

On a Question of Stanojkovski: Abelian Subgroups of Breadth Two Distinguish Vaughan-Lee's Groups 8.5.14 and 8.5.15

Alper Ferudun*

October 14, 2026

Abstract

At the problem session of the Oberwolfach workshop *Computational Group Theory* (June 2025), M. Stanojkovski asked whether an invariant simpler than the order of the automorphism group can show that two groups G_1 and G_2 of order p^8 , class 2 and exponent p (p an odd prime) are not isomorphic. They are the groups 8.5.14 and 8.5.15 of Vaughan-Lee's list, whose presentations and automorphism group orders are due to Vaughan-Lee, and they are the one pair of 5-generator groups of order p^8 that the geometric invariants of O'Brien and Stanojkovski did not separate in their computations. For a group G of class 2 let $\mathcal{A}(G)$ be the set of abelian subgroups $A \geq G'$ with $|A : G'| = p^2$ all of whose elements outside G' have centraliser of index p^2 . We prove that $|\mathcal{A}(G_1)| = 1$ and $|\mathcal{A}(G_2)| = 3$ for every odd prime p and every quadratic non-residue ω in the presentation of G_1 ; hence $G_1 \not\cong G_2$. The proof is uniform in p : the elements of breadth two form, in the projective space of G/G' , a plane and a cubic scroll; the members of $\mathcal{A}(G)$ are the lines of this locus on which the commutator map vanishes; and the hypothesis on ω enters only through $t^2 \neq \omega$. We also determine the commuting graph on the elements of breadth two, whose numbers of edges differ by p , and we show that G_1 depends only on the square class of ω and is isomorphic to G_2 when ω is a square. The pair had already been separated without automorphism groups in the classification literature: Copetti's thesis of 2004, following Brahana's paper of 1951, attaches to the space of commutator forms a pencil of conics, which contains double lines only for 8.5.15. We show that $|\mathcal{A}(G)| - 1$ is the number of these double lines, so that $|\mathcal{A}(G)|$ is a group-theoretic form of their invariant. Breadth and centralisers are classical notions; whether either invariant is simpler in the intended sense is for the proposers to judge. This is an unrefereed note.

1 Introduction

1.1 The question

Let p be an odd prime and ω an integer prime to p . In the variety of groups of exponent p and nilpotency class at most 2 consider the groups

$$\begin{aligned} G_1 &= \langle a, b, c, d, e \mid [c, b], [d, b], [e, c], [e, d], [d, c] = [b, a], [e, b] = [c, a], [e, a] = [d, a]^\omega \rangle, \\ G_2 &= \langle a, b, c, d, e \mid [d, a], [e, a], [c, b], [d, b], [e, c], [d, c] = [b, a], [e, b] = [c, a] \rangle, \end{aligned}$$

where a commutator without right-hand side is set equal to 1. When ω is a primitive root modulo p , these are the groups 8.5.14 and 8.5.15 of Vaughan-Lee's list of the groups of class 2, exponent p and order at most p^8 , with his presentations [VL15, §8.5]. Both have order p^8 (Lemma 2.1). Vaughan-Lee found $|\text{Aut } G_1| = 2(p-1)(p^2-1)p^{17}$ and $|\text{Aut } G_2| = 2(p-1)^3p^{17}$, and the same number

*Mercury Software GmbH. Email: alper@mercurycodelab.com. GitHub: <https://github.com/AlperTheKing>.
Unrefereed preprint. CC BY 4.0.

$p^5 + 2p^4 - p^3 - p^2$ of conjugacy classes for both [VL15, p. 29]. In the problem session of the Oberwolfach workshop *Computational Group Theory* (2025), M. Stanojkovski stated these two presentations, with ω a primitive element of $\mathbb{F}_p$ and the labels of [VL15], and asked [DENRD25, p. 1443]:

Is there a “simpler invariant” for non-isomorphism testing of these groups?

The background is the work of O’Brien and Stanojkovski [OS26], reported in her lecture at the workshop [DENRD25, pp. 1399–1400]. After a choice of bases of G/G' and G' , the commutator map of a group of class 2 and exponent p is given by a skew-symmetric matrix of linear forms, the commutator matrix, which has an “adjoint”; the degrees, dimensions, primary decompositions, numbers of rational points and of components, and spans of the varieties defined by the determinantal ideals of these two matrices are isomorphism invariants [OS26, Theorem 2.3]. O’Brien and Stanojkovski computed these invariants, for $3 \leq p \leq 37$, for the 22 five-generator groups of order p^8 with derived subgroup of order p^3 . They distinguish all of them except the cases (14) and (15), which are G_1 and G_2 ; that these two are not isomorphic is known from Vaughan-Lee’s orders of the automorphism groups [OS26, §4.1 and Table 2]. The question asks for a simpler certificate of this non-isomorphism. The classification of the 22 groups goes back to Brahana [Bra51, Bra58]. In Copetti’s thesis the two groups are the orbits 14 and 15 of 3-dimensional spaces of alternating forms [Cop04, Theorem 7.22] [OS26, §4.1], and Copetti proves that these orbits are different by a pencil of conics, without automorphism groups [Cop04, Lemma 7.21]; according to [Cop04, p. 82] the argument is modelled on [Bra51, pp. 548–549]. So the two groups had been told apart by an invariant other than the order of the automorphism group before the question was asked; Remark 7.3 shows that this classical invariant and ours count the same objects. The question is record OWR-14299292-013 of the UnsolvedMath collection [ula26], where it is listed as open; in version 1.6.0 the statement of the record is the source’s question quoted above, and another snapshot of the collection (revision 372682f) restates it with both presentations, asking for “an invariant simpler than automorphism-group order” that proves non-isomorphism.

Conventions. A presentation in the variety defines the largest group of exponent p and class at most 2 that is generated by five elements satisfying the relations. The commutator convention does not matter: in a group of class 2 one has $xyx^{-1}y^{-1} = [x^{-1}, y^{-1}] = x^{-1}y^{-1}xy$, and a convention in which $[x, y]$ and $[y, x]$ are interchanged inverts every commutator, which leaves the relations unchanged because each of them is homogeneous in the commutators. The source and [VL15] take ω primitive; every primitive root is a quadratic non-residue, and our results hold for every non-residue. Vaughan-Lee fixes a primitive ω throughout, for consistency, and remarks for a group of order p^6 that any non-residue gives the same group [VL15, pp. 4–5]; Proposition C below shows that for G_1 the non-residue hypothesis is exactly the right one.

1.2 Results

For a finite p -group G and $x \in G$, the *breadth* $b(x)$ is defined by $|G : C_G(x)| = p^{b(x)}$; it is a classical notion.

Definition 1.1. For a finite p -group G of class at most 2 let $\mathcal{A}(G)$ be the set of abelian subgroups A of G with $G' \leq A$, $|A : G'| = p^2$, and $b(x) = 2$ for every $x \in A \setminus G'$.

Since $\mathcal{A}(G)$ is defined in terms of G alone (an isomorphism maps derived subgroups, abelian subgroups and centralisers onto the corresponding subgroups), its cardinality is an isomorphism invariant. For G_1 and G_2 its members are abelian subgroups of order p^5 .

Theorem A. *Let p be an odd prime and ω a quadratic non-residue modulo p . Then*

$$\mathcal{A}(G_1) = \{\langle b, c \rangle G'_1\}, \quad \mathcal{A}(G_2) = \{\langle b, c \rangle G'_2, \langle b, d \rangle G'_2, \langle c, e \rangle G'_2\}.$$

In particular $|\mathcal{A}(G_1)| = 1 \neq 3 = |\mathcal{A}(G_2)|$, and $G_1 \not\cong G_2$.

The proof (Sections 2 to 4) uses only the alternating bilinear map $B: V \times V \rightarrow W$ given by commutation, where $V = G/G' \cong \mathbb{F}_p^5$ and $W = G' \cong \mathbb{F}_p^3$. The points of $\mathbb{P}(V)$ of breadth 2 form the union of a plane $\mathbb{P}(R)$, the radical of the only form of rank 2 in the net of scalar forms $\eta \circ B$ ($\eta \in W^*$), and the rational points of a cubic scroll Z , the closure of the radicals of the forms of rank 4; the two meet along the line D spanned by the images of b and c . The members of $\mathcal{A}(G)$ correspond to the lines of this locus on which B vanishes. In both groups D is such a line; the others are rulings of the scroll, and in G_1 the rulings on which B vanishes are those with parameter t satisfying $t^2 = \omega$, which are not defined over $\mathbb{F}_p$. The same geometry gives a second invariant.

Theorem B. *Let $\Gamma(G)$ be the graph whose vertices are the subgroups $\langle x \rangle G'$ with $b(x) = 2$, two distinct vertices $\langle x \rangle G'$ and $\langle x' \rangle G'$ being adjacent if $[x, x'] = 1$. For every odd prime p and every non-residue ω , the graph $\Gamma(G_1)$ has p^2 vertices of degree $p+1$, $p+1$ of degree $2p$ and p^2+p of degree $2p+1$, and $\frac{3}{2}p(p+1)^2$ edges; the graph $\Gamma(G_2)$ has p^2 vertices of degree $p+1$, $3p+1$ of degree $2p$ and p^2-p of degree $2p+1$, and $\frac{1}{2}(3p^3+6p^2+p)$ edges. So $\Gamma(G_1)$ has exactly p more edges than $\Gamma(G_2)$.*

For ω prime to p write $G_1(\omega)$ for the group G_1 defined with this ω ; it depends only on ω modulo p .

Proposition C. (a) $G_1(\omega) \cong G_1(\omega s^2)$ for every integer s prime to p . (b) If $\omega \equiv s^2 \pmod{p}$, then $G_1(\omega) \cong G_2$. Hence all $G_1(\omega)$ with ω a non-residue are isomorphic to each other, those with ω a residue are isomorphic to G_2 , and by Theorem A the two types are distinguished by $|\mathcal{A}| \in \{1, 3\}$.

Section 7 shows that the usual cheaper invariants coincide for the two groups, that the configuration of the points of breadth 2 separates them (Remark 7.2), and that $|\mathcal{A}(G)| - 1$ is the number of double lines in the pencil of conics of Brahana and Copetti (Remark 7.3).

