Mathematische Annalen
https://doi.org/10.1007/s00208-021-02193-8

Mathematische Annalen

Hessian matrices, automorphisms of p-groups, and torsion points of elliptic curves

Mima Stanojkovski[1] · Christopher Voll[2]

Received: 21 December 2019 / Revised: 13 April 2021 / Accepted: 22 April 2021

Abstract

We describe the automorphism groups of finite p-groups arising naturally via Hessian determinantal representations of elliptic curves defined over number fields. Moreover, we derive explicit formulas for the orders of these automorphism groups for elliptic curves of j-invariant 1728 given in Weierstrass form. We interpret these orders in terms of the numbers of 3-torsion points (or flex points) of the relevant curves over finite fields. Our work greatly generalizes and conceptualizes previous examples given by du Sautoy and Vaughan-Lee. It explains, in particular, why the orders arising in these examples are polynomial on Frobenius sets and vary with the primes in a nonquasipolynomial manner.

Mathematics Subject Classification 20D15 · 11G20 · 14M12

Contents

Communicated by Andreas Thom.

✉ Christopher Voll
C.Voll.98@cantab.net

Mima Stanojkovski
mima.stanojkovski@mis.mpg.de

1 Max-Planck-Institute for Mathematics in the Sciences, Inselstrasse 22, 04103 Leipzig, Germany

2 Fakultät für Mathematik, Universität Bielefeld, 33501 Bielefeld, Germany

1 Introduction and main results

In the study of general questions about finite p-groups it is frequently beneficial to focus on groups in natural families. Often, this affords an additional geometric point of view on the original group-theoretic questions. When considering, for instance, the members of a family $(\mathbf{G}(\mathbb{F}_p))_{p \text{ prime}}$ of groups of $\mathbb{F}_p$-rational points of a unipotent group scheme $\mathbf{G}$, it is of interest to understand the interplay between properties of the abstract groups $\mathbf{G}(\mathbb{F}_p)$ with the structure of the group scheme $\mathbf{G}$. Specifically, geometric insights into the automorphism group $\mathrm{Aut}(\mathbf{G})$ of $\mathbf{G}$ translate into uniform statements about the automorphism groups $\mathrm{Aut}(\mathbf{G}(\mathbb{F}_p))$.

In this paper we use this approach to compute the orders of the automorphism groups of groups and Lie algebras $\mathbf{G}_{\mathrm{B}}(F)$ resp. $\mathfrak{g}_{\mathrm{B}}(F)$ defined in terms of a matrix of linear forms B, where F is a finite field of odd characteristic. In the case that B is a Hessian determinantal representation of an elliptic curve, we give an explicit formula for $|\mathrm{Aut}(\mathfrak{g}_{\mathrm{B}}(F))|$; up to a scalar, this formula also gives $|\mathrm{Aut}(\mathbf{G}_{\mathrm{B}}(F))|$. We consequently apply this result to a parametrized family of elliptic curves and interpret this formula in terms of arithmetic invariants of the relevant curves; cf. Theorem 1.4. Notwithstanding the fact that our main results are formulated for finite fields, the underpinning structural analysis applies to a larger class of fields, potentially even more general rings.

The following theorem is a condensed summary of the main results of this paper. Throughout we denote, given an elliptic curve E and $n \in \mathbb{N}$, by $E[n]$ the n-torsion points of E.

Theorem 1.1 *Let E be an elliptic curve over $\mathbb{Q}$ and let F be a finite field of odd characteristic p over which E has good reduction. Write, moreover, $\mathrm{Aut}_O(E)$ for the automorphism group of the elliptic curve E and assume that $|E[2](F)| = 4$. Then there exist groups $\mathbf{G}_1(F)$, $\mathbf{G}_2(F)$, and $\mathbf{G}_3(F)$ such that the following hold:*

(1) each $\mathbf{G}_i(F)$ is a group of order $|F|^9$, exponent p, and nilpotency class 2;
(2) for each $i = 1, 2, 3$, there exists $T_i \leq E \rtimes \mathrm{Aut}_O(E)$ such that

$$|\mathrm{Aut}(\mathbf{G}_i(F))| = |F|^{18} \cdot |\mathrm{GL}_2(F)| \cdot |T_i(F)| \cdot |\mathrm{Gal}(F/\mathbb{F}_p)|.$$

Moreover, if $\delta \in F \setminus \{0\}$ is such that $E = E_\delta$ is given by $y^2 = x^3 - \delta x$ over F, then

$$|T_i(F)| = |E_\delta[3](F)| \cdot \gcd(|F| - 1, [\lceil 4/i \rceil])$$

and, for $i \neq j$, the groups $\mathbf{G}_i(F)$ and $\mathbf{G}_j(F)$ are isomorphic if and only if $\{i, j\} = \{2, 3\}$ and $p \equiv 1 \bmod 4$. Any two groups associated with distinct values of δ are non-isomorphic.

We remark that, at least apart from characteristic 3, Theorem 1.1 covers all elliptic curves over $\mathbb{Q}$ with j-invariant 1728. It also implies that, for certain values of δ, the function

$$p \mapsto |\mathrm{Aut}(\mathbf{G}_i(\mathbb{F}_p))|$$

is polynomial on Frobenius sets of primes; see Sect. 1.5.2 for definitions and details.

In the remainder of the introduction we progressively illustrate some of the paper's ideas. These include explicit constructions, motivation, and broader context. We will prove Theorem 1.1 in Sect. 5.2.

1.1 A Hessian determinantal representation

Let y_1, y_2, and y_3 be independent variables and define the polynomial

$$f_1(y_1, y_2, y_3) = y_1^3 - y_1 y_3^2 - y_2^2 y_3 \in \mathbb{Z}[y_1, y_2, y_3]. \tag{1.1}$$

The *Hessian* (*polynomial*) $\mathrm{Hes}(f_1)$ of f_1 is the determinant $\det(\mathrm{H}(f_1))$ of the *Hessian matrix* $\mathrm{H}(f_1) = \left(\frac{\partial^2 f_1}{\partial y_i \partial y_j}\right)_{ij} \in \mathrm{Mat}_3(\mathbb{Z}[y_1, y_2, y_3])$ associated with f_1. The Hessian matrix of $\mathrm{Hes}(f_1)$, in turn, gives

$$\mathrm{B}_{1,1}(y_1, y_2, y_3) \stackrel{\mathrm{def}}{=} \frac{\mathrm{H}(\mathrm{Hes}(f_1))}{48} = \begin{pmatrix} y_3 & -y_2 & y_1 \\ -y_2 & -y_1 & 0 \\ y_1 & 0 & y_3 \end{pmatrix} \in \mathrm{Mat}_3(\mathbb{Z}[y_1, y_2, y_3]). \tag{1.2}$$

We note that the equation

$$48^3 f_1 = \mathrm{Hes}(\mathrm{Hes}(f_1)) = 48^3 \det(\mathrm{B}_{1,1}) \tag{1.3}$$

is satisfied. The matrix $\mathrm{B}_{1,1}$ is thus a *linear symmetric determinantal representation* of the polynomial f_1.

1.2 Finite *p*-groups from matrices of linear forms

For every prime p, the representation (1.2) gives rise to a finite p-group $\mathbf{G}_{1,1}(\mathbb{F}_p)$ via the following presentation:

$$\begin{aligned} \mathbf{G}_{1,1}(\mathbb{F}_p) = \langle e_1, e_2, e_3, f_1, f_2, f_3, g_1, g_2, g_3 \mid \\ & \text{class 2, exponent } p, \langle e_1, e_2, e_3\rangle \text{ and } \langle f_1, f_2, f_3\rangle \text{ abelian}, \\ & [e_1, f_1] = [e_3, f_3] = g_3, \; [e_1, f_2] = [e_2, f_1] = g_2^{-1}, \\ & [e_1, f_3] = [e_2, f_2]^{-1} = [e_3, f_1] = g_1, \; [e_2, f_3] = [e_3, f_2] = 1, \rangle. \end{aligned} \tag{1.4}$$

Indeed, the group relations $[e_1, f_3] = [e_2, f_2]^{-1} = [e_3, f_1] = g_1$ reflect the linear relations $b_{13} = -b_{22} = b_{31} = y_1$ among the entries of the matrix $\mathrm{B}_{1,1} = (b_{ij})$; the group relation $[e_2, f_3] = 1$ reflects the linear relation $b_{23} = 0$ etc. (This ad-hoc definition is a special case of a general construction recalled in Sect. 2.2.) If p is odd, then $\mathbf{G}_{1,1}(\mathbb{F}_p)$ is a group of order p^9, exponent p, and nilpotency class 2.

In [9], du Sautoy and Vaughan-Lee computed the orders of the automorphism groups of the groups $\mathbf{G}_{1,1}(\mathbb{F}_p)$, for primes $p > 3$. This was a major step towards their aim of showing that the numbers of immediate descendants of these groups of order p^{10} and exponent p are not a PORC-function of the primes; see Theorem 1.2 and Sects. 1.5.2

and 1.5.3. (The groups G_p defined in [9] can easily be seen to be isomorphic to the groups $\mathbf{G}_{1,1}(\mathbb{F}_p)$.) The purpose of the present paper is twofold: first, to generalize these computations to a larger class of groups (or rather, group schemes); second, to give a conceptual interpretation of the computations in [9] in terms of Hessian matrices and torsion points of elliptic curves. We reach both aims in Theorem 1.4.

As we now explain, Theorem 1.4 provides new insight, even where it reproduces old results. To see this, note that $f_1 = \det(\mathrm{B}_{1,1})$ defines the elliptic curve

$$E_1 : \; y^2 = x^3 - x$$

over $\mathbb{Q}$. Recall that we denote, given an elliptic curve E over a field F, by $E[3]$ the group of 3-torsion points of E. The collection of its F-rational points $E[3](F)$ is then isomorphic to a subgroup of $\mathbb{Z}/(3) \times \mathbb{Z}/(3)$. The following is a special case of our Theorem 1.4.

Theorem 1.2 (du Sautoy–Vaughan-Lee). *Assume that $p > 3$. Then the following holds:*

$$|\operatorname{Aut}(\mathbf{G}_{1,1}(\mathbb{F}_p))| = \gcd(p-1, 4)\, |\mathrm{GL}_2(\mathbb{F}_p)| p^{18} \cdot |E_1[3](\mathbb{F}_p)|.$$

We write μ_4 for the group scheme of 4th roots of unity. We remark that the factor

$$\gcd(p-1, 4) = |\mu_4(\mathbb{F}_p)| = 3 + \left(\frac{-1}{p}\right) \in \{2, 4\}$$

depends only on the equivalence class of p modulo 4. In stark contrast, it follows from the analysis of [9] that

$$|E_1[3](\mathbb{F}_p)| = \begin{cases} 9, & \text{if } p \equiv 1 \bmod 12 \text{ and there exist solutions in } \mathbb{F}_p \times \mathbb{F}_p \\ & \text{to } y^2 = x^3 - x \text{ and } x^4 + 6x^2 - 3 = 0, \\ 3, & \text{if } p \equiv -1 \bmod 12, \\ 1, & \text{otherwise.} \end{cases} \tag{1.5}$$

This case distinction is not constant on primes with fixed residue class modulo any modulus. A concise, explicit description of $|\operatorname{Aut}(\mathbf{G}_{1,1}(\mathbb{F}_p))|$, which is implicit in [9], is given in [28, Sec. 5.2]. Via our Lemma 3.10, one can recover (1.5) from it. In fact, (1.5) uses du Sautoy and Vaughan-Lee's formulation in terms of the solvability of the quartic $x^4 + 6x^2 - 3$ among the $\mathbb{F}_p$-rational points of E_1. One of the main contributions of the present article is to connect this condition with the structure of the group of 3-torsion points of E_1, affording an arithmetic interpretation. We remark that the 3-torsion points of E_1 are exactly the flex points of E_1, i.e. the points which also annihilate $\mathrm{Hes}(f_1) = 8(y_3^3 + 3y_1^2 y_3 - 3y_1 y_2^2)$; see Lemma 3.7.

1.3 Generalization 1: further Hessian representations

Our first generalization of Theorem 1.2 is owed to the fact that the Hessian matrix $\mathrm{B}_{1,1}$ in (1.2) has two natural “siblings”.

Indeed, let $f \in \mathbb{C}[y_1, y_2, y_3]$ be a homogeneous cubic polynomial defining a smooth projective curve. It is a well-known algebro-geometric fact that the *Hessian equation*

$$\alpha f = \mathrm{Hes}(\beta f + \mathrm{Hes}(f)) \tag{1.6}$$

has exactly three solutions $(\alpha, \beta) \in \mathbb{C}^2$, yielding pairwise inequivalent linear symmetric determinantal representations of f over $\mathbb{C}$; see also Sect. 1.4. In fact, *any* linear symmetric representation of f is equivalent to one arising in this way. For modern accounts of this classical construction, which is presumably due to Hesse [15], see, for instance, [21, Prop. 5], [5, Sec. 5], and [14, Ch. II.2].

One of the three solutions of the Hessian equation for the specific polynomial $f = f_1$ defined in (1.1) is $(\alpha, \beta) = (48^3, 0)$; cf. (1.3). A short computation yields the two others, viz. $(\alpha, \beta) = (4(48)^3, \pm 24)$. This leads us to complement (1.2) as follows:

$$\begin{aligned}
\mathrm{B}_{1,1}(\mathbf{y}) &\overset{\text{def}}{=} \frac{\mathrm{H}(\mathrm{Hes}(f_1))}{48} = \begin{pmatrix} y_3 & -y_2 & y_1 \\ -y_2 & -y_1 & 0 \\ y_1 & 0 & y_3 \end{pmatrix}, \\
\mathrm{B}_{2,1}(\mathbf{y}) &\overset{\text{def}}{=} \frac{\mathrm{H}(+24 f_1 + \mathrm{Hes}(f_1))}{48} = \begin{pmatrix} 3y_1 + y_3 & -y_2 & y_1 - y_3 \\ -y_2 & -y_1 - y_3 & -y_2 \\ y_1 - y_3 & -y_2 & -y_1 + y_3 \end{pmatrix}, \\
\mathrm{B}_{3,1}(\mathbf{y}) &\overset{\text{def}}{=} \frac{\mathrm{H}(-24 f_1 + \mathrm{Hes}(f_1))}{48} = \begin{pmatrix} -3y_1 + y_3 & -y_2 & y_1 + y_3 \\ -y_2 & -y_1 + y_3 & y_2 \\ y_1 + y_3 & y_2 & y_1 + y_3 \end{pmatrix}.
\end{aligned} \tag{1.7}$$

The identities $4f_1 = 4\det(\mathrm{B}_{1,1}) = \det(\mathrm{B}_{2,1}) = \det(\mathrm{B}_{3,1})$ are easily verified. Straightforward generalizations of the presentation (1.4) yield, for every odd prime p, groups $\mathbf{G}_{i,1}(\mathbb{F}_p)$ of order p^9, exponent p, and nilpotency class 2. The following generalizes Theorem 1.2.

Theorem 1.3 *Assume that p is odd and let $i \in \{1, 2, 3\}$. Then the following holds:*

$$|\operatorname{Aut}(\mathbf{G}_{i,1}(\mathbb{F}_p))| = \gcd(p-1, \lceil 4/i \rceil)\, |\mathrm{GL}_2(\mathbb{F}_p)| p^{18} \cdot |E_1[3](\mathbb{F}_p)|.$$

Note that the factor $\gcd(p-1, \lceil 4/i \rceil)$ is constant equal to 2 for $i \in \{2, 3\}$. That the cases $i = 1, 2, 3$ are not entirely symmetric suggests a corresponding asymmetry in the three solutions to the Hessian equation (1.6). The geometric fact ([23, Thm. 1(1)]) that they correspond to the nontrivial 2-torsion points of E_1 may help to shed light on this phenomenon.

1.4 Generalization 2: base extension and families of elliptic curves

We generalize Theorem 1.2 further, simultaneously in two directions. To this end, let δ be a nonzero integer and define

$$f_\delta(y_1, y_2, y_3) = y_1^3 - \delta y_1 y_3^2 - \delta y_2^2 y_3 \in \mathbb{Z}[y_1, y_2, y_3], \tag{1.8}$$

generalizing (1.1). Denoting by $\delta^{\frac{1}{2}}$ a fixed square root of δ, a short computation yields that the Hessian equation (1.6) has the three solutions $((48\delta^2)^3, 0)$ and $(4(48\delta^2)^3, \pm 24\delta^{\frac{3}{2}})$. Generalizing the matrices of linear forms defined in (1.7), we set, in $\mathrm{Mat}_3(\mathbb{Z}_\delta[\delta^{\frac{1}{2}}][y_1, y_2, y_3])$,

$$\mathrm{B}_{1,\delta}(\mathbf{y}) \stackrel{\text{def}}{=} \frac{\mathrm{H}(\mathrm{Hes}(f_\delta))}{48\delta^2} = \begin{pmatrix} y_3 & -y_2 & y_1 \\ -y_2 & -y_1 & 0 \\ y_1 & 0 & \delta y_3 \end{pmatrix},$$

$$\mathrm{B}_{2,\delta}(\mathbf{y}) \stackrel{\text{def}}{=} \frac{\mathrm{H}(+24\delta^{\frac{3}{2}} f_\delta + \mathrm{Hes}(f_\delta))}{48\delta^2} = \begin{pmatrix} 3\delta^{-\frac{1}{2}} y_1 + y_3 & -y_2 & y_1 - \delta^{\frac{1}{2}} y_3 \\ -y_2 & -y_1 - \delta^{\frac{1}{2}} y_3 & -\delta^{\frac{1}{2}} y_2 \\ y_1 - \delta^{\frac{1}{2}} y_3 & -\delta^{\frac{1}{2}} y_2 & -\delta^{\frac{1}{2}} y_1 + \delta y_3 \end{pmatrix},$$

$$\mathrm{B}_{3,\delta}(\mathbf{y}) \stackrel{\text{def}}{=} \frac{\mathrm{H}(-24\delta^{\frac{3}{2}} f_\delta + \mathrm{Hes}(f_\delta))}{48\delta^2} = \begin{pmatrix} -3\delta^{-\frac{1}{2}} y_1 + y_3 & -y_2 & y_1 + \delta^{\frac{1}{2}} y_3 \\ -y_2 & -y_1 + \delta^{\frac{1}{2}} y_3 & \delta^{\frac{1}{2}} y_2 \\ y_1 + \delta^{\frac{1}{2}} y_3 & \delta^{\frac{1}{2}} y_2 & \delta^{\frac{1}{2}} y_1 + \delta y_3 \end{pmatrix}, \tag{1.9}$$

where $\mathbb{Z}_\delta$ denotes the localization of $\mathbb{Z}$ with respect to the δ-powers. The identities $4 f_\delta = 4 \det(\mathrm{B}_{1,\delta}) = \det(\mathrm{B}_{2,\delta}) = \det(\mathrm{B}_{3,\delta})$ are easily verified. Clearly, interchanging $\delta^{\frac{1}{2}}$ with its negative just interchanges $\mathrm{B}_{2,\delta}$ and $\mathrm{B}_{3,\delta}$.

