http://ijgt.ui.ac.ir/

International Journal of Group Theory
ISSN (print): 2251-7650, ISSN (on-line): 2251-7669
Vol. x No. x (202x), pp. xx-xx.

www.ui.ac.ir

ON THE ENDOMORPHISM SEMIGROUPS OF EXTRA-SPECIAL p-GROUPS AND AUTOMORPHISM ORBITS

C. P. ANIL KUMAR AND SOHAM SWADHIN PRADHAN*

Abstract. For an odd prime p and a positive integer n, it is well known that there are two types of extra-special p-groups of order p^{2n+1}, first one is the Heisenberg group which has exponent p and the second one is of exponent p^2. This article mainly describes the endomorphism semigroups of both the types of extra-special p-groups and computes their cardinalities as polynomials in p for each n. Firstly a new way of representing the extra-special p-group of exponent p^2 is given. Using the representations, explicit formulae for any endomorphism and any automorphism of an extra-special p-group G for both the types are found. Based on these formulae, the endomorphism semigroup $\text{End}(G)$ and the automorphism group $\text{Aut}(G)$ are described. The endomorphism semigroup image of any element in G is found and the orbits under the action of the automorphism group $\text{Aut}(G)$ are determined. As a consequence it is deduced that, under the notion of degeneration of elements in G, the endomorphism semigroup $\text{End}(G)$ induces a partial order on the automorphism orbits when G is the Heisenberg group and does not induce when G is the extra-special p-group of exponent p^2. Finally we prove that the cardinality of isotropic subspaces of any fixed dimension in a non-degenerate symplectic space is a polynomial in p with non-negative integer coefficients. Using this fact we compute the cardinality of $\text{End}(G)$.

1. Introduction

1.1. **Preamble.** In the literature, for a prime p, a *special* group is defined as an elementary abelian p-group or a p-group where the Frattini subgroup, the commutator subgroup and the center coincide

Communicated by Patrizia Longobardi.
MSC(2010): Primary: 20D15; Secondary: 05E15.
Keywords: Extra-special p-Groups, Heisenberg Groups, Automorphism Groups, Endomorphism Semigroups, Symplectic Groups.
Received: 31 July 2021, Accepted: 29 September 2021.
Article Type: Research Paper.
*Corresponding author.
http://dx.doi.org/10.22108/IJGT.2021.129815.1708

.

and the center is of exponent p. An *extra-special* p-group is a non-abelian special group where the center is of order p. The extra-special p-groups arise in various contexts and are well studied groups. This article mainly studies the endomorphism semigroups of extra-special p-groups and also computes their cardinalities. As a consequence of this new study we answer the question of existence of a certain partial order on the automorphism orbits. However, we mention three different contexts in the literature where these groups arise.

Firstly, they occupy a distinctive place in the representation theory (D. E. Gorenstein [7, Chapter 5, Section 5, Theorem 5.4]), L. Dornhoff [5, Chapter 31, Theorem 31.5], H. Opolka [12]) and the cohomology of finite groups (D. J. Benson and J. F. Carlson [1],[2]).

Secondly, the extra-special p-groups have generated considerable interest in the study of its non-commuting subsets from a group theoretic and combinatorial view point (A. Y. M. Chin [4], M. Isaacs [3], H. Liu and Y. Wang [10], [11]).

Thirdly, the automorphism group of an extra-special p-group is also an important topic of study in the literature. D. L. Winter [14] has determined the structure of $\text{Aut}(G)$ for an extra-special p-group G. More precisely, he has proved that the automorphism group $\text{Aut}(G)$ is the semi-direct product of the normal subgroup N of centrally trivial automorphisms, (that is, those automorphisms which act trivially on the center $\mathcal{Z}(G)$) and a cyclic group of order $(p-1)$ generated by an automorphism of G which is an extension of the generator of $\text{Aut}(\mathcal{Z}(G))$. Moreover, it is shown that the quotient group $\frac{N}{Inn(G)}$ of N by the inner automorphism group $Inn(G)$ is isomorphic to a subgroup of a symplectic group whose structure is also known. It is also known that for an odd prime p, the group $\text{Aut}(G)$ is a split extension of the outer automorphism group $Out(G)$ by $Inn(G)$. For $p = 2$, this need not be true as shown by R. L. Griess Jr. [8]. H. Liu and Y. Wang [9] have determined the structure of the automorphism group of a generalized extra-special p-group.

We summarize briefly the contents of this article. For an odd prime p and a positive integer n, we compute and give an explicit expression for an endomorphism and an automorphism of an extra-special p-group of order p^{2n+1}. More precisely, first we present in an explicitly new way, the extra-special p-group of order p^{2n+1} and of exponent p^2 (Definition 1.3), just similar to one of the standard representations of the Heisenberg group of order p^{2n+1} (Definition 1.2). These definitions are advantageous to write down formulae for any endomorphism and any automorphism for both types of groups (in main Theorems Ω, Σ). Even though the structure of the automorphism group in the literature [14] exists, we derive the formulae for endomorphisms and automorphisms in a very natural and elegant manner. The importance of these explicit formulae is that they facilitate us to compute the endomorphism semigroup images of elements in the group and the automorphism orbits. The notion of *degeneration of elements* (Definition 1.5) via endomorphisms is introduced in the case of finite abelian p-groups by K. Dutta and A. Prasad [6]. This notion gives rise to a partial order on the automorphism orbits as observed by them in [6]. Here for the case of extra-special p-groups we explore the existence of a similar partial order on automorphism orbits. Finally here, we have computed the cardinality of the endomorphism semigroup and the cardinality of the automorphism group of an extra-special

p-group of order p^{2n+1} for both the types as a polynomial in p with integer coefficients for each n. Moreover, while computing the cardinality of the endomorphism group we prove that the cardinality of isotropic subspaces of any fixed dimension in a non-degenerate symplectic space is a polynomial in p with non-negative integer coefficients.

1.2. **Statement of Main Theorems.** We begin this section with a few required definitions in order to state the main theorems.

Definition 1.1 (Extra-special p-group and its Associated Symplectic Form)**.** *Let p be an odd prime. A finite group G is said to be an extra-special p-group if $[G,G]=G'=\mathcal{Z}(G)$ and $\mathcal{Z}(G)$ is of order p. In this case we have that $G'=\mathcal{Z}(G)=\Phi(G)$, the Frattini subgroup of G, and $\frac{G}{\mathcal{Z}(G)}$ is elementary abelian, isomorphic to $\mathbb{Z}_p^{2n}$ for some $n\in\mathbb{N}$. The group G hence has order p^{2n+1} (refer to D. Gorenstein [7,* Chapter 5, Section 5, Theorem 5.2, p. 204]*). It is equipped with a non-degenerate symplectic form $\langle\langle *,*\rangle\rangle$ defined as:*

$$\langle\langle *,*\rangle\rangle : \frac{G}{\mathcal{Z}(G)}\times\frac{G}{\mathcal{Z}(G)}\longrightarrow\mathbb{Z}_p, \langle\langle \overline{x},\overline{y}\rangle\rangle = f(x,y) \text{ with } \overline{x}=x\mathcal{Z}(G), \overline{y}=y\mathcal{Z}(G)$$

where $f: G\times G\longrightarrow\mathbb{Z}_p$ is defined by the equation $[x,y]=z^{f(x,y)}$ for a fixed generator z of $\mathcal{Z}(G)$ (refer to D. J. S. Robinson [13, Chapter 5, p. 145]*).*

Definition 1.2 (Extra-special p-group of First Type: Heisenberg Group)**.** *Let p be an odd prime, n be a positive integer and $\mathbb{Z}_p$ be the finite field order p. For $\underline{u}=(u_1,u_2,\ldots,u_n)^t$, $\underline{w}=(w_1,w_2,\ldots,w_n)^t\in\mathbb{Z}_p^n$ where t stands for transpose, define $\langle\underline{u},\underline{w}\rangle=\sum\limits_{i=1}^{n}u_iw_i\in\mathbb{Z}_p$. Then the Heisenberg group is defined as a set $ES_1(p,n)=\mathbb{Z}_p^n\oplus\mathbb{Z}_p^n\oplus\mathbb{Z}_p$ with the following group operation. For $(\underline{u}^i,\underline{w}^i,z^i)\in ES_1(p,n), i=1,2,$*

$$(\underline{u}^1,\underline{w}^1,z^1).(\underline{u}^2,\underline{w}^2,z^2)=(\underline{u}^1+\underline{u}^2,\underline{w}^1+\underline{w}^2,z^1+z^2+\langle\underline{u}^1,\underline{w}^2\rangle).$$

Definition 1.3 (Extra-special p-group of Second Type: Exponent p^2)**.** *Let p be an odd prime, n be a positive integer and $\mathbb{Z}_{p^i}=\mathbb{Z}/p^i\mathbb{Z}$ be the cyclic ring of order $p^i, i=1,2$. Let $i_{21}:\mathbb{Z}_p=\{0,1,2,\ldots,p-1\}\hookrightarrow\mathbb{Z}_{p^2}=\{0,1,2,\ldots,p^2-1\}$ with $i_{21}(a)=pa$ for $a\in\mathbb{Z}_p$ be the standard inclusion as an abelian group where the generator $1\in\mathbb{Z}_p$ maps to $p\in\mathbb{Z}_{p^2}$. For $\underline{u}=(u_2,u_3,\ldots,u_n)^t,\underline{w}=(w_2,w_3,\ldots,w_n)^t\in\mathbb{Z}_p^{n-1}$, define $\langle\underline{u},\underline{w}\rangle=\sum\limits_{i=2}^{n}u_iw_i\in\mathbb{Z}_p$. The extra-special p-group of second type is defined as a set*

$$ES_2(p,n)=\mathbb{Z}_{p^2}\oplus\mathbb{Z}_p^{n-1}\oplus\mathbb{Z}_p\oplus\mathbb{Z}_p^{n-1}$$

with the following group operation. For $(u_1^i,\underline{u}^i,w_1^i,\underline{w}^i)\in ES_2(p,n), i=1,2,$

$$\begin{aligned}&\big(u_1^1,\underline{u}^1,w_1^1,\underline{w}^1\big).\big(u_1^2,\underline{u}^2,w_1^2,\underline{w}^2\big)=\\&\qquad\big(u_1^1+u_1^2+i_{21}(w_1^2)u_1^1+i_{21}(\langle\underline{u}^1,\underline{w}^2\rangle),\underline{u}^1+\underline{u}^2,w_1^1+w_1^2,\underline{w}^1+\underline{w}^2\big).\end{aligned}$$

Remark 1.4. *Let p be an odd prime and G be an extra-special p-group. Then G is isomorphic to either $ES_1(p,n)$ or $ES_2(p,n)$ for some n. This fact is justified in Section 2. If σ is an endomorphism (resp. automorphism) of G then it gives rise to $\overline{\sigma}$ an endomorphism (resp. automorphism) of $\frac{G}{\mathcal{Z}(G)}$.*

Definition 1.5 (Partial Order on Orbits and the Notion of Degeneration)**.** *Let G be a finite group. Let $\mathrm{Aut}(G), \mathrm{End}(G)$ be its automorphism group and endomorphism semigroup respectively. Let S be the set of automorphism orbits in G. Let $x, y \in G$. We say y is endomorphic to x or x "degenerates to" y if there exists $\sigma \in \mathrm{End}(G)$ such that $\sigma(x) = y$. We say y is automorphic to x if there exists $\sigma \in \mathrm{Aut}(G)$ such that $\sigma(x) = y$. Let O_1, O_2 be two automorphism orbits in G. We say $O_2 \leq O_1$ if for some $x \in O_1$ and for some $y \in O_2$, we have that y is endomorphic to x. The order $\leq$ is in general need not be a partial order. We say the endomorphism semigroup induces a partial order $\leq$ on the automorphism orbits if whenever y is endomorphic to x and x is endomorphic to y then y is automorphic to x. The motivation for the notion of degeneration is given and introduced for the first time by A. Prasad and K. Dutta* [6].

