2014

Groups Acting on Tensor Products

Peter A. Brooksbank
pbrooksb@bucknell.edu

Groups acting on tensor products

Peter A. Brooksbank [a,1], James B. Wilson [b,*]

[a] Department of Mathematics, Bucknell University, Lewisburg, PA 17837, United States
[b] Department of Mathematics, Colorado State University, Fort Collins, CO 80523, United States

A B S T R A C T

Groups preserving a distributive product are encountered often in algebra. Examples include automorphism groups of associative and nonassociative rings, classical groups, and automorphism groups of p-groups. While the great variety of such products precludes any realistic hope of describing the general structure of the groups that preserve them, it is reasonable to expect that insight may be gained from an examination of the universal distributive products: tensor products. We give a detailed description of the groups preserving tensor products over semisimple and semiprimary rings, and present effective algorithms to construct generators for these groups. We also discuss applications of our methods to algorithmic problems for which all currently known methods require an exponential amount of work.

© 2013 Elsevier B.V. All rights reserved.

1. Introduction

Many groups can be described as the set of linear transformations that preserve a distributive product. Obviously this is the case for automorphism groups of algebras, both associative and nonassociative. Among the other well known examples are classical groups, which preserve other forms of distributive products, namely reflexive forms; cf. [1, p. 107]. In more subtle ways, automorphisms of finite p-groups preserve a distributive product that arises from commutation, via the correspondences of Baer [2], and of Kaloujnine, Lazard, and Mal'cev [23]. As the estimates for rings [19], and for p-groups [11], suggest, however, there are simply too many products to have any realistic expectation of understanding the structure of all such groups.

The goal of this paper is to examine the groups preserving tensor products. As tensor products are universal products, the structure of these groups informs us of overall structure of groups preserving distributive products. Tensor products over central simple rings have already been studied in [17, Theorems 3.6 & 4.1]. Here we consider tensor products over semiprimary rings (rings R whose Jacobson radical $J(R)$ is nilpotent and whose quotient $R/J(R)$ is semisimple). This case is surprisingly complicated because of the presence of a nontrivial Jacobson radical.

We begin with a general distributive product $\circ : U \times V \to W$ between abelian groups U, V, and W, also known as a biadditive or bilinear map, or just *bimap*. For simplicity we assume that bimaps are *full* in that $W = U \circ V = \langle u \circ v : u \in U, v \in V \rangle$. An *autotopism* of a bimap $\circ$ is a triple $(f, g; h)$ in $\mathrm{Aut}(U) \times \mathrm{Aut}(V) \times \mathrm{Aut}(W)$ satisfying

$$(\forall u \in U, \forall v \in V) \qquad uf \circ gv = (u \circ v)^h. \tag{1.1}$$

Our notation accommodates the introduction of left and right scalars, so our homomorphisms are evaluated on the right (resp. left) for left modules (resp. right modules), and exponentially for bimodules.

We are principally interested in describing Aut($\circ$), the group of all autotopisms of a bimap $\circ$. Our approach relies on the *ring of adjoints* of $\circ$, defined as

$$\mathrm{Adj}(\circ) = \{(f, g) \in \mathrm{End}(U) \times \mathrm{End}(V)^{\mathrm{op}} : uf \circ v = u \circ gv\}. \tag{1.2}$$

This ring was introduced in [24, p. 2654] and is characterized as the largest ring R acting faithfully on U and V for which $\circ\colon U \times V \to W$ factors through $U \otimes_R V$. We show that tensor products and adjoint rings are Galois connected (Theorem 2.11), and use this connection to prove the following result.

Theorem 1.3. *The autotopism group of a bimap $\circ\colon U \times V \to W$ embeds in*

$$N(\mathrm{Adj}(\circ)) = \{(f, g) \in \mathrm{Aut}(U) \times \mathrm{Aut}(V) : \mathrm{Adj}(\circ)^{(f,g)} = \mathrm{Adj}(\circ)\},$$

with equality precisely when $\circ$ is a tensor product. In turn, the bimap $\circ$ is a tensor product if, and only if, the uniquely defined linear map $U \otimes_{\mathrm{Adj}(\circ)} V \to W$ is an isomorphism.

In several applications, such as constructing automorphism groups of finite p-groups, the bimaps $\circ$ that arise have $U = V$ and are endowed with natural symmetry. In those settings, one is primarily interested in special types of autotopisms called *pseudo-isometries*; see [24, p. 2650]. We therefore consider alternating and symmetric bimaps $\circ$, and study the group of all pseudo-isometries of $\circ$, namely

$$\Psi\mathrm{Isom}(\circ) = \{f\colon (f, g; h) \in \mathrm{Aut}(\circ) \text{ and } f = g\}. \tag{1.4}$$

We prove the following result.

Theorem 1.5. *For an arbitrary nondegenerate alternating or symmetric bimap $\circ\colon V \times V \to W$, the group $\Psi\mathrm{Isom}(\circ)$ embeds naturally in*

$$N^*(\mathrm{Adj}(\circ)) = \{f\colon (f, g) \in N(\mathrm{Adj}(\circ)) \text{ and } f = g\},$$

with equality precisely when $\circ$ is a symmetric or exterior tensor product. Again, the bimap $\circ$ is a tensor product if, and only if, the linear map $V \wedge^{\pm}_{\mathrm{Adj}(\circ)} V \to W$ is an isomorphism.

From our point of view, the crucial aspect of Theorems 1.3 and 1.5 is that Aut($\circ$) and $\Psi\mathrm{Isom}(\circ)$ are shown to act on a known associative, unital ring, which is easy to construct algorithmically [4, Section 4], [5]. So much more is known about the structure of rings than of general distributive products, and even basic features, such as the Jacobson radical and simple factors of Adj($\circ$), clarify the structure of Aut($\circ$). Indeed, Theorems 3.10 and 4.5 give detailed structural descriptions of the groups $N(\mathrm{Adj}(\circ))$ and $N^*(\mathrm{Adj}(\circ))$ in the case when Adj($\circ$) is semiprimary and separable (which holds, for example, whenever U and V are finite-dimensional vector spaces over a field). These structural details are often sufficient to compute generators for autotopism groups efficiently (say in polynomial time), as was observed in [17, Theorem 1.3] for central simple rings.