We also avail ourselves of a general, well-known construction—recalled in detail in Sect. 2.2—which associates, in particular, to each of the $\mathrm{B}_{i,\delta}$ a unipotent group scheme $\mathbf{G}_{i,\delta} = \mathbf{G}_{\mathrm{B}_{i,\delta}}$ defined over $\mathbb{Z}_\delta[\delta^{\frac{1}{2}}]$. For a finite field F in which δ is nonzero and has a (fixed) square root, we denote by $\mathbf{G}_{i,\delta}(F)$ the group of F-rational points of $\mathbf{G}_{i,\delta}$. These groups are p-groups of order $|F|^9$ and nilpotency class 2. We also assume for the rest of the paper that the characteristic of F be odd so that they have exponent p. The groups $\mathbf{G}_{i,\delta}(F)$ have a number of alternative descriptions, including one as generalized Heisenberg groups; cf. Sect. 2.4.1. The following is our first main result.

Theorem 1.4 *Let $\delta \in \mathbb{Z}$ and let F be a finite field of characteristic p not dividing 2δ and cardinality p^f in which δ has a fixed square root. For $i \in \{1, 2, 3\}$, the following holds:*

$$|\operatorname{Aut}(\mathbf{G}_{i,\delta}(F))| = f \cdot \gcd\left(|F| - 1, \lceil 4/i \rceil\right) |\mathrm{GL}_2(F)| \cdot |F|^{18} \cdot |E_\delta[3](F)|.$$

Remark 1.5 The quantity $|E_\delta[3](F)|$ equals 1 unless $p = \mathrm{char}(F) \equiv \pm 1 \bmod 12$. Indeed, it enumerates (the curve's point at infinity and) the simultaneous solutions to the equations $b^2 = a^3 - \delta^{-1} a$ and $3\delta^2 a^4 - 6\delta a^2 - 1 = 0$; cf. Lemma 3.7. The biquadratic equation is solvable in F only if its discriminant $48\delta^2$ is a square in F. By quadratic reciprocity, this happens if and only if $p \equiv \pm 1 \bmod 12$. Following the same reasoning as in [9, § 2.2], one can show that $|E_\delta[3](F)| = 3$ if and only if $p \equiv -1 \bmod 12$ and that, if $p \equiv 1 \bmod 12$, then $|E_\delta[3](F)| \in \{1, 9\}$. Describing the fibres of the maps $p \mapsto |E_\delta[3](\mathbb{F}_p)|$ explicitly seems to be, in general, a difficult problem; see also Sect. 1.5.2.

For any $\delta \in \mathbb{Z}\setminus\{0\}$, the matrices $\mathrm{B}_{i,\delta}(\mathbf{y})$ defined in (1.9) are inequivalent in the following geometric sense: for any $i, j \in \{1, 2, 3\}$ with $i \neq j$, there does not exist $U \in \mathrm{GL}_3(\mathbb{C})$ such that $U\mathrm{B}_{i,\delta}U^{\mathrm{T}} = \mathrm{B}_{j,\delta}$; see [21, Prop. 5]. In light of this, it is natural to ask about isomorphisms between groups of the form $\mathbf{G}_{i,\delta}(F)$. The next result settles this question, at least for finite prime fields.

Theorem 1.6 *Let $i, j \in \{1, 2, 3\}$ and let $\delta, \delta' \in \mathbb{Z}\setminus\{0\}$, and assume that p is a prime not dividing $2\delta\delta'$. Then $\mathbf{G}_{i,\delta}(\mathbb{F}_p) \cong \mathbf{G}_{j,\delta'}(\mathbb{F}_p)$ if and only if $\delta = \delta'$ in $\mathbb{F}_p$ and either*

(1) $i = j$ and, if $i \in \{2, 3\}$, then either

- *(1.a) $\delta^{\frac{1}{2}} = \delta'^{\frac{1}{2}}$ or*
- *(1.b) $\delta^{\frac{1}{2}} = -\delta'^{\frac{1}{2}}$ and $p \equiv 1 \bmod 4$ or*

(2) $\{i, j\} = \{2, 3\}$ and either

- *(2.a) $\delta^{\frac{1}{2}} = -\delta'^{\frac{1}{2}}$ or*
- *(2.b) $\delta^{\frac{1}{2}} = \delta'^{\frac{1}{2}}$ and $p \equiv 1 \bmod 4$.*

1.5 Context and related research

1.5.1 Elliptic curves, torsion points, and linear automorphisms

Theorem 1.1 describes the number of automorphisms of a group of the form $\mathbf{G}_{\mathrm{B}}(F)$, in case that the matrix B is a Hessian determinantal representation of an elliptic curve, in terms of the numbers of such automorphisms that induce automorphisms of the elliptic curve; see Sects. 3 and 4 for details. That 3-torsion points of elliptic curves play a role in this context is, at least *a posteriori*, not entirely surprising. Indeed, for $E = E_\delta$, our proof of Theorem 1.1 relies on the realisability of translations by 3-torsion points of the elliptic curve E_δ by elements of $\mathrm{PGL}_3(F)$, viz. $(\mathrm{Aut}\ \mathbb{P}^2)(F)$. We first show that the only translations of E_δ that lift to $\mathrm{PGL}_3(F)$ are those coming from 3-torsion points; see Lemma 3.9. The actual realisability of these as linear transformations is implicit in the proof of Theorem 1.4. A similar phenomenon is discussed in [19, Rem. B]: under suitable assumptions, translations by n-torsion points of genus one curves embedded into $\mathbb{P}^{n-1}$ are induced by linear automorphisms of $\mathbb{P}^{n-1}$. For an elliptic curve with point at infinity O, this translates to the divisor nO being *very ample* and so, in the case of planar elliptic curves, to $3O$ being very ample. We would like to understand whether the theory of divisors can be used also to show that all other translations are not linear.

With a broader outlook, it is of course of interest to consider groups arising from (not necessarily symmetric) determinantal representations of curves or other algebraic varieties. For the time being, however, a general theory connecting geometric invariants of determinantal varieties with algebraic invariants of finite p-groups associated with these varieties' representations eludes us.

1.5.2 Quasipolynomiality vs. polynomiality on Frobenius sets

Let Π denote the set of rational primes. It was shown in [9] that the function $\Pi \to \mathbb{Z}$, $p \mapsto |\operatorname{Aut}(\mathbf{G}_{1,1}(\mathbb{F}_p))|$ is not quasipolynomial (or Polynomial On Residue Classes (PORC)); cf. [26, Sec. 4.4]. Our result Theorem 1.4 has the following consequence.

Corollary 1.7 *Let $i \in \{1, 2, 3\}$ and assume that δ is the fourth power of an integer. Then the function $p \mapsto |\operatorname{Aut}(\mathbf{G}_{i,\delta}(\mathbb{F}_p))|$ is not PORC.*

Similar results hold for general δ if and only if the function $p \mapsto |E_\delta[3](\mathbb{F}_p)|$ is not constant on sets of primes with fixed residue class modulo some integer; cf. (1.5).

Quasipolynomiality is quite a restrictive property for a counting function. Where it fails, it is natural to look for other arithmetically defined patterns in the variation with the primes. Recall, e.g. from [3] or [17], that a set of primes is a *Frobenius set* if it is a finite Boolean combination of sets of primes defined by the solvability of polynomial congruences. A function $f : \Pi \to \mathbb{Z}$ is *Polynomial On Frobenius Sets* (*POFS*) if there exist a positive integer N, Frobenius sets $\Pi_1, \dots, \Pi_N$ partitioning Π, and polynomials $f_1, \dots, f_N \in \mathbb{Z}[T]$ such that the following holds:

$$p \in \Pi_j \iff f(p) = f_j(p).$$

Our Theorem 1.4 implies, for instance, the following.

Corollary 1.8 *Let $i \in \{1, 2, 3\}$ and assume that δ is the square of an integer if $i \neq 1$. Then the function $p \mapsto |\operatorname{Aut}(\mathbf{G}_{i,\delta}(\mathbb{F}_p))|$ is POFS.*

In fact, for $\delta = 1$ one may take $N = 4$ for $i = 1$ and $N = 3$ for $i \in \{2, 3\}$.

Corollary 1.8 invites a comparison of Theorem 1.4 with a result by Bardestani, Mallahi-Karai, and Salmasian. Indeed, [3, Thm. 2.4] establishes—in notation closer to the current paper—that, for a unipotent group scheme $\mathbf{G}$ defined over $\mathbb{Q}$, the faithful dimension of the p-groups $\mathbf{G}(\mathbb{F}_p)$ (viz. the smallest n such that $\mathbf{G}(\mathbb{F}_p)$ embeds into $\mathrm{GL}_n(\mathbb{C})$) defines a POFS function. For a number of recent related quasipolynomiality results, see [10].

1.5.3 Automorphism groups and immediate descendants

Du Sautoy and Vaughan-Lee embedded their discussion of the automorphism groups of the groups $\mathbf{G}_{1,1}(\mathbb{F}_p)$ in a study of the immediate descendants of order p^{10} and exponent p of these groups of order p^9. In fact, their paper's main result is the statement that the numbers of these descendants is not PORC as a function of p. Theorem 1.2 allows us to give a compact, conceptual formula for these numbers. Let $\mathrm{n}_{1,1}(p)$ denote the number of immediate descendants of $\mathbf{G}_{1,1}(\mathbb{F}_p)$ of order p^{10} and exponent p. Set, moreover, $e(p) = |E_1[3](\mathbb{F}_p)|$ and $m(p) = \gcd(p-1, 4)$.

Corollary 1.9 (du Sautoy–Vaughan-Lee). *Assume that $p > 3$. Then the following holds:*

$$\mathrm{n}_{1,1}(p) = \frac{p^2 + p + 2 - m(p) + e(p)(p-5) + 5m(p)e(p)}{m(p)e(p)}.$$

We hope to come back to the interesting question of how to generalize and conceptualize this work to the groups $\mathbf{G}_{i,\delta}(F)$ for $\delta \in \mathbb{Z}\backslash\{0\}$ and $i \in \{1, 2, 3\}$ in a future paper.

1.5.4 Further examples and related work

In [18], Lee constructed an 8-dimensional group scheme $\mathbf{G}$, via a presentation akin to (1.4), and proved a result which is similar to Theorem 1.2. In particular, he showed that both the orders of $\mathrm{Aut}(\mathbf{G}(\mathbb{F}_p))$ and the numbers of immediate descendants of $\mathbf{G}(\mathbb{F}_p)$ of order p^9 and exponent p vary with p in a nonquasipolynomial way. More precisely, these numbers depend on the splitting behaviour of the polynomial $x^3 - 2$ over $\mathbb{F}_p$ or, equivalently, on the realisability over $\mathbb{F}_p$ of permutations of 3 specific, globally defined points in $\mathbb{P}^1$.

In [29], Vaughan-Lee proved a similar result about p-groups arising from a parametrized family of 7-dimensional unipotent group schemes of nilpotency class 3. He proved that the orders of the automorphism groups of these p-groups, which feature two integral parameters x and y, depend on the splitting behaviour modulo p of the polynomial $t^3 - xt - y \in \mathbb{Z}[t]$.

It is natural to try and further expand the range of computations of automorphisms of p-groups obtained as F-points of finite-dimensional unipotent group schemes, where F is a finite field.

Arithmetic properties of finite p-groups arising as groups of F-rational points of group schemes defined in terms of matrices of linear forms are also a common theme of [2,20,22,24] (with a view towards the enumeration of conjugacy classes) and [3] (with a view towards faithful dimensions; cf. also Sect. 1.5.2).

Slight variations of the group schemes $\mathbf{G}_{1,\delta}$ were highlighted by du Sautoy in the study of the (normal) subgroup growth of the groups of $\mathbb{Z}$-rational points of these group schemes. Indeed, he showed in [8] that the local normal zeta functions of these finitely generated torsion-free nilpotent groups depend essentially on the numbers of $\mathbb{F}_p$-rational points of the reductions of the curves E_δ modulo p; see also [30,31] for explicit formulae and generalizations.

The groups we consider arise via a general construction of nilpotent groups and Lie algebras from symmetric forms. Automorphism groups of such groups and algebras have been studied, e.g. in [4,12,33]. In fact, our Theorem 1.4 may be seen as an explicit version of [12, Thm. 7.2] and [33, Thm. 9.4]. The arithmetic point of view taken in the current paper seems to be new, however.

1.6 Organization and notation

The paper is structured as follows. In Sect. 2 we recall the well-known general construction yielding the nilpotent groups and Lie algebras considered in this paper and set up the notation that will be used throughout the paper. In Sect. 3 we gather some elementary results about automorphisms of elliptic curves. In Sect. 4 we collect a number of structural results of the groups in question necessary to determine their automorphism groups. We apply these, in combination with the results of the previous sections, to give a proof of the paper's main results and their corollaries in Sect. 5.

The notation we use is mainly standard. Throughout, k denotes a number field, with ring of integers $\mathcal{O}_k$. The localization of $\mathcal{O}_k$ with respect to the powers of $\delta \in \mathbb{Z}$ is denoted by $R = \mathcal{O}_{k,\delta}$. By K we denote a field with an R-algebra structure, in practice nearly always an extension of k or a residue field of a nonzero prime ideal of $\mathcal{O}_k$. By F we denote a finite field.

2 Groups and Lie algebras from (symmetric) forms

In this section we work with groups and Lie algebras arising from symmetric matrices of linear forms via a classical construction which we review in Sects. 2.1 and 2.2. Our reasons to restrict our attention to symmetric matrices, rather than discuss more general settings, will become apparent in Sect. 2.3; see also Remark 2.1.

2.1 Global setup

The following is the setup for the whole paper. Let k be a number field with ring of integers $\mathcal{O}_k$. For a nonzero integer δ, we write $R = \mathcal{O}_{k,\delta}$ for the localization of $\mathcal{O}_k$ at the set of δ-powers. Let further d be a positive integer and let U, W, and T be free R-modules of rank d. Let $\mathbf{y} = (y_1, \ldots, y_d)$ be a vector of independent variables and let B be a symmetric matrix whose entries are linear homogeneous polynomials (which may be 0) over R, i.e.

$$\mathrm{B}(\mathbf{y}) = \sum_{\kappa=1}^{d} \mathrm{B}^{(\kappa)} y_\kappa \in \mathrm{Mat}_d(R[y_1, \ldots, y_d]) \tag{2.1}$$

for symmetric matrices $\mathrm{B}^{(\kappa)} \in \mathrm{Mat}_d(R)$. Let further $\mathcal{E} = (e_1, \ldots, e_d)$, $\mathcal{F} = (f_1, \ldots, f_d)$, and $\mathcal{T} = (g_1, \ldots, g_d)$ be R-bases of U, W, and T respectively, allowing us to identify each U, W, and T with R^d. Let, moreover,

$$\phi : U \times W \longrightarrow T, \quad (u, w) \longmapsto u\mathrm{B}w^{\mathrm{T}} \overset{\mathrm{def}}{=} u\mathrm{B}(g_1, \ldots, g_d)w^{\mathrm{T}} \tag{2.2}$$

be the R-bilinear map induced by B with respect to the given bases. Throughout we write $\otimes$ to denote $\otimes_R$. We denote by

$$\tilde{\phi} : U \otimes W \longrightarrow T \tag{2.3}$$

the homomorphism that is given by the universal property of tensor products. By slight abuse of notation, we will use the bar notation $\overline{(\text{-})}$ both for the map

$$U \longrightarrow W, \quad u = \sum_{j=1}^{d} u_j e_j \longmapsto \overline{u} = \sum_{j=1}^{d} u_j f_j$$

and its inverse $W \to U$. We remark that the symmetry of B yields, for $u \in U$ and $w \in W$,

$$\phi(u, w) = u\mathrm{B}w^{\mathrm{T}} = (u\mathrm{B}w^{\mathrm{T}})^{\mathrm{T}} = \overline{w}\mathrm{B}\overline{u}^{\mathrm{T}} = \phi(\overline{w}, \overline{u}). \tag{2.4}$$

We write

$$V = U \oplus W \text{ and } \mathrm{L} = V \oplus T$$

for the free R-modules of ranks $2d$ respectively $3d$. Our notation will reflect that we consider the summands of these direct sums as subsets.
Throughout, K is a field with an R-algebra structure. (In practice, K may be, for instance, an extension of the number field k or one of various residue fields of nonzero prime ideals of $\mathcal{O}_k$ coprime to δ.) By slight abuse of notation we use, in the sequel, the above R-linear notation also for the corresponding K-linear objects obtained from taking tensor products over R. For example, L will also denote the K-vector space $\mathrm{L} \otimes_R K$.

2.2 Groups and Lie algebras

The data (K, B, ϕ) gives the K-vector space L a group structure. Indeed, with

$$\star : \mathrm{L} \times \mathrm{L} \to \mathrm{L}$$
$$((u, w, t), (u', w', t')) \mapsto (u, w, t)\star(u', w', t') = (u + u', w + w', t + t' + \phi(u, w')),$$

the pair $\mathbf{G}_{\mathrm{B}}(K) = (\mathrm{L}, \star)$ is a nilpotent group of class at most 2, viz. the group of K-rational points of an R-defined group scheme $\mathbf{G}_{\mathrm{B}}$ (abelian if and only if $\mathrm{B} = 0$.) It is not difficult to show that in $\mathbf{G}_{\mathrm{B}}(K)$

(1) the identity element is $(0, 0, 0)$,
(2) the inverse of the element (u, w, t) is $(u, w, t)^{-1} = (-u, -w, -t + \phi(u, w))$,
(3) the commutator of any two elements (u, w, t) and (u', w', t') is

$$[(u, w, t), (u', w', t')] = \phi(u, w') - \phi(u', w). \tag{2.5}$$

The data (K, B, ϕ) also endows L with the structure of a graded K-Lie algebra. Indeed, with

$$[\,,\,] : \mathrm{L} \times \mathrm{L} \to \mathrm{L}$$
$$((u, w, t), (u', w', t')) \mapsto [(u, w, t), (u', w', t')] = \phi(u, w') - \phi(u', w), \tag{2.6}$$

the pair $\mathfrak{g}_{\mathrm{B}}(K) = (\mathrm{L}, [\,,\,])$ is a nilpotent K-Lie algebra of nilpotency class at most two, viz. the K-rational points of an R-defined Lie algebra scheme $\mathfrak{g}_{\mathrm{B}}$ (abelian if and only if $\mathrm{B} = 0$). Note that the Lie bracket (2.6) coincides with the group commutator (2.5).