Remark 1.6. *Let p be a prime and G be a finite abelian p-group. Then the endomorphism semigroup* $\mathrm{End}(G)$ *(here an endomorphism algebra) induces a partial order on automorphism orbits* [6].

We introduce some notation before stating the first main theorem.

- Let $e_i^n = (0, \ldots, 0, 1, 0, \ldots, 0)^t \in \mathbb{Z}_p^n$ be the vector with 1 in the i^{th} position and $0's$ elsewhere. Here t stands for transpose.
- Let $\underline{0}^n = (0, \ldots, 0)^t \in \mathbb{Z}_p^n$ be the zero vector.
- $\underline{u}, \underline{w}$ denote vectors in $\mathbb{Z}_p^n$ for some n.
- Let $\Delta = \begin{pmatrix} 0_{n\times n} & I_{n\times n} \\ -I_{n\times n} & 0_{n\times n} \end{pmatrix} \in M_{2n}(\mathbb{Z}_p)$.
- Let $symp^{scalar}(2n, \mathbb{Z}_p) = \{N \in M_{2n}(\mathbb{Z}_p) \mid N^t \Delta N = l\Delta, l \in \mathbb{Z}_p\}$.
- Let $Sp^{scalar}(2n, \mathbb{Z}_p) = \{M \in GL_{2n}(\mathbb{Z}_p) \mid M^t \Delta M = l\Delta, l \in \mathbb{Z}_p^*\}$.

We state the first main theorem of the article.

Theorem Ω.
Let p be an odd prime and n be a positive integer. Let $G = ES_1(p, n)$. Then:

(A) If $\sigma \in \mathrm{End}(G)$ then the induced endomorphism $\overline{\sigma}$ of $\frac{G}{\mathcal{Z}(G)}$ satisfies

$$\langle\langle \overline{\sigma}(\overline{x}), \overline{\sigma}(\overline{y}) \rangle\rangle = l \langle\langle \overline{x}, \overline{y} \rangle\rangle$$

where $l \in \mathbb{Z}_p$ is given by the equation $\sigma(z) = z^l$ for any generator z of $\mathcal{Z}(G)$.

(B) Consider the elements $x_i = (e_i^n, \underline{0}^n, 0), y_i = (\underline{0}^n, e_i^n, 0) \in G, 1 \leq i \leq n$. The endomorphisms σ are in bijection with 7-tuples $(A, B, C, D, \alpha, \beta, l)$ where

$$A = [a_{ij}]_{n\times n}, B = [b_{ij}]_{n\times n}, C = [c_{ij}]_{n\times n}, D = [d_{ij}]_{n\times n} \in M_n(\mathbb{Z}_p), l \in \mathbb{Z}_p$$

such that

$$\overline{\sigma} = \begin{pmatrix} A & C \\ D & B \end{pmatrix} \in symp^{scalar}(2n, \mathbb{Z}_p), \overline{\sigma}^t \Delta \overline{\sigma} = l\Delta \tag{1.1}$$

http://dx.doi.org/10.22108/IJGT.2021.129815.1708

with respect to the ordered basis $\{\overline{x}_1, \overline{x}_2, \dots, \overline{x}_n, \overline{y}_1, \overline{y}_2, \dots, \overline{y}_n\}$ *of* $\frac{G}{\mathcal{Z}(G)} = \mathbb{Z}_p^{2n}$ *and* $\alpha, \beta \in (\mathbb{Z}_p^n)^\vee$ *(dual of* $\mathbb{Z}_p^n$*) such that for* $\underline{u} = (u_1, u_2, \dots, u_n)^t, \underline{w} = (w_1, w_2, \dots, w_n)^t \in \mathbb{Z}_p^n, z \in \mathbb{Z}_p$ *we have*

$$\sigma(\underline{u}, \underline{w}, z) = (A\underline{u} + C\underline{w}, D\underline{u} + B\underline{w}, \widetilde{\sigma}(\underline{u}, \underline{w}, z)) \tag{1.2}$$

satisfying

$$\widetilde{\sigma}(\underline{u}, \underline{w}, z) = \alpha(\underline{u}) + \beta(\underline{w}) + lz + \frac{1}{2}\underline{u}^t(A^tD)\underline{u} + \frac{1}{2}\underline{w}^t(C^tB)\underline{w} + \underline{w}^t(C^tD)\underline{u}. \tag{1.3}$$

It is also implied that if σ *is given as in Equations 1.1, 1.2, 1.3 then* $\sigma \in \mathrm{End}(G)$*.*

(C) *An automorphism is a special case of an endomorhism* σ *for which* $l \in \mathbb{Z}_p^*$ *implying* $\overline{\sigma} \in Sp^{scalar}(2n, \mathbb{Z}_p)$*. It is also implied that if* σ *is given as in Equations 1.1, 1.2, 1.3 and* $l \neq 0$ *then* $\sigma \in \mathrm{Aut}(G)$*.*

(D) *The set of endomorphism semigroup images of an element* $g \in G$ *is given by:*
   - (a) $\{e\}$ *if* $g = e$ *and has cardinality* 1.
   - (b) $\mathcal{Z}(G)$ *if* $g \in \mathcal{Z}(G)\backslash\{e\}$ *and has cardinality* p.
   - (c) G *if* $g \in G\backslash\mathcal{Z}(G)$ *and has cardinality* p^{2n+1}.

(E) *There are three automorphism orbits in* G*. They are given by:*
   - (a) *The identity element* $\{e\}$ *and has cardinality* 1.
   - (b) *The central non-identity elements* $\mathcal{Z}(G)\backslash\{e\}$ *and has cardinality* $p-1$.
   - (c) *The non-central elements* $G\backslash\mathcal{Z}(G)$ *and has cardinality* $p^{2n+1} - p$.

(F) *The endomorphism semigroup induces a partial order (in fact a total order) on automorphism orbits which is given by*

$$\{e\} < \mathcal{Z}(G)\backslash\{e\} < G\backslash\mathcal{Z}(G).$$

We introduce some further notation before stating the second main theorem.

- $\widetilde{\underline{u}}, \widetilde{\underline{w}}$ denote vectors in $\mathbb{Z}_p^n$ for some n.
- Let $i_{21} : \mathbb{Z}_p \hookrightarrow \mathbb{Z}_{p^2}$ be the inclusion of the abelian group $\mathbb{Z}_p$ taking the generator $1 \in \mathbb{Z}_p$ to $p \in \mathbb{Z}_{p^2}$.
- For $u_1 \in \mathbb{Z}_{p^2}$, let $\overline{u}_1 \in \mathbb{Z}_p$ be its reduction modulo p.
- Let $\pi : \mathbb{Z}_p \oplus \mathbb{Z}_p^{n-1} \longrightarrow \mathbb{Z}_p^{n-1}$ be the projection ignoring the first co-ordinate.
- For $G = ES_2(p, n)$ let $H = p\mathbb{Z}_{p^2} \oplus \mathbb{Z}_p^{n-1} \oplus \mathbb{Z}_p \oplus \mathbb{Z}_p^{n-1}$, $K = p\mathbb{Z}_{p^2} \oplus \{\underline{0}^{n-1}\} \oplus \mathbb{Z}_p \oplus \{\underline{0}^{n-1}\} = \mathcal{Z}(H)$ and we have $\mathcal{Z}(G) = p\mathbb{Z}_{p^2} \oplus \{\underline{0}^{n-1}\} \oplus \{0\} \oplus \{\underline{0}^{n-1}\}$.

We state the second main theorem of the article.

Theorem Σ.
Let p *be an odd prime and* n *be a positive integer. Let* $G = ES_2(p, n)$*. Then:*

(A) *If* $\sigma \in \mathrm{End}(G)$ *then the induced endomorphism* $\overline{\sigma}$ *of* $\frac{G}{\mathcal{Z}(G)}$ *satisfies*

$$\langle\langle \overline{\sigma}(\overline{x}), \overline{\sigma}(\overline{y}) \rangle\rangle = l\langle\langle \overline{x}, \overline{y} \rangle\rangle$$

where $l \in \mathbb{Z}_p$ *is given by the equation* $\sigma(z) = z^l$ *for any generator* z *of* $\mathcal{Z}(G)$. *Let* $x_1 = (1, \underline{0}^{n-1}, 0, \underline{0}^{n-1}), y_1 = (0, \underline{0}^{n-1}, 1, \underline{0}^{n-1}), x_i = (0, e^{n-1}_{i-1}, 0, \underline{0}^{n-1}), y_i = (0, \underline{0}^{n-1}, 0, e^{n-1}_{i-1}) \in G$ *for* $2 \leq i \leq n$. *We have*

(a) *For each* $g \in G$ *there exists* $\sigma \in \mathrm{End}(G)$ *such that* $\sigma(x_1) = g$.

(b) *For any* $v \in \{x_2, \ldots, x_n, y_1, y_2, \ldots, y_n\}$ *and any* $h \in H$ *there exists* $\sigma \in \mathrm{End}(G)$ *such that* $\sigma(v) = h$. *Moreover for any* $\sigma \in \mathrm{End}(G), \sigma(v) \in H$.

(B) *The endomorphisms* σ *are in bijection with 7-tuples* $(A, B, C, D, \alpha, \beta, a)$ *where*

$$A = [a_{ij}]_{n\times n}, B = [b_{ij}]_{n\times n}, C = [c_{ij}]_{n\times n}, D = [d_{ij}]_{n\times n} \in M_n(\mathbb{Z}_p)$$

such that

$$\begin{aligned} &a_{12} = a_{13} = \ldots = a_{1n} = 0, c_{11} = c_{12} = \ldots = c_{1n} = 0 \\ &\overline{\sigma} = \begin{pmatrix} A & C \\ D & B \end{pmatrix} \in symp^{scalar}(2n, \mathbb{Z}_p), \overline{\sigma}^t \Delta \overline{\sigma} = a_{11}\Delta \end{aligned} \tag{1.4}$$

with respect to the ordered basis $\{\overline{x}_1, \overline{x}_2, \ldots, \overline{x}_n, \overline{y}_1, \overline{y}_2, \ldots, \overline{y}_n\}$ *of* $\frac{G}{\mathcal{Z}(G)} = \mathbb{Z}_p^{2n}$ *and* $\alpha \in (\mathbb{Z}_p^{n-1})^\vee, \beta \in (\mathbb{Z}_p^n)^\vee, a \in \mathbb{Z}_{p^2}$ *such that for* $(u_1, \underline{u}, w_1, \underline{w}) \in G$ *with* $\widetilde{\underline{u}} = \begin{pmatrix} \overline{u}_1 \\ \underline{u} \end{pmatrix} = (\widetilde{u}_1, \widetilde{u}_2, \ldots, \widetilde{u}_n)^t \in \mathbb{Z}_p^n, \widetilde{\underline{w}} = \begin{pmatrix} w_1 \\ \underline{w} \end{pmatrix} = (\widetilde{w}_1, \widetilde{w}_2, \ldots, \widetilde{w}_n)^t \in \mathbb{Z}_p^n$. *we have*

$$\sigma(u_1, \underline{u}, w_1, \underline{w}) = \sigma(u_1, \underline{u}, \widetilde{\underline{w}}) = (au_1 + i_{21}(s), \pi(A\widetilde{\underline{u}} + C\widetilde{\underline{w}}), D\widetilde{\underline{u}} + B\widetilde{\underline{w}}) \tag{1.5}$$

satisfying

$$\begin{aligned} &a \equiv a_{11} \mod p \text{ with } a_{11} \text{ allowed to be zero,} \\ &s = \alpha(\underline{u}) + \beta(\widetilde{\underline{w}}) + \frac{1}{2}\widetilde{\underline{u}}^t(A^tD)\widetilde{\underline{u}} + \frac{1}{2}\widetilde{\underline{w}}^t(C^tB)\widetilde{\underline{w}} + \widetilde{\underline{w}}^t(C^tD)\widetilde{\underline{u}}. \end{aligned} \tag{1.6}$$

It is also implied that if σ *is given as in Equations* 1.4, 1.5, 1.6 *then* $\sigma \in \mathrm{End}(G)$.