The paper is organized as follows. In Section 2 we develop the necessary background on bimaps, culminating with our Galois connection between bimaps on $U \times V$ and subsets of $\mathrm{End}(U) \times \mathrm{End}(V)^{\mathrm{op}}$ (Theorem 2.11).

In Section 3 we study the autotopism group of an arbitrary bimap, proving Theorem 1.3, and giving a precise structure theorem for $N(\mathrm{Adj}(\circ))$ in the case when Adj($\circ$) is semiprimary and separable (Theorem 3.10). We also describe an algorithm to construct generators for the normalizer of a finite-dimensional matrix algebra, and hence for the autotopism group of a tensor product.

In Section 4, we consider the special case when $\circ$ is symmetric or alternating. We prove Theorem 1.5 and provide an analogue of Theorem 3.10 for rings with involutions (Theorem 4.5).

In the concluding section, we expand on the key applications of our results and algorithms to the problem of computing automorphism groups of finite p-groups, and briefly discuss ongoing work in this area.

2. Homotopisms, isotopisms and pseudo-isometries of bimaps

Our use of rings and modules is standard. A *bi-additive map* (or just *bimap*) is a function $\circ\colon U \times V \to W$, where U, V, W are abelian groups, satisfying the two-sided distributive law

$$\begin{aligned}
(\forall u_1, u_2 \in U, \forall v \in V) \qquad & (u_1 + u_2) \circ v = u_1 \circ v + u_2 \circ v \\
(\forall u \in U, \forall v_1, v_2 \in V) \qquad & u \circ (v_1 + v_2) = u \circ v_1 + u \circ v_2.
\end{aligned}$$

Recall that our bimaps are *full*, in that $W = U \circ V = \langle u \circ v : u \in U, v \in V\rangle$.

Let $\circ\colon U \times V \to W$ and $\diamond\colon U' \times V' \to W'$ be bimaps. A *homotopism* from $\circ$ to $\diamond$ is a triple $(f\colon U \to U', g\colon V \to V'; h\colon W \to W')$ of homomorphisms satisfying

$$(\forall u \in U, \forall v \in V) \qquad (u \circ v)^h = uf \diamond gv. \tag{2.1}$$

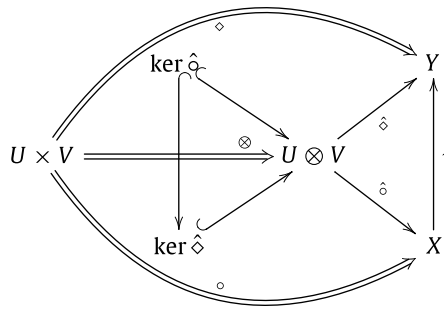Denote by $\mathrm{hom}(\circ, \diamond)$ the set of all homotopisms from $\circ$ to $\diamond$.

Fig. 1. Commutative diagram demonstrating how the bimap $\diamond$ factors through $\circ$ if, and only if, their factorizations through the tensor product have nested kernels. *Double shafted arrows denote bimaps and regular arrows are homomorphisms.*

Remark 2.2. For a product $\circ : U \times V \to W$ to determine a nonassociative ring requires that $U = V = W$. This can result in products that are not full, such as the multiplication of any nilpotent Lie algebra. The restriction to full bimaps can be avoided by considering "weak" homotopisms, which are triples $(f, g; h)$ where h is defined from $U \circ V \to U' \diamond V'$ instead of from $W \to W'$.

The class of bimaps together with homotopisms forms a category, called the *homotopism category*. There are various natural morphisms on classes of bimaps, such as adjoint-morphisms [25], so we name the categories after the morphisms rather than the objects. We are interested primarily in *isotopisms*, namely homotopisms whose constituent maps are all isomorphisms. Define the *autotopism group* of a bimap $\circ : U \times V \to W$ to be

$$\mathrm{Aut}(\circ) = \hom(\circ, \circ) \cap (\mathrm{Aut}(U) \times \mathrm{Aut}(V) \times \mathrm{Aut}(W)). \tag{2.3}$$

We denote the elements of $\mathrm{Aut}(\circ)$ as triples $(f, g; h)$, separating h from f and g to distinguish between two natural $\mathrm{Aut}(\circ)$-modules, namely $U \times V$ and W. As $\circ$ is full, h is determined by $(u \circ v)^h = uf \circ vg$, so the action of $\mathrm{Aut}(\circ)$ on $U \times V$ is faithful.

2.1. Factor equivalence

We now fix two abelian groups U and V and consider bimaps on $U \times V$. For a bimap $\circ : U \times V \to X$ and homomorphism $\tau : X \to Y$ we define the bimap $\circ^\tau : U \times V \to Y$ by

$$(\forall u \in U, \forall v \in V) \qquad u \circ^\tau v = (u \circ v)^\tau.$$

For bimaps $\circ : U \times V \to X$ and $\diamond : U \times V \to Y$, we say $\diamond$ *factors through* $\circ$, and write $\circ \to \diamond$, if there is a homomorphism $\tau : U \circ V \to Y$ such that $\circ^\tau = \diamond$ (equivalently, if $(1_U, 1_V; \tau)$ is a homotopism from $\circ$ to $\diamond$). We say that $\circ$ and $\diamond$ are *factor equivalent*, denoted $\circ \leftrightarrow \diamond$, if $\circ \to \diamond$ and $\diamond \to \circ$. Note that $\circ \leftrightarrow \diamond$ forces $X = U \circ V$ and $Y = U \diamond V$ to be isomorphic (as our bimaps are full). It follows that $\leftrightarrow$ is an equivalence relation on the class of bimaps on $U \times V$, and $\to$ is a partial order on the bimaps on $U \times V$ relative to the equivalence $\leftrightarrow$.

