SMOOTH CUBOIDS IN GROUP THEORY

JOSHUA MAGLIONE AND MIMA STANOJKOVSKI

ABSTRACT. A smooth cuboid can be identified with a 3×3 matrix of linear forms in 3 variables, with coefficients in a field K, whose determinant describes a smooth cubic in the projective plane. To each such matrix one can associate a group scheme over K. We produce isomorphism invariants of these groups in terms of their *adjoint algebras*, which also give information on the number of their maximal abelian subgroups. Moreover, when K is finite, we give a characterization of the isomorphism types of the groups in terms of isomorphisms of elliptic curves and also describe their automorphism groups. We conclude by applying our results to the determination of the automorphism groups and isomorphism testing of finite p-groups of class 2 and exponent p arising in this way.

CONTENTS

1. INTRODUCTION

The Baer correspondence is a classical way of associating an alternating bilinear map with a nilpotent group or a nilpotent Lie algebra over some field K. In the case of groups of prime power order, this is also referred to as the Lazard correspondence and allows one to study groups in the (often easier) context of Lie algebras. As K-bilinear maps can be represented as matrices of linear forms, the study of groups arising from the Baer correspondence, moreover, affords an additional geometric point of view. In this paper, our focus is on a systematic study of the groups, which we call *E-groups*, obtained by inputting matrices of linear forms, whose determinant defines an elliptic curve in $\mathbb{P}^2_K$. This work also expands on both the results and techniques from [48].

1.1. **Notation.** Throughout p denotes an odd prime number, and G a p-group. Moreover, K denotes an arbitrary field and F a finite field of characteristic p and cardinality q. Let n and d be positive integers. For a vector $\boldsymbol{y} = (y_1, \dots, y_d)$, we denote by $K[\boldsymbol{y}]_1$ the vector space of linear homogeneous polynomials with coefficients in K. We write $\mathrm{Mat}_n(K[\boldsymbol{y}]_1)$ for the $n \times n$ matrices of linear forms in $y_1, \dots, y_d$ with coefficients in K.

2020 *Mathematics Subject Classification.* 20D15, 14M12, 68Q25, 11G20, 15A69, 20D45.

Key words and phrases. Finite p-groups, isomorphism testing, automorphism groups, Baer correspondence, Pfaffians, determinantal representations of cubics.

1.2. **Baer correspondence and Pfaffians.** Given a skew-symmetric matrix of linear forms $\mathrm{B} \in \mathrm{Mat}_{2n}(F[\boldsymbol{y}]_1)$, the Baer correspondence associates B with a p-group $G = \mathrm{G}_\mathrm{B}(F)$ of exponent p and class at most 2 with underlying set F^{2n+d}. A *non-degenerate* matrix B completely prescribes the commutator relations on G and ensures that the bilinear map

$$t_G : G/\operatorname{Z}(G) \times G/\operatorname{Z}(G) \longrightarrow G' = [G, G] \tag{1.1}$$

induced by the commutator map on G is F-bilinear (so not just $\mathbb{F}_p$-bilinear). On the other hand, as we explain below, F and B can also be recovered from G.

Given a finite p-group G of class 2 and exponent p, one can construct a skew-symmetric matrix of linear forms B_G over $\mathbb{F}_p$ from the commutator map of G, for example in terms of a minimal generating set of G. Moreover, if F is an extension of $\mathbb{F}_p$ over which the map in (1.1) is F-bilinear, then we can express B_G as a matrix $\mathrm{B} = \mathrm{B}_F$ of linear forms with coefficients in F. If B has an odd number of rows and columns, then $\det(\mathrm{B}) = 0$; otherwise, there exists a homogeneous polynomial $\mathrm{Pf}(\mathrm{B}) \in F[y_1, \dots, y_d]$ of degree n, called the *Pfaffian*, such that $\det(\mathrm{B}) = \mathrm{Pf}(\mathrm{B})^2$. The equation $\mathrm{Pf}(\mathrm{B}) = 0$ defines a projective, degree n hypersurface in $\mathbb{P}_F^{d-1}$, also called a *linear determinantal hypersurface*. There are now many examples in the literature, cf. [48, Sec. 1.5.4], describing how the intrinsic geometry of B strongly influences many invariants of $\mathrm{G}_\mathrm{B}(F)$, like the number of conjugacy classes [6, 39, 41, 42, 43], faithful dimensions [3], automorphism group sizes [17, 48, 50], and the number of immediate descendants [17, 30]. We look at the Baer correspondence in more detail in Section 2.4.

1.3. **Elliptic groups.** The focus of this paper is, in the language of Section 1.2, to study groups $\mathrm{G}_\mathrm{B}(F)$ with $d = n = 3$ and $\mathrm{Pf}(\mathrm{B}) = 0$ defining an elliptic curve. Moreover, we are concerned with isomorphisms and automorphisms of abstract groups.

Definition 1.1. An *elliptic group* (abbreviated to *E-group*) is a group G that is isomorphic to $\mathrm{G}_\mathrm{B}(K)$ where B is a skew-symmetric matrix of linear forms over a field K such that $\mathrm{Pf}(\mathrm{B}) = 0$ defines an elliptic curve in $\mathbb{P}_K^2$. If K is finite of characteristic p, the group G is called an *elliptic p-group*.

From Definition 1.1 it follows that, if $G \cong \mathrm{G}_\mathrm{B}(F)$ is an E-group, then the matrix B belongs to $\mathrm{Mat}_6(F[y_1, y_2, y_3]_1)$ and $|G| = q^9$.

1.4. **Elliptic groups and variations over the primes.** In the study of p-groups, the groups arising from the Baer correspondence are sometimes specializations $\mathrm{G}_\mathrm{B}(\mathfrak{O}_k/\mathfrak{p})$ to a quotient ring or field of global unipotent group schemes G_B over the ring of integers $\mathfrak{O}_k$ of some number field k. In this respect, it is natural to study how the properties of the group $\mathrm{G}_\mathrm{B}(\mathfrak{O}_k/\mathfrak{p})$ vary with $\mathfrak{p}$. Significant concepts in this regard are those of quasipolynomiality (also called *polynomiality on residue classes*, PORC) [25] and *polynomiality on Frobenius sets* (i.e. polynomiality on finite Boolean combinations of sets of primes defined by the solvability of polynomial congruences; cf. [48, Sec. 1.5.2]). Of particular relevance is Higman's PORC conjecture [26] about the function $\{p \in \mathbb{Z} \mid p \text{ prime}\} \to \mathbb{Z}$ enumerating the isomorphism classes of groups of order p^n for fixed n.

We recall that a function $f : \{p \in \mathbb{Z} \mid p \text{ prime}\} \to \mathbb{Z}$ is *quasipolynomial* if there exists a positive integer N and polynomials $f_0, \dots, f_{N-1} \in \mathbb{Z}[x]$ such that

$$f(p) = f_i(p) \quad \text{whenever} \quad p \equiv i \bmod N.$$

In the context of quasipolynomiality, elliptic groups are for instance employed in [17] to construct a family of p-groups where the number of isomorphism classes is not a quasipolynomial in p. More specifically, the elliptic group scheme G is defined over $\mathbb{Z}$, and the family

arises as a collection of central extensions of $\mathrm{G}(\mathbb{F}_p)$. In earlier work, du Sautoy [15] showed that the number of subgroups, resp. normal subgroups, of index p^3 of $\mathrm{G}(\mathbb{Z})$, for almost all primes p, depends on the number of $\mathbb{F}_p$-points on E, written $|E(\mathbb{F}_p)|$. Du Sautoy [16] extended this to show that, for a parametrized family $(E_D)_D$ of elliptic curves given in short Weierstrass form, (infinitely many terms of) the subgroup zeta functions of a resulting parametrized family $(\mathrm{G}_D)_D$ of E-groups depend on $|E_D(\mathbb{F}_p)|$. In the normal subgroup case, these zeta functions were made explicit by Voll [51] as an application of more general results on smooth curves in the plane, which was further generalized in [52] to smooth projective hypersurfaces with no lines. Recently Voll and the second author [48] showed that the automorphism group sizes of a class of elliptic p-groups are multiples of the number of 3-torsion points of the corresponding curves. For more context, not only involving elliptic groups, we refer to [48, Sec. 1.5.2] and the references therein.

1.5. **Groups from points on curves.** As we explain in Section 4, there is a straightforward way to construct examples of elliptic groups from triples (K, E, P) where K is a field, E is an elliptic curve given by a short Weierstrass equation

$$y^2 = x^3 + ax + b \text{ with } a, b \in K \tag{1.2}$$

and $P = (\lambda, \mu)$ is a point in $E(K)$. In this case, the matrix is defined as follows:

$$\mathrm{B}_{E,P} = \begin{pmatrix} 0 & J_{E,P} \\ -J_{E,P}^{\mathrm{t}} & 0 \end{pmatrix} \text{ where } J_{E,P} = \begin{pmatrix} y_1 - \lambda y_3 & y_2 - \mu y_3 & 0 \\ y_2 + \mu y_3 & \lambda y_1 + (a + \lambda^2) y_3 & y_1 \\ 0 & y_1 & -y_3 \end{pmatrix}. \tag{1.3}$$

The matrix $J_{E,P}$ is a particular instance of a *smooth cuboid*: indeed this 3×3 matrix of linear forms in 3 variables can be interpreted as a $(3, 3, 3)$ *cuboid* as in [38], and it is not difficult to see that by homogenizing the *smooth* curve (1.2), one recovers precisely $\mathrm{Pf}(\mathrm{B}_{E,P}) = 0$. For simplicity, we denote the group $\mathrm{G}_{\mathrm{B}_{E,P}}(K)$ by $\mathrm{G}_{E,P}(K)$.

1.6. **The contributions of this paper.** The main results of this paper are Theorems A, B, D, and E. The first three results are proven in Section 5, while the fourth is given in Section 6 together with the necessary computational conventions.

If E is an elliptic curve, we indicate by $\mathcal{O}$ its identity element. If E is given by a Weierstrass equation as in (1.2), then, in projective coordinates, one has $\mathcal{O} = (0 : 1 : 0)$. If E and E' are elliptic curves in the plane with identity elements $\mathcal{O}$ and $\mathcal{O}'$ respectively, then an isomorphism $E \to E'$ is an isomorphism of projective varieties mapping $\mathcal{O}$ to $\mathcal{O}'$. The automorphism group of the elliptic curve E is denoted $\mathrm{Aut}_{\mathcal{O}}(E)$, and its isomorphism type depends only on the j-invariant $j(E)$ of E. Moreover, if P is a point on E, then we write $\mathrm{Aut}_{\mathcal{O}}(E) \cdot P$ for the orbit of P under the action of $\mathrm{Aut}_{\mathcal{O}}(E)$ on E. For a positive integer n, the n-torsion subgroup of E is denoted by $E[n]$. If $\sigma \in \mathrm{Gal}(F/\mathbb{F}_p)$ and E is an elliptic curve defined by $f = 0$ over F, then $\sigma(E)$ is defined by the polynomial $\sigma(f)$, where σ acts on the coefficients of f. Moreover, if $P = (a : b : c) \in E(F)$ then $\sigma(P) \in \sigma(E)(F)$ is defined by $\sigma(P) = (\sigma(a) : \sigma(b) : \sigma(c))$.

The following two theorems greatly generalize Theorem 1.1 from [48].

Theorem A. *Let F be a finite field with $\mathrm{char}(F) = p \geqslant 5$. Let, moreover, E and E' be elliptic curves in $\mathbb{P}^2_F$ given by Weierstrass equations, and let $P \in E(F) \setminus \{\mathcal{O}\}$ and $P' \in E'(F) \setminus \{\mathcal{O}'\}$. Then the following are equivalent.*

1. *The groups $\mathrm{G}_{E,P}(F)$ and $\mathrm{G}_{E',P'}(F)$ are isomorphic.*
2. *There exist $\sigma \in \mathrm{Gal}(F/\mathbb{F}_p)$ and an isomorphism $\varphi : E' \to \sigma(E)$ of elliptic curves such that $\varphi(P') = \sigma(P)$.*

Theorem B. *Let F be a field with $\mathrm{char}(F) = p \geqslant 5$ and cardinality p^e. Let, moreover, E be an elliptic curve in $\mathbb{P}^2_F$ given by a short Weierstrass equation, and let $P \in E(F) \setminus \{\mathcal{O}\}$. Then there exists a subgroup S of $\mathrm{Gal}(F/\mathbb{F}_p)$ such that the following holds:*

$$\frac{|\operatorname{Aut}(\mathrm{G}_{E,P}(F))|}{p^{18e^2}} = |S| \cdot |E[3](F)| \cdot \frac{|\operatorname{Aut}_{\mathcal{O}}(E)|}{|\operatorname{Aut}_{\mathcal{O}}(E) \cdot P|} \cdot \begin{cases} |\operatorname{GL}_2(F)| & \text{if } P \in E[2](F), \\ 2(p^e-1)^2 & \text{otherwise.} \end{cases}$$

For the precise definition of the subgroup S from Theorem B we refer the reader to (2.5); see also Theorem 2.15 and, for an example, Remark 5.11. For the groups $\mathrm{G}_{E,P}(F)$, a generator of the subgroup S can be computed efficiently. This is not necessarily the case for groups $\mathrm{G}_{\mathrm{B}}(F)$, where B is arbitrary.

Combining Theorem B with [54, Th. 2.2.1] and the classification from [2], one obtains that, although the function in (1.4) counting the number of automorphisms of the family $(\mathrm{G}_{E,P}(\mathbb{F}_p))_p$ is polynomial on Frobenius sets, it is almost never quasipolynomial; cf. Corollary C and Remark 1.2 for some more detail.

Corollary C. *Let E be an elliptic curve given by the Weierstrass equation*

$$y^2 = x^3 + ax + b, \quad a, b \in \mathbb{Q}$$

and $P \in E(\mathbb{Q}) \setminus \{\mathcal{O}\}$. Over the set of primes for which E has good reduction, the function

$$p \longmapsto |\operatorname{Aut}(\mathrm{G}_{E,P}(\mathbb{F}_p))| \tag{1.4}$$

is polynomial on Frobenius sets and is quasipolynomial precisely in the following cases:

1. *$a = 0$ and there exists $\beta \in \mathbb{Q}^\times$ such that $b = 2\beta^3$,*
2. *$b \neq 0$ and there exist $h, \ell \in \mathbb{Q}^\times$ such that*

$$h^3 = -16(4a^3 + 27b^2) \text{ and } \ell^2 = (-h - 4a)/3$$

and one of the following holds:

(a) *there exist $\alpha, \beta, m \in \mathbb{Q}$ with $\beta \neq 0$ that satisfy:*

$$m^2 = \alpha^2 + 3\beta^2, \quad a = -3m^2 + 6\beta m, \quad b = 2\alpha^3 + 12\alpha\beta^2 - 6\alpha\beta m;$$

(b) *for $\gamma = -\ell^2 - 4a - 8b/\ell$, the element $-\ell^3 - 8a\ell - 16b + (-\ell^2 + 4b/\ell)\sqrt{\gamma}$ is a square in the splitting field of $(x^2 - \gamma)(x^3 - 1)$.*

Remark 1.2. The case distinction in Corollary C comes from the explicit description, given in [2], of curves E in short Weierstrass form for which the Galois group of

$$\mathbb{Q}(E[3]) = \mathbb{Q}(\{x, y : (x, y) \in E[3](\mathbb{Q}^{\mathrm{sep}})\})$$

is abelian. Thanks to [54, Th. 2.2.1], i.e. the Abelian Polynomial Theorem from [58], $\mathrm{Gal}(\mathbb{Q}(E[3])/\mathbb{Q})$ is abelian if and only if the function $p \mapsto |E[3](\mathbb{F}_p)|$ is quasipolynomial. With one of the classical definitions of heights for elliptic curves (defined for short Weierstrass equations as $\mathrm{ht}(E) = \max\{|a|^3, |b|^2\}$), Theorem 1 from [18] implies that the density of isomorphism classes of rational elliptic curves for which $\mathrm{Gal}(\mathbb{Q}(E[3])/\mathbb{Q})$ is abelian is 0. In particular, this tells us that examples of groups $\mathrm{G}_{E,P}$ as in Corollary C for which $p \mapsto |\operatorname{Aut}(\mathrm{G}_{E,P}(\mathbb{F}_p))|$ is quasipolynomial are very rare.

Theorems A and B and Corollary C concern the groups from Section 1.5, which might not appear to be representative of the class of E-groups. However, up to equivalence, which we define in Section 4, these groups seem to occur with probability 1/2 in the precise sense explained in Section 6.4.

One of the main tools we use to extract the core geometric properties of the groups $\mathrm{G}_{E,P}(F)$ is the adjoint algebra, which has recently been used to understand the structure

of p-groups [9, 10]. We define adjoint algebras in Section 2.2, but remark that their isomorphism types are polynomial-time computable isomorphism invariants of p-groups since they are constructed by solving linear systems. With the notation from Section 2.2, Theorem D follows from combining the more general Theorem 3.13 with Proposition 5.1. The relevance of $\mathcal{O}$ being a flex point is explained in Remark 4.9. In Theorem D, we use the fact that a smooth cubic in the projective plane with a marked rational point has the structure of an elliptic curve.

Theorem D. *Let K be a field with $6K = K$. Let, moreover, $\mathrm{B} \in \mathrm{Mat}_6(K[y_1, y_2, y_3]_1)$ be skew-symmetric with $\mathrm{Pf}(\mathrm{B}) = 0$ defining a smooth cubic E in $\mathbb{P}^2_K$ with a flex point $\mathcal{O} \in E(K)$, and set $G = \mathrm{G}_{\mathrm{B}}(K)$. Then the following hold:*

(1) *There is $P \in E(K) \setminus E[2](K)$ with $G \cong \mathrm{G}_{E,P}(K)$ if and only if $\mathrm{Adj}(\mathrm{B}) \cong \mathbf{X}_1(K)$.*
(2) *There is $P \in E[2](K) \setminus \{\mathcal{O}\}$ with $G \cong \mathrm{G}_{E,P}(K)$ if and only if $\mathrm{Adj}(\mathrm{B}) \cong \mathbf{S}_2(K)$.*

Our next main theorem allows us to constructively recognize elliptic p-groups and to decide whether two such groups are isomorphic. Deciding whether two groups of order n are isomorphic uses, in the worst case, $n^{O(\log n)}$ operations [36], which is just a brute-force search, and the same timing prevails for constructing generators of the automorphism group. General purpose algorithms, like [12] and [19], use induction by constructing known characteristic subgroups, which are subgroups fixed by the automorphism group. Even with recent tools to uncover more characteristic subgroups [9, 33, 34, 56], elliptic p-groups evade capture. Prior to this work, it seems that the best general purpose algorithm [28], together with the reduction from Theorem 2.15, would construct generators for their automorphism group using $O(|G|^{8/9} \log |G|)$ operations (without Theorem 2.15 the number of operations is $|G|^{O(\log |G|)}$). We significantly improve upon this timing.

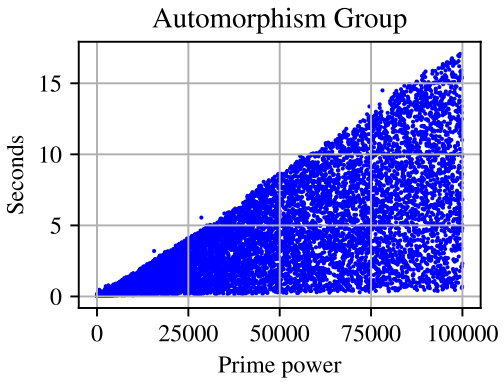

FIGURE 1. The runtimes of a Magma implementation of Theorem E on the prime powers p^e, for $p \notin \{2, 3\}$, up to 10^5.

Theorem E. *There are algorithms that, given groups G_1 and G_2 of order p^{9m}, with $p \geqslant 5$,*

(i) decide if, for each $i \in \{1, 2\}$ and field F of cardinality p^m, there exist
- *an elliptic curve E_i given by a short Weierstrass equation with F-coefficients,*
- *a point $P_i \in E_i(F) \setminus \{(0 : 1 : 0)\}$,*

such that G_i is isomorphic to $\mathrm{G}_{E_i,P_i}(F)$, and if so

(ii) return the possibly empty coset of isomorphisms $G_1 \to G_2$.

The algorithm for (i) is of Las Vegas type and uses $O(m^7 + m \log p)$ field operations. The algorithm for (ii) uses $O(p^m)$ field operations.

Some of the algorithms we use are of *Las Vegas* type. These are randomized algorithms that only return correct answers and for some probability, determined by a user-prescribed upper bound, terminate without an answer.

In Theorem E(*ii*), if the groups are isomorphic, the algorithm returns an isomorphism $G_1 \to G_2$ together with a generating set for $\mathrm{Aut}(G_1)$. In order to demonstrate the efficacy of Theorem E, we have constructed generators for the automorphism groups of several instances of $\mathrm{G}_{E,P}(F)$, built uniformly at random as explained in Section 6.4.

Remark 1.3. As the careful reader has noticed, in our main theorems p is at least 5. The prime 2 is excluded to begin with because there does not exist a group of class 2 and exponent 2. Moreover, if $p \in \{2, 3\}$, elliptic curves need not admit a short Weierstrass form and, in this case, their 3×3 determinantal representations might not be equivalent to any $J_{E,P}$; see Section 1.5 and Section 4.2.

Acknowledgements. We wish to thank Daniele Agostini for his precious help in connection to the proof of Theorem A; Mima especially thanks Daniele for always joyfully welcoming her questions. We also thank Fulvio Gesmundo, Carlo Pagano, and Rosa Winter for pointing out [38], [18], and [2] to us. We thank Andrea Bandini for some clarifications around [2]. We, moreover, thank Francesco Galuppi, Tobias Rossmann, Christopher Voll for their precious comments on an early version of this manuscript. We thank Lars Bügemannskemper for pointing out a typo involving the order of the central automorphisms. We are grateful to the anonymous referees for their careful study of our paper and for their kind and detailed reports, which helped us fix some imprecisions and led to an improvement of the paper.

This project was initiated during a Research in Pairs visit at MFO in March 2022 and was partially supported by the Daimler and Benz Foundation. The first author was supported by the DFG-Graduiertenkolleg "Mathematical Complexity Reduction" and the DFG grant VO 1248/4-1 (project number 373111162). The second author was supported by the DFG – Project-ID 286237555 – TRR 195 and by the Italian program "Rita Levi Montalcini", edition 2020.