1.3 What is new, what is not, and in what sense the invariant is simple

The question is Stanojkovski's [DENRD25], and the pair is the one that the invariants of O'Brien and Stanojkovski [OS26] did not separate. The presentations, the orders of the automorphism groups and the class numbers are Vaughan-Lee's [VL15]. Breadth and centralisers are classical; the passage from a group of class 2 and exponent p to an alternating bilinear map is the classical correspondence of Baer, recalled in [OS26, §2.1]. The groups were classified by Brahana [Bra51, Bra58], who used concepts of projective geometry, by Copetti [Cop04] and by Vaughan-Lee [VL15] [OS26, §§1, 4, 4.1], and the first separation of this pair without automorphism groups is theirs: Copetti's Lemma 7.21 [Cop04], modelled on Brahana [Bra51, pp. 548–549], distinguishes the two orbits by a pencil of conics attached to the only form of rank 2 in the net. By Remark 7.3, $|\mathcal{A}(G)| - 1$ is the number of double lines of that pencil; so $|\mathcal{A}(G)|$ restates their invariant in terms of abelian subgroups and centralisers. Vaughan-Lee's numbers of descendants of order p^9 [VL17, p. 37] separate the pair as well, but they are computed from the automorphism groups. To our knowledge, the invariant $|\mathcal{A}(G)|$ with Theorem A and its uniform proof, Theorem B and Proposition C are not in print in this form; Proposition C, however, is implicit in the completeness of Vaughan-Lee's list (Remark 6.1). We read Chapters 1 and 7 of [Cop04], but not Brahana's papers: [Bra51] is behind a paywall, and the open copy of [Bra58] on the publisher's site refused our automated requests. The paragraph "Scope and priority" at the end gives the details.

"Simpler" is not a formal notion. We think that $|\mathcal{A}(G)|$ qualifies for three reasons. It is defined through orders of subgroups and of centralisers only, whereas the invariant of Brahana and Copetti uses the dual space of commutator forms, its Plücker quadrics and a pencil of conics. It can be computed from the breadths of the $p^4 + p^3 + p^2 + p + 1$ points of $\mathbb{P}(G/G')$ and a count of lines, without automorphism groups or Gröbner bases. And the proof that it separates the pair is a uniform computation, valid for all odd p at once. On the other hand it is not one of the determinantal

invariants of [OS26, Theorem 2.3]; Section 7 shows which features of those invariants coincide for the two groups, that the configuration of the points of breadth 2 does separate them, and that several natural cheaper invariants coincide, among them the class number, the character degrees and the numbers of abelian subgroups containing G' of each order, which form Qiao's polynomial [Qia24]. The proposers may judge the matter otherwise.

2 The groups as alternating maps

Throughout, p is an odd prime, $V = \mathbb{F}_p^5$ with standard basis $e_1, \dots, e_5$, and $W = \mathbb{F}_p^3$ with standard basis w_1, w_2, w_3 . For $\omega \in \mathbb{F}_p^\times$ let $B_1 = B_1^\omega$ and B_2 be the alternating bilinear maps $V \times V \rightarrow W$ whose values $B(e_i, e_j)$, $i > j$, are 0 except for the following ones, where $(i, j) \mapsto w$ stands for $B(e_i, e_j) = w$:

$$B_1 : \quad (2, 1) \mapsto w_1, \quad (3, 1) \mapsto w_2, \quad (4, 1) \mapsto w_3, \quad (5, 1) \mapsto \omega w_3, \quad (5, 2) \mapsto w_2, \quad (4, 3) \mapsto w_1; \quad (1)$$

$$B_2 : \quad (2, 1) \mapsto w_1, \quad (3, 1) \mapsto w_2, \quad (5, 2) \mapsto w_2, \quad (4, 3) \mapsto w_1, \quad (5, 4) \mapsto w_3. \quad (2)$$

In terms of the generators this says $[b, a] = w_1$, $[c, a] = w_2$, and $[d, a] = w_3$ for G_1 , resp. $[e, d] = w_3$ for G_2 ; the other commutators of generators are then given by the relations. For an alternating bilinear map $B: V \times V \rightarrow W$ let $H(B)$ be the set $V \times W$ with the product

$$(v, w)(v', w') = (v + v', w + w' + \tfrac{1}{2}B(v, v')).$$

This is the classical construction of Baer, see [OS26, §2.1]; we include the short proof of what we need.

Lemma 2.1. (a) $H(B)$ is a group of exponent p in which $\{0\} \times W$ is central, and $[(v, w), (v', w')] = (0, B(v, v'))$ for all elements; in particular $H(B)$ has class at most 2.

(b) For $i = 1, 2$ (with ω for G_1) the assignment $a, b, c, d, e \mapsto (e_1, 0), \dots, (e_5, 0)$ extends to an isomorphism $G_i \rightarrow H(B_i)$. Hence $|G_i| = p^8$, the derived subgroup G'_i corresponds to $\{0\} \times W$, and G_i/G'_i is identified with V , the cosets of $a, \dots, e$ with $e_1, \dots, e_5$.

Proof. (a) Both ways of bracketing a product of three elements give $(v + v' + v'', w + w' + w'' + \tfrac{1}{2}(B(v, v') + B(v, v'') + B(v', v'')))$, by bilinearity. The identity is $(0, 0)$, and $(-v, -w)$ is inverse to (v, w) because $B(v, v) = 0$; for the same reason $(v, w)^n = (nv, nw)$ for $n \geq 0$, so the exponent is p . The elements $(0, u)$ are central. For $x = (v, w)$ and $y = (v', w')$ we have $xy = yx(0, B(v, v'))$, hence $x^{-1}y^{-1}xy = (0, B(v, v'))$, which is central.

(b) By (1) and (2) and part (a), the elements $x_k = (e_k, 0)$ of $H(B_i)$ satisfy the defining relations of G_i ; for instance $[x_5, x_1] = (0, \omega w_3) = (0, w_3)^\omega = [x_4, x_1]^\omega$ in $H(B_1)$. Since $H(B_i)$ lies in the variety, there is a homomorphism $\varphi: G_i \rightarrow H(B_i)$ with $a, \dots, e \mapsto x_1, \dots, x_5$. Its image contains the commutators $[x_k, x_l] = (0, B_i(e_k, e_l))$, and these span $\{0\} \times W$ (they include w_1, w_2 and $w_3 = B_1(e_4, e_1)$, resp. $w_3 = B_2(e_5, e_4)$); as $(v, 0) \in x_1^{v_1} \cdots x_5^{v_5}(\{0\} \times W)$, φ is onto and $|G_i| \geq p^8$. Conversely, G_i/G'_i is an elementary abelian group generated by five elements. In a group of class 2 the commutator is bimultiplicative, so G'_i is generated by the ten commutators $[g, h]$ of pairs of generators, which are central of order dividing p ; the relations express seven of them through $[b, a], [c, a], [d, a]$ for G_1 (namely $[e, a] = [d, a]^\omega$, $[e, b] = [c, a]$, $[d, c] = [b, a]$, and the other four are trivial), resp. through $[b, a], [c, a], [e, d]$ for G_2 . So $|G'_i| \leq p^3$ and $|G_i| \leq p^8$. Hence φ is an isomorphism, and it maps G'_i onto the subgroup generated by the commutators, which is $\{0\} \times W$. $\square$

From now on we identify $G = G_i$ with $H(B)$, $B = B_i$. For $v \in V$ let $\text{ad}_v = B(v, \cdot): V \rightarrow W$. If $x = (v, w)$, then by Lemma 2.1(a)

$$C_G(x) = \ker(\text{ad}_v) \times W, \quad \text{so} \quad b(x) = \text{rank ad}_v.$$

The breadth depends only on v , and for $v \neq 0$ only on the point $\langle v \rangle$ of the projective space $\mathbb{P}(V) \cong \mathbb{P}^4(\mathbb{F}_p)$; we speak of the breadth $b(v)$ of a vector or a point. The subgroups A with $G' \leq A \leq G$ are the sets $A = U \times W$ with $U \leq V$ a subspace, and A is abelian if and only if $B(U, U) = 0$. If $U = \langle u, u' \rangle$ is 2-dimensional, this means $B(u, u') = 0$, because B is alternating. We identify 2-dimensional subspaces of V with lines of $\mathbb{P}(V)$ and call a line $\ell = \mathbb{P}(U)$ *isotropic* if $B(U, U) = 0$, and *good* if it is isotropic and all its $p + 1$ points have breadth 2.

Lemma 2.2. *The map $A \mapsto \mathbb{P}(A/G')$ is a bijection from $\mathcal{A}(G)$ onto the set of good lines of $\mathbb{P}(V)$.*

Proof. This is the dictionary just described: $|A : G'| = p^2$ means $\dim U = 2$, A is abelian if and only if $\mathbb{P}(U)$ is isotropic, and the elements of $A \setminus G'$ are the (v, w) with $0 \neq v \in U$. $\square$

3 The locus of breadth two

3.1 The net of forms

Write $B = \sum_k B^{(k)} w_k$ with scalar alternating forms $B^{(k)}$ on V , and for $y = (y_1, y_2, y_3) \in \mathbb{F}_p^3$ let $f_y = y_1 B^{(1)} + y_2 B^{(2)} + y_3 B^{(3)}$ (the composition of B with the linear form $\sum y_k w_k^*$ on W). Its Gram matrix $M(y) = (f_y(e_i, e_j))$ is, by (1) and (2),

$$M_1(y) = \begin{pmatrix} 0 & -y_1 & -y_2 & -y_3 & -\omega y_3 \\ y_1 & 0 & 0 & 0 & -y_2 \\ y_2 & 0 & 0 & -y_1 & 0 \\ y_3 & 0 & y_1 & 0 & 0 \\ \omega y_3 & y_2 & 0 & 0 & 0 \end{pmatrix}, \quad M_2(y) = \begin{pmatrix} 0 & -y_1 & -y_2 & 0 & 0 \\ y_1 & 0 & 0 & 0 & -y_2 \\ y_2 & 0 & 0 & -y_1 & 0 \\ 0 & 0 & y_1 & 0 & -y_3 \\ 0 & y_2 & 0 & y_3 & 0 \end{pmatrix}.$$

Up to sign and the choice of bases this is the commutator matrix of [OS26, §2.1]. For $y \neq 0$ let $\text{rad } f_y = \{v \in V : f_y(v, \cdot) = 0\}$, the kernel of $M(y)$.

