Proceedings of the Royal Society of Edinburgh, page 1 of 26
DOI:10.1017/prm.2018.159

Duality between p-groups with three characteristic subgroups and semisimple anti-commutative algebras

S. P. Glasby
Centre for Mathematics of Symmetry and Computation, University of Western Australia, 35 Stirling Highway, Perth 6009, Australia (Stephen.Glasby@uwa.edu.au)

Frederico A. M. Ribeiro* **and Csaba Schneider**
Departamento de Matemática, Instituto de Ciências Exatas, Universidade Federal de Minas Gerais, Av. Antônio Carlos 6627, Belo Horizonte, MG, Brazil (fred321@gmail.com; csaba@mat.ufmg.br)

(MS received 14 November 2017; accepted 18 September 2018)

Let p be an odd prime and let G be a non-abelian finite p-group of exponent p^2 with three distinct characteristic subgroups, namely 1, G^p and G. The quotient group G/G^p gives rise to an anti-commutative $\mathbb{F}_p$-algebra L such that the action of $\mathrm{Aut}(L)$ is irreducible on L; we call such an algebra IAC. This paper establishes a duality $G \leftrightarrow L$ between such groups and such IAC algebras. We prove that IAC algebras are semisimple and we classify the simple IAC algebras of dimension at most 4 over certain fields. We also give other examples of simple IAC algebras, including a family related to the m-th symmetric power of the natural module of $\mathrm{SL}(2,\mathbb{F})$.

Keywords: characteristic subgroups; p-groups; anti-commutative algebras

2010 *Mathematics subject classification:* Primary: 20D15; 20C20; 20E15; 20F28; 17A30; 17A36

1. Introduction

Building on earlier work by Taunt [17] and by the first and the third authors in collaboration with Pálfy [7], we continue, in this paper, our investigation into the structure of finite groups with a unique non-trivial and proper characteristic subgroup. Such a group is said to be UCS. In [7], finite UCS p-groups were studied. The exponent of a finite UCS p-group is either p or p^2. If p is an odd prime and G is a UCS p-group of exponent p^2, then the Frattini quotient $V = G/\Phi(G)$ is an irreducible $\mathrm{Aut}(G)$-module and V is an epimorphic image of the exterior square $\wedge^2 V$. An epimorphism $\wedge^2 V \to V$ can be viewed as an anti-commutative multiplication on the vector space V which turns V into a non-associative and anti-commutative algebra $\mathcal{L}(G)$ defined in § 3. Further, by theorem 1.1(a) below, the automorphism

* Current address: Departamento de Matemática, Centro Federal de Educação, Técnológica de Minas Gerais, CEFET-MG, Av. Amazonas 7675, Belo, Horizonte, MG, Brasil.

group of $\mathcal{L}(G)$ is induced by $\mathrm{Aut}(G)$, and is irreducible on V. The main results of this paper explore the connection between G and $\mathcal{L}(G)$.

To state the first main theorem of the paper, let UCS_{p^2} denote the set of isomorphism classes of finite UCS p-groups of exponent p^2 and, for an odd prime p, let IAC_p denote the set of isomorphism classes of finite-dimensional anti-commutative algebras L over the field $\mathbb{F}_p$ of p elements such that $\mathrm{Aut}(L)$ is irreducible on L. Such an algebra will be referred to as an IAC algebra.

THEOREM 1.1. *If p is an odd prime, then the map $G \mapsto \mathcal{L}(G)$ is a bijection between UCS_{p^2} and IAC_p. Further, if $G \in \mathrm{UCS}_{p^2}$ and $L = \mathcal{L}(G)$ then the following hold.*

(a) *There is an isomorphism $\mathrm{Aut}(G)/\mathrm{Aut}_C(G) \cong \mathrm{Aut}(L)$ where $\mathrm{Aut}_C(G)$ denotes the group of central automorphisms of G.*

(b) *There is a bijection between the set of subalgebras of L and the set of powerful subgroups of G that contain $\Phi(G)$.*

(c) *The bijection in part* (b) *restricts to a bijection between ideals of L and powerfully embedded subgroups of G containing $\Phi(G)$.*

(d) *For $k \geqslant 2$, we have that $G^{\times k} \in \mathrm{UCS}_{p^2}$ and $\mathcal{L}(G^{\times k}) \cong L^{\oplus k}$.*

The first statement of theorem 1.1 follows from theorem 3.5, while parts (a), (b), (c) and (d) follow from theorem 3.6, proposition 4.4 and from theorem 4.3.

In the second part of the paper, we prove several results about small-dimensional IAC algebras over various fields, which can be summarized in the following theorem.

THEOREM 1.2. *The following are valid for a field $\mathbb{F}$.*

(a) *A finite-dimensional IAC algebra over $\mathbb{F}$ is the direct sum of pairwise isomorphic simple IAC algebras.*

(b) *If $\mathrm{char}(\mathbb{F}) \neq 2$, then a non-abelian 3-dimensional IAC algebra over $\mathbb{F}$ is a simple Lie algebra.*

(c) *Suppose that $\mathbb{F}$ is a finite field of $q = p^f$ elements where p is an odd prime. Then the number of isomorphism types of 4-dimensional IAC algebras over $\mathbb{F}$ is* (i) 0 *if $p = 5$,* (ii) 1 *if f is even or $p \equiv \pm 1 \pmod 5$, and* (iii) 2 *if f is odd and $p \equiv \pm 2 \pmod 5$.*

(d) *If $m \geqslant 2$, $m \equiv 2 \pmod 4$, and either $\mathrm{char}(\mathbb{F}) = 0$ or $2m < \mathrm{char}(\mathbb{F})$, then there is an $(m+1)$-dimensional IAC algebra L over $\mathbb{F}$ whose automorphism group contains a subgroup isomorphic to $\mathrm{SL}(2, \mathbb{F})$ acting absolutely irreducibly on L.*

Theorem 1.2 follows from theorem 4.2, proposition 5.1, and theorems 5.3 and 8.1. Note that $p^f \equiv \pm 2 \pmod 5$ holds if and only if f is odd and $p \equiv \pm 2 \pmod 5$.

UCS p-groups are atypical, since finite p-groups usually have a rich structure of characteristic subgroups, which is used in the optimization of the standard algorithms for computing $\mathrm{Aut}(G)$; see for instance [**6**, **19**]. However, when G does not have characteristic subgroups apart from the usual verbal subgroups, such

optimization techniques fail. In particular, the algorithms for computing $\mathrm{Aut}(G)$ that are based on orbit-stabilizer calculation would perform poorly on UCS p-groups. Nevertheless, theorem 1.1 shows that UCS p-groups of exponent p^2 have a rigid algebraic structure that, in theory, can be exploited also in automorphism group computations, in a way which is rather similar to the philosophy pursued by Wilson and his collaborators in their recent work [**4**, **5**, **20**].

Following [**7**], we say that a G-module V is an ESQ module if $V \cong \wedge^2 V/U$ for some G-submodule U (see also § 5.2). IAC algebras are related to irreducible ESQ G-modules. It was observed in [**2**] that a similar connection exists between Lie algebra modules that satisfy the corresponding property and IAC algebras. Indeed, the authors of [**2**] considered the exterior squares of some irreducible representations of the Lie algebra $\mathfrak{sl}(2)$ in the same way as we consider such representations for $\mathrm{GL}(2,\mathbb{F})$ in theorem 7.1 and they defined non-associative anti-commutative algebras as we do in theorem 8.1. In addition, they explicitly computed the structure constant tables for the resulting 3, 7 and 11-dimensional algebras, noting that the 3-dimensional algebra is the simple Lie algebra $\mathfrak{sl}(2)$ (as implied also by our proposition 5.1), while the 7-dimensional algebra is the non-Lie simple Malcev algebra. This fact is further exploited in [**3**] for the study of the polynomial identities of the Malcev algebra.

In § 2, we review some known properties of UCS p-groups before we establish in § 3 a duality between the class of UCS p-groups of exponent p^2, and the class of IAC algebras. In § 4 we prove that IAC algebras are semisimple, and that their subalgebras correspond to powerful subgroups of UCS groups. We address the classification of simple IAC algebras of dimension at most 4 in § 5, and an infinite class of examples of simple IAC algebras, with widely varying dimensions, is given in § 6. We prove a general version, which is valid also in prime characteristic, of the Clebsch–Gordan decomposition for tensor squares, exterior squares and symmetric squares of $\mathrm{GL}(2,\mathbb{F})$-modules in § 7, and apply it in § 8 to construct some simple IAC algebras related to representations of $\mathrm{SL}(2,\mathbb{F})$.

2. UCS p-groups of exponent p^2

Let us start by recalling some standard notions of finite group theory. If G is a group and k is an integer, then G^k denotes the subgroup of G generated by k-th powers. To avoid confusion, the k-fold direct power of G is denoted by $G^{\times k}$. The commutator subgroup G' of G is the subgroup generated by all commutators $[x,y] = x^{-1}y^{-1}xy$ with $x,\ y \in G$. The Frattini subgroup $\Phi(G)$ is the intersection of all the maximal subgroups of G. It is well-known that if G is a finite p-group, then $\Phi(G) = G'G^p$. The centre $\mathsf{Z}(G)$ of G is the subgroup of G consisting of elements $g \in G$ such that $gx = xg$ holds for all $x \in G$.

A subgroup N of a group G is called *characteristic* if it is invariant under each automorphism $\alpha \in \mathrm{Aut}(G)$. For instance, the subgroups G', G^k, $\Phi(G)$ are characteristic. A group G with a **u**nique non-trivial proper **c**haracteristic **s**ubgroup is abbreviated as a *UCS group*. Finite UCS groups were studied by Taunt [**17**] and later finite UCS p-groups were explored by the first and the third authors in collaboration with Pálfy [**7**]. The characteristic subgroups of a finite UCS p-group G are 1, $\Phi(G)$ and G, and consequently the exponent of G is either p or p^2.

It is useful to review some properties of UCS groups.

LEMMA 2.1 ([7, lemma 3]). *Suppose that G is a finite non-abelian UCS p-group and $1 \lhd N \lhd G$ are the only characteristic subgroups of G. Then the following hold:*

(a) *$G' = \Phi(G) = \mathsf{Z}(G) = N$ and $G^p = 1$ or $G^p = N$;*

(b) *the groups G/N and N are elementary abelian p-groups.*

LEMMA 2.2 ([7, theorem 4]). *Let G be a finite p-group such that $G/\Phi(G)$ and $\Phi(G)$ are non-trivial elementary abelian p-groups. Then G is a UCS group if and only if $\mathrm{Aut}(G)$ induces an irreducible linear group on both $G/\Phi(G)$ and on $\Phi(G)$.*

Consider, for a group G, the natural homomorphism $G \to G/\Phi(G)$. For $g \in G$ and for $H \leqslant G$ we define

$$\overline{g} = g\Phi(G) \quad \text{and} \quad \overline{H} = H\Phi(G)/\Phi(G).$$

In particular, $\overline{G} = G/\Phi(G)$.

LEMMA 2.3 ([7, theorem 4(iii)]). *Let G be a finite UCS p-group of odd exponent p^2. Then the map $\varphi\colon \overline{G} \to \Phi(G)$ defined by $\overline{g}\varphi = g^p$ is a well-defined isomorphism between the $\mathbb{F}_p\mathrm{Aut}(G)$-modules $\overline{G}$ and $\Phi(G)$. In particular, $|\overline{G}| = |\Phi(G)|$.*

Suppose that G is a UCS p-group of odd exponent p^2 and let $g \in G$. By lemma 2.3, defining $\overline{g}^p = \overline{g}\varphi = g^p$, we obtain a well-defined isomorphism between the $\mathbb{F}_p\mathrm{Aut}(G)$-modules $\overline{G}$ and $\Phi(G)$. If $h \in \Phi(G)$, then let $h^{1/p}$ denote the unique preimage $h\varphi^{-1} \in \overline{G}$ of h under φ. Thus for every $\overline{g} \in \overline{G}$ and $h \in \Phi(G)$ we have

$$(\overline{g}^p)^{1/p} = \overline{g} \quad \text{and} \quad (h^{1/p})^p = h. \tag{2.1}$$

THEOREM 2.4 [17, theorem 2.1]. *Suppose that G is a UCS group, and N is its proper non-trivial characteristic subgroup. Assume further that $\mathrm{Aut}(G)$ fixes no non-trivial element of $N \cup G/N$. Then for all $k \geqslant 1$ the k-th direct power $G^{\times k}$ is a UCS group, and $N^{\times k}$ is a characteristic subgroup of $G^{\times k}$.*

3. UCS p-groups and IAC algebras

We consider non-associative[1] algebras L over a field $\mathbb{F}$ satisfying $xx = 0$ for all $x \in L$. Our focus will be when $\mathrm{char}(\mathbb{F}) \neq 2$. Such an algebra is called *anti-commutative* because $yx = -xy$ holds for all $x, y \in L$. As these algebras are more similar to Lie algebras than to associative algebras, we henceforth write the product xy as $[\![x, y]\!]$. An anti-commutative algebra L for which $\mathrm{Aut}(L)$ acts irreducibly on L will be called *IAC algebra* (for **i**rreducible and **a**nti-**c**ommutative).

