Theorem 5.1. *Let p be an odd prime, t a quadratic non-residue modulo p.*

(i) *There is only one, up to isomorphism, class of special p-groups of rank 2, order p^5, and exponent p. It is capable and has presentation:*

$$< p_1, p_2, p_3, q_1, q_2 | p_i^p = q_j^p = 1, [p_i, q_j] = [q_1, q_2] = [p_2, p_3] = 1 \text{ for } 1 \leq i \leq 3,\ 1 \leq j \leq 2,$$
$$[p_1, p_2] = q_1, [p_1, p_3] = q_2 > .$$

(ii) *There are 3 isomorphism classes of special p-groups of rank 2, order p^6, and exponent p, given by presentations:*

$$< p_1, p_2, p_3, p_4, q_1, q_2 | p_i^p = q_j^p = 1, [p_i, q_j] = [q_1, q_2] = [p_1, p_2] = [p_3, p_4] = [p_1, p_4] = [p_2, p_3] = 1$$
$$\text{for } 1 \leq i \leq 4,\ 1 \leq j \leq 2,\ [p_1, p_3] = q_1, [p_2, p_4] = q_2 >;$$

$$< p_1, p_2, p_3, p_4, q_1, q_2 | p_i^p = q_j^p = 1, [p_i, q_j] = [q_1, q_2] = [p_1, p_2] = [p_3, p_4] = [p_2, p_3] = 1$$
$$\text{for } 1 \leq i \leq 4,\ 1 \leq j \leq 2,\ [p_1, p_3] = q_1, [p_2, p_4] = q_1, [p_1, p_4] = q_2 >;$$

$$< p_1, p_2, p_3, p_4, q_1, q_2 | p_i^p = q_j^p = 1, [p_i, q_j] = [q_1, q_2] = [p_1, p_2] = [p_3, p_4] = 1$$
$$\text{for } 1 \leq i \leq 4,\ 1 \leq j \leq 2,\ [p_1, p_3] = q_1, [p_2, p_4] = q_1, [p_1, p_4] = q_2, [p_2, p_3] = q_2^t >;$$

All three groups are capable.

(iii) *There are two isomorphism classes of special p-groups of rank 2, order p^7, and exponent p, given by the presentations:*

$$< p_1, p_2, p_3, p_4, p_5, q_1, q_2 | p_i^p = q_j^p = 1, [p_i, q_j] = [q_1, q_2] = [p_i, p_k] = 1,\ \text{for } 1 \leq i \leq 5,$$
$$1 \leq j \leq 2,\ i + 1 < k \leq 5, [p_1, p_2] = q_1, [p_3, p_4] = q_1, [p_2, p_3] = q_2, [p_4, p_5] = q_2 >;$$

$$< p_1, p_2, p_3, p_4, p_5, q_1, q_2 | p_i^p = q_j^p = 1, [p_i, q_j] = [q_1, q_2] = 1, [p_1, p_3] = q_1, [p_1, p_4] = q_2, [p_2, p_5] = q_2$$

$$\textit{for } 1 \leq i \leq 5,\ 1 \leq j \leq 2, [p_i, p_j] = 0 \textit{ for all other } 1 \leq i < j \leq 5 > .$$

The first group is capable, the second has cyclic epicenter equal to $< q_2 >$.

(iv) *For every odd* $n = 2m + 3$ *with* $m \geq 2$ *there is unique isomorphism class of special* p*-groups of rank 2, order* p^n*, and exponent* p *which has cyclic epicenter. It has presentation*

$$< p_1, \ldots, p_m, q_0, q_1, \ldots, q_m, c_1, c_2 | p_i^p = q_j^p = 1, [p_i, c_k] = [q_j, c_k] = [c_1, c_2] = 1,$$

$$\textit{for } 1 \leq i, j \leq m,\ 1 \leq k \leq 2,\ [p_1, q_0] = c_1, [p_i, q_i] = c_2 \ \textit{ for } i = 1, \ldots, m,$$

$$[p_i, p_j] = [q_i, q_j] = [p_i, q_j] = [q_0, q_j] = 1 \textit{ for any } 1 \leq i, j \leq m,\ i \neq j,$$

$$[p_i, q_0] = 1 \textit{ for } 2 \leq i \leq m >$$

and its epicenter is generated by c_2.

(v) *For every even* $n = 2m + 2$ *with* $m \geq 3$ *there are two isomorphism classes of special* p*-groups of rank 2, order* p^n*, and exponent* p *which have cyclic epicenter. They are given by the following presentations:*

$$< p_1, \ldots, p_m, q_1, \ldots, q_m, c_1, c_2 | p_i^p = q_j^p = 1, [p_i, c_k] = [q_j, c_k] = [c_1, c_2] = 1,$$

$$\textit{for } 1 \leq i, j \leq m,\ 1 \leq k \leq 2,\ [p_1, q_1] = c_1, [p_i, q_i] = c_2 \ \textit{ for } i = 2, \ldots, m,$$

$$[p_i, p_j] = [q_i, q_j] = [p_i, q_j] = 1 \textit{ for any } 1 \leq i, j \leq m,\ i \neq j >$$