Lemma 3.1. *For $0 \neq v \in V$ we have $b(v) = 3 - \dim\{y \in \mathbb{F}_p^3 : v \in \text{rad } f_y\}$.*

Proof. $v \in \text{rad } f_y$ means that the linear form $\sum y_k w_k^*$ vanishes on the image of ad_v . So the space in question is the annihilator of im ad_v in W^* , of dimension $3 - \text{rank ad}_v$. $\square$

For a 4×4 alternating matrix $A = (a_{ij})$ let $\text{Pf}(A) = a_{12}a_{34} - a_{13}a_{24} + a_{14}a_{23}$, so that $\det A = \text{Pf}(A)^2$. Let $\text{Pf}_k(y)$ be the Pfaffian of $M(y)$ with the k -th row and column deleted, and $\mathbf{v}(y) = (\text{Pf}_1, -\text{Pf}_2, \text{Pf}_3, -\text{Pf}_4, \text{Pf}_5)$. A direct computation gives

$$\begin{aligned} G_1 : \quad & (\text{Pf}_1, \dots, \text{Pf}_5) = (y_1 y_2, \omega y_1 y_3, -y_2 y_3, -y_2^2, y_1^2), \\ & \mathbf{v}(y) = (y_1 y_2, -\omega y_1 y_3, -y_2 y_3, y_2^2, y_1^2); \end{aligned} \tag{3}$$

$$\begin{aligned} G_2 : \quad & (\text{Pf}_1, \dots, \text{Pf}_5) = (y_1 y_2, y_2 y_3, y_1 y_3, -y_2^2, y_1^2), \\ & \mathbf{v}(y) = (y_1 y_2, -y_2 y_3, y_1 y_3, y_2^2, y_1^2), \end{aligned} \tag{4}$$

and $M(y)\mathbf{v}(y) = 0$ identically in both cases: each entry of $M(y)\mathbf{v}(y)$ is a sum of at most four cubic monomials which cancel in pairs (for instance the first entry for G_1 is $\omega y_1^2 y_3 + y_2^2 y_3 - y_2^2 y_3 - \omega y_1^2 y_3$). Let $c = (0 : 0 : 1) \in \mathbb{P}^2(\mathbb{F}_p)$.

Lemma 3.2. *Let $0 \neq y \in \mathbb{F}_p^3$.*

(a) *If $(y_1, y_2) \neq (0, 0)$, then f_y has rank 4 and $\text{rad } f_y = \langle \mathbf{v}(y) \rangle$.*

(b) If $y_1 = y_2 = 0$, then f_y is a multiple of $f_c = B^{(3)}$, which has rank 2; its radical $R = \text{rad } f_c$ is

$$\begin{aligned} G_1 : \quad f_c(x, x') &= (x_4 + \omega x_5)x'_1 - x_1(x'_4 + \omega x'_5), & R &= \langle e_2, e_3, e_5 - \omega e_4 \rangle, \\ G_2 : \quad f_c(x, x') &= x_5x'_4 - x_4x'_5, & R &= \langle e_1, e_2, e_3 \rangle; \end{aligned}$$

that is, $R = \{x_1 = 0, x_4 + \omega x_5 = 0\}$ for G_1 and $R = \{x_4 = x_5 = 0\}$ for G_2 .

(c) For both groups the five Pfaffians generate the ideal $(y_1^2, y_2^2, y_1y_2, y_1y_3, y_2y_3)$ of $\mathbb{F}_p[y_1, y_2, y_3]$.

Proof. (a) One of $\text{Pf}_5 = y_1^2$ and $\text{Pf}_4 = -y_2^2$ is non-zero, so $M(y)$ has an invertible principal 4×4 submatrix and rank at least 4; an alternating matrix of odd size has even rank, so the rank is 4. As $\mathbf{v}(y) \neq 0$ (it has the coordinates y_2^2 and y_1^2) and $M(y)\mathbf{v}(y) = 0$, the kernel is $\langle \mathbf{v}(y) \rangle$. (b) and (c) are read off from (1), (2), (3) and (4) (ω is a unit). $\square$

So the net $\{f_y\}$ contains exactly one form of rank 2 up to scalars, and all its other non-zero forms have rank 4.

3.2 The points of breadth two

Let $Q = \{\langle \mathbf{v}(y) \rangle : y \in \mathbb{P}^2(\mathbb{F}_p) \setminus \{c\}\}$ and let $S \subset \mathbb{P}(V)$ be the set of points of breadth 2.

Lemma 3.3. (a) *The map $y \mapsto \langle \mathbf{v}(y) \rangle$ is injective on $\mathbb{P}^2(\mathbb{F}_p) \setminus \{c\}$, and $Q \cap \mathbb{P}(R) = \emptyset$.*

(b) *Every non-zero $v \in V$ has breadth 2 or 3; $S = \mathbb{P}(R) \sqcup Q$ and $|S| = 2p^2 + 2p + 1$. In particular $Z(G) = G'$.*

Proof. (a) If $y_1 \neq 0$ we may take $y_1 = 1$; then $\mathbf{v}(1, y_2, y_3) = (y_2, -\omega y_3, -y_2y_3, y_2^2, 1)$ for G_1 and $(y_2, -y_2y_3, y_3, y_2^2, 1)$ for G_2 , a vector with last coordinate 1 from which (y_2, y_3) is read off. If $y_1 = 0$, then $y_2 \neq 0$, and $\mathbf{v}(0, 1, y_3)$ is $(0, 0, -y_3, 1, 0)$, resp. $(0, -y_3, 0, 1, 0)$, with last coordinate 0, which determines y_3 . This proves injectivity. If $\mathbf{v}(y) \in R$, then for G_1 we get $y_1y_2 = 0$ and $y_2^2 + \omega y_1^2 = 0$, whence $y_1 = y_2 = 0$ (only $\omega \neq 0$ is used), and for G_2 we get $y_2^2 = y_1^2 = 0$; so $y = c$.

(b) By Lemma 3.2 the radicals of the non-zero forms of the net are R (for $y \in \langle c \rangle$) and the lines $\langle \mathbf{v}(y) \rangle$ (for $y \notin \langle c \rangle$). If $v \neq 0$ lay in $\text{rad } f_y \cap \text{rad } f_{y'}$ for linearly independent y, y' , these radicals would be two different members of this family by (a), and two different members meet only in 0, again by (a). So the space in Lemma 3.1 has dimension at most 1, $b(v) \geq 2$, and $b(v) = 2$ exactly when $v \in R$ or $\langle v \rangle = \langle \mathbf{v}(y) \rangle$ for some $y \neq c$. Hence $S = \mathbb{P}(R) \sqcup Q$, of size $(p^2 + p + 1) + (p^2 + p)$. Finally $Z(G) = \{(v, w) : b(v) = 0\} = \{0\} \times W = G'$. $\square$

3.3 The scroll

Let $X = (X_1, \dots, X_5)$ be coordinates on V , let

$$N_1(X) = \begin{pmatrix} X_5 & X_1 & X_2 \\ X_1 & X_4 & \omega X_3 \end{pmatrix}, \quad N_2(X) = \begin{pmatrix} X_5 & X_1 & X_3 \\ X_1 & X_4 & -X_2 \end{pmatrix},$$

and let $Z \subset \mathbb{P}(V) = \mathbb{P}^4(\mathbb{F}_p)$ be the set of (rational) points at which $\text{rank } N(X) \leq 1$, that is, the common zeros of the three 2×2 minors

$$\begin{aligned} G_1 : \quad q_1 &= X_4X_5 - X_1^2, & q_2 &= \omega X_3X_5 - X_1X_2, & q_3 &= \omega X_1X_3 - X_2X_4; \\ G_2 : \quad q_1 &= X_4X_5 - X_1^2, & q_2 &= -(X_1X_3 + X_2X_5), & q_3 &= -(X_1X_2 + X_3X_4). \end{aligned}$$

Over an algebraically closed field these equations define a rational normal cubic scroll; we shall not use this. Let $D = \mathbb{P}\langle e_2, e_3 \rangle$, let $\ell_\infty = \mathbb{P}\langle e_3, e_4 \rangle$ for G_1 and $\ell_\infty = \mathbb{P}\langle e_2, e_4 \rangle$ for G_2 , and for $t \in \mathbb{F}_p$ let

$$P_t = te_1 + t^2e_4 + e_5, \quad Q_t = \begin{cases} -\omega e_2 - te_3 & (G_1), \\ -te_2 + e_3 & (G_2), \end{cases} \quad \ell_t = \mathbb{P}\langle P_t, Q_t \rangle.$$

The lines ℓ_t and ℓ_∞ are the *rulings*; D is the *directrix*.

Lemma 3.4. *The set Z and the lines just defined have the following properties.*

- (a) $N_1(\mathbf{v}(y))$ is the product of the column $(y_1, y_2)^\top$ and the row $(y_1, y_2, -\omega y_3)$, and $N_2(\mathbf{v}(y))$ that of $(y_1, y_2)^\top$ and (y_1, y_2, y_3) ; so $Q \subset Z$. Moreover $\mathbf{v}(1, t, s) = P_t + sQ_t$, and $\mathbf{v}(0, 1, s) = e_4 - se_3$ (G_1), resp. $e_4 - se_2$ (G_2).
- (b) The points of Z with $X_5 \neq 0$ are the points $\langle \mathbf{v}(1, t, s) \rangle$, $t, s \in \mathbb{F}_p$.
- (c) $Z \cap \{X_5 = 0\} = D \cup \ell_\infty$.
- (d) $Z = Q \sqcup D$, $\mathbb{P}(R) \cap Z = D$, and $S = \mathbb{P}(R) \cup Z$.
- (e) The lines of $\mathbb{P}(V)$ all of whose points lie in Z are exactly D , ℓ_∞ and the ℓ_t , $t \in \mathbb{F}_p$.

Proof. (a) is a direct substitution of (3), (4); for instance, for G_1 the first row of $N_1(\mathbf{v}(y))$ is $(y_1^2, y_1y_2, -\omega y_1y_3) = y_1(y_1, y_2, -\omega y_3)$.

(b) Let $X_5 = 1$. Then $\text{rank } N(X) \leq 1$ says that the second row is X_1 times the first: $X_4 = X_1^2$ and $\omega X_3 = X_1X_2$ (G_1), resp. $-X_2 = X_1X_3$ (G_2). So $X = (X_1, X_2, X_1X_2/\omega, X_1^2, 1) = \mathbf{v}(1, X_1, -X_2/\omega)$ for G_1 and $X = (X_1, -X_1X_3, X_3, X_1^2, 1) = \mathbf{v}(1, X_1, X_3)$ for G_2 . The converse is (a).

(c) If $X_5 = 0$, then $q_1 = 0$ gives $X_1 = 0$, and the minors reduce to $-X_2X_4$ (G_1), resp. $-X_3X_4$ (G_2). So $X_4 = 0$, which means $X \in D$, or $X_2 = 0$, resp. $X_3 = 0$, which means $X \in \ell_\infty$; and conversely.