Remark 2.1 The property of B being symmetric is not an isomorphism invariant of $\mathbf{G}_{\mathrm{B}}(K)$. Indeed, linear changes of coordinates on U and W preserve the isomorphism type of $\mathbf{G}_{\mathrm{B}}(K)$ but result in a transformation $\mathrm{B} \mapsto P^{\mathrm{T}}\mathrm{B}Q$ for some $P, Q \in \mathrm{GL}_d(K)$. For computations, however, the symmetric setting proved much more conventient to work with. Clearly, symmetric coordinate changes (i.e. $P = Q$) preserve the matrix's symmetry.

We focus on groups $\mathbf{G}_{\mathrm{B}}(K)$ where B is a symmetric 3×3 determinantal representation of a planar elliptic curve E. As discussed in Sect. 1.3, there are, over the algebraic closure of K, three inequivalent such representations $\mathrm{B}_1, \mathrm{B}_2, \mathrm{B}_3$, where *inequivalent* means that they belong to three distinct orbits under the standard action of $\mathrm{GL}_3(K)^2$ on 3×3 matrices of linear forms. In particular, equivalent representations yield isomorphic groups, but, as our Theorem 1.6 shows, inequivalent representations might yield isomorphic groups.

In the case that $K = F$ is a finite field of odd characteristic p, the groups $\mathbf{G}_{\mathrm{B}}(F)$ are the finite p-groups associated with the Lie algebras $\mathfrak{g}_{\mathrm{B}}(F)$ by means of the classical Baer correspondence ([1]). It was anticipated, in the case at hand, in Brahana's work ([6]) and extended in the much more general (and better known) Lazard correspondence; [16, Exa. 10.24]. It implies, in particular, that $|\operatorname{Aut}(\mathbf{G}_{\mathrm{B}}(\mathbb{F}_p))| = |\operatorname{Aut}(\mathfrak{g}_{\mathrm{B}}(\mathbb{F}_p))|$ and, more generally, that $|\operatorname{Aut}(\mathbf{G}_{\mathrm{B}}(F))| = |\operatorname{Aut}_{\mathbb{F}_p}(\mathfrak{g}_{\mathrm{B}}(F))|$, where $\operatorname{Aut}_{\mathbb{F}_p}(\mathfrak{g}_{\mathrm{B}}(F))$ denotes the automorphisms of $\mathfrak{g}_{\mathrm{B}}(F)$ as $\mathbb{F}_p$-Lie algebra.

To lighten notation we will, in the sequel, not always notationally distinguish between the K-Lie algebra scheme $\mathfrak{g} = \mathfrak{g}_{\mathrm{B}}$ and its K-rational points. We trust that the respective contexts will prevent misunderstandings.

2.3 Groups of Lie algebra automorphisms

By $\operatorname{Aut}_K(\mathfrak{g}) = \operatorname{Aut}(\mathfrak{g})$ we denote the automorphism group of the K-Lie algebra $\mathfrak{g}$. Define, additionally,

$$\begin{aligned}
\operatorname{Aut}_V(\mathfrak{g}) &= \{\alpha \in \operatorname{Aut}(\mathfrak{g}) \mid \alpha(V) = V\},\\
\operatorname{Aut}_V^{\mathrm{f}}(\mathfrak{g}) &= \{\alpha \in \operatorname{Aut}_V(\mathfrak{g}) \mid \alpha(U) = U,\ \alpha(W) = W\},\\
\operatorname{Aut}_V^{=}(\mathfrak{g}) &= \{\alpha \in \operatorname{Aut}_V^{\mathrm{f}}(\mathfrak{g}) \mid \forall u \in U : \alpha(\overline{u}) = \overline{\alpha(u)}\}.
\end{aligned}$$

We remark that $\operatorname{Aut}_V(\mathfrak{g})$ is nothing but the centralizer $\mathrm{C}_{\operatorname{Aut}(\mathfrak{g})}(V)$ considered with respect to the action of $\operatorname{Aut}(\mathfrak{g})$ on the Grassmannian of L. Our choice of bases allows us to identify $\operatorname{Aut}(\mathfrak{g})$ with a subgroup of $\mathrm{GL}_{3d}(K)$. We may thus view each element α of $\operatorname{Aut}(\mathfrak{g})$ as a matrix of the form

$$\alpha = \begin{pmatrix} A_U & A_{WU} & 0 \\ A_{UW} & A_W & 0 \\ C & D & A_T \end{pmatrix} \in \mathrm{GL}_{3d}(K), \tag{2.7}$$

where $A_U, A_{WU}, A_{UW}, A_W, C, D, A_T$ are elements of $\mathrm{Mat}_d(K)$. The subgroup $\operatorname{Aut}_V(\mathfrak{g})$ of $\operatorname{Aut}(\mathfrak{g})$ comprises those matrices with entries $C = D = 0$ in (2.7). It is easy to show that

$$\mathrm{Aut}(\mathfrak{g}) = \mathrm{Hom}_K(V, T) \rtimes \mathrm{Aut}_V(\mathfrak{g}) \cong K^{2d^2} \rtimes \mathrm{Aut}_V(\mathfrak{g}). \tag{2.8}$$

We also observe that every element of $\mathrm{Aut}_V^{\mathrm{f}}(\mathfrak{g})$ is of the form

$$\mathrm{diag}(A_U, A_W, A_T) = \begin{pmatrix} A_U & 0 & 0 \\ 0 & A_W & 0 \\ 0 & 0 & A_T \end{pmatrix}$$

and belongs to $\mathrm{Aut}_V^{=}(\mathfrak{g})$ if and only if, in addition, $A_U = A_W$.
We define the map $\psi : \mathrm{GL}_2(K) \to \mathrm{Aut}(\mathfrak{g})$ by

$$M = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mapsto \psi(M) = ((u, w, t) \mapsto (au + b\overline{w}, c\overline{u} + dw, (ad - bc)t)).$$

Lemma 2.2 *The map ψ is an injective homomorphism of groups.*

Proof We show that ψ is well-defined. Addition in the Lie algebra is clearly respected, so it suffices to show that the Lie brackets are respected, too. Let (u, w, t) and (u', w', t') in $\mathfrak{g}$ and let $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}_2(K)$. Set $\Delta = \det(M)$. Equation (2.4) then implies the identities

$$\begin{aligned}
[\psi(M)(u, w, t), \psi(M)(u', w', t')] &= [(au + b\overline{w}, c\overline{u} + dw, \Delta t), (au' + b\overline{w'}, c\overline{u'} + dw', \Delta t')] \\
&= \phi(au + b\overline{w}, c\overline{u'} + dw') - \phi(au' + b\overline{w'}, c\overline{u} + dw) \\
&= ad\phi(u, w') + bc\phi(\overline{w}, \overline{u'}) - ad\phi(u', w) - bc\phi(\overline{w'}, \overline{u}) \\
&= \Delta(\phi(u, w') - \phi(u', w)) \\
&= \psi(M)([(u, w, t), (u', w', t')]).
\end{aligned}$$

To show that ψ is an injective homomorphism is a routine check. □

Let $u, u' \in U$ and let $w \in W$. Then one easily computes

$$\begin{aligned}
[u, u' + w] &= \phi(u, w) - \phi(u', 0) = \phi(u, w) = \phi(\overline{w}, \overline{u}) = \phi(\overline{w}, \overline{u}) - \phi(0, \overline{u'}) \\
&= [\overline{u'} + \overline{w}, \overline{u}] = [\overline{u' + w}, \overline{u}].
\end{aligned}$$

In particular, U is an abelian subalgebra of $\mathfrak{g}$ and, by symmetry, so is W. As a consequence of this fact and Lemma 2.2, for each $M \in \mathrm{GL}_2(K)$, the subspaces $\psi(M)(U)$ and $\psi(M)(W) = \psi\left(M \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\right)(U)$ are 3-dimensional abelian subalgebras of $\mathfrak{g}$ that are contained in V.

Lemma 2.3 *Let A_U and A_W be elements of $\mathrm{GL}_d(K)$ and set $D = A_U A_W^{-1}$. Then the conditions*

(1) there exists $A_T \in \mathrm{GL}_d(K)$ *such that* $\mathrm{diag}(A_U, A_W, A_T) \in \mathrm{Aut}^{\mathrm{f}}_V(\mathfrak{g})$*;*
(2) the equality $D^{\mathrm{T}}\mathrm{B} = \mathrm{B}D$ *holds;*
(3) the subspace $X = \{w + \overline{w}D^{\mathrm{T}} \mid w \in W\}$ *is a complement of* U *in* V *satisfying* $[X, X] = 0$*;*

are related in the following way:

$$(1) \implies (2) \iff (3).$$

Proof (1) $\Rightarrow$ (2): A given element $\gamma \in \mathrm{GL}(T)$ corresponds, via the identification $T \cong K^d$ induced by the basis $\mathcal{T}$, to a matrix $A_T \in \mathrm{GL}_d(K)$. We denote by $\gamma(y_1), \ldots, \gamma(y_d) \in K[y_1, \ldots, y_d]$ the images of the variables $y_1, \ldots, y_d$ under A_T, acting on $K[y_1, \ldots, y_d]$ in the standard way. Writing $\mathrm{B} = \mathrm{B}(y_1, \ldots, y_d)$, we analogously define

$$\mathrm{B}_\gamma = \mathrm{B}(\gamma(y_1), \ldots, \gamma(y_d)) \in \mathrm{Mat}_d(K[y_1, \ldots, y_d]).$$

Given $A_U, A_W \in \mathrm{GL}_d(K)$, the matrix $\mathrm{diag}(A_U, A_W, A_T)$ is an element of $\mathrm{Aut}^{\mathrm{f}}_V(\mathfrak{g})$ if and only if there exists a $\gamma \in \mathrm{GL}(T)$ with $A_U^{\mathrm{T}}\mathrm{B}A_W = \mathrm{B}_\gamma$. As B is symmetric, so is B_γ. Hence

$$A_U^{\mathrm{T}}\mathrm{B}A_W = \mathrm{B}_\gamma \iff A_W^{\mathrm{T}}\mathrm{B}A_U = \mathrm{B}_\gamma$$

and thus $\mathrm{diag}(A_U, A_W, A_T)$ belongs to $\mathrm{Aut}^{\mathrm{f}}_V(\mathfrak{g})$ if and only if so does $\mathrm{diag}(A_W, A_U, A_T)$. Consequently, $\mathrm{diag}(A_U, A_W, A_T)$ belongs to $\mathrm{Aut}^{\mathrm{f}}_V(\mathfrak{g})$ if and only if so is $\mathrm{diag}(A_W^{-1}, A_U^{-1}, A_T^{-1})$. It follows that if the matrix $\mathrm{diag}(A_U, A_W, A_T)$ belongs to $\mathrm{Aut}^{\mathrm{f}}_V(\mathfrak{g})$, then $D^{\mathrm{T}}\mathrm{B} = \mathrm{B}D$ holds.

(2) $\Leftrightarrow$ (3): Clearly X is a complement of U in V. We obtain that X is an abelian subalgebra of $\mathfrak{g}$ if and only if, for any choice of $w, w' \in W$, the element $[w + \overline{w}D^{\mathrm{T}}, w' + \overline{w'}D^{\mathrm{T}}]$ is trivial. This happens if and only if, for all $w, w' \in W$, the following equalities hold:

$$\overline{w'}D^{\mathrm{T}}\mathrm{B}w^{\mathrm{T}} = \overline{w}D^{\mathrm{T}}\mathrm{B}w'^{\mathrm{T}} = (\overline{w}D^{\mathrm{T}}\mathrm{B}w'^{\mathrm{T}})^{\mathrm{T}} = \overline{w'}\mathrm{B}D\overline{w}^{\mathrm{T}}.$$

As a consequence, X is abelian if and only if $D^{\mathrm{T}}\mathrm{B} = \mathrm{B}D$. □

Lemma 2.4 *Assume that all* d*-dimensional abelian subalgebras of* $\mathfrak{g}$ *that are contained in* V *are of the form* $\psi(M)(U)$ *for some* $M \in \mathrm{GL}_2(K)$*. Then the following hold:*

(1) $\mathrm{Aut}_V(\mathfrak{g}) = \psi(\mathrm{GL}_2(K))\,\mathrm{Aut}^{\mathrm{f}}_V(\mathfrak{g})$.
(2) $K^\times \rtimes \mathrm{Aut}^{=}_V(\mathfrak{g}) \cong \mathrm{Aut}^{\mathrm{f}}_V(\mathfrak{g}) \leq \{\mathrm{diag}(\lambda A, A, A_T) \mid \lambda \in K^\times, A, A_T \in \mathrm{GL}_d(K)\}$.
(3) $\psi(\mathrm{GL}_2(K)) \cap \mathrm{Aut}^{\mathrm{f}}_V(\mathfrak{g}) = \{\mathrm{diag}(\lambda\,\mathrm{Id}_d, \nu\,\mathrm{Id}_d, \lambda\nu\,\mathrm{Id}_d) \mid \lambda, \nu \in K^\times\} \cong K^\times \times K^\times$.
(4) If $K = F$ *is a finite field, then*

$$|\,\mathrm{Aut}_V(\mathfrak{g})| = \frac{|\,\mathrm{GL}_2(F)| \cdot |\,\mathrm{Aut}^{\mathrm{f}}_V(\mathfrak{g})|}{(|F|-1)^2} = \frac{|\,\mathrm{GL}_2(F)| \cdot |\,\mathrm{Aut}^{=}_V(\mathfrak{g})|}{|F|-1}.$$

Proof (1): Let $\alpha \in \mathrm{Aut}_V(\mathfrak{g})$. By assumption, there is $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ in $\mathrm{GL}_2(K)$ such that

$$\alpha(U) = \langle ae_i + cf_i \mid i = 1, \ldots, d\rangle \text{ and } \alpha(W) = \langle be_i + df_i \mid i = 1, \ldots, d\rangle.$$

For such an M, the element $\psi(M)^{-1} \circ \alpha$ belongs to $\mathrm{Aut}_V^{\mathrm{f}}(\mathfrak{g})$, equivalently α is an element of $\psi(\mathrm{GL}_2(K))\,\mathrm{Aut}_V^{\mathrm{f}}(\mathfrak{g})$. This shows that $\mathrm{Aut}_V(\mathfrak{g}) \subseteq \psi(\mathrm{GL}_2(K))\,\mathrm{Aut}_V^{\mathrm{f}}(\mathfrak{g})$; the converse inclusion is clear.

(2): Let X be a d-dimensional abelian subalgebra of $\mathfrak{g}$ that is contained in V. It follows from the assumptions that either $X = U$ or there exists $\lambda \in K$ such that

$$X = \{w + \lambda\overline{w} \mid w \in W\}.$$

In other words, the complements of U in V that are also abelian subalgebras of $\mathfrak{g}$ are parametrized by the scalar matrices in $\mathrm{Mat}_d(K)$. Lemma 2.3 yields that, if $\mathrm{diag}(A_U, A_W, A_T)$ is an element of $\mathrm{Aut}_V^{\mathrm{f}}(\mathfrak{g})$, then there exists $\lambda \in K^\times$ such that $A_U = \lambda A_W$. By Lemma 2.2, the subgroup

$$N = \{\mathrm{diag}(\lambda\,\mathrm{Id}_d, \mathrm{Id}_d, \lambda\,\mathrm{Id}_d)\} \cong K^\times$$

of $\mathrm{GL}_{3d}(K)$ is actually a subgroup of $\mathrm{Aut}_V^{\mathrm{f}}(\mathfrak{g})$, which is easily seen to be normal. Moreover, the intersection $N \cap \mathrm{Aut}_V^{=}(\mathfrak{g})$ is trivial, by definition of $\mathrm{Aut}_V = (\mathfrak{g})$.

(4): Follows directly from the definition of $\mathrm{Aut}_V^{\mathrm{f}}(\mathfrak{g})$.

(5): Follows from combining (1), (2), and (3).

□

In order to prove Theorem 1.4 in Sect. 5.1, we will make use of Lemma 2.4 via Proposition 4.10.

Recall that, for any $A \in \mathrm{GL}_d(K)$, the isomorphism $U \times W \to U \times W$, defined by $(u, w) \mapsto (uA^{\mathrm{T}}, wA^{\mathrm{T}})$, induces a unique isomorphism $A \otimes A : U \otimes W \to U \otimes W$. Recall, moreover, the maps ϕ and $\tilde{\phi}$ defined in (2.2) and (2.3), respectively.

Lemma 2.5 *Let $A \in \mathrm{GL}_d(K)$ and assume that the image of ϕ spans T. Then the following are equivalent:*

(1) $(A \otimes A)(\ker\tilde{\phi}) \subseteq \ker\tilde{\phi}$*;*
(2) there exists $A_T \in \mathrm{GL}_d(K)$ such that $\mathrm{diag}(A, A, A_T) \in \mathrm{Aut}(\mathfrak{g})$.

Proof (1) $\Rightarrow$ (2): Assume that $(A \otimes A)(\ker\tilde{\phi}) \subseteq \ker\tilde{\phi}$. Then $A \otimes A$ induces an isomorphism of T in the following way. For $j \in \{1, \ldots, d\}$, choose an element $v_j \in U \otimes W$ such that $\tilde{\phi}(v_j) = g_j$. Define $A_T : T \to T$ to be the K-linear homomorphism that is induced by

$$g_j \mapsto A_T(g_j) = \tilde{\phi}((A \otimes A)v_j)$$

for $j = 1, \ldots, d$. The map A_T is well-defined since $A \otimes A$ stabilizes the kernel of $\tilde{\phi}$. Moreover, the following diagram is commutative.

$$\begin{array}{ccc} U \otimes W & \xrightarrow{\tilde{\phi}} & T \\ {\scriptstyle A\otimes A}\downarrow & & \downarrow{\scriptstyle A_T} \\ U \otimes W & \xrightarrow{\tilde{\phi}} & T \end{array}$$

Since $\tilde{\phi} \circ (A \otimes A)$ is surjective, A_T is surjective and thus an isomorphism. In particular, $\mathrm{diag}(A, A, A_T) : U \oplus W \oplus T \to U \oplus W \oplus T$ is an automorphism of the K-Lie algebra $\mathfrak{g}$.