(C) *An automorphism is a special case of an endomorphism* σ *for which* $a_{11} \in \mathbb{Z}_p^*$ *implying that* $\overline{\sigma} \in Sp^{scalar}(2n, \mathbb{Z}_p)$. *It is also implied that if* σ *is given as in Equations* 1.4, 1.5, 1.6 *and* $a_{11} \neq 0 \mod p$ *then* $\sigma \in \mathrm{Aut}(G)$.

As a consequence we have in addition

(a) $b_{11} = 1$.

(b) $b_{21} = b_{31} = \ldots = b_{n1} = c_{21} = c_{31} = \ldots = c_{n1} = 0$.

(c) $\sigma(x_1) = x_1^{a_{11}} g$ *for some* $g \in H$.

(d) $\sigma(y_1) = y_1 h$ *for some* $h \in \mathcal{Z}(G)$.

(e) *For* $2 \leq i \leq n, \sigma(x_i), \sigma(y_i) \in H \backslash K$.

(D) *The set of endomorphism semigroup images of an element* $g \in G$ *is given by:*

(a) $\{e\}$ *if* $g = e$ *and has cardinality* 1.

(b) $\mathcal{Z}(G)$ *if* $g \in \mathcal{Z}(G) \backslash \{e\}$ *and has cardinality* p.

(c) H *if* $g \in H \backslash \mathcal{Z}(G)$ *and has cardinality* p^{2n}.

(d) *G if $g \in G\backslash H$ and has cardinality p^{2n+1}.*

(E) *There are $(p+2)$ automorphism orbits if $n=1$ and $(p+3)$ automorphism orbits if $n>1$. They are given by:*

(a) *The identity element $\{e\}$ and has cardinality 1.*

(b) *The central non-identity elements $\mathcal{Z}(G)\backslash\{e\}$ and has cardinality $p-1$.*

(c) *For $b \in \mathbb{Z}_p^*, \mathcal{O}_b = p\mathbb{Z}_{p^2} \times \{\underline{0}^{n-1}\} \times \{b\} \times \{\underline{0}^{n-1}\}$ and has cardinality p.*

(d) *$G\backslash H$, that is, all elements of order p^2 and has cardinality $p^{2n+1}-p^{2n}$.*

(e) *if $n>1$ then we have one more orbit $H\backslash K$ and has cardinality $p^{2n}-p^2$.*

(F) *In this group, there exist two elements which are endomorphic to each other but they are not automorphic. The endomorphism semigroup does not induce a partial order on automorphism orbits. In particular the set*

$$H\backslash\mathcal{Z}(G) = \bigsqcup_{b\in\mathbb{Z}_p^*}\mathcal{O}_b \bigsqcup (H\backslash K)$$

is a disjoint union of p automorphism orbits.

2. Preliminaries

It is well known that any extra-special p-group has exponent either p or p^2 and has order p^{2n+1} for some $n \in \mathbb{N}$. Moreover for any prime p and $n \in \mathbb{N}$ there are only two non-isomophic extra-special p-groups of order p^{2n+1} (refer to D. E. Gorenstein [7, Chapter 5, Theorem 5.2, p. 204]). We also observe that for an odd prime p, $ES_1(p,n)$ is an extra-special p-group of order p^{2n+1} and exponent p, $ES_2(p,n)$ is an extra-special p-group of order p^{2n+1} and exponent p^2. Hence it follows that for an odd prime p, if an extra-special p-group of order p^{2n+1} is of exponent p then it is isomorphic to $ES_1(p,n)$ and if it is of exponent p^2 then it is isomorphic to $ES_2(p,n)$. We also give one more way of presenting the group $ES_i(p,n)$ using a symplectic form for $i=1,2$ which will be useful to prove certain results.

Definition 2.1 (Alternative Definition for $ES_1(p,n)$)**.** *Let p be an odd prime. Let $\widetilde{ES}_1(p,n) = \mathbb{Z}_p^n \oplus \mathbb{Z}_p^n \oplus \mathbb{Z}_p$. Let $\langle\langle *,* \rangle\rangle$ be a non-degenerate symplectic bilinear form on $\mathbb{Z}_p^{2n}$ given by the matrix Δ with respect to the standard basis. Then the group structure on $\widetilde{ES}_1(p,n)$ is defined as: For $(\underline{u}^i, \underline{w}^i, z^i) \in \widetilde{ES}_1(p,n), i=1,2$ we have*

$$(\underline{u}^1,\underline{w}^1,z^1).(\underline{u}^2,\underline{w}^2,z^2) = \left(\underline{u}^1+\underline{u}^2, \underline{w}^1+\underline{w}^2, z^1+z^2+\frac{1}{2}\left\langle\left\langle \begin{pmatrix}\underline{u}^1\\ \underline{w}^1\end{pmatrix}, \begin{pmatrix}\underline{u}^2\\ \underline{w}^2\end{pmatrix}\right\rangle\right\rangle\right).$$

Definition 2.2 (Alternative Definition for $ES_2(p,n)$)**.** *Let p be an odd prime, n be a positive integer and $\mathbb{Z}_{p^i}$ be the cyclic ring of order $p^i, i=1,2$. Let $i_{21}: \mathbb{Z}_p = \{0,1,2,\ldots p-1\} \hookrightarrow \mathbb{Z}_{p^2} = \{0,1,2,\ldots,p^2-1\}$ with $i_{21}(a) = pa$ for $a \in \mathbb{Z}_p$ be the standard inclusion as an abelian group where the generator $1 \in \mathbb{Z}_p$ maps to $p \in \mathbb{Z}_{p^2}$. Let*

$$\widetilde{ES}_2(p,n) = \mathbb{Z}_{p^2} \oplus \mathbb{Z}_p^{n-1} \oplus \mathbb{Z}_p \oplus \mathbb{Z}_p^{n-1}.$$

Then the group structure on $\widetilde{ES}_2(p,n)$ is defined as follows. Let $\langle\langle *,* \rangle\rangle$ be the non-degenerate symplectic bilinear form on $\mathbb{Z}_p^{2n}$ given by the matrix Δ with respect to the standard basis. Let

http://dx.doi.org/10.22108/IJGT.2021.129815.1708

$(u_1^i, \underline{u}^i, w_1^i, \underline{w}^i) \in ES_2(p,n)$, $i = 1,2$. Let $\underline{\widetilde{u}}^i = \begin{pmatrix} \overline{u}_1^i \\ \underline{u}^i \end{pmatrix}, \underline{\widetilde{w}}^i = \begin{pmatrix} w_1^i \\ \underline{w}^i \end{pmatrix} \in \mathbb{Z}_p^n$ for $i = 1,2$ where $\overline{u}_1^i$ is reduction of u_1^i modulo p. Then

$$(u_1^1, \underline{u}^1, w_1^1, \underline{w}^1).(u_1^2, \underline{u}^2, w_1^2, \underline{w}^2) = \left(u_1^1 + u_1^2 + \frac{1}{2} i_{21}\left(\left\langle\left\langle \begin{pmatrix} \underline{\widetilde{u}}^1 \\ \underline{\widetilde{w}}^1 \end{pmatrix}, \begin{pmatrix} \underline{\widetilde{u}}^2 \\ \underline{\widetilde{w}}^2 \end{pmatrix} \right\rangle\right\rangle\right), \underline{u}^1 + \underline{u}^2, w_1^1 + w_1^2, \underline{w}^1 + \underline{w}^2\right).$$

Remark 2.3. *The analogy between the definitions of $ES_1(p,n)$ and $\widetilde{ES}_1(p,n)$ carries over to the definitions of $ES_2(p,n)$ and $\widetilde{ES}_2(p,n)$ as given in Theorem 2.4.*

We state the theorem.

Theorem 2.4. *$ES_l(p,n) \cong \widetilde{ES}_l(p,n), l = 1,2.$*

Proof. We prove for $l = 1$ first. Let $\underline{u}^i = (u_1^i, u_2^i, \ldots, u_n^i)^t, \underline{w}^i = (w_1^i, w_2^i, \ldots, w_n^i)^t \in \mathbb{Z}_p^n, i = 1,2$. Let $\underline{u} = (u_1, u_2, \ldots, u_n)^t, \underline{w} = (w_1, w_2, \ldots, w_n)^t \in \mathbb{Z}_p^n$. Let $\langle \underline{u}, \underline{w} \rangle = \sum_{j=1}^{n} u_j w_j \in \mathbb{Z}_p$. Let us fix the symplectic form as

$$\left\langle\left\langle \begin{pmatrix} \underline{u}^1 \\ \underline{w}^1 \end{pmatrix}, \begin{pmatrix} \underline{u}^2 \\ \underline{w}^2 \end{pmatrix} \right\rangle\right\rangle = \sum_{j=1}^{n} (u_j^1 w_j^2 - u_j^2 w_j^1) = \langle \underline{u}^1, \underline{w}^2 \rangle - \langle \underline{u}^2, \underline{w}^1 \rangle.$$

Define a map $\lambda : \widetilde{ES}_1(p,n) \longrightarrow ES_1(p,n)$ given by

$$\lambda(\underline{u}, \underline{w}, z) = (\underline{u}, \underline{w}, z + \frac{1}{2}(\sum_{j=1}^{n} u_j w_j)) = \left(\underline{u}, \underline{w}, z + \frac{1}{2}\langle \underline{u}, \underline{w} \rangle\right).$$

It is easy to check that λ is an isomorphism.

We prove for $l = 2$. For $i = 1,2$ let $u_1^i \in \mathbb{Z}_{p^2}, w_1^i \in \mathbb{Z}_p, \underline{u}^i, \underline{w}^i \in \mathbb{Z}_p^{n-1}$. For $i = 1,2$ let $\underline{\widetilde{u}}^i = \begin{pmatrix} \overline{u}_1^i \\ \underline{u}^i \end{pmatrix} = (\widetilde{u}_1^i, \widetilde{u}_2^i, \ldots, \widetilde{u}_n^i)^t, \underline{\widetilde{w}}^i = \begin{pmatrix} w_1^i \\ \underline{w}^i \end{pmatrix} = (\widetilde{w}_1^i, \widetilde{w}_2^i, \ldots, \widetilde{w}_n^i)^t \in \mathbb{Z}_p^n$ where $\overline{u}_1^i$ is reduction modulo p of $u_1^i \in \mathbb{Z}_{p^2}$. Let $u_1 \in \mathbb{Z}_{p^2}, w_1 \in \mathbb{Z}_p, \underline{u}, \underline{w} \in \mathbb{Z}_p^{n-1}$. Let $\underline{\widetilde{u}} = \begin{pmatrix} \overline{u}_1 \\ \underline{u} \end{pmatrix} = (\widetilde{u}_1, \widetilde{u}_2, \ldots, \widetilde{u}_n)^t, \underline{\widetilde{w}} = \begin{pmatrix} \overline{w}_1 \\ \underline{w} \end{pmatrix} = (\widetilde{w}_1, \widetilde{w}_2, \ldots, \widetilde{w}_n)^t \in \mathbb{Z}_p^n$. Let $\langle \underline{\widetilde{u}}, \underline{\widetilde{w}} \rangle = \sum_{j=1}^{n} \widetilde{u}_j \widetilde{w}_j \in \mathbb{Z}_p$. The symplectic form is given as

$$\left\langle\left\langle \begin{pmatrix} \underline{\widetilde{u}}^1 \\ \underline{\widetilde{w}}^1 \end{pmatrix}, \begin{pmatrix} \underline{\widetilde{u}}^2 \\ \underline{\widetilde{w}}^2 \end{pmatrix} \right\rangle\right\rangle = \sum_{j=1}^{n} (\widetilde{u}_j^1 \widetilde{w}_j^2 - \widetilde{u}_j^2 \widetilde{w}_j^1) = \langle \underline{\widetilde{u}}^1, \underline{\widetilde{w}}^2 \rangle - \langle \underline{\widetilde{u}}^2, \underline{\widetilde{w}}^1 \rangle.$$

Define a map $\delta : \widetilde{ES}_2(p,n) \longrightarrow ES_2(p,n)$ given by

$$\delta(u_1, \underline{u}, w_1, \underline{w}) = \left(u_1 + \frac{1}{2} i_{21}(\langle \underline{\widetilde{u}}, \underline{\widetilde{w}} \rangle), \underline{u}, w_1, \underline{w}\right).$$

It is easy to check that δ is an isomorphism. This completes the proof of the theorem. □

We prove a general proposition regarding extra-special p-groups.