(d) By (a)–(c), the points of Z are the $\langle \mathbf{v}(1, t, s) \rangle$ and the points of $D \cup \ell_\infty$; the points of ℓ_∞ other than $\langle e_3 \rangle$, resp. $\langle e_2 \rangle$, are the $\langle \mathbf{v}(0, 1, s) \rangle$, and $\langle e_3 \rangle$, $\langle e_2 \rangle$ lie on D . So $Z = Q \cup D$. Since $e_2, e_3 \in R$ we have $D \subset \mathbb{P}(R)$, and $Q \cap \mathbb{P}(R) = \emptyset$ by Lemma 3.3. The rest follows from $S = \mathbb{P}(R) \sqcup Q$.

(e) The lines D and ℓ_∞ lie in Z by (c), and the points of ℓ_t are $\langle Q_t \rangle \in D$ and $\langle P_t + sQ_t \rangle = \langle \mathbf{v}(1, t, s) \rangle \in Q$. Conversely let $\ell \subset Z$ be a line. If $\ell \subset \{X_5 = 0\}$, then $\ell \subset D \cup \ell_\infty$ by (c); if $\ell \neq D$, at most one of its $p+1 \geq 4$ points lies on D , the others lie on ℓ_∞ , and $\ell = \ell_\infty$. Otherwise ℓ meets $\{X_5 = 0\}$ in exactly one point $\langle Q' \rangle$, and choosing $P' \in \ell$ with $X_5(P') = 1$, the other points of ℓ are $\langle P' + sQ' \rangle$, $s \in \mathbb{F}_p$, all with $X_5 = 1$. By (b), $X_4 = X_1^2$ at these points. Write $X_1(P' + sQ') = \alpha + s\beta$ and $X_4(P' + sQ') = \gamma + s\delta$. The polynomial $(\alpha + s\beta)^2 - \gamma - s\delta$ has degree at most 2 and $p \geq 3$ zeros in $\mathbb{F}_p$, so it is zero: $\beta = 0$, $\delta = 0$ and $\gamma = \alpha^2$. Put $t = \alpha$; then Q' has $X_1 = X_4 = X_5 = 0$. For G_1 , by (b) the affine-linear identity $\omega X_3 = tX_2$ in s holds at the points $P' + sQ'$, hence $\omega X_3(Q') = tX_2(Q')$ and $\omega X_3(P') = tX_2(P')$. As $Q' \neq 0$, we get $X_2(Q') \neq 0$, so Q' is a multiple of $(0, \omega, t, 0, 0) = -Q_t$, and $P' = P_t - (X_2(P')/\omega)Q_t$. For G_2 the identity $-X_2 = tX_3$ gives in the same way $Q' \in \langle Q_t \rangle$ and $P' = P_t + X_3(P')Q_t$. In both cases $\ell = \ell_t$. $\square$

4 Proof of Theorem A

By Lemma 2.2 we have to determine the good lines, that is, the isotropic lines ℓ all of whose points lie in $S = \mathbb{P}(R) \cup Z$ (Lemma 3.4(d)).

Case 1: $\ell \subset \mathbb{P}(R)$. Choose the following bases u_1, u_2, u_3 of R ; by (1) and (2),

$$\begin{aligned} G_1: \quad u_1 = e_2, \quad u_2 = e_3, \quad u_3 = e_5 - \omega e_4: \quad & B(u_1, u_2) = 0, \quad B(u_1, u_3) = -w_2, \quad B(u_2, u_3) = \omega w_1; \\ G_2: \quad u_1 = e_1, \quad u_2 = e_2, \quad u_3 = e_3: \quad & B(u_1, u_2) = -w_1, \quad B(u_1, u_3) = -w_2, \quad B(u_2, u_3) = 0. \end{aligned}$$

For linear forms λ, μ write $(\lambda \wedge \mu)(x, x') = \lambda(x)\mu(x') - \mu(x)\lambda(x')$. With the dual basis u_1^*, u_2^*, u_3^* of R^* , the restriction of B to R is $\omega w_1 \otimes (u_2^* \wedge u_3^*) - w_2 \otimes (u_1^* \wedge u_3^*)$ for G_1 and $-w_1 \otimes (u_1^* \wedge u_2^*) - w_2 \otimes (u_1^* \wedge u_3^*)$ for G_2 . If λ, μ are linearly independent forms on the 3-dimensional space R and $U \leq R$ is a plane, then $\lambda \wedge \mu$ vanishes on $U \times U$ if and only if $U \supseteq \ker \lambda \cap \ker \mu$. Indeed, if it vanishes, the restrictions of λ and μ to U are proportional, so a non-zero combination $\alpha\lambda + \beta\mu$ vanishes on U , and $U = \ker(\alpha\lambda + \beta\mu) \supseteq \ker \lambda \cap \ker \mu$; conversely, if U contains the line $\ker \lambda \cap \ker \mu$, both restrictions factor through the 1-dimensional space $U/(\ker \lambda \cap \ker \mu)$, so they are proportional and $\lambda \wedge \mu$ vanishes on U . A plane $U \leq R$ is isotropic if and only if both coordinate forms of $B|_R$ vanish on it, that is, if and only if U contains $\langle u_1 \rangle = \ker u_2^* \cap \ker u_3^*$ and $\langle u_2 \rangle = \ker u_1^* \cap \ker u_3^*$ (for G_1), resp. $\langle u_3 \rangle$ and $\langle u_2 \rangle$ (for G_2). In both cases $U = \langle e_2, e_3 \rangle$. This plane is isotropic ($[c, b] = 1$ in both groups) and all its points lie in R . So the only good line in $\mathbb{P}(R)$ is $D = \mathbb{P}\langle e_2, e_3 \rangle$, which corresponds to $\langle b, c \rangle G'$.

Case 2: $\ell \not\subset \mathbb{P}(R)$. Then ℓ meets the plane $\mathbb{P}(R)$ in at most one point, so at least $p \geq 3$ of its points lie in Z . In coordinates on $\ell \cong \mathbb{P}^1$, each of q_1, q_2, q_3 restricts to a binary quadratic form with at least three zeros in $\mathbb{P}^1(\mathbb{F}_p)$, which is therefore zero. So all points of ℓ lie in Z , and by Lemma 3.4(e) the line ℓ is D , ℓ_∞ or some ℓ_t , $t \in \mathbb{F}_p$. Here $D \subset \mathbb{P}(R)$ is excluded. All points of ℓ_∞ and of the ℓ_t lie in S (Lemma 3.4(d)), so these lines are good if and only if B vanishes on a pair of spanning vectors. Expanding with (1) and (2) gives

$$G_1 : \quad B(P_t, Q_t) = t(\omega - t^2)w_1 + (t^2 - \omega)w_2, \quad B(e_4, e_3) = w_1; \quad (5)$$

$$G_2 : \quad B(P_t, Q_t) = 2t^2w_1 - 2tw_2, \quad B(e_4, e_2) = 0. \quad (6)$$

For G_1 , $B(P_t, Q_t) = 0$ if and only if $t^2 = \omega$, which has no solution in $\mathbb{F}_p$ because ω is a non-residue, and ℓ_∞ is not isotropic: there is no good line in Case 2. For G_2 , ℓ_t is good if and only if $t = 0$ (as p is odd), and ℓ_∞ is good; these are $\ell_0 = \mathbb{P}\langle e_5, e_3 \rangle$ and $\ell_\infty = \mathbb{P}\langle e_2, e_4 \rangle$.

By Lemma 2.2 the good lines D of G_1 , and D, ℓ_∞, ℓ_0 of G_2 , correspond to $\langle b, c \rangle G'_1$, and to $\langle b, c \rangle G'_2$, $\langle b, d \rangle G'_2$, $\langle c, e \rangle G'_2$. This proves Theorem A. $\square$

Remark 4.1. The hypotheses enter as follows. That p is odd is used for the variety and Lemma 2.1 (the factor $\frac{1}{2}$), for the three points needed in Case 2 and in Lemma 3.4(e), and for $2 \neq 0$ in (6). That $\omega \neq 0$ is used throughout. In the proof of Theorem A, the hypothesis that ω is a non-residue is used only once, in $t^2 \neq \omega$; the proof of Theorem B uses it in the same form, $\omega z_1^2 \neq z_2^2$.

Remark 4.2. If $\omega \equiv s^2 \pmod{p}$, the same proof gives two further good lines ℓ_s and ℓ_{-s} for $G_1(\omega)$, so $|\mathcal{A}(G_1(\omega))| = 3$. Since $Q_{\pm s} = -s^2(e_2 \pm e_3/s)$ and $P_{\pm s} = \pm s(e_1 \pm se_4 \pm e_5/s)$, the two extra members of $\mathcal{A}(G_1(\omega))$ are, in additive notation in G/G' ,

$$\langle b + c/s, a + sd + e/s \rangle G' \quad \text{and} \quad \langle b - c/s, a - sd - e/s \rangle G'.$$

This agrees with Proposition C(b).

Remark 4.3. Over the field $\mathbb{F}_p(\sqrt{\omega})$ with p^2 elements, the identity (5) shows that the two rulings $\ell_{\pm\sqrt{\omega}}$ of the scroll of G_1 are isotropic; they are conjugate under the Frobenius map and meet D in the conjugate points $\langle e_2 \pm e_3/\sqrt{\omega} \rangle$. So besides D the group G_1 has two isotropic rulings, neither of them defined over $\mathbb{F}_p$ (and ℓ_∞ is not isotropic), whereas the two isotropic rulings ℓ_0, ℓ_∞ of G_2 are defined over $\mathbb{F}_p$. The invariant $|\mathcal{A}(G)|$ counts the rational ones. Remark 7.2 characterises the isotropic rulings by the position of $\mathbb{P}(R)$ relative to the scroll.