Let p be an odd prime and let G be a UCS p-group of exponent p^2. By lemma 2.3, the map $\overline{G} \to \Phi(G)$, defined by $\overline{x} \mapsto x^p$ is an isomorphism of $\mathrm{Aut}(G)$-modules. Given $\lambda \in \mathbb{F}_p$ and $\overline{x} \in \overline{G}$, considering λ as an integer between 0 and $p-1$, the

[1] Precisely, we assume that the binary operation $L \times L \to L$ may or may not be associative.

scalar action $\lambda\overline{x} = \overline{x^\lambda}$ is well-defined and turns $\overline{G}$ into a vector space over $\mathbb{F}_p$. It is less obvious that the following product $[\![\overline{x}, \overline{y}]\!]$ for $\overline{x},\ \overline{y} \in \overline{G}$ is well-defined:

$$[\![\overline{x}, \overline{y}]\!] = [x, y]^{1/p} \quad \text{where } x,\ y \in G \quad \text{and } [x, y] = x^{-1}y^{-1}xy. \tag{3.1}$$

Henceforth $\mathcal{L}(G) = (\overline{G}, +, [\![\cdot, \cdot]\!])$ will denote this $\mathbb{F}_p$-algebra.

LEMMA 3.1. *Suppose that p is an odd prime and G is a finite UCS p-group of exponent p^2. Then $\mathcal{L}(G)$ defined above is an IAC algebra over $\mathbb{F}_p$.*

Proof. We first prove that the operation $[\![\cdot, \cdot]\!]$ given by equation (3.1) is well-defined. Let $v_1,\ v_2,\ w_1,\ w_2 \in G$ such that $\overline{v}_1 = \overline{v}_2$ and $\overline{w}_1 = \overline{w}_2$. Then $v_2 = v_1 z_v$ and $w_2 = w_1 z_w$ with $z_v,\ z_w \in \Phi(G)$. As z_v and z_w are central, and G has nilpotency class 2, we obtain that $[v_2, w_2] = [v_1, w_1]$, and so $[v_2, w_2]^{1/p} = [v_1, w_1]^{1/p}$. Thus the value of $[\![\cdot, \cdot]\!]$ is independent of the choice of coset representatives, and $[\![\cdot, \cdot]\!]$ is well-defined.

We prove next that $[\![\cdot, \cdot]\!]$ distributes over the addition in $\overline{G}$. Take $u, v, w \in G$ and note that $[u, vw] = [u, v][u, w]$ holds since G has nilpotency class 2. Therefore

$$[\![\overline{u}, \overline{v} + \overline{w}]\!] = [u, vw]^{1/p} = ([u, v][u, w])^{1/p} = [u, v]^{1/p}[u, w]^{1/p} = [\![u, v]\!] + [\![u, w]\!].$$

In addition, $[\![\overline{v}, \overline{v}]\!] = [v, v]^{1/p} = 1^{1/p}$, equals the zero element of $\overline{G}$. Hence $[\![\overline{v}, \overline{v}]\!] = 0$ for all $\overline{v} \in \overline{G}$. An automorphism $\alpha \in \mathrm{Aut}(G)$ induces an $\mathbb{F}_p$-linear transformation $\overline{\alpha}\colon \overline{G} \to \overline{G}$ and a (restricted) isomorphism $\alpha{\downarrow}\colon \Phi(G) \to \Phi(G)$. Then, by lemma 2.3, the map $\varphi\colon \overline{x} \mapsto x^p$ intertwines $\alpha{\downarrow}$ and $\overline{\alpha}$, i.e.

$$\varphi(\alpha{\downarrow}) = \overline{\alpha}\varphi \quad \text{or} \quad (\alpha{\downarrow})\varphi^{-1} = \varphi^{-1}\overline{\alpha}. \tag{3.2}$$

Hence

$$\begin{aligned}[\![\overline{u}, \overline{v}]\!]\overline{\alpha} &= [u, v]^{1/p}\overline{\alpha} = [u, v]\varphi^{-1}\overline{\alpha} = [u, v](\alpha{\downarrow})\varphi^{-1} = [u\alpha, v\alpha]\varphi^{-1} \\ &= [u\alpha, v\alpha]^{1/p} = [\![\overline{u}\,\overline{\alpha}, \overline{v}\,\overline{\alpha}]\!].\end{aligned}$$

Thus $\overline{\alpha} \in \mathrm{Aut}(\mathcal{L}(G))$. By lemma 2.2, $\mathrm{Aut}(G)$ induces an irreducible subgroup of $\mathrm{GL}(\overline{G})$. Thus $\mathrm{Aut}(\mathcal{L}(G))$ is irreducible on $\overline{G}$, and $\mathcal{L}(G)$ is an IAC algebra as claimed. □

In characteristic 2, we need not have $|G/\Phi(G)| = |\Phi(G)|$ as in lemma 2.3. For example, a non-abelian group G of order 8 is UCS and satisfies $|G/\Phi(G)| = 4 > 2 = |\Phi(G)|$. Although our construction of $\mathcal{L}(G)$ works more generally, namely when $p > 2$ and G satisfies $1 < \Phi(G) \leqslant \mathsf{Z}(G)$, $|\overline{G}| = |\Phi(G)|$, and $G^{p^2} = 1$, the resulting anti-commutative algebra $\mathcal{L}(G)$ need not be an irreducible $\mathrm{Aut}(L)$-module when G is not a UCS group.

Given an algebra L, the subspace $[\![L, L]\!]$ generated by all products $[\![x, y]\!]$ with $x,\ y \in L$ is invariant under $\mathrm{Aut}(L)$. Thus if L is an IAC algebra, we have $[\![L, L]\!] = 0$ or $[\![L, L]\!] = L$. If $L = \mathcal{L}(G)$ for some finite UCS p-group G of exponent p^2, then $[\![L, L]\!] = 0$ occurs if and only if G is abelian. We will usually assume that this is not the case; that is, $[\![L, L]\!] = L$ holds. Adopting the terminology from Lie algebras, an anti-commutative algebra L is said to be *abelian* if $[\![L, L]\!] = 0$.

The following result shows that the construction in lemma 3.1 can be reversed.

THEOREM 3.2. *Given an odd prime p and a finite-dimensional IAC algebra L over $\mathbb{F}_p$, there exists a finite UCS p-group $G = \mathcal{G}(L)$ of exponent p^2 such that $\mathcal{L}(G) \cong L$.*

In theorem 3.5 we show that $\mathcal{G} = \mathcal{L}^{-1}$, see remark 3.4.

Proof. Suppose that L has (finite) dimension r over $\mathbb{F}_p$ and $\{v_1, \ldots, v_r\}$ is a basis. If L is abelian, then we take G to be the homocyclic group $(C_{p^2})^r$. Clearly, $\mathcal{L}(G) \cong L$ in this case, and so in the rest of the proof we assume that L is a non-abelian IAC algebra.

Let $H = H_{p,r}$ be the r-generator free group in the variety of groups that have exponent dividing p^2, nilpotency class at most 2 and have the property that all p-th powers are central. Assume that $c_k^{(i,j)}$ are the structure constants of L; that is,

$$[\![v_i, v_j]\!] = \sum_{k=1}^{r} c_k^{(i,j)} v_k \tag{3.3}$$

for all $1 \leqslant i < j \leqslant r$. We consider the constants $c_k^{(i,j)}$ as elements of the field $\mathbb{F}_p$ as well as integers in $\{0, \ldots, p-1\}$. Suppose that $h_1, \ldots, h_r$ are generators of H. Define $N \leqslant H$ as the subgroup

$$N = \left\langle [h_i, h_j]^{-1} \prod_{k=1}^{r} (h_k^p)^{c_k^{(i,j)}} \mid 1 \leqslant i < j \leqslant r \right\rangle. \tag{3.4}$$

As $N \leqslant \Phi(H) \leqslant \mathsf{Z}(H)$, the subgroup N is normal in H. Further, considering $\Phi(H)$ as an $\mathbb{F}_p$-vector space, the given generators of N are linearly independent, and hence $|N| = p^{\binom{r}{2}}$.

Set $G = H/N$. Then G is a finite p-group, and so the Frattini subgroup of G is

$$G^p G' = (H/N)^p (H/N)' = (H^p H' N)/N = \Phi(H)/N.$$

On the other hand, since $\Phi(G) = G^p G'$ and the relations in N imply that $G' \leqslant G^p$, we find that $\Phi(G) = G^p$. Since $\Phi(G) \leqslant \mathsf{Z}(G)$ and $\Phi(G)^p = 1$, the map $\varphi\colon \overline{G} \to \Phi(G)$ defined by $\overline{g} \mapsto g^p$ is a surjective $\mathrm{Aut}(G)$-module homomorphism. Since $|\Phi(H)| = p^{r+\binom{r}{2}}$ by [7, p. 87], we have $|\overline{G}| = |\Phi(G)| = p^r$, and the map $\overline{g} \mapsto g^p$ is an isomorphism.

As remarked before this theorem, G satisfies sufficient conditions for us to construct the anti-commutative algebra $\mathcal{L}(G)$, as in lemma 3.1. Set $g_i = h_i N$ for $1 \leqslant i \leqslant r$, and define the linear map $\xi\colon L \to \overline{G}$ by $v_i \xi = \overline{g}_i$ for all i. We claim that ξ is an isomorphism of $\mathbb{F}_p$-algebras. Indeed, by (3.1) and (3.4) we have

$$[\![v_i\xi, v_j\xi]\!] = [\![\overline{g}_i, \overline{g}_j]\!] = [g_i, g_j]^{1/p} = \left(\prod_{k=1}^{r} (g_k^p)^{c_k^{(i,j)}} \right)^{1/p}.$$

Using (2.1) and (3.3) this equals

$$\prod_{k=1}^{r} ((\overline{g}_k^p)^{1/p})^{c_k^{(i,j)}} = \prod_{k=1}^{r} (\overline{g}_k)^{c_k^{(i,j)}} = [\![v_i, v_j]\!]\xi.$$

Since $|L| = |\overline{G}| = p^r$ and ξ is surjective, it follows that ξ is an $\mathbb{F}_p$-isomorphism.

We claim that G is a UCS p-group of exponent p^2. The construction of the p-group G ensures that $\overline{G}$ and $\Phi(G)$ are elementary abelian. By lemma 2.2, it suffices to show that $\mathrm{Aut}(G)$ acts irreducibly on $\overline{G}$ and on $\Phi(G)$. Fix $\alpha \in \mathrm{Aut}(L)$ and write

$$v_i\alpha = \sum_{k=1}^{r} a_{ik}v_k \quad \text{where } i \in \{1, \ldots, r\} \quad \text{and } a_{ik} \in \mathbb{F}_p.$$

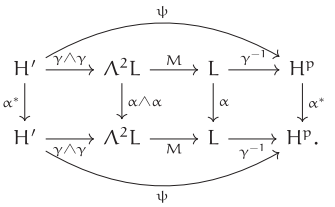
As H is a relatively free group, there is a homomorphism $\alpha^*\colon H \to H$ satisfying

$$h_i\alpha^* = \prod_{k=1}^{r} h_k^{a_{ik}} \quad \text{where } a_{ik} \in \{0, 1, \ldots, p-1\}.$$

By Burnside's Basis Theorem, $\alpha^* \in \mathrm{Aut}(H)$.

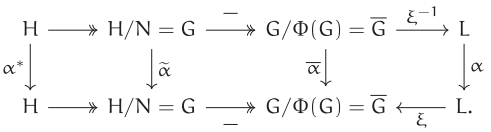
We claim that N is invariant under α^*. Define $\psi\colon H' \to H^p$ as the linear map that acts on the generators of H' by $[h_i, h_j]\psi = \prod_{k=1}^{r}(h_k^p)^{c_k^{(i,j)}}$ for all $i < j$. Note that the subgroup N equals $\{h^{-1}(h\psi) \mid h \in H'\}$. It suffices to show that $\psi\alpha^* = \alpha^*\psi$, since this equality implies that $(h^{-1}(h\psi))\alpha^* = (h\alpha^*)^{-1}(h\alpha^*)\psi$ for all $h \in H'$, and, in turn, that N is invariant under α^*. Define $\gamma\colon H^p \to L$ by $h_i^p\gamma = v_i$ and observe that γ is a linear isomorphism. Similarly $\gamma \wedge \gamma\colon H' \to \wedge^2 L$ defined by $[h_i, h_j] \mapsto v_i \wedge v_j$ is a linear isomorphism onto the exterior square $\wedge^2 L$ of L. The map $M\colon \wedge^2 L \to L$ defined by $(u \wedge v)M = [\![u, v]\!]$ is an epimorphism since $L = [\![L, L]\!]$.

These maps are illustrated in diagram (3.5):



(3.5)

Since each square piece of diagram (3.5) is commutative, it follows that $\psi = (\gamma \wedge \gamma)M\gamma^{-1}$. Therefore $\psi\alpha^* = \alpha^*\psi$, as claimed, which, in turn, implies that N is invariant under α^*. Hence α^* induces an automorphism $\widetilde{\alpha}$ of $G = H/N$. Recall that $\xi\colon L \to \overline{G}$ satisfies $v_i\xi = \overline{g}_i$. It is straightforward to see that the following diagram (3.6) is commutative:



(3.6)

Hence the equation $\overline{\alpha} = \xi^{-1}\alpha\xi$ relates $\alpha \in \mathrm{Aut}(L)$ and $\overline{\alpha} \in \mathrm{Aut}(\overline{G})$. Therefore $\xi^{-1}\mathrm{Aut}(L)\xi$ is contained in the group induced by $\mathrm{Aut}(G)$ on $\overline{G}$, and so $\mathrm{Aut}(G)$ acts irreducibly on $\overline{G}$. At the start of the proof we showed that $\overline{G}$ and $\Phi(G)$ are isomorphic as $\mathrm{Aut}(G)$-modules. Thus $\mathrm{Aut}(G)$ is irreducible on $\Phi(G)$ also, and by lemma 2.2, G is a UCS p-group of exponent p^2. □

Finite p-groups are commonly expressed using *polycyclic presentations*, see [**9**, Chapter 8].