(2) $\Rightarrow$ (1): Let $u \in U$ and let $w \in W$, which we also regard as elements of $\mathfrak{g}$. Then

$$\begin{aligned} A_T \circ \tilde{\phi}(u \otimes w) &= A_T(\tilde{\phi}(u \otimes w)) = A_T([u, w]) \\ &= [uA^{\mathrm{T}}, wA^{\mathrm{T}}] = \phi(uA^{\mathrm{T}}, wA^{\mathrm{T}}) = \tilde{\phi} \circ (A \otimes A)(u \otimes w) \end{aligned}$$

holds and so we are done. □

Remark 2.6 We exploit the symmetry of B, for example, in the following way. Let $v = \sum_{i,j=1}^{d} a_{ij} e_i \otimes f_j$ be an element of $U \otimes W$ and set $C = A^{\mathrm{T}}\mathrm{B}A$, which is by definition a symmetric matrix. Then we have the identities

$$\begin{aligned} \tilde{\phi}((A \otimes A)(v)) = \tilde{\phi}\left(\sum_{i,j=1}^{d} a_{ij}(e_i A^{\mathrm{T}}) \otimes (f_j A^{\mathrm{T}})\right) &= \sum_{i,j=1}^{d} a_{ij}\tilde{\phi}\left((e_i A^{\mathrm{T}}) \otimes (f_j A^{\mathrm{T}})\right) \\ = \sum_{i,j=1}^{d} a_{ij}\phi\left((e_i A^{\mathrm{T}}), (f_j A^{\mathrm{T}})\right) &= \sum_{i,j=1}^{d} a_{ij} e_i A^{\mathrm{T}}\mathrm{B}A f_j^{\mathrm{T}} \\ = \sum_{i,j=1}^{d} a_{ij} e_i C f_j^{\mathrm{T}}. \end{aligned}$$

After defining the "dual" element v^* of v as $v^* = \sum_{i,j=1}^{d} a_{ij} e_j \otimes f_i$, they entail the identity $\tilde{\phi}((A \otimes A)(v)) = \tilde{\phi}((A \otimes A)(v^*))$. We will put this to use in Sect. 5.1.

2.4 Alternative descriptions

The groups $\mathbf{G}_{\mathrm{B}}(K)$ defined in Sect. 2.2 have alternative descriptions as follows.

2.4.1 Heisenberg groups

Let $\mathbf{H}$ be the group scheme of upper unitriangular 3×3-matrices. Then $\mathbf{G}_{\mathrm{B}}(K)$ is equal to $\mathbf{H}(\mathcal{A})$, where $\mathcal{A} = Kg_1 \oplus \cdots \oplus Kg_d$ is the K-algebra given by setting

$$g_r \cdot g_s = (\mathrm{B}(g_1, \ldots, g_d))_{rs}$$

for $r, s \in \{1, \ldots, d\}$. Note that the algebra $\mathcal{A}$ is commutative (as the matrix B is symmetric) but in general not associative. The group $\mathbf{H}(\mathcal{A})$ is nilpotent of class at most 2, and abelian if and only if $\mathrm{B} = 0$. If $\mathcal{A}$ is associative, then $\mathbf{H}(\mathcal{A})$ is called a *Verardi group*; c.f. [12].

We may recover the Lie algebra $\mathfrak{g}_{\mathrm{B}}(K)$ defined in Sect. 2.2 from the group $\mathbf{G}_{\mathrm{B}}(K)$. Indeed, we find that $\mathfrak{g}_{\mathrm{B}}(K)$ is isomorphic to the graded Lie algebra

$$(\mathbf{G}_{\mathrm{B}}(K)/Z(\mathbf{G}_{\mathrm{B}}(K))) \oplus Z(\mathbf{G}_{\mathrm{B}}(K)),$$

with Lie bracket induced by the commutator in $\mathbf{G}_{\mathrm{B}}(K)$. It is easy to show that this isomorphism induces a dimension-preserving bijection between subalgebras of $\mathfrak{g}_{\mathrm{B}}(K)$ and subgroups of $\mathbf{G}_{\mathrm{B}}(K)$; cf. also [13, Rem. on p. 206]. In view of the identification of the group $\mathbf{G}_{\mathrm{B}}(K)$ with $\mathbf{H}(\mathcal{A})$ we may identify $\mathfrak{g}_{\mathrm{B}}(K)$ with $\mathfrak{h}(\mathcal{A})$, where $\mathfrak{h}$ is the Lie algebra scheme of strict uppertriangular 3×3-matrices.

2.4.2 Alternating hulls of (symmetric) module representations

Specifying (K, B, ϕ) amounts to defining a module representation $\theta^{\bullet} : T^* \to \mathrm{Hom}(W, U^*)$ in the sense of [22, § 2.2], the "bullet dual" of a module representation $\theta : U \to \mathrm{Hom}(W, T)$ as explained in [22, § 4.1]. Here, for an R-module M we write M^* for the usual dual. The group $\mathbf{G}_{\mathrm{B}}(K)$ is isomorphic to the group $\mathsf{G}_{\Lambda(\theta^{\bullet})}(K)$ associated with the alternating hull $\Lambda(\theta^{\bullet})$ of the bullet dual $\theta^{\bullet}$ of θ (see [22, § 7.2]) in [22, § 7.1] and equal to the group $\mathsf{H}_{\theta^{\bullet}}(K)$ defined in [22, § 7.3]. As remarked by Rossmann, this construction also features in [33, § 9.2].

2.4.3 Central extensions and cohomology

The group $\mathbf{G}_{\mathrm{B}}(K)$ is a central extension of the abelian group $V = U \oplus W$ by T and corresponding to the 2-cocycle

$$\phi^V : V \times V \to T, \quad (u + w, u' + w') \longmapsto \phi(u, w')$$

in $\mathrm{Z}^2(V, T)$, where the action of V on T is taken to be trivial. This classical construction can be found, for example, in [7, Ch. IV]. The equivalence classes of central extensions of V by T, in the sense of [7, Ch. IV.1], are in 1-to-1 correspondence with the elements of $\mathrm{H}^2(V, T)$. Equivalence being a stronger notion than isomorphism, the image of ϕ^V in $\mathrm{H}^2(V, T)$ will generally not suffice to determine the isomorphism type of $\mathbf{G}_{\mathrm{B}}(K)$.

3 Automorphisms and torsion points of elliptic curves

3.1 General notation and standard facts

Let K be a field and let E be an elliptic curve over K with point at infinity O. For a positive integer n, we write $E[n]$ for the n-torsion subgroup of E and $E(K)$ resp.

$E[n](K)$ for the K-rational points of E resp. $E[n]$. We define, additionally,

$$\mathrm{Aut}(E) = \{\varphi : E \to E \mid \varphi \text{ automorphism of } E \text{ as projective curve}\},$$

containing as a subgroup the automorphisms of E as elliptic curve, or invertible isogenies,

$$\mathrm{Aut}_O(E) = \{\varphi : E \to E \mid \varphi \in \mathrm{Aut}(E), \varphi(O) = O\};$$

for more information, see for example [25, Chap. III.4]. Except for the notation for the automorphism groups, we will refer to results from and notation used in [25, Chap. III]. We warn the reader that in [25] the notation $\mathrm{Aut}(E)$ denotes what we defined as $\mathrm{Aut}_O(E)$.

In Sect. 3.2 we determine, for specific elliptic curves, which of their endomorphisms are induced by (or lift to) linear transformations of the plane. To this end we define

$$\overline{\mathcal{X}_E} = \{\overline{\varphi} \mid \varphi \in \mathrm{GL}_3(K),\ \overline{\varphi}(E) \subseteq E\} \subseteq \mathrm{PGL}_3(K).$$

We write, additionally, $\overline{\mathrm{c}}_E$ for the natural homomorphism

$$\overline{\mathrm{c}}_E : \overline{\mathcal{X}_E} \longrightarrow \mathrm{Aut}(E), \quad \overline{\varphi} \longmapsto \overline{\varphi}_{|E}.$$

Remark 3.1 Any endomorphism φ of E as a projective curve can be written as a composition $\varphi = \tau \circ \alpha$, where τ is a translation and α is an isogeny $E \to E$. In other words, each element of $\mathrm{Aut}(E)$ can be written as the composition of a translation with an element of $\mathrm{Aut}_O(E)$. There thus exists an isomorphism

$$\mathrm{Aut}(E) \cong E \rtimes \mathrm{Aut}_O(E).$$

For more information see, for example, [25, Exa. III.4.7].

Lemma 3.2 *Assume that K is algebraically closed. Then there exists a subset $\mathcal{U}$ of K^3 of cardinality 4 such that the projective image of $\mathcal{U}$ is contained in $E(K)$ and any 3 elements of $\mathcal{U}$ form a basis of K^3.*

Proof Let $Q_1, \ldots, Q_4 \in E(K)$ be four points of coprime orders $|Q_i|$ with respect to addition in E. Then, for each $(i, j) \in \{1, 2, 3, 4\}^2$, the order $|Q_i + Q_j|$ is the least common multiple of $|Q_i|$ and $|Q_j|$. Hence the definition of the group law implies that no three points of $\{Q_1, Q_2, Q_3, Q_4\}$ lie on the same projective line. Any collection of non-zero lifts of the Q_i to elements of K^3 will do. □

Lemma 3.3 *The map $\overline{\mathrm{c}}_E : \overline{\mathcal{X}_E} \longrightarrow \mathrm{Aut}(E)$ is injective.*

Proof Without loss of generality we assume that K is algebraically closed. Let $\varphi \in \mathrm{GL}_3(K)$ be such that $\overline{\varphi} \in \ker \overline{\mathrm{c}}_E$. Let, moreover, $\tilde{E}$ be the affine variety corresponding to E in K^3. Since φ induces the identity on E, every element of $\tilde{E}(K)$ is an eigenvector of φ. Then, Lemma 3.2 yields not only that φ is diagonalisable, but also that all eigenvectors have the same eigenvalue. In particular, there exists $\lambda \in K^\times$ such that φ equals scalar multiplication by λ and thus $\overline{\varphi}$ is trivial. □

3.2 A parametrized family of elliptic curves

Let $\delta \neq 0$ be an integer, let K be a field of characteristic not dividing 2δ, and let E_δ be the elliptic curve defined over K by

$$y^2 = x^3 - \frac{1}{\delta}x.$$

The projectivisation of E_δ, obtained by setting $z = \delta^{-1}$, is given by

$$x^3 - \delta x z^2 - \delta y^2 z = 0 \tag{3.1}$$

and has point at infinity equal to $O = (0 : 1 : 0)$. The j-invariant of E_δ being equal to 1728, the automorphism group $\mathrm{Aut}_O(E_\delta)$ consists of all maps of the form $(x, y) \mapsto (\omega^2 x + \rho, \omega^3 y)$, where (ω, ρ) satisfies $\omega^4 = 1$ and $\delta\rho^3 = \rho$ with $\rho \neq 0$ only if $\mathrm{char}(K) = 3$; see [25, Thm. III.10.1, Prop. A.1.2]. To lighten the notation, we will write $\mathcal{X}$ for $\mathcal{X}_{E_\delta}$ and $\overline{\mathrm{c}}$ for $\overline{c}_{E_\delta}$.

Lemma 3.4 *Let (ω, ρ) be such that $\omega^4 = 1$ and $\delta\rho^3 = \rho$ with $\rho \neq 0$ only if char$(K) = 3$. Let further $\alpha \in \mathrm{Aut}_O(E_\delta)$ be defined by $(x, y) \mapsto (\omega^2 x + \rho, \omega^3 y)$. Then the matrix*

$$\overline{A} = \begin{pmatrix} \omega^2 & 0 & \rho \\ 0 & \omega^3 & 0 \\ 0 & 0 & 1 \end{pmatrix} \in \mathrm{PGL}_3(K)$$

belongs to $\overline{\mathcal{X}}$ and $\overline{\mathrm{c}}^{-1}(\alpha) = \{\overline{A}\}$.

Proof Proving that $\overline{A}$ induces α is straightforward; uniqueness follows from Lemma 3.3. □

In the next lemma, let $\delta^{\frac{1}{2}}$ be a solution of $X^2 - \delta = 0$ and set $\widetilde{K} = K[\delta^{\frac{1}{2}}]$. Let, moreover,

$$P_1 = (0, 0),\ \ P_2 = (\delta^{\frac{1}{2}}, 0),\ \text{ and } P_3 = (-\delta^{\frac{1}{2}}, 0);$$

these are the nontrivial 2-torsion points of E_δ over $\widetilde{K}$. For a point Q of E_δ we denote, additionally, by τ_Q the translation

$$\tau_Q : E_\delta \to E_\delta, \quad P \mapsto P + Q.$$

As pointed out in Remark 3.1, the map τ_Q is an element of $\mathrm{Aut}(E_\delta)$.

Lemma 3.5 *Let $Q = (a, b)$ be a point of E_δ such that $\tau_Q \in \mathrm{im}\,\overline{c}_\delta$. Then $Q \notin \{P_1, P_2, P_3\}$.*

Proof Let $A \in \mathrm{GL}_3(K)$ be such that $\overline{c}_\delta(\overline{A}) = \tau_Q$. Without loss of generality, assume that $K = \widetilde{K}$. For a contradiction we assume, moreover, that $Q = P_1$; the other cases are analogous. Since P_1 is an element of order 2, we find that

$$\tau_Q(O) = P_1, \quad \tau_Q(P_1) = O, \quad \tau_Q(P_2) = P_3, \quad \text{and} \quad \tau_Q(P_3) = P_2.$$

As a consequence, there exist $\nu, \gamma, \varepsilon \in K^\times$ such that

$$(0,0,1)A^{\mathrm{T}} = \nu(0,1,0), \quad (\delta^{\frac{1}{2}}, 0, \delta^{-1})A^{\mathrm{T}} = \gamma(-\delta^{\frac{1}{2}}, 0, \delta^{-1}), \quad (-\delta^{\frac{1}{2}}, 0, \delta^{-1})A^{\mathrm{T}} \\ = \varepsilon(\delta^{\frac{1}{2}}, 0, \delta^{-1}).$$

It follows that

$$\begin{aligned} 2\nu(0,1,0) &= (0,0,2)A^{\mathrm{T}} = \delta((\delta^{\frac{1}{2}}, 0, \delta^{-1}) + (-\delta^{\frac{1}{2}}, 0, \delta^{-1}))A^{\mathrm{T}} \\ &= \gamma(-\delta^{\frac{3}{2}}, 0, 1) + \varepsilon(\delta^{\frac{3}{2}}, 0, 1) \end{aligned}$$

and therefore $\nu = 0$. Contradiction. □

Lemma 3.6 *Let $Q = (a, b)$ be a point of E_δ such that $\tau_Q \in \operatorname{im} \overline{c}_\delta$. Then $3\delta^2 a^4 - 6\delta a^2 - 1 = 0$.*

Proof Let $A = (a_{ij})_{i,j} \in \mathrm{GL}_3(K)$ be such that $\overline{c}_\delta(\overline{A}) = \tau_Q$. Observe that τ_Q maps the point O to Q and its inverse $-Q$ to O. Moreover, if (x, y) is an element of $E_\delta \backslash \{\pm Q\}$, then

$$\tau_Q((x,y)) = \left(\frac{a_{11}x + a_{12}y + \delta^{-1}a_{13}}{\delta a_{31}x + \delta a_{32}y + a_{33}}, \frac{a_{21}x + a_{22}y + \delta^{-1}a_{23}}{\delta a_{31}x + \delta a_{32}y + a_{33}} \right) \in E_\delta. \tag{3.2}$$

However, using the addition formulas (see e.g. [25, Chap. III.2]) and assuming that $(x, y) \neq \pm Q$, one also gets that

$$\tau_Q((x,y)) = (x', y') = \left(\frac{(b-y)^2 - (a+x)(a-x)^2}{(a-x)^2}, \frac{(y-b)x' - (ay - bx)}{a - x} \right). \tag{3.3}$$

By Lemma 3.5 $Q \notin \{P_1, P_2, P_3\}$, and thus (3.2), (3.3), and the fact that $b^2 = a^3 - \delta^{-1}a$ imply that

$$\begin{aligned} \tau_Q(P_1) &= \left(\frac{\delta^{-1}a_{13}}{a_{33}}, \frac{\delta^{-1}a_{23}}{a_{33}} \right) && = \left(-\frac{1}{\delta a}, \frac{b}{\delta a^2} \right) \\ \tau_Q(P_2) &= \left(\frac{\delta^{\frac{1}{2}}a_{11} + \delta^{-1}a_{13}}{\delta^{\frac{3}{2}}a_{31} + a_{33}}, \frac{\delta^{\frac{1}{2}}a_{21} + \delta^{-1}a_{23}}{\delta^{\frac{3}{2}}a_{31} + a_{33}} \right) && = \left(\frac{\delta^{\frac{1}{2}}a + 1}{\delta a - \delta^{\frac{1}{2}}}, -\frac{2b}{(\delta^{\frac{1}{2}}a - 1)^2} \right) \\ \tau_Q(P_3) &= \left(\frac{-\delta^{\frac{1}{2}}a_{11} + \delta^{-1}a_{23}}{-\delta^{\frac{3}{2}}a_{31} + a_{33}}, \frac{-\delta^{\frac{1}{2}}a_{21} + \delta^{-1}a_{23}}{-\delta^{\frac{3}{2}}a_{31} + a_{33}} \right) && = \left(\frac{1 - \delta^{\frac{1}{2}}a}{\delta^{\frac{1}{2}} + \delta a}, -\frac{2b}{(\delta^{\frac{1}{2}}a + 1)^2} \right). \end{aligned}$$

As a consequence, we are looking to solve the following system of equations:

(E1) $-aa_{13} = a_{33}$,
(E2) $a^2a_{23} = ba_{33}$,
(E3) $(\delta a - \delta^{\frac{1}{2}})(\delta^{\frac{1}{2}}a_{11} + \delta^{-1}a_{13}) = (\delta^{\frac{1}{2}}a + 1)(\delta^{\frac{3}{2}}a_{31} + a_{33})$,
(E4) $(\delta^{\frac{1}{2}}a - 1)^2(\delta^{\frac{1}{2}}a_{21} + \delta^{-1}a_{23}) = -2b(\delta^{\frac{3}{2}}a_{31} + a_{33})$,
(E5) $(\delta a + \delta^{\frac{1}{2}})(-\delta^{\frac{1}{2}}a_{11} + \delta^{-1}a_{13}) = (1 - \delta^{\frac{1}{2}}a)(-\delta^{\frac{3}{2}}a_{31} + a_{33})$,
(E6) $(\delta^{\frac{1}{2}}a + 1)^2(-\delta^{\frac{1}{2}}a_{21} + \delta^{-1}a_{23}) = -2b(-\delta^{\frac{3}{2}}a_{31} + a_{33})$.