$$< p_1, \ldots, p_m, q_1, \ldots, q_m, c_1, c_2 | p_i^p = q_j^p = 1, [p_i, c_k] = [q_j, c_k] = [c_1, c_2] = 1,$$

$$\textit{for } 1 \leq i, j \leq m,\ 1 \leq k \leq 2,\ [p_1, q_2] = c_1, [p_i, q_i] = c_2 \ \textit{ for } i = 1, \ldots, m,$$

$$[p_i, q_1] = [q_1, q_j] = [p_1, p_j] = [p_i, p_j] = [q_i, q_j] = [p_i, q_j] = 1 \textit{ for any } 2 \leq i, j \leq m,\ i \neq j,$$

$$[p_1, q_j] = 1 \textit{ for any } 3 \leq j \leq m >$$

and both groups have epicenter generated by c_2.

All other special p*-groups of rank 2 are unicentral.*

In order to prove this theorem we need to review various results related to groups of exponent p and nilpotency class 2. To this end, consider the category EX_p of p-groups G of class 2 and exponent p, where p is an odd prime. As in the previous sections, to any object of EX_p we associate the $\mathbb{F}_p$-vector spaces $U_G = G/[G,G]$, $W_G = [G,G]$ and an alternating bilinear map $B_G : U \times U \longrightarrow W$ defined by $B_G(a,b) = [g,h]$, where $a = g[G,G]$, $b = h[G,G]$. Note that the image of B spans W_G. This leads us to consider the category ALT_p whose objects are alternating bilinear maps $B : U \times U \longrightarrow W$ such that U, W are finite dimensional vector spaces over $\mathbb{F}_p$ and the image of B spans W. A morphism between $B_1 : U_1 \times U_1 \longrightarrow W_1$ and $B_2 : U_2 \times U_2 \longrightarrow W_2$ is a pair (h_U, h_W), where $h_U : U_1 \longrightarrow U_2$ and $h_W : W_1 \longrightarrow W_2$ are linear maps such that $h_W B_1 = B_2(h_U \times h_U)$. The **rank** of B is, by definition, the dimension of W and $\dim U$ is the **dimension** of B. It is clear that the association $G \mapsto B_G$ is a functor $\mathcal{L}$ from EX_p to ALT_p.

Proposition 5.2.

(i) *Every object of* ALT_p *is isomorphic to an object of the form* $\mathcal{L}(G)$ *for some group* G *in* EX_p*.*

(ii) *The functor* $\mathcal{L}$ *is full.*

(iii) *A morphism* $f : H \longrightarrow G$ *is an isomorphism in* EX_p *iff* $\mathcal{L}(f)$ *is an isomorphism in* ALT_p*.*

Proof. Consider a group G in EX_p. Choose a basis $u_1, \ldots, u_s$ of U_G and let $g_1, \ldots, g_s$ be elements of G such that $u_i = g_i + W_G$. Consider the set of all elements of G of the form $g_1^{a_1} \ldots g_s^{a_s}$, where $a_i \in \mathbb{F}_p$ for $i = 1, 2, \ldots, s$. This is a transversal of U_G in G. Thus every element of G is in a unique way expressible as $w g_1^{a_1} \ldots g_s^{a_s}$, where $w \in W$ and $a_i \in \mathbb{F}_p$. A simple calculation yields the following equality:

$$(wg_1^{a_1} \ldots g_s^{a_s})(vg_1^{b_1} \ldots g_s^{b_s}) = (w + v + \sum_{i>j} a_i b_j B(u_i, u_j)) g_1^{a_1+b_1} \ldots g_s^{a_s+b_s}. \tag{3}$$

To prove part (i), consider an object $B : U \times U \longrightarrow W$ of ALT_p. Choose a basis $u_1, \ldots, u_s$ of U. It is a simple calculation to check that the function $f : U \times U \longrightarrow W$

given by $f(\sum a_i u_i, \sum b_i u_i) = \sum_{i>j} a_i b_j B(u_i, u_j)$ is a 2-cocycle which defines a group G in EX_p such that $\mathcal{L}(G)$ isomorphic to (U, W, B).

Suppose now that H, G are groups in EX_p and that (h_U, h_W) is a morphism from $\mathcal{L}(H)$ to $\mathcal{L}(G)$. Choose a basis of $u_1, \ldots, u_s$ of U_G such that $u_1, \ldots, u_t$ is a basis of the image of $h_U : U_H \longrightarrow U_G$. Let $v_1, \ldots, v_t$ be elements of U_H such that $h_U(v_i) = u_i$ for $i = 1, \ldots, t$. Complete the vectors $v_1, \ldots, v_t$ to a basis $v_1, \ldots, v_r$ of U_H by adding a basis $v_{t+1}, \ldots, v_r$ of $\ker h_U$. Finally, choose $h_1, \ldots, h_r$ in H and $g_1, \ldots, g_s \in G$ such that $h_i[H, H] = v_i$ and $g_i[G, G] = u_i$. We define a function $f : H \longrightarrow G$ by the formula $f(wh_1^{a_1} \ldots h_r^{a_r}) = h_W(w) g_1^{a_1} \ldots g_t^{a_t}$. It is a straightforward computation, using (3), to verify that f is a homomorphism such that $\mathcal{L}(f) = (h_U, H_W)$. This proves part (ii).