Proposition 2.5. *Let G be an extra-special p-group (refer to Definition 1.1). Let $z \in \mathcal{Z}(G)$ be a fixed generator such that $[g_1, g_2] = z^{f(g_1,g_2)}$ for $g_1, g_2 \in G$ and $f : G \times G \longrightarrow \mathbb{Z}_p$. Let $\overline{f} : \frac{G}{\mathcal{Z}(G)} \times \frac{G}{\mathcal{Z}(G)} \longrightarrow \mathbb{Z}_p$ be its associated non-degenerate symplectic bilinear form defined as $\overline{f}(\overline{g_1}, \overline{g_2}) = f(g_1, g_2)$. Then we have:*

(1) For $\sigma \in \mathrm{End}(G)$, $\overline{f}(\overline{\sigma}(\overline{g_1}), \overline{\sigma}(\overline{g_2})) = l\overline{f}(\overline{g_1}, \overline{g_2})$ for any $g_1, g_2 \in G$ where $\sigma(z) = z^l, l \in \mathbb{Z}_p$ and $\overline{\sigma}$ is the induced endomorphism of $\frac{G}{\mathcal{Z}(G)}$.
(2) For $\sigma \in \mathrm{Aut}(G)$, $\overline{f}(\overline{\sigma}(\overline{g_1}), \overline{\sigma}(\overline{g_2})) = l\overline{f}(\overline{g_1}, \overline{g_2})$ for any $g_1, g_2 \in G$ where $\sigma(z) = z^l, l \in \mathbb{Z}_p^*$ and $\overline{\sigma}$ is the induced automorphism of $\frac{G}{\mathcal{Z}(G)}$.

Proof. We have

$$z^{lf(g_1,g_2)} = \sigma(z^{f(g_1,g_2)}) = \sigma[g_1, g_2] = [\sigma(g_1), \sigma(g_2)] = z^{f(\sigma(g_1),\sigma(g_2))}.$$

Now the proposition follows. □

2.1. **Some Commutative Diagrams on Extra-special p-Groups.** We show that certain diagrams of groups and maps for the extra-special p-group of the first type are commutative. First we observe that $\mathcal{Z}(ES_1(p, n)) = \{\underline{0}^n\} \oplus \{\underline{0}^n\} \oplus \mathbb{Z}_p = \mathcal{Z}(\widetilde{ES}_1(p, n))$. Let

$$\pi_1 : ES_1(p, n) = \mathbb{Z}_p^n \oplus \mathbb{Z}_p^n \oplus \mathbb{Z}_p \longrightarrow \frac{ES_1(p, n)}{\mathcal{Z}(ES_1(p, n))} = \mathbb{Z}_p^n \oplus \mathbb{Z}_p^n,$$

$$\widetilde{\pi}_1 : \widetilde{ES}_1(p, n) = \mathbb{Z}_p^n \oplus \mathbb{Z}_p^n \oplus \mathbb{Z}_p \longrightarrow \frac{\widetilde{ES}_1(p, n)}{\mathcal{Z}(\widetilde{ES}_1(p, n))} = \mathbb{Z}_p^n \oplus \mathbb{Z}_p^n$$

be the quotient maps of groups. Let the induced maps be

$$\Phi_1 : \mathrm{Aut}(ES_1(p, n)) \longrightarrow \mathrm{Aut}\left(\frac{ES_1(p, n)}{\mathcal{Z}(ES_1(p, n))}\right) = GL_{2n}(\mathbb{Z}_p),$$

$$\widetilde{\Phi}_1 : \mathrm{Aut}(\widetilde{ES}_1(p, n)) \longrightarrow \mathrm{Aut}\left(\frac{\widetilde{ES}_1(p, n)}{\mathcal{Z}(\widetilde{ES}_1(p, n))}\right) = GL_{2n}(\mathbb{Z}_p).$$

Then the following two diagrams commute.

$$\begin{array}{ccccccccc}
0 \longrightarrow & \mathbb{Z}_p = \mathcal{Z}(\widetilde{ES}_1(p, n)) & \hookrightarrow & \widetilde{ES}_1(p, n) & \xrightarrow{\widetilde{\pi}_1} & \mathbb{Z}_p^n \oplus \mathbb{Z}_p^n & \longrightarrow 0 \\
& Id \downarrow \| & & \lambda \downarrow & & Id \downarrow \| & \\
0 \longrightarrow & \mathbb{Z}_p = \mathcal{Z}(ES_1(p, n)) & \hookrightarrow & ES_1(p, n) & \xrightarrow{\pi_1} & \mathbb{Z}_p^n \oplus \mathbb{Z}_p^n & \longrightarrow 0
\end{array}$$

(2.1)

$$\begin{array}{ccc}
\mathrm{Aut}(\widetilde{ES}_1(p, n)) & \xrightarrow{\widetilde{\Phi}_1} & GL_{2n}(\mathbb{Z}_p) \\
\lambda\circ(*)\circ\lambda^{-1} \downarrow \cong & & Id \downarrow \| \\
\mathrm{Aut}(ES_1(p, n)) & \xrightarrow{\Phi_1} & GL_{2n}(\mathbb{Z}_p)
\end{array}$$

Here λ is as defined in the proof of Theorem 2.4. In particular we get that $Im(\widetilde{\Phi}_1) = Im(\Phi_1) \subset GL_{2n}(\mathbb{Z}_p)$.

Proposition 2.6. *$Im(\widetilde{\Phi}_1) = Im(\Phi_1) = Sp^{scalar}(2n, \mathbb{Z}_p)$.*

Proof. For $\overline{\sigma} \in Sp^{scalar}(2n, \mathbb{Z}_p)$ we can define an automorphism $\sigma \in \mathrm{Aut}(\widetilde{ES}_1(p,n))$ such that $\widetilde{\Phi}_1(\sigma) = \overline{\sigma}$ as follows.

$$\sigma(\underline{v}, z) = (\overline{\sigma}(\underline{v}), lz) \text{ where } \overline{\sigma}^t \Delta \overline{\sigma} = l\Delta, (\underline{v}, z) \in \mathbb{Z}_p^{2n} \oplus \mathbb{Z}_p = \widetilde{ES}_1(p,n).$$

Hence we have $Sp^{scalar}(2n, \mathbb{Z}_p) \subseteq Im(\widetilde{\Phi}_1) = Im(\Phi_1) \subset GL_{2n}(\mathbb{Z}_p)$. Now use Proposition 2.5 to conclude equality. $\square$

We show that certain diagrams of groups and maps for the extra-special p-group of the second type are commutative. First we observe that $\mathcal{Z}(ES_2(p,n)) = p\mathbb{Z}_{p^2} \oplus \{\underline{0}^{n-1}\} \oplus \{0\} \oplus \{\underline{0}^{n-1}\} = \mathcal{Z}(\widetilde{ES}_2(p,n))$. Let

$$\begin{aligned}
\pi_2 : ES_2(p,n) = \mathbb{Z}_{p^2} \oplus \mathbb{Z}_p^{n-1} \oplus \mathbb{Z}_p \oplus \mathbb{Z}_p^{n-1} \longrightarrow \\
\frac{ES_2(p,n)}{\mathcal{Z}(ES_2(p,n))} = \mathbb{Z}_p \oplus \mathbb{Z}_p^{n-1} \oplus \mathbb{Z}_p \oplus \mathbb{Z}_p^{n-1} = \mathbb{Z}_p^{2n}, \\
\widetilde{\pi}_2 : \widetilde{ES}_2(p,n) = \mathbb{Z}_{p^2} \oplus \mathbb{Z}_p^{n-1} \oplus \mathbb{Z}_p \oplus \mathbb{Z}_p^{n-1} \longrightarrow \\
\frac{\widetilde{ES}_2(p,n)}{\mathcal{Z}(\widetilde{ES}_2(p,n))} = \mathbb{Z}_p \oplus \mathbb{Z}_p^{n-1} \oplus \mathbb{Z}_p \oplus \mathbb{Z}_p^{n-1} = \mathbb{Z}_p^{2n},
\end{aligned}$$

be the quotient maps of groups. Let the induced maps be

$$\Phi_2 : \mathrm{Aut}(ES_2(p,n)) \longrightarrow \mathrm{Aut}\left(\frac{ES_2(p,n)}{\mathcal{Z}(ES_2(p,n))}\right) = GL_{2n}(\mathbb{Z}_p),$$
$$\widetilde{\Phi}_2 : \mathrm{Aut}(\widetilde{ES}_2(p,n)) \longrightarrow \mathrm{Aut}\left(\frac{\widetilde{ES}_2(p,n)}{\mathcal{Z}(\widetilde{ES}_2(p,n))}\right) = GL_{2n}(\mathbb{Z}_p).$$

Then the following two diagrams commute.

$$\begin{array}{ccccccccc}
0 \longrightarrow & p\mathbb{Z}_{p^2} = \mathcal{Z}(\widetilde{ES}_2(p,n)) & \hookrightarrow & \widetilde{ES}_2(p,n) & \xrightarrow{\widetilde{\pi}_2} & \mathbb{Z}_p^{2n} & \longrightarrow 0 \\
& Id \downarrow \| & & \delta \downarrow & & Id \downarrow \| & \\
0 \longrightarrow & p\mathbb{Z}_{p^2} = \mathcal{Z}(ES_2(p,n)) & \hookrightarrow & ES_2(p,n) & \xrightarrow{\pi_2} & \mathbb{Z}_p^{2n} & \longrightarrow 0
\end{array}$$

(2.2)

$$\begin{array}{ccc}
\mathrm{Aut}(\widetilde{ES}_2(p,n)) & \xrightarrow{\widetilde{\Phi}_2} & GL_{2n}(\mathbb{Z}_p) \\
\delta\circ(*)\circ\delta^{-1} \downarrow \cong & & Id \downarrow \| \\
\mathrm{Aut}(ES_2(p,n)) & \xrightarrow{\Phi_2} & GL_{2n}(\mathbb{Z}_p)
\end{array}$$

Here δ is as defined in the proof of Theorem 2.4. In particular we get that $Im(\widetilde{\Phi}_2) = Im(\Phi_2) \subset GL_{2n}(\mathbb{Z}_p)$. We describe this image exactly in Proposition 4.1.

3. Proof of the First Main Theorem

In this section we prove first main Theorem Ω.