Let $U \otimes V$ denote the usual tensor product of U and V (as abelian groups) and let $\otimes : U \times V \to U \otimes V$ denote the associated bimap. The universal property of tensor products asserts that every bimap $\circ : U \times V \to X$ factors uniquely through $\otimes : U \times V \to U \otimes V$. Writing $\hat{\circ} : U \otimes V \to X$ for the implied homomorphism, so that $\circ = \otimes^{\hat{\circ}}$, we have $u \circ v = (u \otimes v)^{\hat{\circ}}$ for all $u \in U$ and all $v \in V$. Hence, for a bimap $\diamond$ on $U \times V$,

$$\circ \to \diamond \quad \Longleftrightarrow \quad \ker \hat{\circ} \subseteq \ker \hat{\diamond}. \tag{2.4}$$

Fig. 1 illustrates this correspondence.

Associated to each subgroup K of $U \otimes V$ is a bimap

$$\bullet = \bullet(K) : U \times V \to (U \otimes V)/K,$$

defined by

$$(\forall u \in U, \forall v \in V) \qquad u \bullet v = u \otimes v + K. \tag{2.5}$$

Fig. 1 also shows that, for every bimap $\circ : U \times V \to X$, we have $\circ \leftrightarrow \bullet(\ker \hat{\circ})$. We regard $\bullet(\ker \hat{\circ})$ as the *regular representation* of $\circ$ since it is a canonical representative of the factor-equivalence class containing $\circ$. This establishes a bijection $\circ \mapsto \ker \hat{\circ}$ from the factor-equivalence classes on $U \times V$ to the set of subgroups of $U \otimes V$.

We now define meets and joins for bimaps on $U \times V$ in a manner that respects factor equivalence. For bimaps $\circ : U \times V \to X$ and $\diamond : U \times V \to Y$, let

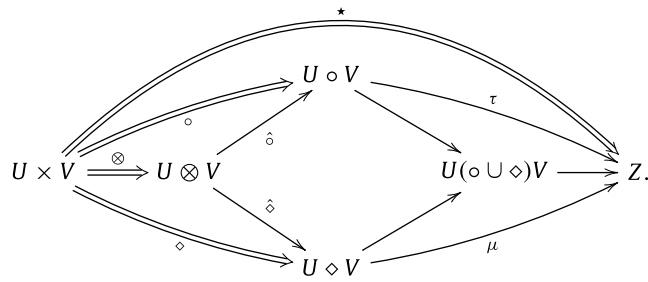$$W = \{(u \circ v, u \diamond v) : u \in U, v \in V\} \leqslant X \times Y,$$

Fig. 2. Commutative diagram showing that if $\circ \to \star$ and $\diamond \to \star$ then $(\circ \cup \diamond) \to \star$. The point is that the middle of the diagram is a pushout for $(\hat{\circ}, \hat{\diamond})$.

and define $(\circ \cap \diamond) \colon U \times V \to W$ by

$$(\forall u \in U, \forall v \in V) \qquad u(\circ \cap \diamond)v = (u \circ v, u \diamond v). \tag{2.6}$$

For the join $\circ \cup \diamond$, let $J = \langle (u \circ v, -u \diamond v) \colon u \in U, v \in V \rangle \leqslant X \times Y$. Now define $(\circ \cup \diamond) \colon U \times V \to W/J$ so that

$$(\forall u \in U, \forall v \in V) \qquad u(\circ \cup \diamond)v = (u \circ v, u \diamond v) + J. \tag{2.7}$$

Both $\cap$ and $\cup$ generalize to arbitrary sets of bimaps on $U \times V$.

Proposition 2.8. *The factor-equivalence classes of bimaps on $U \times V$ form a lattice under $\to$, $\cap$ and $\cup$ that is isomorphic to the lattice of subgroups of $U \otimes V$ under $\subseteq$, $\cap$, and $+$. A bimap $\circ$ is at the top if $U \circ V = 0$, and at the bottom if $\hat{\circ} \colon U \otimes V \to U \circ V$ is an isomorphism.*

Proof. Observe that $U(\circ \cup \diamond)V = ((U \circ V) \oplus (U \diamond V))/J$ is a pushout for the pair $(\hat{\circ}, \hat{\diamond})$ in the category of abelian groups. Furthermore, if $\star \colon U \times V \to Z$ is a bimap and $\circ, \diamond \to \star$, then the associated homomorphisms $U \circ V \to Z$ and $U \diamond V \to Z$ create a commutative square from $U \otimes V$ to Z (see Fig. 2). The universal property of the pushout implies that $\circ \cup \diamond \to \star$, and we see that $\cup$ is indeed a join. Fig. 2 also illustrates that $\circ \cup \diamond \leftrightarrow \bullet(\ker \hat{\circ} + \ker \hat{\diamond})$. In similar fashion, $\circ \cap \diamond \leftrightarrow \bullet(\ker \hat{\circ} \cap \ker \hat{\diamond})$ and serves as the meet. $\square$

Remark 2.9. The meet $\circ \cap \diamond$ of bimaps $\circ \colon U \times V \to Y$ and $\diamond \colon U \times V \to Y$ has appeared elsewhere as a bimap $U \times V \to X \oplus Y$, for example in [4, p. 1976]. We have modified our definition of $\circ \cap \diamond$ here to ensure that it is a full bimap.

2.2. A Galois connection

A *Galois connection* between partially ordered sets $(P, \leqslant)$ and $(Q, \subseteq)$ is a pair of functions $\perp \colon P \to Q$ and $\top \colon Q \to P$ such that

$$(\forall p \in P, \forall q \in Q) \qquad q^{\top} \leqslant p \iff q \subseteq p^{\perp}.$$

The reader is referred to [9] for equivalent definitions and interpretations of Galois connections. In this section we exhibit a Galois connection between the lattice of factor-equivalence classes of bimaps on $U \times V$ and the lattice of subsets of the ring $\mathrm{End}(U) \times \mathrm{End}(V)^{\mathrm{op}}$.