Suppose now that $\mathcal{L}(f) = (h_U, h_W)$ is an isomorphism. Since h_U is an isomorphism, we have $\ker f \subseteq [H, H]$ and $G = [G, G]f(H)$. Since h_W is an isomorphism, we conclude that $\ker f = 1$ and $[G, G] = [f(H), h(H)] \subseteq f(H)$. It follows that f is both injective and surjective, i.e. is an isomorphism. This proves part (iii). □

Remark 5.3. It is easy to see that the group G in EX_p corresponding to an object $B : U \times U \longrightarrow W$ of ALT_p can be given by the following presentation. Choose a basis $u_1, \ldots, u_m$ of U and a basis $w_1, \ldots, w_n$ of B. Then $B = B_1 w_1 + \ldots + B_n w_n$, where $B_1, \ldots, B_n$ are alternating bilinear forms on U. Set $a_{i,j,k} = B_k(u_i, u_j)$. We have

$$G =< p_1, \ldots, p_m, q_1, \ldots, q_n | p_i^p = q_j^p = 1, [q_j, q_k] = [p_i, q_j] = 1 \text{ for any } 1 \leq i \leq m \text{ and}$$

$$1 \leq j, k \leq n,\ [p_i, p_j] = \prod_{k=1}^{n} q_k^{a_{i,j,k}} \text{ for any } 1 \leq i < j \leq m >$$

Remark 5.4. It follows from Proposition 5.2 that the problem of classifying groups G in EX_p of rank k (i.e. such that $\dim[G, G] = p^k$) is equivalent to classification of isomorphism types of objects of rank k in ALT_p. For $k = 1$ it is a classical question of classifying bilinear alternating forms (and translates into classification of extra-special p-groups). The case of $k = 2$ can be handled with the help of a very nice work by R. Scharlau [8]. Note that, according to (ii) of Proposition 3.8, any group G in EX_p can be factored as $G_1 \times Z$, where Z is elementary abelian and G_1 is special of exponent p. Special groups in EX_p correspond to non-degenerate objects in ALT, i.e objects for which the map $u \mapsto B(u, -)$ is an injective homomorphism from U to the space of linear maps $U \longrightarrow W$.

To an object $B : U\times U \longrightarrow W$ of ALT_p we associate a subspace X_B of $U\otimes W$ spanned by all elements of the form $a\otimes B(b,c)+b\otimes B(c,a)+c\otimes B(a,b)$ with $a,b,c\in U$.

As a special case of Theorem 3.10 we have the following result.

Theorem 5.5. *Let G be a finite p-group of nilpotency class 2 and exponent p. An element w belongs to the epicenter $Z^*(G)$ if and only if $w\in W_G$ and $U_G\otimes w\subseteq X_{B_G}$.*

This result motivates the following definition.

Definition 5.6. Let $B : U\times U \longrightarrow W$ be an object of ALT_p. We define $Z^*(B)$ as the subspace consisting of all $w\in W$ such $U\otimes w\subseteq X_B$.

The problem of determining the epicenter of G is therefore reduced to a linear algebra problem of finding $Z^*(B_G)$.

As a first application of the ideas discussed in this section we get the following result, conjectured by Heineken and Nikolova.

Theorem 5.7. *Let G be a capable p group of nilpotency class 2 with commutator elementary abelian of rank k. Then the rank of $G/Z(G)$ is at most $2k+\binom{k}{2}$.*

Proof. Let $U=G/Z(G)$, $W=[G,G]$. Then $B : U\times U \longrightarrow W$, defined by $B(g[G,G],h[G,G])=[g,h]$, is an element of ALT_p. Since G is capable, Proposition 3.9 implies that there is no non-trivial element $w\in W$ such that $U\otimes w\subseteq X_B$. By Proposition 5.2, there is a group P in EX_p such that $\mathcal{L}(P)\cong B$. The group P is capable by Theorem 5.5. Now $P=P_1\times A$ with A central and P_1 special. Note that $Z(P_1)=[P,P]\cong[G,G]$ has rank k and $G/Z(G)\cong P_1/[P_1,P_1]$. The result follows now from Theorem 1 in [5], which proves the bound for special p-groups of exponent p. $\square$

The following straightforward observation is often useful.

Lemma 5.8. *Let $B : U\times U \longrightarrow W$ be an object of ALT_p and let S be a basis of U. Then X_B is spanned by elements of the form $a\otimes B(b,c)+b\otimes B(c,a)+c\otimes B(a,b)$ with $a,b,c\in S$.* $\square$

We say that an object $B : U\times U \longrightarrow W$ of ALT_p is decomposable if U can be decomposed into a non-trivial direct sum $U=U_1+U_2$ such that $B(u_1,u_2)=0$ for any $u_1\in U_1$ and $u_2\in U_2$. Note that we do not require that the image $B(U_i\times U_i)$ spans W.