5 The commuting graph on the elements of breadth two

The vertices of $\Gamma(G)$ are the points of S (Lemma 2.1), and two points $\langle x \rangle \neq \langle x' \rangle$ are adjacent if and only if $B(x, x') = 0$; this does not depend on the representatives because B is bilinear. For $x \in S$ let

$\pi_x = \mathbb{P}(\ker \text{ad}_x)$, a projective plane containing x ; the neighbours of x are the points of $S \cap \pi_x$ other than x . We need two identities, obtained by expanding with (1), (2), (3) and (4). First, for $x \in R$, written as $x = (0, x_2, x_3, -\omega x_5, x_5)$ for G_1 and $x = (x_1, x_2, x_3, 0, 0)$ for G_2 ,

$$B(x, \mathbf{v}(y)) = (y_2 L_x(y), -y_1 L_x(y), 0), \quad L_x(y) = \begin{cases} x_2 y_1 - x_3 y_2 + \omega x_5 y_3 & (G_1), \\ x_2 y_1 - x_3 y_2 + x_1 y_3 & (G_2), \end{cases} \quad (7)$$

in the coordinates w_1, w_2, w_3 . Second, for all $y, z \in \mathbb{F}_p^3$,

$$B(\mathbf{v}(z), \mathbf{v}(y)) = \Lambda(y, z) \cdot (-(y_2 z_3 - y_3 z_2), y_1 z_3 - y_3 z_1, -(y_1 z_2 - y_2 z_1)), \quad (8)$$

where $\Lambda(y, z) = \omega y_1 z_1 - y_2 z_2$ for G_1 and $\Lambda(y, z) = y_1 z_2 + y_2 z_1$ for G_2 . The second factor in (8) is, up to signs, the cross product of y and z ; it vanishes if and only if y and z are proportional.

Proof of Theorem B. We count, for each $x \in S$, the points of $\mathbb{P}(R) \cap \pi_x$ and of $Q \cap \pi_x$; recall $S = \mathbb{P}(R) \sqcup Q$.

(a) $x \in \mathbb{P}(R)$, *neighbours in $\mathbb{P}(R)$* . In the basis u_1, u_2, u_3 of Case 1 of Section 4, write $x = \alpha u_1 + \beta u_2 + \gamma u_3$ and $x' = \alpha' u_1 + \beta' u_2 + \gamma' u_3$. For G_1 , $B(x, x') = 0$ means $\beta \gamma' = \gamma \beta'$ and $\alpha \gamma' = \gamma \alpha'$. If $\gamma \neq 0$, this forces $x' \in \langle x \rangle$; if $\gamma = 0$, that is $x \in D$, it means $\gamma' = 0$, so $R \cap \ker \text{ad}_x = \langle u_1, u_2 \rangle$. For G_2 the conditions are $\alpha \beta' = \beta \alpha'$ and $\alpha \gamma' = \gamma \alpha'$, with the same conclusion ($\alpha \neq 0$, resp. $x \in D$ and $\alpha' = 0$). So $|\mathbb{P}(R) \cap \pi_x|$ is $p + 1$ for $x \in D$ and 1 for $x \in \mathbb{P}(R) \setminus D$.

(b) $x \in \mathbb{P}(R)$, *neighbours in Q* . For $y \neq c$ we have $(y_1, y_2) \neq (0, 0)$, so by (7) $\mathbf{v}(y)$ commutes with x if and only if $L_x(y) = 0$. The linear form L_x is non-zero (its coefficients are, up to the factor ω , coordinates of $x \neq 0$), so $\{L_x = 0\}$ is a line of $\mathbb{P}^2(\mathbb{F}_p)$ with $p + 1$ points, and it passes through c if and only if the coefficient of y_3 vanishes, that is, if and only if $x \in D$. By Lemma 3.3(a), $|Q \cap \pi_x|$ is p for $x \in D$ and $p + 1$ for $x \in \mathbb{P}(R) \setminus D$.

Hence each of the $p + 1$ points of D has degree $(p + 1) + p - 1 = 2p$, and each of the p^2 points of $\mathbb{P}(R) \setminus D$ has degree $1 + (p + 1) - 1 = p + 1$, in both groups.

(c) $x = \langle \mathbf{v}(z) \rangle \in Q$, *neighbours in $\mathbb{P}(R)$* . By (b), a point $x' \in R$ commutes with $\mathbf{v}(z)$ if and only if $L_{x'}(z) = 0$; for fixed z this is a non-zero linear condition on x' , because $(z_1, z_2) \neq (0, 0)$. So $R \cap \ker \text{ad}_x$ is a plane and $|\mathbb{P}(R) \cap \pi_x| = p + 1$.

(d) $x = \langle \mathbf{v}(z) \rangle \in Q$, *neighbours in Q* . By (8), for $y \neq z$ in $\mathbb{P}^2(\mathbb{F}_p) \setminus \{c\}$ the points $\mathbf{v}(y)$ and $\mathbf{v}(z)$ commute if and only if y lies on the line $\Lambda_z = \{y : \Lambda(y, z) = 0\}$, whose coefficient vector $(\omega z_1, -z_2, 0)$, resp. $(z_2, z_1, 0)$, is non-zero; Λ_z passes through c , so it has p points other than c . For G_1 , z lies on Λ_z if and only if $\omega z_1^2 = z_2^2$, which is impossible for $(z_1, z_2) \neq (0, 0)$ because ω is a non-residue; so $|Q \cap \pi_x| = p + 1$ for every $x \in Q$. For G_2 , $z \in \Lambda_z$ if and only if $2z_1 z_2 = 0$, that is, z lies on one of the lines $\{y_1 = 0\}$, $\{y_2 = 0\}$ through c ; by Lemma 3.4(a) these are the $2p$ points $\langle \mathbf{v}(0, 1, s) \rangle$ and $\langle \mathbf{v}(1, 0, s) \rangle = \langle e_5 + s e_3 \rangle$ of Q , which lie on ℓ_∞ and ℓ_0 . For them $|Q \cap \pi_x| = p$, and for the other $p^2 - p$ points of Q it is $p + 1$.

By (c) and (d), every point of Q has degree $(p + 1) + (p + 1) - 1 = 2p + 1$ in $\Gamma(G_1)$; in $\Gamma(G_2)$ the $2p$ points of Q on $\ell_\infty \cup \ell_0$ have degree $(p + 1) + p - 1 = 2p$ and the other $p^2 - p$ have degree $2p + 1$. Together with (a) and (b) this is the stated degree pattern, and half the sum of the degrees is $\frac{1}{2}(3p^3 + 6p^2 + 3p) = \frac{3}{2}p(p + 1)^2$ for G_1 and $\frac{1}{2}(3p^3 + 6p^2 + p)$ for G_2 . $\square$

Remark 5.1. In both graphs the vertices of degree $2p$ are exactly the points on the members of $\mathcal{A}(G)$: the $p + 1$ points of D for G_1 , and the $3p + 1$ points of $D \cup \ell_\infty \cup \ell_0$ for G_2 . So Theorems A and B are two readings of the same geometry. For a square ω the proof of (d) changes ($z \in \Lambda_z$ if and only if $z_2 = \pm s z_1$) and gives the pattern of G_2 , as it must by Proposition C.

6 The square class of ω

Proof of Proposition C. Exponents of elements are taken modulo p ; for s prime to p , $1/s$ denotes an inverse of s modulo p . We use that if five elements of a group H in the variety satisfy the relations of a presentation and generate H , then the presentation maps onto H , and that an epimorphism between groups of the same finite order is an isomorphism. All groups involved have order p^8 by Lemma 2.1, which holds for every $\omega \in \mathbb{F}_p^\times$.

(a) In $G_1(\omega)$ put $a' = a$, $b' = b^{1/s}$, $c' = c$, $d' = d^{1/s}$ and $e' = e^s$. As commutation is bimultiplicative, $[c', b'] = [d', b'] = [e', c'] = [e', d'] = 1$, $[d', c'] = [d, c]^{1/s} = [b, a]^{1/s} = [b', a']$, $[e', b'] = [e, b] = [c, a] = [c', a']$, and

$$[e', a'] = [e, a]^s = [d, a]^{\omega s} = ([d, a]^{1/s})^{\omega s^2} = [d', a']^{\omega s^2}.$$

So $a', \dots, e'$ satisfy the relations of $G_1(\omega s^2)$. Their images $e_1, e_2/s, e_3, e_4/s, se_5$ in V form a basis, so they generate $G_1(\omega)$ modulo $G_1(\omega)'$, hence generate $G_1(\omega)$ (the derived subgroup is the Frattini subgroup). Therefore $G_1(\omega s^2) \cong G_1(\omega)$.

(b) Let $\omega \equiv s^2$. In $G_1(\omega)$ put

$$a' = (d^\omega e^{-1})^2, \quad b' = b c^{1/s}, \quad c' = b c^{-1/s}, \quad d' = a^s d^{s^2} e, \quad e' = a^{-s} d^{s^2} e,$$

whose images in V are $2(\omega e_4 - e_5)$, $e_2 + e_3/s$, $e_2 - e_3/s$, $P_s = s e_1 + s^2 e_4 + e_5$ and $P_{-s} = -s e_1 + s^2 e_4 + e_5$. Expanding with (1) (and $\omega = s^2$) gives

$$\begin{aligned} [d', a'] &= [e', a'] = [c', b'] = [d', b'] = [e', c'] = 1, \\ [d', c'] &= [b', a'] = -2s w_1 + 2w_2, \quad [e', b'] = [c', a'] = 2s w_1 + 2w_2; \end{aligned}$$

for instance $B(P_s, \omega e_4 - e_5) = s\omega B(e_1, e_4) - sB(e_1, e_5) = -s\omega w_3 + s\omega w_3 = 0$, using $B(e_4, e_5) = 0$. These are the defining relations of G_2 . The matrix of the images of $a', \dots, e'$ in the basis $e_1, \dots, e_5$ has determinant $16s^2$, which is non-zero as p is odd. As in (a), $a', \dots, e'$ generate $G_1(\omega)$, and $G_2 \cong G_1(\omega)$.

The last statement follows from (a), (b) and Theorem A: if ω and ω' are non-residues, then $\omega' \equiv \omega s^2$ for some s . $\square$

The images of d' and e' are the points $P_{\pm s}$ of the two extra good rulings $\ell_{\pm s}$ of Remark 4.2, and b', c' span D ; so the isomorphism maps the three good lines of G_2 onto those of $G_1(s^2)$. The generators were found from this observation.

Remark 6.1 (Relation to Vaughan-Lee's list). Vaughan-Lee's list contains every group of class 2 and exponent p of order at most p^8 , for every odd p [VL15, Theorem 3 and §2]; so each $G_1(\omega)$ is isomorphic to one of the listed groups, and in this sense Proposition C is implicit in the classification. Vaughan-Lee takes ω primitive throughout and remarks, for a group of order p^6 , that any non-residue gives the same group [VL15, pp. 4–5]; part (a) is the analogous statement for 8.5.14. We did not find the identification (b) of $G_1(s^2)$ with 8.5.15 stated in the parts of [VL15] that we read. Proposition C is consistent with the orders of the automorphism groups, $2(p-1)(p^2-1)p^{17}$ for 8.5.14 and $2(p-1)^3p^{17}$ for 8.5.15 [VL15, p. 29]: the matrices given there for the action of $\text{Aut}(G_1)$ on G/G' contain the blocks $\begin{pmatrix} \alpha & \beta \\ \omega\beta & \alpha \end{pmatrix}$, $(\alpha, \beta) \neq (0, 0)$, in the rows and columns of b and c , whose determinant $\alpha^2 - \omega\beta^2$ is the norm form of $\mathbb{F}_p(\sqrt{\omega})/\mathbb{F}_p$; they form a cyclic group of order $p^2 - 1$, matching the factor $p^2 - 1$ and the pair of conjugate rulings of Remark 4.3. None of this is used in our proofs. The class numbers are discussed in Section 7.