Recall that we regard U as a right $\mathrm{End}(U)$-module and a left $\mathrm{End}(U)^{\mathrm{op}}$-module. Thus, subsets S of $\mathrm{End}(U) \times \mathrm{End}(V)^{\mathrm{op}}$ act on the right of U and on the left of V so that one may form the tensor product $\otimes_S \colon U \times V \to U \otimes_S V$. We say that a bimap $\circ \colon U \times V \to W$ is *mid S-linear* if it factors through $\otimes_S$:

$$(\forall s \in S, \forall u \in U, \forall v \in V) \qquad us \circ v = u \circ sv. \tag{2.10}$$

For a fixed bimap $\circ \colon U \times V \to W$, recall from (1.2) that

$$\mathrm{Adj}(\circ) = \{(x, y) \in \mathrm{End}(U) \times \mathrm{End}(V)^{\mathrm{op}} \colon \forall u \in U, \forall v \in V, ux \circ v = u \circ yv\},$$

a subring of $\mathrm{End}(U) \times \mathrm{End}(V)^{\mathrm{op}}$. We can now formulate the Galois connection.

Theorem 2.11. *Let U and V be abelian groups. If $S \subseteq \mathrm{End}(U) \times \mathrm{End}(V)^{\mathrm{op}}$, and $\circ \colon U \times V \to W$ is a bimap, then*

$$\otimes_S \to \circ \quad \textit{if, and only if,} \quad S \subseteq \mathrm{Adj}(\circ).$$

This establishes a Galois connection between the lattice of factor-equivalence classes of bimaps on $U \times V$ and the lattice of subsets of $\text{End}(U) \times \text{End}(V)^{\text{op}}$. *Moreover,*

(i) $\text{Adj}(\otimes_{\text{Adj}(\circ)}) = \text{Adj}(\circ)$, *and*
(ii) $\otimes_{\text{Adj}(\otimes_S)} \leftrightarrow \otimes_S$.

Hence $\text{Adj}(\otimes_{-})$ *and* $\otimes_{\text{Adj}(-)}$ *are closure operators on the two lattices.*

Proof. First, if $\circ$ factors through $\otimes_S$ then there is a (unique) map $\hat{\circ} \colon U \otimes_S V \to W$ such that $u \circ v = (u \otimes v)^{\hat{\circ}}$ for all $u \in U$ and all $v \in V$. For each $s \in S$,

$$(\forall u \in U, \forall v \in V) \qquad us \circ v = (us \otimes v)^{\hat{\circ}} = (u \otimes sv)^{\hat{\circ}} = u \circ sv.$$

So $S \subseteq \text{Adj}(\circ)$. Conversely, suppose $S \subseteq \text{Adj}(\circ)$. Define $\tau \colon U \otimes_S V \to U \circ V$ on pure tensors, sending $u \otimes v \mapsto u \circ v$, and extending linearly. For each $s \in S$,

$$(\forall u \in U, \forall v \in V) \qquad (us \otimes v)^{\tau} = us \circ v = u \circ sv = (u \otimes sv)^{\tau}.$$

It follows that τ is well-defined, and hence that $\circ$ factors through $\otimes_S$.

Both (i) and (ii) are general properties of Galois connections, but their proof in context is straight-forward. For (i), we have $\text{Adj}(\circ) \subseteq \text{Adj}(\otimes_{\text{Adj}(\circ)})$. For the reverse inclusion, we know that $\otimes_{\text{Adj}(\circ)} \to \circ$, so there exists $\tau \colon U \otimes_{\text{Adj}(\circ)} V \to U \circ V$ such that $u \circ v = (u \otimes v)^{\tau}$ for all $u \in U, v \in V$. For each $s = (x, y) \in \text{Adj}(\otimes_{\text{Adj}(\circ)})$,

$$(\forall u \in U, \forall v \in V) \qquad us \circ v = (ux \otimes v)^{\tau} = (u \otimes yv)^{\tau} = u \circ sv,$$

so that $s \in \text{Adj}(\circ)$. Similarly for (ii), we have $\otimes_{\text{Adj}(\otimes_S)} \to \otimes_S$. Since $S \subseteq \text{Adj}(\otimes_S)$, the identity map on pure tensors extends linearly to a well-defined map $U \otimes_S V \to U \otimes_{\text{Adj}(\otimes_S)} V$. It follows that $\otimes_S \to \otimes_{\text{Adj}(\otimes_S)}$. $\square$

A consequence of Theorem 2.11 is that a bimap $\circ$ on $U \times V$ is a tensor product (i.e. it possesses the universal mapping property for some set $S \subseteq \text{End}(U) \times \text{End}(V)^{\text{op}}$) if, and only if, $\circ \leftrightarrow \otimes_{\text{Adj}(\circ)}$. This proves the last assertion of Theorem 1.3.

Note that if R is any ring, and $\cdot_R$ is its multiplication, mapping $R \times R \to R$, then $\text{Adj}(\cdot_R) = \{(u \mapsto ur, v \mapsto rv) : r \in R\} \cong R$. In that sense adjoint rings are arbitrary. Their representations, however, are more constrained, in the sense that a subring S of $\text{End}(U) \times \text{End}(V)^{\text{op}}$ seems rather unrelated to its closure, $\text{Adj}(\otimes_S)$. For instance, there are commutative subrings S of $\text{End}(U) \times \text{End}(V)^{\text{op}}$, having nontrivial Jacobson radical, for which $\text{Adj}(\otimes_S)$ is noncommutative and simple.

3. Autotopisms and normalizers

Having introduced the homotopism category of bimaps and some of its basic properties, we now consider the automorphism groups in the category.