Lemma 5.9. *Let $U = U_1 + U_2$ be a decomposition of an object $B : U \times U \longrightarrow W$ of* ALT_p *and let W_i be the subspace of W spanned by $B(U_i \times U_i)$. Then $X_B = X_{B_1} + X_{B_2} + U_1 \otimes W_2 + U_2 \otimes W_1$, where $B_i : U_i \times U_i \longrightarrow W_i$ is the restriction of B to U_i.*

Proof. The inclusion $X_{B_1} + X_{B_2} + U_1 \otimes W_2 + U_2 \otimes W_1 \subseteq X_B$ is a straightforward consequence of the definition of X_B. The opposite inclusion follows from Lemma 5.8 applied to a basis S which is a union of a basis of U_1 and a basis of U_2. □

As a straightforward corollary we get the following lemma.

Lemma 5.10. *Let $B : U \times U \longrightarrow W$ be an object of* ALT_p *of rank 1. Then B has decomposition $U = U_1 + U_2$ such that $W_1 = 0$ and B_2 is non-degenerate. If U_2 has dimension 2 then $X_B = U_1 \otimes W$. Otherwise, $X_B = U \otimes W$.* □

Proposition 5.11. *Let $B : U \times U \longrightarrow W$ be a decomposable non-degenerate object of rank 2 of* ALT_p*. Then $\dim U \geq 6$ and $Z^*(B) = W$ unless B is isomorphic to one of the following objects.*

(i) *U has a basis u_1, v_1, u_2, v_2 and W has a basis w_1, w_2 such that $B(u_1, v_1) = w_1$, $B(u_2, v_2) = w_2$ and $B(u_1, u_2) = B(v_1, v_2) = B(u_1, v_2) = B(u_2, v_1) = 0$. We have $Z^*(B) = \{0\}$.*

(ii) *U has a basis $u_1, u_2, \ldots u_m, v_1, v_2, \ldots, v_m$ for some $m \geq 3$ and W has a basis w_1, w_2 such that $B(u_1, v_1) = w_1$, $B(u_i, v_i) = w_2$ for $i = 2, \ldots, m$, and $B(u_i, u_j) = B(v_i, v_j) = B(u_i, v_j) = 0$ for any $1 \leq i, j \leq m$, $i \neq j$. The subspace $Z^*(B)$ is spanned by w_2.*

(iii) *U has a basis $u_1, u_2, \ldots u_m, v_0, v_1, v_2, \ldots, v_m$ for some $m \geq 2$ and W has a basis w_1, w_2 such that $B(u_1, v_0) = w_1$, $B(u_i, v_i) = w_2$ for $i = 1, \ldots, m$, $B(u_i, u_j) = B(v_i, v_j) = B(u_i, v_j) = B(v_0, v_j) = 0$ for any $1 \leq i, j \leq m$, $i \neq j$, and $B(u_i, v_0) = 0$ for $2 \leq i \leq m$. The subspace $Z^*(B)$ is spanned by w_2.*

(iv) *U has a basis $u_0, u_1, \ldots u_m, v_0, v_1, v_2, \ldots, v_m$ for some $m \geq 2$ and W has a basis w_1, w_2 such that $B(u_0, v_1) = w_1$, $B(u_i, v_i) = w_2$ for $i = 0, \ldots, m$, $B(u_i, v_0) = B(v_0, v_j) = B(u_0, u_j) = B(u_i, u_j) = B(v_i, v_j) = B(u_i, v_j) = 0$ for any $1 \leq i, j \leq m$, $i \neq j$, and $B(u_0, v_j) = 0$ for $2 \leq j \leq m$. The subspace $Z^*(B)$ is spanned by w_2.*

Proof. Consider a decomposition $U = U_1 + U_2$ of $B : U \times U \longrightarrow W$. Let W_i be the subspace of W spanned by $B(U_i \times U_i)$ and let $B_i : U_i \times U_i \longrightarrow W_i$ be the restriction of B to U_i.

Suppose first that there is such a decomposition of B with $W_1 = W_2 = W$. Then $X_B = U \otimes W$ by Lemma 5.9. Furthermore $\dim U_i \geq 3$ for $i = 1, 2$, so $\dim U \geq 6$.

Suppose now that B has a decomposition with both W_1 and W_2 of dimension 1. Choose bases w_1 of W_1 and w_2 of W_2. Then, for $i = 1, 2$, we have $B_i = b_i w_i$ with b_i an alternating bilinear form on U_i. Since B is non-degenerate, both b_1 and b_2 are non-degenerate as well. It follows that each b_i decomposes into an orthogonal sum of two dimensional non-degenerate alternating forms.

If both U_1 and U_2 have dimension at least 4, then we can decompose b_1 and b_2 into orthogonal direct sums $U_1 = U_{11} + U_{12}$ and $U_2 = U_{21} + U_{22}$. Then $U = (U_{11} + U_{21}) + (U_{12} + U_{22})$ is another decomposition of B, for which the corresponding subspaces W_1 and W_2 are both equal to W. As we have shown above, this implies that $X_B = U \otimes W$ and $\dim U \geq 6$.

If both U_1, U_2 have dimension 2, then there is a basis u_1, v_1 of U_1 and u_2, v_2 of U_2 such that $b_1(u_1, v_1) = 1 = b_2(u_2, v_2)$. Thus B is isomorphic to the object (i). By Lemma 5.9, we have $X_B = U_1 \otimes W_2 + U_2 \otimes W_1$ and $Z^*(B) = \{0\}$.