COROLLARY 3.3. *Let L be an IAC algebra over $\mathbb{F}_p$, p odd, with basis $\{v_1, \ldots, v_r\}$ and suppose $[\![v_i, v_j]\!] = \sum_{k=1}^{r} c_k^{(i,j)} v_k$ where $c_k^{(i,j)} \in \mathbb{F}_p$. Then the UCS group $\mathcal{G}(L)$ defined in theorem 3.2 is isomorphic to the group given by the polycyclic presentation*

$$G = \langle g_1, \ldots, g_r, z_1, \ldots, z_r \mid$$
$$g_i^p = z_i, \quad z_i^p = [z_j, g_i] = [z_i, z_j] = 1, \quad [g_i, g_j] = \prod_{k=1}^{r} z_k^{c_k^{(i,j)}}, i < j\rangle. \tag{3.7}$$

Proof. Identify the scalars $c_k^{(i,j)} \in \mathbb{F}_p$ in (3.7) with integers in the set $\{0, 1, \ldots, p-1\}$. The group presentation (3.7) is called a polycyclic presentation, and it has the property that the elements of the group defined by the presentation can be expressed in the form $g_1^{x_1} \cdots g_r^{x_r} z_1^{x_{r+1}} \cdots z_r^{x_{2r}}$ where the exponents satisfy $0 \leqslant x_i \leqslant p-1$ for $1 \leqslant i \leqslant 2r$. This shows that $|G| \leqslant p^{2r}$. If equality holds, the presentation is called *consistent*, see [**9**, page 280].

Recall in the proof of theorem 3.2 that $\mathcal{G}(L) := H/N$ where $H = H_{p,r}$ and N is the normal subgroup defined by (3.4). Suppose, as in the proof of theorem 3.2, that H is generated by $h_1, \ldots, h_r$. Since the map $\chi\colon G \to H/N$ defined by $g_i\chi = h_i N$ and $z_i\chi = h_i^p N$ preserves the relations in (3.7), it is a homomorphism. However χ is surjective, so χ is an isomorphism, and the presentation (3.7) must be consistent. □

As introduced in the introduction, for a prime p, we let IAC_p denote the set of isomorphism classes of finite dimensional IAC algebras over $\mathbb{F}_p$ and we let UCS_{p^2} denote the set of isomorphism classes of finite UCS p-groups of exponent p^2.

REMARK 3.4. Let p be an odd prime. We have well-defined maps on isomorphism classes $\mathrm{UCS}_{p^2} \to \mathrm{IAC}_p$ with $[G] \mapsto [\mathcal{L}(G)]$ as per lemma 3.1 and $\mathrm{IAC}_p \to \mathrm{UCS}_{p^2}$ with $[L] \mapsto [\mathcal{G}(L)]$ as per theorem 3.2. It is convenient to identify isomorphism classes $[G]$ and $[L]$ with G and L respectively, and use $=$ instead of $\cong$. With this abuse in mind, $\mathcal{L}$ and $\mathcal{G}$ can be viewed as mutually inverse functions.

THEOREM 3.5. *Let p be an odd prime.*

(a) *If G is a finite UCS group of exponent p^2, then $\mathcal{G}(\mathcal{L}(G)) = G$.*

(b) *If L is a finite-dimensional IAC algebra over $\mathbb{F}_p$, then $\mathcal{L}(\mathcal{G}(L)) = L$.*

Therefore the maps $\mathcal{G}\colon \mathrm{IAC}_p \to \mathrm{UCS}_{p^2}$ and $\mathcal{L}\colon \mathrm{UCS}_{p^2} \to \mathrm{IAC}_p$ are bijections.

Proof. (a) Let G be a finite UCS p-group of exponent p^2, say with r generators. Suppose that $\{g_1, \ldots, g_r\}$ is a minimal generating set for G. Since $G' = G^p$ there

exist constants $c_k^{(i,j)}$ satisfying:

$$[g_i, g_j] = \prod_{k=1}^{r} (g_k^p)^{c_k^{(i,j)}} \text{ where } 1 \leqslant i < j \leqslant r \quad \text{and } 0 \leqslant c_k^{(i,j)} \leqslant p-1. \tag{3.8}$$

Introducing redundant generators $z_k := g_k^p$ we see that G has a polycyclic presentation of the form (3.7). It follows from (3.1) that $[\![\overline{g}_i, \overline{g}_j]\!] = \sum_{k=1}^{r} c_k^{(i,j)} \overline{g}_k$. Therefore the numbers $c_k^{(i,j)}$, interpreted as elements of the field $\mathbb{F}_p$, are structure constants of $L := \mathcal{L}(G)$. By corollary 3.3 the group $\mathcal{G}(L)$ has a polycyclic presentation of the form (3.7) involving the *same* $c_k^{(i,j)}$. This proves that $\mathcal{G}(\mathcal{L}(G)) \cong G$ as desired.

(b) Let L be a finite-dimensional IAC algebra over $\mathbb{F}_p$. Theorem 3.2 proves precisely that $\mathcal{L}(\mathcal{G}(L)) \cong L$ where the minimal number of generators of $\mathcal{G}(L)$ is $\dim(L)$. □

We denote the kernel of the homomorphism $\mathrm{Aut}(G) \to \mathrm{Aut}(G/\mathsf{Z}(G))$ by $\mathrm{Aut}_C(G)$. The elements of $\mathrm{Aut}_C(G)$ are called *central automorphisms* of G.

THEOREM 3.6. *Let G be an r-generator UCS p-group of exponent p^2 where $p > 2$, and let $L = \mathcal{L}(G)$. Then* $\mathrm{Aut}(G)/\mathrm{Aut}_C(G) \cong \mathrm{Aut}(L)$ *where* $\mathrm{Aut}_C(G)$ *is elementary abelian of order* p^{r^2}.

Proof. Let G be an r-generator UCS p-group of exponent p^2. Write $A = \mathrm{Aut}(G)$. Each $\alpha \in A$ induces an $\overline{\alpha} \in \mathrm{Aut}(\overline{G})$ defined by $\overline{g\alpha} = (g\alpha)\Phi(G)$ and $\alpha \mapsto \overline{\alpha}$ is a homomorphism. The additive group of $L := \mathcal{L}(G)$ is $\overline{G}$, and it was shown in the proof of theorem 3.2 that $\alpha \mapsto \overline{\alpha}$ defines a *surjective* homomorphism $\mathrm{Aut}(G) \to \mathrm{Aut}(L)$. The kernel K of this epimorphism comprises those $\alpha \in A$ with $\overline{g}\,\overline{\alpha} = \overline{g}$ for all $g \in G$. Since $\Phi(G) = \mathsf{Z}(G)$, K is the group $\mathrm{Aut}_C(G)$ of central automorphisms. Therefore, $\mathrm{Aut}(G)/\mathrm{Aut}_C(G) \cong \mathrm{Aut}(L)$ as claimed.

Let $\alpha \in K$ be a central automorphism. Then $g\alpha = gz_g$ for some $z_g \in Z(G)$ for all $g \in G$. Since $[g_1\alpha, g_2\alpha] = [g_1, g_2]$ and $G' = \mathsf{Z}(G)$, we see that α acts as the identity on $\mathsf{Z}(G)$. Hence z_g depends only on the coset $g\Phi(G) = \overline{g}$ and we may write $z_{\overline{g}} = z_g$. This gives a function $\overline{G} \to \mathsf{Z}(G)$ defined by $\overline{g} \mapsto z_{\overline{g}}$. There is a well-known isomorphism $\mathrm{Aut}_C(G) \to \mathrm{Hom}_{\mathbb{F}_p}(\overline{G}, \mathsf{Z}(G))$ taking α to the map $\overline{g} \mapsto z_{\overline{g}}$. However, $\mathrm{Hom}_{\mathbb{F}_p}(\overline{G}, \mathsf{Z}(G))$ is isomorphic to the additive group of $r \times r$ matrices over $\mathbb{F}_p$. Thus $\mathrm{Aut}_C(G)$ is elementary abelian of order p^{r^2}. (By contrast, the group $\mathrm{Inn}(G)$ of inner automorphisms, which is a subgroup of $\mathrm{Aut}_C(G)$, has order only p^r.) □

4. The structure of UCS *p*-groups and IAC algebras

In this section, we prove that a finite-dimensional IAC algebra over an arbitrary field is semisimple in the sense that it is a direct sum of pairwise isomorphic simple algebras. This leads naturally to the study of simple IAC algebras in § 5. As noted in the introduction, invariant non-associative algebra structures also appeared in the study of finite simple groups, and a result similar to our theorem 4.2 was proved in [**12**, lemma 2.4]. Since our context is somewhat different, we present our theorem with a proof. We will also extend the group–algebra duality established in § 3. In

proposition 4.4 we exhibit a bijection between subalgebras of L and powerful subgroups of $G = \mathcal{G}(L)$ that contain $\Phi(G)$. This is reminiscent of the duality between field extensions and groups in Galois theory, because the substructures match.

Let V be a vector space. An irreducible subgroup H of $\mathrm{GL}(V)$ is called *imprimitive* if there is an H-invariant direct sum decomposition $V = V_1 \oplus \cdots \oplus V_\ell$ with $\ell \geqslant 2$. We call the decomposition $V = V_1 \oplus \cdots \oplus V_\ell$ an *imprimitivity decomposition* for H. If no such decomposition exists, we call H *primitive*. By the irreducibility of the acting group, an imprimitivity decomposition is necessarily equidimensional; that is $\dim V_i = \dim V_j$ for all subspaces $V_i,\ V_j$ of the decomposition.

Suppose that $V = V_1 \oplus \cdots \oplus V_\ell$ is an imprimitivity decomposition for an irreducible subgroup $H \leqslant \mathrm{GL}(V)$. Then the action of H induces a permutation group on the set $\{V_1, \ldots, V_\ell\}$. Further, H is isomorphic (as a linear group) to a subgroup of the wreath product $\mathrm{GL}(r/\ell, \mathbb{F}) \wr K$ where $r = \dim V$ and $K \leqslant \mathsf{S}_\ell$ is permutationally isomorphic to the group induced by H on $\{V_1, \ldots, V_\ell\}$. The structure of $\mathrm{GL}(r/\ell, \mathbb{F}) \wr \mathsf{S}_\ell$ is described in [**16**, § 15]. The following theorem is commonly attributed to Clifford, see [**16**, lemma 4, § 15].

THEOREM 4.1. *The following hold.*

(a) *Given a vector space V_1 over a field $\mathbb{F}$, a non-trivial subgroup $A_1 \leqslant \mathrm{GL}(V_1)$ and a transitive subgroup $P \leqslant \mathsf{S}_\ell$, the subgroup $A_1 \wr P$ of $\mathrm{GL}((V_1)^{\oplus \ell})$ is irreducible if and only if A_1 is irreducible on V_1.*

(b) *Suppose that $A \leqslant \mathrm{GL}(V)$ is irreducible on the vector space V and preserves the imprimitivity decomposition $V = V_1 \oplus \cdots \oplus V_\ell$. Then A is conjugate in $\mathrm{GL}(V)$ to a subgroup of $\mathrm{GL}(V_1) \wr \mathsf{S}_\ell$. Further, A is transitive on $\{V_1, \ldots, V_\ell\}$ and the setwise stabilizer A_{V_1} is irreducible on V_1.*

Using Lie theoretic notation, the *centre* of an anti-commutative algebra L is

$$\mathsf{Z}(L) := \{x \in L \mid [\![x, y]\!] = 0 \text{ for all } y \in L\}.$$

Since $\mathsf{Z}(L)$ is invariant under $\mathrm{Aut}(L)$, we see, for a non-abelian IAC algebra L, that $\mathsf{Z}(L) = 0$.

The next theorem shows that an IAC algebra (over an arbitrary field) is semisimple. See [**12**, lemma 2.4] for a similar result.

THEOREM 4.2. *The following hold.*

(a) *Suppose L_0 is a simple IAC algebra, and $\ell \geqslant 1$ is an integer. Then the direct sum $L = (L_0)^{\oplus \ell}$ is an IAC algebra. Further, if L_0 is non-abelian, then $L = (L_0)^{\oplus \ell}$ has precisely ℓ minimal ideals namely the given direct summands, and in particular $\mathrm{Aut}(L) = \mathrm{Aut}(L_0) \wr \mathsf{S}_\ell$.*

(b) *Let L be an IAC algebra of finite dimension. Then $L \cong I^{\oplus \ell}$ for some simple IAC subalgebra I of L and some $\ell \geqslant 1$. Further, if L is non-abelian, then ℓ is the number of minimal ideals of L.*

Proof. (a) If L_0 is abelian, then so is L. Thus $\dim(L_0) = 1$ and $\mathrm{Aut}(L) = \mathrm{GL}(L)$ acts irreducibly. Hence L is IAC.