2. Tensors and unipotent group schemes

Fix finite-dimensional K-vector spaces U, W, V, V', and T. By a 3-*tensor* (or simply *tensor*, throughout), we mean a K-bilinear map $t : V \times V' \to T$, that is, for all $u, v \in V$, all $u', v' \in V'$, and all $\lambda, \mu \in K$, the following holds

$$t(u + \lambda v, u' + \mu v') = t(u, u') + \lambda t(v, u') + \mu t(u, v') + \lambda\mu t(v, v').$$

A tensor $t : V \times V \to T$ is *alternating* if, for all $v \in V$, one has $t(v, v) = 0$.

Definition 2.1. Let $t : V \times V \to T$ be a tensor. A subspace $U \leqslant V$ is *totally isotropic* with respect to t if, for every $u, u' \in U$, one has $t(u, u') = 0$, in other words if the restriction of t to $U \times U$ is the zero map.

Note that, if $t : V \times V \to T$ is alternating, every line in V is totally isotropic.

Definition 2.2. An alternating tensor $t : V \times V \to T$ is *isotropically decomposable* if there exist totally isotropic subspaces $U, W \leqslant V$ such that $V = U \oplus W$.

By choosing bases for U, W, and T, we may write $t : U \times W \to T$ as a matrix of linear forms or as a system of forms; that is, a sequence of matrices over K. Let $\{e_1, \ldots, e_m\}$,

$\{f_1, \ldots, f_n\}$, and $\{g_1, \ldots, g_d\}$ be bases for U, W, and T, respectively. For $i \in [m]$, $j \in [n]$, and $k \in [d]$, define $b_{ij}^{(k)} \in K$ such that

$$t(e_i, f_j) = \sum_{k=1}^{d} b_{ij}^{(k)} g_k.$$

The matrix of linear forms $\mathrm{B} = (b_{ij}) \in \mathrm{Mat}_{m\times n}(K[\boldsymbol{y}]_1)$ corresponding to t is given by

$$b_{ij} = \sum_{k=1}^{d} b_{ij}^{(k)} y_k.$$

In the sequel we will always assume that a tensor $t : U \times W \to T$ is given together with a choice of bases for U, W, T. If $t : V \times V \to T$ is an alternating tensor, we take the same basis on the first and the second copy of V and, if V is given by an isotropic decomposition $U \oplus W$, we assume that the basis on V is the composite of a basis of U and a basis of W.

Remark 2.3. Since every 3-tensor t is, with respect to a choice of bases, given by a matrix B of linear forms, throughout the paper everything that is defined for tensors will also apply to matrices of linear forms.

If $t : V \times V \to T$ is an alternating tensor, just as matrices of linear forms associated with t vary as the bases for V and T vary, so does the corresponding Pfaffian. We will say that $\mathrm{Pf}(t) \in K[\boldsymbol{y}]$ is a Pfaffian for t if there exists some choice of bases for V and T whose associated matrix of linear forms B satisfies $\mathrm{Pf}(t) = \mathrm{Pf}(\mathrm{B})$.

Definition 2.4. A tensor $t : U \times W \to T$ is *nondegenerate* if the following are satisfied:

(i) $t(u, W) = 0$ implies $u = 0$, and
(ii) $t(U, w) = 0$ implies $w = 0$.

We say that t is *full* if $t(U, W) = T$. A tensor t is *fully nondegenerate* if t is both nondegenerate and full.

2.1. **Maps between 3-tensors.** In this section we present various types of maps between tensors that we will exploit in later sections for the determination of isomorphisms between groups and Lie algebras. Many of these definitions can be found in [9].

Definition 2.5. Two K-tensors $s : U \times W \to T$ and $t : U' \times W' \to T'$ are *equivalent* if $T = T'$ and there exist K-linear isomorphisms $\alpha : U \to U'$ and $\beta : W \to W'$ such that for all $u \in U$ and all $w \in W$, one has $t(\alpha(u), \beta(w)) = s(u, w)$; equivalently, the following diagram commutes

$$\begin{array}{ccc} U \times W & \xrightarrow{\ s\ } & T \\ {\scriptstyle\alpha}\downarrow \quad \downarrow{\scriptstyle\beta} & & \downarrow{\scriptstyle\mathrm{id}} \\ U' \times W' & \xrightarrow{\ t\ } & T' \end{array}$$

In the case $U = W$, $U' = W'$, and $\alpha = \beta$, we say the two tensors are *isometric*.

Relevant to our context is a different form of equivalence from Definition 2.5, namely, *pseudo-isometry*. Isomorphisms of groups induce this weaker equivalence, which is considered in more detail in the next section.

Definition 2.6. Let $L \subset K$ be a subfield and let $s : V \times V \to T$ and $t : V' \times V' \to T'$ be K-tensors. An *L-pseudo-isometry* from s to t is a pair (α, β) such that $\alpha : V \to V'$ and

$\beta : T \to T'$ are L-linear isomorphisms and for all $u, v \in V$, the equality $t(\alpha(u), \alpha(v)) = \beta(s(u, v))$ holds; equivalently the following diagram commutes:

$$\begin{array}{ccc} V \times V & \xrightarrow{\quad s \quad} & T \\ {\scriptstyle\alpha}\downarrow \quad \downarrow{\scriptstyle\alpha} & & \downarrow{\scriptstyle\beta} \\ V' \times V' & \xrightarrow{\quad t \quad} & T' \end{array}$$

The set of L-pseudo-isometries from s to t is denoted $\Psi\mathrm{Isom}_L(s, t)$ and, if $\Psi\mathrm{Isom}_L(s, t)$ is non-empty, s and t are called *L-pseudo-isometric*. If $s = t$, then the group of L-pseudo-isometries of t is denoted by $\Psi\mathrm{Isom}_L(t)$ instead of $\Psi\mathrm{Isom}_L(t, t)$.

Remark 2.7. We emphasize that $\Psi\mathrm{Isom}_L(s, t)$ has more structure than an arbitrary set. Indeed, identifying V with V' and T with T', we can view $\Psi\mathrm{Isom}_L(s, t)$ both as a left $\Psi\mathrm{Isom}_L(t)$-coset and a right $\Psi\mathrm{Isom}_L(s)$-coset of $\mathrm{GL}_L(V) \times \mathrm{GL}_L(T)$. That is, if $(\alpha, \beta) \in \Psi\mathrm{Isom}_L(s, t)$, while $(\gamma, \delta) \in \Psi\mathrm{Isom}_L(t)$ and $(\varepsilon, \zeta) \in \Psi\mathrm{Isom}_L(s)$, then the following holds:

$$(\gamma\alpha, \delta\beta), (\alpha\varepsilon, \beta\zeta) \in \Psi\mathrm{Isom}_L(s, t).$$

Because $\Psi\mathrm{Isom}_L(t) \cdot (\alpha, \beta) = (\alpha, \beta) \cdot \Psi\mathrm{Isom}_L(s) = \Psi\mathrm{Isom}_L(s, t)$, we will just refer to $\Psi\mathrm{Isom}_L(s, t)$ as a coset.

Remark 2.8. If G is a p-group with central elementary abelian derived subgroup, then its commutator determines a fully nondegenerate $\mathbb{F}_p$-tensor $t_G : G/\operatorname{Z}(G) \times G/\operatorname{Z}(G) \to G'$ given by $(g \operatorname{Z}(G), h \operatorname{Z}(G)) \mapsto [g, h]$. If G and H are two such p-groups whose tensors t_G and t_H are $\mathbb{F}_p$-pseudo-isometric, then G and H are *isoclinic*, cf. [22]. If, in addition, both G and H have exponent p, then G and H are isomorphic.

Definition 2.9. Let $L \subset K$ be a subfield and let $s : U \times W \to T$ and $t : U' \times W' \to T'$ be K-tensors. An *L-isotopism* from s to t is a triple (α, β, γ) such that $\alpha : U \to U'$, $\beta : W \to W'$, and $\gamma : T \to T'$ are L-linear isomorphisms and for all $(u, w) \in U \times W$, the equality $t(\alpha(u), \beta(w)) = \gamma(s(u, w))$ holds; equivalently the following diagram commutes:

$$\begin{array}{ccc} U \times W & \xrightarrow{\quad s \quad} & T \\ {\scriptstyle\alpha}\downarrow \quad \downarrow{\scriptstyle\beta} & & \downarrow{\scriptstyle\gamma} \\ U' \times W' & \xrightarrow{\quad t \quad} & T' \end{array}$$

If $s = t$, then the triple (α, β, γ) is called an *L-autotopism* of t and the group of L-autotopisms of t is denoted by $\mathrm{Auto}_L(t)$.

Remark 2.10. Assume $\mathrm{M} \in \mathrm{Mat}_n(F[y_1, \ldots, y_d]_1)$ realizes the tensor $\tilde{t} : U \times W \to T$. Then the autotopism group of M can be described as

$$\mathrm{Auto}_F(\mathrm{M}) = \left\{ (X, Y, Z) \in \mathrm{GL}_n(F) \times \mathrm{GL}_n(F) \times \mathrm{GL}_d(F) \;\middle|\; X^{\mathrm{t}} \mathrm{M}(\boldsymbol{y}) Y = \mathrm{M}(Z\boldsymbol{y}) \right\}.$$

In particular, if $U \oplus W = V$ is an isotropic decomposition for the tensor $t : V \times V \to T$ inducing $\tilde{t}$ and with associated matrix B, then every triple $(X, Y, Z) \in \mathrm{Auto}_F(\tilde{t})$ yields an element of $\Psi\mathrm{Isom}_F(t)$ via the following:

$$\begin{aligned} \begin{pmatrix} X^{\mathrm{t}} & 0 \\ 0 & Y^{\mathrm{t}} \end{pmatrix} \mathrm{B} \begin{pmatrix} X & 0 \\ 0 & Y \end{pmatrix} &= \begin{pmatrix} X^{\mathrm{t}} & 0 \\ 0 & Y^{\mathrm{t}} \end{pmatrix} \begin{pmatrix} 0 & \mathrm{M} \\ -\mathrm{M}^{\mathrm{t}} & 0 \end{pmatrix} \begin{pmatrix} X & 0 \\ 0 & Y \end{pmatrix} \\ &= \begin{pmatrix} 0 & X^{\mathrm{t}} \mathrm{M}(\boldsymbol{y}) Y \\ -Y^{\mathrm{t}} \mathrm{M}(\boldsymbol{y})^{\mathrm{t}} X & 0 \end{pmatrix} = \begin{pmatrix} 0 & \mathrm{M}(Z\boldsymbol{y}) \\ -\mathrm{M}(Z\boldsymbol{y})^{\mathrm{t}} & 0 \end{pmatrix} = \mathrm{B}(Z\boldsymbol{y}). \end{aligned}$$

2.2. **Algebras associated to 3-tensors.** Throughout this subsection, we use tensors rather than matrices of linear forms, but the content applies to both. These algebras are also found in [9].

Let $t : U \times W \to T$ be a K-tensor. The *centroid* of t is the K-subalgebra of $\mathcal{E} = \mathrm{End}_K(U) \times \mathrm{End}_K(W) \times \mathrm{End}_K(T)$ defined by

$$\mathrm{Cent}(t) = \left\{ (\alpha, \beta, \gamma) \in \mathcal{E} \;\middle|\; \begin{array}{c} \forall u \in U,\ \forall w \in W, \\ t(\alpha(u), w) = t(u, \beta(w)) = \gamma(t(u, w)) \end{array} \right\}. \tag{2.1}$$

Let $c = (\alpha, \beta, \gamma) \in \mathrm{Cent}(t)$, and suppose $\mathrm{Cent}(t)$ acts on U, W, and T by respectively applying α, β, and γ. Then for each pair $(u, w) \in U \times W$, we have

$$c \cdot t(u, w) = t(c \cdot u, w) = t(u, c \cdot w).$$

Thus, t is $\mathrm{Cent}(t)$-bilinear. Additionally, the centroid satisfies the following universal property. If t is also A-bilinear for some K-algebra A, then there is a unique ring homomorphism $A \to \mathrm{Cent}(t)$ such that the action of A on U, W, and T is that of $\mathrm{Cent}(t)$; cf. [55, Lem. 6.8(ii)].

Lemma 2.11. *If t is fully-nondegenerate, then $\mathrm{Cent}(t)$ is commutative.*

Proof. Take $(\alpha, \beta, \gamma), (\alpha', \beta', \gamma') \in \mathrm{Cent}(t)$; then for all $u \in U$ and all $w \in W$,

$$t(\alpha\alpha'(u), w) = t(\alpha'(u), \beta(w)) = \gamma'(t(u, \beta(w))) = \gamma'(t(\alpha(u), w)) = t(\alpha'\alpha(u), w).$$

This implies that $t((\alpha\alpha' - \alpha'\alpha)(u), w) = 0$, and since t is fully-nondegenerate, it follows that $\alpha\alpha' = \alpha'\alpha$. Similar arguments hold for the other coordinates as well. □

For a ring R, we denote by R^{op} the *opposite ring* of R, with opposite product given by $x \cdot_{\mathrm{op}} y = yx$ for all $x, y \in R$. The *adjoint algebra* of t is the K-algebra

$$\mathrm{Adj}(t) = \left\{ (\alpha, \beta) \in \mathrm{End}(U) \times \mathrm{End}(W)^{\mathrm{op}} \;\middle|\; \begin{array}{c} \forall u \in U,\ \forall w \in W, \\ t(\alpha(u), w) = t(u, \beta(w)) \end{array} \right\}. \tag{2.2}$$

If $t : V \times V \to T$ is alternating, then the natural anti-isomorphism $* : \mathrm{Adj}(t) \to \mathrm{Adj}(t)^{\mathrm{op}}$, given by $(\alpha, \beta) \mapsto (\beta, \alpha)$, makes $\mathrm{Adj}(t)$ a *$*$-algebra*, cf. Section 2.3. To see this, let $(\alpha, \beta) \in \mathrm{Adj}(t)$. Then for all $u, v \in V$, one has

$$t(\beta(u), v) = -t(v, \beta(u)) = -t(\alpha(v), u) = t(u, \alpha(v)),$$

from which it follows that $(\beta, \alpha) \in \mathrm{Adj}(t)^{\mathrm{op}}$.

We define a module version of the adjoint algebra. For this, let $t : U \times W \to T$ and $s : U' \times W' \to T'$ be K-tensors. Identifying T with T', the *adjoint module* of s and t is

$$\mathrm{Adj}(s, t) = \left\{ (\alpha, \beta) \in \mathrm{Hom}(U', U) \times \mathrm{Hom}(W, W') \;\middle|\; \begin{array}{c} \forall u' \in U',\ \forall w \in W, \\ t(\alpha(u'), w) = s(u', \beta(w)) \end{array} \right\}. \tag{2.3}$$

We remark that $\mathrm{Adj}(s, t)$ is a left $\mathrm{Adj}(t)$-module and a right $\mathrm{Adj}(s)$-module via defining

$$(\gamma, \delta) \cdot (\alpha, \beta) = (\gamma\alpha, \beta\delta) \quad \text{and} \quad (\alpha, \beta) \cdot (\varepsilon, \zeta) = (\alpha\varepsilon, \zeta\beta),$$

for all $(\alpha, \beta) \in \mathrm{Adj}(s, t)$, all $(\gamma, \delta) \in \mathrm{Adj}(t)$, and all $(\varepsilon, \zeta) \in \mathrm{Adj}(s)$.

The key computational advantage to the vector spaces in (2.1), (2.2), and (2.3) is that they are simple to compute, since they are given by a system of linear equations, and carry useful structural information. Although they are computed by solving a linear system, this is the computational bottleneck for Theorem E(i).

2.3. **Structure of Artinian $*$-rings.** We will need specific structural information about $*$-rings. We follow the treatment given in [10, Sec. 2] and, only in Section 2.3, use right action in accordance to the existing literature on $*$-algebras.

A *$*$-ring* is a pair $(A, *)$ where A is an Artinian ring and $* : A \to A^{\mathrm{op}}$ is a ring homomorphism such that, for all $a \in A$, the equality $(a^*)^* = a$ holds. A *$*$-homomorphism* $\varphi : (A, *_A) \to (B, *_B)$ is a ring homomorphism $A \to B$ such that $\varphi(a^{*_A}) = \varphi(a)^{*_B}$. A *$*$-ideal* is an ideal I of A such that $I^* = I$. A $*$-ring A is *simple* if its only $*$-ideals are 0 and A. Moreover, from [10, Th. 2.1], the Jacobson radical of a $*$-ring is a $*$-ideal, and the quotient by the Jacobson radical R decomposes into a direct sum of simple $*$-rings. If A is a $*$-ring with Jacobson radical R such that $S = A/R$, then we write $A \cong R \rtimes S$.

For finite fields of odd characteristic, we can completely describe the simple $*$-rings. Using the notation from [10], we have the following classification.

Theorem 2.12 ([10, Th. 2.2])**.** *Let $(A, *)$ be a simple $*$-algebra over F. Then there is a positive integer n such that $(A, *)$ is $*$-isomorphic to one of the following:*

- *(i)* $\mathbf{O}_n^{\varepsilon}(F) = (\mathrm{Mat}_n(F), X \mapsto DX^{\mathrm{t}}D^{-1})$*, where D is one of the diagonal matrices in $\{I_n, I_{n-1} \oplus \omega\}$, for a non-square $\omega \in F$, and $\varepsilon \in \{+, -, \circ\}$ according to whether the form $(u, v) \mapsto u^{\mathrm{t}}Dv$ induces an orthogonal geometry of type ε.*
- *(ii)* $\mathbf{U}_n(L) = (\mathrm{Mat}_n(L), X \mapsto \overline{X}^{\mathrm{t}})$*, where $\alpha \mapsto \overline{\alpha}$ is the nontrivial Galois automorphism of the degree two extension L/F.*
- *(iii)* $\mathbf{S}_{2n}(F) = (\mathrm{Mat}_{2n}(F), X \mapsto JX^{\mathrm{t}}J^{-1})$*, where J is the n-fold direct sum of $\left(\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right)$.*
- *(iv)* $\mathbf{X}_n(F) = (\mathrm{Mat}_n(F) \oplus \mathrm{Mat}_n(F), (X, Y) \mapsto (Y^{\mathrm{t}}, X^{\mathrm{t}}))$.

We stress that in this paper we are mostly concerned with *(iii)* and *(iv)* from the last classification. We mention *(i)* primarily for Theorem 3.13 for the values $n = 1$ and $\varepsilon = \circ$, in which case $\mathbf{O}_n^{\varepsilon}(K) = \mathbf{O}_1^{\varepsilon}(K)$ is a field isomorphic to K.

2.4. **Unipotent group schemes and nilpotent Lie algebras from 3-tensors.** Let $t : V \times V \to T$ be an alternating K-tensor and assume that $K = 2K$. Then the set $V \oplus T$, with multiplication given by

$$(v, w) \cdot (v', w') = (v + v', w + w' + \frac{1}{2}t(v, v')),$$

is a nilpotent group (of class at most 2), called the *Baer group associated with t*. The commutator map of $\mathrm{G}_t(K) = (V \oplus T, \cdot)$ is given by

$$((v, w), (v', w')) \longmapsto \big[(v, w), (v', w')\big] = (0, t(v, v')).$$

Interpreting the last commutator map as a Lie bracket, the Lie algebra $\mathfrak{g}_t(K)$ associated to t is precisely $V \oplus T$ together with this Lie product. We note that this construction is the same as in [48], where t is assumed to be isotropically decomposable (and the associated half-matrix B to be symmetric).

The (Baer) group scheme G_t associated to t is determined in the following way – without requiring $K = 2K$; see [43, Sec. 2.4]. Fix bases $(v_1, \ldots, v_n)$ and $(w_1, \ldots, w_d)$ of V and T respectively. Let L be an associative commutative unital K-algebra, and identify $\mathrm{G}_t(L)$ with the set $(V \otimes_K L) \oplus (T \otimes_K L)$. For $\ell \in L$, we abbreviate $v_i \otimes \ell$ and $w_j \otimes \ell$ to ℓv_i and ℓw_j in $V \otimes_K L$ and $T \otimes_K L$ respectively.

We define the multiplication $\bullet$ on $\mathrm{G}_t(L)$ as follows. For $v = a_1v_1 + \cdots + a_nv_n$ and $v' = b_1v_1 + \cdots + b_nv_n$ with $a_1, \ldots, a_n, b_1, \ldots, b_n \in L$, we set

$$v \bullet v' = v + v' - \sum_{1 \leqslant i < j \leqslant n} a_jb_i \cdot t(v_i, v_j).$$

Additionally, for all $x \in \mathrm{G}_t(L)$ and $w \in T \otimes_K L$, define $x \bullet w = x + w = w \bullet x$. This determines the group structure and is independent of the chosen bases: shall the tensors be given in terms of a matrix B of linear forms, we will write $\mathrm{G}_{\mathrm{B}}(L)$ for the resulting group. The last construction defines a representable functor from the category of K-algebras (associative, commutative, and unital) to groups; namely, via $L \mapsto ((V \otimes_K L) \oplus (T \otimes_K L), \bullet)$. Concretely, if $K = 2K$, then $\mathrm{G}_t(K)$ is isomorphic to the Baer group associated with t since the two groups yield pseudo-isometric commutator tensors. One approaches Lie algebras in a similar fashion.

Our main source of unipotent group schemes comes from linear determinantal representations of elliptic curves, but this change of perspective from determinantal representations to nilpotent groups comes with a few subtleties. For example, the specific Pfaffian hypersurface associated to the linear Pfaffian representation is an invariant in the equivalence class as given in Definition 3.4. However for nilpotent groups of class 2, the Pfaffian hypersurface is not an invariant of the group – the next theorem, essentially due to Baer [1], illustrates this point.

Theorem 2.13. *Let $s : V \times V \to T$ and $t : V' \times V' \to T'$ be alternating, full K-tensors, where $\mathrm{char}(K) = p > 2$. Then the following hold.*

1. *The K-Lie algebras $\mathfrak{g}_s(K)$ and $\mathfrak{g}_t(K)$ are isomorphic if and only if s and t are K-pseudo-isometric.*
2. *The groups $\mathrm{G}_s(K)$ and $\mathrm{G}_t(K)$ are isomorphic if and only if s and t are $\mathbb{F}_p$-pseudo-isometric.*

Proof. We prove the claim for groups as the Lie algebras statement is similar. Since s and t are full, the commutator subgroups of $\mathrm{G}_s(K)$ and $\mathrm{G}_t(K)$ are equal to $0 \oplus T$ and $0 \oplus T'$, respectively. An isomorphism from $\mathrm{G}_s(K)$ to $\mathrm{G}_t(K)$ induces an isomorphism of their commutator subgroups and their abelianizations. These yield $\mathbb{F}_p$-linear isomorphisms $V \to V'$ and $T \to T'$, so s and t are $\mathbb{F}_p$-pseudo-isometric.