Proof. Here $G = ES_1(p,n)$. Let $\sigma \in \text{End}(G)$ and $\overline{\sigma} \in \text{End}(\frac{G}{\mathcal{Z}(G)}) = M_{2n}(\mathbb{Z}_p)$. Let $\overline{\sigma} = \begin{pmatrix} A & C \\ D & B \end{pmatrix}$ with $A, B, C, D \in M_n(\mathbb{Z}_p)$. Hence there exists a map $\widetilde{\sigma} : G \longrightarrow \mathbb{Z}_p$ such that for $(\underline{u}, \underline{w}, z) \in G$ we have $\sigma(\underline{u}, \underline{w}, z) = (A\underline{u} + C\underline{w}, D\underline{u} + B\underline{w}, \widetilde{\sigma}(\underline{u}, \underline{w}, z))$. Using Proposition 2.5 we have

$$\overline{\sigma} = \begin{pmatrix} A & C \\ D & B \end{pmatrix} \in symp^{scalar}(2n, \mathbb{Z}_p)$$

and $A^tB - D^tC = l.\text{Id}_{n\times n}$ where $\overline{\sigma}^t\Delta\overline{\sigma} = l\Delta$. So we also have $A^tD = D^tA, C^tB = B^tC$. This computation does not give the explicit form of σ as we do not know $\widetilde{\sigma}$.
We compute the explicit form of $\widetilde{\sigma}$. The homomorphism condition gives us that, for $(\underline{u}^i, \underline{w}^i, z^i) \in G, i = 1, 2$,

$$\begin{aligned}\widetilde{\sigma}(\underline{u}^1 + \underline{u}^2, \underline{w}^1 + \underline{w}^2, z^1 + z^2 + \langle \underline{u}^1, \underline{w}^2\rangle) = \widetilde{\sigma}(\underline{u}^1, \underline{w}^1, z^1) + \widetilde{\sigma}(\underline{u}^2, \underline{w}^2, z^2) + \\ \langle A\underline{u}^1 + C\underline{w}^1, D\underline{u}^2 + B\underline{w}^2\rangle.\end{aligned} \tag{3.1}$$

Putting $\underline{w}^1 = \underline{w}^2 = \underline{0}^n, z^1 = z^2 = 0$ we get that

$$\widetilde{\sigma}(\underline{u}^1 + \underline{u}^2, \underline{0}^n, 0) = \widetilde{\sigma}(\underline{u}^1, \underline{0}^n, 0) + \widetilde{\sigma}(\underline{u}^2, \underline{0}^n, 0) + \langle A\underline{u}^1, D\underline{u}^2\rangle. \tag{3.2}$$

Similarly we have

$$\widetilde{\sigma}(\underline{0}^n, \underline{w}^1 + \underline{w}^2, 0) = \widetilde{\sigma}(\underline{0}^n, \underline{w}^1, 0) + \widetilde{\sigma}(\underline{0}^n, \underline{w}^2, 0) + \langle C\underline{w}^1, B\underline{w}^2\rangle. \tag{3.3}$$

We conclude the following.

- $\widetilde{\sigma}(\underline{0}^n, \underline{0}^n, 0) = 0$.
- Since $(\underline{u}, \underline{w}, z) = (\underline{0}^n, \underline{w}, z).(\underline{u}, \underline{0}^n, 0)$ and $(\underline{0}^n, \underline{w}, z) = (\underline{0}^n, \underline{w}, 0).(\underline{0}^n, \underline{0}^n, z)$ we have from Equation 3.1 that

$$\begin{aligned}\widetilde{\sigma}(\underline{u}, \underline{w}, z) &= \widetilde{\sigma}(\underline{0}^n, \underline{w}, z) + \widetilde{\sigma}(\underline{u}, \underline{0}^n, 0) + \langle C\underline{w}, D\underline{u}\rangle \\ &= \widetilde{\sigma}(\underline{u}, \underline{0}^n, 0) + \widetilde{\sigma}(\underline{0}^n, \underline{w}, 0) + \widetilde{\sigma}(\underline{0}^n, \underline{0}^n, z) + \langle C\underline{w}, D\underline{u}\rangle.\end{aligned} \tag{3.4}$$

- If we define $\widetilde{\sigma}_1(\underline{u}) = \widetilde{\sigma}(\underline{u}, \underline{0}^n, 0) - \frac{1}{2}\langle A\underline{u}, D\underline{u}\rangle$ then from Equation 3.2 and $A^tD = D^tA$ we conclude that $\widetilde{\sigma}_1(\underline{0}^n) = 0, \widetilde{\sigma}_1(\underline{u}^1 + \underline{u}^2) = \widetilde{\sigma}_1(\underline{u}^1) + \widetilde{\sigma}_1(\underline{u}^2)$. Hence

$$\widetilde{\sigma}(\underline{u}, \underline{0}^n, 0) = \alpha(\underline{u}) + \frac{1}{2}\langle A\underline{u}, D\underline{u}\rangle \text{ for some } \alpha \in (\mathbb{Z}_p^n)^\vee. \tag{3.5}$$

- Similarly from Equation 3.3 and $C^tB = B^tC$ we conclude that

$$\widetilde{\sigma}(\underline{0}^n, \underline{w}, 0) = \beta(\underline{w}) + \frac{1}{2}\langle C\underline{w}, B\underline{w}\rangle \text{ for some } \beta \in (\mathbb{Z}_p^n)^\vee. \tag{3.6}$$

http://dx.doi.org/10.22108/IJGT.2021.129815.1708

- We observe that

$$\widetilde{\sigma}(\underline{0}^n,\underline{0}^n,z^1+z^2)=\widetilde{\sigma}(\underline{0}^n,\underline{0}^n,z^1)+\widetilde{\sigma}(\underline{0}^n,\underline{0}^n,z^2) \Rightarrow \widetilde{\sigma}(\underline{0}^n,\underline{0}^n,z)=lz \text{ for some } l\in\mathbb{Z}_p. \tag{3.7}$$

- From Equations 3.4, 3.5, 3.6, 3.7 we conclude that

$$\widetilde{\sigma}(\underline{u},\underline{w},z)=\alpha(\underline{u})+\beta(\underline{w})+lz+\frac{1}{2}\langle A\underline{u},D\underline{u}\rangle+\frac{1}{2}\langle C\underline{w},B\underline{w}\rangle+\langle C\underline{w},D\underline{u}\rangle \tag{3.8}$$

for some $\alpha,\beta\in(\mathbb{Z}_p^n)^\vee, l\in\mathbb{Z}_p$ where l satisfies $\overline{\sigma}^t\Delta\sigma=l\Delta$.

Conversely if $\overline{\sigma}=\begin{pmatrix}A & C\\ D & B\end{pmatrix}\in symp^{scalar}(2n,\mathbb{Z}_p)$ with $\overline{\sigma}^t\Delta\overline{\sigma}=l\Delta$ and Equation 3.8 holds, then it is clear that Equation 3.1 holds and σ is an endomorphism of G. This proves (A),(B) in Theorem Ω. In case of $\mathrm{Aut}(G)$, the proof is similar except that here for $\sigma\in\mathrm{Aut}(G)$, we have $l\in\mathbb{Z}_p^*$, that is, it is not allowed to be zero. This proves (C) in Theorem Ω.
We prove (D). In case $\sigma\in\mathrm{End}(G)$ we allow l to be zero. Using Equations 1.2, 1.3, we conclude that the endomorphism semigroup image of $g\in G$ is given by (a) $\{e\}$ if $g=e$, (b) $\mathcal{Z}(G)$ if $g\in\mathcal{Z}(G)\backslash\{e\}$, (c) G if $g\in G\backslash\mathcal{Z}(G)$.
We prove (E). Using Equations 1.2, 1.3 we conclude that there are three automorphism orbits as follows. The identity element $\{e\}$ is clearly an orbit. The non-identity central elements $\mathcal{Z}(G)\backslash\{e\}$ form an orbit, as automorphisms act transitively on the non-identity central elements because we can choose any non-zero value for l. Now the non-central elements $G\backslash\mathcal{Z}(G)$ form an orbit as the group $Sp^{scalar}(2n,\mathbb{Z}_p)$ acts transitively on $\mathbb{Z}_p^{2n}\backslash\{\underline{0}^{2n}\}$ and using inner automorphisms we can change the central co-ordinate to any central co-ordinate for the non-central elements.
It is clear that endomorphism semigroup $\mathrm{End}(G)$ induces a partial order (total order) on the automorphism orbits. This proves (F) and thereby completes the proof of first main Theorem Ω. $\square$

Using first main Theorem Ω we have the following corollary.

Corollary 3.1. *Let $G=ES_1(p,n)$.*

(1) $\sigma\in\mathrm{Aut}(G)$ is an inner-automorphism if and only if $\overline{\sigma}=Id_{2n\times 2n}$. In this case $\widetilde{\sigma}(\underline{u},\underline{w},z)=\alpha(\underline{u})+\beta(\underline{w})+z$ for some $\alpha,\beta\in(\mathbb{Z}_p^n)^\vee$ for any $(\underline{u},\underline{w},z)\in G$.

(2) We have an exact sequence

$$1\longrightarrow\frac{G}{\mathcal{Z}(G)}\cong Inn(G)\hookrightarrow\mathrm{Aut}(G)\longrightarrow Sp^{scalar}(2n,\mathbb{Z}_p)\longrightarrow 1.$$

(3)

$$\begin{aligned}|\,\mathrm{Aut}(G)\,|&=p^{2n}\,|\,Sp^{scalar}(2n,\mathbb{Z}_p)\,|\\&=p^{2n}(p-1)\,|\,Sp(2n,\mathbb{Z}_p)\,|=p^{n^2+2n}(p-1)\prod_{j=1}^{n}(p^{2j}-1).\end{aligned}$$

The cardinality of $\mathrm{End}(G)$ for $G=ES_1(p,n)$ is computed in Section 5, Theorem 5.3.

4. Proof of the Second Main Theorem

In this section we prove second main Theorem Σ.

Proof. Here $G = ES_2(p,n)$. Let $\sigma \in \mathrm{End}(G)$ and $\overline{\sigma} \in \mathrm{End}(\frac{G}{\mathcal{Z}(G)}) = M_{2n}(\mathbb{Z}_p)$. Let

$$\overline{\sigma} = \begin{pmatrix} A & C \\ D & B \end{pmatrix} \text{ with } A = [a_{ij}], B = [b_{ij}], C = [c_{ij}], D = [d_{ij}] \in M_n(\mathbb{Z}_p).$$

Then for $x_1 = (1, \underline{0}^{n-1}, 0, \underline{0}^{n-1}), \sigma(x_1) = (a_{11}, \underline{0}^{n-1}, 0, \underline{0}^{n-1}).g$ for some element $g \in H$. So for $z = (p, \underline{0}^{n-1}, 0, \underline{0}^{n-1}) \in \mathcal{Z}(G)$ we have $\sigma(z) = (a_{11}p, \underline{0}^{n-1}, 0, \underline{0}^{n-1})$. Now using Proposition 2.5 we have $\overline{\sigma} \in symp^{scalar}(2n, \mathbb{Z}_p)$ and $A^tB - D^tC = a_{11}.\mathrm{Id}_{n\times n}$ where $\overline{\sigma}^t\Delta\overline{\sigma} = a_{11}\Delta$. We also have $A^tD = D^tA, C^tB = B^tC$.

Since the order of x_1 is p^2 we have $o(\sigma(x_1)) = p^2 \Longleftrightarrow a_{11} \not\equiv 0 \mod p$. Since the order of $x_i = (0, e_{i-1}^{n-1}, 0, \underline{0}^{n-1})$ is p we have $o(\sigma(x_i)) \mid p \Rightarrow a_{1i} \equiv 0 \mod p$ for $2 \leq i \leq n$. Since the order of $y_i = (0, \underline{0}^{n-1}, 0, e_{i-1}^{n-1})$ is p we have $o(\sigma(y_i)) \mid p \Rightarrow c_{1i} \equiv 0 \mod p$ for $2 \leq i \leq n$. Similarly for $y_1 = (0, \underline{0}^{n-1}, 1, \underline{0}^{n-1})$ we have $c_{11} \equiv 0 \mod p$.