Suppose now that L_0 is non-abelian. Let $L_1, \ldots, L_\ell$ be the summands of the direct sum decomposition of L. Then, for $i \geqslant 1$, L_i is a minimal ideal of L. We claim that each minimal ideal I coincides with L_i for some $i \geqslant 1$. Assume, seeking a contradiction, that $I \neq L_i$ for all $i \geqslant 1$. Then, the minimality of I implies $[\![L_i, I]\!] \subseteq L_i \cap I = 0$ for all $i \geqslant 1$. Thus $[\![L, I]\!] = 0$, and so $I \leqslant \mathsf{Z}(L)$; this is a contradiction as $\mathsf{Z}(L) = 0$. Therefore $L_1, \ldots, L_\ell$ are all the minimal ideals of L as claimed. Now $\mathrm{Aut}(L)$ contains the wreath product $W = \mathrm{Aut}(L_0) \wr \mathsf{S}_\ell$ and W is an irreducible subgroup of $\mathrm{GL}(L)$ by theorem 4.1(a). Thus L is an IAC algebra. The group $\mathrm{Aut}(L)$ permutes the minimal ideals of L, and hence $L = L_1 \oplus \cdots \oplus L_\ell$ is an imprimitivity decomposition of $\mathrm{Aut}(L)$. Further, the stabilizer of L_i in $\mathrm{Aut}(L)$ induces a group of automorphisms of L_i, which shows, by theorem 4.1(b), that $\mathrm{Aut}(L) \leqslant \mathrm{Aut}(L_0) \wr \mathsf{S}_\ell$. Therefore, $\mathrm{Aut}(L) = \mathrm{Aut}(L_0) \wr \mathsf{S}_\ell$ as claimed.

(b) Let L be a finite-dimensional IAC algebra and set $A = \mathrm{Aut}(L)$. If L is abelian, then $L = \mathbb{F}^{\oplus \ell}$ where $\ell = \dim(L)$, and each copy of $\mathbb{F}$ is a simple IAC algebra of dimension 1. Thus in this case the assertion is valid. Suppose that L is non-abelian. As noted above, $\mathsf{Z}(L) = 0$. Let I be a minimal ideal of L and set $\mathcal{I} = \{I\alpha \mid \alpha \in A\}$. Define $K = \sum_{J \in \mathcal{I}} J$; then K is a non-trivial ideal of L which is invariant under A. Thus $K = L$ because A acts irreducibly on L. We show that the sum $\sum_{J \in \mathcal{I}} J$ is direct. Given $J_0 \in \mathcal{I}$, set $\overline{J}_0 = \sum_{J \in \mathcal{I} \setminus \{J_0\}} J$. We are required to show that $J_0 \cap \overline{J}_0 = 0$. If $J \in \mathcal{I} \setminus \{J_0\}$, then $J_0 \cap J \trianglelefteqslant L$, and, by the minimality of J, we have that $J_0 \cap J = 0$. On the other hand, $[\![J_0, J]\!] \leqslant J_0 \cap J$, and hence $[\![J_0, J]\!] = 0$. Thus J_0 centralizes each of the elements of $\mathcal{I} \setminus \{J_0\}$, which gives that $[\![J_0, \overline{J}_0]\!] = 0$. Then

$$[\![J_0 \cap \overline{J}_0, L]\!] = [\![J_0 \cap \overline{J}_0, J_0 + \overline{J}_0]\!] = [\![J_0 \cap \overline{J}_0, J_0]\!] = 0,$$

which implies that $J_0 \cap \overline{J}_0 \leqslant \mathsf{Z}(L)$, and, in turn, that $J_0 \cap \overline{J}_0 = 0$. Thus L is equal to the direct sum $\bigoplus_{J \in \mathcal{I}} J$ as claimed. Write $L \cong I^{\oplus \ell}$ where I is a minimal ideal of L and $\ell = |\mathcal{I}|$.

It remains to show that I is IAC. As I inherits anti-commutativity from L, we need to show that $\mathrm{Aut}(I)$ is irreducible on I. Since $\mathrm{Aut}(L)$ permutes the elements of $\mathcal{I}$, the decomposition $L = \bigoplus_{J \in \mathcal{I}} J$ is an imprimitivity decomposition for $\mathrm{Aut}(L)$. Let A_I denote the setwise stabilizer of I in $\mathrm{Aut}(L)$. Then A_I induces a group of automorphisms of I that is irreducible on I by theorem 4.1(b). Hence I is an IAC algebra. □

THEOREM 4.3. *Let G be a finite UCS p-group of exponent p^2 for some odd prime p and let $k \geqslant 1$. Then $G^{\times k}$ is a UCS p-group of exponent p^2 and $\mathcal{L}(G^{\times k}) \cong \mathcal{L}(G)^{\oplus k}$.*

Proof. The assertion of the theorem holds if G is abelian, and so we may assume that G is non-abelian. Certainly $G^{\times k}$ has exponent p^2. Moreover,

$$\Phi(G^{\times k}) = \Phi(G)^{\times k} \quad \text{and} \quad G^{\times k}/\Phi(G^{\times k}) \cong (G/\Phi(G))^{\times k} = \overline{G}^{\times k}.$$

By lemma 2.2, $\mathrm{Aut}(G)$ is irreducible on $\overline{G}$ and on $\Phi(G)$. Further, since G is non-abelian, $\overline{G}$ and $\Phi(G)$ are non-trivial $\mathrm{Aut}(G)$-modules. Since $\mathrm{Aut}(G) \wr \mathsf{S}_k \leqslant$

$\mathrm{Aut}(G^{\times k})$, it follows from theorem 4.1(a) that $\mathrm{Aut}(G^{\times k})$ acts irreducibly on $G^{\times k}/\Phi(G^{\times k})$ and on $\Phi(G^{\times k})$, and thus $G^{\times k}$ is a UCS p-group, by lemma 2.2.

We now prove that $\mathcal{L}(G^{\times k}) \cong \mathcal{L}(G)^{\oplus k}$. Let G_i denote the i-th copy of G in the direct product $G^{\times k}$. Set $L = \mathcal{L}(G^{\times k})$ and, for $i = 1, \ldots, k$, let $L_i = G_i\Phi(G^{\times k})/\Phi(G^{\times k})$. We claim that $L_i \trianglelefteqslant L$. First, if $\overline{u},\ \overline{v} \in L_i$ with $u,\ v \in G_i$, then $[\![\overline{u}, \overline{v}]\!] = [u, v]^{1/p} \in L_i$. Hence $L_i \leqslant L$. If $g_i \in G_i$ and $g_j \in G_j$ with $i \neq j$, then $[g_i, g_j] = 1$, and so $[\![\overline{g}_i, \overline{g}_j]\!] = 0$. This shows that L_i is an ideal of L for each $i \in \{1, \ldots, k\}$. Since

$$\mathcal{L}(G^{\times k}) = G^{\times k}/\Phi(G^{\times k}) = \bigoplus_{i=1}^{k} G_i\Phi(G^{\times k})/\Phi(G^{\times k}) = \bigoplus_{i=1}^{k} L_i,$$

and each L_i is isomorphic to $\mathcal{L}(G)$, we obtain that $\mathcal{L}(G^{\times k}) = \mathcal{L}(G)^{\oplus k}$. □

Powerful p-groups were introduced by Lubotzky and Mann [**15**]. A finite p-group G is said to be *powerful* if $G' \leqslant G^p$ when $p > 2$, and $G' \leqslant G^4$ when $p = 2$. A subgroup N of a p-group G is said to be *powerfully embedded* in G if $[N, G] \leqslant N^p$ when $p > 2$ and $[N, G] \leqslant N^4$ when $p = 2$. A powerfully embedded subgroup of G is always normal in G.

Proposition 4.4. *Let G be a finite UCS p-group of odd exponent p^2, and $L = \mathcal{L}(G)$.*

(a) *There is a bijection between the set of subalgebras of L and the set of powerful subgroups of G that contain $\Phi(G)$.*

(b) *The ideals of L correspond, via part* (a)*, to powerfully embedded subgroups of G.*

Proof. There is a bijection $H \leftrightarrow \overline{H} := H/\Phi(G)$ between the set of subgroups of G that contain $\Phi(G)$, and the set of subgroups of the quotient $\overline{G} = G/\Phi(G)$. The subgroups of $\overline{G}$ are precisely the linear subspaces of L. We show first that H is a powerful subgroup of G if and only if $\overline{H}$ is a subalgebra of L which we henceforth denote as $\overline{H} \leqslant L$.

Suppose that $\overline{H} \leqslant L$ and let $h_1,\ h_2 \in H$. Then $[\![\overline{h_1}, \overline{h_2}]\!] \in \overline{H}$, and so $[\![\overline{h_1}, \overline{h_2}]\!] = \overline{h}$ with $h \in H$. The definition in (3.1) of the product in L implies that $[h_1, h_2] = h^p$, which shows that $H' \leqslant H^p$, and hence H is powerful. Conversely, suppose that H is powerful. Suppose $h_1,\ h_2 \in H$. Then $(h_1h_2)^p = h_1^p h_2^p$ since $p > 2$, so the subgroup $H^p = \langle h^p \mid h \in H \rangle$ equals the subset $\{h^p \mid h \in H\}$. Since $H' \leqslant H^p$, it follows that $[h_1, h_2] = h^p$ for some $h \in H$. Thus $[\![\overline{h_1}, \overline{h_2}]\!] = [h_1, h_2]^{1/p} = \overline{h} \in \overline{H}$ by (3.1), and so $\overline{H} \leqslant L$.

Suppose now that H is powerfully embedded in G. We have, for every $h \in H$ and $g \in G$, that $[h, g] = h_0^p$ for some $h_0 \in H$, and so $[\![\overline{h}, \overline{g}]\!] = [h, g]^{1/p} = \overline{h_0} \in \overline{H}$. Hence $\overline{H} \trianglelefteqslant L$. On the other hand, suppose $I \trianglelefteqslant L$. Then $I = \overline{H}$ for some $H \leqslant G$ with $\Phi(G) \leqslant H$. Since $\overline{H}$ is an ideal, for every $h \in H$ and $g \in G$ we have $[\![\overline{h}, \overline{g}]\!] = \overline{h_0}$ for some $h_0 \in H$. Hence, $[h, g]^{1/p} = \overline{h_0}$, and so $[h, g] = h_0^p$. Thus $[H, G] \leqslant H^p$ and H is powerfully embedded in G. □

By theorem 4.2, every non-trivial proper ideal of an IAC algebra is a direct summand. Now we state and prove a corresponding result for UCS p-groups of exponent p^2.

COROLLARY 4.5. *Let G be a finite UCS p-group with odd exponent p^2. There exists a subgroup H of G satisfying the following conditions:*

(a) *H is powerfully embedded in G and $\Phi(G) < H$, and*

(b) *H is minimal among the subgroups of G satisfying* (a).

There exists a UCS subgroup H_0 of G of exponent p^2 such that $G = (H_0)^k$ for some $k \geqslant 1$, and $H_0\Phi(G) = H$.

Proof. A subgroup H satisfying conditions (a) and (b) does exist because $G' \leqslant G^p$ and G satisfies condition (a). Set $L = \mathcal{L}(G)$ and $L_0 = H/\Phi(G)$. By lemma 3.1, L is an IAC algebra, and $L_0 \trianglelefteqslant L$ by proposition 4.4. Since L_0 is minimal, and hence simple, $L = (L_0)^{\oplus k}$ for some $k \geqslant 1$ by theorem 4.2(b). However, $H_0 = \mathcal{G}(L_0)$ is a UCS group of exponent p^2 by theorem 3.2, and so too is $(H_0)^{\times k}$ by theorem 4.3. However, $\mathcal{L}((H_0)^{\times k}) = \mathcal{L}(H_0)^{\oplus k} = \mathcal{L}(\mathcal{G}(L_0))^{\oplus k} = (L_0)^{\oplus k} = L$. Therefore $\mathcal{L}((H_0)^{\times k}) = \mathcal{L}(G)$. We obtain, by theorem 3.5, that $(H_0)^{\times k} = \mathcal{G}(\mathcal{L}((H_0)^{\times k})) = \mathcal{G}(\mathcal{L}(G)) = G$, and similarly $L_0 = \mathcal{L}(\mathcal{G}(L_0)) = \mathcal{L}(H_0)$. Finally, since $L_0 = H_0/\Phi(H_0) = H/\Phi(G)$, we have $H = H_0\Phi(G)$. □

By theorem 2.4 (also by theorem 4.3), if G is a UCS p-group of exponent p^2, then $G^{\times k}$ is also a UCS p-group of exponent p^2. Hence in the class UCS_{p^2}, the groups that cannot be decomposed non-trivially as direct powers can be viewed as basic building blocks. The final result of this section gives sufficient and necessary conditions for a UCS p-group of exponent p^2 to be indecomposable as a direct power of a smaller such group. The corollary follows easily from theorem 4.3 and corollary 4.5.