Remark 6.2 (The encoding in the proposers' repository). The Magma file `reps-5-3.m` of [OS24] encodes 8.5.14 by a commutator matrix in which $[d, a] = [e, a]^\omega$, that is, by $G_1(1/\omega)$ in our notation: its matrix $B_{14}(y)$ satisfies $-B_{14}(y_1, y_2, y_3) = M_1(y_1, y_2, \omega y_3)$ with ω replaced by $1/\omega$ in M_1 . Since

$1/\omega$ is again a non-residue, this is the same group by Proposition C(a). Its matrix $B_{15}(y)$ equals $-M_2(y)$. The first and the third verification runs computed $|\mathcal{A}|$ directly for these two matrices as well (Section 8).

7 Other invariants of the pair

Proposition 7.1. *For every odd prime p and every non-residue ω , the following numbers are the same for G_1 and G_2 .*

- (a) *The numbers of points of $\mathbb{P}(G/G')$ of breadth 2 and 3: $n_2 = 2p^2 + 2p + 1$ and $n_3 = p^4 + p^3 - p^2 - p$.*
- (b) *The class number $k(G) = p^5 + 2p^4 - p^3 - p^2$.*
- (c) *The number $a_i(G)$ of abelian subgroups $A \geq G'$ with $|A : G'| = p^i$: $a_0 = 1$, $a_1 = p^4 + p^3 + p^2 + p + 1$, $a_2 = p^3 + 2p^2 + p + 1$, and $a_i = 0$ for $i \geq 3$.*
- (d) *The number of lines of $\mathbb{P}(G/G')$ all of whose points have breadth 2: $p^2 + 2p + 2$.*
- (e) *The character degrees: G has p^5 irreducible characters of degree 1, $p^4 - p^3$ of degree p and $p^4 - p^2$ of degree p^2 .*

Proof. (a) is Lemma 3.3. (b) An element (v, w) has $|C_G((v, w))| = p^{8-b(v)}$, so

$$k(G) = \frac{1}{|G|} \sum_{g \in G} |C_G(g)| = \sum_{v \in V} p^{3-b(v)} = p^3 + n_2(p-1)p + n_3(p-1) = p^5 + 2p^4 - p^3 - p^2.$$

(c) Every 1-dimensional subspace is isotropic. An isotropic plane through a point x is a line through x in the projective space $\mathbb{P}(\ker \text{ad}_x)$ of dimension $4 - b(x)$, so there are $p + 1$ of them if $b(x) = 2$ and one if $b(x) = 3$; counting pairs (point, isotropic plane through it) gives $a_2 = (n_2(p+1) + n_3)/(p+1) = p^3 + 2p^2 + p + 1$. If U were an isotropic subspace of dimension 3, every non-zero $x \in U$ would satisfy $U \leq \ker \text{ad}_x$, hence $b(x) \leq 2$, and each of the $p^2 + p + 1$ lines of $\mathbb{P}(U)$ would be good, contradicting Theorem A; so $a_3 = 0$, and then $a_i = 0$ for $i \geq 3$. (d) The lines in $\mathbb{P}(R)$ are the $p^2 + p + 1$ lines of a plane. A line in S not contained in $\mathbb{P}(R)$ lies in Z by the argument of Case 2 of Section 4, which does not use isotropy, so it is ℓ_∞ or some ℓ_t by Lemma 3.4(e); conversely these $p + 1$ lines lie in S (Lemma 3.4(d)). (e) As $Z(G) = G'$ (Lemma 3.3), an irreducible character χ restricts to $G' = W$ as $\chi(1)\lambda$ for a linear character λ of W . If $\lambda = 1$, χ is one of the p^5 linear characters. Otherwise $\lambda(w) = \zeta^{\eta(w)}$ with ζ a primitive p -th root of unity and $0 \neq \eta = \sum y_k w_k^*$, so that $\lambda([g, h]) = \zeta^{f_y(v, v')}$ for $g = (v, w)$, $h = (v', w')$. If $v \notin \text{rad } f_y$, choose h with $\lambda([g, h]) \neq 1$; then $\chi(g) = \chi(h^{-1}gh) = \chi(g[g, h]) = \lambda([g, h])\chi(g)$, so $\chi(g) = 0$. If $v \in \text{rad } f_y$, then g is central modulo $\ker \lambda \subseteq \ker \chi$, so $|\chi(g)| = \chi(1)$. Hence $1 = \langle \chi, \chi \rangle = p^{8-\text{rank } f_y} \chi(1)^2 / p^8$, that is, $\chi(1)^2 = p^{\text{rank } f_y}$, and since the characters lying over λ satisfy $\sum \chi(1)^2 = |G : G'| = p^5$, there are $p^{5-\text{rank } f_y}$ of them. By Lemma 3.2 there are $p - 1$ non-zero y with $\text{rank } f_y = 2$ and $p^3 - p$ with $\text{rank } f_y = 4$; this gives $(p - 1)p^3$ characters of degree p and $(p^3 - p)p$ of degree p^2 . $\square$

The class numbers in (b) are those of [VL15, p. 29], so (b) is a consistency check of Lemma 3.3. Qiao [Qia24, §1.3.3] attaches to a p -group P of class 2 and exponent p the polynomial $\text{Ab}(P, x) = 1 + \sum_{i \geq 1} a_i(P) x_p^i$, where x_p^i is a fixed polynomial in x of degree i , and identifies it with the totally-isotropic polynomial of the associated space of alternating matrices. By (c) this polynomial is the same for G_1 and G_2 . Since elements of G commute pairwise if and only if their images span an isotropic subspace of V , (c) also shows that for every $r \geq 2$ the number of r -tuples of pairwise commuting elements of G is the same for G_1 and G_2 : it is $p^{3r} \sum_d a_d N_{d,r}$, where $N_{d,r}$ is the number of r -tuples

that span a given d -dimensional space. Part (e) refines (b) from the number of irreducible characters to their degrees. The invariant $|\mathcal{A}(G)|$ refines the count a_2 by breadth: among the $p^3 + 2p^2 + p + 1$ abelian subgroups $A \geq G'$ of order p^5 , it counts those whose elements outside G' all have breadth 2. Without the isotropy condition the count (d) does not separate the groups either.

The determinantal invariants. In the notation of [OS26, §2], the commutator matrix $B(y)$ is, up to sign and the choice of bases, our $M(y)$, and the (i, κ) entry of its adjoint $B^\bullet(x)$ is $\sum_j B_{ij}^{(\kappa)} x_j$, so that $B^\bullet(x)$ has the rank of ad_x . For $k \leq 5$ and $\ell \leq 3$ let $I_k(B)$ and $J_\ell(B^\bullet)$ be the ideals of $k \times k$ minors, as in [OS26, Theorem 2.3], and n_p the number of $\mathbb{F}_p$ -points of the affine variety of an ideal. In [OS26, Table 2] the cases (14) and (15) both have $n_p(I_4(B)) = p$, $\deg I_4(B) = 3$, $n_p(J_3(B^\bullet)) = 2p^3 - p$ (written $I_3(B^\bullet)$ there) and degrees (1, 3) of the ideals of a minimal primary decomposition of $J_3(B^\bullet)$. Our results account for these values.

- By Lemma 3.2(c), the ideals generated by the 4×4 Pfaffians of $M_1(y)$ and $M_2(y)$ coincide. Moreover every 4×4 minor of $M(y)$ is $\pm \text{Pf}_i \text{Pf}_j$ for some i, j (a direct computation, done by the third verification run of Section 8; it reflects the classical fact that the adjugate of an alternating matrix of order 5 is the product of its vector of signed Pfaffians with its transpose), so $I_4(B)$ is the square $(y_1, y_2)^2 (y_1, y_2, y_3)^2$ of the Pfaffian ideal, for both groups. The affine variety of $I_4(B)$ is $\{y : \text{rank } M(y) \leq 2\} = \{y_1 = y_2 = 0\}$, with p points, and its projective variety is the single point c . In degree $d \geq 4$ the monomials outside $I_4(B)$ are y_3^d , $y_1 y_3^{d-1}$ and $y_2 y_3^{d-1}$, so the Hilbert function of $\mathbb{F}_p[y]/I_4(B)$ is 1, 3, 6, 10, 3, 3, 3, ... for every p (as the program of this note finds for $p \leq 7$, and the first verification run over $\mathbb{Q}$), and the point c has multiplicity 3; this is the value $\deg I_4(B) = 3$. It is not the degree of the scroll.
- The affine variety of $J_3(B^\bullet)$ is the set of $x \in V$ with $\text{rank ad}_x \leq 2$, that is, 0 and the vectors of breadth 2; by Lemma 3.3 it has $1 + (p-1)(2p^2 + 2p + 1) = 2p^3 - p$ points. Its projectivisation is the union of the plane $\mathbb{P}(R)$ and the cubic scroll Z , which meet along the line D (Lemma 3.4(d)); this is consistent with the degrees (1, 3) of the primary components, the 3 being the degree of the scroll.

So the Pfaffian ideals and the ideals $I_4(B)$ coincide, the rank loci of B coincide, and the rank loci of $B^\bullet$ have the same numbers of points and components of the same degrees. This is consistent with, and partly explains, the finding of O'Brien and Stanojkovski that the invariants of [OS26, Theorem 2.3] do not separate the pair for $3 \leq p \leq 37$; we have not proved that all these invariants coincide for every p . The rank loci of $B^\bullet$ themselves are not the same, however: the plane $\mathbb{P}(R)$ lies differently with respect to the scroll, and $|\mathcal{A}(G)|$ can be read off from its position.