Finally, if exactly one of U_1, U_2 has dimension 2, then we may assume that $\dim U_1 = 2$ and then choose bases u_1, v_1 of U_1 and $u_2, \ldots, u_m, v_2, \ldots, u_m$ of U_2 such that $b_1(u_1, v_1) = 1 = b_2(u_i, v_i)$ for $i = 2, \ldots, m$ and $b_2(u_i, v_j) = b_2(u_i, u_j) = b_2(v_i, v_j) = 0$ for any $2 \leq i, j \leq m$, $i \neq j$. This shows that B isomorphic to the object (ii). Lemmas 5.9 and 5.10 imply that $X_B = U \otimes W_2 + U_2 \otimes W_1$ and $Z^*(B) = W_2$.

It remains to consider the case when in any decomposition of B exactly one of W_1, W_2 has dimension 2. Choose a decomposition in which $W_1 = W$ has dimension 2 and U_1 has smallest dimension possible. Let w_2 be a basis of W_2. Choose $w_1 \in W$ such that w_1, w_2 is a basis of W and let V be the subspace of W spanned by w_1. Then B_1 can be written as $bw_1 + dw_2$, where b and d are alternating bilinear forms on U_1. Set $\hat{B}_1 = bw_1$. Then, by Lemma 5.9, $X_B = X_{\hat{B}_1} + U_1 \otimes W_2 + U_2 \otimes W = X_{\hat{B}_1} + U \otimes W_2 + U_2 \otimes V$. We may decompose U_1 into a direct sum $K + L$, where K is the subspace of all $u \in U_1$ such that $b(u, -) = 0$ and b restricted to L is non-degenerate. If $\dim L > 2$ then $X_{\hat{B}_1} = U_1 \otimes V$

by Lemma 5.10, so $X_B = U \otimes W$ and $\dim U \geq 6$. Thus we may assume that $\dim L = 2$. Again by Lemma 5.10, we have $X_{\hat{B}_1} = K \otimes V$ and $X_B = U \otimes W_2 + (U_2 + K) \otimes V$. It follows that $Z^*(B) = W_2$ Let p, q is a basis of L such that $b(p, q) = 1$. If there are $g, h \in K$ such that $d(g, h) \neq 0$ then $U_1 = H + A$ where H is spanned by g, h and A is the orthogonal complement to H with respect to d. It follows then that $U = A + (H + U_2)$ is another decomposition of B, in which either both W_1 W_2 have dimension 1 or $W_1 = W$ and W_2 has dimension 1. The former case is not possible as B has no decomposition with both W_1, W_2 one dimensional. The latter case is also not possible, as $\dim A < \dim U_1$ and U_1 was chosen of least possible dimension. It follows that the restriction of d to K is trivial. If $\dim K \geq 3$, then both $d(w_1, -), d(w_2, -)$ would vanish on a non-zero $z \in K$, and this would mean that $B(-, z) = 0$ contradicting the non-degeneracy of B. Thus $1 \leq \dim K \leq 2$.

Suppose that K has dimension 1 and let k be a basis of K. Then at least one of the values $d(p, k)$, $d(q, k)$ is not 0. We may adjust our choices of p, q, k so that $d(p, k) = 1$. Set $u_1 = p$, $v_0 = q + d(q, p)k + d(k, q)p$, $v_1 = k$ and let $u_2, \ldots, u_m, v_2, \ldots, u_m$ be a basis of U_2 such that $B_2(u_i, v_i) = w_2$ for $i = 2, \ldots, m$ and $B_2(u_i, v_j) = B_2(u_i, u_j) = B_2(v_i, v_j) = 0$ for any $2 \leq i, j \leq m$, $i \neq j$. It follows that B is isomorphic to the object (iii).

Suppose now that K has dimension 2. Suppose that d is degenerate. Then the subspace M of all $u \in U_1$ such that $d(u, -) = 0$ has dimension 2. Any element u of $M \cap K$ satisfies $B_1(u, -) = 0$, hence $u = 0$. Thus $M \cap K = \{0\}$ and therefore $M + K = U_1$. This however implies that d is trivial on U_1, a contradiction. Thus d is non-degenerate. Let g, h be a basis of K. The kernel of $d(h, -)$ has dimension 3 and contains g and h. Thus there is g_1 not in K such that $d(h, g_1) = 0$. As d is non-degenerate, we have $d(g, g_1) \neq 0$. We may choose g_1 so that $d(g, g_1) = 1$. The subspace of U_1 of vectors d-orthogonal to both g and g_1 is two dimensional and it contains h, so it has a basis h, h_1 for some $h_1 \in U_1$. Clearly $d(h, h_1) \neq 0$ and we may choose h_1 so that $d(h, h_1) = 1$. It is clear that g, h, g_1, h_1 are linearly independent, hence they form a basis of U_1. It follows that $r := b(g_1, h_1) \neq 0$. Set $u_0 = -h_1$, $u_1 = rg$, $v_0 = h$, $v_1 = r^{-1}g_1$. Let $u_2, \ldots, u_m, v_2, \ldots, u_m$ be a basis of U_2 such that $B_2(u_i, v_i) = w_2$ for $i = 2, \ldots, m$ and $B_2(u_i, v_j) = B_2(u_i, u_j) = B_2(v_i, v_j) = 0$ for any $2 \leq i, j \leq m$, $i \neq j$. It follows that B is isomorphic to the object (iv). □