Conversely if $\alpha : V \to V'$ and $\beta : T \to T'$ are $\mathbb{F}_p$-linear isomorphisms with $(\alpha, \beta) \in \Psi\mathrm{Isom}_{\mathbb{F}_p}(s, t)$, then for all $v, v' \in V$ and all $w, w' \in T$, the following holds:

$$\begin{aligned}(\alpha(v), \beta(w)) \cdot (\alpha(v'), \beta(w')) &= (\alpha(v + v'), \beta(w + w') + \frac{1}{2} t(\alpha(v), \alpha(v'))) \\ &= (\alpha(v + v'), \beta(w + w' + \frac{1}{2} s(v, v'))).\end{aligned}$$

In other words, $\mathrm{diag}(\alpha, \beta)$ yields an isomorphism of groups. □

For an F-vector space V with a fixed basis $\mathcal{B}$, we extend the action of $\mathrm{Gal}(F/\mathbb{F}_p)$ from F to V in the following way:

$$\mathrm{Gal}(F/\mathbb{F}_p) \longrightarrow \mathrm{Aut}_{\mathbb{F}_p}(V), \quad \sigma \longmapsto \left(u = \sum_{b \in \mathcal{B}} c_b b \mapsto \sigma(u) = \sum_{b \in \mathcal{B}} \sigma(c_b) b \right).$$

Definition 2.14. Let $t : V \times V \to T$ be an F-tensor and let $\sigma \in \mathrm{Gal}(F/\mathbb{F}_p)$. For a fixed choice of bases for V and T, the tensor ${}^{\sigma}t : V \times V \to T$ is defined by

$${}^{\sigma}t(u, v) = \sigma t(\sigma^{-1}(u), \sigma^{-1}(v)).$$

On the level of matrices of linear forms, if $t(u, v) = u^{\mathrm{t}} \mathrm{B}\, v$, then ${}^{\sigma}t(u, v) = u^{\mathrm{t}}(\sigma(\mathrm{B}))v$, where the action of σ on B is entry-wise, so $\sigma(\mathrm{B}) = (\sigma(b_{ij}))$.

The action of $\mathrm{Gal}(F/\mathbb{F}_p)$ on an F-tensor $t : V \times V \to T$ depends on the choice of F-bases for V and T, and different choices of bases may yield different F-pseudo-isometry classes. This shall not concern us because this does not happen on the level of $\mathbb{F}_p$-pseudo-isometries – our primary focus when working with $\mathrm{Gal}(F/\mathbb{F}_p)$ – as σ is $\mathbb{F}_p$-linear.

The next theorem has many appearances in different guises [7, 48, 57], and it describes the group $\Psi\mathrm{Isom}_{\mathbb{F}_p}(t)$ as a subgroup of a direct product of F-semilinear groups. The *F-semilinear group* of V is $\mathrm{GL}_F(V) \rtimes \mathrm{Gal}(F/\mathbb{F}_p)$, and for a fixed basis of V, it acts on V by mapping v to $(X, \sigma)v = X\sigma(v)$. For $(X, \sigma), (Y, \tau) \in \mathrm{GL}_F(V) \rtimes \mathrm{Gal}(F/\mathbb{F}_p)$, we compute that $(X, \sigma) \cdot (Y, \tau) = (X\sigma Y\sigma^{-1}, \sigma\tau)$, and we extend this operation to the larger $(\mathrm{GL}_F(V) \times \mathrm{GL}_F(T)) \rtimes \mathrm{Gal}(F/\mathbb{F}_p)$ by setting

$$(\alpha, \beta, \sigma) \cdot (\gamma, \delta, \tau) = (\alpha\sigma\gamma\sigma^{-1}, \beta\sigma\delta\sigma^{-1}, \sigma\tau). \tag{2.4}$$

Then the *F-semilinear pseudo-isometry group* of t is

$$\mathrm{S\Psi I}_{F/\mathbb{F}_p}(t) = \{(\alpha, \beta, \sigma) \in (\mathrm{GL}_F(V) \times \mathrm{GL}_F(T)) \rtimes \mathrm{Gal}(F/\mathbb{F}_p) \mid (\alpha, \beta) \in \Psi\mathrm{Isom}_F({}^{\sigma}t, t)\}$$

with the induced multiplication. Note that, though the definition of $\mathrm{S\Psi I}_{F/\mathbb{F}_p}(t)$ we gave clearly depends on a choice of bases of V and T, its isomorphism type does not. We will write $\mathrm{Gal}_t(F/\mathbb{F}_p)$ for the following:

$$\mathrm{Gal}_t(F/\mathbb{F}_p) = \{\sigma \in \mathrm{Gal}(F/\mathbb{F}_p) \mid \Psi\mathrm{Isom}_F({}^{\sigma}t, t) \neq \varnothing\}. \tag{2.5}$$

By using the operation from (2.4), a calculation shows that $\mathrm{Gal}_t(F/\mathbb{F}_p)$ is a subgroup of $\mathrm{Gal}(F/\mathbb{F}_p)$.

Theorem 2.15. *Let $t : V \times V \to T$ be an alternating, fully nondegenerate F-tensor. If $\mathrm{Cent}(t) \cong F$, then the following hold:*

1. $\mathrm{Aut}(\mathrm{G}_t(F)) \cong \mathrm{Hom}_{\mathbb{F}_p}(V, T) \rtimes \mathrm{S\Psi I}_{F/\mathbb{F}_p}(t)$ *and*
2. $|\mathrm{S\Psi I}_{F/\mathbb{F}_p}(t)| = |\Psi\mathrm{Isom}_F(t)| \cdot |\mathrm{Gal}_t(F/\mathbb{F}_p)|$.

Proof. Let $\mathfrak{g} = \mathfrak{g}_t(F)$ be the Lie algebra associated to $G = \mathrm{G}_t(F)$. Since G is of class 2 with exponent $p > 2$, the Baer correspondence guarantees that $\mathrm{Aut}(G) \cong \mathrm{Aut}_{\mathbb{F}_p}(\mathfrak{g})$. Since t is full, $T = [\mathfrak{g}, \mathfrak{g}]$, so every endomorphism of $\mathfrak{g} = V \oplus T$ maps T into T. Thus, we have a split exact sequence of groups

$$1 \longrightarrow \mathrm{Hom}_{\mathbb{F}_p}(V, T) \longrightarrow \mathrm{Aut}_{\mathbb{F}_p}(\mathfrak{g}) \longrightarrow \Psi\mathrm{Isom}_{\mathbb{F}_p}(t) \longrightarrow 1,$$

where the penultimate map is given by $\alpha \mapsto (\alpha_V, \alpha_T)$ with $\alpha_V : V \to V$ given by $v + T \mapsto \alpha(v) + T$ and $\alpha_T = \alpha|_T$ is the restriction of α to T.

The group $\Psi\mathrm{Isom}_{\mathbb{F}_p}(t)$ acts on $\mathrm{Cent}(t)$ via conjugation. If $(X, Y, Z) \in \mathrm{Cent}(t)$ and $(\alpha, \beta) \in \Psi\mathrm{Isom}_{\mathbb{F}_p}(t)$, then $(\alpha X\alpha^{-1}, \alpha Y\alpha^{-1}, \beta Z\beta^{-1})$ belongs to $\mathrm{Cent}(t)$. This defines a homomorphism $\gamma : \Psi\mathrm{Isom}_{\mathbb{F}_p}(t) \to \mathrm{Aut}(\mathrm{Cent}(t))$, where $\mathrm{Aut}(\mathrm{Cent}(t))$ denotes the automorphism group of $\mathrm{Cent}(t)$ as a unital $\mathbb{F}_p$-algebra. Since $\mathrm{Cent}(t) \cong F$, the kernel of this map is $\Psi\mathrm{Isom}_F(t)$. The choice of an isomorphism $\varphi : \mathrm{Aut}(\mathrm{Cent}(t)) \to \mathrm{Gal}(F/\mathbb{F}_p)$ yields the following exact sequence of groups:

$$1 \longrightarrow \Psi\mathrm{Isom}_F(t) \longrightarrow \Psi\mathrm{Isom}_{\mathbb{F}_p}(t) \longrightarrow \mathrm{Gal}(F/\mathbb{F}_p).$$

We show that $\mathrm{im}(\varphi \circ \gamma) = \mathrm{Gal}_t(F/\mathbb{F}_p)$. Given $\sigma \in \mathrm{Gal}_t(F/\mathbb{F}_p)$, we have that $\sigma \in \mathrm{im}(\varphi \circ \gamma)$ if and only if there exists $(X, Y) \in \mathrm{GL}_F(V) \times \mathrm{GL}_F(T)$ such that $(\alpha, \beta) = (X\sigma, Y\sigma) \in \Psi\mathrm{Isom}_{\mathbb{F}_p}(t)$. This condition is equivalent to the equation

$$t(X\sigma(u), X\sigma(v)) = t(\alpha(u), \alpha(v)) = \beta t(u, v) = Y\sigma t(u, v) = Y({}^{\sigma}t(\sigma(u), \sigma(v))). \tag{2.6}$$

being verified for all $u, v \in V$. However, since σ induces an automorphism of V, the outer equality of (2.6) is equivalent to having $(X, Y) \in \Psi\mathrm{Isom}_F({}^{\sigma}t, t)$, meaning that $\sigma \in \mathrm{Gal}_t(F/\mathbb{F}_p)$. As a result, the following is a short exact sequence:

$$1 \longrightarrow \Psi\mathrm{Isom}_F(t) \longrightarrow \Psi\mathrm{Isom}_{\mathbb{F}_p}(t) \longrightarrow \mathrm{Gal}_t(F/\mathbb{F}_p) \longrightarrow 1.$$

In particular, the size of $\Psi\mathrm{Isom}_{\mathbb{F}_p}(t)$ is equal to $|\Psi\mathrm{Isom}_F(t)| \cdot |\mathrm{Gal}_t(F/\mathbb{F}_p)|$.

We conclude by showing that $\Psi\mathrm{Isom}_{\mathbb{F}_p}(t)$ and $\mathrm{S}\Psi\mathrm{I}_{F/\mathbb{F}_p}(t)$ are isomorphic. For this, note that, if $(\alpha, \beta) \in \Psi\mathrm{Isom}_{\mathbb{F}_p}(t)$ is such that $\varphi\gamma((\alpha, \beta)) = \sigma$, then $(\alpha\sigma^{-1}, \beta\sigma^{-1})$ belongs to $\Psi\mathrm{Isom}_F({}^{\sigma}t, t)$. Therefore, the map

$$\mathrm{S}\Psi\mathrm{I}_{F/\mathbb{F}_p}(t) \longrightarrow \Psi\mathrm{Isom}_{\mathbb{F}_p}(t) \quad \text{given by} \quad (\alpha, \beta, \sigma) \longmapsto (\alpha\sigma, \beta\sigma)$$

defines an isomorphism. Putting everything together, the theorem follows. □

Following [21, Sec. 4], we say two homogeneous polynomials $f, g \in F[y_1, \ldots, y_d]$ are *projectively semi-equivalent* if there exist $M = (m_{ij}) \in \mathrm{GL}_d(F)$, $\sigma \in \mathrm{Gal}(F/\mathbb{F}_p)$, and $\lambda \in F^{\times}$ such that

$$(\sigma(f))(m_{11}y_1 + \cdots + m_{1d}y_d, \ldots, m_{d1}y_1 + \cdots + m_{dd}y_d) = \lambda g(\boldsymbol{y}), \tag{2.7}$$

where $(\sigma(f))(\boldsymbol{y})$ is the polynomial obtained by applying σ to the coefficients of f. If $\sigma = 1$, then we just say that f and g are *projectively equivalent*. Projective equivalence yields an isomorphism of the varieties of f and g, but the converse is not true in general. Moreover projective semi-equivalence need not induce an isomorphism of varieties of f and g but of $\sigma(f)$ and g instead. The following corollary collects some direct geometric implications of Theorem 2.13, some more will be presented in Section 3.

Corollary 2.16. *Assume that $s : V \times V \to T$ and $t : V' \times V' \to T'$ are fully-nondegenerate, that $\mathrm{Cent}(t) \cong \mathrm{Cent}(s) \cong F$, and that $\mathrm{G}_s(F) \cong \mathrm{G}_t(F)$. Let $\mathrm{Pf}(s)$ and $\mathrm{Pf}(t)$ be Pfaffians over F of s and t, respectively. Then the following hold.*

1. *The polynomials $\mathrm{Pf}(s)$ and $\mathrm{Pf}(t)$ are projectively semi-equivalent.*
2. *The F-points of the singular loci of $\mathrm{Pf}(s)$ and $\mathrm{Pf}(t)$ are in bijection.*
3. *The polynomials $\mathrm{Pf}(s)$ and $\mathrm{Pf}(t)$ have the same splitting behavior, i.e. the degrees of their irreducible factors, counted with multiplicities, are the same.*

Proof. Thanks to Theorem 2.13(2), there exist $\mathbb{F}_p$-linear isomorphisms $\alpha : V \to V'$ and $\beta : T \to T'$ such that for all $u, v \in V$,

$$t(\alpha(u), \alpha(v)) = \beta(s(u, v)). \tag{2.8}$$

Then the following map $\mathrm{Cent}(s) \to \mathrm{Cent}(t)$ is an isomorphism of $\mathbb{F}_p$-algebra:

$$(X, Y, Z) \longmapsto (\kappa_\alpha(X), \kappa_\alpha(Y), \kappa_\beta(Z)) := (\alpha X \alpha^{-1}, \alpha Y \alpha^{-1}, \beta Z \beta^{-1}).$$

Let $\varphi_s : F \to \mathrm{Cent}(s)$ and $\varphi_t : F \to \mathrm{Cent}(t)$ be field isomorphisms, so s and t are F-bilinear via φ_s and φ_t, respectively. Since s and t are fully-nondegenerate, the maps $\pi_s : \mathrm{Cent}(s) \to \mathrm{End}_{\mathbb{F}_p}(T)$ and $\pi_t : \mathrm{Cent}(t) \to \mathrm{End}_{\mathbb{F}_p}(T')$ given by

$$(X, Y, Z) \longmapsto Z \quad \text{and} \quad (X', Y', Z') \longmapsto Z',$$

respectively, are injective, so $\mathrm{im}(\pi_s) \cong \mathrm{im}(\pi_t) \cong F$. Set $\psi_s = \pi_s\varphi_s$ and $\psi_t = \pi_t\varphi_t$, so $\sigma = \psi_t^{-1}\kappa_\beta\psi_s \in \mathrm{Gal}(F/\mathbb{F}_p)$. Thus, β is F-semilinear: for all $u, v \in T$ and all $\lambda \in F$,

$$\beta(u + \lambda v) = \beta(u + \psi_s(\lambda)v) = \beta(u) + \kappa_\beta\psi_s(\lambda)\beta(v) = \beta(u) + \sigma(\lambda)\beta(v).$$

By a similar argument, α is also F-semilinear for some $\sigma' \in \mathrm{Gal}(F/F_p)$.

Choose F-bases for V, V', T, and T'. Since both α and β are F-semilinear, there exist F-matrices M and N such that α is given by (N, σ') and β by (M, σ) relative to our choice of bases. If $u, v \in V$ are basis vectors, then (2.8) implies

$$t(Nu, Nv) = t(\alpha(u), \alpha(v)) = \beta(s(u, v)) = M\sigma(s(u, v)). \tag{2.9}$$

With $\lambda = \det(N)^2 \in F^\times$, the equality in (2.9) implies (2.7) for the Pfaffians of s and t over F. Hence, (1) holds. The other statements (2) and (3) easily follow from (1). □

3. Tensors and irreducible Pfaffians

In the study of elliptic p-groups $\mathrm{G}_t(F)$, the number of the maximal totally isotropic subspaces of V is a fundamental invariant. We will show in this section that there are four possible situations for the isotropic subspaces, distinguished by the adjoint algebra of t. These four possibilities fit into two larger frameworks: B is either isotropically-decomposable or isotropically-indecomposable. As a matter of fact, we prove this within the much larger framework of groups for which $\mathrm{Pf}(t)$ is an irreducible variety. We eventually make an additional "genericity" assumption, which is satisfied by all tensors coming from E-groups.

3.1. Pfaffians and isotropic subspaces.

In this section we present a number of results on isotropic subspaces with respect to an alternating tensor with irreducible Pfaffian.

Lemma 3.1. *Let $t : V \times V \to T$ be an alternating K-tensor. If $\mathrm{Pf}(t) \neq 0$ and $U \leqslant V$ is totally isotropic, then $2 \dim_K U \leqslant \dim_K V$.*

Proof. From $\mathrm{Pf}(t) \neq 0$ it follows that $\dim_K V = 2n$ for some $n \geqslant 1$. For a contradiction, let U be a totally isotropic subspace of V with $\dim_K U \geqslant n+1$. Extend a basis of U to a basis of V, and with this basis represent t as the following matrix of linear forms

$$\mathrm{B} = \begin{pmatrix} 0 & \mathrm{M}_1 \\ -\mathrm{M}_1^{\mathrm{t}} & \mathrm{M}_2 \end{pmatrix}, \text{ with } \mathrm{M}_1, \mathrm{M}_2 \in \mathrm{Mat}_n(K[y_1, \dots, y_d]_1), \ \mathrm{M}_2^{\mathrm{t}} = -\mathrm{M}_2 .$$

Note that M_1 contains a zero column since $\dim_K U \geqslant n+1$, and so, for some $u \in K^\times$, the equality $\mathrm{Pf}(t) = u \det(\mathrm{M}_1) = 0$ holds. Contradiction. □

Definition 3.2. Let $t : V \times V \to T$ be an alternating K-tensor. The set of totally isotropic subspaces of V of dimension $\frac{1}{2}\dim_K V$ is denoted $\mathcal{T}(t)$.

Lemma 3.3. *Let $t : V \times V \to T$ be an alternating K-tensor such that $\mathrm{Pf}(t)$ is irreducible over K. If $U, W \in \mathcal{T}(t)$, then either $U = W$ or $U \cap W = 0$.*

Proof. Fix $U, W \in \mathcal{T}(t)$. Suppose $U \cap W \neq 0$ and $U \neq W$. Let $\mathcal{B}_{U\cap W}$ be a basis of $U \cap W$, and extend it to bases of U and W, denoted by $\mathcal{B}_U$ and $\mathcal{B}_W$, respectively. Extend $\mathcal{B}_U \cup \mathcal{B}_W$ to a basis $\mathcal{B}$ of V. Let B be a matrix of linear forms associated to t via this choice of basis for V. Since $\mathrm{Pf}(t) \neq 0$, we know that $\dim_K V = 2n$ for some $n \geqslant 1$. It follows that there exist $n \times n$ matrices M_1 and M_2 of linear forms, with M_2 skew-symmetric, such that

$$\mathrm{B} = \begin{pmatrix} 0 & \mathrm{M}_1 \\ -\mathrm{M}_1^{\mathrm{t}} & \mathrm{M}_2 \end{pmatrix}.$$

By construction, there are two overlapping $n \times n$ blocks of zeros (corresponding to U and W) along the diagonal of B. In particular M_1 is block-upper triangular, and therefore $\det(M_1)$ is not irreducible in $K[y_1, \dots, y_d]$. Since $\mathrm{Pf}(t)/\det(\mathrm{M}_1)$ is a non-zero scalar, we have reached a contradiction. □

We remark that the proof of Lemma 3.3 may be further generalized to describe the intersection of $U, W \in \mathcal{T}(t)$ for Pfaffians that split into a product of irreducible polynomials.

Definition 3.4. Let $\mathcal{V}$ be a hypersurface in $\mathbb{P}_K^{d-1}$ of degree n and let $I(\mathcal{V}) \subseteq K[\boldsymbol{y}]$ be the ideal of $\mathcal{V}$. The following notions are defined as follows:

(1) if $\mathrm{M}, \mathrm{M}' \in \mathrm{Mat}_n(K[\boldsymbol{y}]_1)$ are such that $\det \mathrm{M}, \det \mathrm{M}' \in I(\mathcal{V})$, then
$$\mathrm{M} \sim \mathrm{M}' \iff \text{there exist } X, Y \in \mathrm{GL}_n(K) \text{ with } \mathrm{M}' = X\,\mathrm{M}\,Y.$$
(2) if $\mathrm{M} \in \mathrm{Mat}_n(K[\boldsymbol{y}]_1)$ is such that $\det \mathrm{M} \in I(\mathcal{V})$, then
$$[\mathrm{M}] = \{\mathrm{M}' \in \mathrm{Mat}_n(K[\boldsymbol{y}]_1) : \mathrm{M} \sim \mathrm{M}'\}.$$
(3) $\mathcal{L}_{\mathcal{V}}$ is the set of all $[\mathrm{M}]$ where M is as in (2).
(4) $\mathcal{L}_{\mathcal{V}}^{\mathrm{sym}}$ is the subset of $\mathcal{L}_{\mathcal{V}}$ consisting of all $[\mathrm{M}]$ with a symmetric representative.

We remark that the relation $\sim$ defined above is the standard equivalence relation considered in the study of determinantal varieties, cf. Definition 2.5. Moreover, it is clear that, for any two equivalent elements M, M', there exists $u \in K^\times$ such that $\det \mathrm{M} = u \det \mathrm{M}'$. When $n = d$, we refer to M as a *cuboid*, which is *smooth*, if $\det \mathrm{M}$ is a smooth polynomial in $K[\boldsymbol{y}]$. The name smooth cuboids is borrowed from [38, Sec. 2]; cf. Remark 5.7.