In Section 3.1 we show, for an arbitrary bimap $\circ \colon U \times V \to W$, that the autotopism group $\text{Aut}(\circ)$ is naturally represented as a normalizer, $N(\text{Adj}(\circ))$, within $\text{Aut}(U) \times \text{Aut}(V)$, thereby completing the proof of Theorem 1.3. In Section 3.2, we describe $N(A)$ for semiprimary separable subrings A of $\text{End}(U) \times \text{End}(V)^{\text{op}}$, and hence also $\text{Aut}(\otimes_S)$ for $S \subseteq \text{End}(U) \times \text{End}(V)^{\text{op}}$ having $\text{Adj}(\otimes_S)$ semiprimary and separable. This includes the autotopisms of tensor products of finite-dimensional vector spaces. Finally, in Section 3.3, we present an algorithm to construct $N(A)$.

3.1. Autotopisms acting on adjoints

For abelian groups U, V, and subring A of $\text{End}(U) \times \text{End}(V)^{\text{op}}$, define the *normalizer* of A to be

$$\begin{aligned} N(A) &= \left\{ (f, g) \colon \forall (x, y) \in A, \ (x, y)^{(f, g)} = (f^{-1}xf, gyg^{-1}) \in A \right\} \\ &\subseteq \text{Aut}(U) \times \text{Aut}(V). \end{aligned} \tag{3.1}$$

Theorem 3.2. *Let U and V be abelian groups.*

(i) *If $\circ$ is a bimap on $U \times V$ then* $\text{Aut}(\circ)|_{\text{Aut}(U) \times \text{Aut}(V)} \subseteq N(\text{Adj}(\circ))$.
(ii) *If $S \subseteq \text{End}(U) \times \text{End}(V)^{\text{op}}$ then* $\text{Aut}(\otimes_S)|_{\text{Aut}(U) \times \text{Aut}(V)} = N(\text{Adj}(\otimes_S))$.

Proof. For (i), let $(f, g; h) \in \text{Aut}(\circ)$. For each $(x, y) \in \text{Adj}(\circ)$ and all $u \in U, v \in V$,

$$ux^f \circ v = (uf^{-1}x \circ g^{-1}v)^h = (uf^{-1} \circ yg^{-1}v)^h = u \circ y^g v.$$

Therefore, $(x, y)^{(f, g)} \in \text{Adj}(\circ)$, so that $\text{Aut}(\circ)|_{\text{Aut}(U) \times \text{Aut}(V)}$ normalizes $\text{Adj}(\circ)$.

For (ii) we require the reverse containment in the case that $\circ \leftrightarrow \otimes_S = \otimes_{\text{Adj}(\otimes_S)}$ for some $S \subseteq \text{End}(U) \times \text{End}(V)^{\text{op}}$. Suppose that $(f, g) \in N(\text{Adj}(\otimes_S))$. We construct $h \in \text{Aut}(U \otimes_S V)$ such that $(f, g; h) \in \text{Aut}(\otimes_S)$. If such h exists, it is uniquely defined

by $(u \otimes v)^h = uf \otimes gv$, for each $u \in U$ and each $v \in V$. Accordingly h exists if this definition is well-defined (respects the tensor product relations). For all $u, u' \in U$ and all $v, v' \in V$,

$$((u + u') \otimes v)^h = uf \otimes gv + u'f \otimes gv = (u \otimes v)^h + (u' \otimes v)^h, \text{ and}$$

$$(u \otimes (v + v'))^h = uf \otimes gv + uf \otimes gv' = (u \otimes v)^h + (u \otimes v')^h.$$

Finally, let $s = (x, y) \in S \subseteq \mathrm{Adj}(\otimes_S)$. As $(f, g) \in N(\mathrm{Adj}(\otimes_S))$, it follows that $(x^f, y^g) \in \mathrm{Adj}(\otimes_S)$. Now, for each $u \in U$ and each $v \in V$,

$$(us \otimes v)^h = uxf \otimes gv = ufx^f \otimes gv = uf \otimes y^g gv = uf \otimes gyv = (u \otimes sv)^h.$$

Therefore h is well-defined on $U \otimes_S V$, so that $(f, g; h) \in \mathrm{Aut}(\otimes_S)$. As $\circ \leftrightarrow \otimes_S$, $\mathrm{Aut}(\otimes_S)|_{\mathrm{Aut}(U) \times \mathrm{Aut}(V)} = \mathrm{Aut}(\circ)|_{\mathrm{Aut}(U) \times \mathrm{Aut}(V)}$, which completes the proof. $\square$

Proof of Theorem 1.3. Recall from Section 2 that for a full bimap $\circ$, each autotopism $(f, g; h)$ has h determined by (f, g) and so $\mathrm{Aut}(\circ)$ is faithfully represented on $U \times V$. Thus, the first assertion of Theorem 1.3 follows immediately from Theorem 3.2(i). As commented earlier, the second assertion follows from the Galois connection; specifically, from Theorem 2.11(i). $\square$

3.2. Normalizers of matrix rings

Theorem 3.2 states that the groups $\mathrm{Aut}(\circ)$ act as automorphisms of the rings $\mathrm{Adj}(\circ)$. We can use the well-developed structure of rings to limit the behavior of $\mathrm{Aut}(\circ)$.

In this section we pursue a more precise description of $N(\mathrm{Adj}(\circ))$ for k-bilinear maps $U \times V \to W$, where k is a field, and U, V and W are finite-dimensional k-vector spaces. The proof actually applies to any adjoint ring which is separable and semiprimary. Since we are unable at present to describe which subrings of $\mathrm{End}(U) \times \mathrm{End}(V)^{\mathrm{op}}$ are adjoint rings we assume anything is possible. The resulting structure theorem (Theorem 3.10) is technical, but each component is implied by well-known properties of rings. We need this level of detail for timing estimates of various algorithms, such as those in Section 3.3 and [6]. The ring-theoretic properties we use are found in [8, Sections 3, 5, 6].