For $(u_1, \underline{u}, w_1, \underline{w}) \in G$, let $\widetilde{\underline{u}} = \begin{pmatrix} \overline{u}_1 \\ \underline{u} \end{pmatrix} = (\widetilde{u}_1, \widetilde{u}_2, \ldots, \widetilde{u}_n)^t \in \mathbb{Z}_p^n, \widetilde{\underline{w}} = \begin{pmatrix} w_1 \\ \underline{w} \end{pmatrix} = (\widetilde{w}_1, \widetilde{w}_2, \ldots, \widetilde{w}_n)^t \in \mathbb{Z}_p^n$. Hence we have

$$\sigma(u_1, \underline{u}, w_1, \underline{w}) = (\widetilde{a}u_1 + i_{21}(\widetilde{s}), \pi(A\widetilde{\underline{u}} + C\widetilde{\underline{w}}), D\widetilde{\underline{u}} + B\widetilde{\underline{w}})$$

for some $\widetilde{a} \in \mathbb{Z}_{p^2}, \widetilde{s} \in \mathbb{Z}_p$ such that $\widetilde{a} \equiv a_{11} \mod p$.

This computation does not give the explicit form of σ as we do not know $i_{21}(\widetilde{s})$. Just similar to the proof of Theorem Ω(B) we compute $\widetilde{s}$ and obtain

$$\widetilde{s} = \widetilde{\alpha}(\widetilde{\underline{u}}) + \beta(\widetilde{\underline{w}}) + \frac{1}{2}\langle A\widetilde{\underline{u}}, D\widetilde{\underline{u}}\rangle + \frac{1}{2}\langle C\widetilde{\underline{w}}, B\widetilde{\underline{w}}\rangle + \langle C\widetilde{\underline{w}}, D\widetilde{\underline{u}}\rangle$$

for some $\widetilde{\alpha}, \beta \in (\mathbb{Z}_p^n)^\vee$. Here we can change $\widetilde{\alpha}(\widetilde{\underline{u}})$ to $\alpha(\underline{u})$ for some $\alpha \in (\mathbb{Z}_p^{n-1})^\vee$ by shifting multiple of $\overline{u}_1$ to the first term in $\widetilde{a}u_1 + i_{21}(\widetilde{s})$ to obtain $au_1 + i_{21}(s)$ without changing the residue class of $\widetilde{a}$ modulo p. So we get

$$\sigma(u_1, \underline{u}, w_1, \underline{w}) = (au_1 + i_{21}(s), \pi(A\widetilde{\underline{u}} + C\widetilde{\underline{w}}), D\widetilde{\underline{u}} + B\widetilde{\underline{w}}) \tag{4.1}$$

for some $a \in \mathbb{Z}_{p^2}$ such that $a \equiv a_{11} \mod p$ where

$$s = \alpha(\underline{u}) + \beta(\widetilde{\underline{w}}) + \frac{1}{2}\langle A\widetilde{\underline{u}}, D\widetilde{\underline{u}}\rangle + \frac{1}{2}\langle C\widetilde{\underline{w}}, B\widetilde{\underline{w}}\rangle + \langle C\widetilde{\underline{w}}, D\widetilde{\underline{u}}\rangle. \tag{4.2}$$

Conversely if σ is as given in Equation 4.1 and s in Equation 4.2 with the matrix $\overline{\sigma} = \begin{pmatrix} A & C \\ D & B \end{pmatrix} \in symp^{scalar}(2n, \mathbb{Z}_p)$ satisfying $\overline{\sigma}^t\Delta\overline{\sigma} = a_{11}\Delta$ and $a_{12} = \ldots = a_{1n} = c_{11} = c_{12} = \ldots = c_{1n} = 0$ then $\sigma \in \mathrm{End}(G)$. Also in the converse if in addition $a_{11} \not\equiv 0 \mod p$, that is, $a \in \mathbb{Z}_{p^2}^*$ then $\sigma \in \mathrm{Aut}(G)$.

The additional consequences of $\sigma \in \mathrm{Aut}(G)$ are as follows. We conclude that σ induces automorphisms of the following three subgroups of G.

$$H = \langle x_1^p, x_2, x_3, \ldots, x_n, y_1, y_2, \ldots, y_n\rangle, K = \mathcal{Z}(H) = \langle x_1^p, y_1\rangle, \mathcal{Z}(G) = \langle x_1^p\rangle.$$

http://dx.doi.org/10.22108/IJGT.2021.129815.1708

Hence $\sigma(y_1) = y_1^{b_{11}} x_1^{pr}$ with $b_{11} \neq 0$, for some $r \in \{0, 1, \ldots, p-1\}$ and $b_{j1} = 0 = c_{j1},\ 2 \leq j \leq n$. We have $A^t B - D^t C = a_{11} \mathrm{Id}_{n\times n} \Rightarrow a_{11} b_{11} \equiv a_{11} \mod p \Rightarrow b_{11} = 1$. This proves (A),(B),(C).

We prove (D). Using Equations 1.5, 1.6, the endomorphic images of any element g in G is given as follows. It is $\{e\}$ if $g = e$. It is $\mathcal{Z}(G)$ if $g \in \mathcal{Z}(G) \backslash \{e\}$.

It is G if $g \in G \backslash H$ since an element of order p^2 can get mapped to any element under an endomorphism. First we will show that an element $g = (a, A_{21}, d_{11}, D_{21}) \in G$ of order p^2 is automorphic to the element $(1, \underline{0}^{n-1}, 0, \underline{0}^{n-1})$ where $a \equiv a_{11} \not\equiv 0 \mod p$. Consider the automorphism $\sigma \in \mathrm{Aut}(G)$ such that $\overline{\sigma}$ equals

$$\begin{pmatrix} a_{11} & 0_{1\times(n-1)} & 0 & 0_{1\times(n-1)} \\ A_{21} & a_{11} I_{(n-1)\times(n-1)} & 0_{(n-1)\times 1} & 0_{(n-1)\times(n-1)} \\ d_{11} & D_{12} & 1 & B_{12} \\ D_{21} & 0_{(n-1)\times(n-1)} & 0_{(n-1)\times 1} & I_{(n-1)\times(n-1)} \end{pmatrix} \text{where } D_{12} = D_{21}^t, B_{12} = \frac{-A_{21}^t}{a_{11}}.$$

This automorphism can be used to move $(1, \underline{0}^{n-1}, 0, \underline{0}^{n-1})$ to $(b, A_{21}, d_{11}, D_{21})$ where $b \equiv a \equiv a_{11} \mod p$. We can change $(b, A_{21}, d_{11}, D_{21})$ to $(a, A_{21}, d_{11}, D_{21})$ further by another inner automorphism. Now we will show that

$$\mathrm{End}(G).(1, \underline{0}^{n-1}, 0, \underline{0}^{n-1}) = G.$$

For this the following matrix can be further used.

$$\begin{pmatrix} 0 & 0_{1\times(n-1)} & 0 & 0_{1\times(n-1)} \\ A_{21} & 0_{(n-1)\times(n-1)} & 0_{(n-1)\times 1} & 0_{(n-1)\times(n-1)} \\ d_{11} & 0_{1\times(n-1)} & 0 & 0_{1\times(n-1)} \\ D_{21} & 0_{(n-1)\times(n-1)} & 0_{(n-1)\times 1} & 0_{(n-1)\times(n-1)} \end{pmatrix} \in symp^{scalar}(2n, \mathbb{Z}_p).$$

It is H if $g \in H \backslash \mathcal{Z}(G)$ since a non-central element of order p can get mapped under an endomorphism to any element of order at most p. If $g = (pz, \underline{u}, w_1, \underline{w}) \in H$ then there are two cases. Either $\underline{u}$ or $\underline{w}$ is non-zero or both $\underline{u}$ or $\underline{w}$ are zero and $w_1 \neq 0$.

Suppose $\underline{u}$ or $\underline{w}$ is non-zero. Then we show that g is automorphic to $(0, e_1^{n-1}, 0, \underline{0}^{n-1})$. Let $M = \begin{pmatrix} A_{22} & C_{22} \\ D_{22} & B_{22} \end{pmatrix} \in Sp(2n-2, \mathbb{Z}_p)$ be such that the first column of M is $\begin{pmatrix} \underline{u} \\ \underline{w} \end{pmatrix}$. Consider an automorphism $\sigma \in \mathrm{Aut}(G)$ such that $\overline{\sigma}$ equals

$$\begin{pmatrix} 1 & 0_{1\times(n-1)} & 0 & 0_{1\times(n-1)} \\ A_{21} & A_{22} & 0_{(n-1)\times 1} & C_{22} \\ d_{11} & D_{12} & 1 & B_{12} \\ D_{21} & D_{22} & 0_{(n-1)\times 1} & B_{22} \end{pmatrix}$$

where $D_{12} = D_{21}^t A_{22} - A_{21}^t D_{22},\ B_{12} = D_{21}^t C_{22} - A_{21}^t B_{22}$. Here we choose D_{21} and A_{21} such that $(D_{12})_{11} = (D_{21}^t A_{22} - A_{21}^t D_{22})_{11} = w_1$. Note that such choices of D_{21} and A_{21} exist because the matrix M is invertible and its first column is non-zero. σ moves $(0, e_1^{n-1}, 0, \underline{0}^{n-1})$ to $(pz', \underline{u}, w_1, \underline{w}) \in H$ for some z'. Using another inner automorphism $(pz', \underline{u}, w_1, \underline{w})$ can be mapped to $(pz, \underline{u}, w_1, \underline{w}) = g$. We will show that

$$\mathrm{End}(G).(0, e_1^{n-1}, 0, \underline{0}^{n-1}) = H.$$

Let $M = \begin{pmatrix} A_{22} & 0_{(n-1)\times(n-1)} \\ D_{22} & 0_{(n-1)\times(n-1)} \end{pmatrix} \in symp^{scalar}(2n-2, \mathbb{Z}_p)$ where the first column of A_{22} and D_{22} are given and rest of the columns of A_{22}, D_{22} are zero. The following matrix can be further used to show that $\mathrm{End}(G).(0, e_1^{n-1}, 0, \underline{0}^{n-1}) = H$.

$$\begin{pmatrix} 0 & 0_{1\times(n-1)} & 0 & 0_{1\times(n-1)} \\ 0_{(n-1)\times 1} & A_{22} & 0_{(n-1)\times 1} & 0_{(n-1)\times(n-1)} \\ 0 & D_{12} & 0 & 0_{1\times(n-1)} \\ 0_{(n-1)\times 1} & D_{22} & 0_{(n-1)\times 1} & 0_{(n-1)\times(n-1)} \end{pmatrix} \text{ where } D_{12} = (w, \underline{0}^{n-1}) \text{ for given } w.$$

We consider second case when both $\underline{u} = 0 = \underline{w} = 0$ and $w_1 \neq 0$. In this case we show that

$$\mathrm{End}(G).(pz, \underline{0}^{n-1}, w_1, \underline{0}^{n-1}) = H.$$

For this following matrix can be used.

$$\begin{pmatrix} 0 & 0_{1\times(n-1)} & 0 & 0_{1\times(n-1)} \\ 0_{(n-1)\times 1} & 0_{(n-1)\times(n-1)} & C_{21} & 0_{(n-1)\times(n-1)} \\ 0 & 0_{1\times(n-1)} & b_{11} & 0_{1\times(n-1)} \\ 0_{(n-1)\times 1} & 0_{(n-1)\times(n-1)} & B_{21} & 0_{(n-1)\times(n-1)} \end{pmatrix} \in symp^{scalar}(2n, \mathbb{Z}_p).$$

This proves (D).