COROLLARY 4.6. *The following are equivalent for a non-abelian finite UCS p-group of odd exponent p^2:*

(a) *G cannot be written as a direct product $H^{\times k}$ where H is a UCS p-group and $k \geqslant 2$;*

(b) *G does not contain a powerfully embedded proper subgroup N such that $\Phi(G) < N$;*

(c) *$\mathcal{L}(G)$ is a simple algebra.*

5. Simple IAC algebras of dimension at most 4

For an anti-commutative algebra of dimension r we have $\dim[\![L, L]\!] \leqslant \binom{r}{2}$. Thus an r-dimensional IAC algebra is abelian and simple if $r = 1$, and abelian and non-simple if $r = 2$. In this section, we classify simple IAC algebras of dimension 3 and 4 in proposition 5.1 and theorem 5.3, respectively.

5.1. 3-dimensional IAC algebras

The proof of the following proposition uses ideas from the proof of [7, lemma 9].

PROPOSITION 5.1. *If L is a non-abelian 3-dimensional IAC algebra over a field $\mathbb{F}$ of characteristic different from 2, then L is a simple Lie algebra and* $\mathrm{Aut}(L) \cong \mathsf{SO}(3,\mathbb{F})$.

Proof. Suppose that L is a non-abelian 3-dimensional IAC algebra. Let $e = \{e_1, e_2, e_3\}$ be a basis for L and set $f_1 = [\![e_2, e_3]\!]$, $f_2 = [\![e_3, e_1]\!]$ and $f_3 = [\![e_1, e_2]\!]$. Since $[\![L, L]\!] = L$, we have that $f = \{f_1, f_2, f_3\}$ is also a basis for L. Write $f_i = \sum_{j=1}^{3} a_{ij} e_j$ where $a_{ij} \in \mathbb{F}$ and $i \in \{1, 2, 3\}$, and consider the 3×3 invertible matrix $A = (a_{ij})$. We claim that L satisfies the Jacobi identity if and only if A is symmetric. Since L is 3-dimensional, L satisfies the Jacobi identity if and only if the following equation holds:

$$0 = [\![e_1, [\![e_2, e_3]\!]]\!] + [\![e_2, [\![e_3, e_1]\!]]\!] + [\![e_3, [\![e_1, e_2]\!]]\!] = [\![e_1, f_1]\!] + [\![e_2, f_2]\!] + [\![e_3, f_3]\!].$$

Using the linear combinations for the f_i, we obtain the equivalent equation:

$$a_{12}[\![e_1, e_2]\!] + a_{13}[\![e_1, e_3]\!] + a_{21}[\![e_2, e_1]\!] + a_{23}[\![e_2, e_3]\!] + a_{31}[\![e_3, e_1]\!] + a_{32}[\![e_3, e_2]\!] = 0.$$

Finally, the last equation is equivalent to the statement that A is a symmetric matrix.

We now prove that A is a symmetric matrix. Let $g \in \mathrm{Aut}(L)$ and let $[g]_e$ and $[g]_f$ denote the matrices that represent g in the bases e and f, respectively. We claim that $[g]_f = \det[g]_e([g]_e)^{-t}$ where $(\cdot)^{-t}$ denotes the inverse transpose operation. Let $[g]_e = (g_{ij})$ and $[g]_f = (f_{ij})$. As $g \in \mathrm{Aut}(L)$, we have

$$\begin{aligned} f_1 g &= [\![e_2, e_3]\!]g = [\![e_2 g, e_3 g]\!] = [\![g_{21}e_1 + g_{22}e_2 + g_{23}e_3, g_{31}e_1 + g_{32}e_2 + g_{33}e_3]\!] \\ &= (g_{22}g_{33} - g_{23}g_{32})[\![e_2, e_3]\!] + (g_{23}g_{31} - g_{21}g_{33})[\![e_3, e_1]\!] \\ &\quad + (g_{21}g_{32} - g_{22}g_{31})[\![e_1, e_2]\!]. \end{aligned}$$

This gives the first of the following equations, the others follow by cyclic permutations:

$$\begin{aligned} f_1 g &= (g_{22}g_{33} - g_{23}g_{32})f_1 + (g_{23}g_{31} - g_{21}g_{33})f_2 + (g_{21}g_{32} - g_{22}g_{31})f_3; \\ f_2 g &= (g_{32}g_{13} - g_{33}g_{12})f_1 + (g_{33}g_{11} - g_{31}g_{13})f_2 + (g_{31}g_{12} - g_{32}g_{11})f_3; \\ f_3 g &= (g_{12}g_{23} - g_{13}g_{22})f_1 + (g_{13}g_{21} - g_{11}g_{23})f_2 + (g_{11}g_{22} - g_{12}g_{21})f_3. \end{aligned} \tag{5.1}$$

By Cramer's Rule, the 3×3 system (5.1) has coefficient matrix $\det([g]_e)([g]_e)^{-t}$. Therefore, $[g]_f = \det([g]_e)([g]_e)^{-t}$, as claimed. For $v \in L$, let $[v]_e$ and $[v]_f$ denote vector representations of v in the bases e and f, respectively. The matrix $A = (a_{ij})$ acts as a basis transformation matrix from the basis e to the basis f and $[v]_f = [v]_e A$. Therefore, $[g]_e = A[g]_f A^{-1}$ and so $[g]_e = A \det([g]_e)([g]_e)^{-t} A^{-1}$, which implies that $[g]_e A [g]_e^t = \det([g]_e)A$. This says that g preserves the bilinear form $(u, v) \mapsto [u]_e A([v]_e)^t$ up to a scalar multiple. In the next paragraph, we prove that $A^t = A$.

Consider the group $\mathcal{G}(A) := \{B \in \mathrm{GL}(3,\mathbb{F}) \mid BAB^t = \det(B)A\}$. The previous paragraph shows that $g \in \mathrm{Aut}(L)$ implies $[g]_e \in \mathcal{G}(A)$. Let J be the skew-symmetric matrix $A - A^t$, and define $\mathcal{G}(J) = \{B \in \mathrm{GL}(3,\mathbb{F}) \mid BJB^t = \det(B)J\}$ similarly. Clearly $\mathcal{G}(A)$ is a subgroup of $\mathcal{G}(J)$. Note that if $w \in \ker(J)$ and $B \in \mathcal{G}(J)$, then

$$wBJ = wBJB^tB^{-t} = \det(B)wJB^{-t} = 0.$$

Hence $\mathcal{G}(J)$ fixes the subspace

$$\ker(J) = \{v \in \mathbb{F}^3 \mid vJ = 0\}.$$

Since $\mathrm{Aut}(L)$, considered as a subgroup of $\mathrm{GL}(3,\mathbb{F})$, is contained in $\mathcal{G}(A)$ and $\mathcal{G}(A) \leqslant \mathcal{G}(J)$ and $\mathrm{Aut}(L)$ acts irreducibly on L, we see that $\ker(J)$ must be 0 or L. Further, since the matrix $J = A - A^t$ is skew-symmetric, we obtain that

$$\det(J) = \det(J^t) = \det(-J) = (-1)^3\det(J), \quad \text{and so } 2\det(J) = 0.$$

Thus, since $\mathrm{char}(\mathbb{F}) \neq 2$, $\det(J) = 0$. Therefore, $\ker(J) \neq 0$, and hence $\ker(J) = L$. Thus $A - A^t = J = 0$, and A is symmetric, as claimed. As explained in the first paragraphs of this proof, we obtain that L is a Lie algebra. Since L is non-abelian and IAC, theorem 4.2 implies that L is the direct sum of pairwise isomorphic simple IAC algebras. As $\dim L = 3$ and an IAC algebra of dimension 1 is abelian (see the paragraph before proposition 5.1), the algebra L must be simple.

Let $g \in \mathrm{Aut}(L)$. Since $[g]_e \leqslant \mathcal{G}(A)$ we see that $[g]_eA([g]_e)^t = \det(g)A$. However, A is an invertible 3×3 matrix, so taking determinants gives $\det(g)^2\det(A) = \det(g)^3\det(A)$. Hence $\det(g) = 1$, and g preserves the symmetric bilinear form defined by A. Hence we have shown that $\mathrm{Aut}(L)$ lies in the subgroup $\mathsf{SO}(3,\mathbb{F})$ of $\mathcal{G}(A)$. Suppose $g \in \mathsf{SO}(3,\mathbb{F})$. The steps in the second paragraph of the proof are reversible, so it follows that $g \in \mathrm{Aut}(L)$. Thus we conclude that $\mathrm{Aut}(L) \cong \mathsf{SO}(3,\mathbb{F})$, as desired. □

Proposition 5.1 can be reversed: a 3-dimensional simple Lie algebra is IAC. This follows from the fact that the automorphism group of a 3-dimensional simple Lie algebra is isomorphic to the irreducible group $\mathsf{SO}(3,\mathbb{F})$ stabilizing its Killing form. If $\mathbb{F}$ is a finite field or an algebraically closed field of characteristic different from 2, then the only 3-dimensional simple Lie algebra over $\mathbb{F}$, up to isomorphism, is the classical Lie algebra $\mathfrak{sl}(2,\mathbb{F})$ which is IAC. More generally, if $n \geqslant 2$, and $\mathbb{F}$ is a field of characteristic 0 or of characteristic p such that $p \nmid n$, then the group $\mathrm{GL}(n,\mathbb{F})$ acts on the simple Lie algebra $\mathfrak{sl}(n,\mathbb{F})$ by the adjoint action $g\colon x \mapsto x^g = g^{-1}xg$ for all $x \in \mathfrak{sl}(n,\mathbb{F})$ and $g \in \mathrm{GL}(n,\mathbb{F})$. Since this action is irreducible (see [**1**, lemma 5.4.10]), the simple Lie algebra $\mathfrak{sl}(n,\mathbb{F})$ is IAC. It would be interesting to study whether all known finite-dimensional simple Lie algebras are IAC, but this problem goes beyond the scope of this paper. By [**8**, Hauptsatz], if L is a finite-dimensional Chevalley-type simple Lie algebra in characteristic different from 2, then L is IAC.

Interesting examples of IAC algebras can also be found among Malcev algebras. For a field $\mathbb{F}$ of characteristic different from 2, the algebra $\mathbb{O}(\mathbb{F})$ of octonions can be viewed as an anti-commutative algebra under the multiplication $[\![a,b]\!] = ab - ba$. If $\mathrm{char}(\mathbb{F}) \neq 3$, then the algebra $(\mathbb{O}(\mathbb{F}), +, [\![\cdot,\cdot]\!])$ is not a Lie algebra, since $\mathbb{O}(\mathbb{F})$ is not associative. Further, the algebra $(\mathbb{O}(\mathbb{F}), +, [\![\cdot,\cdot]\!])$ can be written as $\mathbb{F} \oplus M$ where

M is a 7-dimensional anti-commutative algebra and the simple exceptional group $G_2(\mathbb{F})$ acts irreducibly on M (see [**21**, § 4.3]). Hence M is an IAC algebra. By [**14**, theorem 3.11], non-Lie central simple Malcev algebras over fields of characteristic different from 2 or 3 are 7-dimensional and can be defined similarly to the algebra M above. By [**14**, theorem 3.11], over a finite field of characteristic different from 2, there is a unique isomorphism type of central simple non-Lie Malcev algebras; namely, the algebra M defined above.

5.2. 4-dimensional IAC algebras

In [**7**, theorem 17], the authors classified 4-generator UCS p-groups with exponent p^2. The bijection in theorem 3.5 gives a classification of 4-dimensional simple IAC algebras over $\mathbb{F}_p$ where p is an odd prime. Using the ideas of the proof of [**7**, theorem 17], this classification is extended in theorem 5.3 to all finite fields of characteristic different from 2.

The concept of ESQ-modules was defined in [**7**]. Let us recall the definition.

Definition 5.2. *For a group H and a field $\mathbb{F}$, an $\mathbb{F}H$-module V is called an* ESQ-module *(for **e**xterior **s**elf-**q**uotient) if there exists an $\mathbb{F}H$-submodule U of $\wedge^2 V$ such that $\wedge^2 V/U \cong V$. In this case, H is called an* ESQ subgroup *of* $\mathrm{GL}(V)$.

If A is a non-abelian finite-dimensional IAC algebra over a field $\mathbb{F}$, then the product map $\psi\colon \wedge^2 A \to A$, defined by $(u \wedge v)\psi = [\![u, v]\!]$, is an epimorphism of $\mathrm{Aut}(A)$-modules. Hence $\wedge^2 A/\ker\psi \cong A$, and so A is an irreducible ESQ $\mathbb{F}\mathrm{Aut}(A)$-module. Conversely, let V be an irreducible ESQ-module for a group H over a field $\mathbb{F}$ and let $U \leqslant \wedge^2 V$ such that $\wedge^2 V/U \cong V$. Assume that $\psi\colon \wedge^2 V \to V$ is an epimorphism with kernel U. Then we can define an anti-commutative product on V by setting $[\![u, v]\!] = (u \wedge v)\psi$ and we obtain that $(V, +, [\![\cdot,\cdot]\!])$ is an IAC algebra whose automorphism group contains H as a subgroup.