Before stating the main structure theorem, we set up some notation and establish some preliminary results. Fix a field k, finite-dimensional k-spaces U, V, and let A be a k-subalgebra of $\mathrm{End}_k(U) \times \mathrm{End}_k(V)^{\mathrm{op}}$. Let $J = J(A)$ be the Jacobson radical of A. Define the *radical series* of A to be the finite module chain

$$U \oplus V > UJ \oplus JV > \cdots > UJ^c \oplus J^c V > UJ^{c+1} \oplus J^{c+1}V = 0. \tag{3.3}$$

As each ideal J^i is characteristic in A, the radical series is $N(A)$-invariant. For convenience we let $J^0 = A$. The main theme is to choose bases for U and V such that A is block upper triangular, and such that the action of $N(A)$ on A permutes the blocks within each radical section but otherwise respects the block decomposition. We choose these bases with some additional properties in mind.

First, Wedderburn's principal theorem [16, p. 374] establishes the existence of a subalgebra $S \leqslant A$ such that $A = J \oplus S$ as a k-vector space. As S is semisimple, so UJ^i splits in U as an S-module for each $i \in \{0, \ldots, c\}$; likewise $J^i V$ splits in V. Hence, there are S-submodules $X_0, \ldots, X_c \leqslant U$ and $Y_0, \ldots, Y_c \leqslant V$ such that for all $0 \leqslant i \leqslant c$,

$$UJ^i = X_i \oplus \cdots \oplus X_c \qquad J^i V = Y_i \oplus \cdots \oplus Y_c. \tag{3.4}$$

For each $i \in \{0, \ldots, c\}$, J is in the kernel of the induced action of A on UJ^i/UJ^{i+1} and $J^i V/J^{i+1}V$, so these modules are (A/J)-modules, and hence semisimple. As S splits with J in A, so $UJ^i/UJ^{i+1} \cong X_i$ as S-modules. Therefore, bases for U and V that exhibit the decompositions $U = X_0 \oplus \cdots \oplus X_c$ and $V = Y_0 \oplus \cdots \oplus Y_c$ will express A in block upper triangular form with S represented as block-diagonal matrices.

It is convenient to state our main structure theorem with reference to the group

$$N(S; J) = \mathrm{Stab}_{N(S)}(\{(UJ^i, J^i V) : 0 \leqslant i \leqslant c\}). \tag{3.5}$$

Our preliminary results describe some structural properties of this group. Let $\mathcal{E}$ be the set of central-primitive idempotents of S [8, Section 3]. Then the minimal ideals of S are precisely the ideals $I = eSe = Se$, where $e \in \mathcal{E}$. Next, we define an equivalence relation $\sim$ on $\mathcal{E}$, where

$$e \sim e' \iff \begin{array}{l} eSe \cong e'Se' \text{ as rings, and for all } i \in \{0, \ldots, c\}, \\ \dim X_i e = \dim X_i e' \text{ and } \dim eY_i = \dim e'Y_i. \end{array} \tag{3.6}$$

With this notation, we have the following result.

Lemma 3.7. *Let S be a semisimple complement to the Jacobson radical, J, of a subalgebra of $\mathrm{End}_k(U) \times \mathrm{End}_k(V)^{\mathrm{op}}$, and let $\mathcal{E}$ be the set of central-primitive idempotents of S. Then, for each $e \in \mathcal{E}$, the following hold.*

(i) *For $i \in \{0, \ldots, c\}$, $X_i e$ is a direct sum of isomorphic simple S-submodules of X_i, and eY_i is a direct sum of isomorphic simple S-submodules of Y_i.*

(ii) *For $e' \in \mathcal{E}$, $e \sim e'$ if, and only if, there exists $g \in N(S; J)$ with $e^g = e'$ such that g acts as the identity on $\mathcal{E} - \{e, e'\}$.*

Proof. For each $e \in \mathcal{E}$, $X_i e$ is a faithful eSe-module and, as e is central-primitive, eSe is simple. Therefore, each $X_i e$ is a direct sum of isomorphic simple eSe-modules and every S-submodule of X_i that is isomorphic to a submodule of $X_i e$ is contained in $X_i e$; see [8, Section 3].

Now suppose $e' \in \mathcal{E} - \{e\}$. If $e \sim e'$, then $eSe \cong e'Se'$ and both are simple Artinian rings. As such, each is isomorphic to $M_{d_e}(\Delta_e)$ for some positive integer d_e and finite-dimensional division algebra Δ_e over k. Thus, both $X_i e$ and $X_i e'$ are direct sums of multiple copies of Δ_e. Since $\dim X_i e = \dim X_i e'$ for each i, it follows that $X_i e \cong X_i e'$ as Δ_e-vector spaces. Hence, there is a Δ_e-semilinear isomorphism from $X_i e$ to $X_i e'$. The same applies to the right modules eY_i and $e'Y_i$.

Fix Δ_e-semilinear transformations $\varphi_i \colon X_i e \to X_i e'$ and $\psi_i \colon eY_i \to e'Y_i$. Since $U = \bigoplus_{i=0}^{c} \bigoplus_{e \in \mathcal{E}} X_i e$, we define $\varphi \in \mathrm{End}(U)$ as φ_i from $X_i e \to X_i e'$, as $\varphi_i^{-1} \colon X_i e' \to X_i e$, and as the identity on $X_i f \to X_i f$ for each $f \in \mathcal{E} - \{e, e'\}$. Mimic this construction to create $\psi \in \mathrm{End}(V)^{\mathrm{op}}$ which interchanges eY_i with $e'Y_i$ for each $i \in \{0, \ldots, c\}$. It follows that $e^{(\varphi, \psi)} = e'$, and $(\varphi, \psi) \in N(S; J)$. □

Fix $e \in \mathcal{E}$. As in the proof of Lemma 3.7, $eSe \cong \mathbb{M}_{d_e}(\Delta_e)$ for a positive integer d_e and finite-dimensional division k-algebra Δ_e. Furthermore, for each $i \in \{0, \ldots, c\}$ there is are pairs $(m_i(e), n_i(e))$ of non-negative integers such that

$$X_i e \cong \Delta_e^{d_e} \otimes_k k^{m_i(e)} \quad \text{and} \quad eY_i \cong \Delta_e^{d_e} \otimes_k k^{n_i(e)} \tag{3.8}$$

as eSe-modules. The following is an explicit description of the subgroup of $N(S; J)$ that normalizes every simple ideal of S.