Proposition 3.5. *Let $t : V \times V \to T$ be an alternating K-bilinear map with an irreducible Pfaffian and associated matrix $\mathrm{B} \in \mathrm{Mat}_{2n}(K[y_1, \ldots, y_d]_1)$. If $|\mathcal{T}(t)| \geqslant 2$, then there exists $\mathrm{M} \in \mathrm{Mat}_n(K[\boldsymbol{y}]_1)$ such that B is pseudo-isometric to*
$$\begin{pmatrix} 0 & \mathrm{M} \\ -\mathrm{M}^{\mathrm{t}} & 0 \end{pmatrix}$$
and exactly one of the following holds:

(1) $|\mathcal{T}(t)| > 2$ *and* $[\mathrm{M}] \in \mathcal{L}_{\mathcal{V}}^{\mathrm{sym}}$.
(2) $|\mathcal{T}(t)| = 2$ *and* $[\mathrm{M}] \in \mathcal{L}_{\mathcal{V}} \setminus \mathcal{L}_{\mathcal{V}}^{\mathrm{sym}}$.

Proof. Suppose $|\mathcal{T}(t)| \geqslant 2$, and take $U, W \in \mathcal{T}(t)$ to be distinct. Then Lemma 3.3 yields $U \cap W = 0$, so there exists $\mathrm{M} \in \mathrm{Mat}_n(K[\boldsymbol{y}]_1)$ and a choice of basis for V such that
$$\mathrm{B} = \begin{pmatrix} 0 & \mathrm{M} \\ -\mathrm{M}^{\mathrm{t}} & 0 \end{pmatrix}.$$
Since t has non-zero Pfaffian, t is nondegenerate, so M defines a non-degenerate tensor $\tilde{t} : U \times W \to T$. Fix bases of U and W, and let $W \to U$ be the linear map identifying the chosen bases, written as $w \mapsto \overline{w}$.

Let $X \in \mathcal{T}(t)$, and assume without loss of generality that $X \cap U = 0$. Then both W and X are complements of U in V, so there is $D \in \mathrm{Mat}_n(K)$ such that $X = \{w + D\overline{w} \mid w \in W\}$. Fix such a D. Now X is totally isotropic if and only if, for all $w, w' \in W$, the element $t(w + D\overline{w}, w' + D\overline{w'})$ is trivial. This happens if and only if, for all $w, w' \in W$, one has
$$0 = \begin{pmatrix} \overline{w}^{\mathrm{t}} D^{\mathrm{t}} & w^{\mathrm{t}} \end{pmatrix} \begin{pmatrix} 0 & \mathrm{M} \\ -\mathrm{M}^{\mathrm{t}} & 0 \end{pmatrix} \begin{pmatrix} D\overline{w'} \\ w' \end{pmatrix} = -\overline{w}^{\mathrm{t}}\,\mathrm{M}^{\mathrm{t}}\,Dw' + \overline{w}^{\mathrm{t}} D^{\mathrm{t}}\,\mathrm{M}\,w'. \tag{3.1}$$
We conclude from (3.1) that X is totally isotropic if and only if $D^{\mathrm{t}}\,\mathrm{M} = \mathrm{M}^{\mathrm{t}}\,D = (D^{\mathrm{t}}\,\mathrm{M})^{\mathrm{t}}$, equivalently
$$\begin{pmatrix} D^{\mathrm{t}} & 0 \\ 0 & I \end{pmatrix} \begin{pmatrix} 0 & \mathrm{M} \\ -\mathrm{M}^{\mathrm{t}} & 0 \end{pmatrix} \begin{pmatrix} D & 0 \\ 0 & I \end{pmatrix} = \begin{pmatrix} 0 & D^{\mathrm{t}}\,\mathrm{M} \\ -D^{\mathrm{t}}\,\mathrm{M} & 0 \end{pmatrix}. \tag{3.2}$$

Call B' the matrix on the right hand side of (3.2). If D is invertible, then $X \neq W$ and B and B' are K-pseudo-isometric. This proves (1). If D is not invertible, then let $w \in W \setminus \{0\}$ be such that $D\overline{w} = 0$. it follows that

$$w = w + D\overline{w} \in X \cap W,$$

and so Lemma 3.3 yields $X = W$, which proves (2) and completes the proof. □

Corollary 3.6. *Let $t : V \times V \to T$ be an alternating F-tensor such that $\mathrm{Pf}(t)$ describes an elliptic curve in $\mathbb{P}^2_F$. Then $\dim V = 2 \dim T = 6$ and $|\mathcal{T}(t)|$ takes values in $\{0, 1, 2, q+1\}$.*

Proof. An elliptic curve in $\mathbb{P}^2_F$ is defined by a homogeneous cubic polynomial in 3 variables and therefore the dimensions of V and T are respectively 6 and 3. Moreover, if $|\mathcal{T}(t)| > 2$, then Proposition 3.5 yields that t can be represented by a symmetric matrix of linear forms. The claim follows from [48, Prop. 4.10]. □

3.2. **Adjoint algebras of half-generic tensors.** Before dealing directly with the specific situation where $n = 3$ and $\mathrm{M} = J_{E,P}$, we turn to the more general case of half-generic tensors (see Definition 3.8), for which $|\mathcal{T}(t)| \geqslant 1$. In this case, indeed, we have some more characteristic information given by the existence of maximal totally isotropic subspaces. As we will see, the adjoint algebra can tell exactly how many such subspaces are present and whether the equivalence class of B satisfies some additional symmetry constraints. As supported by computational evidence, when $|\mathcal{T}(t)| = 0$, we expect to find that $\mathrm{Adj}(t) \cong K$. The adjoint algebras for half-generic tensors in the case when $|\mathcal{T}(t)| \geqslant 2$ are, thanks to Proposition 3.5, already determined without much additional work. We analyze the case where $|\mathcal{T}(t)| = 1$ in Lemmas 3.10 and 3.11.

Lemma 3.7. *Let $\mathrm{M} \in \mathrm{Mat}_n(K[\boldsymbol{y}]_1)$ and write*

$$\mathrm{B} = \begin{pmatrix} 0 & \mathrm{M} \\ -\mathrm{M}^{\mathrm{t}} & 0 \end{pmatrix}.$$

Then the following holds:

$$\mathrm{Adj}(\mathrm{B}) = \left\{ \left(\begin{pmatrix} A_{11} & A_{12} \\ A_{21} & A_{22} \end{pmatrix}, \begin{pmatrix} B_{11} & B_{12} \\ B_{21} & B_{22} \end{pmatrix} \right) : \begin{array}{c} (A_{11}, B_{22}), (B_{11}, A_{22}) \in \mathrm{Adj}(\mathrm{M}), \\ (A_{21}, -B_{21}) \in \mathrm{Adj}(\mathrm{M}, \mathrm{M}^{\mathrm{t}}), \\ (A_{12}, -B_{12}) \in \mathrm{Adj}(\mathrm{M}^{\mathrm{t}}, \mathrm{M}) \end{array} \right\}.$$

Proof. For $i, j \in [2]$, let $A_{ij}, B_{ij} \in \mathrm{Mat}_n(K)$. Then

$$\begin{pmatrix} A_{11}^{\mathrm{t}} & A_{21}^{\mathrm{t}} \\ A_{12}^{\mathrm{t}} & A_{22}^{\mathrm{t}} \end{pmatrix} \begin{pmatrix} 0 & \mathrm{M} \\ -\mathrm{M}^{\mathrm{t}} & 0 \end{pmatrix} = \begin{pmatrix} 0 & \mathrm{M} \\ -\mathrm{M}^{\mathrm{t}} & 0 \end{pmatrix} \begin{pmatrix} B_{11} & B_{12} \\ B_{21} & B_{22} \end{pmatrix}$$

implies that the following equations hold:

$$-A_{21}^{\mathrm{t}}\,\mathrm{M}^{\mathrm{t}} = \mathrm{M}\,B_{21}, \quad A_{11}^{\mathrm{t}}\,\mathrm{M} = \mathrm{M}\,B_{22}, \quad -A_{22}^{\mathrm{t}}\,\mathrm{M}^{\mathrm{t}} = -\mathrm{M}^{\mathrm{t}}\,B_{11}, \quad A_{12}^{\mathrm{t}}\,\mathrm{M} = -\mathrm{M}^{\mathrm{t}}\,B_{12}. \qquad \square$$

Definition 3.8. A skew-symmetric matrix $\mathrm{B} \in \mathrm{Mat}_{2n}(K[\boldsymbol{y}]_1)$ is *half-generic* if B is pseudo-isometric to $\left(\begin{smallmatrix} 0 & \mathrm{M} \\ -\mathrm{M}^{\mathrm{t}} & \mathrm{S} \end{smallmatrix}\right)$ where $\mathrm{M}, \mathrm{S} \in \mathrm{Mat}_n(K[\boldsymbol{y}]_1)$ satisfy

$$\mathrm{Adj}(\mathrm{M}) \cong K \quad \text{and} \quad \mathrm{Adj}(\mathrm{M}, \mathrm{M}^{\mathrm{t}}) = \mathrm{Adj}(\mathrm{M}^{\mathrm{t}}, \mathrm{M}) = \begin{cases} \mathrm{Adj}(\mathrm{M}) & \text{if } \mathrm{M}^{\mathrm{t}} = \mathrm{M}, \\ 0 & \text{otherwise.} \end{cases}$$

If M can be chosen to satisfy $\mathrm{M}^{\mathrm{t}} = \mathrm{M}$, then B is *symmetrically half-generic* and *asymmetrically half-generic* if no such M exists.

Remark 3.9. In the situation described in Definition 3.8, both $\mathrm{Adj}(\mathrm{M})$ and $\mathrm{Adj}(\mathrm{M}^{\mathrm{t}}, \mathrm{M})$ are as small as possible. This is what we expect in general for "most" linear determinantal representations, motivating the name "half-generic". Indeed, if $\mathrm{M} = \mathrm{M}_1\, y_1 + \ldots + \mathrm{M}_d\, y_d$ with $\mathrm{M}_1, \ldots, \mathrm{M}_d \in \mathrm{Mat}_n(K)$, then the following hold:

$$\mathrm{Adj}(\mathrm{M}) = \bigcap_{i=1}^{d} \mathrm{Adj}(\mathrm{M}_i) \qquad\qquad \mathrm{Adj}(\mathrm{M}, \mathrm{M}^{\mathrm{t}}) = \bigcap_{i=1}^{d} \mathrm{Adj}(\mathrm{M}_i, \mathrm{M}_i^{\mathrm{t}}).$$

Generically, both $\mathrm{Adj}(\mathrm{M}_i)$ and $\mathrm{Adj}(\mathrm{M}_i, \mathrm{M}_i^{\mathrm{t}})$ define a codimension n^2 subspace of K^{2n^2}, so for sufficiently large d, generically $\mathrm{Adj}(\mathrm{M})$ and $\mathrm{Adj}(\mathrm{M}, \mathrm{M}^{\mathrm{t}})$ are given as in Definition 3.8.

Because half-genericity is defined for pseudo-isometry classes, it makes sense to extend Definition 3.8 to tensors, via the choice of a basis. Alternating tensors $t : V \times V \to T$ with $|\mathcal{T}(t)| \geqslant 1$ and whose Pfaffian defines an elliptic curve are half-generic, cf. Remark 5.2.

Lemma 3.10. *Let $t : V \times V \to T$ be an asymmetrically half-generic K-tensor such that $|\mathcal{T}(t)| = 1$. Then $\mathrm{Adj}(t)$ is $*$-isomorphic to $\mathbf{O}_1(K)$.*

Proof. Let $\mathrm{B} \in \mathrm{Mat}_{2n}(K[\boldsymbol{y}])$ be associated with t and in the form given in Definition 3.8. Since t is asymmetrically half-generic, $\mathrm{Adj}(\mathrm{M}, \mathrm{M}^{\mathrm{t}}) = \mathrm{Adj}(\mathrm{M}^{\mathrm{t}}, \mathrm{M}) = 0$, and hence by a computation similar to that carried out in the proof of Lemma 3.7, we have

$$\mathrm{Adj}(\mathrm{B}) = \left\{ \left(\begin{pmatrix} aI_n & \Gamma \\ 0 & (a-k)I_n \end{pmatrix}, \begin{pmatrix} (a-k)I_n & \Phi \\ 0 & aI_n \end{pmatrix} \right) \;\middle|\; \begin{array}{c} a, k \in K,\ \Gamma, \Phi \in \mathrm{Mat}_n(K), \\ \Gamma^{\mathrm{t}}\,\mathrm{M} + \mathrm{M}^{\mathrm{t}}\,\Phi = k\mathrm{S} \end{array} \right\}. \tag{3.3}$$

Now we consider the K-vector space

$$L = \left\{ (\Gamma, \Phi, k) \in \mathrm{Mat}_n(K)^2 \oplus K \mid \Gamma^{\mathrm{t}}\,\mathrm{M} + \mathrm{M}^{\mathrm{t}}\,\Phi = k\mathrm{S} \right\},$$

which we will show to be trivial. First, we show that $\dim_K L \leqslant 1$. For this note that, if $(\Gamma, \Phi, 0) \in L$, then $(\Gamma, -\Phi) \in \mathrm{Adj}(\mathrm{M}^{\mathrm{t}}, \mathrm{M}) = 0$. Now, if $(\Gamma, \Phi, k), (\Gamma', \Phi', k') \in L$ with $k \neq 0$, then there exists $\lambda \in K$ such that $\lambda k = k'$. It follows that $(\lambda\Gamma - \Gamma', \lambda\Phi - \Phi', 0) \in L$ and therefore $(\lambda\Gamma, \lambda\Phi, \lambda k) = (\Gamma', \Phi', k')$. This proves the claim.

Suppose now, for a contradiction, that $\dim_K L = 1$, and let $(X, Y, 1) \in L$. Since S is skew-symmetric, also $(Y, X, -1)$ belongs to L. It follows that $(X + Y, -(X + Y)) \in \mathrm{Adj}(\mathrm{M}^{\mathrm{t}}, \mathrm{M})$, equivalently $Y = -X$. Hence, $\dim_K \mathrm{Adj}(t) = 2$, and the following holds:

$$\mathrm{Adj}(\mathrm{B}) = \left\{ \left(\begin{pmatrix} aI_n & kX \\ 0 & (a-k)I_n \end{pmatrix}, \begin{pmatrix} (a-k)I_n & -kX \\ 0 & aI_n \end{pmatrix} \right) \;\middle|\; \begin{array}{c} a, k \in K,\ X \in \mathrm{Mat}_n(K), \\ X^{\mathrm{t}}\,\mathrm{M} - \mathrm{M}^{\mathrm{t}}\,X = \mathrm{S} \end{array} \right\}.$$

In particular, $\mathrm{Adj}(\mathrm{B})$ contains

$$(\alpha, \alpha^*) = \left(\begin{pmatrix} 0 & -X \\ 0 & I_n \end{pmatrix}, \begin{pmatrix} I_n & X \\ 0 & 0 \end{pmatrix} \right).$$

It follows that $\alpha\alpha^* = \alpha^*\alpha = 0$. Hence, for all $u, v \in V$, we compute

$$t(\alpha(u), \alpha(v)) = t(u, \alpha^*\alpha(v)) = 0 = t(\alpha\alpha^*(u), v) = t(\alpha^*(u), \alpha^*(v)).$$

It follows that $\alpha(V)$ and $\alpha^*(V)$ are two distinct n-dimensional, totally isotropic subspaces, which contradicts $|\mathcal{T}(t)| = 1$. We have proven that $\dim_K L = 0$, from which we derive that $\mathrm{Adj}(\mathrm{B}) \cong K \cong \mathbf{O}_1(K)$. □

Recall from Section 2.3 that the notation $A \cong R \rtimes S$ indicates that R is the Jacobson radical of the $*$-ring A and that $A/R \cong S$.

Lemma 3.11. *Let $t : V \times V \to T$ be a symmetrically half-generic K-tensor such that $|\mathcal{T}(t)| = 1$. Assume that* $\mathrm{char}(K) \neq 2$. *Then* $\mathrm{Adj}(t)$ *is $*$-isomorphic to $K \rtimes \mathbf{O}_1(K)$ and, if $(\alpha, \beta) \neq (0,0)$ is in the Jacobson radical of* $\mathrm{Adj}(t)$, *then $\mathcal{T}(t) = \{\alpha(V)\}$.*

Proof. Suppose, without loss of generality, that the matrix B associated with t is given in the form from Definition 3.8 with $\mathrm{M}^{\mathrm{t}} = \mathrm{M}$. It follows from the assumptions that $\mathrm{Adj}(\mathrm{M}^{\mathrm{t}}, \mathrm{M}) = \mathrm{Adj}(\mathrm{M}) \cong K$ and in the same way as in Lemma 3.10 we derive

$$\mathrm{Adj}(\mathrm{B}) = \left\{ \left(\begin{pmatrix} \Gamma_{11} & \Gamma_{12} \\ kI_n & \Gamma_{22} \end{pmatrix}, \begin{pmatrix} \Phi_{11} & \Phi_{12} \\ -kI_n & \Phi_{22} \end{pmatrix} \right) \;\middle|\; \begin{array}{c} k \in K,\ \Gamma_{ij}, \Phi_{ij} \in \mathrm{Mat}_n(K), \\ \Gamma_{11}^{\mathrm{t}}\,\mathrm{M} - \mathrm{M}\,\Phi_{22} = -k\mathrm{S}, \\ \Gamma_{22}^{\mathrm{t}}\,\mathrm{M} - \mathrm{M}\,\Phi_{11} = k\mathrm{S}, \\ \Gamma_{12}^{\mathrm{t}}\,\mathrm{M} + \mathrm{M}\,\Phi_{12} = \mathrm{S}\Phi_{22} - \Gamma_{22}^{\mathrm{t}}\mathrm{S} \end{array} \right\}.$$

Since $\mathrm{Adj}(\mathrm{M}) \cong K$, the K-vector space

$$P = \left\{ (\Gamma, \Phi, k) \in \mathrm{Mat}_n(K)^2 \oplus K \mid \Gamma^{\mathrm{t}}\,\mathrm{M} - \mathrm{M}\,\Phi = k\mathrm{S} \right\}$$

has dimension 1 or 2. Indeed $(\Gamma, \Phi, 0) \in P$ is equivalent to $(\Gamma, \Phi) \in \mathrm{Adj}(\mathrm{M})$: the forward implication implies that $\dim_K P \leqslant 2$ while the reverse one ensures $\dim_K P \geqslant 1$.

We claim that $\dim_K P = 1$ and we prove so working by contradiction. To this end, assume that $\dim_K P = 2$ and let $\{(I_n, I_n, 0), (X, Y, 1)\}$ be a basis of P. Since S is skew-symmetric, $(Y, X, 1)$ also belongs to P, so $(X - Y, Y - X) \in \mathrm{Adj}(\mathrm{M})$. Hence, there exists $\rho \in K$ such that $X - Y = \rho I_n = Y - X$. This implies $2(X - Y) = 0$, and since $\mathrm{char}(K) \neq 2$, we derive $X = Y$. Define now $\mathrm{S}' = \mathrm{S}X + X^{\mathrm{t}}\mathrm{S}$. With this, we have

$$\mathrm{Adj}(\mathrm{B}) = \left\{ \left(\begin{pmatrix} aI_n - kX & C \\ kI_n & bI_n + kX \end{pmatrix}, \begin{pmatrix} bI_n + kX & D \\ -kI_n & aI_n - kX \end{pmatrix} \right) \;\middle|\; \begin{array}{c} a, b, k \in K,\ C, D \in \mathrm{Mat}_n(K), \\ C^{\mathrm{t}}\,\mathrm{M} + \mathrm{M}\,D = (a-b)\mathrm{S} - k\mathrm{S}' \\ X^{\mathrm{t}}\,\mathrm{M} - \mathrm{M}\,X = \mathrm{S} \end{array} \right\}.$$

Now we consider the following vector space:

$$P' = \left\{ (C, D, c, d) \in \mathrm{Mat}_n(K)^2 \oplus K^2 \mid C^{\mathrm{t}}\,\mathrm{M} + \mathrm{M}\,D = c\mathrm{S} - d\mathrm{S}' \right\}.$$

Note that, whenever $(C, D, c, 0) \in P'$, the element $(C, -D, c)$ belongs to P. It then follows from $\dim_K P = 2$ that $\dim_K P' \in \{2, 3\}$. If $\dim_K P' = 2$, then a basis for P' is $\{(I_n, -I_n, 0, 0), (X, -X, 1, 0)\}$ and

$$\mathrm{Adj}(\mathrm{B}) = \left\{ \left(\begin{pmatrix} aI_n & cI_n + (a-b)X \\ 0 & bI_n \end{pmatrix}, \begin{pmatrix} bI_n & -cI_n + (b-a)X \\ 0 & aI_n \end{pmatrix} \right) \;\middle|\; \begin{array}{c} a, b, c \in K, \\ X^{\mathrm{t}}\,\mathrm{M} - \mathrm{M}\,X = \mathrm{S} \end{array} \right\}.$$

In particular, $\mathrm{Adj}(\mathrm{B})$ contains the following element:

$$(\alpha, \alpha^*) = \left(\begin{pmatrix} 0 & -X \\ 0 & I_n \end{pmatrix}, \begin{pmatrix} I_n & X \\ 0 & 0 \end{pmatrix} \right). \tag{3.4}$$

It follows that $\alpha(V)$ and $\alpha^*(V)$ are two distinct n-dimensional, totally isotropic subspaces, which contradicts $|\mathcal{T}(t)| = 1$. This proves that $\dim_K P' \neq 2$, so $\dim_K P' = 3$.

Let now $\{(I_n, -I_n, 0, 0), (X, -X, 1, 0), (Y, Z, \ell, 1)\}$ be a basis of P'. Since both S and S' are skew-symmetric, we have $(Z, Y, -\ell, -1) \in P'$, so $(Y + Z, Y + Z, 0, 0) \in P'$. The characteristic of K being different from 2, this implies that $Z = -Y$. Thus, if $C, D \in \mathrm{Mat}_n(K)$ and $a, b, k \in K$ are such that

$$C^{\mathrm{t}}\,\mathrm{M} + \mathrm{M}\,D = (a-b)\mathrm{S} - k\mathrm{S}',$$

then the following holds: for some $c \in K$,

$$C = cI_n + (a - b - k\ell)X + kY = -D.$$

Thus, taking $b = 1$ and $a = c = k = 0$, we see that the element in (3.4) is also contained in Adj(B); contradiction. In particular $\dim_K P' \neq 3$, which yields that $\dim_K P \neq 2$ and, consequently, that $\dim_K P = 1$.