Theorem 5.3. *Let $\mathbb{F}_q$ be a finite field of q elements and assume that the characteristic of $\mathbb{F}_q$ is not* 2. *Then the following are valid.*

(a) *If* $\mathrm{char}(\mathbb{F}_q) = 5$, *then there exists no* 4*-dimensional simple IAC algebra over $\mathbb{F}_q$.*

(b) *If* $q \equiv \pm 1 \pmod 5$, *then there exists, up to isomorphism, a unique* 4*-dimensional simple IAC algebra over $\mathbb{F}_q$. Further, this algebra is isomorphic to the algebra given by the presentation*

$$\begin{aligned}\langle e_1, e_2, e_3, e_4 \mid\ & [\![e_1, e_2]\!] = e_1 + e_2 + 5e_3 + 3e_4,\\ & [\![e_1, e_3]\!] = -4e_1 - 4e_2 + 0e_3 - 2e_4,\\ & [\![e_1, e_4]\!] = 2e_1 + 4e_2 - 4e_3 - 2e_4,\\ & [\![e_2, e_3]\!] = -3e_1 - 1e_2 + 1e_3 + 3e_4\\ & [\![e_2, e_4]\!] = 2e_1 + 0e_2 + 4e_3 + 4e_4,\\ & [\![e_3, e_4]\!] = -3e_1 - 5e_2 - e_3 - e_4\rangle.\end{aligned}$$

(c) *If* $q \equiv \pm 2 \pmod 5$, *then, up to isomorphism, there are exactly two* 4*-dimensional simple IAC algebras over* $\mathbb{F}_q$*; one of these algebras is given by the presentation in statement* (b).

Moreover, the automorphism group of the algebra presented in (b) *is* $\mathrm{AGL}(1,5)$, *while the automorphism group of the second algebra in* (c) *is* C_5.

Proof. Since the proof follows the ideas in [7, theorem 17], we only give a sketch; the details can be filled in by the reader consulting [7, theorem 17].

(a) It follows from [7, theorem 16] that no irreducible ESQ subgroup of $\mathrm{GL}(4,q)$ exists if $5 \mid q$, and hence over finite fields of characteristic 5, there are no 4-dimensional simple IAC algebras. This proves (a).

Suppose $q = p^k$ where $p \neq 5$ is a prime and $k \geqslant 1$. By quadratic reciprocity, $5 \in (\mathbb{F}_q^\times)^2$ if and only if $q \equiv \pm 1 \pmod 5$. To see this note first that $q \equiv \pm 2 \pmod 5$ implies $p \equiv \pm 2 \pmod 5$ and k is odd, so $5 \notin (\mathbb{F}_p^\times)^2$ and $5 \notin (\mathbb{F}_q^\times)^2$. On the other hand, if $5 \in (\mathbb{F}_q^\times)^2$, then either k is even and $5 \in (\mathbb{F}_{p^2}^\times)^2 \leqslant (\mathbb{F}_q^\times)^2$, or k is odd and $p \equiv \pm 1 \pmod 5$ and so $5 \in (\mathbb{F}_p^\times)^2 \leqslant (\mathbb{F}_q^\times)^2$.

(b) Let L be a 4-dimensional simple IAC algebra over $\mathbb{F}_q$ and set $A = \mathrm{Aut}(L)$. By the discussion preceding this theorem, A is an irreducible ESQ-subgroup of $\mathrm{GL}(4,q)$. We can argue, as in the proof of [7, theorem 17], that $A \leqslant \mathrm{AGL}(1,5)$ contains C_5 and that if $A = \mathrm{AGL}(1,5)$, then L is isomorphic to the algebra presented in (b). By [7, theorem 16], $5 \in (\mathbb{F}_q^\times)^2$ if and only if no proper subgroup of $\mathrm{AGL}(1,5)$ is irreducible. Hence in this case the algebra L presented in statement (b) is, up to isomorphism, the unique simple IAC algebra of dimension 4 over $\mathbb{F}_q$, and $\mathrm{Aut}(L) = \mathrm{AGL}(1,5)$.

(c) Assume now that $q \equiv \pm 2 \pmod 5$. One possibility by [7, theorem 17] is that a simple 4-dimensional IAC algebra L is given by the presentation (b), and $\mathrm{Aut}(L) = \mathrm{AGL}(1,5)$. Suppose now that $A \neq \mathrm{AGL}(1,5)$. The cyclic subgroup C_5 of $\mathrm{AGL}(1,5)$ is contained in A, and it is irreducible since $q \equiv \pm 2 \pmod 5$. Let V be a 4-dimensional vector space over $\mathbb{F}_q$. Let $a \in \mathrm{GL}(4,q)$ be an element of order 5, which is unique up to conjugacy. Then the $\langle a \rangle$-module $\wedge^2 V$ can be written as $\wedge^2 V = W \oplus C$ where $W \cong V$ and C is the 2-dimensional fixed-point space of a. An IAC algebra structure on V is determined by an epimorphism $\varphi\colon \wedge^2 V \to V$. As in the proof of [7, theorem 17], there is a bijection between the set of such linear epimorphisms and the set of subspaces N of $V \oplus \wedge^2 V$ such that $\dim N = 4$, $N \cap V = 0$, and $N \cap \wedge^2 V = C$. If fact, identifying V and W with the field $\mathbb{F}_{q^4}$, we may define, for each $w \in W \backslash \{0\}$ such a subspace N_w exactly as in [7, theorem 17]. Now using the argument in [7, theorem 17], the multiplicative group of $\mathbb{F}_{q^4}$ acts on the set of subspaces N_w, inducing isomorphisms between the associated IAC algebras, with 5 orbits corresponding to the cosets of the multiplicative subgroup $(\mathbb{F}_{q^4}^\times)^5$. Then $\mathrm{Gal}(\mathbb{F}_{q^4} : \mathbb{F}_q) \cong C_4$ also acts on the set of these subspaces N_w, also inducing isomorphism between the associated algebras, fusing the 4 orbits that correspond to non-trivial cosets and leaving the fifth orbit invariant. Therefore, there are two $\mathbb{F}_{q^4}^\times \rtimes \mathrm{Gal}(\mathbb{F}_{q^4} : \mathbb{F}_q)$-orbits on the set of subspaces N_w, and there are two isomorphism types of simple 4-dimensional IAC algebras. □

The IAC algebras given in theorem 5.3(b,c) are members of an infinite family: take $t = 5$ in the following theorem and note that $\mathrm{A\Gamma L}(1,5) = \mathrm{AGL}(1,5)$.

THEOREM 5.4. *If t and q are powers of distinct primes such that $t > 3$, then there exists a $(t-1)$-dimensional IAC algebra over $\mathbb{F}_q$ whose automorphism group contains $A\Gamma L(1,t)$ acting in its irreducible representation of dimension $t-1$.*

Proof. By [7, theorem 18] the $(t-1)$-dimensional module for $A\Gamma L(1,t)$ over $\mathbb{F}_q$ is irreducible and ESQ. The result now follows from the preamble to theorem 5.3. □

6. r-dimensional simple IAC algebras

In this section, we construct an infinite family of finite-dimensional simple IAC algebras. We will work under the following hypothesis.

HYPOTHESIS 6.1. *Fix an integer $b \geqslant 2$. Let $n > 1$ be a divisor of $b^2 + b - 1$. Since $b(b+1) \equiv 1 \pmod{n}$, b is invertible modulo n, and let r be the multiplicative order of b modulo n. Suppose that $r > 1$ and let q be a prime power such that $n \mid (q-1)$. Let $V = (\mathbb{F}_q)^r$ have basis $e_0, e_1, \ldots, e_{r-1}$.*

There are infinitely many choices for a prime-power q with $q \equiv 1 \pmod{n}$ by Dirichlet's Theorem on primes in an arithmetic progression.

Let ζ be an n-th root of unity in $\mathbb{F}_q$ and let G be the subgroup of $\mathrm{GL}(r, \mathbb{F})$ generated by the matrices

$$A = \begin{bmatrix} 0 & 1 & & 0 \\ & & \ddots & \\ 0 & 0 & & 1 \\ 1 & 0 & \ldots & 0 \end{bmatrix} \quad \text{and} \quad B = \begin{bmatrix} \zeta & 0 & \ldots & 0 \\ 0 & \zeta^b & & 0 \\ & & \ddots & \\ 0 & 0 & \ldots & \zeta^{b^{r-1}} \end{bmatrix}.$$

Direct calculation shows that $A^r = B^n = 1$ and $BA = AB^{b^{-1}}$ where b^{-1} denotes the inverse of b modulo n. Let $V = (\mathbb{F}_q)^r$, and consider V and its exterior square $\wedge^2 V$ as G-modules. Since B is a diagonal matrix with pairwise distinct eigenvalues, and A cyclically permutes the 1-dimensional eigenspaces of B, we obtain that G acts irreducibly on V.

PROPOSITION 6.2. *Assume hypothesis 6.1 and let*

$$U_1 = \langle e_i \wedge e_j \mid j - i \equiv 1 \bmod r \rangle = \langle e_0 \wedge e_1, e_1 \wedge e_2, \ldots, e_{r-2} \wedge e_{r-1}, e_{r-1} \wedge e_0 \rangle;$$
$$U_2 = \langle e_i \wedge e_j \mid j - i \not\equiv 1 \bmod r \rangle.$$

Then the following are valid:

(a) $\wedge^2 V = U_1 \oplus U_2$ *is a G-invariant decomposition;*

(b) *the map $\psi \colon V \to U_1$ defined by $e_i\psi = e_{i+1} \wedge e_{i+2}$ reading subscripts modulo r is a G-module isomorphism; and*

(c) *V is an ESQ G-module.*

Proof. (a) Reduce the indices i modulo r if $i \geqslant r$. Then $\{e_i \wedge e_{i+1} \mid 0 \leqslant i \leqslant r-1\}$ is a basis of U_1. Since $(e_i \wedge e_{i+1})A = e_{i+1} \wedge e_{i+2}$, we see that $U_1 A = U_1$. A similar

argument shows that $U_2A = U_2$. Since B is a diagonal matrix, we see that $\langle e_i \wedge e_j\rangle B = \langle e_i \wedge e_j\rangle$ for all $i < j$, and hence $U_1B = U_1$ and $U_2B = U_2$. Thus $\wedge^2 V = U_1 \oplus U_2$ is a G-invariant decomposition, as claimed.

(b) Note first that $b^2 + b \equiv 1 \mod n$ implies $\zeta^{b^2+b} = \zeta$ and $\zeta^{b^{i+2}+b^{i+1}} = \zeta^{b^i}$. Let us verify that ψ commutes with A and with B:

$$\begin{aligned} e_iA\psi &= e_{i+1}\psi = e_{i+2} \wedge e_{i+3} = (e_{i+1} \wedge e_{i+2})A = e_i\psi A;\\ e_iB\psi &= \zeta^{b^i} e_i\psi = \zeta^{b^i}(e_{i+1} \wedge e_{i+2}) = \zeta^{b^{i+1}+b^{i+2}}(e_{i+1} \wedge e_{i+2})\\ &= (e_{i+1} \wedge e_{i+2})B = e_i\psi B. \end{aligned}$$

Since ψ is surjective and $\dim(V) = \dim(V\psi) = \dim(U_1)$, we obtain that ψ is a bijection. Thus ψ is an isomorphism of G-modules.

(c) This follows from (b) and the above fact that V is an irreducible G-module. □

Using the ESQ G-module V constructed before proposition 6.2, we can construct an IAC algebra L that corresponds to V.

Corollary 6.3. *Assume hypothesis 6.1. Let L be the vector space $V = (\mathbb{F}_q)^r$ with an anti-commutative product defined on the basis $\{e_0, e_1, \dots, e_{r-1}\}$ by*

$$\begin{aligned} [\![e_0, e_1]\!] &= e_{r-1},\\ [\![e_{i-1}, e_i]\!] &= e_{i-2} \quad \textit{for } i = 2, 3, \dots, r-1,\\ [\![e_{r-1}, e_0]\!] &= e_{r-2},\\ [\![e_i, e_j]\!] &= 0 \quad \textit{if } \ j - i \neq \pm 1 \pmod r. \end{aligned}$$

Then L is an r-dimensional simple IAC algebra.

Proof. It follows from proposition 6.2 that L is IAC. Let us show that L is simple. Suppose that $I \trianglelefteq L$ and let $v \in I\backslash\{0\}$. Write $v = v_0e_0 + \cdots + v_{r-1}e_{r-1}$ with $v_i \in \mathbb{F}_q$. Suppose without loss of generality that $v_0 \neq 0$. Then using the multiplication table of L, we obtain that

$$[\![[\![v, e_1]\!], e_0]\!] = [\![v_0e_{r-1} - v_2e_0, e_0]\!] = v_0e_{r-2}.$$

Hence $e_{r-2} \in I$. Multiplying e_{r-2} with the elements $e_{r-1}, e_0, \dots e_{r-3}$, we obtain that $e_i \in I$ for all $i \in \{0, \dots, r-1\}$. Thus $I = L$, and so L is simple as claimed. □

7. The Clebsch–Gordan formula for the exterior square

The aim of § 8 is to present a class of ESQ modules for the group $\mathrm{SL}(2, \mathbb{F})$. In this section, we prove a general version of the Clebsch–Gordan Formula for the exterior squares of the representations of $\mathrm{GL}(2, \mathbb{F})$ on spaces of homogeneous polynomials that is valid over fields of characteristic p. Such results are usually proved for $\mathrm{SL}(2, \mathbb{F})$, but generalizing to $\mathrm{GL}(2, \mathbb{F})$ does not require much more effort.