Remark 7.2 (The position of the plane $\mathbb{P}(R)$). The planes of $\mathbb{P}(V)$ that contain the line D are the points of the projective plane $\mathbb{P}(V/D)$, on which X_1, X_4, X_5 are coordinates in both groups. The rulings ℓ_t and ℓ_∞ give the $p+1$ points $(t : t^2 : 1)$ and $(0 : 1 : 0)$ of the conic $C : X_1^2 = X_4 X_5$, and $\mathbb{P}(R)$ gives the point $r = (0 : -\omega : 1)$ for G_1 and $r = (1 : 0 : 0)$ for G_2 , which is not on C . A hyperplane of $\mathbb{P}(V)$ that contains $\mathbb{P}(R)$ corresponds to a line of $\mathbb{P}(V/D)$ through r , and it contains exactly the rulings whose points lie on this line. The polar line of r with respect to C is $X_4 = \omega X_5$ for G_1 and $X_1 = 0$ for G_2 , so the tangents to C through r touch C at the points with $t^2 = \omega$, none of which is rational, resp. at the points of ℓ_0 and ℓ_∞ . Comparing with Case 2 of Section 4: a ruling is isotropic if and only if it is the only ruling in the hyperplane spanned by $\mathbb{P}(R)$ and this ruling, and $|\mathcal{A}(G)| - 1$ is the number of rational tangents to C through r .

The set S determines $\mathbb{P}(R)$, the only plane contained in S (another plane in S would contain at least $p^2 + p$ lines of S not lying in $\mathbb{P}(R)$, but there are only $p+1$ such lines by Proposition 7.1(d)), and it determines the rulings, the other lines contained in S . Hence the sets S of G_1 and G_2 are not projectively equivalent. For instance, a hyperplane not containing $\mathbb{P}(R)$ meets S in at most

$(p+1) + (2p+1)$ points (a line of $\mathbb{P}(R)$ and, by Lemma 3.3(a), the points of a conic of $\mathbb{P}^2(\mathbb{F}_p)$), and one containing $\mathbb{P}(R)$ meets it in $p^2 + p + 1 + mp$ points, where m is the number of rulings in it; so exactly two hyperplanes meet S in $p^2 + 2p + 1$ points for G_2 , and none for G_1 . In terms of the groups: exactly two maximal subgroups of G_2 , and none of G_1 , contain exactly $p^2 + 2p + 1$ of the subgroups $\langle x \rangle G'$ with $b(x) = 2$. As an isomorphism of groups induces a linear isomorphism of the rank loci of $B^\bullet$ (see the proof of [OS26, Theorem 2.3]), the rank locus of $B^\bullet$, as a configuration up to linear isomorphism, separates the two groups; only its numerical invariants listed in [OS26, Theorem 2.3] fail to do so (for $3 \leq p \leq 37$, by [OS26, §4.1]).

Remark 7.3 (The invariant of Brahana and Copetti). In [Cop04, Theorem 7.22] the orbits 14 and 15 are the spaces $\langle [a_1, a_2] + [a_3, a_4], [a_1, a_3] + [a_2, a_5], [a_1, \omega a_4 + a_5] \rangle$ and $\langle [a_1, a_2] + [a_3, a_4], [a_1, a_3] + [a_2, a_5], [a_4, a_5] \rangle$ of 2-vectors. If $[a_i, a_j]$ is read as the form $e_i^* \wedge e_j^*$ on V , the second is the net $\{f_y\}$ of G_2 , and the first is that of $G_1(1/\omega)$, the same group as G_1 by Proposition C(a). Copetti's proof that the two orbits are different [Cop04, Lemma 7.21] uses the only decomposable element of the space, here $f_c = u \wedge v$ with $\langle u, v \rangle = R^\perp$, and the pencil of conics cut out on the space by the quadrics $Q_x: x_1 B_5 - x_2 B_4 + x_3 B_3 - x_4 B_2 + x_5 B_1 = 0$, $x \in \langle u, v \rangle$, where $B_1, \dots, B_5$ are the Plücker quadrics; the pencil of orbit 15 contains double lines and that of orbit 14 does not. On the net, B_{6-k} is the Pfaffian Pf_k of $M(y)$, so the conic of x is $\{y : x(\mathbf{v}(y)) = 0\}$. For $x \in R^\perp$ we have $x(\mathbf{v}(1, t, s)) = x(P_t)$ and $x(\mathbf{v}(0, 1, s)) = x(e_4)$ by Lemma 3.4(a), because Q_t, e_3 and e_2 lie in R ; so the conic of x is the union of the lines of $\mathbb{P}^2(\mathbb{F}_p)$ through c that correspond to the rulings in the hyperplane $x = 0$, which contains $\mathbb{P}(R)$. Thus the pencil is the pencil of hyperplanes through $\mathbb{P}(R)$ of Remark 7.2, and its double lines are the hyperplanes containing exactly one ruling. Explicitly, the pencil is $\alpha y_1 y_2 + \beta(y_2^2 + \omega y_1^2)$ for G_1 , without a double line because $\alpha^2 - 4\omega\beta^2 \neq 0$ for $(\alpha, \beta) \neq (0, 0)$, and $\alpha y_2^2 + \beta y_1^2$ for G_2 , with the double lines y_1^2 and y_2^2 , which correspond to ℓ_∞ and ℓ_0 . Hence, for G_1 and G_2 ,

$$|\mathcal{A}(G)| = 1 + (\text{the number of double lines in the pencil of [Cop04, Lemma 7.21]}),$$

and Theorem A restates the classical invariant in terms of abelian subgroups and centralisers. According to [Cop04, p. 82], the argument of [Cop04, Lemma 7.21] is modelled on [Bra51, pp. 548–549] and outlined in [Bra58, p. 650]; we have not seen these pages.

8 Computations and reproducibility

Theorems A and B, Proposition C and Proposition 7.1, all lemmas and the remarks are proved by the written arguments above, for every odd prime p ; no proof depends on a computation. The computations are tests. The reproducibility package has five parts: the program of this note, the programs of the first write-up, and the programs of three independent verification runs.

The program of this note (`check_note.py`, Python with sympy, about ten seconds). It starts from the two presentations as text, forms the seven relation vectors in $\Lambda^2 V$, checks that they are independent and that $[b, a], [c, a], [d, a]$, resp. $[b, a], [c, a], [e, d]$, span a complement, and derives the tables (1), (2). It then checks as identities in $\mathbb{Z}[\omega, y, z, t, s, 1/s]$ the matrices $M(y)$, the Pfaffians and $\mathbf{v}(y)$, $M(y)\mathbf{v}(y) = 0$, the radical R , the factorisation of $N(\mathbf{v}(y))$ in Lemma 3.4(a) and the parametrisation in (b), (5), (6), the restriction of B to R , (7), (8), the counting identities of Theorem B and Proposition 7.1, the relations in the proof of Proposition C with the determinant $16s^2$, the two extra members of Remark 4.2 (and that $a - sd + e/s$, with the other sign, is not one of them), and the statements on B_{14}, B_{15} in Remark 6.2. Finally, for $p = 3, 5, 7$, for G_2 and for $G_1(\omega)$ with every $\omega \in \mathbb{F}_p^\times$ (15 groups), it computes the breadth of every point of $\mathbb{P}(V)$ and checks the decomposition of Lemma 3.4(d); runs through all $\binom{5}{2}_p$ planes (1210, 20306 and 140050); counts the isotropic ones, the lines inside S , the isotropic 3-spaces and $|\mathcal{A}(G)|$ with its members; and computes the degrees

and edges of $\Gamma(G)$ and the class number. It also computes the Hilbert function of $\mathbb{F}_p[y]/I_4(B)$ in degrees $0, \dots, 8$. All results agree with Theorems A and B, Proposition C and Proposition 7.1 and Remarks 4.2 and 5.1: $|\mathcal{A}(G_1(\omega))| = 1$ with member $\langle b, c \rangle G'$ for the 6 non-residues, and $|\mathcal{A}| = 3$ with the predicted members for G_2 and for the 6 residues. When the sign of e/s in the prediction of Remark 4.2, or a single coefficient in (5), or one exponent in a presentation was changed deliberately, the program reported failures.

The programs with which the results were first obtained (original/): a symbolic check of the identities of Sections 3 to 5 and one of Proposition C (sympy); an enumeration over all points of $\mathbb{P}(V)$, computing breadths, all isotropic planes as lines through a point x in $\mathbb{P}(\ker \text{ad}_x)$, $|\mathcal{A}(G)|$ and $\Gamma(G)$, in 17 runs with $p \in \{3, 5, 7, 11, 13\}$, including non-residues that are not primitive and four residues; and the search that produced the generators of Proposition C(b), for $(p, s) \in \{(3, 1), (5, 2), (7, 3), (11, 5), (13, 4)\}$.

Three independent verification runs, each with its own programs and their recorded outputs (verification_run_A/, verification_run_B/, independent_run_2/); see the next paragraph. Together they enumerated all planes for $p \leq 23$ (the first run: $p \in \{3, 5, 7, 11, 13, 17, 19, 23\}$; the second: $p \leq 13$ with every $\omega \in \mathbb{F}_p^\times$, and $p = 17$ by a second algorithm) and all isotropic lines, as decomposable vectors of the relation space, for $p \leq 13$ with every ω and for $p = 17$ (the third), and computed inside the groups themselves, by explicit multiplication, for $p = 3$ (all three runs) and $p = 5$ (the second). When this note was written, all programs of the package with a recorded output were run again from a copy of the package, except the longest runs; every output was identical to the recorded one (RERUN_LOG.txt). The third run ran all of them again from the archive, the longest included, with the same result (independent_run_2/r2_package_rerun.txt).

Verification. The results were first obtained, with proofs, together with the programs in original/. Three independent verification runs, all AI-assisted, followed; each wrote its own programs from the definitions. The first two worked separately before this note was written, and neither saw the other's report; the third examined the final text of this note and the package.

The first run (A) compared the statement with the source and with [VL15], and re-derived the proofs of Lemma 2.1 (with the order argument used here), of Lemmas 3.3 and 3.4, of Theorem A, of Theorem B and of Proposition C line by line. Its programs derive the commutator tables from the presentations, recompute every identity symbolically, and enumerate all 2-dimensional subspaces of $\mathbb{F}_p^5$ through reduced row echelon forms, with breadths from the 3×3 minors of ad_x and radicals by elimination, for the source's presentations at $p \in \{3, 5, 7, 11, 13, 17, 19, 23\}$ and for the matrices B_{14} , B_{15} of [OS24] at $p \leq 13$, with residues and with non-residues that are not primitive. It computed in the group of order 3^8 itself, by multiplication only (centraliser orders, the class number 369, all 1210 subgroups $A \geq G'$ with $|A : G'| = 9$, of which 49 are abelian and 1, resp. 3, lie in $\mathcal{A}$), counted the automorphisms for $p = 3$ (the orders $2(p-1)(p^2-1)p^{17}$ and $2(p-1)^3p^{17}$ of [VL15], and the same order for $G_1(1)$ and G_2), and computed the Hilbert function of $I_4(B)$.