We prove (E). Using Equations 1.5, 1.6, the automorphism orbits in G are given as follows. The identity element $\{e\}$ is an orbit. The non-identity central elements $\mathcal{Z}(G)\backslash\{e\}$ is another orbit. For any automorphism σ with $\overline{\sigma} = \begin{pmatrix} A & C \\ D & B \end{pmatrix}$ we have $c_{11} = c_{21} = \ldots = c_{n1} = 0$, $b_{11} = 1, b_{21} = b_{31} = \ldots = b_{n1} = 0$. So the set $\mathcal{O}_b = p\mathbb{Z}_{p^2} \times \{\underline{0}^{n-1}\} \times \{b\} \times \{\underline{0}^{n-1}\}$ for $b \in \mathbb{Z}_p^*$ is an orbit. We observe that elements of order p^2 forms an orbit, that is, $G\backslash H$ is an orbit and for $n > 1$ the set $H\backslash K = H\backslash\mathcal{Z}(H)$ is an orbit. This proves (E).

We prove (F). Any element in $\mathcal{O}_{b_1}$ is endomorphic to any element in $\mathcal{O}_{b_2}$ for $b_1, b_2 \in \mathbb{Z}_p^*$. However for $0 \neq b_1 \neq b_2 \neq 0$ any element of $\mathcal{O}_{b_1}$ is not automorphic to any element of $\mathcal{O}_{b_2}$. This implies that the endomorphism semigroup does not induce a partial order on the automorphism orbits.

This completes the proof of second main Theorem Σ. □

For $\Phi_2, \widetilde{\Phi}_2$ as defined in Section 2.1 we describe the group $\mathrm{Im}(\Phi_2) = \mathrm{Im}(\widetilde{\Phi}_2) \subset Sp^{scalar}(2n, \mathbb{Z}_p)$ and set of endomorphisms in $\mathrm{End}(\frac{G}{\mathcal{Z}(G)}) = M_{2n}(\mathbb{Z}_p)$ which are induced by the elements in the endomorphism semigroup of $G = ES_2(p, n)$.

Proposition 4.1. *Let $G = ES_2(p, n)$. Then*

(1) $Im(\Phi_2) = Im\Big(\operatorname{Aut}(G) \longrightarrow \operatorname{Aut}(\frac{G}{\mathcal{Z}(G)})\Big) = \Big\{\overline{\sigma} = \begin{pmatrix} A & C \\ D & B \end{pmatrix} \in Sp^{scalar}(2n, \mathbb{Z}_p) \mid A = [a_{ij}], B = [b_{ij}], C = [c_{ij}], D = [d_{ij}] \in M_n(\mathbb{Z}_p)$ *with* $a_{11} \neq 0, b_{11} = 1, a_{12} = \ldots = a_{1n} = c_{11} = c_{12} = \ldots = c_{1n} = 0 = c_{21} = c_{31} = \ldots = c_{n1} = b_{21} = b_{31} = \ldots = b_{n1}$ *and* $\overline{\sigma}^t \Delta \overline{\sigma} = a_{11}\Delta\Big\}$.

(2) $Im\Big(\operatorname{End}(G) \longrightarrow \operatorname{End}(\frac{G}{\mathcal{Z}(G)})\Big) = Im(\Phi_2) \bigsqcup \Big\{\overline{\sigma} = \begin{pmatrix} A & C \\ D & B \end{pmatrix} \in symp^{scalar}(2n, \mathbb{Z}_p) \mid A = [a_{ij}], B = [b_{ij}], C = [c_{ij}], D = [d_{ij}] \in M_n(\mathbb{Z}_p)$ *with* $a_{11} = a_{12} = \ldots = a_{1n} = c_{11} = c_{12} = \ldots = c_{1n} = 0$ *and* $\overline{\sigma}^t \Delta \overline{\sigma} = 0_{2n\times 2n}\Big\}$.

(3) $\sigma \in \operatorname{Aut}(G)$ *is an inner-automorphism if and only if* $\overline{\sigma} = Id_{2n\times 2n}$. *In this case for any* $(u_1, \underline{u}, w_1, \underline{w}) \in G$ *with* $\underset{\sim}{\underline{w}} = \begin{pmatrix} w_1 \\ \underline{w} \end{pmatrix}$ *we have*

$$\sigma(u_1, \underline{u}, w_1, \underline{w}) = (au_1 + i_{21}\big(\alpha(\underline{u}) + \beta(\underset{\sim}{\underline{w}})\big), \underline{u}, w_1, \underline{w})$$

for some $\alpha \in (\mathbb{Z}_p^{n-1})^\vee, \beta \in (\mathbb{Z}_p^n)^\vee, a \in \mathbb{Z}_{p^2}^*$ *such that* $a \equiv 1 \mod p$.

(4) *We have an exact sequence*

$$1 \longrightarrow \frac{G}{\mathcal{Z}(G)} \cong Inn(G) \hookrightarrow \operatorname{Aut}(G) \longrightarrow Im(\Phi_2) \longrightarrow 1.$$

(5)

$$\mid Im(\Phi_2) \mid = p^{2n-1}(p-1) \mid Sp(2n-2, \mathbb{Z}_p) \mid .$$

(6)

$$\begin{aligned} \mid \operatorname{Aut}(G) \mid &= p^{2n} \mid Im(\Phi_2) \mid \\ &= p^{n^2+2n}(p-1)\prod_{j=1}^{n-1}(p^{2j}-1). \end{aligned}$$

Proof. This follows from the proof of second main Theorem Σ. □

The cardinality of $\operatorname{End}(G)$ for $G = ES_2(p, n)$ is computed in Section 5, Theorem 5.3.

5. **Order of Endomorphism Semigroups of Extra-Special p-Groups**

In this section we compute the cardinality of $\operatorname{End}(G)$ for $G = ES_i(p, n), i = 1, 2$ for an odd prime p and a positive integer n. First we note that $\operatorname{Im}\Big(\operatorname{End}(G) \longrightarrow \operatorname{End}(\frac{G}{\mathcal{Z}(G)})\Big)$ is a disjoint union of $\operatorname{Im}\Big(\operatorname{Aut}(G) \longrightarrow \operatorname{Aut}(\frac{G}{\mathcal{Z}(G)})\Big)$ and an algebraic set defined over $\mathbb{Z}_p$ given as follows. Let $\langle\langle *, * \rangle\rangle : \mathbb{Z}_p^{2n} \times \mathbb{Z}_p^{2n} \longrightarrow \mathbb{Z}_p$ be the non-degenerate symplectic bilinear form given by

$$\langle\langle v, w\rangle\rangle = \sum_{i=1}^{n}(v_i w_{n+i} - v_{n+i}w_i).$$

Let $e_i = e_i^{2n}, f_i = e_{n+i}^{2n} \in \mathbb{Z}_p^{2n}, 1 \le i \le n$ be the standard basis such that $\langle\langle e_i, f_j\rangle\rangle = \delta_{ij}, \langle\langle e_i, e_j\rangle\rangle = 0 = \langle\langle f_i, f_j\rangle\rangle, 1 \le i, j \le n$. Let $V_1 = \langle e_2, \ldots, e_n, f_1, f_2, \ldots, f_n\rangle$. Let $E_i = \mathrm{Im}\Big(\mathrm{End}(G) \longrightarrow \mathrm{End}(\frac{G}{\mathcal{Z}(G)})\Big)$ where $G = ES_i(p,n), i = 1, 2$. Then the following holds.

- If $G = ES_1(p,n)$ then $E_1 = \mathrm{Im}(\Phi_1)\bigsqcup X$ where the algebraic set $X = \{N \in M_{2n}(\mathbb{Z}_p) \mid N^t\Delta N = 0\}$ and Φ_1 is as defined in Section 2.1. So $|\mathrm{End}(G)| = p^{2n}|E_1|$ using Equations 1.2,1.3 in Theorem Ω.
- If $G = ES_2(p,n)$ then $E_2 = \mathrm{Im}(\Phi_2)\bigsqcup Y$ where the algebraic set $Y = \{N \in M_{2n}(\mathbb{Z}_p) \mid N^t\Delta N = 0,\ \mathrm{Im}(N) \subseteq V_1\}$ and Φ_2 is as defined in Section 2.1. So $|\mathrm{End}(G)| = p^{2n}|E_2|$ using Equations 1.5,1.6 in Theorem Σ.

Definition 5.1 (Isotropic Subspace)**.** *Let $\langle\langle *, *\rangle\rangle : \mathbb{Z}_p^{2n} \times \mathbb{Z}_p^{2n} \longrightarrow \mathbb{Z}_p$ be a non-degenerate symplectic bilinear form. A subspace $W \subset \mathbb{Z}_p^{2n}$ is said to be isotropic if for all $v, w \in W, \langle\langle v, w\rangle\rangle = 0$.*

It is well known that the p-binomial coefficient $\binom{n}{k}_p$ is a polynomial in p with non-negative integer coefficients for any $0 \le k \le n$ and $n \ne 0$. We state a theorem about enumeration.

Theorem 5.2. *Let $\langle\langle *, *\rangle\rangle : \mathbb{Z}_p^{2n} \times \mathbb{Z}_p^{2n} \longrightarrow \mathbb{Z}_p$ be the standard non-degenerate symplectic bilinear form. Let $e_i = e_i^{2n}, f_i = e_{n+i}^{2n} \in \mathbb{Z}_p^{2n}, 1 \le i \le n$ and $V_1 = \langle e_2, e_3, \ldots, e_n,\ f_1, f_2, \ldots, f_n\rangle$. Let $X = \{N \in M_{2n}(\mathbb{Z}_p) \mid N^t\Delta N = 0\}, Y = \{N \in M_{2n}(\mathbb{Z}_p) \mid N^t\Delta N = 0,\ Im(N) \subseteq V_1\}$. For $0 \le k \le n, Isot_k(\mathbb{Z}_p^{2n}) = \{W \subset \mathbb{Z}_p^{2n} \mid W \text{ is a } k\text{-dimensional isotropic subspace}\}$ and $Isot_k(V_1) = \{W \subset V_1 \subset \mathbb{Z}_p^{2n} \mid W \text{ is a } k\text{-dimensional isotropic subspace}\}$. Let $\alpha_k(p,n) = |Isot_k(\mathbb{Z}_p^{2n})|, \beta_k(p,n) = |Isot_k(V_1)|$. Let $\gamma_k(p,n) = |\{f : \mathbb{Z}_p^{2n} \twoheadrightarrow \mathbb{Z}_p^k \mid f \text{ is a surjective linear map}\}|$. Then we have the following.*

(1) $|X| = \sum_{k=0}^{n} \alpha_k(p,n)\gamma_k(p,n)$.

(2) $|Y| = \sum_{k=0}^{n} \beta_k(p,n)\gamma_k(p,n)$.

(3) For each $0 \le k \le n, \alpha_k(p,n), \beta_k(p,n)$ are polynomials in p with non-negative integer coefficients with

  (a) $\alpha_0(p,n) = 1$ *and for* $1 \le k \le n, \alpha_k(p,n) = \binom{n}{k}_p \prod_{i=0}^{k-1}(p^{n-i}+1)$.

  (b) $\beta_0(p,n) = 1, \beta_1(p,n) = \binom{2n-1}{1}_p$ *and for* $2 \le k \le n$

$$\beta_k(p,n) = \left(p^k(p^{n-k}+1)\binom{n-1}{k}_p + \binom{n-1}{k-1}_p\right)\prod_{i=1}^{k-1}(p^{n-i}+1).$$

(4) For each $0 \le k \le n, \gamma_k(p,n)$ is a polynomial in p with integer coefficients with $\gamma_0(p,n) = 1$ and for $1 \le k \le n, \gamma_k(p,n) = p^{2nk} - \sum_{i=0}^{k-1}\binom{k}{i}_p \gamma_i(p,n)$.