It remains to compute $Z^*(B)$ for indecomposable objects of rank 2 in ALT_p. This will be based on a beautiful result of Scharlau [8]. To state Schralu's result, we consider the category $\mathrm{ALT}(K)$, whose objects are triples (V, B_1, B_2), where V is a finite dimensional vector space over the field K and B_1, B_2 are alternating bilinear forms on V. We will call objects of $\mathrm{ALT}(K)$ bialternating modules. A morphism between two bialternating modules (V, B_1, B_2), (V', B_1', B_2') is a linear map f from V to V' which satisfies $B_i(v, w) = B_i'(f(v), f(w))$ for $i = 1, 2$. An orthogonal sum of (V, B_1, B_2), (V', B_1', B_2') is the object $(V \oplus V', B_1 \perp B_1', B_2 \perp B_2')$. An object is called indecomposable if it is not isomorphic to an orthogonal sum of two object of lower dimension. Scharlau proved that every bilaternating module is isomorphic to an orthogonal sum of indecomposable bialternating modules and any two such decompositions consist of the same isomorphism types of indecomposable modules (Krull-Schmidt type theorem). In addition, the indecomposable objects in $\mathrm{ALT}(K)$ are, up to isomorphism, classified by the following list:

type 1: $A_f = (K^{2n}, B_1, B_2)$, where $n \geq 1$, $f(x) = x^n - a_n x^{n-1} - \ldots - a_1$ is a power of an irreducible polynomial over K, $B_1(e_i, e_j) = 0$ for all $i < j$ except $B_1(e_i, e_{i+n}) = 1$ for $i = 1, 2, \ldots, n$, $B_2(e_i, e_j) = 0$ for all $i < j$ except $B_2(e_i, e_{1+i+n}) = 1$ when $1 \leq i < n$ and $B_2(e_n, e_{n+i}) = a_i$ for $i = 1, \ldots, n$.

type 2: $E_n = (K^{2n}, B_1, B_2)$, where $n \geq 1$, $B_1(e_i, e_j) = 0$ for all $i < j$ except $B_1(e_i, e_{1+i+n}) = 1$ when $1 \leq i < n$, $B_2(e_i, e_j) = 0$ for all $i < j$ except $B_2(e_i, e_{i+n}) = 1$ for $i = 1, \ldots, n$.

type 3: $F_n = (K^{2n+1}, B_1, B_2)$, where $n \geq 0$, $B_1(e_i, e_j) = 0$ for all $i < j$ except $B(e_i, e_{i+1}) = 1$ for any odd i between 1 and n, $B_2(e_i, e_j) = 0$ for all $i < j$ except $B(e_i, e_{i+1}) = 1$ for any even i between 1 and n.

Consider now an alternating bilinear map $B : U \times U \longrightarrow W$ of rank 2 in ALT_p. Any choice of ordered basis w_1, w_2 of W allows us to write $B = B_1 w_1 + B_2 w_2$, where B_1, B_2 are alternating bilinear forms on U. Thus, any choice of a basis of W allows us to represent B as a bialternating module (U, B_1, B_2). It is clear that B is indecomposable if and only if the corresponding bialternating module is decomposable.

Proposition 5.12. *Let $B : U \times U \longrightarrow W$ be an indecomposable object of rank 2 in ALT_p. If $\dim U \geq 6$ then $Z^*(B) = W$.*

Proof. Choose a basis w_1, w_2 of W and consider the irreducible bialternating module (U, B_1, B_2), where $B = B_1 w_1 + B_2 w_2$.

Suppose first that (U, B_1, B_2) is of type 1. Then there is a basis $u_1, \dots, u_n, v_1, \dots, v_n$ of U such that $B(u_i, u_j) = B(v_i, v_j) = 0$ for $1 \le i, j \le n$, $B(u_i, v_i) = w_1$, $B(u_n, v_i) = a_i w_2$ for $i = 1, \dots, n-1$, $B(u_n, v_n) = w_1 + a_n w_2$, $B(u_i, v_{i+1}) = w_2$ for $i = 1, \dots, n-1$ and $B(u_i, v_j) = 0$ in all other cases. For simplicity, we will write $< a, b, c >$ for $a \otimes B(b, c) + b \otimes B(c, a) + c \otimes B(a, b)$. Then $< v_k, u_1, v_1 >= v_k \otimes w_1$ and $< v_k, u_1, v_2 >= v_k \otimes w_2$ for $k > 2$. Also, $< v_1, u_2, v_2 >= v_1 \otimes w_1$, $< v_1, u_2, v_3 >= v_1 \otimes w_2$, $< v_2, u_2, v_3 >= v_2 \otimes w_2 - v_3 \otimes w_1$, $< v_2, u_1, v_1 >= v_2 \otimes w_1 - v_1 \otimes w_2$. It follows that X_B contains all tensors of the form $v_i \otimes w_j$, $i = 1, \dots, n$, $j = 1, 2$. Now $< u_k, u_1, v_1 >= u_k \otimes w_1$, $k = 2, \dots, n-1$. Also $< u_1, u_2, v_3 >= u_1 \otimes w_2$ and $< u_n, u_1, v_1 >= u_n \otimes w_1 - a_1 u_1 \otimes w_2$, $< u_1, u_n, v_n >= u_1 \otimes (w_1 + a_n w_2)$. This shows that $u_i \otimes w_1 \in X_B$ for $i = 1, \dots, n$. Now $< u_k, u_{k-1}, v_k >= u_k \otimes w_2 - u_{k-1} \otimes w_1$ for $k = 2, \dots, n-1$, so $u_i \otimes w_2 \in X_B$ for $i = 1, \dots, n-1$. Finally, $< u_n, u_1, v_2 >= u_n \otimes w_2 - a_2 u_1 \otimes w_2$, so $u_n \otimes w_2 \in X_B$. Thus we have $X_B = U \otimes W$ and $Z^*(B) = W$.