We conclude by observing that $\mathrm{Adj}(t) \cong K \rtimes \mathbf{O}_1(K)$ because

$$\mathrm{Adj}(\mathrm{B}) = \left\{ \left(\begin{pmatrix} aI_n & bI_n \\ 0 & aI_n \end{pmatrix}, \begin{pmatrix} aI_n & -bI_n \\ 0 & aI_n \end{pmatrix} \right) \;\middle|\; a, b \in K \right\}. \tag{3.5}$$

We also see from (3.5) that if $0 \neq (\alpha, -\alpha)$ is in the radical of Adj(B), then $\alpha(V) \in \mathcal{T}(t)$. □

Proposition 3.12. *Let $t : V \times V \to T$ be a K-tensor with irreducible Pfaffian. If $\mathrm{Adj}(t)$ is $*$-isomorphic to either $\mathbf{X}_1(K)$ or $\mathbf{S}_2(K)$, then $|\mathcal{T}(t)| = 2$ or $|\mathcal{T}(t)| > 2$, respectively.*

Proof. Let $\varphi : \mathrm{Adj}(t) \to A$ be a $*$-isomorphism, where A is either $\mathbf{X}_1(K)$ or $\mathbf{S}_2(K)$.

If $A = \mathbf{X}_1(K)$ and $(X, Y) = \varphi^{-1}((1, 0))$, then Theorem 2.12 yields that $XY = 0 = YX$ and $X + Y = I_{2n}$. Then $U = XV$ and $W = YV$ are totally isotropic subspaces and satisfy $U + W = V$. In particular, $|\mathcal{T}(t)| \geqslant 2$. To show that equality holds, we assume for a contradiction that $U' \in \mathcal{T}(t) \setminus \{U, W\}$. Then thanks to Lemma 3.3, we write $V = U \oplus U'$. Taking $\alpha : V \to U$ and $\beta : V \to U'$ to be projections such that $\alpha_{|U} = \mathrm{id}_U$ and $\beta_{|U'} = \mathrm{id}_{U'}$, it follows that $(\alpha, \beta) \in \mathrm{Adj}(t)$ and so the dimensions of A and $\mathrm{Adj}(t)$ do not coincide.

Assume now that $A = \mathbf{S}_2(K)$ and define

$$(X_1, Y_1) = \varphi^{-1}\left(\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \right) \quad \text{and} \quad (X_2, Y_2) = \varphi^{-1}\left(\begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} \right).$$

Theorem 2.12 yields that $X_1Y_1 = Y_1X_1 = 0 = X_2Y_2 = Y_2X_2$. Therefore X_1V, X_2V, and Y_1V are totally isotropic subspaces. Moreover, as $X_1 + Y_1$, $X_1 + X_2$, and $X_2 + Y_1$ are invertible, Lemma 3.3 ensures that they are distinct. In particular $|\mathcal{T}(t)| > 2$. □

In the following, all isomorphisms concerning adjoint algebras are taken as $*$-algebras.

Theorem 3.13. *Let $t : V \times V \to T$ be a full, half-generic K-tensor with irreducible Pfaffian. Then $\mathrm{Cent}(t) \cong K$, and the following hold.*

1. *$|\mathcal{T}(t)| = 1$ and t asymmetrically half-generic imply $\mathrm{Adj}(t) \cong \mathbf{O}_1(K)$.*
2. *$|\mathcal{T}(t)| = 1$, t symmetrically half-generic, and $2K = K$ imply $\mathrm{Adj}(t) \cong K \rtimes \mathbf{O}_1(K)$.*
3. *$|\mathcal{T}(t)| = 2$ if and only if $\mathrm{Adj}(t) \cong \mathbf{X}_1(K)$.*
4. *$|\mathcal{T}(t)| > 2$ if and only if $\mathrm{Adj}(t) \cong \mathbf{S}_2(K)$.*

Proof. Let $\mathrm{B} \in \mathrm{Mat}_{2n}(K[\boldsymbol{y}]_1)$ be the matrix associated with t. Since the Pfaffian is non-zero, we write $\dim_K V = 2n$. If $|\mathcal{T}(t)| = 1$, then Lemmas 3.10 and 3.11 settle (1)–(2). If $|\mathcal{T}(t)| = 2$, we know from Proposition 3.5, that B is asymmetrically half-generic. In this case Lemma 3.7 yields

$$\mathrm{Adj}(\mathrm{B}) = \left\{ \left(\begin{pmatrix} aI_n & 0 \\ 0 & bI_n \end{pmatrix}, \begin{pmatrix} bI_n & 0 \\ 0 & aI_n \end{pmatrix} \right) \;\middle|\; a, b \in K \right\} \cong \mathbf{X}_1(K). \tag{3.6}$$

This proves the forward direction of (3). If, on the other hand, $|\mathcal{T}(t)| > 2$, then B is symmetrically half-generic by Proposition 3.5. By Lemma 3.7, we have

$$\mathrm{Adj}(\mathrm{B}) = \left\{ \left(\begin{pmatrix} aI_n & bI_n \\ cI_n & dI_n \end{pmatrix}, \begin{pmatrix} dI_n & -bI_n \\ -cI_n & aI_n \end{pmatrix} \right) \;\middle|\; a, b, c, d \in K \right\} \cong \mathbf{S}_2(K). \tag{3.7}$$

Thus, the forward direction of (4) follows from (3.7). The reverse directions for (3) and (4) follow from Proposition 3.12.

We conclude by showing that $\mathrm{Cent}(t) \cong K$. Because $\mathrm{Pf}(t)$ is irreducible and t is full, t is fully-nondegenerate. Thus, Lemma 2.11 ensures that $\mathrm{Cent}(t)$ is commutative. Moreover,

from [8, Th. A], we know that $\mathrm{Cent}(t)$ embeds into the center of $\mathrm{Adj}(t)$ which is, in the four cases of this theorem, always isomorphic to K. This ends the proof. □

4. Determinantal representations of cubics

Let E be an elliptic curve in $\mathbb{P}^2_K$ with identity element $\mathcal{O}$. Let $E(K)$ denote the K-rational points of E and $\oplus$ the addition on E. If $P \in E(K)$ and m is a positive integer, we write $\ominus P$ for the opposite of P and $[m]P \in E(K)$ and $E[m]$, respectively, for the sum of m copies of P and the m-torsion subgroup of E. We write $\mathrm{Aut}(E)$ for the group of automorphisms of E as a projective curve, and $\mathrm{Aut}_{\mathcal{O}}(E)$ for the automorphism group of the elliptic curve E. In particular, $\mathrm{Aut}_{\mathcal{O}}(E)$ comprises the elements of $\mathrm{Aut}(E)$ that fix $\mathcal{O}$. We let $\mathrm{Div}(E)$ be the Weil divisor group of E and $\mathrm{Div}^0(E)$ the degree 0 part of the divisor group of E. We denote the class of D in the Picard group $\mathrm{Pic}(E)$ by $[D]$ and write $\mathrm{Pic}^0(E)$ for the degree 0 part of $\mathrm{Pic}(E)$. If $D \in \mathrm{Div}(E)$, denote by $\mathcal{L}(D)$ the sheaf of D, which is also commonly denoted by $\mathcal{O}_E(D)$. Our notation is mostly adherent to the one from [46, Ch. II] and we refer the reader to [23, 46] for the geometric background of Sections 4 and 5.

4.1. Divisors on elliptic curves.

In this section, we recall some basic facts on divisors.

Lemma 4.1 ([23, Prop. II.6.13]). *Let $D, D' \in \mathrm{Div}(E)$. Then the following are equivalent:*
(1) $[D] = [D']$,
(2) $\mathcal{L}(D)$ *and* $\mathcal{L}(D')$ *are isomorphic.*

Let $\mathcal{L}_0$ denote the collection of isomorphism classes of non-effective degree 0 line bundles on E. As a consequence of Lemma 4.1 one can easily derive that the map

$$\mathrm{Pic}^0(E) \setminus \{0\} \longrightarrow \mathcal{L}_0, \quad [D] \longmapsto \mathcal{L}(D) \tag{4.1}$$

is a well-defined bijection. Moreover, [46, Prop. III.3.4] ensures that the following map is a well-defined bijection:

$$E \setminus \{\mathcal{O}\} \longrightarrow \mathrm{Pic}^0(E) \setminus \{0\}, \quad P \longmapsto [P - \mathcal{O}]. \tag{4.2}$$

Lemma 4.2 (Abel's Theorem, cf. [46, Cor. III.3.5]). *Let $D = \sum_{P \in E(K)} n_P P \in \mathrm{Div}(E)$. Then $[D] = 0$ if and only if $\sum_{P \in E(K)} n_P = 0$ and $\bigoplus_{P \in E(K)} [n_P]P = 0$.*

4.2. Linear representations and non-effective line bundles.

This short section collects a few results on equivalence classes of determinantal representations of cubics from [27], which build upon the seminal paper [4] of Beauville.

Lemma 4.3 ([27, Th. 5.2]). *Let C be a smooth genus 1 curve in $\mathbb{P}^2_K$. Then there is a natural bijection between the following sets:*
(1) *the set $\mathcal{L}_C$ as given in Definition 3.4(3),*
(2) *the set of isomorphism classes of non-effective line bundles of degree 0 on C.*

Definition 4.4. Let $\mathcal{C}$ denote the collection of smooth genus 1 curves in $\mathbb{P}^2_K$ and write

$$\mathcal{L}_{\mathcal{C}} = \bigcup_{C \in \mathcal{C}} \mathcal{L}_C.$$

For each choice of $\mathrm{M} \in \mathcal{L}_{\mathcal{C}}$, the notation $[\![\mathrm{M}]\!]$ is used for the orbit of M with respect to the action of $\Gamma = \mathrm{GL}_3(K) \times \mathrm{GL}_3(K) \times \mathrm{GL}_3(K)$ on $\mathcal{L}_{\mathcal{C}}$ that is defined by

$$\Gamma \times \mathcal{L}_{\mathcal{C}} \longrightarrow \mathcal{L}_{\mathcal{C}},$$
$$((X, Y, Z), \mathrm{M}(\boldsymbol{y})) \longmapsto X^{\mathrm{t}}\, \mathrm{M}(Z\boldsymbol{y})Y.$$

Moreover, $\mathcal{M}_{\mathcal{C}}$ denotes the collection of all $[\![\mathrm{M}]\!]$ where $\mathrm{M} \in \mathcal{L}_{\mathcal{C}}$.

Proposition 4.5. *Let $\mathcal{C}$ denote the collection of smooth genus 1 curves in $\mathbb{P}^2_K$. Let $[\mathrm{M}], [\mathrm{M}'] \in \mathcal{L}_{\mathcal{C}}$ and write C and C' for the curves defined by $\det \mathrm{M} = 0$ and $\det \mathrm{M}' = 0$, respectively. Let, moreover, $\mathcal{L}$ and $\mathcal{L}'$ be degree 0 non-effective line bundles on C resp. C' associated to M and M' as in Lemma 4.3. Then the following are equivalent:*

(1) $[\![\mathrm{M}]\!] = [\![\mathrm{M}']\!]$,
(2) *there exists a linear isomorphism $\gamma : C \to C'$ such that $\gamma^*\mathcal{L}' = \mathcal{L}$.*

Proof. Rephrasing Definition 4.4, one has that $[\![\mathrm{M}]\!] = [\![\mathrm{M}']\!]$ if and only if there exists $Z \in \mathrm{GL}_3(K)$ such that $[\mathrm{M}'(\boldsymbol{y})] = [\mathrm{M}(Z\boldsymbol{y})]$. By calling γ the map $C \to C'$ that is induced by Z, it follows from Lemma 4.3 that $[\![\mathrm{M}]\!] = [\![\mathrm{M}']\!]$ if and only if $\gamma^*\mathcal{L}' = \mathcal{L}$. □

4.3. **Explicit Weierstrass representations.** Until the end of the present section, let $a, b \in K$ with $4a^3 + 27b^2 \neq 0$ and let E denote the elliptic curve

$$E \ : \ y^2z = x^3 + axz^2 + bz^3. \tag{4.3}$$

In this paper, when talking of a *Weierstrass equation* of a curve E we will mean an equation of the form (4.3), commonly referred to as a short Weierstrass equation of E. In the following definition, the matrix $J_{E,P}$ is equivalent, in the sense of Definition 3.4, to the matrix M_P from [27, Ex. 7.6].

Definition 4.6. Let $P = (\lambda, \mu, 1) \in E(K)$. Then $J_{E,P} \in \mathrm{Mat}_3(K[x, y, z])$ is defined by

$$J_{E,P} = J_{E,P}(x, y, z) = \begin{pmatrix} x - \lambda z & y - \mu z & 0 \\ y + \mu z & \lambda x + (a + \lambda^2)z & x \\ 0 & x & -z \end{pmatrix}.$$

Moreover, the matrix $\mathrm{B}_{E,P} = \mathrm{B}_{E,P}(x, y, z) \in \mathrm{Mat}_6(K[x, y, z])$ is defined as

$$\mathrm{B}_{E,P} = \begin{pmatrix} 0 & J_{E,P} \\ -J_{E,P}^{\mathrm{t}} & 0 \end{pmatrix}$$

and the group $\mathrm{G}_{\mathrm{B}_{E,P}}(K)$ is denoted $\mathrm{G}_{E,P}(K)$.

Note that all (projective) points in $E(K) \setminus \{\mathcal{O}\}$ are of the form $(\lambda, \mu, 1)$ as in Definition 4.6. The following result is the combination of Theorem 5.2, i.e. this paper's Lemma 4.3, and Proposition 7.1 from [27]; cf. also [27, Ex. 7.6]. For an alternative reference, see for instance [40, Th. 1].

Proposition 4.7. *Assume $6K = K$. Then the following hold:*

(1) *the following map is a well-defined bijection*

$$E(K) \setminus \{\mathcal{O}\} \longrightarrow \mathcal{L}_E, \quad P \longmapsto [J_{E,P}].$$

(2) *for $P \in E(K) \setminus \{\mathcal{O}\}$, one has*

$$[J_{E,P}] \in \mathcal{L}_E^{\mathrm{sym}} \iff P \in E[2](K).$$

Remark 4.8. Let $P = (\lambda, \mu, 1) \in E(K)$. Then the following hold:

(1) $J_{E,P}^{\mathrm{t}} = J_{E,\ominus P}$.
(2) $J_{E,P}$ is symmetric if and only if $\mu = 0$, equivalently P has order 2 in $E(K)$.

(3) if $\mu = 0$, then $J_{E,P}$ is equivalent to the following "Hessian matrix":

$$\mathrm{H}_{E,P} = \begin{pmatrix} 3\lambda x + az & y & a\lambda z + ax + 3bz \\ y & x - \lambda z & -\lambda y \\ a\lambda z + ax + 3bz & -\lambda y & a\lambda x + 3\lambda bz + 3bx - a^2 z \end{pmatrix}.$$

This matrix corresponds to one of the three solutions to Hesse's system for E; cf. [24] and, with direct connection to this paper's work, [48, Eq. (1.6)].

Remark 4.9 (Flex points for linearity)**.** An elliptic curve $\tilde{E}$ in $\mathbb{P}^2_K$ is defined by a smooth cubic in $K[y_1, y_2, y_3]$ which, however, need not be in short Weierstrass form. For a K-linear change of coordinates to exist in order to express $\tilde{E}$ by a short Weierstrass equation, a sufficient condition is for $\tilde{E}$ to have a flex point over K. This is explicitly explained in [14, Sec. 4.4] and accounts of this transformation can also be found in [46, Prop. III.3.1] and [47, Sec. 1.3]. Via this change of coordinates, the flex point is mapped to the point at infinity $\mathcal{O} = (0 : 1 : 0)$, given in projective coordinates, which is also taken to be the identity for the group law on $\tilde{E}$. Once this identification is made, it is a classical result that the collection of flex points in $\tilde{E}(K)$ coincides with $\tilde{E}[3](K)$ where the unique element of order 1 is precisely $\mathcal{O}$; cf. [20, Ex. 5.37].

5. Proofs of Theorems A, B, and D

Relying on a number of techniques including the employment of Lie algebras (via the Baer correspondence) and results on the realization of elliptic curves as zero sets of determinants of 3×3 matrices of linear forms, in Sections 5.1, 5.2, and 5.3 we prove Theorems D, A, and B in the forms of Corollary 5.3, Theorem 5.6, and Corollary 5.10, respectively. To this end, we let E denote the elliptic curve

$$E \ : \ y^2 z = x^3 + axz^2 + bz^3, \quad a, b \in K \text{ with } 4a^3 + 27b^2 \neq 0.$$

5.1. **Adjoint algebras for E-groups and the proof of Theorem D.** We are now ready to describe the structure of the adjoint algebras of E-groups coming from an isotropically decomposable B with upper-right corner $\mathrm{M} = J_{E,P}$.

Proposition 5.1. *Assume $K = 2K$, and let $P = (\lambda, \mu, 1) \in E(K)$. Then one has*

$$\mathrm{Adj}(J_{E,P}) = \{(kI_3, kI_3) \mid k \in K\}, \quad \text{and} \quad \mathrm{Adj}(J_{E,P}, J_{E,P}^{\mathrm{t}}) = \begin{cases} \mathrm{Adj}(J_{E,P}) & \text{if } \mu = 0, \\ 0 & \text{otherwise.} \end{cases}$$

Proof. Let $\boldsymbol{z} = (z_1, z_2, z_3)$ be variables. The adjoint algebra $\mathrm{Adj}(J_{E,P})$ is determined by a linear system of 27 equations in 18 variables. We describe an $M(\boldsymbol{z}) \in \mathrm{Mat}_{18\times 27}(K[\boldsymbol{z}])$ such that the left kernel of $M(\lambda, \mu, a + \lambda^2)$ is in bijection with $\mathrm{Adj}(J_{E,P})$. Write $J_{E,P} = Ax + By + Cz$ for $A, B, C \in \mathrm{Mat}_3(K)$ computable from Definition 4.6, and define

(5.1)

$$M(\boldsymbol{z}) = \begin{bmatrix} -A & 0 & 0 & -B & 0 & 0 & -C & 0 & 0 \\ 0 & -A & 0 & 0 & -B & 0 & 0 & -C & 0 \\ 0 & 0 & -A & 0 & 0 & -B & 0 & 0 & -C \\ E_{11} & z_1E_{21} + E_{31} & E_{21} & E_{21} & E_{11} & 0 & -z_1E_{11} - z_2E_{21} & z_2E_{11} + z_3E_{21} & -E_{31} \\ E_{12} & z_1E_{22} + E_{32} & E_{22} & E_{22} & E_{12} & 0 & -z_1E_{12} - z_2E_{22} & z_2E_{12} + z_3E_{22} & -E_{32} \\ E_{13} & z_1E_{23} + E_{33} & E_{23} & E_{23} & E_{13} & 0 & -z_1E_{13} - z_2E_{23} & z_2E_{13} + z_3E_{23} & -E_{33} \end{bmatrix},$$

where E_{ij} is the 3×3 matrix with 1 in the (i, j)-entry and 0 elsewhere.

By performing Gaussian elimination over $K[\boldsymbol{z}]$ on the columns of $M(\boldsymbol{z})$, one can conclude that the left kernel of $M(\boldsymbol{z})$ is 1-dimensional, regardless of the values of λ, μ, or

a. The computations have been carried out in SageMath [49] and Magma [5]. Now, since the adjoint algebra is unital, the left kernel of $M(\boldsymbol{z})$ being 1-dimensional implies that $\mathrm{Adj}(J_{E,P}) \cong K$.

For $\mathrm{Adj}(J_{E,P}, J_{E,P}^{\mathrm{t}})$, Remark 4.8(2) ensures that, if $\mu = 0$, then $\mathrm{Adj}(J_{E,P}, J_{E,P}^{\mathrm{t}}) = \mathrm{Adj}(J_{E,P})$. Now assume that $\mu \neq 0$. A matrix $M'(\boldsymbol{z})$ whose left kernel defines a basis for $\mathrm{Adj}(J_{E,P}, J_{E,P}^{\mathrm{t}})$, at $\boldsymbol{z} = (\lambda, \mu, a + \lambda^2)$, is obtained from $M(\boldsymbol{z})$ by replacing the three blocks $-C$ with $-C^{\mathrm{t}}$. By performing Gaussian elimination over $K[\boldsymbol{z}]$ one can show that $M'(\boldsymbol{z})$ has full rank, implying $\mathrm{Adj}(J_{E,P}, J_{E,P}^{\mathrm{t}}) = 0$. These computations have also been carried out in SageMath and Magma. □

Remark 5.2. The consequence of Proposition 5.1, combined with Remark 4.8, is that for all skew-symmetric matrices $\mathrm{S} \in \mathrm{Mat}_3(K)$, the matrix $\mathrm{B} = \begin{pmatrix} 0 & J_{E,P} \\ -J_{E,P}^{\mathrm{t}} & \mathrm{S} \end{pmatrix}$ is half-generic.

Corollary 5.3. *Let $t : V \times V \to T$ be a fully-nondegenerate alternating K-tensor whose Pfaffian defines a smooth cubic E in $\mathbb{P}^2_K$ with a flex point $\mathcal{O} \in E(K)$. Assume $6K = K$. Then the following hold.*

(1) $|\mathcal{T}(t)| = 2$ *if and only if* $\mathrm{Adj}(t) \cong \mathbf{X}_1(K)$.
(2) $|\mathcal{T}(t)| > 2$ *if and only if* $\mathrm{Adj}(t) \cong \mathbf{S}_2(K)$.

Proof. Since t is fully-nondegenerate with a Pfaffian defining a smooth cubic in $\mathbb{P}^2_K$, one has $\dim_K V = 6$ and $\dim_K T = 3$. Let $\mathrm{B} \in \mathrm{Mat}_6(K[y_1, y_2, y_3]_1)$ be associated with t.