Combining (E3) and (E4) one gets

$$-2\delta^{\frac{1}{2}}b(\delta^{\frac{3}{2}}a_{11} + a_{13}) = (\delta a^2 - 1)(\delta^{\frac{3}{2}}a_{21} + a_{23})$$

while combining (E5) and (E6) one gets

$$-2\delta^{\frac{1}{2}}b(-\delta^{\frac{3}{2}}a_{11} + a_{13}) = (1 - \delta a^2)(-\delta^{\frac{3}{2}}a_{21} + a_{23}).$$

From the last two equalities, we derive

(E7) $-2ba_{13} = (\delta a^2 - 1)\delta a_{21}$
(E8) $-2\delta^2 ba_{11} = (\delta a^2 - 1)a_{23}$

Combining (E4) and (E6) one gets

$$\begin{aligned} -2\delta^{\frac{3}{2}}ba_{31} &= (\delta^{\frac{1}{2}}a - 1)^2(\delta^{\frac{1}{2}}a_{21} + \delta^{-1}a_{23}) + 2ba_{33} \\ &= -(\delta^{\frac{1}{2}}a + 1)^2(-\delta^{\frac{1}{2}}a_{21} + \delta^{-1}a_{23}) - 2ba_{33} \end{aligned}$$

from which it follows that

$$2ba_{33} - 2\delta aa_{21} + (\delta a^2 + 1)\delta^{-1}a_{23} = 0.$$

With the use of (E2) for a_{23} and of (E7) and (E1) for a_{21}, one may rewrite this equation as

$$\begin{aligned} 0 &= 2ba_{33} - 2\delta aa_{21} + (\delta a^2 + 1)\delta^{-1}a_{23} = 2ba_{33} - \frac{4ba_{33}}{\delta a^2 - 1} + \frac{(\delta a^2 + 1)ba_{33}}{\delta a^2} \\ &= \frac{ba_{33}}{\delta a^2(\delta a^2 - 1)}(3\delta^2a^4 - 6\delta a^2 - 1). \end{aligned}$$

But ba_{33} is nonzero, since A is invertible and $\pm Q \notin \{P_1, P_2, P_3\}$, and so it follows that $3\delta^2a^4 - 6\delta a^2 - 1 = 0$. □

We now give a geometric interpretation of the quartic polynomial featuring in Lemma 3.6.

Lemma 3.7 *Let $Q = (a, b)$ be an element of E_δ. Then the following are equivalent:*

(1) Q is a 3-torsion point of E_δ;

(2) Q is a flex point of E_δ;
(3) $3\delta^2a^4 - 6\delta a^2 - 1 = 0$.

Proof (1) $\Leftrightarrow$ (2): This is classical; see, for instance, [11, Exe. 5.37].

(2) $\Leftrightarrow$ (3): Let f_δ be as in (1.8). The point $(a, b) \in E_\delta$ is a flex point if and only if it is a solution to

$$0 = \mathrm{Hes}(f_\delta(x, y, \delta^{-1})) = 8(1 - 3\delta^2xy^2 + 3\delta x^2).$$

Using $b^2 = a^3 - \delta^{-1}a$ one easily checks that this holds if and only if $3\delta^2a^4 - 6\delta a^2 - 1 = 0$. □

Proposition 3.8 *The image of* $\overline{\mathrm{c}}$ *is isomorphic to a subgroup of* $E_\delta[3] \rtimes \mathrm{Aut}_O(E_\delta)$.

Proof Combine Remark 3.1 with Lemmas 3.4, 3.6, and 3.7. □

Lemma 3.9 *Let $Q = (a, b)$ be a point of $E_\delta[3]$ and assume that $A \in \mathrm{GL}_3(K)$ is such that $\overline{\mathrm{c}}(\overline{A}) = \tau_Q$. Then there exists $\nu \in K^\times$ such that, up to a scalar,*

$$A = \begin{pmatrix} \delta ab + 2ab\nu & \delta a^2 & -2\delta a^2 b\nu \\ (-3\delta - 2\nu)b^2 & \delta ab & 2\delta ab^2\nu \\ (1 - 2\nu a^2)b & a & 2\delta a^3 b\nu \end{pmatrix}.$$

Proof From the addition formulas we derive

$$\begin{aligned} \tau_Q(O) &= Q = (a : b : \delta^{-1}), \\ \tau_Q((0 : 0 : 1)) &= (-(\delta a)^{-1} : b(\delta a^2)^{-1} : \delta^{-1}), \\ \tau_Q(Q) = [2]Q &= -Q = (a : -b : \delta^{-1}), \\ \tau_Q([2]Q) &= O = (0 : 1 : 0). \end{aligned}$$

Moving to affine coordinates (u_1, u_2, u_3) we may find $\lambda, \nu, \gamma \in K^\times$ such that

$$(0, 1, 0)A^{\mathrm{T}} = \lambda(\delta a, \delta b, 1), \qquad (0, 0, 1)A^{\mathrm{T}} = \nu(-a, b, a^2),$$
$$(\delta a, \delta b, 1)A^{\mathrm{T}} = (\delta a, -\delta b, 1), \qquad (\delta a, -\delta b, 1)A^{\mathrm{T}} = \gamma(0, 1, 0).$$

Since $2\delta b(0, 1, 0) = (\delta a, \delta b, 1) - (\delta a, -\delta b, 1)$, we deduce that

$$\delta a = 2\delta^2 ab\lambda, \quad -\delta b - \gamma = 2\delta^2 b^2\lambda, \quad 1 = 2\delta b\lambda,$$

whence $\gamma = -2\delta b$ and $\gamma\lambda = -1$. Up to a scalar, we may rewrite the above system as

$$(0, 1, 0)A^{\mathrm{T}} = (a(2b)^{-1}, 2^{-1}, (2\delta b)^{-1}), \qquad (0, 0, 1)A^{\mathrm{T}} = \nu(-a, b, a^2),$$
$$(\delta a, \delta b, 1)A^{\mathrm{T}} = (\delta a, -\delta b, 1), \qquad (\delta a, -\delta b, 1)A^{\mathrm{T}} = (0, -2\delta b, 0).$$

This implies that

$$(1,0,0)A^{\mathrm{T}} = \left(\frac{\delta+2\nu}{2\delta}, \frac{(-3\delta-2\nu)b}{2\delta a}, \frac{1-2\nu a^2}{2\delta a}\right).$$

Multiplying A by $2\delta ab$ gives the claim. □

We close this section with an observation in the special case when $\delta = \varepsilon^4$ for some $\varepsilon \in K$. As explained in Sect. 1.2, it is used to establish (1.5). To contextualize this situation, we remark that, when $\delta' \in \mathbb{Z}\backslash\{0\}$ and $6\delta'$ is not divisible by char(K), then the elliptic curves E_δ and $E_{\delta'}$ are isomorphic over K if and only if there exists some $\varepsilon \in K$ such that $\delta = \delta'\varepsilon^4$; cf. [25, Ch. III.1]. Indeed, an isomorphism $E_\delta \to E_{\delta'}$ is given by the invertible isogeny $(x, y) \mapsto (\varepsilon^2 x, \varepsilon^3 y)$.

Lemma 3.10 *Assume that char$(K) \neq 3$ and that $\delta = \varepsilon^4$ for some $\varepsilon \in K$. Define, moreover,*

$$\begin{aligned}
\mathcal{S}_0 &= \{(a,b) \in K^2 \mid b^2 = a^3 - a \text{ and } a^4 + 6a^2 - 3 = 0\},\\
\mathcal{S}_1 &= \{(a,b) \in K^2 \mid b^2 = a^3 - a \text{ and } 3a^4 - 6a^2 - 1 = 0\},\\
\mathcal{S}_{1,\delta} &= \{(a,b) \in K^2 \mid b^2 = a^3 - \delta^{-1}a \text{ and } 3\delta^2 a^4 - 6\delta a^2 - 1 = 0\}.
\end{aligned}$$

Then there exists bijections

$$E_\delta[3](K)\backslash\{O\} \longrightarrow \mathcal{S}_{1,\delta} \longrightarrow \mathcal{S}_1 \longrightarrow \mathcal{S}_0.$$

Proof Lemma 3.7 yields a bijection $E_\delta[3](K)\backslash\{O\} \to \mathcal{S}_{1,\delta}$. A bijection $\mathcal{S}_{1,\delta} \to \mathcal{S}_1$ is given by the restriction of the isogeny $(a, b) \mapsto (\varepsilon^2 a, \varepsilon^3 b)$. For the last arrow note that, with

$$\mathcal{S}_2 = \{(a,b) \in K^2 \mid 1 - a^2 + ab^2 = 0 \text{ and } a^4 + 6a^2 - 3 = 0\}$$

and the fact that char$(K) \neq 3$, the maps

$$\mathcal{S}_1 \longrightarrow \mathcal{S}_2,\ (a,b) \longmapsto \left(-\frac{1}{a}, \frac{b}{a}\right), \text{ and } \mathcal{S}_2 \longrightarrow \mathcal{S}_1,\ (a,b) \longmapsto \left(-\frac{1}{a}, -\frac{b}{a}\right),$$

are well-defined and mutually inverse bijections. The sets $\mathcal{S}_2$ and $\mathcal{S}_0$ are in bijection as, for a fixed element $a \in K$ with $a^3 + 6a^2 - 3 = 0$, we find that $a \neq 0$ and thus the solutions to the equation $b^2 = a^3 - a$ are in bijection with the solutions of the equation $b^2 = \frac{a^2-1}{a}$. □

4 Degeneracy loci and automorphisms of *p*-groups

This section brings together the constructions from Sect. 2 and the facts about automorphisms of elliptic curves from Sect. 3. In the case that the determinant of the matrix of linear forms B determines a elliptic curve E, we define an explicit homomorphism

$$\overline{c}_{\mathrm{B}} : \mathrm{Aut}_{\overline{V}}^{=}(\mathfrak{g}_{\mathrm{B}}) \to \mathrm{Aut}(E).$$

In the case that, in addition, B is a Hessian matrix and F is a finite field of odd characteristic, the current section's main result Corollary 4.14 yields a formula for $|\mathrm{Aut}(\mathfrak{g}_{\mathrm{B}}(F))|$ in terms of the size of the image of $\overline{c}_{\mathrm{B}}$. To prove Theorem 1.4 in Sect. 5.1 we are just left with determining this image size explicitly.

Throughout Sect. 4 we continue to use the notation introduced in Sect. 2.1. Recall, in particular, the definition (2.1) of the matrix of linear forms $\mathrm{B}(\mathbf{y}) \in \mathrm{Mat}_d(R[y_1, \ldots, y_d])$ in terms of "structure constants" $\mathrm{B}_{ij}^{(\kappa)} \in R$.

4.1 Duality, degeneracy loci, and centralizer dimensions

Definition 4.1 Let $\mathbf{x} = (x_1, \ldots, x_d)$ be a vector of algebraically independent variables. The *dual* of $\mathrm{B}(\mathbf{y})$ is defined as

$$\mathrm{B}^{\bullet}(\mathbf{x}) = \left(\sum_{j=1}^{d} \mathrm{B}_{ij}^{(\kappa)} x_j \right)_{i\kappa} \in \mathrm{Mat}_d(R[x_1, \ldots, x_d]).$$

Remark 4.2 The matrices $\mathrm{B}(\mathbf{y})$ and $\mathrm{B}^{\bullet}(\mathbf{x})$ are, in a precise sense, dual to one another. Indeed, as we pointed out in Sect. 2.4.2, the matrix B characterizes a module representation $\theta^{\bullet} : T^* \to \mathrm{Hom}(W, U^*)$. The dual matrix $\mathrm{B}^{\bullet}$ then characterizes the module representation $\theta = (\theta^{\bullet})^{\bullet} : U \to \mathrm{Hom}(W, T)$; see [22, § 4.1] and Definition 4.3. In particular, they satisfy

$$\mathrm{B}^{\bullet}(\mathbf{x})\mathbf{y}^{\mathrm{T}} = \mathrm{B}(\mathbf{y})\mathbf{x}^{\mathrm{T}}. \tag{4.1}$$

The matrices $\mathrm{B}(\mathbf{y})$ and $\mathrm{B}^{\bullet}(\mathbf{x})$ are also closely related to the "commutator matrices" defined in [20, Def. 2.1]. In this paper's notation, we find that, for vectors of algebraically independent variables $\mathbf{Y} = (Y_1, \ldots, Y_d)$ and $\mathbf{X} = (\mathbf{X}_1, \mathbf{X}_2) = (X_1, \ldots, X_d, X_{d+1}, \ldots, X_{2d})$,

$$B(\mathbf{Y}) = \begin{pmatrix} 0 & \mathrm{B}(\mathbf{Y}) \\ -\mathrm{B}(\mathbf{Y}) & 0 \end{pmatrix} \quad \text{and} \quad A(\mathbf{X}) = \begin{pmatrix} \mathrm{B}^{\bullet}(\mathbf{X}_1) \\ -\mathrm{B}^{\bullet}(\mathbf{X}_2) \end{pmatrix}.$$

This is consistent with the descriptions [22, Rem. 7.10] of $B(\mathbf{Y})$ and [22, Rem. 7.6 (ii)] of $A(\mathbf{X})$. The fact that the bottom part of $A(\mathbf{X})$ is, up to a sign, equal to its top part (and not its $\circ$-dual in the sense of [22, § 4.1]) reflects the symmetry of B; see [22, Prop. 4.12].

Definition 4.3 The *left-regular representation* of U is the homomorphism

$$\Phi : U \to \mathrm{Hom}(W, T), \quad u \mapsto \Phi_u : (w \mapsto \phi(u, w)).$$

Lemma 4.4 *Let $u \in U$, $w \in W$, and let $D \in \mathrm{Mat}_d(K)$. Then the following hold:*

(1) $\Phi_u(w) = w\mathrm{B}^\bullet(u)$.
(2) If $D^\mathrm{T}\mathrm{B} = \mathrm{B}D$ *holds, then* D *stabilizes* $\ker \mathrm{B}(u)$.

Proof (1): Straightforward. (2): Let $v \in \ker \mathrm{B}(u)$. Then the assumption implies that $\mathrm{B}(u)Dv^\mathrm{T} = D^\mathrm{T}\mathrm{B}(u)v^\mathrm{T} = 0$. □

We next observe that matrices of linear forms that are, as the ones in (1.9), defined as Hessian matrices, have a remarkable self-duality property.

Lemma 4.5 *Assume that* $d = 3$ *and let* $g(y_1, y_2, y_3) \in R[y_1, y_2, y_3]$ *be a homogeneous cubic polynomial. The* Hessian matrix *of g, viz.*

$$\mathrm{B_g(y) = H(g(y))} = \left(\frac{@\mathrm{g}(\mathbf{y})}{@\mathrm{y_i}@\mathrm{y_j}}\right)_{\mathrm{ij}} \in \mathrm{Mat_3(R[\mathbf{y}])},$$

satisfies

$$\mathrm{B}d_g = \mathrm{B}_g = \mathrm{B}_g^\mathrm{T}.$$

Proof We write $g(\mathbf{y}) = \sum_{\mathbf{e}\in\mathbb{N}_0^3,\, \sum e_i=3} \lambda_\mathbf{e}\mathbf{y}^\mathbf{e}$ and use the shorthand notation (α, β, γ) for the linear form $\alpha y_1 + \beta y_2 + \gamma y_3$. One easily computes

$$\mathrm{B}_g(\mathbf{y}) = \begin{pmatrix} (6\lambda_{300}, 2\lambda_{210}, 2\lambda_{201}) & (2\lambda_{210}, 2\lambda_{120}, \lambda_{111}) & (2\lambda_{201}, \lambda_{111}, 2\lambda_{102}) \\ (2\lambda_{210}, 2\lambda_{120}, \lambda_{111}) & (2\lambda_{120}, 6\lambda_{030}, 2\lambda_{021}) & (\lambda_{111}, 2\lambda_{021}, 2\lambda_{012}) \\ (2\lambda_{201}, \lambda_{111}, 2\lambda_{102}) & (\lambda_{111}, 2\lambda_{021}, 2\lambda_{012}) & (2\lambda_{102}, 2\lambda_{012}, 6\lambda_{003}) \end{pmatrix},$$

from which the claim follows by inspection. □

Definition 4.6 (1) The *affine degeneracy locus of* $\mathrm{B}(\mathbf{y})$ is the closed subscheme $\mathcal{V}_\mathrm{B}$ of $\mathbb{A}^d$ defined by the equation $\det(\mathrm{B}(\mathbf{y})) = 0$. The set

$$\mathcal{V}_\mathrm{B}(U) = \{u \in U \mid \det(\mathrm{B}(u)) = 0\}$$

is the *affine degeneracy locus of* $\mathrm{B}(\mathbf{y})$ *in* U.

(2) The *projective degeneracy locus of* $\mathrm{B}(\mathbf{y})$ is the closed subscheme $\mathbb{P}\mathcal{V}_\mathrm{B}$ of $\mathbb{P}^{d-1}$ defined by the equation $\det(\mathrm{B}(\mathbf{y})) = 0$. The set

$$\mathbb{P}\mathcal{V}_\mathrm{B}(U) = \{u \in \mathbb{P}U \mid \det(\mathrm{B}(u)) = 0\}$$

is the *projective degeneracy locus* $\mathbb{P}\mathcal{V}_\mathrm{B}(U)$ *of* $\mathrm{B}(\mathbf{y})$ *in* U.

Corollary 4.7 (to Lemma 4.5). *Assume that* $d = 3$ *and let* $g(\mathbf{y}) \in R[\mathbf{y}]$ *be a homogeneous cubic polynomial with Hessian matrix* B_g*. Then* $\mathcal{V}_{B_g} = \mathcal{V}_{B_g^\bullet}$.