The second run (B) re-derived the proofs, computed the tables from the presentations, enumerated all planes and the isotropic 3-spaces for $p \leq 13$ and every $\omega \in \mathbb{F}_p^\times$ (40 runs) and the lines on Z for $p \leq 11$, used a second algorithm with deliberately wrong inputs for $p = 5, 7$ and 17 (all detected), computed inside the groups by explicit multiplication for $p = 3$ and for $G_1(2)$ at $p = 5$ (class number 4225, 181 abelian $A \geq G'$ of order p^5 , $|\mathcal{A}| = 1$), ran the original programs again from a copy and obtained identical outputs, and searched the literature.

Neither of these two runs found a mathematical error. The corrections they required were made: the count $2p^3 - p = 1 + (p-1)(2p^2 + 2p + 1)$ in Section 7; the reading of $\deg I_4(B) = 3$ as the multiplicity of a point, not the degree of the scroll; the sign of e/s in Remark 4.2; the author of [Lee16]; the classification sources [Bra51, Cop04], which were missing from the first write-up and which these

runs could not read; the statement about [OS26], which is now that our results are consistent with their computations for $p \leq 37$; the place where the restatement of the problem in [ula26] is found; the description of Vaughan-Lee’s convention on ω and of the blocks in his automorphism matrices; the encoding in [OS24] (Remark 6.2); and the relation to Qiao’s polynomial (Section 7). The proof that $a_3 = 0$ in Proposition 7.1(c), part (d) of Proposition 7.1 and the program `check_note.py` were added when this note was written; the third run examined them.

The third run examined the final text of this note and the package line by line, as if nothing had been checked. It read again the problem and the lecture abstract in [DENRD25], Sections 1, 2 and 8.5 of [VL15], Sections 2 and 4 of [OS26], Section 1 of [Qia24] and the file `reps-5-3.m`, and it read Chapters 1 and 7 of [Cop04], which the earlier runs could not reach, and [VL17, p. 37]. It re-derived every proof and found no error in a theorem, proposition or lemma. Its programs, written without using those of the note or of the earlier runs, work in Brahana’s model: the relation space $K \leq \Lambda^2 V$ of each presentation, the breadth of x as $\dim(x \wedge V + K) - 7$, and the isotropic lines as the decomposable vectors of K , found with the Plücker relations on all points of $\mathbb{P}(K)$. For G_2 , B_{14} , B_{15} and $G_1(\omega)$ with every $\omega \in \mathbb{F}_p^\times$ for $p \leq 13$, and for five of these groups each at $p = 17$ and $p = 19$, they confirmed Theorems A and B, Proposition 7.1 with the character degrees, and Remarks 4.2, 5.1, 7.2 and 7.3 (the tangents through r , the hyperplane counts, and the double lines of the pencil of [Cop04, Lemma 7.21], computed from its definition). The run checked 75 identities symbolically, among them those of Sections 3 to 5, Proposition C and the factorisation of the 4×4 minors of $M(y)$; computed in the groups of order 3^8 by multiplication only, in a polycyclic model; detected deliberately wrong inputs; and ran the whole package again from the archive, with outputs identical to the recorded ones. The corrections it required were made: the credit to Brahana and Copetti for separating the pair without automorphism groups, in the abstract, Section 1 and below, with Remark 7.3; the replacement of the closing sentence of the first version of Section 7, which said that $|\mathcal{A}(G)|$ is not a function of the rank loci, by Remark 7.2; the reference [Bra58]; the statement on [VL17]; the character degrees in Proposition 7.1; the range $p \leq 11$ of the second run for the lines on Z ; and the description of this run.

Scope and priority. The note answers the question of [DENRD25] in the following sense: Theorem A gives an isomorphism invariant, defined through orders of subgroups and centralisers, which takes different values on G_1 and G_2 , with a proof for every odd prime p and every non-residue ω , in particular for every primitive ω as in the source. Whether this invariant is “simpler” in the sense intended by the proposers is a judgment and not a theorem; Section 1.3 gives our reasons, and the proposers may judge otherwise. The question, the pair of groups and the finding that the invariants of [OS26] do not separate it are due to Stanojkovski and to O’Brien and Stanojkovski [DENRD25, OS26]; the presentations, the orders of the automorphism groups and the class numbers are due to Vaughan-Lee [VL15]; the classification of these groups is due to Brahana, Copetti and Vaughan-Lee [Bra51, Bra58, Cop04, VL15], and the first separation of this pair without automorphism groups, by a pencil of conics, to Copetti and Brahana [Cop04, Lemma 7.21] [Bra51, pp. 548–549]; breadth, centralisers and the correspondence of Baer are classical. By Remark 7.3, Theorem A is a group-theoretic form of that classical invariant. To our knowledge the invariant $|\mathcal{A}(G)|$ with Theorem A and its uniform proof, Theorem B and Proposition C are not in print in this form; Proposition C is implicit in the completeness of the list of [VL15] (Remark 6.1).

What was read: the problem and the abstract of Stanojkovski’s lecture in the open PDF of [DENRD25] on the publisher’s site (pp. 1443 and 1399–1400, fetched on 14 October 2026); of [VL15], in arXiv version 1, Sections 1 and 2 (pp. 1–5) and the entries 8.5.11 to 8.5.17 (pp. 28–30); [OS26] completely, in arXiv version 3, the journal version not being compared; of [OS24], the file `reps-5-3.m` and the README, and, by the first two verification runs, the file `invariants.m`; of [Qia24], in arXiv

version 2, Section 1; of [Cop04], in the copy of the ANU repository fetched by the third verification run on 14 October 2026, Chapters 1 and 7 (Theorems 7.17 and 7.22 and Lemma 7.21 with their proofs); of [VL17], the introduction and p. 37; of [WYZ20] and of the other works found in the searches, the abstracts. Not read: Brahana’s papers [Bra51], which is behind a paywall, and [Bra58], whose open copy on the publisher’s site refused our automated requests on 14 October 2026. What we say about them is taken from [Cop04] and [OS26]. The earlier attempts to reach [Cop04] (two by the first verification run and one at the first writing) had failed.

The searches were made on 14 October 2026, for the first write-up, by the three verification runs and at the writing: queries to the arXiv (for the authors of the problem and of [OS26], and for abstracts with “exponent p ” together with “class 2” or “class two”, with “Vaughan-Lee”, “Brahana”, “Pfaffian”, “alternating bilinear”, “commutator matrix”, “abelian subgroups” or “breadth”), to Crossref, zbMATH and Semantic Scholar, the lists of citing works in OpenAlex (of [OS26], [VL15], [Bra51] and [Bra58]), the repository [OS24], and seven web searches. OpenAlex lists no work citing [OS26] and three works citing [VL15], namely [Lee16], [VL17] and [WYZ20]. Of these, [VL17, p. 37] gives for both groups the numbers of descendants of order p^9 and exponent p , $(p + 37)/2$ and $(p + 81)/2$ for $p \geq 5$, which differ but are computed from the automorphism groups; [Lee16] and [WYZ20] do not treat the pair, and according to its abstract [WYZ20] gives representatives of these groups, in the case of five generators and derived subgroup of order p^3 , only for $p = 3$. The other works citing [Bra51] or [Bra58] in OpenAlex do not treat the pair, as far as their titles and available abstracts show. The closest work is [Cop04] (with [Bra51]), whose invariant is related to ours by Remark 7.3. We found no statement of $|\mathcal{A}(G)|$, of Theorem B or of Proposition C; a search that finds nothing is not a proof of novelty, and no priority is claimed beyond the statements above.

AI-assisted tools were used to search the problem corpus and the literature, to find the arguments, to write and run the verification programs, and to help prepare this manuscript. The author has reviewed the proofs, the computations and the sources and is responsible for all claims. The note has not been peer reviewed.

References

- [Bra51] H. R. Brahana. Finite metabelian groups and the lines of a projective four-space. *American Journal of Mathematics*, 73(3):539–555, 1951. doi:10.2307/2372306.
- [Bra58] H. R. Brahana. Metabelian p -groups with five generators and orders p^{12} and p^{11} . *Illinois Journal of Mathematics*, 2(4B):641–717, 1958. doi:10.1215/ijm/1255448335.
- [Cop04] Annalisa Copetti. Finite-dimensional Lie algebras of nilpotency class 2. Master’s thesis, Australian National University, 2004. URL: <https://openresearch-repository.anu.edu.au/handle/1885/150852>.
- [DENRD25] Heiko Dietrich, Bettina Eick, Gabriele Nebe, and Colva Roney-Dougal. Computational Group Theory. *Oberwolfach Reports*, 22(2):1389–1450, 2025. Report 27/2025 (workshop of 1–6 June 2025); problem of M. Stanojkovski in the Summary of the Problem Session, p. 1443; abstract of Stanojkovski’s lecture, pp. 1399–1400. doi:10.4171/owr/2025/27.
- [Lee16] Seungjai Lee. A class of descendant p -groups of order p^9 and Higman’s PORC conjecture. *Journal of Algebra*, 468:440–447, 2016. doi:10.1016/j.jalgebra.2016.08.042.
- [OS24] E. A. O’Brien and Mima Stanojkovski. Geometric invariants for finite p -groups. Magma code, <https://github.com/eamonnaobrien/Invariants-class2-pgroups>, 2024. GitHub repository.

- [OS26] E. A. O'Brien and Mima Stanojkovski. Geometric invariants for p -groups of class 2 and exponent p . *Journal of Algebra*, 703:266–278, 2026. Cited from arXiv version 3 (25 March 2026). `arXiv:2411.19555`, doi:10.1016/j.jalgebra.2025.08.029.
- [Qia24] Youming Qiao. A q -analogue of graph independence polynomials with a group-theoretic interpretation, 2024. Version 2 (2026). `arXiv:2408.09963`.
- [ula26] ulamai. UnsolvedMath. Hugging Face dataset, <https://huggingface.co/datasets/ulamai/UnsolvedMath>, 2026. Version 1.6.0; record OWR-14299292-013.
- [VL15] Michael Vaughan-Lee. The automorphisms of class two groups of prime exponent, 2015. Version 1. `arXiv:1501.00678`.
- [VL17] Michael Vaughan-Lee. The class three groups of order p^9 with exponent p , 2017. `arXiv:1702.04898`.
- [WYZ20] Zheyang Wan, Yu Ye, and Chi Zhang. Extension of elementary p -groups and its application in classification of groups of prime exponent, 2020. `arXiv:2003.12802`.