First we assume $|\mathcal{T}(t)| \geqslant 2$. Without loss of generality, assume B is isotropically decomposed with top right 3×3 block equal to M. Since $\mathrm{char}(K) \notin \{2, 3\}$ and $\mathrm{Pf}(\mathrm{B})$ has a K-rational flex, Remark 4.9 together with Proposition 4.5 ensure the existence of a pair (E, P) such that $[\![\mathrm{M}]\!] = [\![J_{E,P}]\!]$. Therefore, $\mathrm{Adj}(\mathrm{M}) \cong \mathrm{Adj}(J_{E,P})$, and by Proposition 5.1, the tensor t is half-generic. The forward directions for both (1) and (2) follow from Theorem 3.13. The reverse directions for both follow from Proposition 3.12. □

Proof of Theorem D. If t is the tensor associated to the matrix B from Theorem D, then by Corollary 5.3 the following equivalences hold

$$|\mathcal{T}(t)| = 2 \iff \mathrm{Adj}(t) \cong \mathbf{X}_1(K), \quad |\mathcal{T}(t)| > 2 \iff \mathrm{Adj}(t) \cong \mathbf{S}_2(K).$$

Relying on B being (a)symmetrically half-generic, as is done in the proof Theorem 3.13, combining Proposition 5.1 with Remark 4.8 we deduce that

$$|\mathcal{T}(t)| = 2 \iff P \in E(K) \setminus E[2](K), \quad |\mathcal{T}(t)| > 2 \iff P \in E[2](K) \setminus \{\mathcal{O}\}. \qquad \square$$

5.2. **Isomorphism testing via isogenies and the proof of Theorem A.** In this section, we give necessary and sufficient conditions for two groups of the form $\mathrm{G}_{E,P}(F)$ and $\mathrm{G}_{E',P'}(F)$ to be isomorphic.

Lemma 5.4. *Define the following matrices in* $\mathrm{GL}_3(K)$*:*

$$X_0 = \begin{pmatrix} -1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \quad \text{and} \quad Z_0 = \begin{pmatrix} -1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & -1 \end{pmatrix}.$$

For every elliptic curve E in short Weierstrass form over K and every $P \in E(K) \setminus \{\mathcal{O}\}$, the following equality holds:

$$\begin{pmatrix} 0 & X_0 \\ X_0 & 0 \end{pmatrix} \mathrm{B}_{E,P}(Z_0 \boldsymbol{y}) \begin{pmatrix} 0 & X_0 \\ X_0 & 0 \end{pmatrix} = \mathrm{B}_{E,P}(\boldsymbol{y}).$$

For the next result, recall that a group G acts *k-transitively* on a set X if its induced action $g\cdot(x_1,\dots,x_k)=(g(x_1),\dots,g(x_k))$ on the subset of X^k of all elements with pairwise distinct entries is transitive. The next result is an easy consequence of [48, Prop. 4.10].

Lemma 5.5. *Let E be an elliptic curve in short Weierstrass form over the field K and let $P\in E[2](K)\setminus\{\mathcal{O}\}$. Define, moreover, $\psi:\mathrm{GL}_2(K)\to\mathrm{GL}_6(K)$ by*

$$\begin{pmatrix} a & b\\ c & d\end{pmatrix}\longmapsto\begin{pmatrix} aI_3 & bI_3\\ cI_3 & dI_3\end{pmatrix}.$$

Then $\psi(\mathrm{GL}_2(K))$ acts 2-transitively on $\mathcal{T}(\mathrm{B}_{E,P})$.

Theorem 5.6. *Let E and E' be elliptic curves in $\mathbb{P}^2_F$ given by Weierstrass equations, and let $P\in E(F)\setminus\{\mathcal{O}\}$ and $P'\in E'(F)\setminus\{\mathcal{O}'\}$. Assume $\mathrm{char}(F)=p\geqslant 5$. Then the following are equivalent.*

1. *The F-Lie algebras $\mathfrak{g}_{E,P}(F)$ and $\mathfrak{g}_{E',P'}(F)$ are isomorphic.*
2. *The set $\Psi\mathrm{Isom}_F(\mathrm{B}_{E,P},\mathrm{B}_{E',P'})$ is nonempty.*
3. *There exists an isomorphism $\varphi:E\to E'$ of elliptic curves such that $\varphi(P)=P'$.*

Proof. Let $t:U\times W\to T$ and $t':U'\times W'\to T'$ be the F-tensors defined by $J_{E,P}$ and $J_{E',P'}$, respectively. Up to postcomposing with the automorphisms from Lemma 5.4 or Lemma 5.5, the Lie algebras $\mathfrak{g}_{E,P}(F)$ and $\mathfrak{g}_{E',P'}(F)$ are isomorphic if and only if there exists an isomorphism $\mathfrak{g}_{E,P}(F)\to\mathfrak{g}_{E',P'}(F)$ mapping U to U' and W to W', which is equivalent to saying there are matrices $X,Y,Z\in\mathrm{GL}_3(F)$ such that (X,Y,Z) is an F-isotopism $t\to t'$. In particular, $\mathfrak{g}_{E,P}(F)$ and $\mathfrak{g}_{E',P'}(F)$ are isomorphic if and only if $[\![J_{E',P'}]\!]=[\![J_{E,P}]\!]$; cf. Definition 4.4.

Now let $\mathcal{L}$ and $\mathcal{L}'$ be line bundles on $C=E$ and $C'=E'$ and let $\gamma:E\to E'$ be linear as given by Proposition 4.5. Without loss of generality, we take $\mathcal{L}=\mathcal{L}(P-\mathcal{O})$ and $\mathcal{L}'=\mathcal{L}(P'-\mathcal{O}')$; cf. (4.1) and (4.2). Moreover, note that the line bundles $\mathcal{M}=\mathcal{L}(3\mathcal{O})$ and $\mathcal{M}'=\mathcal{L}(3\mathcal{O}')$ define the given embeddings of $E\to\mathbb{P}^2_F$ and $E'\to\mathbb{P}^2_F$; see also [46, Prop. III.3.1]. In particular, the condition on the map γ can be replaced with the existence of a (not necessarily linear) isomorphism $\delta:E\to E'$ such that

$$\delta^*\mathcal{L}'=\mathcal{L}\text{ and }\delta^*\mathcal{M}'=\mathcal{M}. \tag{5.2}$$

We now show that the existence of δ satisfying (5.2) is equivalent to the existence of an isomorphism of elliptic curves $\varphi:E\to E'$ with the property that $\varphi(P)=P'$. By using the symbol δ also for the map $\mathrm{Div}(E)\to\mathrm{Div}(E')$ that is induced by δ, we rewrite (5.2) as

$$\delta^*\mathcal{L}'=\mathcal{L}\text{ and }\mathcal{L}(3\delta^{-1}(\mathcal{O}'))=\delta^*\mathcal{L}(3\mathcal{O}')=\delta^*\mathcal{M}'=\mathcal{M}=\mathcal{L}(3\mathcal{O}).$$

We derive from Lemma 4.1 that $[3\delta^{-1}(\mathcal{O}')]=[3\mathcal{O}]$, in other words $[3(\delta^{-1}(\mathcal{O}')-3\mathcal{O})]=0$. It now follows from Abel's Theorem, i.e. Lemma 4.2, that $[3](\delta^{-1}(\mathcal{O}')\ominus\mathcal{O})=\mathcal{O}$ and so $\delta^{-1}(\mathcal{O}')$ belongs to $E[3](F)$. Let τ denote translation by $\delta^{-1}(\mathcal{O}')$ on E. We then get that $\delta\circ\tau:E\to E'$ is an isomorphism of elliptic curves. Set $\varphi=\delta\circ\tau$. To conclude the proof, we show that $\varphi(P)=P'$. For this, note that $\varphi^*\mathcal{L}=\varphi^*\mathcal{L}(P-\mathcal{O})=\mathcal{L}(\varphi^{-1}(P)-\varphi^{-1}(\mathcal{O}))$. As a consequence, (5.2) and Lemma 4.1 yield

$$[\varphi^{-1}(P')-\mathcal{O}]=[\varphi^{-1}(P')-\varphi^{-1}(\mathcal{O}')]=[P-\mathcal{O}].$$

Abel's Theorem implies now that $\varphi^{-1}(P')=P$ equivalently that $\varphi(P)=P'$. □

Proof of Theorem A. Let $t:U\times W\to T$ and $t':U'\times W'\to T'$ be the F-tensors defined by $J_{E,P}$ and $J_{E',P'}$, respectively. By Theorem 2.13, the groups $\mathrm{G}_{E,P}(F)$ and $\mathrm{G}_{E',P'}(F)$ are isomorphic if and only if there exists an $\mathbb{F}_p$-pseudo isometry between t and t'. From

Corollary 5.3, we know that $\mathrm{Cent}(t) \cong \mathrm{Cent}(t') \cong F$. Thus, arguing as in the proof of Theorem 2.15, we get that $\Psi\mathrm{Isom}_{\mathbb{F}_p}(t,t')$ can be considered as contained in the set $\Psi\mathrm{Isom}_F(t,t') \times \mathrm{Gal}(F/\mathbb{F}_p)$. Therefore, t and t' are $\mathbb{F}_p$-pseudo isometric if and only if there exists $\sigma \in \mathrm{Gal}(F/\mathbb{F}_p)$ such that ${}^\sigma t$ and t' are F-pseudo isometric. The matrix of linear forms associated to ${}^\sigma t$ is $\mathrm{B}_{\sigma(E),\sigma(P)}$. Again by Theorem 2.13, the tensors ${}^\sigma t$ and t' are F-pseudo isometric if and only if $\mathfrak{g}_{\sigma(E),\sigma(P)}(F)$ and $\mathfrak{g}_{E',P'}(F)$ are isomorphic F-Lie algebras. To conclude apply Theorem 5.6. □

Remark 5.7 (The work of Ng)**.** For a nice overview of the geometry of the Γ-orbits of $\mathcal{L}_\mathcal{C}$ we refer to [38, Sec. 2]. Theorem 5.6 is a specialized variation of Theorem 1 of [38], which classifies the complex Γ-orbits in terms of triples (E, L_1, L_2) where L_1 and L_2 are particularly chosen line bundles on E; cf. (5.2). The study in [38] goes beyond the smooth case classifying also singular cuboids up to Γ-equivalence. In future work, we hope to come back to the investigation of the class of groups arising from this last family.

5.3. **Automorphisms of elliptic groups and the proof of Theorem B.** In this section we compute the size of the automorphism group of a group arising from a tensor satisfying $\mathcal{T}(t) \geqslant 2$ and whose Pfaffian class defines a cubic with a flex point over F. Indeed, using pseudo-isometries, any such curve can be put in short Weierstrass equation, and thus the group in question will be isomorphic to a group of the form $\mathrm{G}_{E,P}(F)$.

Theorem 5.8. *Let E be an elliptic curve in $\mathbb{P}^2_F$ given by a Weierstrass equation, and let $P \in E(F) \setminus \{\mathcal{O}\}$. Assume that* $\mathrm{char}(F) = p \geqslant 5$*. Then*

$$|\Psi\mathrm{Isom}_F(\mathrm{B}_{E,P})| = \frac{|\mathrm{Aut}_\mathcal{O}(E)|}{|\mathrm{Aut}_\mathcal{O}(E) \cdot P|} \cdot |E[3](F)| \cdot \begin{cases} |\mathrm{GL}_2(F)| & \text{if } P \in E[2](F), \\ 2(q-1)^2 & \text{otherwise.} \end{cases}$$

Proof. Let $t : V \times V \to T$ be the tensor defined by $\mathrm{B}_{E,P} \in \mathrm{Mat}_6(F[y_1,y_2,y_3])$ and let $\mathfrak{g} = \mathfrak{g}_t(F)$ be the Lie algebra of $\mathrm{G}_t(F)$ via the Baer correspondence. We compute the order of $\Psi\mathrm{Isom}_F(t)$. Following the strategy in [48], we work with the automorphism group $\mathrm{Aut}(\mathfrak{g}) = \mathrm{Aut}_F(\mathfrak{g})$ of the F-algebra $\mathfrak{g}$. For this, let U, W be distinct elements of $\mathcal{T}(t)$ corresponding to the base choice yielding $\mathrm{B}_{E,P}$ and note that $V = U \oplus W$. We define the following subgroups of $\mathrm{Aut}(\mathfrak{g})$:

- $\mathrm{Aut}_V(\mathfrak{g}) = \{\alpha \in \mathrm{Aut}(\mathfrak{g}) \mid \alpha(V) = V\}$ and
- $\mathrm{Aut}^f_V(\mathfrak{g}) = \{\alpha \in \mathrm{Aut}(\mathfrak{g}) \mid \alpha(U) = U,\ \alpha(W) = W\}$.

Since t is full, if $(\alpha, \beta) \in \Psi\mathrm{Isom}_F(t)$, then α uniquely determines β. In particular, we have that $\Psi\mathrm{Isom}_F(t) \cong \mathrm{Aut}_V(\mathfrak{g})$. We now look at the action of $\mathrm{Aut}_V(\mathfrak{g})$ on $\mathcal{T}(t)$. Using Lemmas 5.4 and 5.5, we derive that this action is 2-transitive. It follows that the stabilizer of the pair (U, W) is equal to $\mathrm{Aut}^f_V(\mathfrak{g})$ and has index $|\mathcal{T}(t)|(|\mathcal{T}(t)| - 1)$ in $\mathrm{Aut}_V(\mathfrak{g})$. By Corollary 3.6, it thus holds that

$$|\Psi\mathrm{Isom}_F(\mathrm{B}_{E,P})| = |\mathrm{Aut}_V(\mathfrak{g})| = |\mathrm{Aut}^f_V(\mathfrak{g})| \cdot \begin{cases} q(q+1) & \text{if } P \in E[2](F), \\ 2 & \text{otherwise.} \end{cases} \tag{5.3}$$

To determine $|\mathrm{Aut}^f_V(\mathfrak{g})|$ we note that, via Remark 2.10, an element

$$\mathrm{diag}(X,Y,Z) = \begin{pmatrix} X & 0 & 0 \\ 0 & Y & 0 \\ 0 & 0 & Z \end{pmatrix} \in \mathrm{GL}_9(F), \text{ with } X,Y,Z \in \mathrm{GL}_3(F)$$

belongs to $\mathrm{Aut}_V^f(\mathfrak{g})$ if and only if $X^{\mathrm{t}} J_{E,P}(Z\boldsymbol{y})Y = J_{E,P}(\boldsymbol{y})$. Since the change of coordinates given by Z maps E to itself, the following map is well defined

$$\varphi : \mathrm{Aut}_V^f(\mathfrak{g}) \to \mathrm{Aut}(E), \quad \mathrm{diag}(X, Y, Z) \mapsto Z.$$

Thus, φ maps into the linear part of $\mathrm{Aut}(E)$, namely those automorphisms of E that extend to linear transformations of $\mathbb{P}^2_F$. From the proof of Theorem 5.6, we know that

$$|\operatorname{im}\varphi| = |E[3](F)| \cdot |\{\varphi \in \mathrm{Aut}_{\mathcal{O}}(E) : \varphi(P) = P\}| = |E[3](F)| \cdot \frac{|\mathrm{Aut}_{\mathcal{O}}(E)|}{|\mathrm{Aut}_{\mathcal{O}}(E) \cdot P|}.$$

We claim that $|\ker\varphi| = (q-1)^2$. To prove this, we start by observing that

$$\ker\varphi = \{\mathrm{diag}(X, Y, cI_3) \mid X, Y \in \mathrm{GL}_3(F),\, c \in F^\times, X^{\mathrm{t}} J_{E,P}(c\boldsymbol{y})Y = J_{E,P}(\boldsymbol{y})\}.$$

The last equality in the definition of $\ker\varphi$ can be rewritten as $(cX^{\mathrm{t}})J_{E,P}Y = J_{E,P}$, so since Y is invertible, we get a map

$$\ker\varphi \longrightarrow \mathrm{Adj}(J_{E,P}), \quad \mathrm{diag}(X, Y, cI_3) \longmapsto (cX, Y^{-1}).$$

All elements of the form $(aI_3, bI_3, (ab)^{-1}I_3)$ with $a, b \in F^\times$ are elements of $\ker\varphi$, and as a consequence of Proposition 5.1, the converse is also true. Indeed, if $\mathrm{diag}(X, Y, cI_3)$ belongs to $\ker\varphi$, then (cX, Y^{-1}) is an element of $\mathrm{Adj}(J_{E,P}) = \{(kI_3, kI_3) \mid k \in F\}$. In particular, there exists $k \in F^\times$ such that $cX = kI_3 = Y^{-1}$. It then follows that $X = c^{-1}kI_3$ and $Y = k^{-1}I_3$. Thus, $\ker\varphi = \{(aI_3, bI_3, (ab)^{-1}I_3) \mid a, b \in F^\times\}$, and we conclude that $|\ker\varphi| = |F^\times|^2 = (q-1)^2$. Since $|\mathrm{GL}_2(F)| = q(q+1)(q-1)^2$ the proof is complete. □

For an elliptic curve E in $\mathbb{P}^2_F$ given by a short Weierstrass equation and $P \in E(F)\setminus\{\mathcal{O}\}$, we write

$$\mathrm{Gal}_{E,P}(F/\mathbb{F}_p) = \{\sigma \in \mathrm{Gal}(F/\mathbb{F}_p) \,:\, \Psi\mathrm{Isom}(\mathrm{B}_{E,P}, \mathrm{B}_{\sigma(E),\sigma(P)}) \neq \varnothing\}.$$

The following two corollaries follow in a straightforward way from Theorem 2.15 and Theorem 5.8. Note that the denominators on the left side are $|\mathrm{Hom}_F(V,T)|$ and $|\mathrm{Hom}_{\mathbb{F}_p}(V,T)|$, respectively.

Corollary 5.9. *Let E be an elliptic curve in $\mathbb{P}^2_F$ given by a Weierstrass equation. Moreover, let $P \in E(F) \setminus \{\mathcal{O}\}$. Assume that $\mathrm{char}(F) = p \geqslant 5$. Then the following holds:*

$$\frac{|\mathrm{Aut}_F(\mathfrak{g}_{E,P}(F))|}{q^{18}} = |E[3](F)| \cdot \frac{|\mathrm{Aut}_{\mathcal{O}}(E)|}{|\mathrm{Aut}_{\mathcal{O}}(E) \cdot P|} \cdot \begin{cases} |\mathrm{GL}_2(F)| & \text{if } P \in E[2](F), \\ 2(q-1)^2 & \text{otherwise.} \end{cases}$$

Corollary 5.10. *Let E be an elliptic curve in $\mathbb{P}^2_F$ given by a Weierstrass equation and $P \in E(F) \setminus \{\mathcal{O}\}$. Assume that $\mathrm{char}(F) = p \geqslant 5$ and $|F| = p^e$. Then the following holds:*

$$\frac{|\mathrm{Aut}(\mathrm{G}_{E,P}(F))|}{p^{18e^2}} = |\mathrm{Gal}_{E,P}(F/\mathbb{F}_p)| \cdot |E[3](F)| \cdot \frac{|\mathrm{Aut}_{\mathcal{O}}(E)|}{|\mathrm{Aut}_{\mathcal{O}}(E) \cdot P|} \cdot \begin{cases} |\mathrm{GL}_2(F)| & \text{if } P \in E[2](F), \\ 2(p^e-1)^2 & \text{otherwise.} \end{cases}$$

Remark 5.11. Let E be an elliptic curve given by the Weierstrass equation (4.3) over F and let $P = (\lambda, \mu, 1) \in E(F)$. To compute the size of $\mathrm{Gal}_{E,P}(F/\mathbb{F}_p)$ one can rely on Theorem 5.6 in the following way. For σ to belong to $\mathrm{Gal}_{E,P}(F/\mathbb{F}_p)$ a necessary and sufficient condition is that $\Psi\mathrm{Isom}_F(\mathrm{B}_{E,P}, \mathrm{B}_{\sigma(E),\sigma(P)})$ be non-empty. Thanks to Theorem 5.6 the last condition is equivalent to the existence of an isomorphism of elliptic curves $\varphi : E \to \sigma(E)$ such that $\varphi(P) = \sigma(P)$. With the aid of, for instance, [46, Tab. III.3.1, p. 45], one shows

that such a φ is given by a map $(x,y) \mapsto (u^2x, u^3y)$ where $u \in F$ is chosen such that $(\sigma(\lambda), \sigma(\mu)) = (u^2\lambda, u^3\mu)$ and

$$(u^4, u^6) = \begin{cases} (u^4, \sigma(b)b^{-1}) & \text{if } a = 0 \quad (\text{equiv. } j(E) = 0), \\ (\sigma(a)a^{-1}, u^6) & \text{if } b = 0 \quad (\text{equiv. } j(E) = 1728), \\ (\sigma(a)a^{-1}, \sigma(b)b^{-1}) & \text{otherwise.} \end{cases}$$

Example 5.12. Let E be the elliptic curve defined over $\mathbb{F}_5$ by $y^2 = x^3 - 2x$ and note that $E[2](\mathbb{F}_5) = \{\mathcal{O}, (0,0)\}$ while, setting $F = \mathbb{F}_5[\sqrt{2}]$, we get

$$E[2](F) = \{\mathcal{O}, (0,0), (\sqrt{2}, 0), (-\sqrt{2}, 0)\}.$$

The matrices $J_{E,P}$ corresponding to $P \in E[2](F) \setminus \{\mathcal{O}\}$ are equivalent to the Hessian matrices given in [48, Sec. 1.4] where δ is chosen to be 2. We show that for each choice of P, the group $\mathrm{Gal}_{E,P}(F/\mathbb{F}_p)$ coincides with $\mathrm{Gal}(F/\mathbb{F}_p)$. For this, we note that in this case $b = 0$, so we can identify $\mathrm{Aut}_{\mathcal{O}}(E)$ with $\mathbb{F}_5^\times$; cf. [46, Sec. III.10]. Following the notation from Remark 5.11, we fill the following table:

σ	u^4	$\sigma(0,0)$	$\sigma(\sqrt{2},0)$	$\sigma(-\sqrt{2},0)$
id	1	$(0,0)$	$(\sqrt{2},0)$	$(-\sqrt{2},0)$
$x \mapsto x^5$	1	$(0,0)$	$(-\sqrt{2},0)$	$(\sqrt{2},0)$

Taking $u = 1$ in the first row and $u = 2$ in the second yields the claim.