Lemma 4.8 (cf. [32, Lem. 1]). *Assume that* $\mathbb{P}\mathcal{V}_B$ *is smooth. Then, for* $u \in U$*, the following holds:*

$$\mathrm{rk}\, B(u) = \begin{cases} 0, & \textit{if } u = 0, \\ d-1, & \textit{if } u \in \mathcal{V}_B(U)\backslash\{0\}, \\ d, & \textit{otherwise}. \end{cases}$$

Remark 4.9 Write $v \in V$ as $v = u + w$ with $u \in U$ and $w \in W$. One checks easily that $\mathrm{C}_V(v) = \{v' \in V \mid [v, v'] = 0\}$, the intersection of V with the centralizer $\mathrm{C}_{\mathfrak{g}}(v)$ of v in $\mathfrak{g}$, has K-dimension

$$\dim_K \mathrm{C}_V(v) = 2d - \mathrm{rk}\begin{pmatrix} \mathrm{B}^\bullet(u) \\ -\mathrm{B}^\bullet(w) \end{pmatrix};$$

cf. also Lemma 4.41 and Remark 4.2. In particular, if $v = u$ is an element of U and $\mathbb{P}\mathcal{V}_{\mathrm{B}^\bullet}$ is smooth, then $\dim_K \mathrm{C}_V(u) = 2d - \mathrm{rk}\,\mathrm{B}^\bullet(u)$ and so, by Lemma 4.8, the following holds:

$$\dim_K \mathrm{C}_V(u) = \begin{cases} 2d, & \text{if } u = 0, \\ d+1, & \text{if } u \in \mathcal{V}_{\mathrm{B}^\bullet}(U)\backslash\{0\}, \\ d, & \text{otherwise.} \end{cases} \tag{4.2}$$

If, additionally, $d = 3$ and $\mathrm{B} = \mathrm{B}^\bullet$, as in the situation described in Lemma 4.5, then we find that $\dim_K \mathrm{C}_V(u) = 6 - \mathrm{rk}\,\mathrm{B}(u)$ and hence

$$\dim_K \mathrm{C}_V(u) = \begin{cases} 6, & \text{if } u = 0, \\ 4, & \text{if } u \in \mathcal{V}_{\mathrm{B}}(U)\backslash\{0\}, \\ 3, & \text{otherwise.} \end{cases} \tag{4.3}$$

We remark that this applies, in particular, to the matrices $\mathrm{B}_{i,\delta}$ defined in (1.9)

4.2 Implications for automorphism groups of *p*-groups

For the rest of the section we assume that $d = 3$. We mainly describe, in Proposition 4.10, the 3-dimensional abelian subalgebras of $\mathfrak{g}$ that are contained in V. This allows us to apply Lemma 2.4, leading to a refined formula for $|\mathrm{Aut}(\mathfrak{g}_{\mathrm{B}}(F))|$ in the case that F is a finite field and $\mathbb{P}\mathcal{V}_{\mathrm{B}}$ and $\mathbb{P}\mathcal{V}_{\mathrm{B}^\bullet}$ are elliptic curves; see Corollary 4.14.

Proposition 4.10 *Assume that $\mathbb{P}\mathcal{V}_B$ and $\mathbb{P}\mathcal{V}_{B^\bullet}$ are elliptic curves. Then the 3-dimensional abelian subalgebras of $\mathfrak{g}$ that are contained in V are exactly those of the form $\psi(M)(U)$ for some $M \in \mathrm{GL}_2(K)$.*

Proof Let X be a 3-dimensional abelian subalgebra of $\mathfrak{g}$ that is contained in V. Assume first that $X \cap U \neq \{0\}$. We claim that $X = U$ and assume, for a contradiction, that $X \neq U$. Then there exists $u \in X \cap U$ with centralizer $\mathrm{C}_V(u)$ of dimension at least 4 and such that X is contained in $\mathrm{C}_V(u)$. Then (4.2) implies that $\dim_K \mathrm{C}_V(u) = 4$ or, equivalently, that the kernel of 8_u has dimension 1. Let $w \in W$ be such that $\ker 8_u = Kw$ and define $Y = U \oplus \ker 8_u$ so that Y has dimension 4. Since X and U do not coincide, it follows that $Y = X + U$ and $X \cap U$ has dimension 2. We let $t \in X$ be such that $X = (X \cap U) \oplus Kt$ and denote by $\pi_U : V \to U$ resp. $\pi_W : V \to W$ the natural projections. Since t belongs to Y, we have $\pi_W(t) = \lambda t$ for some $\lambda \in K^\times$. It follows that

$$0 = \phi(X \cap U, t) = \phi(X \cap U, \pi_U(t) + \pi_W(t)) = \phi(X \cap U, \pi_W(t)) = \lambda\phi(X \cap U, w),$$

which implies that Y is an abelian subalgebra of $\mathfrak{g}$ of dimension 4. As a consequence, w is a central element and so, by Lemma 4.4(1), the rank of $\mathrm{B}^{\bullet}(w)$ is zero; contradiction to Lemma 4.8. To conclude, in this case one can take $M = \mathrm{Id}_2$ to get that $X = \psi(M)(U) = U$.

Assume now that $X \cap U = \{0\}$. Then X is a complement of U in V, as W is, and thus there exists $D \in \mathrm{Mat}_3(K)$ such that $X = \{w + \overline{w}D^{\mathrm{T}} \mid w \in W\}$. Fix such a D. By Lemma 2.3, it satisfies $D^{\mathrm{T}}\mathrm{B} = \mathrm{B}D$. We claim that D is a scalar matrix, i.e. $D = \lambda\,\mathrm{Id}_3$ for some $\lambda \in K$. For this we may, without loss of generality, assume that K is algebraically closed. Indeed, solving $D^{\mathrm{T}}\mathrm{B} = \mathrm{B}D$ over K reduces to solving a system of 9 linear equations in 9 indeterminates and, if $D^{\mathrm{T}}\mathrm{B} = \mathrm{B}D$ implies that D is scalar over an algebraic closure of K, then the same holds over K. Let $\mathcal{U}$ be a subset of $\mathcal{V}_{\mathrm{B}^{\bullet}}(U)$ of cardinality 4 such that any 3 of its elements form a basis of U; such $\mathcal{U}$ exist by Lemma 3.2. By (4.1) there exists, for each $u \in \mathcal{U}$, an element $w_u \in W\backslash\{0\}$, unique up to scalar multiplication, such that

$$\mathrm{B}^{\bullet}(u){w_u}^{\mathrm{T}} = 0 = \mathrm{B}(w_u)u^{\mathrm{T}}.$$

In particular, combining Lemma 4.8 and (4.1) yields a well-defined bijection

$$\{\mathbb{P}(Ku) \mid u \in \mathcal{U}\} \longrightarrow \{\mathbb{P}(Kw_u) \mid u \in \mathcal{U}\}, \quad \mathbb{P}(Ku) \mapsto \mathbb{P}(\ker \mathrm{B}^{\bullet}(u))$$

with inverse $\mathbb{P}(Kw) \mapsto \mathbb{P}(\ker \mathrm{B}(w))$. It follows from Lemma 4.4(2) and Lemma 4.8 that each $u \in \mathcal{U}$ is an eigenvector with respect to D with eigenvalue $\lambda_u \in K$, say. The fact that any three elements of $\mathcal{U}$ generate U yields the existence of a $\lambda \in K$ such that for each $u \in U$ one has $\lambda = \lambda_u$; in particular, the matrix D is equal to $\lambda\,\mathrm{Id}_3$. For such λ, defining $M = \begin{pmatrix} 1 & \lambda \\ 0 & 1 \end{pmatrix}$ yields that $X = \psi(M)(U)$. □

Corollary 4.11 *Let F be a finite field of odd characteristic and assume that $\mathbb{P}\mathcal{V}_B$ and $\mathbb{P}\mathcal{V}_{B^{\bullet}}$ are elliptic curves over F. Then the following holds:*

$$\mathrm{Aut}_{\mathbb{F}_p}(\mathfrak{g}_B(F)) \cong \mathrm{Aut}(\mathfrak{g}_B(F)) \rtimes \mathrm{Gal}(F/\mathbb{F}_p).$$

Proof Write $\mathfrak{g}$ for $\mathfrak{g}_{\mathrm{B}}(F)$ and let $\mathrm{C}_{\mathfrak{g}}$ denote the centroid of $\mathfrak{g}$, as defined in [33, § 1.1]. Using Proposition 4.10 and extending the arguments of Lemmas 2.3 and Lemma 2.4, it is not difficult to see that $\mathrm{C}_{\mathfrak{g}}$ is the collection of all the scalar multiplications on $\mathfrak{g}$ by elements of F and so $\mathrm{C}_{\mathfrak{g}} \cong F$. As a consequence of [33, Thm. 1.2(D)] (cf. also [33, §5]) we obtain an exact sequence

$$1 \to \mathrm{Aut}(\mathfrak{g}) \to \mathrm{Aut}_{\mathbb{F}_p}(\mathfrak{g}) \to \mathrm{Gal}(F/\mathbb{F}_p).$$

The map

$$\sigma \mapsto \left(\sum_{i=1}^{3} (\lambda_i e_i + \mu_i f_i + \nu_i g_i) \mapsto \sum_{i=1}^{3} (\sigma(\lambda_i) e_i + \sigma(\mu_i) f_i + \sigma(\nu_i) g_i) \right)$$

being a section $\mathrm{Gal}(F/\mathbb{F}_p) \to \mathrm{Aut}_{\mathbb{F}_p}(\mathfrak{g})$ it is, in fact, a split short exact sequence. The result follows. □

Remark 4.12 Proposition 4.10 generalizes the computations in [9, §7] for $\mathrm{B} = \mathrm{B}_{1,1}$ defined in (1.9).

As mentioned in Sect. 2, Proposition 4.10 allows us to apply Lemma 2.4 in the proof of Theorem 1.4. This lemma reduces the determination of the order of the automorphism group of $\mathfrak{g}_\mathrm{B}$ to the analysis of the structure of the subgroup $\mathrm{Aut}_V^{=}(\mathfrak{g}_\mathrm{B})$ of $\mathrm{Aut}(\mathfrak{g}_\mathrm{B})$. In the next proposition, let $\pi : \mathrm{Aut}_V^{=}(\mathfrak{g}_\mathrm{B}(F)) \to \mathrm{PGL}_3(F)$ be the map defined by $\mathrm{diag}(A, A, A_T) \mapsto \overline{A}$, where $\overline{A}$ is the image in $\mathrm{PGL}_3(K)$ of A.

Proposition 4.13 *Assume that $\mathbb{P}\mathcal{V}_{B^\bullet}$ is an elliptic curve. Then the map*

$$\overline{c}_B : \mathrm{Aut}_V^{=}(\mathfrak{g}_B) \longrightarrow \mathrm{Aut}(\mathbb{P}\mathcal{V}_{B^\bullet}), \quad \mathrm{diag}(A, A, A_T) \longmapsto \overline{A}_{|\mathcal{V}_{B^\bullet}},$$

is a well-defined homomorphism of groups and satisfies $\overline{c}_B = \overline{c}_{\mathbb{P}\mathcal{V}_B^\bullet} \circ \pi$.

Proof The elements of $\mathrm{Aut}_V^{=}(\mathfrak{g}_\mathrm{B})$ stabilize the abelian subalgebra U and, being Lie algebra homomorphisms, respect the centralizer dimensions $\dim \mathrm{C}_V(u)$ of the elements $u \in U$. More concretely, if φ belongs to $\mathrm{Aut}_V^{=}(\mathfrak{g}_\mathrm{B})$, then, thanks to Remark 4.9, the following hold:

$$\varphi(0) = 0, \quad \varphi(\mathcal{V}_{\mathrm{B}^\bullet}(U)\backslash\{0\}) = \mathcal{V}_{\mathrm{B}^\bullet}(U)\backslash\{0\}, \quad \varphi(U\backslash\mathcal{V}_{\mathrm{B}^\bullet}(U)) = U\backslash\mathcal{V}_{\mathrm{B}^\bullet}(U).$$

In particular, any element of $\mathrm{Aut}_V^{=}(\mathfrak{g}_\mathrm{B})$ induces a bijection $\mathcal{V}_{\mathrm{B}^\bullet}(U)\backslash\{0\} \longrightarrow \mathcal{V}_{\mathrm{B}^\bullet}(U)\backslash\{0\}$ and so projectivisation yields the homomorphism $\overline{c}_\mathrm{B}$. □

The idea of appealing to the subgroup $\mathrm{Aut}_V^{=}(\mathfrak{g})$ in order to determine the structure of $\mathrm{Aut}(\mathfrak{g})$ was already pursued in [9]. This notwithstanding, the map $\overline{c}_\mathrm{B}$ holds the key to the realization of the added value brought about by our geometric point of view. Indeed, the determination of the image of $\overline{c}_\mathrm{B}$ plays a decisive role in the proof of Theorem 1.4 by means of the following corollary.

Corollary 4.14 *Let F be a finite field of odd characteristic and assume that $\mathbb{P}\mathcal{V}_B$ and $\mathbb{P}\mathcal{V}_{B^\bullet}$ are elliptic curves over F. Then the following hold:*

$$|\mathrm{Aut}(\mathfrak{g}_B(F))| = \frac{|\mathrm{Aut}_V^{=}(\mathfrak{g}_B(F))| \cdot |\mathrm{GL}_2(F)| \cdot |F|^{18}}{|F| - 1} = |\mathrm{im}\, \overline{c}_B| \cdot |\mathrm{GL}_2(F)| \cdot |F|^{18}.$$

Proof The combination of (2.8), Proposition 4.10, and Lemma 2.44 yields that

$$|\operatorname{Aut}(\mathfrak{g}_{\mathrm{B}}(F))| = \frac{|\operatorname{Aut}_V^{=}(\mathfrak{g}_{\mathrm{B}}(F))| \cdot |\mathrm{GL}_2(F)| \cdot |F|^{18}}{|F|-1} = \frac{|\ker \overline{c}_{\mathrm{B}}| \cdot |\operatorname{im} \overline{c}_{\mathrm{B}}| \cdot |\mathrm{GL}_2(F)| \cdot |F|^{18}}{|F|-1}.$$

The claim follows as Lemmas 3.3 and 2.43 imply that $\ker \overline{c}_{\mathrm{B}} = \{\lambda \,\mathrm{Id}_9 \mid \lambda \in F^{\times}\} \cong F^{\times}$. □

5 Proofs of the main results and their corollaries

We prove Theorem 1.4 and its Corollaries 1.7-1.9 in Sect. 5.1 and Theorem 1.6 in Sect. 5.2, where we also prove Theorem 1.1.

5.1 Automorphisms

We continue to use the setup from Sect. 3.2 and combine it with that from Sect. 2.1. Recall that δ is a nonzero integer and that K is a field of characteristic not dividing 2δ. Assume further that K contains a fixed square root $\delta^{\frac{1}{2}}$ of δ. For $i \in \{1, 2, 3\}$, let $\mathrm{B}_{i,\delta}$ be as in (1.9), and denote by $\phi_{i,\delta}$ and $\widetilde{\phi}_{i,\delta}$, respectively, the associated bilinear and linear maps defined in (2.2) resp. (2.3). The image of $\phi_{i,\delta}$ spans T so $\widetilde{\phi}_{i,\delta}$ is surjective.

Write $\mathbf{G}_{i,\delta} = \mathbf{G}_{\mathrm{B}_{i,\delta}}$ and $\mathfrak{g}_{i,\delta} = \mathfrak{g}_{\mathrm{B}_{i,\delta}}$, respectively, for the group and the Lie algebra (schemes) associated with the data $(K, B_{i,\delta}, \phi_{i,\delta})$ in Sect. 2.2. We recall that, if $K = F$ is a finite field of order q and odd characteristic p, then the finite p-group $\mathbf{G}_{i,\delta}(F)$ has exponent p, nilpotency class 2, and order q^9, while the F-Lie algebra $\mathfrak{g}_{i,\delta}$ has F-dimension 9 and nilpotency class 2. We are looking to compute the order of $\operatorname{Aut}(\mathfrak{g}_{i,\delta}(F))$. For this, we will use Corollary 4.14. Indeed, the matrix $\mathrm{B}_{i,\delta}$ is Hessian and therefore satisfies $\mathrm{B}_{i,\delta} = \mathrm{B}^{\bullet}_{i,\delta}$; see Lemma 4.5. Observe that $\mathbb{P}\mathcal{V}_{\mathrm{B}_{i,\delta}}$ is identified with the elliptic curve E_δ via the projectivisation (3.1). Let

$$\overline{c}_{\mathrm{B}_{i,\delta}} : \operatorname{Aut}_V^{=}(\mathfrak{g}_{i,\delta}) \to \operatorname{Aut}(E_\delta)$$

be the homomorphism from Proposition 4.13. By Proposition 3.8, its image is isomorphic to a subgroup of $E_\delta[3] \rtimes \operatorname{Aut}_O(E_\delta)$, which leads us to consider the homomorphism

$$\begin{aligned} \overline{c}_{i,\delta} :\ & \operatorname{Aut}_V^{=}(\mathfrak{g}_{i,\delta}) \longrightarrow E_\delta[3] \rtimes \operatorname{Aut}_O(E_\delta), \\ & \operatorname{diag}(A, A, A_T) \longmapsto \overline{c}_{\mathrm{B}_{i,\delta}}(\operatorname{diag}(A, A, A_T)) = (Q_A, \alpha_A). \end{aligned} \tag{5.1}$$

Corollary 4.14 reduces the proof of Theorem 1.4 to the explicit determination of the image size of $\overline{c}_{i,\delta}$. To this end, we will make use of the following specific version of Lemma 2.5.

Lemma 5.1 *Let $A \in \mathrm{GL}_3(K)$ and define the following subsets of $U \otimes W$:*

$$\mathcal{K}^*_{1,\delta} = \{e_2 \otimes f_3, \delta e_1 \otimes f_1 - e_3 \otimes f_3, e_1 \otimes f_3 + e_2 \otimes f_2\},$$

$$\mathcal{K}^*_{2,\delta} = \{(\delta^{\frac{1}{2}}e_1 + e_3) \otimes f_3, e_2 \otimes f_3 - \delta^{\frac{1}{2}}e_1 \otimes f_2, \delta e_1 \otimes f_1 + 2\delta^{\frac{1}{2}}e_2 \otimes f_2 + e_3 \otimes f_3\},$$
$$\mathcal{K}^*_{3,\delta} = \{(\delta^{\frac{1}{2}}e_1 - e_3) \otimes f_3, e_2 \otimes f_3 + \delta^{\frac{1}{2}}e_1 \otimes f_2, \delta e_1 \otimes f_1 - 2\delta^{\frac{1}{2}}e_2 \otimes f_2 + e_3 \otimes f_3\}.$$

Then the following are equivalent:

(1) $(A \otimes A)(\mathcal{K}^*_{i,\delta}) \subseteq \ker \widetilde{\phi}_{i,\delta}$*;*
(2) there exists $A_T \in \mathrm{GL}_3(K)$ *such that* $\mathrm{diag}(A, A, A_T) \in \mathrm{Aut}(\mathfrak{g}_{i,\delta})$.