Lemma 3.9. *Let S be a semisimple complement to the Jacobson radical, J, of a subalgebra of $\mathrm{End}_k(U) \times \mathrm{End}_k(V)^{\mathrm{op}}$, and $\mathcal{E}$ the set of central-primitive idempotents of S. Then the subgroup of $N(S; J)$ that normalizes every ideal eSe ($e \in \mathcal{E}$) of S is isomorphic to*

$$\prod_{e \in \mathcal{E}} \Gamma\mathrm{L}_{d_e}(\Delta_e) \otimes_k \left(\prod_{i=0}^{c} \mathrm{GL}_{m_i(e)}(k) \times \mathrm{GL}_{n_i(e)}(k) \right).$$

Proof. Let $(\varphi, \psi) \in N(S; J)$ be such that $eSe^{(\varphi, \psi)} = eSe$ for every $e \in \mathcal{E}$. Fix $e \in \mathcal{E}$. Then (φ, ψ) induces a ring automorphism τ_e of $eSe \cong \mathbb{M}_{d_e}(\Delta_e)$. The Skolem–Noether theorem [8, (3.62)] shows that τ_e is conjugation by a Δ-semilinear transformation. Also, $\Gamma\mathrm{L}_{d_e}(\Delta_e)$ acts diagonally on Ue, which is isomorphic as Δ_e-module to $\Delta_e^{d_e(m_0+\cdots+m_c)}$, and also on eV, isomorphic to $\Delta_e^{d_e(n_0+\cdots+n_c)}$.

Let $\tau = (\tau_e : e \in \mathcal{E}) \in \mathrm{End}(U) \times \mathrm{End}(V)^{\mathrm{op}}$. Notice $eSe^{(\varphi, \psi)} = eSe^{\tau}$ and $(X_i \tau, \tau Y_i) = (X_i, Y_i)$ so $\tau \in N(S; J)$. Finally, $\tau' = (\varphi, \psi)\tau^{-1}$ centralizes S and lies in $N(S; J)$. Therefore, τ' is the identity on the S-simple submodules of the S-semisimple modules X_i and Y_i. In particular, τ' acts on $X_i e$ as $1 \otimes_k \mathrm{GL}_{m_i(e)}(k)$ and on eY_i as $1 \otimes_k \mathrm{GL}_{n_i(e)}(k)$, in the decomposition of (3.8). □

We can now state the full structure theorem for $N(A)$.

Theorem 3.10. *Let A be a subalgebra of $\mathrm{End}(U) \times \mathrm{End}(V)^{\mathrm{op}}$. Let $J = J(A)$ be the Jacobson radical of A, and S a semisimple complement to J in A. Let $\mathcal{E}$ be the set of central-primitive idempotents of S, and $N(S; J)$ the group defined in (3.5). Then the following hold.*

(i) $N(A) = \langle 1 + J, N(S) \cap N(A) \rangle$.

(ii) $N(S) \cap N(A) = \mathrm{Stab}_{N(S)}(J) = \{(x, y) \in N(S) : J^{(x, y)} = J\}$.

(iii) *For each $e \in \mathcal{E}$ there is a positive integer d_e and a finite-dimensional division k-algebra Δ_e such that $eSe \cong \mathbb{M}_{d_e}(\Delta_e)$ and*

$$\prod_{e \in \mathcal{E}} \mathrm{GL}_{d_e}(\Delta_e) \leqslant N(S) \cap N(A) \leqslant N(S; J).$$

(iv) *Let $\mathcal{F} = \{\sum_{e' \sim e} e' : e \in \mathcal{E}\}$. Then $N(S; J) = \prod_{f \in \mathcal{F}} N(fSf; J)$, where*

$$N(fSf; J) = \mathrm{Stab}_{N(fSf)}(\{(Uj^i f, fJ^i V) : 0 \leqslant i \leqslant c\}).$$

(v) *Let $f \in \mathcal{F}$, and suppose $f = \sum_{e' \sim e} e'$ for some $e \in \mathcal{E}$. Put $d_f = d_e$, $\Delta_f = \Delta_e$, $r_f = |\{e' \in \mathcal{E} : e' \sim e\}|$, $d_f m_i(f) = \dim_{\Delta_e} Uj^i e / Uj^{i+1}e$, and $d_f n_i(f) = \dim_{\Delta_e} eJ^i V / eJ^{i+1}V$. Then*

$$N(fSf; J) = \left(\Gamma\mathrm{L}_{d_f}(\Delta_f) \otimes_k \prod_{j=0}^{c} \mathrm{GL}_{m_i(f)}(k) \times \mathrm{GL}_{n_i(f)}(k) \right) \wr S_{r_f}.$$

Proof. For (i), we recall the theorem of Mal'cev asserting that $1 + J \leqslant A^{\times} \leqslant N(A)$ acts transitively on the set of semisimple complements to J in A. Thus, for each $\varphi \in N(A)$ there exists $z \in J$ with $S^{\varphi} = S^{1+z}$, so that $(1+z)\varphi^{-1} \in N(S) \cap N(A)$.

For (ii), since $N(S) \cap N(A)$ acts as ring automorphisms on A, it follows that $N(S) \cap N(A) \leqslant \mathrm{Stab}_{N(S)}(J)$. Also, if $(\varphi, \psi) \in \mathrm{Stab}_{N(S)}(J)$ and $(x, y) \in A$, then $(x, y) = (w + s, z + t)$ for $w, z \in J$ and $s, t \in S$. As $(w, z)^{(\varphi, \psi)} \in J$ and $(s, t)^{(\varphi, \psi)} \in S$, we have $(x, y)^{(\varphi, \psi)} = (w, z)^{(\varphi, \psi)} + (s, t)^{(\varphi, \psi)} \in J + S = A$, so that $(\varphi, \psi) \in N(A)$.