Example 5.13. Let $f(x) = x^2 - x + 2 \in \mathbb{F}_5[x]$, which is irreducible. Set $F = \mathbb{F}_5[x]/(f(x))$, and let $\alpha \in F$ be a root of f. Let E be the elliptic curve in $\mathbb{P}^2_F$ given by $y^2 = x^3 + \alpha x + \alpha$. The j-invariant of E is $\alpha - 1$. Let $\sigma \in \mathrm{Gal}(F/\mathbb{F}_5)$ be the map $x \mapsto x^5$ so that $\sigma(E)$ is defined by $y^2 = x^3 + \alpha^5 x + \alpha^5$. The j-invariant of $\sigma(E)$ is $\alpha^5 - 1 = -\alpha$, so the elliptic curves E and $\sigma(E)$ are not isomorphic. Let now $P = (\alpha^3, \alpha) \in E(F)$ and note that $\sigma(P) = (\alpha^{15}, \alpha^5) \in \sigma(E)(F)$. It follows that $\mathfrak{g} = \mathfrak{g}_{E,P}(F)$ and $\mathfrak{g}_\sigma = \mathfrak{g}_{\sigma(E),\sigma(P)}(F)$ are not isomorphic as F-Lie algebras – that is, there is no F-linear isomorphism $\mathfrak{g} \to \mathfrak{g}_\sigma$ since E and $\sigma(E)$ are not isomorphic. However, $(I_9, \sigma) \in \mathrm{GL}_9(F) \rtimes \mathrm{Gal}(F/\mathbb{F}_5)$ yields an F-semilinear isomorphism $\mathfrak{g} \to \mathfrak{g}_\sigma$. Thus, as $\mathbb{F}_5$-Lie algebras, $\mathfrak{g} \cong \mathfrak{g}_\sigma$ and, consequently, $\mathrm{G}_{E,P}(F) \cong \mathrm{G}_{\sigma(E),\sigma(P)}(F)$. To make this isomorphism explicit, observe that

$$J = J_{E,P} = \begin{pmatrix} x - \alpha^3 z & y - \alpha z & 0 \\ y + \alpha z & \alpha^3 x + (\alpha + \alpha^6) z & x \\ 0 & x & -z \end{pmatrix}. \tag{5.4}$$

Viewing F as a 2-dimensional vector space with basis $\{1, \alpha\}$ over $\mathbb{F}_5$, we rewrite J from (5.4) as an $\mathbb{F}_5$-tensor $\mathbb{F}_5^6 \times \mathbb{F}_5^6 \to \mathbb{F}_5^6$. The associated matrix of linear forms is

$$\overline{J} = \begin{pmatrix} x_1 + 2z_1 + z_2 & x_2 + 3z_1 + 3z_2 & y_1 - z_2 & y_2 + 2z_1 - z_2 & 0 & 0 \\ x_2 + 3z_1 + 3z_2 & 3x_1 + x_2 - z_1 + z_2 & y_2 + 2z_1 - z_2 & 3y_1 + y_2 + 2z_1 + z_2 & 0 & 0 \\ y_1 + z_2 & y_2 + 3z_1 + z_2 & 3x_1 - x_2 + 2z_1 + z_2 & 2x_1 + 2x_2 + 3z_1 + 3z_2 & x_1 & x_2 \\ y_2 + 3z_1 + z_2 & 3y_1 + y_2 + 3z_1 - z_2 & 2x_1 + 2x_2 + 3z_1 + 3z_2 & x_1 - x_2 - z_1 + z_2 & x_2 & 3x_1 + x_2 \\ 0 & 0 & x_1 & x_2 & -z_1 & -z_2 \\ 0 & 0 & x_2 & 3x_1 + x_2 & -z_2 & 2z_1 - z_2 \end{pmatrix}.$$

We do the same construction for the matrix $\sigma(J)$ associated to $\sigma(E)$ and $\sigma(P)$:

$$\overline{\sigma(J)} = \begin{pmatrix} x_1 + 3z_1 - z_2 & x_2 + 2z_1 + 2z_2 & y_1 - z_1 + z_2 & y_2 + 3z_1 & 0 & 0 \\ x_2 + 2z_1 + 2z_2 & 3x_1 + x_2 + z_1 - z_2 & y_2 + 3z_1 & 3y_1 + y_2 + 3z_2 & 0 & 0 \\ y_1 + z_1 - z_2 & y_2 + 2z_1 & 2x_1 + x_2 + 3z_1 - z_2 & 3x_1 + 3x_2 + 2z_1 + 2z_2 & x_1 & x_2 \\ y_2 + 2z_1 & 3y_1 + y_2 + 2z_2 & 3x_1 + 3x_2 + 2z_1 + 2z_2 & -x_1 + x_2 + z_1 - z_2 & x_2 & 3x_1 + x_2 \\ 0 & 0 & x_1 & x_2 & -z_1 & -z_2 \\ 0 & 0 & x_2 & 3x_1 + x_2 & -z_2 & 2z_1 - z_2 \end{pmatrix}.$$

To define the isomorphism corresponding to (I_9, σ), we define a 6×6 block diagonal matrix $D = \mathrm{diag}(X, X, X)$ by setting

$$X = \begin{pmatrix} 1 & 1 \\ 0 & -1 \end{pmatrix}.$$

Note that $X^{-1} = X$. One can check that $D^{\mathrm{t}}\overline{J}(D\boldsymbol{x})D = \overline{\sigma(J)}$, implying that

$$\begin{pmatrix} D^{\mathrm{t}} & 0 \\ 0 & D^{\mathrm{t}} \end{pmatrix} \begin{pmatrix} 0 & \overline{J}(D\boldsymbol{x}) \\ -\overline{J}^{\mathrm{t}}(D\boldsymbol{x}) & 0 \end{pmatrix} \begin{pmatrix} D & 0 \\ 0 & D \end{pmatrix} = \begin{pmatrix} 0 & \overline{\sigma(J)} \\ -\overline{\sigma(J)}^{\mathrm{t}} & 0 \end{pmatrix}.$$

Thus, $(\mathrm{diag}(D, D), D)$ is an $\mathbb{F}_5$-pseudo isometry, and therefore, $\mathrm{G}_{E,P}(F) \cong \mathrm{G}_{\sigma(E),\sigma(P)}(F)$. This argument also shows that the Galois part of $\mathrm{Aut}(\mathrm{G}_{E,P}(F))$ must be trivial – otherwise one would for example get that E and $\sigma(E)$ are isomorphic. Theorem 2.15 yields

$$\mathrm{Aut}(\mathrm{G}_{E,P}(F)) \cong \mathrm{Hom}_{\mathbb{F}_5}(\mathbb{F}_5^{12}, \mathbb{F}_5^6) \rtimes \Psi\mathrm{Isom}_F(\mathrm{B}_{E,P}).$$

6. Isomorphism testing for E-groups

The main goal of this section is to prove Theorem E, which we do in Section 6.3. For this, we develop a number of algorithms to recognize when a p-group is (isomorphic to) an E-group. We even consider the more general situation computing an isotropic decomposition of alternating tensors with irreducible Pfaffian in Section 6.2. We end with a discussion in Section 6.4 about our implementation of Theorem E in Magma [5], where we also provide some examples.

6.1. **Computational models for finite groups.** Common computational models for finite groups are given by (small) sets of generators in either (1) matrix groups over finite fields [32] or (2) permutation groups [44]. Although polycyclic and "power-commutator" presentations seem to work well in practice, it is not known whether multiplication with these presentations can be done in polynomial time [31].

Throughout, we work with the "permutation group quotient" model proposed by Kantor and Luks in [29]. This avoids issues where the given p-group G can only be faithfully represented as a permutation group on a set whose size is approximately $|G|$; see Neumann's example in [37]. The following proposition ensures that we can efficiently go from groups to tensors using the permutation group quotient model. With appropriate bounds for the prime p, one can achieve this for the matrix group model as well [32].

Proposition 6.1 ([29, Sec. 4])**.** *Given a group G as a quotient of a permutation group, each of the following problems has an algorithm that runs in time polynomial in $\log|G|$.*

1. *Compute $|G|$.*
2. *Given $x, x_1, \ldots, x_k \in G$ either write x as a word in $\{x_1, \ldots, x_k\}$, or else prove $x \notin \langle x_1, \ldots, x_k\rangle$.*
3. *Find generators for $\mathrm{Z}(G)$ and for $[G, G]$.*
4. *Decide if G is nilpotent of class 2.*
5. *If G is nilpotent of class 2, construct the commutator tensor of G as a matrix of linear forms.*

6.2. **Isotropic decompositions.** We depart from the focused setting of E-groups, and we consider the more general setting of computing an isotropic decomposition for an alternating F-tensor $t : V \times V \to T$.

Theorem 6.2. *Let* $\mathrm{B} \in \mathrm{Mat}_{2n}(F[y_1, \ldots, y_d]_1)$ *be skew-symmetric. Then there exist Las Vegas algorithms, using* $O(n^6 d + n^2 d^5)$ *and* $O(n^6 d)$ *operations in* F *respectively, to do the following.*

1. *Write* B *over* $C = \mathrm{Cent}(\mathrm{B})$*, provided* C *is a field, call it* B_C*.*
2. *Return* $X \in \mathrm{GL}_{2n}(F)$ *such that* $X^{\mathrm{t}} \mathrm{B}_C X$ *gives an isotropic decomposition whenever* B_C *is decomposable with irreducible Pfaffian.*

We prove Theorem 6.2 with the next two lemmas. Common to both algorithms, and also their bottleneck, is computing a basis of a large system of linear equations.

Lemma 6.3. *There exists a Las Vegas algorithm that, given* $\mathrm{B} \in \mathrm{Mat}_{m \times n}(F[y_1, \ldots, y_d]_1)$*, decides whether its centroid is a field extension* C/F *and, if so, returns the matrix of linear forms* B_C *over* C *using* $O(mnd(m^2 + n^2 + d^2)^2)$ *operations in* F*.*

Proof. Algorithm. Compute a basis for the centroid $C = \mathrm{Cent}(\mathrm{B})$ by solving a system of linear equations. Use [11, Th. 1.3] to determine if C is a field or not, and if C is a field, then find a generator $X = (X_1, X_2, X_3)$ of C as a unital F-algebra. If C is not a field, then just return B, so we assume C is a field. Let $V_1 = F^m$, $V_2 = F^n$, and $V_3 = F^d$. Find a maximal set of nonzero vectors $\mathcal{B}_i$ in V_i which are all in different X_i orbits. For each $(u, v) \in \mathcal{B}_1 \times \mathcal{B}_2$, write $u^{\mathrm{t}} \mathrm{B}\, v$ as $\sum_{w \in \mathcal{B}_3} f_{u,v}^{(w)}(X) w$, where $f_{u,v}^{(w)}(z) \in F[z]$. Return the matrix $\mathrm{B}_C = (f_{u,v}^{(w)}(X))_{u,v,w}$, running through all $(u, v, w) \in \mathcal{B}_1 \times \mathcal{B}_2 \times \mathcal{B}_3$.

Correctness. We only ever proceed beyond the construction of a basis for C if C is a field. In this case, the V_i are C-vector spaces. The sets $\mathcal{B}_i$ are C-bases for the V_i.

Complexity. A basis for the centroid C is computed by solving a homogeneous system of mnd linear equations in $m^2 + n^2 + d^2$ variables over F. By [11, Th. 1.3], determining whether or not C is a field is done constructively in polynomial time using a Las Vegas algorithm, but this complexity is dominated by the complexity to compute a basis for C. The complexity to find bases $\mathcal{B}_i$ and rewrite B over C is also dominated by the complexity for the centroid. □

Lemma 6.4. *There is an algorithm that, given* $\mathrm{B} \in \mathrm{Mat}_{2n}(F[y_1, \ldots, y_d]_1)$ *skew-symmetric, returns* $X \in \mathrm{GL}_{2n}(F)$ *such that* $X^{\mathrm{t}} \mathrm{B} X$ *gives an isotropic decomposition whenever* B *is decomposable with irreducible Pfaffian, using* $O(n^6 d)$ *operations in* F*.*

Proof. Algorithm. Compute $A = \mathrm{Adj}(\mathrm{B})$. Determine if A is isomorphic to either $\mathbf{X}_1(F)$ or $\mathbf{S}_2(F)$. If not, report that B is not isotropically decomposable with an irreducible Pfaffian. Otherwise, construct an isomorphism of $*$-algebras $\varphi : A \to S$, where S is either $\mathbf{X}_1(F)$ or $\mathbf{S}_2(F)$. Set

$$\mathcal{E} = \begin{cases} \{E_{11}, E_{22}\} & \text{if } S = \mathbf{S}_2(F), \\ \{(1,0), (0,1)\} & \text{if } S = \mathbf{X}_1(F), \end{cases}$$

where E_{ij} is the matrix with 1 in the (i, j) entry and 0 elsewhere. For each $e \in \mathcal{E}$, set $(Y, Z) = \varphi^{-1}(e) \in A$ and let $U_e \leqslant F^n$ be the column span of Y. Let $\mathcal{B}$ a basis for F^{2n} containing bases for U_e for all $e \in \mathcal{E}$, and return the transition matrix $X \in \mathrm{GL}_{2n}(F)$.

Correctness. By Theorem 3.13, if B is isotropically decomposable with an irreducible Pfaffian, then A is isomorphic to either $\mathbf{X}_1(F)$ or $\mathbf{S}_2(F)$. In both cases, $\mathcal{E}$ is a set of elements in S whose images induce distinct, n-dimensional, totally-isotropic subspaces; cf. the proof of Proposition 3.12. To show that U_e is totally-isotropic, set $(Y, Z) = \varphi^{-1}(e)$. For each $u, v \in F^{2n}$ one has $u^{\mathrm{t}} Y^{\mathrm{t}} \mathrm{B}\, Y v = u^{\mathrm{t}} \mathrm{B}\, Z Y v = 0$, proving that U_e is totally isotropic.

Complexity. A basis for Adj(B) is constructed by solving $n^2 d$ (homogeneous) linear equations in $2n^2$ variables. By [10, Th. 4.1], the complexity for the constructive recognition of $*$-algebras is dominated by the cost of constructing a basis for Adj(B). □

Proof of Theorem 6.2. Use Lemma 6.3 for (1), and for (2), apply Lemma 6.4. □

6.3. **Isomorphism testing of E-groups and the proof of Theorem E.** Theorem 6.2 is almost enough to prove the first two statements of Theorem E. The next lemma fills the gap by providing an algorithm to find flex points on smooth cubics; cf. Remark 4.9.

Lemma 6.5. *Given a homogeneous cubic $f \in F[y_1, y_2, y_3]$, there exists an algorithm that decides if f is smooth and if so returns all $a \in F^3 \setminus \{(0,0,0)\}$ such that $f(a) = 0$ and a is a flex point of f, which uses $O(\log q)$ field operations.*

Proof. Algorithm. Compute a Gröbner basis $\mathcal{G}_1$ for the ideal

$$I_1 = \langle \partial f/\partial y_1, \partial f/\partial y_2, \partial f/\partial y_3, f \rangle \text{ of } F[y_1, y_2, y_3]$$

using the lexicographical monomial order. Let $g \in \mathcal{G}_1$ be homogeneous with at most 2 variables. Factor g using univariate algorithms [53, Ch. 14], and use those solutions to find all the solutions to the polynomial system determined by $\mathcal{G}_1$. If a solution exists, declare f "singular," and return a singular point. Otherwise f is smooth.

Compute the determinant of the Hessian matrix of f, which yields a homogeneous cubic $H \in F[y_1, y_2, y_3]$. Construct a Gröbner basis $\mathcal{G}_2$ for the ideal $I_2 = \langle f, H \rangle$ using the lexicographical monomial order. Return the set of solutions to the polynomial system determined by $\mathcal{G}_2$ in the same fashion as above.

Correctness. The algorithm to decide whether f is smooth is correct by definition and the fact that $\langle \mathcal{G}_1 \rangle = I_1$. The existence of such a $g \in \mathcal{G}_1$ is the content of the Elimination Theorem [13, Sec. 3.1]. If the algorithm starts to compute the flexes, we know that f is, therefore, smooth. By Bézout's theorem the number of flex points is bounded above by 9. Thus, I_2 is 0-dimensional and the flexes are the solutions to the polynomial system determined by $\mathcal{G}_2$.

Complexity. Computing a Gröbner basis for a set of polynomials whose degree and number of variables are constant is done using $O(1)$ field operations. We can solve the polynomial systems determined by $\mathcal{G}_i$ by calling a constant number of univariate factoring algorithms. Since the degrees are bounded by some absolute constant, factoring is done using $O(\log q)$ field operations [53, Ch. 14]. □

Proof of Theorem E(i). By Corollary 5.3, if the G_i are elliptic groups, the $\mathrm{Cent}(t_{G_i})$ are finite extensions of $\mathbb{F}_p$. Write t_{G_i} as a matrix of linear forms $\widetilde{\mathrm{B}}_i \in \mathrm{Mat}_{6m}(\mathbb{F}_p[y_1, \ldots, y_{3m}]_1)$. Use Theorem 6.2(1) to express $\widetilde{\mathrm{B}}_i$ as a matrix of linear forms $\mathrm{B}_i \in \mathrm{Mat}_6(F[y_1, y_2, y_3]_1)$ over the centroid F of $\widetilde{\mathrm{B}}_i$, using $O(m^7)$ field operations. If the algorithm fails at any stage, then G_i is not an elliptic group. Otherwise compute the Pfaffians of B_i. Then apply Lemma 6.5 to decide if the Pfaffians are elliptic curves containing flex points; this uses $O(\log |F|) = O(m \log p)$ field operations. If they are not, then G_i is not isomorphic to some $\mathrm{G}_{E,P}(F)$. □

Now our objective is to develop the algorithms that feed into the algorithm for Theorem 6.8, which is the main algorithm for Theorem E(*ii*). We first describe some algorithms, which will be used in Theorem 6.8, that use a constant number of field operations.

Lemma 6.6. *Assume* $\mathrm{char}(F) \geqslant 5$. *Given an elliptic curve* E *in short Weierstrass form, there is an algorithm returning the set of automorphisms* $\mathrm{Aut}_{\mathcal{O}}(E)$ *as a subgroup of* $\mathrm{GL}_3(F)$ *using* $O(\log q)$ *field operations.*

Proof. Algorithm. Let $\mu_n(F)$ be the set of roots of $x^n - 1$ in F. Define $\mathcal{R}$ to be $\mu_2(F)$, $\mu_4(F)$, $\mu_6(F)$ respectively when $j(E) \neq 0, 1728$ or $j(E) = 1728$ or $j(E) = 0$. Return the subset $\{\mathrm{diag}(\omega^2, \omega^3, 1) \mid \omega \in \mathcal{R}\}$ of $\mathrm{GL}_3(F)$.

Correctness. It follows from [46, Th. III.10.1].

Complexity. Factoring constant-degree univariate polynomials is done using $O(\log q)$ field operations [53, Ch. 14]. □

The following is relevant in view of Remark 2.10.

Proposition 6.7. *Assume* $\mathrm{char}(F) \geqslant 5$. *Given an elliptic curve* E *in short Weierstrass form and* $P \in E(F)$, *there is an algorithm returning a generating set for* $\mathrm{Auto}_F(J_{E,P})$ *using* $O(q^{1/4} \log q)$ *field operations.*

Proof. Algorithm. Initialize $\mathcal{X} = \varnothing$. Use Lemma 6.6 to construct $\mathrm{Aut}_{\mathcal{O}}(E)$, and use Lemma 6.5 to get the set R of flexes of E over F. For each $\Omega \in \mathrm{Aut}_{\mathcal{O}}(E)$ fixing P construct a nonzero $(X_\omega, Y_\omega) \in \mathrm{Adj}(J_{E,P}, J_{E,P}(\Omega \boldsymbol{y}))$ and include $(X_\omega, Y_\omega^{-1}, \Omega)$ in $\mathcal{X}$. For each $Q \in R$, let $\tau_Q \in \mathrm{GL}_3(F)$ be the linear map given by translation by Q on E, and construct a nonzero $(X_Q, Y_Q) \in \mathrm{Adj}(J_{E,P}, J_{E,P}(\tau_Q \boldsymbol{y}))$ and include (X_Q, Y_Q^{-1}, τ_Q) in $\mathcal{X}$. Find $a \in F$ such that $\langle a \rangle = F^\times$. Then return $\mathcal{X} \cup \{(aI_3, I_3, aI_3), (I_3, aI_3, aI_3)\}$.

Correctness. As explained in Remark 4.9, the set R is equal to $E[3](F)$. As it is evident from Remark 2.10 and the proof of Theorem 5.8, the map $\mathrm{Auto}_F(J_{E,P}) \to \mathrm{Aut}_V^f(\mathfrak{g}_{E,P}(F))$ given by $(X, Y, Z) \mapsto \mathrm{diag}(X, Y, Z)$ is an isomorphism, and thus correctness follows from the arguments there presented.

Complexity. The cardinalities of $\mathrm{Aut}_{\mathcal{O}}(E)$ and $E[3](F) = R$ are bounded from above by 6 and 9, respectively. The complexity is dominated by the complexity to find a primitive element of F. From the theorem of [45], finding $a \in F^\times$ such that $\langle a \rangle = F^\times$ can be done in time $O(q^{1/4} \log q)$. □

Theorem 6.8. *Assume* $\mathrm{char}(F) = p \geqslant 5$. *There exists an algorithm that, given a subfield* $L \subset F$ *and isotropically decomposable* $\mathrm{B}, \mathrm{B}' \in \mathrm{Mat}_6(F[y_1, y_2, y_3]_1)$ *whose Pfaffians define elliptic curves in* $\mathbb{P}^2_F$ *with flex points over* L, *returns the possibly empty coset* $\Psi\mathrm{Isom}_L(\mathrm{B}, \mathrm{B}')$ *using* $O(q)$ *field operations.*

Proof. Algorithm. Use Theorem 6.2(2) to rewrite B and B′ such that they are isotropically decomposed. Let $\mathrm{M}, \mathrm{M}' \in \mathrm{Mat}_3(F[y_1, y_2, y_3]_1)$ be the top right 3×3 blocks in B and B′, respectively. Construct $Z, Z' \in \mathrm{GL}_3(F)$ with the property that both $f = \det(\mathrm{M}(Z\boldsymbol{y}))$ and $f' = \det(\mathrm{M}'(Z'\boldsymbol{y}))$ yield short Weierstrass forms of the curves E and E'.