Proof Consider the following supersets of $\mathcal{K}^*_{i,\delta}$ of $\mathcal{K}_{i,\delta}$ in $U \otimes W$:

$$\mathcal{K}_{1,\delta} = \mathcal{K}^*_{1,\delta} \cup \{e_3 \otimes f_2, e_1 \otimes f_3 - e_3 \otimes f_1, e_1 \otimes f_2 - e_2 \otimes f_1\},$$
$$\mathcal{K}_{2,\delta} = \mathcal{K}^*_{2,\delta} \cup \{e_3 \otimes (\delta^{\frac{1}{2}} f_1 + f_3), \delta^{\frac{1}{2}}e_2 \otimes f_1 - e_3 \otimes f_2, e_2 \otimes f_3 - e_3 \otimes f_2\},$$
$$\mathcal{K}_{3,\delta} = \mathcal{K}^*_{3,\delta} \cup \{e_3 \otimes (\delta^{\frac{1}{2}} f_1 - f_3), \delta^{\frac{1}{2}}e_2 \otimes f_1 + e_3 \otimes f_2, e_2 \otimes f_3 - e_3 \otimes f_2\}.$$

The kernel of $\widetilde{\phi}_{i,\delta}$ is spanned by $\mathcal{K}_{i,\delta}$ over K. It follows, however, from Remark 2.6 that to check whether $(A \otimes A)(\ker \widetilde{\phi}_{i,\delta})$ is contained in $\ker \widetilde{\phi}_{i,\delta}$ it suffices to check if $(A \otimes A)(\mathcal{K}^*_{i,\delta})$ is annihilated by $\widetilde{\phi}_{i,\delta}$. Indeed, the elements of $\mathcal{K}_{i,\delta} \backslash \mathcal{K}^*_{i,\delta}$ are equal to the negatives of their respective duals or duals to members of $\mathcal{K}^*_{i,\delta}$. To conclude we apply Lemma 2.5. □

Lemma 5.2 *Let* $\alpha \in \mathrm{Aut}_O(E_\delta)$*. The following are equivalent:*

(1) There exist $A, A_T \in \mathrm{GL}_3(K)$ *such that* $\overline{c}_{i,\delta}(\mathrm{diag}(A, A, A_T)) = (O, \alpha)$*;*
(2) $\alpha^{\lceil 4/i \rceil} = \mathrm{id}_{E_\delta}$.

Proof Let (ω, ρ) be such that $\omega^4 = 1$ and $\delta\rho^3 = \rho$ with $\rho \neq 0$ only if $\mathrm{char}(K) = 3$. Let $\alpha \in \mathrm{Aut}_O(E_\delta)$ be the invertible isogeny defined by $(x, y) \mapsto (\omega^2 x + \rho, \omega^3 y)$ and observe that, if $i \in \{2, 3\}$, then $\lceil 4/i \rceil = 2$. By Lemma 3.4, the matrix

$$A = \begin{pmatrix} \omega^2 & 0 & \rho \\ 0 & \omega^3 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

is the unique element of $\mathrm{GL}_3(K)$, up to scalar multiplication, inducing α.

We start by considering $i = 1$. A necessary condition for $(A \otimes A)(\mathcal{K}^*_{1,\delta})$ to be contained in $\ker \widetilde{\phi}_{1,\delta}$ is that $0 = \widetilde{\phi}_{1,\delta}((A \otimes A)(e_1 \otimes f_3 + e_2 \otimes f_2)) = \omega^2 \rho g_3$, equivalently $\rho = 0$. It is not difficult to show, for $\rho = 0$, that $(A \otimes A)(\mathcal{K}^*_{1,\delta})$ is contained in $\ker \widetilde{\phi}_{1,\delta}$ and so, by Lemma 5.1, there exists $A_T \in \mathrm{GL}_3(K)$ such that $\mathrm{diag}(A, A, A_T)$ is an automorphism of $\mathfrak{g}_{1,\delta}(K)$. By the definition of $\overline{c}_{1,\delta}$, the pair (O, α) is contained in its image.

Let now $i \in \{2, 3\}$. Computing $(A \otimes A)(e_2 \otimes f_3 \mp \delta^{\frac{1}{2}} e_1 \otimes f_2)$ for $i = 2$ resp. $i = 3$ we get that

$$(A \otimes A)(e_2 \otimes f_3 \mp \delta^{\frac{1}{2}} e_1 \otimes f_2) \in \ker \widetilde{\phi}_{i,\delta} \iff \omega^2 \rho \pm \omega^2 \delta^{\frac{1}{2}} \mp \delta^{\frac{1}{2}} = 0.$$

If $\rho = 0$, one sees that $\omega^2 = 1$ is a necessary and sufficient condition for the image $(A \otimes A)(\mathcal{K}_{i,\delta}^*)$ to be contained in $\ker \widetilde{\phi}_{i,\delta}$. Assume, in conclusion, that $\rho \neq 0$ and thus that $\mathrm{char}(K) = 3$: we show that $\alpha \notin \mathrm{im}\, \overline{c}_{i,\delta}$. We work by contradiction, assuming that $\widetilde{\phi}_{i,\delta}((A \otimes A)(\mathcal{K}_{i,\delta}^*)) = \{0\}$. It follows then that $\delta\rho^2 = 1$ and so we find that

$$1 = \delta\rho^2 = \delta^2(\pm 1 \mp \omega^2)^2\omega^{-4} = 2\delta^2(1 - \omega^2).$$

In particular, $\omega^2 = -1$ and so that $\rho = \mp 2\delta^{\frac{1}{2}}$. From

$$\widetilde{\phi}_{i,\delta}(A \otimes A)(\delta e_1 \otimes f_1 \pm 2\delta^{\frac{1}{2}} e_2 \otimes f_2 + e_3 \otimes f_3) = 0$$

we then get that $0 = (\pm\delta^{\frac{1}{2}} + 2\rho)g_1 + (\pm 2\rho\delta^{\frac{1}{2}} + \delta)g_3$ and so, from the coefficient of g_3, we derive that $\delta = \pm 2\rho\delta^{\frac{1}{2}} = -4\delta = -\delta$. Contradiction. We conclude with Lemma 5.1. □

Lemma 5.3 *Let $Q = (a, b)$ be an element of $E_\delta[3]$. Then there exist $A, A_T \in \mathrm{GL}_3(K)$ such that*

$$\overline{c}_{i,\delta}(\mathrm{diag}(A, A, A_T)) = (Q, \mathrm{id}_E).$$

Proof Up to scalar multiplication, Lemma 3.9 yields that a necessary condition for the existence of such a pair (A, A_T) is the existence of $\nu \in K^\times$ such that

$$A = A(\nu) = \begin{pmatrix} \delta ab + 2ab\nu & \delta a^2 & -2\delta a^2 b\nu \\ (-3\delta - 2\nu)b^2 & \delta ab & 2\delta ab^2\nu \\ (1 - 2\nu a^2)b & a & 2\delta a^3 b\nu \end{pmatrix}.$$

We set $\nu = -\delta/(\delta a^2 + 1)$ and claim that, for this matrix $A = A(\nu)$, there exists $A_T = A_T(\nu)$ such that $\overline{c}_{i,\delta}(\mathrm{diag}(A, A, A_T))$ is equal to (Q, id_E). Indeed, checking (e.g. with SageMath [27]) identities involving the matrix $C = A^{\mathrm{T}}\mathrm{B}_{i,\delta}A$ defined in Remark 2.6, one shows that $(A \otimes A)(\mathcal{K}_{i,\delta}^*) \subseteq \ker \widetilde{\phi}_{i,\delta}$. We conclude with Lemma 5.1. □

Corollary 5.4 *Let F be a finite field of characteristic not dividing 2δ in which δ has a fixed square root. Then the following holds:*

$$|\mathrm{Aut}(\mathfrak{g}_{i,\delta}(F))| = \gcd(|F| - 1, \lceil 4/i \rceil)\, |\mathrm{GL}_2(F)| \cdot |F|^{18} \cdot |E_\delta[3](F)|.$$

Proof Combining Lemmas 5.2 and 5.3 allows us to describe the image of the homomorphism $\overline{c}_{i,\delta}$ (cf. (5.1)) and hence, by Corollary 4.14, the order of $\mathrm{Aut}(\mathfrak{g}_{i,\delta}(F))$. □

To prove Theorem 1.4 it now suffices to note that $|\mathrm{Aut}(\mathbf{G}_{i,\delta}(F))| = |\mathrm{Aut}_{\mathbb{F}_p}(\mathfrak{g}_{i,\delta}(F))|$ by the Bear correspondence. We may thus conclude by combining Corllary 4.11 and and Lemma 5.4.

We conclude by proving Corollaries 1.7-1.9. To this end, let p be a prime not dividing 6δ and let $\mathrm{n}_{1,1}(p)$ denote the number of immediate descendants of $\mathbf{G}_{1,1}(\mathbb{F}_p)$ of order p^{10} and exponent p. In [9, Sec. 4] it is shown that neither of the two functions

$$p \longmapsto |\operatorname{Aut}(\mathbf{G}_{1,1}(\mathbb{F}_p))|, \quad p \longmapsto \mathrm{n}_{1,1}(p)$$

are PORC, the second being so as a consequence of the first. Combining Theorem 1.3 with Lemma 3.7, this amounts to saying that the function $\Pi \to \mathbb{Z}$, $p \mapsto |E_1[3](\mathbb{F}_p)|$ is not constant on residue classes modulo a fixed integer. Corollary 1.7 now follows from Theorem 1.4 and Lemma 3.10. To prove Corollary 1.8, observe that the function $p \mapsto |E[3](\mathbb{F}_p)|$ is constant on Frobenius sets for any elliptic curve E defined over $\mathbb{Q}$. To prove Corollary 1.9 one may proceed as in [9, Sec. 11], i.e. by counting orbits of the induced action of $\operatorname{im}\bar{c}_{1,1}$ on $\mathbb{F}_p^3$ by means of Burnside's lemma. One checks easily that our formula for the descendants matches the values listed in [28, Sec. 5].

5.2 Isomorphisms

While we focussed so far on automorphisms of groups and Lie algebras of the form described in Sect. 2.2, we now turn to isomorphisms between such objects. The section's main aim is to prove Theorem 1.6. To this end, we state and work with a number of results that have close counterparts in Sect. 2. Their proofs being entirely analogous, we omit most of them. We also restrict to the case that $\operatorname{char}(K) \neq 3$, to lighten notation.

Let $i, j \in \{1, 2, 3\}$ and $\delta, \delta' \in \mathbb{Z}\setminus\{0\}$. Assume that the characteristic of K does not divide $2\delta\delta'$ and that K contains square roots $\delta^{\frac{1}{2}}$ and $\delta'^{\frac{1}{2}}$ of δ resp. δ', which we fix. We write $U_{i,\delta}$, $W_{i,\delta}$, $T_{i,\delta}$, $V_{i,\delta}$ for the modules U, W, T, V from Sect. 2.1. In particular, $U_{i,\delta} \oplus W_{i,\delta} \oplus T_{i,\delta}$ is the underlying vector space of $\mathfrak{g}_{i,\delta}(K)$. In a similar fashion, we will write

$$(e_1^{(i,\delta)}, e_2^{(i,\delta)}, e_3^{(i,\delta)}), \quad (f_1^{(i,\delta)}, f_2^{(i,\delta)}, f_3^{(i,\delta)}), \quad (g_1^{(i,\delta)}, g_2^{(i,\delta)}, g_3^{(i,\delta)})$$

for the bases $\mathcal{E} = \mathcal{E}^{(i)}$, $\mathcal{F} = \mathcal{F}^{(i)}$, $\mathcal{T} = \mathcal{T}^{(i)}$ from Sect. 2.1. Analogous indexing pertains to the pair (j, δ'). With respect to these bases, we may view Lie algebra isomorphisms $\mathfrak{g}_{i,\delta}(K) \to \mathfrak{g}_{j,\delta'}(K)$ as matrices in $\mathrm{GL}_9(K)$. With these identifications, an isomorphism $\alpha : \mathfrak{g}_{i,\delta}(K) \to \mathfrak{g}_{j,\delta'}(K)$ satisfying $\alpha(U_{i,\delta}) = U_{j,\delta'}, \alpha(W_{i,\delta}) = W_{j,\delta'}$, and $\alpha(T_{i,\delta}) = T_{j,\delta'}$, is of the form $\alpha = \operatorname{diag}(A_U, A_W, A_T)$ for some $A_U, A_W, A_T \in \mathrm{GL}_3(K)$.

Lemma 5.5 *If $\mathfrak{g}_{i,\delta}(K) \cong \mathfrak{g}_{j,\delta'}(K)$, then there exists an isomorphism $\alpha : \mathfrak{g}_{i,\delta}(K) \to \mathfrak{g}_{j,\delta'}(K)$ such that the following hold:*

(1) $\alpha(U_{i,\delta}) = U_{j,\delta'}$, $\alpha(W_{i,\delta}) = W_{j,\delta'}$, and $\alpha(T_{i,\delta}) = T_{j,\delta'}$.
(2) The map α induces isomorphisms of projective curves $\alpha_U, \alpha_W : E_\delta \to E_{\delta'}$.

Proof Let $\alpha' : \mathfrak{g}_{i,\delta}(K) \to \mathfrak{g}_{j,\delta'}(K)$ be an isomorphism and assume, without loss of generality, that $\alpha'(V_{i,\delta}) = V_{j,\delta'}$. Then $\alpha'(U_{i,\delta})$ and $\alpha'(W_{i,\delta})$ are 3-dimensional abelian subalgebras of $\mathfrak{g}_{j,\delta'}(K)$ that are contained in $V_{j,\delta'}$. Let $M \in \mathrm{GL}_2(K)$ be such that $\psi(M)(\alpha'(U_{i,\delta})) = U_{j,\delta'}$ and $\psi(M)(\alpha'(W_{i,\delta})) = W_{j,\delta'}$; cf. Proposition 4.10. Define $\alpha = \psi(M) \circ \alpha'$. By (4.3), the Lie algebra isomorphism α induces isomorphisms of projective curves $\alpha_U, \alpha_W : E_\delta \to E_{\delta'}$, corresponding to the restrictions of α to $U_{i,\delta}$ resp. $W_{i,\delta}$. □

The following is a variation of Lemma 2.3. We omit the analogous proof.

Lemma 5.6 *Let A_U and A_W be elements of $\mathrm{GL}_3(K)$ and set $D = A_U A_W^{-1}$. Then the conditions*

(1) there exists $A_T \in \mathrm{GL}_3(K)$ such that $\mathrm{diag}(A_U, A_W, A_T) : \mathfrak{g}_{i,\delta}(K) \to \mathfrak{g}_{j,\delta'}(K)$ is an isomorphism;
(2) the equality $D^{\mathrm{T}} B_{j,\delta'} = B_{j,\delta'} D$ holds;
(3) the subspace $X = \{w + \overline{w} D^{\mathrm{T}} \mid w \in W_{j,\delta'}\}$ is a complement of $U_{j,\delta'}$ in $V_{j,\delta'}$ satisfying $[X, X] = 0$;

are related in the following way:

$$(1) \implies (2) \iff (3).$$

Lemma 5.7 *If $\mathfrak{g}_{i,\delta}(K) \cong \mathfrak{g}_{j,\delta'}(K)$, then there exists an isomorphism $\beta : \mathfrak{g}_{i,\delta}(K) \to \mathfrak{g}_{j,\delta'}(K)$ and $A, A_T \in \mathrm{GL}_3(K)$ such that the following hold:*

(1) $\beta = \mathrm{diag}(A, A, A_T)$.
(2) There exists $\varepsilon \in K$ such that $\delta = \varepsilon^4 \delta'$ and A induces the invertible isogeny

$$E_\delta \longrightarrow E_{\delta'}, \quad (x, y) \longmapsto (\varepsilon^2 x, \varepsilon^3 y).$$

Proof Let α be as in Lemma 5.5 and write $\beta = \mathrm{diag}(A, A, A_T)$ for matrices A_U, A_W, A_T in $\mathrm{GL}_3(K)$. Let, moreover, α_U, α_W denote the projective curve isomorphisms $E_\delta \to E_{\delta'}$ induced by A_U resp. A_W.

(1): By Proposition 4.10, every 3-dimensional abelian subalgebra of $\mathfrak{g}_{j,\delta'}(K)$ that is contained in $V_{j,\delta'}$ is of the form $\psi(M)(U_{j,\delta'})$ for some $M \in \mathrm{GL}_2(K)$. Equivalently, if X is such a subalgebra, then either $X = U_{j,\delta'}$ or $X = \{w + \lambda\overline{w} \mid w \in W_{j,\delta'}\}$ for some $\lambda \in K$. The matrix $D = A_U A_W^{-1}$ being invertible, Lemma 5.6 yields the existence of a unique $\lambda_0 \in K^\times$ such that $A_U = \lambda_0 A_W$. We conclude by defining $\beta = \psi(\mathrm{diag}(\lambda_0^{-1}, 1)) \circ \alpha$.

(2): Let β be as in (1) and set $P = \alpha_U(O)$. Then the map $\alpha = \tau_{-P} \circ \alpha_U$ is an invertible isogeny $E_\delta \to E_{\delta'}$ which satisfies $\tau_P = \alpha_U \circ \alpha^{-1}$. The assumptions and Lemma 3.4 imply that τ_P is induced by an element of $\mathrm{PGL}_3(K)$ and so, by the combination of Lemma 3.6 with Lemma 3.7, that the point P has order dividing 3. By Lemma 5.3 we may choose matrices $A', A'_T \in \mathrm{GL}_3(K)$ with the property that $\mathrm{diag}(A', A', A'_T) \in \mathrm{Aut}(\mathfrak{g}_{j,\delta'}(K))$ and $\overline{c}_{j,\delta'}(\mathrm{diag}(A', A', A'_T)) = (P, \mathrm{id}_E)$. To conclude, define $\beta' = \mathrm{diag}(A', A', A'_T)^{-1} \circ \beta$, which induces an invertible isogeny $\alpha' : E_\delta \to E_{\delta'}$. In particular, there exists $\varepsilon \in K$ satisfying $\delta = \varepsilon^4 \delta'$ and $\alpha'(x, y) = (\varepsilon^2 x, \varepsilon^3 y)$. □

The following is a variation of Lemma 2.5. We omit the analogous proof.