Let $\mathbb{F}$ be a field of characteristic different from 2 and let $\mathbb{F}[X,Y]$ be the algebra of polynomials over $\mathbb{F}$ in two indeterminates. An action of $\mathrm{GL}(2,\mathbb{F})$ on $\mathbb{F}[X,Y]$ is given by

$$\left(\sum \lambda_{ij} X^i Y^j\right) A = \sum \lambda_{ij} (a_{11}X + a_{12}Y)^i (a_{21}X + a_{22}Y)^j \tag{7.1}$$

where $A = \begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix}$. For each integer $m \geqslant 0$, the subspace of homogeneous polynomials of degree m is invariant under this action. This space has dimension $m+1$ since $\{X^i Y^{m-i} \mid 0 \leqslant i \leqslant m\}$ is a basis. When $\mathrm{char}(\mathbb{F}) = 0$ this space is denoted V_m, and it is an irreducible $\mathbb{F}G$-module for each $m \geqslant 0$. However, if $\mathbb{F} = \mathbb{F}_q$ is a finite field, say with $\mathrm{char}(\mathbb{F}_q) = p$, we use a different definition when $p \leqslant m < q$. In this case, the homogeneous polynomials of degree p have a proper submodule, namely $\langle X^p, Y^p \rangle$. The irreducible $\mathrm{SL}(2,\mathbb{F}_q)$-modules in characteristic p were determined by Brauer and Nesbitt, and described clearly in [**1**, theorem 5.2.3]. There are q pairwise non-isomorphic and absolutely irreducible $\mathbb{F}G$-modules which we denote $V_0, V_1, \ldots, V_{q-1}$. If $m < p$, then V_m denotes the subspace of homogeneous polynomials of degree m as above. If $p \leqslant m < q$, the definition of V_m depends on the p-adic expansion $m = m_0 + m_1 p + \cdots + m_k p^k$ of m where $m_i \in \{0, 1, \ldots, p-1\}$ and $k := \lfloor \log_p m \rfloor$. We set $V_m = V_{m_0} \otimes V_{m_1}^{\phi} \otimes \cdots \otimes V_{m_k}^{\phi^k}$ where V^{ϕ} denotes the $\mathbb{F}G$-module obtained from V by twisting by the field automorphism $\phi\colon \mathbb{F} \to \mathbb{F}$ with $\lambda\phi = \lambda^p$, see [**10**, definition VII.1.13].

We are interested in irreducible ESQ-modules, i.e. irreducible modules V which are a quotient of their exterior square. The decomposition of $V_m \otimes V_n$ as a module over $\mathrm{SL}(2,\mathbb{C})$ was described by Clebsch and Gordan, see [**13**, theorem 2.6.3]. Our primary interest is in $\mathrm{GL}(2,\mathbb{F})$-module decompositions when $\mathbb{F}$ is finite. In the following theorem, V_m is the $\mathrm{GL}(2,\mathbb{F})$-module of homogeneous polynomials of degree m and $V_{\det}$ is the 1-dimensional $\mathrm{GL}(2,\mathbb{F})$-module on which $\mathrm{GL}(2,\mathbb{F})$ acts by the rule $vg = (\det g)v$ for all $v \in V_{\det}$ and $g \in \mathrm{GL}(2,\mathbb{F})$. For a G-module V, we let $S^2 V$ denote the symmetric square of V.

THEOREM 7.1. *Let $\mathbb{F}$ be a field of characteristic different from 2 and let $G = \mathrm{GL}(2,\mathbb{F})$. Then the following decompositions hold where the summands are irreducible $\mathbb{F}G$-modules.*

(a) *If $m + n < \mathrm{char}(\mathbb{F})$ or $\mathrm{char}(\mathbb{F}) = 0$, then*

$$V_m \otimes V_n \cong \bigoplus_{i=0}^{\min(m,n)} V_{\det}^{\otimes i} \otimes V_{m+n-2i}.$$

(b) *If $0 \leqslant 2m < \mathrm{char}(\mathbb{F})$ or $\mathrm{char}(\mathbb{F}) = 0$, then*

$$\wedge^2 V_m \cong \bigoplus_{\substack{i=1 \\ i \text{ odd}}}^{m} V_{\det}^{\otimes i} \otimes V_{2m-2i} \quad \text{and} \quad S^2 V_m \cong \bigoplus_{\substack{i=0 \\ i \text{ even}}}^{m} V_{\det}^{\otimes i} \otimes V_{2m-2i}.$$

Proof. (a) Assume, without loss of generality, that $m \leqslant n$. We prove the result by induction on m. The case when $m = 0$ is clearly true. We view $\mathbb{F}[X_1, Y_1, X_2, Y_2]$ as an

$\mathbb{F}G$-module, by adapting the action (7.1) separately for the indeterminates $X_1,\ Y_1$ and for $X_2,\ Y_2$. Let $V_m(X_1, Y_1)$ be the submodule of $\mathbb{F}[X_1, Y_1]$ comprising the degree m homogeneous polynomials, and define $V_n(X_2, Y_2) \leqslant \mathbb{F}[X_2, Y_2]$ similarly. The product set

$$V_{m,n} := V_m(X_1, Y_1)V_n(X_2, Y_2)$$

is an $\mathbb{F}G$-module. Further, $V_m(X_1, Y_1) \cong V_m$ and $V_n(X_2, Y_2) \cong V_n$. The multiplication map $\psi\colon V_m(X_1, Y_1) \otimes V_n(X_2, Y_2) \to V_{m,n}$ defined by

$$(f(X_1, Y_1) \otimes g(X_2, Y_2))\psi = f(X_1, Y_1)g(X_2, Y_2)$$

is a well-defined surjective $\mathbb{F}G$-module homomorphism as an easy calculation shows that

$$((f \otimes g)A)\psi = (f \otimes g)\psi A \quad \text{for all } A \in \mathrm{GL}(2, \mathbb{F}).$$

Comparing dimensions shows that ψ is an $\mathbb{F}G$-isomorphism, and $V_m \otimes V_n \cong V_{m,n}$.

We now show $V_{m,n}$ and $V_{m-1,n-1} \oplus V_{m+n}$ are isomorphic $\mathbb{F}G$-modules. Towards this end we will define an epimorphism π and a monomorphism δ.

Every element of $V_{m,n}$ has the form $\sum_{i=0}^{m}\sum_{j=0}^{n} \lambda_{ij}X_1^iY_1^{m-i}X_2^jY_2^{n-j}$ where $\lambda_{ij} \in \mathbb{F}$. The evaluation homomorphism $X_2 \mapsto X_1,\ Y_2 \mapsto Y_1$ gives rise to the following map

$$\pi\colon V_{m,n} \to V_{m+n}(X_1, Y_1)\colon X_1^iY_1^{m-i}X_2^jY_2^{n-j} \mapsto X_1^{i+j}Y_1^{m+n-i-j}. \tag{7.2}$$

It is straightforward to see that π is an $\mathbb{F}G$-epimorphism. We now show that the $\mathbb{F}G$-submodule $W := (X_1^mX_2^n)\mathbb{F}G$ of $V_{m,n}$ generated by $X_1^mX_2^n$ is isomorphic to V_{m+n}. If $m + n < \mathrm{char}(\mathbb{F})$ or $\mathrm{char}(\mathbb{F}) = 0$, then V_{m+n} is an irreducible $\mathbb{F}G$-module. Since $W\pi$ is a non-zero submodule of V_{m+n}, we have $W\pi = V_{m+n}$ and $\dim(W) \geqslant m + n + 1$. Conversely, suppose $g = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}(2, \mathbb{F})$. The Binomial Theorem gives

$$\begin{aligned}(X_1^mX_2^n)g &= (aX_1 + bY_1)^m(aX_2 + bY_2)^n \\ &= \sum_{i=0}^{m}\binom{m}{i}(aX_1)^i(bY_1)^{m-i}\sum_{j=0}^{n}\binom{n}{j}(aX_2)^j(bY_2)^{n-j}.\end{aligned}$$

Collecting terms involving a^kb^{m+n-k}, where $k = i + j$, gives

$$(X_1^mX_2^n)g = \sum_{k=0}^{m+n} a^kb^{m+n-k}h_k$$

where h_k is the polynomial $\sum_{i+j=k}\binom{m}{i}\binom{n}{j}X_1^iY_1^{m-i}X_2^jY_2^{n-j}$. This shows that W is spanned by $h_0, h_1, \ldots, h_{m+n}$. Therefore, $\dim(W) \leqslant m + n + 1$. Hence $\dim(W) = m + n + 1$, and π restricted to W gives an $\mathbb{F}G$-isomorphism $W \to V_{m+n}$.

Note that $\mathbb{F}[X_1, Y_1, X_2, Y_2]$ is an integral domain, and multiplying by a non-zero element in an integral domain is an injective map. Multiplying by $r := X_1Y_2 - Y_1X_2$

gives the map

$$\delta\colon V_{\det}\otimes V_{m-1,n-1}\to V_{m,n},\quad 1\otimes h(X_1,Y_1,X_2,Y_2)\mapsto r\cdot h(X_1,Y_1,X_2,Y_2). \tag{7.3}$$

Observe first that rA equals

$$\begin{aligned}&(a_{11}X_1+a_{12}Y_1)(a_{21}X_2+a_{22}Y_2)\\&\quad-(a_{21}X_1+a_{22}Y_1)(a_{11}X_2+a_{12}Y_2)=(\det A)r\end{aligned} \tag{7.4}$$

where $A=\begin{pmatrix}a_{11}&a_{12}\\a_{21}&a_{22}\end{pmatrix}$. It follows from (7.4) that $rA=\det(A)r$ for $A\in\mathrm{GL}(2,\mathbb{F})$, and hence $\langle r\rangle=V_{\det}$. Let $h=h(X_1,Y_1,X_2,Y_2)\in V_{m-1,n-1}$. We show that δ is an $\mathbb{F}G$-homomorphism:

$$\begin{aligned}&((1\otimes h)A)\delta=(\det(A)(hA))\delta=\det(A)(hA)r\quad\text{and}\\&((1\otimes h)\delta)A=(hr)A=(hA)\det(A)r.\end{aligned}$$

The subspaces $\mathrm{im}\delta=(X_1Y_2-Y_1X_2)V_{m-1,n-1}$ and $W=(X_1^mX_2^n)\mathbb{F}G$ of $V_{m,n}$ intersect trivially. Thus $V_{m,n}$ has a submodule isomorphic to $(V_{\det}\otimes V_{m-1,n-1})\oplus V_{m+n}$. However,

$$\begin{aligned}\dim((V_{\det}\otimes V_{m-1,n-1})\oplus V_{m+n})&=mn+(m+n+1)\\&=(m+1)(n+1)=\dim V_{m,n},\end{aligned}$$

and this implies

$$(V_{\det}\otimes V_{m-1,n-1})\oplus V_{m+n}\cong V_{m,n}\cong V_m\otimes V_n.$$

The decomposition (a) now follows by induction on m. Observe that when $\mathrm{char}(\mathbb{F})=p$, then hypothesis $m+n<p$ clearly implies that $(m-1)+(n-1)<p$.

(b) Denote the symmetric and exterior squares of V_m by S^2V_m and $\wedge^2V_m$, respectively. Since $\mathrm{char}(\mathbb{F})\neq 2$ we have $V_m\otimes V_m=S^2V_m\oplus\wedge^2V_m$. Our proof uses induction on m. The formulas are true for $m=0$ because $\wedge^2V_0=0$ (here the sum is empty), and $S^2V_0=V_0$. Suppose $m=1$. A calculation similar to (7.4) shows that $(X\otimes Y-Y\otimes X)A=\det(A)(X\otimes Y-Y\otimes X)$, and hence

$$\wedge^2V_1=\langle X\wedge Y\rangle\cong V_{\det},\quad\text{and}\quad S^2V_1=\langle X\odot X,X\odot Y,Y\odot Y\rangle\cong V_2,$$

where $u\wedge v:=(u\otimes v-v\otimes u)/2$ and $u\odot v:=(u\otimes v+v\otimes u)/2$. Thus the stated decompositions of $\wedge^2V_m$ and S^2V_m are valid for $m=1$. Suppose now that $m\geqslant 2$.

Recall the definitions in part (a) of the monomorphism δ, and the epimorphism π. Let $f(X_1, Y_1) \in V_m(X_1, Y_1)$ and $g(X_2, Y_2) \in V_m(X_2, Y_2)$ be arbitrary. Then

$$V_{m,m} = V_m(X_1, Y_1)V_m(X_2, Y_2) \cong V_m \otimes V_m \cong \wedge^2 V_m \oplus S^2 V_m$$

where

$$\wedge^2 V_m = \langle f(X_1, Y_1)g(X_2, Y_2) - g(X_1, Y_1)f(X_2, Y_2)\rangle, \text{ and} \tag{7.5}$$

$$S^2 V_m = \langle f(X_1, Y_1)g(X_2, Y_2) + g(X_1, Y_1)f(X_2, Y_2)\rangle. \tag{7.6}$$

The following calculation may be used to show that $(S^2 V_{m-1})\delta \leqslant \wedge^2 V_m$:

$$\begin{aligned}(X_1Y_2 - Y_1X_2)&(f(X_1, Y_1)g(X_2, Y_2) + g(X_1, Y_1)f(X_2, Y_2)) \\ &= f(X_1, Y_1)X_1 g(X_2, Y_2)Y_2 - g(X_1, Y_1)Y_1 f(X_2, Y_2)X_2 \\ &\quad - [f(X_1, Y_1)Y_1 g(X_2, Y_2)X_2 - g(X_1, Y_1)X_1 f(X_2, Y_2)Y_2].\end{aligned}$$

The left side lies in $(S^2 V_{m-1})\delta$ by (7.5), and the right side lies in $\wedge^2 V_m$ by (7.6). Thus $V_{\det} \otimes (S^2 V_{m-1}) \cong (S^2 V_{m-1})\delta \leqslant \wedge^2 V_m$. This containment, however, is an equality because

$$\begin{aligned}\dim(S^2 V_{m-1})\delta &= \dim(S^2 V_{m-1}) \\ &= \binom{\dim(V_{m-1}) + 1}{2} = \binom{m+1}{2} = \dim(\wedge^2 V_m).\end{aligned}$$

The inductive decomposition for $S^2 V_{m-1}$ and the isomorphism $V_{\det} \otimes (S^2 V_{m-1}) \cong \wedge^2 V_m$ together imply the desired decomposition for $\wedge^2 V_m$.