Set $\mathrm{N} = \mathrm{M}(Z\boldsymbol{y})$ and $\mathrm{N}' = \mathrm{M}'(Z'\boldsymbol{y})$ and find $P \in E(F)$ and $P' \in E'(F)$ such that $\mathrm{Adj}(J_{E,P}, \mathrm{N})$ and $\mathrm{Adj}(J_{E',P'}, \mathrm{N}')$ are nontrivial. Determine if there exists $\sigma \in \mathrm{Gal}(F/L)$ and an isomorphism $\varphi : E' \to \sigma(E)$ of elliptic curves such that $P' \mapsto \sigma(P)$. If no such σ exists, return $\varnothing$; otherwise, let φ be represented by a matrix in $\mathrm{GL}_3(F)$ as given in Lemma 6.6 and choose

- $(X_1, Y_1) \in \mathrm{Adj}(J_{\sigma(E),\sigma(P)}, \mathrm{N}) \setminus \{0\}$,
- $(X_2, Y_2) \in \mathrm{Adj}(J_{E',P'}, \mathrm{N}') \setminus \{0\}$, and
- $(X_3, Y_3) \in \mathrm{Adj}(J_{E',P'}, J_{\sigma(E),\sigma(P)}(\varphi \boldsymbol{y})) \setminus \{0\}$.

Set, moreover, $\alpha = \mathrm{diag}(X_2X_3^{-1}\sigma X_1^{-1}, Y_2^{-1}Y_3\sigma Y_1)$ and $\beta = (Z')^{-1}\varphi^{-1}\sigma Z$. Now, use Proposition 6.7 to construct a generating set $\mathcal{X}$ for $\mathrm{Auto}_F(J_{E,P})$ and write

$$\mathcal{Y}_1 = \left\{ \left(\begin{pmatrix} X_1\gamma X_1^{-1} & 0 \\ 0 & Y_1^{-1}\delta Y_1 \end{pmatrix}, Z^{-1}\varepsilon Z \right) \;\middle|\; (\gamma,\delta,\varepsilon) \in \mathcal{X} \right\}.$$

If $P \in E[2](F)$, then set

$$\mathcal{Y}_2 = \left\{ \left(\begin{pmatrix} aI_3 & bX_1Y_1 \\ cY_1^{-1}X_1^{-1} & dI_3 \end{pmatrix}, (ad-bc)I_3 \right) \;\middle|\; \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}_2(F) \right\}. \tag{6.1}$$

If $P \notin E[2](F)$, then set

$$\mathcal{Y}_2 = \left\{ \left(\begin{pmatrix} 0 & X_1X_0Y_1 \\ Y_1^{-1}X_0X_1^{-1} & 0 \end{pmatrix}, Z^{-1}Z_0Z \right) \;\middle|\; (X_0,Z_0) \text{ as in Lemma 5.4} \right\}. \tag{6.2}$$

Return the generating set $\mathcal{Y} = \mathcal{Y}_1 \cup \mathcal{Y}_2$ for $\Psi\mathrm{Isom}_F(\mathrm{B})$ and $(\alpha,\beta) \in \Psi\mathrm{Isom}_L(\mathrm{B},\mathrm{B}')$.

Correctness. For the existence of the matrices Z and Z' use Remark 4.9. Assume there exists $P \in E(F)$ such that $[\mathrm{N}] = [J_{E,P}]$. By definition, there exist $X, Y \in \mathrm{GL}_3(F)$ such that $X^{\mathrm{t}}\,\mathrm{N}\,Y = J_{E,P}$. Thus, $(A,B) \in \mathrm{Adj}(\mathrm{N}, J_{E,P})$ if and only if $(AX, Y^{-1}B) \in \mathrm{Adj}(J_{E,P})$. By Proposition 5.1, the latter is 1-dimensional and all non-zero elements are invertible. Thus, $\mathrm{Adj}(\mathrm{N}, J_{E,P})$ is non-trivial if and only if $[\mathrm{N}] = [J_{E,P}]$. Since $\det(\mathrm{N}) = 0$ defines a short Weierstrass equation and $\mathrm{char}(F) \geqslant 5$, Proposition 4.7 ensures the existence and uniqueness of such a P. A similar argument holds for N' and $J_{E',P'}$.

If there is no isomorphism of $\varphi : E' \to \sigma(E)$ mapping P' to $\sigma(P)$, then Theorem A guarantees that B and B′ are not L-pseudo-isometric. Otherwise, the isomorphism is linear being represented by a matrix in $\mathrm{GL}_3(F)$. Hence in this case, $J_{E',P'}(\varphi\boldsymbol{y})$ is equivalent to $J_{\sigma(E),\sigma(P)}$, and the adjoint algebra $\mathrm{Adj}(J_{E',P'}(\varphi\boldsymbol{y}), J_{\sigma(E),\sigma(P)})$ is 1-dimensional by a similar argument as before. Proposition 6.7 and direct calculations show that $\mathcal{Y} \subset \Psi\mathrm{Isom}_F(\mathrm{B})$ and $(\alpha,\beta) \in \Psi\mathrm{Isom}_L(\mathrm{B},\mathrm{B}')$. That $\langle\mathcal{Y}\rangle = \Psi\mathrm{Isom}_F(\mathrm{B})$ follows from the proof of Theorem 5.8.

Complexity. The complexity is dominated by listing and finding the unique points P and P'. There are at most $O(q)$ points, and listing the points on an elliptic curve can be done using $O(q)$ field operations. □

Proof of Theorem E(ii). We assume the algorithm for Theorem E(i) has already been carried out successfully. Thus, the matrices B_1 and B_2 associated to t_{G_1} and t_{G_2} are written over their centroids, F, and are decomposable. Now use the algorithm in Theorem 6.8 with $L = \mathbb{F}_p$. □

6.4. **Implementation.** We have implemented the algorithms in this section in the computer algebra system Magma [5], and they are publicly available [35]. The plot in Figure 1 shows the runtimes on an Intel Xeon Gold 6138 2.00 GHz running Magma V2.26-11.

We describe the process shown in Figure 1 from Section 1.6. For each prime-power $q = p^e$ up to 10^5, avoiding integers with $p \in \{2,3\}$, we construct an elliptic curve in short Weierstrass form $y^2 = x^3 + ax + b$, by choosing $(a,b) \in \mathbb{F}_q^2$ uniformly at random and discarding any pair (a,b) satisfying $4a^3 + 27b^2 = 0$. For each elliptic curve E, we choose $P \in E(\mathbb{F}_q) \setminus \{\mathcal{O}\}$ uniformly at random. After writing $\mathrm{B}_{E,P}$ over $\mathbb{F}_p$, our tensor is still represented with convenient choices of bases. In order to remove this bias, we randomly construct $X \in \mathrm{GL}_{6e}(\mathbb{F}_p)$ and $Z \in \mathrm{GL}_{3e}(\mathbb{F}_p)$, and set $\mathrm{B} = X^{\mathrm{t}}\,\mathrm{B}_{E,P}(Z\boldsymbol{y})X$. We finally construct generators for the automorphism group of $\mathrm{G}_{\mathrm{B}}(\mathbb{F}_p)$ using Theorem E.

Theorem A gives us a characterization of the isomorphism classes of elliptic p-groups for $p \notin \{2,3\}$. Such a characterization lends itself more easily to explicit computations.

In Table 1, for each prime-power $q \in [5, 97]$, with q not equal to 2^e or 3^e, we compute the number of isomorphism classes, denoted by N_q, of the $G = \mathrm{G}_{E,P}(F)$ such that $|G| = q^9$.

q	N_q	q	N_q	q	N_q	q	N_q	q	N_q
5	31	19	381	37	1409	53	2863	73	5405
7	57	23	551	41	1723	59	3539	79	6321
11	131	25	385	43	1893	61	3785	83	6971
13	185	29	871	47	2255	67	4557	89	8011
17	307	31	993	49	1393	71	5111	97	9509

TABLE 1. The number of isomorphism classes N_q of the $\mathrm{G}_{E,P}(F)$.

The data in Table 1 provides good evidence that the following conjecture seems true; in particular this would imply that the function $p \mapsto N_p$ is quasipolynomial.

Conjecture 6.9. *For primes $p \geqslant 5$, we have*

$$N_p = p^2 + p - \gcd(p-2, 3) + \gcd(p-1, 4).$$

It is clear that Conjecture 6.9 cannot be true for prime-powers: for example,

$$N_{25} = 385 \neq 653 = 25^2 + 25 - \gcd(25-2, 3) + \gcd(25-1, 4).$$

Question 6.10. For fixed e, is $p \mapsto N_{p^e}$ a quasipolynomial?

It may seem that the tensors we consider, namely $\mathrm{B}_{E,P}$, are somewhat rare in general. Indeed, the existence of 3-dimensional totally-isotropic subspaces of F^6 should not occur "at random". However, this is not the case. Let $\mathrm{B} \in \mathrm{Mat}_6(F[y_1, y_2, y_3]_1)$ whose Pfaffian defines an elliptic curve in $\mathbb{P}^2_F$. By Corollary 3.6, there are four cases for $|\mathcal{T}(\mathrm{B})|$, namely 0, 1, 2, and $q+1$. By Theorem 3.13, if $|\mathcal{T}(\mathrm{B})| \geqslant 1$, then there are three different $*$-semisimple types: $\mathbf{O}_1(F)$, $\mathbf{X}_1(F)$, and $\mathbf{S}_2(F)$. From computer evidence, it seems that $\mathrm{Adj}(\mathrm{B}) \cong \mathbf{U}_1(L)$, where L/F is a quadratic extension, whenever $\mathcal{T}(\mathrm{B}) = \varnothing$.

For primes $p \in [3, 1000]$, we constructed 1000 matrices $\mathrm{B} \in \mathrm{Mat}_6(\mathbb{F}_p[y_1, y_2, y_3]_1)$ where $\mathrm{Pf}(\mathrm{B})$ defines an elliptic curve in $\mathbb{P}^2_{\mathbb{F}_p}$. Each B was constructed uniformly at random: there are 36 homogeneous linear polynomials, so we chose 108 elements from $\mathbb{F}_p$ uniformly at random to build B, discarding matrices until they satisfied the required condition. The outcome of the experiment is shown in Figure 2. It seems that, as $p \to \infty$, the probability of $\mathrm{Adj}(\mathrm{B}) \cong \mathbf{X}_1(F)$ is equal to 0.5, which seems to also be equal to the probability of $\mathrm{Adj}(\mathrm{B}) \cong \mathbf{U}_1(L)$. In other words, it seems that for "random" $\mathrm{B} \in \mathrm{Mat}_6(\mathbb{F}_p[y_1, y_2, y_3]_1)$, we have either $|\mathcal{T}(\mathrm{B})| = 2$ or $|\mathcal{T}(\mathrm{B})| = 0$ at 50% of the time.

REFERENCES

[1] R. Baer. Groups with abelian central quotient group. *Trans. Amer. Math. Soc.*, 44(3):357–386, 1938.

[2] A. Bandini and L. Paladino. Number fields generated by the 3-torsion points of an elliptic curve. *Monatsh. Math.*, 168(2):157–181, 2012.

[3] M. Bardestani, K. Mallahi-Karai, and J. Salmasian. Kirillov's orbit method and polynomiality of the faithful dimension of p-groups. *Compos. Math.*, 155(8):1618–1654, 2019.

[4] A. Beauville. Determinantal hypersurfaces. *Mich. Math. J.*, 48:39–64, 2000.

[5] W. Bosma, J. Cannon, and C. Playoust. The Magma algebra system. I. The user language. volume 24, pages 235–265. 1997. Computational algebra and number theory (London, 1993).

[6] N. Boston and M. I. Isaacs. Class numbers of p-groups of a given order. *J. Algebra*, 279(2):810–819, 2004.

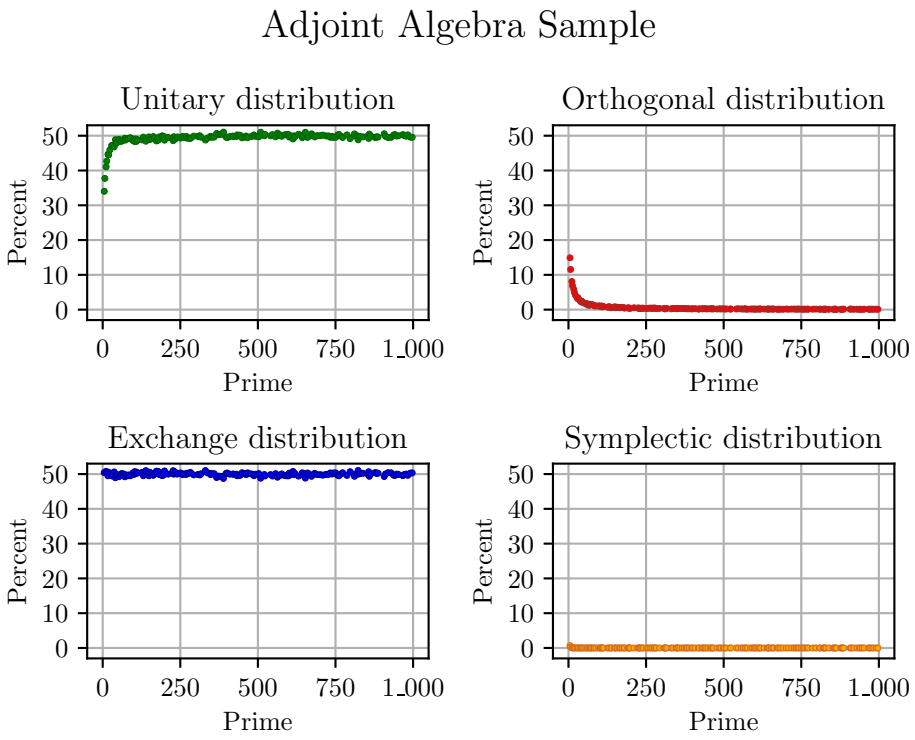

FIGURE 2. The isomorphism type for the $*$-semisimple part of the adjoint algebra for randomly constructed tensors.

[7] P. A. Brooksbank, J. Maglione, and J. B. Wilson. A fast isomorphism test for groups whose Lie algebra has genus 2. *J. Algebra*, 473:545–590, 2017.
[8] P. A. Brooksbank, J. Maglione, and J. B. Wilson. Exact sequences of inner automorphisms of tensors. *J. Algebra*, 545:43–63, 2020.
[9] P. A. Brooksbank, E. A. O'Brien, and J. B. Wilson. Testing isomorphism of graded algebras. *Trans. Amer. Math. Soc.*, 372(11):8067–8090, 2019.
[10] P. A. Brooksbank and J. B. Wilson. Computing isometry groups of Hermitian maps. *Trans. Amer. Math. Soc.*, 364(4):1975–1996, 2012.
[11] P. A. Brooksbank and J. B. Wilson. The module isomorphism problem reconsidered. *J. Algebra*, 421:541–559, 2015.
[12] J. J. Cannon and D. F. Holt. Automorphism group computation and isomorphism testing in finite groups. *J. Symbolic Comput.*, 35(3):241–267, 2003.
[13] D. A. Cox, J. Little, and D. O'Shea. *Ideals, varieties, and algorithms*. Undergraduate Texts in Mathematics. Springer, Cham, fourth edition, 2015. An introduction to computational algebraic geometry and commutative algebra.
[14] J. Cremona. G1CRPC: Rational points on curves, 2003. https://www.cise.ufl.edu/research/SpaceTimeUncertainty/Spatial3D/crem03.pdf.
[15] M. du Sautoy. A nilpotent group and its elliptic curve: non-uniformity of local zeta functions of groups. *Israel J. Math.*, 126:269–288, 2001.
[16] M. du Sautoy. Counting subgroups in nilpotent groups and points on elliptic curves. *J. Reine Angew. Math.*, 549:1–21, 2002.
[17] M. P. F. du Sautoy and M. Vaughan-Lee. Non-PORC behaviour of a class of descendant p-groups. *J. Algebra*, 361:287–312, 2012.
[18] W. Duke. Elliptic curves with no exceptional primes. *C. R. Acad. Sci. Paris Sér. I Math.*, 325(8):813–818, 1997.

[19] B. Eick, C. R. Leedham-Green, and E. A. O'Brien. Constructing automorphism groups of p-groups. *Comm. Algebra*, 30(5):2271–2295, 2002.
[20] W. Fulton. *Algebraic curves. An introduction to algebraic geometry*. W. A. Benjamin, Inc., New York-Amsterdam, 1969.
[21] F. Grunewald and D. Segal. Reflections on the classification of torsion-free nilpotent groups. In *Group theory*, pages 121–158. Academic Press, London, 1984.
[22] P. Hall. The classification of prime-power groups. *J. Reine Angew. Math.*, 182:130–141, 1940.
[23] R. Hartshorne. *Algebraic geometry*. Graduate Texts in Mathematics, No. 52. Springer-Verlag, New York-Heidelberg, 1977.
[24] O. Hesse. Über die Elimination der Variabeln aus drei algebraischen Gleichungen vom zweiten Grade mit zwei Variabeln. *J. Reine Angew. Math.*, 28:68–96, 1844.
[25] G. Higman. Enumerating p-groups. I. Inequalities. *Proc. London Math. Soc. (3)*, 10:24–30, 1960.
[26] G. Higman. Enumerating p-groups. II. problems whose solution is porc. *Proc. London Math. Soc. (3)*, 10:566–582, 1960.
[27] Y. Ishitsuka. A positive proportion of cubic curves over $\mathbb{Q}$ admit linear determinantal representations. *J. Ramanujan Math. Soc.*, 32(3):231–257, 2017.
[28] G. Ivanyos and Y. Qiao. Algorithms based on $*$-algebras, and their applications to isomorphism of polynomials with one secret, group isomorphism, and polynomial identity testing. *SIAM J. Comput.*, 48(3):926–963, 2019.
[29] W. M. Kantor and E. M. Luks. Computing in quotient groups. In *Proceedings of the Twenty-Second Annual ACM Symposium on Theory of Computing*, STOC '90, pages 524–534, New York, NY, USA, 1990. Association for Computing Machinery.
[30] S. Lee. A class of descendant p-groups of order p^9 and Higman's PORC conjecture. *J. Algebra*, 468:440–447, 2016.
[31] C. R. Leedham-Green and L. H. Soicher. Symbolic collection using Deep Thought. *LMS J. Comput. Math.*, 1:9–24, 1998.
[32] E. M. Luks. Computing in solvable matrix groups. In *33rd Annual Symposium on Foundations of Computer Science, Pittsburgh, Pennsylvania, USA, 24-27 October 1992*, pages 111–120. IEEE Computer Society, 1992.
[33] J. Maglione. Efficient characteristic refinements for finite groups. *J. Symbolic Comput.*, 80(part 2):511–520, 2017.
[34] J. Maglione. Filters compatible with isomorphism testing. *J. Pure Appl. Algebra*, 225(3):Paper No. 106528, 28, 2021.
[35] J. Maglione. EGroups, ver. 1.0, 2022. https://github.com/joshmaglione/egroups.
[36] G. L. Miller. On the $n \log n$ isomorphism technique (preliminary report). In *Proceedings of the 10th annual ACM symposium on theory of computing, STOC'78, San Diego, CA, USA, May 1–3, 1978*, pages 51–58. New York, NY: Association for Computing Machinery (ACM), 1978.
[37] P. M. Neumann. Some algorithms for computing with finite permutation groups. In *Proceedings of groups—St. Andrews 1985*, volume 121 of *London Math. Soc. Lecture Note Ser.*, pages 59–92. Cambridge Univ. Press, Cambridge, 1986.
[38] K. O. Ng. The classification of $(3, 3, 3)$ trilinear forms. *J. Reine Angew. Math.*, 468:49–75, 1995.
[39] E. A. O'Brien and C. Voll. Enumerating classes and characters of p-groups. *Trans. Amer. Math. Soc.*, 367(11):7775–7796, 2015.
[40] G. V. Ravindra and A. Tripathi. Torsion points and matrices defining elliptic curves. *Internat. J. Algebra Comput.*, 24(6):879–891, 2014.
[41] T. Rossmann. 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.
[42] T. Rossmann. On the enumeration of orbits of unipotent groups over finite fields. 2022. arXiv:2208.04646.
[43] T. Rossmann and C. Voll. Groups, graphs, and hypergraphs: average sizes of kernels of generic matrices with support constraints. *Mem. Amer. Math. Soc.*, 294(1465):v+120, 2024.
[44] A. Seress. *Permutation group algorithms*, volume 152 of *Cambridge Tracts in Mathematics*. Cambridge University Press, Cambridge, 2003.
[45] I. Shparlinski. On finding primitive roots in finite fields. *Theoret. Comput. Sci.*, 157(2):273–275, 1996.
[46] J. H. Silverman. *The arithmetic of elliptic curves*, volume 106 of *Graduate Texts in Mathematics*. Springer, Dordrecht, second edition, 2009.

[47] J. H. Silverman and J. T. Tate. *Rational points on elliptic curves*. Undergraduate Texts in Mathematics. Springer, Cham, second edition, 2015.
[48] M. Stanojkovski and C. Voll. Hessian matrices, automorphisms of p-groups, and torsion points of elliptic curves. *Math. Ann.*, 381(1-2):593–629, 2021.
[49] The Sage Developers. *SageMath, the Sage Mathematics Software System (Version 8.7)*, 2019. See https://www.sagemath.org.
[50] M. Vaughan-Lee. Non-PORC behaviour in groups of order p^7. *J. Algebra*, 500:30–45, 2018.
[51] C. Voll. Zeta functions of groups and enumeration in Bruhat-Tits buildings. *Amer. J. Math.*, 126:1005–1032, 2004.
[52] C. Voll. Functional equations for local normal zeta functions of nilpotent groups. *Geom. Func. Anal. (GAFA)*, 15:274–295, 2005. with an appendix by A. Beauville.
[53] J. von zur Gathen and J. Gerhard. *Modern computer algebra*. Cambridge University Press, Cambridge, third edition, 2013.
[54] J. Weinstein. Reciprocity laws and Galois representations: recent breakthroughs. *Bull. Amer. Math. Soc. (N.S.)*, 53(1):1–39, 2016.
[55] J. B. Wilson. Existence, algorithms, and asymptotics of direct product decompositions, I. *Groups Complex. Cryptol.*, 4(1):33–72, 2012.
[56] J. B. Wilson. More characteristic subgroups, Lie rings, and isomorphism tests for p-groups. *J. Group Theory*, 16(6):875–897, 2013.
[57] J. B. Wilson. On automorphisms of groups, rings, and algebras. *Comm. Algebra*, 45(4):1452–1478, 2017.
[58] B. F. Wyman. What is a reciprocity law? *Amer. Math. Monthly*, 79:571–586; correction, ibid. 80 (1973), 281, 1972.

(Joshua Maglione) University of Galway, School of Mathematical and Statistical Sciences
Email address: joshua.maglione@universityofgalway.ie

(Mima Stanojkovski) Università di Trento, Dipartimento di Matematica
Email address: mima.stanojkovski@unitn.it