Lemma 5.8 *Let A be an element of* $\mathrm{GL}_3(K)$. *Then the following are equivalent:*

(1) $(A \otimes A)(\ker \tilde{\phi}_{i,\delta}) \subseteq \ker \tilde{\phi}_{j,\delta'}$;
(2) there exists $A_T \in \mathrm{GL}_3(K)$ *such that* $\mathrm{diag}(A, A, A_T) : \mathfrak{g}_{i,\delta}(K) \to \mathfrak{g}_{j,\delta'}(K)$ *is an isomorphism.*

Lemma 5.9 *Let* $\beta = \mathrm{diag}(A, A, A_T)$ *and* $\beta' = \mathrm{diag}(A', A', A'_T)$ *be Lie algebra isomorphisms* $\mathfrak{g}_{i,\delta}(K) \to \mathfrak{g}_{j,\delta'}(K)$ *such that A and A' induce the same invertible isogeny* $E_\delta \to E_{\delta'}$. *Then $\overline{A}$ and $\overline{A'}$ are equal in* $\mathrm{PGL}_3(K)$.

Proof Since $\beta^{-1} \circ \beta'$ is an automorphism of $\mathfrak{g}_{i,\delta}(K)$ inducing the identity on E_δ, Lemma 3.3 yields the claim. □

Proposition 5.10 *Assume that $i < j$. The following are equivalent:*

(1) The Lie algebras $\mathfrak{g}_{i,\delta}(K)$ *and* $\mathfrak{g}_{j,\delta'}(K)$ *are isomorphic.*
(2) The equality $\delta = \delta'$ *holds in K,* $\{i, j\} = \{2, 3\}$, *and either*

(a) $\delta^{\frac{1}{2}} = -\delta'^{\frac{1}{2}}$ *or*
(b) $\delta^{\frac{1}{2}} = \delta'^{\frac{1}{2}}$ *and K contains a primitive 4th root of unity.*

Proof (2) ⇒ (1): If $\delta'^{\frac{1}{2}} = -\delta^{\frac{1}{2}}$, it is obvious from inspection of (1.9) that $\mathfrak{g}_{i,\delta}(K) \cong \mathfrak{g}_{j,\delta'}(K)$. Assume thus that $\delta'^{\frac{1}{2}} = \delta^{\frac{1}{2}}$ and let $\omega \in \mu_4(K)$ have order 4. Then the map

$$\alpha = \mathrm{diag}(-1, -\omega, 1, -1, -\omega, 1, -1, \omega, 1)$$

is an isomorphism $\mathfrak{g}_{2,\delta}(K) \to \mathfrak{g}_{3,\delta'}(K)$.

(1) ⇒ (2): Let $\beta = \mathrm{diag}(A, A, A_T) : \mathfrak{g}_{i,\delta}(K) \to \mathfrak{g}_{j,\delta'}(K)$ be an isomorphism as in Lemma 5.7, let $\varepsilon \in K$ be such that $\delta = \varepsilon^4\delta'$, and assume that A induces the invertible isogeny $E_\delta \to E_{\delta'}$, $(x, y) \mapsto (\varepsilon^2 x, \varepsilon^3 y)$. By Lemma 5.9, the matrix A equals $\mathrm{diag}(\varepsilon^2, \varepsilon^3, 1)$, up to a scalar.

Assume first, for a contradiction, that $i = 1$. By Lemma 5.8, the element $e_2^{(1,\delta)} \otimes f_3^{(1,\delta)}$, belonging to $\ker \tilde{\phi}_{1,\delta}$, satisfies

$$0 = \tilde{\phi}_{j,\delta'}\left((A \otimes A)(e_2^{(1,\delta)} \otimes f_3^{(1,\delta)})\right) = \tilde{\phi}_{j,\delta'}\left(\varepsilon^3 e_2^{(j,\delta')} \otimes f_3^{(j,\delta')}\right) \in \{\pm\varepsilon^3\delta'^{\frac{1}{2}} g_2^{(j,\delta')}\};$$

contradiction.

Assume now that $(i, j) = (2, 3)$ and let $\mathcal{K}^*_{2,\delta}$ and $\mathcal{K}^*_{3,\delta'}$ be as in Lemma 5.1. Observe that $\mathcal{K}^*_{2,\delta}$ is contained in $\ker \tilde{\phi}_{2,\delta}$ and, analogously, $\mathcal{K}^*_{3,\delta'}$ is contained in $\ker \tilde{\phi}_{3,\delta'}$. Lemma 5.8 implies that $\tilde{\phi}_{3,\delta'}\left((A \otimes A)(\mathcal{K}^*_{2,\delta})\right) = \{0\}$ and so the span of $\tilde{\phi}_{3,\delta'}(\mathcal{K}^*_{2,\delta}) \cup \mathcal{K}^*_{3,\delta'}$ in $U_{3,\delta'} \otimes W_{3,\delta'}$ is contained in $\ker \tilde{\phi}_{3,\delta'}$. As a consequence, the elements

$$(A \otimes A)\left((\delta^{\frac{1}{2}} e_1^{(2,\delta)} + e_3^{(2,\delta)}) \otimes f_3^{(2,\delta)}) + (\delta^{\frac{1}{2}} e_1^{(2,\delta)} - e_3^{(2,\delta)}) \otimes f_3^{(2,\delta)}\right) \text{ and}$$

$$(A \otimes A)\Big((\delta e_1^{(2,\delta)} \otimes f_1^{(2,\delta)} + 2\delta^{\frac{1}{2}} e_2^{(2,\delta)} \otimes f_2^{(2,\delta)} + e_3^{(2,\delta)} \otimes f_3^{(2,\delta)}) \\ - (\delta e_1^{(2,\delta)} \otimes f_1^{(2,\delta)} - 2\delta^{\frac{1}{2}} e_2^{(2,\delta)} \otimes f_2^{(2,\delta)} + e_3^{(2,\delta)} \otimes f_3^{(2,\delta)})\Big)$$

belong to $\ker \tilde{\phi}_{3,\delta'}$. Applying $\tilde{\phi}_{3,\delta'}$ and using the fact that the basis elements $g_k^{(3,\delta')}$ for $k = 1, 2, 3$ are linearly independent, we derive

$$\delta^{\frac{1}{2}}\varepsilon^2 + \delta'^{\frac{1}{2}} = 0, \quad \delta^{\frac{1}{2}}\varepsilon^6 + \delta'^{\frac{1}{2}} = 0, \quad \delta\varepsilon^4 - \delta' = 0.$$

It follows that $\varepsilon^4 = 1$, that $\delta'^{\frac{1}{2}} = -\varepsilon^2\delta^{\frac{1}{2}}$, and that $\delta = \delta'$. We conclude observing that, if $\varepsilon^2 = 1$, then we get $\delta'^{\frac{1}{2}} = -\delta^{\frac{1}{2}}$ while, if ε is a primitive 4th root of unity, then $\delta'^{\frac{1}{2}} = \delta^{\frac{1}{2}}$. □

Proposition 5.11 *The following are equivalent:*

(1) The Lie algebras $\mathfrak{g}_{i,\delta}(K)$ and $\mathfrak{g}_{i,\delta'}(K)$ are isomorphic.
(2) The equality $\delta = \delta'$ holds in K and, if $i \in \{2, 3\}$, then either

(a) $\delta^{\frac{1}{2}} = \delta'^{\frac{1}{2}}$ or
(b) $\delta^{\frac{1}{2}} = -\delta'^{\frac{1}{2}}$ and K contains a primitive 4th root of unity.

Proof (2) $\Rightarrow$ (1) If $i = 1$, the statement is clear. Assume now that $i \in \{2, 3\}$. If $\delta^{\frac{1}{2}} = \delta'^{\frac{1}{2}}$, then $\mathrm{B}_{i,\delta} = \mathrm{B}_{i,\delta'}$ implying that $\mathfrak{g}_{i,\delta}(K) \cong \mathfrak{g}_{i,\delta'}(K)$. Assume now that $\delta^{\frac{1}{2}} = -\delta'^{\frac{1}{2}}$ and that K contains a primitive 4th root of unity. Then $\mathrm{B}_{2,\delta} = \mathrm{B}_{3,\delta'}$ and so Proposition 5.10 yields $\mathfrak{g}_{2,\delta}(K) \cong \mathfrak{g}_{3,\delta'}(K) \cong \mathfrak{g}_{2,\delta'}(K) \cong \mathfrak{g}_{3,\delta}(K)$.

(1) $\Rightarrow$ (2) Assume $\mathfrak{g}_{i,\delta}(K) \cong \mathfrak{g}_{i,\delta'}(K)$ and let $\beta = \mathrm{diag}(A, A, A_T) : \mathfrak{g}_{i,\delta}(K) \to \mathfrak{g}_{i,\delta'}(K)$ be an isomorphism as in Lemma 5.7. Then there exist $\varepsilon \in K$ such that $\delta^{\frac{1}{2}} = \varepsilon^2\delta'^{\frac{1}{2}}$ and, up to a scalar multiple, the matrix A equals $\mathrm{diag}(\varepsilon^2, \varepsilon^3, 1)$; see Lemma 5.9. We fix such ε and proceed by considering the cases $i = 1$ and $i \in \{2, 3\}$ separately.

If $i = 1$, then $g_1^{(1,\delta)} = [e_1^{(1,\delta)}, f_3^{(1,\delta)}] = -[e_2^{(1,\delta)}, f_2^{(1,\delta)}]$ in $\mathfrak{g}_{1,\delta}(K)$, whence

$$\varepsilon^2 g_1^{(1,\delta')} = \beta([e_1^{(1,\delta)}, f_3^{(1,\delta)}]) = -\beta([e_2^{(1,\delta)}, f_2^{(1,\delta)}]) = -\varepsilon^6(-g_1^{(1,\delta')}).$$

As a result, $\varepsilon^4 = 1$ and so $\delta = \delta'$.

If $i \in \{2, 3\}$, then $-\delta^{\frac{1}{2}} g_2^{(i,\delta)} = \delta^{\frac{1}{2}}[e_1^{(i,\delta)}, f_2^{(i,\delta)}] = \pm[e_2^{(i,\delta)}, f_3^{(i,\delta)}]$, whence

$$\delta^{\frac{1}{2}}\varepsilon^5(-g_2^{(i,\delta')}) = \delta^{\frac{1}{2}}\beta([e_1^{(i,\delta)}, f_2^{(i,\delta)}]) = \pm\beta([e_2^{(i,\delta)}, f_3^{(i,\delta)}]) = \pm\varepsilon^3(\mp\delta'^{\frac{1}{2}} g_2^{(i,\delta')}) = -\varepsilon^3\delta'^{\frac{1}{2}} g_2^{(i,\delta')}.$$

It follows that $\varepsilon^4 = 1$, which yields $\delta = \delta'$ and, in particular, $\delta^{\frac{1}{2}} = \delta'^{\frac{1}{2}}$ or $\delta^{\frac{1}{2}} = -\delta'^{\frac{1}{2}}$. If $\delta^{\frac{1}{2}} = -\delta'^{\frac{1}{2}}$, then Proposition 5.10 yields that K possesses a primitive 4th root of unity. □

Theorem 5.12 *The K-Lie algebras $\mathfrak{g}_{i,\delta}(K)$ and $\mathfrak{g}_{j,\delta'}(K)$ are isomorphic if and only if $\delta = \delta'$ in K and either*

(1) $i = j$ and, if $i \in \{2, 3\}$, then either

(1.a) $\delta^{\frac{1}{2}} = \delta'^{\frac{1}{2}}$ or
(1.b) $\delta^{\frac{1}{2}} = -\delta'^{\frac{1}{2}}$ and K contains a primitive 4th root of unity or

(2) $\{i, j\} = \{2, 3\}$ and either

(2.a) $\delta^{\frac{1}{2}} = -\delta'^{\frac{1}{2}}$ or
(2.b) $\delta^{\frac{1}{2}} = \delta'^{\frac{1}{2}}$ and K contains a primitive 4th root of unity.

Proof Combine Propositions 5.10 and 5.11. □

Theorem 1.6 is the special case of Theorem 5.12 for $K = \mathbb{F}_p$, via the Baer correspondence.

We conclude the paper by proving Theorem 1.1. The groups $\mathbf{G}_i(F)$ are defined by solving the equation (1.6) associated to the Weierstrass form of E and then applying the construction from Sect. 2.2. We have exactly three solutions to (1.6), corresponding to the three nontrivial 2-torsion points of E, thanks to [23, Thm. 1] and Theorem 1.1(1) is clear from the construction of $\mathbf{G}_i(F)$. Theorem 1.1(2) is a result of the combination of Lemma 4.5, Corollary 4.14, and Corollary 4.11. The rest of Theorem 1.1 is given by Proposition 3.8 and Theorem 1.6.

Acknowledgements We are very grateful to Alex Galanakis, Avinash Kulkarni, Josh Maglione, Eamonn O'Brien, Uri Onn, Giulio Orecchia, Tobias Rossmann, Michael Vaughan-Lee, and James Wilson for mathematical discussions. We thank the anonymous referee for comments that helped us improve this paper's exposition.

References

1. Baer, R.: Groups with abelian central quotient group. Trans. Am. Math. Soc. **44**(3), 357–386 (1938)
2. Boston, N., Isaacs, M.I.: Class numbers of p-groups of a given order. J. Algebra **279**(2), 810–819 (2004)
3. Bardestani, M., Mallahi-Karai, K., Salmasian, J.: Kirillov's orbit method and polynomiality of the faithful dimension of p-groups. Compos. Math. **155**(8), 1618–1654 (2019)
4. Brooksbank, P.A., Maglione, J., Wilson, J.B.: A fast isomorphism test for groups whose Lie algebra has genus 2. J. Algebra **473**, 545–590 (2017)
5. Buckley, A., Plestenjak, B.: Explicit determinantal representations of up to quintic bivariate polynomials. Linear Multilinear Algebra **66**(11), 2266–2285 (2018)
6. Brahana, H.R.: Metabelian groups and pencils of bilinear forms. Am. J. Math. **57**(3), 645–667 (1935)
7. Brown, K.S.: Cohomology of Groups, Graduate Texts in Mathematics, vol. 87. Springer, New York (1982)

8. du Sautoy, M.P.F.: Counting subgroups in nilpotent groups and points on elliptic curves. J. Reine Angew. Math. **549**, 1–21 (2002)
9. du Sautoy, M.P.F., Vaughan-Lee, M.: Non-PORC behaviour of a class of descendant p-groups. J. Algebra **361**, 287–312 (2012)
10. Eick, B., Vaughan-Lee, M.: Counting p-groups and Lie algebras using PORC formulae. J. Algebra **545**, 198–212 (2020)
11. Fulton, W.: Algebraic Curves. An Introduction to Algebraic Geometry. W. A. Benjamin Inc, New York (1969)
12. Grundhöfer, T., Stroppel, M.: Automorphisms of Verardi groups: small upper triangular matrices over rings. Beiträge Algebra Geom. **49**(1), 1–31 (2008)
13. Grunewald, F.J., Segal, D., Smith, G.C.: Subgroups of finite index in nilpotent groups. Invent. Math. **93**(1), 185–223 (1988)
14. Harris, J.: Galois groups of enumerative problems. Duke Math. J. **46**(4), 685–724 (1979)
15. Hesse, O.: Über die Elimination der Variabeln aus drei algebraischen Gleichungen vom zweiten Grade mit zwei Variabeln. J. Reine Angew. Math. **28**, 68–96 (1844)
16. Khukhro, E.I.: p-automorphisms of finite p-groups, London Mathematical Society Lecture Note Series, vol. 246. Cambridge University Press, Cambridge (1998)
17. Lagarias, J.C.: Sets of primes determined by systems of polynomial congruences. Ill. J. Math. **27**(2), 224–239 (1983)
18. Lee, S.: A class of descendant p-groups of order p^9 and Higman's PORC conjecture. J. Algebra **468**, 440–447 (2016)
19. O'Neil, C.: Jacobians of genus one curves. Math. Res. Lett. **8**(1–2), 125–140 (2001)
20. O'Brien, E.A., Voll, C.: Enumerating classes and characters of p-groups. Trans. Am. Math. Soc. **367**(11), 7775–7796 (2015)
21. Plaumann, D., Sturmfels, B., Vinzant, C.: Computing linear matrix representations of Helton-Vinnikov curves, mathematical methods in systems, optimization, and control. In: Dym, H., de Oliveira, M.C., Putinar, M. (eds.) Operator Theory: Advances and Applications, vol. 222, pp. 259–277. Birkhäuser/Springer Basel AG, Basel (2012)
22. Rossmann, T.: The average size of the kernel of a matrix and orbits of linear groups, II: duality. J. Pure Appl. Algebra **224**(4), 106203, 28 (2020)
23. Ravindra, G.V., Tripathi, A.: Torsion points and matrices defining elliptic curves. Int. J. Algebra Comput. **24**(6), 879–891 (2014)
24. Rossmann, T., Voll, C.: Groups, graphs, and hypergraphs: average sizes of kernels of generic matrices with support constraints. arXiv: 1908.09589 (2019)
25. Silverman, J.H.: The Arithmetic of Elliptic Curves, 2nd ed. Graduate Texts in Mathematics, vol. 106. Springer, Dordrecht (2009). (MR 2514094)
26. Stanley, R.P.: Enumerative Combinatorics, Volume 1, Second ed. Cambridge Studies in Advanced Mathematics, vol. 49. Cambridge University Press, Cambridge (2012)
27. The Sage Developers: Sagemath, the Sage Mathematics Software System (Version 8.7) (2019) https://www.sagemath.org. Accessed 21 Dec 2019
28. Vaughan-Lee, M.: Graham Higman's PORC conjecture. Jahresber. Dtsch. Math.-Ver. **114**(2), 89–106 (2012)
29. Vaughan-Lee, M.: Non-PORC behaviour in groups of order p^7. J. Algebra **500**, 30–45 (2018)
30. Voll, C.: Zeta functions of groups and enumeration in Bruhat-Tits buildings. Am. J. Math. **126**, 1005–1032 (2004)
31. Voll, C.: Functional equations for local normal zeta functions of nilpotent groups. Geom. Funct. Anal. **15**, 274–295 (2005). (with an appendix by A. Beauville)
32. Voll, C.: Zeta functions of nilpotent groups–singular Pfaffians, essays in geometric group theory. In: Narasimha-Sastry, N.S. (ed.) Ramanujan Mathematical Society. Lecture Notes Series, vol. 9, pp. 145–159. Ramanujan Mathematical Society, Mysore (2009)
33. Wilson, J.B.: On automorphisms of groups, rings, and algebras. Commun. Algebra **45**(4), 1452–1478 (2017)