Suppose now that (U, B_1, B_2) is of type 2. Using the basis w_2, w_1 we associate to B the module (U, B_2, B_1), which is of type 1 with $f(x) = x^n$. Thus $Z^*(B) = W$ by the previous case.

Finally, suppose that (U, B_1, B_2) is of type 3. Then $\dim U = n \ge 7$ is odd and there is a basis $u_1, \dots, u_n$ of U such that $B(u_i, u_{i+1}) = w_1$ for i odd, $B(u_i, u_{i+1}) = w_2$ for i even and $B(u_i, u_j) = 0$ if $|i - j| > 1$. We have $< u_k, u_1, u_2 >= u_k \otimes w_1$ for $k = 4, \dots, n$, $< u_k, u_5, u_6 >= u_k \otimes w_1$ for $k < 4$, $< u_k, u_2, u_3 >= u_k \otimes w_2$ for $k = 5, \dots, n$, $< u_k, u_6, u_7 >= u_k \otimes w_2$ for $k < 5$. This proves that $X_B = U \otimes W$ and $Z^*(B) = W$. □

Lemma 5.13. *Let $B : U \times U \longrightarrow W$ be a non-degenerate object of ALT_p of rank 2 and dimension 3. Then there is a basis u_1, u_2, u_3 of U and w_1, w_2 of W such that $B(u_1, u_2) = w_1, B(u_1, u_2) = w_2, B(u_2, u_3) = 0$. Moreover, $Z^*(B) = \{0\}$.*

Proof. We have $B = B_1 w_1 + B_2 w_2$ It is clear that (U, B_1, B_2) is indecomposable, hence must isomorphic to F_3.

Alternatively, without referring to Scharlau's classification, one easily finds a basis v_1, v_2, v_3 of U such that $w_1 = B(v_1, v_2)$, $w_2 = B(v_1, v_3)$ is a basis of W. Then $B(v_2, v_3) =$

$aw_1 + bw_2$ for some $a, b \in \mathbb{F}_p$. Now set $u_1 = v_1$, $u_2 = v_2 - av_1$, $u_3 = v_3 + bv_1$. By Lemma 5.8, the space X_B has basis $u_2 \otimes w_2 - u_3 \otimes w_1$, hence $Z^*(B) = \{0\}$. □

Lemma 5.14. *Let t be a quadratic non-residue modulo p. There are three isomorphisms classes of object $B : U \times U \longrightarrow W$ of ALT_p which are non-degenerate of rank 2 and dimension 4, given by the following list:*

(i) *U has a basis u_1, u_2, v_1, v_2 and W has a basis w_1, w_2 such that $B(u_1, v_1) = w_1$, $B(u_2, v_2) = w_2$ and $B(u_1, u_2) = B(v_1, v_2) = B(u_1, v_2) = B(u_2, v_1) = 0$.*

(ii) *U has a basis u_1, u_2, v_1, v_2 and W has a basis w_1, w_2 such that $B(u_1, v_1) = B(u_2, v_2) = w_1$, $B(u_1, v_2) = w_2$, $B(u_2, v_1) = B(u_1, u_2) = B(v_1, v_2) = 0$.*

(iii) *U has a basis u_1, u_2, v_1, v_2 and W has a basis w_1, w_2 such that $B(u_1, v_1) = B(u_2, v_2) = w_1$, $B(u_1, v_2) = w_2$, $B(u_2, v_1) = tw_2$, $B(u_1, u_2) = B(v_1, v_2) = 0$*

In each case we have $Z^*(B) = \{0\}$.

Proof. If B is decomposable, then B satisfies (i) and $Z^*(B) = \{0\}$ by Proposition 5.11.

Suppose that B is indecomposable. Choose a basis η_1, η_2 of W and consider the bialternating module $(U, B_1, B_2))$, where $B = B_1\eta_1 + B_2\eta_2$. The bialternating module is either of type 1 or 2.