Proof. If $N \in M_{2n}(\mathbb{Z}_p)$ and $N^t\Delta N = 0$, that is, $\mathrm{Im}(N)$ is an isotropic subspace of $\mathbb{Z}_p^{2n}$ then $\dim(\mathrm{Im}(N)) \le n$. So (1) and (2) immediately follow.

We prove $3(a)$. It is clear that $\alpha_0(p,n) = 1$. For $1 \le k \le n$, let $T_k = \{(v_1, v_2, \ldots, v_k) \in (\mathbb{Z}_p^{2n})^k \mid (v_1, v_2, \ldots, v_k)$ is an ordered k-tuple of linearly independent vectors whose span is isotropic$\}$. Then we have

$$|T_k| = (p^{2n}-1)(p^{2n-1}-p)\dots(p^{2n-(k-1)}-p^{k-1}).$$

Hence we have

$$\alpha_k(p,n) = \frac{(p^{2n}-1)(p^{2n-1}-p)\dots(p^{2n-(k-1)}-p^{k-1})}{(p^k-1)(p^k-p)\dots(p^k-p^{k-1})} = \binom{n}{k}_p \prod_{i=0}^{k-1}(p^{n-i}+1).$$

We prove $3(b)$. It is clear that $\beta_0(p,n) = 1, \beta_1(p,n) = \binom{2n-1}{1}_p$. For $2 \le k \le n$, let $S_k = \{(v_1, v_2, \dots, v_k) \in (\mathbb{Z}_p^{2n})^k \mid (v_1, v_2, \dots, v_k)$ is an ordered k-tuple of linearly independent vectors whose span is isotropic and is contained in $V_1\}$.

Let $L \subset (\mathbb{Z}_p^{2n}, \langle\langle *, * \rangle\rangle)$ be a subspace. We make the following observations.

- $\dim L + \dim L^\perp = 2n, (L^\perp)^\perp = L, V_1^\perp = \langle f_1 \rangle$.
- $f_1 \in L \iff V_1^\perp \subseteq L \iff L^\perp \subseteq V_1 \iff L^\perp \cap V_1 = L^\perp$.
- $f_1 \notin L \iff V_1^\perp \nsubseteq L \iff L^\perp \nsubseteq V_1 \iff L^\perp \cap V_1 \subsetneq L^\perp$ and of co-dimension one.

Let $k = 2$. We have $p^{2n-1}-1$ choices for $v_1 \in V_1$ out of which $(p-1)$ choices of v_1 are non-zero multiples of f_1 and $p^{2n-1}-p$ choices of v_1 are not multiples of f_1. In the first case $v_2 \in \langle v_1 \rangle^\perp \cap V_1$ has $p^{2n-1}-p$ choices. In the latter case there are $p^{2n-2}-p$ choices for $v_2 \in \langle v_1 \rangle^\perp \cap V_1$. So

$$|S_2| = (p-1)(p^{2n-1}-p) + (p^{2n-1}-p)(p^{2n-2}-p) = (p^{2n-1}-p)(p^{2n-2}-1).$$

So

$$\begin{aligned}\beta_2(p,n) &= \frac{(p^{2n-2}-1)(p^{2n-2}-1)}{(p^2-1)(p^2-p)} \\ &= (p^{n-1}+1)\left(p^2(p^{n-2}+1)\binom{n-1}{2}_p + \binom{n-1}{1}_p\right).\end{aligned}$$

Extending the same argument for $3 \le k \le n$ we get

$$|S_k| = (p^{2n-1}-p)(p^{2n-2}-p^2)\dots(p^{2n-(k-1)}-p^{k-1})(p^{2n-k}-1).$$

We also have

$$\begin{aligned}\beta_k(p,n) &= \frac{(p^{2n-1}-p)(p^{2n-2}-p^2)\dots(p^{2n-(k-1)}-p^{k-1})(p^{2n-k}-1)}{(p^k-1)(p^k-p)\dots(p^k-p^{k-1})} \\ &= \left(p^k(p^{n-k}+1)\binom{n-1}{k}_p + \binom{n-1}{k-1}_p\right)\prod_{i=1}^{k-1}(p^{n-i}+1).\end{aligned}$$

We prove (4). It is clear that $\gamma_0(p,n) = 1$. To compute the number of surjective maps we consider all maps from $\mathbb{Z}_p^{2n} \longrightarrow \mathbb{Z}_p^k$ and subtract the number of maps of rank less than k. Hence we get for $1 \le k \le n$,

$$\gamma_k(p,n) = p^{2nk} - \sum_{i=0}^{k-1}\binom{k}{i}_p \gamma_i(p,n).$$

This completes the proof of the theorem. □

http://dx.doi.org/10.22108/IJGT.2021.129815.1708

Theorem 5.3. *(1) For $G = ES_1(p,n)$ we have*

$$|\operatorname{End}(G)| = p^{n^2+2n}(p-1)\prod_{j=1}^{n}(p^{2j}-1) + p^{2n}\sum_{k=0}^{n}\alpha_k(p,n)\gamma_k(p,n).$$

(2) For $G = ES_2(p,n)$ we have

$$|\operatorname{End}(G)| = p^{n^2+2n}(p-1)\prod_{j=1}^{n-1}(p^{2j}-1) + p^{2n}\sum_{k=0}^{n}\beta_k(p,n)\gamma_k(p,n).$$

Proof. First we observe that for $G = ES_1(p,n)$, $|\operatorname{End}(G)| = |\operatorname{Aut}(G)| + p^{2n}|X|$ and for $G = ES_2(p,n)$, $|\operatorname{End}(G)| = |\operatorname{Aut}(G)| + p^{2n}|Y|$ where X, Y are as defined in Theorem 5.2. Now using Theorem 5.2, Corollary 3.1(3), we conclude (1) and then again using Theorem 5.2 and Proposition 4.1(6), we conclude (2). This completes the proof of the theorem. □

Example 5.4. *For $n = 1$ and $G = ES_1(p,1)$ we obtain $|\operatorname{Aut}(G)| = p^3(p-1)(p^2-1)$ and $|\operatorname{End}(G)| = p^3(p-1)(p^2-1) + p^2(1 + \binom{1}{1}_p(p+1)(p^2-1)) = p^6$.*
For $n = 1$ and $G = ES_2(p,1)$ we obtain $|\operatorname{Aut}(G)| = p^3(p-1)$ and $|\operatorname{End}(G)| = p^3(p-1) + p^2(1 + \binom{1}{1}_p(p^2-1)) = 2p^4 - p^3$.

6. An Open Question

This article leads to an open question which we pose in this section. In general for a finite group, its center and commutator subgroup are characteristic subgroups. However it is not true that an endomorphism maps the center into itself, but an endomorphism maps commutator subgroup into itself. Any automorphism or any endomorphism gives rise to a pair of automorphisms and endomorphisms of the commutator subgroup and the abelianization of whole group respectively. The automorphism group and the endomorphism algebra for finite abelian groups are known. We pose the following open question.

Question 6.1. *Let p be a prime. Let G be a p-group such that $G' = [G,G]$ is a non-trivial abelian group, that is, G is a non-abelian metabelian p-group. Then:*

- *Determine the automorphism orbits in G.*
- *Determine the endomorphism semigroup image of any element in G.*
- *Determine for which type of such groups G the endomorphism semigroup induces a partial order on the automorphism orbits.*

In addition for the group G in Question 6.1, if the center coincides with the commutator subgroup then any endomorphism maps the center into itself. Moreover for such a group, if $\mathcal{Z}(G)$ is elementary abelian, then we have a non-degenerate skew symmetric bilinear map $\frac{G}{\mathcal{Z}(G)} \times \frac{G}{\mathcal{Z}(G)} \longrightarrow \mathcal{Z}(G)$. An example of such a group is given below.

Example 6.2. *Let p be a prime, r be a positive integer and $q = p^r$. Let $\mathbb{F}_q$ be the finite field with q elements. An example of a non-abelian metabelian p-group G which satisfies $[G,G] = G' = \mathcal{Z}(G)$ and*

$\mathcal{Z}(G)$ is elementary abelian is the Heisenberg group $H^n(\mathbb{F}_q) = \mathbb{F}_q^n \oplus \mathbb{F}_q^n \oplus \mathbb{F}_q$ over $\mathbb{F}_q$ of order q^{2n+1}. The group structure is defined in a similar manner as in $ES_1(p,n)$. The answer to Question 6.1 can be explored in the case of $H^n(\mathbb{F}_q)$.

Acknowledgments

The work is done while both the authors are post doctoral fellows at Harish-Chandra Research Institute, Prayagraj-INDIA. Both the authors thank Prof. Amritanshu Prasad and Prof. Sunil Kumar Prajapati for mentioning the problem of finding automorphism orbits in extra-special p-groups. The authors also thank Prof. Manoj Kumar Yadav for suggesting a lot of improvements in the article.

References

[1] D. J. Benson and J. F. Carlson, The cohomology of extraspecial groups, *Bull. London Math. Soc.*, **24** (1992) 209–235.

[2] D. J. Benson and J. F. Carlson, Corrigendum: the Cohomology of Extraspecial groups, *Bull. London Math. Soc.*, **25** (1993) 498–498.

[3] E. A. Bertram, Some applications of graph theory to finite groups, *Discrete Math.*, **44** (1983) 31–43.

[4] A. Y. M. Chin, On non-commuting sets in an extraspecial p-group, *J. Group Theory*, **8** (2005) 189–194.

[5] L. Dornhoff, *Group representation theory*, Part A: Ordinary representation theory, Pure and Applied Mathematics, **7**, Marcel Dekker, Inc., New York, 1971 pp. 1–254.

[6] K. Dutta and A. Prasad, Degenerations and orbits in finite abelian groups, *J. Combin. Theory Ser. A*, **118** (2011) 1685–1694.

[7] D. E. Gorenstein, Finite Groups, *AMS Chelsea Publishing*, **301** (1968) pp. 519.

[8] R. L. Griess Jr., Automorphisms of Extraspecial Groups and Nonvanishing of Degree 2 Cohomology, *Pacific J. Math.*, **48** (1973) 403–422.

[9] H. Liu and Y. Wang, The automorphism group of a generalized extraspecial p-group, *Sci. China Math.*, **53** (2010) 315–334.

[10] H. Liu and Y. Wang, On non-commuting sets in a generalized extraspecial p-group, *Acta Math. Sinica*, **55** (2012) 975–980.

[11] H. Liu and Y. Wang, On Non-commuting Sets in Certain Finite p-Groups, *Algebra Colloq.*, **22** (2015) 555–560.

[12] H. Opolka, Projective Representations of Extra-Special p-Groups, *Glasgow Math. J.*, **19** (1978) 149–152.

[13] D. J. S. Robinson, *A course in the theory of groups*, Graduate Texts in Mathematics, **80**, Springer-Verlag, New York-Berlin, 1982.

[14] D. L. Winter, The automorphism group of an extraspecial p-group, *Rocky Mountain J. Math.*, **2** 159–168.

Chudamani Pranesachar Anil Kumar

School of Mathematics, Harish-Chandra Research Institute, Chhatnag Road, Jhunsi 211019, Prayagraj, INDIA

Email: akcp1728@gmail.com

Soham Swadhin Pradhan

School of Mathematics, Harish-Chandra Research Institute, Chhatnag Road, Jhunsi 211019, Prayagraj, INDIA

Email: soham.spradhan@gmail.com