A similar argument using (7.5) and (7.6) shows that $(\wedge^2 V_{m-1})\delta \leqslant S^2 V_m$:

$$\begin{aligned}(X_1Y_2 - Y_1X_2)&(f(X_1, Y_1)g(X_2, Y_2) - g(X_1, Y_1)f(X_2, Y_2)) \\ &= f(X_1, Y_1)X_1 g(X_2, Y_2)Y_2 + g(X_1, Y_1)Y_1 f(X_2, Y_2)X_2 \\ &\quad - [f(X_1, Y_1)Y_1 g(X_2, Y_2)X_2 + g(X_1, Y_1)X_1 f(X_2, Y_2)Y_2].\end{aligned}$$

Thus $V_{\det} \otimes (\wedge^2 V_{m-1}) \cong (\wedge^2 V_{m-1})\delta \leqslant S^2 V_m$ is an $\mathbb{F}G$-submodule of $S^2 V_m$. By part (a), V_{2m} is an $\mathbb{F}G$-submodule of $V_m \otimes V_m$. Our hypotheses imply that V_{2m} is irreducible. Since $V_{2m} \not\leqslant \wedge^2 V_m$, we see that $V_{2m} \leqslant S^2 V_m$ and it intersects $(\wedge^2 V_{m-1})\delta \cong V_{\det} \otimes \wedge^2 V_{m-1}$ trivially. Therefore, $(V_{\det} \otimes \wedge^2 V_{m-1}) \oplus V_{2m} \leqslant S^2 V_m$. Comparing dimensions shows that $(V_{\det} \otimes \wedge^2 V_{m-1}) \oplus V_{2m} = S^2 V_m$. The inductive decomposition for $\wedge^2 V_{m-1}$ implies the desired decomposition for $S^2 V_m$. This proves part (b). □

When $\mathrm{char}(\mathbb{F}) = p$, the hypothesis $m + n < p$ in theorem 7.1(a) is necessary essentially because $\langle X^p, Y^p\rangle$ is a proper submodule of the homogeneous polynomials of degree p. Nevertheless, it is possible to relax the hypothesis $m + n < p$ when the number of carries when adding m to n in base-p is zero.

COROLLARY 7.2. *Suppose $\mathbb{F}_q$ has characteristic p where $q = p^e$. Let m, n be integers with $0 \leqslant m, n < q$ and with p-adic expansions $m = \sum_{j \geqslant 0} m_i p^j$ and $n = \sum_{j \geqslant 0} n_i p^j$.*

If $m_j + n_j < p$ for each $j \geqslant 0$, then the following $\mathrm{GL}(2, \mathbb{F}_q)$*-decomposition holds where the modules are twisted by powers of the automorphism $\lambda^\phi = \lambda^p$, as per* [**10**, definition VII.1.13]*:*

$$V_m \otimes V_n = \bigotimes_{j \geqslant 0} \bigoplus_{i=0}^{\min(m_j, n_j)} (V_{\det}^{\otimes i} \otimes V_{m_j + n_j - 2i})^{\phi^j}.$$

Proof. This follows from $V_m \otimes V_n = \bigotimes_{j \geqslant 0} V_{m_j}^{\phi^j} \otimes \bigotimes_{j \geqslant 0} V_{n_j}^{\phi^j} = \bigotimes_{j \geqslant 0} (V_{m_j} \otimes V_{n_j})^{\phi^j}$, and theorem 7.1(a). □

8. Simple IAC algebras associated to $\mathrm{SL}(2, \mathbb{F})$

Since V_0 is a trivial $\mathrm{SL}(2, \mathbb{F})$-module, theorem 7.1(b) may be used to determine when V_m is an ESQ-module. We need $2m - 2i = m$ to have a solution with i odd. Thus $i = m/2$ and $m \equiv 2 \pmod 4$.

THEOREM 8.1. *Let V_m be the above* $\mathrm{SL}(2, \mathbb{F})$*-module where $m \equiv 2 \pmod 4$ and where the field $\mathbb{F}$ satisfies* $\mathrm{char}(\mathbb{F}) = 0$ *or* $2m < \mathrm{char}(\mathbb{F})$*. Then V_m is an absolutely irreducible ESQ-module. Further, if $|\mathbb{F}| \geqslant 5$, the corresponding IAC algebra L is simple.*

Proof. We know that V_m is an absolutely irreducible $\mathrm{SL}(2, \mathbb{F})$-module both when $\mathrm{char}(\mathbb{F})$ is zero or prime, c.f. [**1**, theorem 5.2.3], [**13**, theorem 2.6.3] and [**18**, pp. 57–59]. The preamble to this theorem showed that V_m is a quotient of $\wedge^2 V_m$. Thus we may turn $L = V_m$ into an anti-commutative algebra satisfying $[\![L, L]\!] = L$, as in § 1. Since $\mathrm{SL}(2, \mathbb{F})$ acts irreducibly on $L = V_m$, we see that L is an IAC algebra.

It remains to prove that L is a simple IAC algebra. By theorem 4.2(b), $L = I_1 \oplus \cdots \oplus I_\ell$ where $I_1, \ldots, I_\ell$ are the minimal ideals of L and $\ell \geqslant 1$. The group $\mathrm{SL}(2, \mathbb{F})$ permutes the set $X = \{I_1, \ldots, I_\ell\}$ transitively. Since $Z = \mathsf{Z}(\mathrm{SL}(2, \mathbb{F}))$ acts as the identity on this set, the projective linear group $\mathrm{PSL}(2, \mathbb{F})$ acts on X. Further, $L \cong I_1^{\oplus \ell}$ where I_1 is a simple IAC algebra, and so $\dim I_1 \geqslant 3$, which implies that $\ell = \dim(V_m)/\dim(I_1) \leqslant (m+1)/3$.

It is well-known that $\mathrm{PSL}(2, \mathbb{F})$ is a simple group for $|\mathbb{F}| \geqslant 5$. Suppose $\ell > 1$. The homomorphism $\mathrm{PSL}(2, \mathbb{F}) \to \mathsf{S}_\ell$ is faithful, and the image is transitive on ℓ points. This is impossible if $\mathbb{F}$ is infinite, as S_ℓ is finite and $\mathrm{PSL}(2, \mathbb{F})$ is not. Thus $|\mathbb{F}| = q$ is finite. Set $p = \mathrm{char}(\mathbb{F})$. The minimal degree d of a transitive permutation representation of $\mathrm{PSL}(2, \mathbb{F}_q)$ is $q + 1$ except for $q = 5, 7, 9, 11$ in these cases $d = 5, 7, 6, 11$, respectively [**11**, Table 5.2.A, p. 175]. In all the cases we have $2q/3 \leqslant d$. Our hypothesis $2m < p$ implies

$$\frac{2p}{3} \leqslant \frac{2q}{3} \leqslant d \leqslant \ell \leqslant \frac{m+1}{3} < \frac{p/2+1}{3}.$$

This is false for all primes p, so we conclude that $\ell = 1$, and L is simple. □

REMARK 8.2. Theorem 8.1 can be generalized to include ESQ H-modules where $\mathrm{SL}(2,\mathbb{F}_q) < H \leqslant \mathrm{GL}(2,\mathbb{F}_q)$. For example, if $m \equiv 2 \pmod 4$ and $i = m/2$ is a multiple of $|H : \mathrm{SL}(2,\mathbb{F}_q)|$, then $V_{\det}^{\otimes i}$ is a trivial H-module and $L = V_m$ can be turned into an IAC algebra with $H \leqslant \mathrm{Aut}(L)$.

Combining the special case of $\mathbb{F} = \mathbb{F}_p$ in theorem 8.1 with the bijection in theorem 3.5 gives the following corollary stating the existence of another infinite family of UCS p-groups of exponent p^2.

COROLLARY 8.3. *Let $p \geqslant 3$ be a prime, and let m be a natural number such that $2m < p$. Then there exists an $(m+1)$-generator UCS p-group G with exponent p^2 such that the subgroup induced by $\mathrm{Aut}(G)$ on $\overline{G}$ contains $\mathrm{SL}(2,p)$ acting in its absolutely irreducible representation of dimension $m+1$ over the field $\mathbb{F}_p$. Further, G cannot be written as a direct product $(G_0)^{\times k}$ where G_0 is a smaller UCS p-group.*

Acknowledgements

The first author gratefully acknowledges the support of the Australian Research Council Discovery Grant DP160102323. The third author thanks CNPq for Bolsa de Produtividade em Pesquisa Project 308773/2016-0, and Universal Project 475399/2013-7, as well as acknowledging the hospitality and financial support of the Centre for the Mathematics of Symmetry and Computation (CMSC) of UWA during visits in 2014 and 2017. The second author is grateful to Fapemig for a PhD scholarship and financially supporting his visit to the CMSC. We thank the referee for helpful suggestions.

References

1 J. N. Bray, D. F. Holt and C. M. Roney-Dougal. *The maximal subgroups of the low-dimensional finite classical groups*, London Mathematical Society Lecture Note Series, vol. 407 (Cambridge: Cambridge University Press, 2013).

2 M. Bremner and I. Hentzel. Invariant nonassociative algebra structures on irreducible representations of simple Lie algebras. *Experiment. Math.* **13** (2004), 231–256.

3 M. R. Bremner and A. Douglas. The simple non-Lie Malcev algebra as a Lie-Yamaguti algebra. *J. Algebra* **358** (2012), 269–291.

4 P. A. Brooksbank and J. B. Wilson. Computing isometry groups of Hermitian maps. *Trans. Amer. Math. Soc.* **364** (2012), 1975–1996.

5 P. A. Brooksbank, J. Maglione and J. B. Wilson. A fast isomorphism test for groups whose Lie algebra has genus 2. *J. Algebra* **473** (2017), 545–590.

6 B. Eick, C. R. Leedham-Green and E. A. O'Brien. Constructing automorphism groups of p-groups. *Comm. Algebra* **30** (2002), 2271–2295.

7 S. P. Glasby, P. P. Pálfy and C. Schneider. p-groups with a unique proper non-trivial characteristic subgroup. *J. Algebra* **348** (2011), 85–109.

8 G. Hiss. Die adjungierten Darstellungen der Chevalley-Gruppen. *Arch. Math. (Basel)* **42** (1984), 408–416 (German).

9 D. F. Holt, B. Eick and E. A. O'Brien. *Handbook of computational group theory*. Discrete Mathematics and its Applications (Boca Raton) (Boca Raton, FL: Chapman & Hall/CRC, 2005).

10 B. Huppert and N. Blackburn. *Finite groups. II*, Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences], vol. 242 (Berlin-New York: Springer-Verlag, 1982), AMD, 44.

11 P. Kleidman and M. Liebeck. *The subgroup structure of the finite classical groups*, London Mathematical Society Lecture Note Series, vol. 129 (Cambridge: Cambridge University Press, 1990).
12 P. B. Kleidman, U. Meierfrankenfeld and A. J. E. Ryba. HS $< E_7(5)$. *J. London Math. Soc. (2)* **60** (1999), 95–107.
13 E. Kowalski. An introduction to the representation theory of groups, Graduate Studies in Mathematics, vol. 155 (Providence, RI: American Mathematical Society, 2014).
14 E. N. Kuzmin. Structure and representations of finite dimensional Malcev algebras. *Quasigroups Related Systems* **22** (2014), 97–132.
15 A. Lubotzky and A. Mann. Powerful p-groups. I. Finite groups. *J. Algebra* **105** (1987), 484–505.
16 D. A. Suprunenko. *Matrix groups*. Translated from the Russian; Translation edited by K. A. Hirsch; Translations of Mathematical Monographs, vol. 45 (Providence, R.I.: American Mathematical Soc., 1976).
17 D. R. Taunt. Finite groups having unique proper characteristic subgroups. I. *Proc. Cambridge Philos. Soc.* **51** (1955), 25–36.
18 C. B. Thomas. Representations of finite and Lie groups (London: Imperial College Press, 2004).
19 J. B. Wilson. More characteristic subgroups, Lie rings, and isomorphism tests for p-groups. *J. Group Theory* **16** (2013), 875–897.
20 J. B. Wilson. On automorphisms of groups, rings, and algebras. *Comm. Algebra* **45** (2017), 1452–1478.
21 R. A. Wilson. *The finite simple groups*, volume 251 of Graduate Texts in Mathematics (London: Springer-Verlag London, Ltd., 2009).