If (U, B_1, B_2) is of type 2 then, considering the basis η_2, η_1 of W we get the bialternating module $(U, B_2, B_1))$ which is of type 1 with $f(x) = x^2$. Thus we may assume that $(U, B_1, B_2))$ is of type 1. Let f be the associated polynomial. Then $f(x) = (x + \alpha)^2 - \delta$, where $\alpha, \delta \in \mathbb{F}_p$ and either $\delta = 0$ of δ is not a square in $\mathbb{F}_p$. Note that $a_1 = \delta - \alpha^2$ and $a_2 = -2\alpha$. Let e_1, e_2, e_3, e_4 be a basis of U such that $B(e_1, e_2) = B(e_3, e_4) = 0$, $B(e_1, e_3) = \eta_1$, $B(e_2, e_4) = \eta_1 + a_2\eta_2$, $B(e_2, e_3) = a_1\eta_2$, $B(e_1, e_4) = \eta_2$. Choose $s \in \mathbb{F}_p - \{0\}$ and let $u_1 = e_1$, $u_2 = s(\alpha e_1 + e_2)$, $v_1 = e_3 - \alpha e_4$, $v_2 = s^{-1}e_4$, $w_1 = \eta_1 - \alpha\eta_2$, $w_2 = s^{-1}\eta_2$. Then u_1, u_2, v_1, v_2 is a basis of U, w_1, w_2 is a basis of W, and $B(u_1, u_2) = B(v_1, v_2) = 0$, $B(u_1, v_1) = w_1$, $B(u_2, v_2) = w_1$, $B(u_2, v_1) = s^2\delta w_2$, $B(u_1, v_2) = w_2$. When $\delta = 0$, we see that B satisfies (ii). When δ is a non-square, we may choose s so that $s^2\delta = t$ and therefore B satisfies (iii).

The fact that in each case we have $Z * (B) = \{0\}$ is a simple computation using Lemma 5.8.

It remains to see that the three types are pairwise non-isomorphic. It is clear that BN can not satisfy (i) and either of (ii), (iii) as then it would be both decomposable and indecomposable. To see that B can not satisfy both (ii) and (iii), note that if it satisfies (ii) then the alternating bilinear form B_2 (corresponding to the basis w_1, w_2) is degenerate. On the other hand, if B satisfies (iii) then in every basis η_1, η_2 of W the corresponding alternating bilinear forms B_1, B_2 are both non-degenerate. □

Lemma 5.15. *There are two isomorphisms classes of object $B : U \times U \longrightarrow W$ of* ALT_p *which are non-degenerate of rank 2 and dimension 5, given by the following list:*

(i) *U has a basis u_1, u_2, v_0, v_1, v_2 and W has a basis w_1, w_2 such that $B(u_1, v_0) = w_1$, $B(u_i, v_i) = w_2$ for $i = 1, 2$, $B(u_1, u_2) = B(v_1, v_2) = B(u_2, v_0)B(u_i, v_j) = B(v_0, v_j) = 0$ for any $1 \leq i, j \leq 2$, $i \neq j$. The subspace $Z^*(B)$ is spanned by w_2.*

(ii) *U has a basis u_1, u_2, u_3, u_4, u_5 and W has a basis w_1, w_2 such that $B(u_1, u_2) = B(u_3, u_4) = w_1$, $B(u_2, u_3) = B(u_4, u_5) = w_2$, $B(u_i, u_j) = 0$ for all i, j such that $j - i \geq 2$. We have $Z^*(B) = \{0\}$.*

Proof. If B is decomposable then it satisfies (i) by Proposition 5.11. If B is indecomposable, then choosing a basis w_1, w_2 of W, the corresponding bialternating module is of type 3, i.e. isomorphic to F_2. This means that it satisfies (ii). The fact that in this case $Z^*(B) = \{0\}$ is a simple computation based on Lemma 5.8. □

Proof of Theorem 5.1: By Proposition 5.2, Theorem 5.5, and Remark 5.3 the theorem is just a translation to groups of the above results obtained for non-degenerate objects of rank 2 in ALT_p.

References

[1] F. R. Beyl, U. Felgner, P. Schmid, *On groups occurring as center factor groups*, J. Algebra 61 (1979), 161-177.

[2] F. R. Beyl, J. Tappe, *Group extensions, representations and the Schur multiplicator*, Lecture Notes in Mathematics, 958, Springer-Verlag 1982.

[3] N. Blackburn, L. Evens, *Schur multipliers of p-groups*, J. Reine Angew. Math. 309 (1979), 100-113.

[4] H. Heineken, *Nilpotent groups of class 2 that can appear as central quotient groups*, Rend. Sem. Mat. Univ. Padova, 84 (1990), 241-248.

[5] H. Heineken, D. Nikolova, *Class two nilpotent capable groups*, Bull. Austral. Math. Soc. 54 (1996), 347-352.

[6] G. Karpilovsky, **The Schur multiplier**, Oxford University Press 1987, .

[7] S. McKay, *Finite p-groups*, Queen Mary Maths Notes, 18, University of London, Queen Mary, School of Mathematical Sciences, London, 2000.

[8] R. Scharlau, *Paare alternierender Formen*, Math. Z. 147 (1976), 13-19.

Department of Mathematical Sciences, Binghamton University, P.O. Box 6000, Binghamton, NY 13892-6000, USA

E-mail address: `mazur@math.binghamton.edu`