For (iii), we have $S = \bigoplus_{e \in \mathcal{E}} eSe$ with $eSe \cong \mathbb{M}_{d_e}(\Delta_e)$. Hence, $\prod_{e \in \mathcal{E}} \mathrm{GL}_{d_e}(\Delta_e) = S^{\times} \leqslant N(S) \cap N(A)$. Clearly, $N(S) \cap N(A)$ stabilizes the radical series (3.3), so $N(S) \cap N(A) \leqslant N(S; J)$.

Finally, (iv) and (v) follow directly from Lemmas 3.7 and 3.9. □

3.3. An algorithm to construct $N(A)$

In this section, we present an algorithmic version of Theorem 3.10. Although we anticipate practical uses for such an algorithm as a stand-alone function, it is already proving to be a valuable component in the algorithmic study of p-groups. We discuss this matter further in the concluding section. The complexity of the algorithm is difficult to predict, but it is roughly a function of the size of the Jacobson radical of $\mathrm{Adj}(\circ)$. For convenience, we shall mostly think of k in this section as a finite field, although extensions to algebraic number fields are possible.

Let $A \leqslant \mathbb{M}_a(k) \times \mathbb{M}_b(k)$ be given (we assume, as the enveloping algebra of some set of generators). First, we compute a Wedderburn decomposition $A = J \oplus S$, along with a decomposition of S into its minimal ideals $\{eSe : e \in \mathcal{E}\}$, where $\mathcal{E}$ is the set of central-primitive idempotents of S. Rónyai has shown that the complexity of decomposing algebras in this way is essentially that of factoring polynomials over k [21]. If k is a finite field, this can be done in polynomial time using randomized algorithms of the *Las Vegas* variety. (Such algorithms only return answers that are correct, but there is also a small chance that failure is reported.) Details may be found in [7, Section 4], [10,13].

Next, the idempotents $\mathcal{E}$ are partitioned to form the $\mathcal{F}$ of Theorem 3.10(iv). This applies the equivalence relation $\sim$ of Lemma 3.7. In particular, if $e, e' \in \mathcal{E}$ then $e \sim e'$ requires only that $d_e = d_{e'}$, that $\Delta_e \cong \Delta_{e'}$, and that dimensions of various Δ_e-vector spaces agree. Of those requirements, the only significant challenge is to test whether $\Delta_e \cong \Delta_{e'}$.

In fact, to build the permutations in $N(S; A)$ promised by Lemma 3.7, we really need an explicit isomorphism between the two division algebras. In the case when k is a finite field, isomorphism type is determined by dimension, and we require an isomorphism between field extensions K and L of k. In the context of the algorithm, the extensions K and L are specified, respectively, by generators ρ and μ (matrices of the same degree with entries in k). We use the following idea suggested to us by W.M. Kantor: compute the minimal polynomial of ρ over the base field k, and factor this polynomial over L; then, for any root $\tau \in L$, the assignment $\rho \mapsto \tau$ determines a linear transformation conjugating K to L.

We remark that isomorphism testing of general division algebras over $\mathbb{Q}$ is not known to be easy except for quaternionic instances [15].

The final step, for each $e \in \mathcal{E}$ and $0 \leqslant i \leqslant c$, is to decompose $X_i e = \Delta_e^{d_e} \otimes_k k^{m_i(e)}$ and $eY_i = \Delta_e^{d_e} \otimes_k k^{n_i(e)}$. This is done with a randomized Las Vegas algorithm known as the MeatAxe [12,14]. The action of $\Gamma\mathrm{L}_{d_e}(\Delta_e) \otimes (\mathrm{GL}_{m_i(e)}(k) \oplus \mathrm{GL}_{n_i(e)}(k))$ on $(X_i e, eY_i)$ is then immediate from the decomposition. We have thus proved:

Theorem 3.11. *For finite fields k, there is a polynomial-time Las Vegas algorithm that given a k-subalgebra $A \leqslant \mathbb{M}_u(k) \times \mathbb{M}_v(k)$ computes generators for the group $\langle 1 + J, N(S; J) \rangle$, along with its order and composition factors.*

Finally, by Theorem 3.10(ii), to build $N(A) = \langle 1+J, \mathrm{Stab}_{N(S;J)}(J) \rangle$ one must next construct $\mathrm{Stab}_{N(S;J)}(J)$. In general, it seems that one can do little better than simply to build a permutation presentation of $N(S; J)$ on J and compute the stabilizer as a permutation group, of course taking advantage of the decomposition in Theorem 3.10(iii). The problem of finding stabilizers in permutation groups is thought to be difficult [18, Section 4], and we do not expect an efficient general solution to the problem (see, for example, the construction in Section 3.4). We have, however, established the following result.

Theorem 3.12. *There is a polynomial-time Las Vegas algorithm that, given a semisimple subalgebra of $\mathrm{End}(U) \times \mathrm{End}(V)^{\mathrm{op}}$, where U and V finite-dimensional vector spaces over a finite field, constructs generators for $N(A)$.*

3.4. An example

We conclude this section with a construction which shows that computing $N(A)$ is at least as hard as computing $\mathrm{Aut}(\circ)$ for an arbitrary bimap $\circ$, and that the latter is essentially a generic "quadratic stabilizer" problem for which no efficient solution is known (details in Section 5.2). Thus, it is likely not through a lack of understanding that we have failed to achieve polynomial time for the general problem. We stress, however, that not all rings are adjoint rings, and in fact the rings we construct are not known to be adjoint rings. Hence, although the examples in our family give some indication of the difficulty of constructing $\mathrm{Aut}(\otimes_S)$ for $S \subset \mathrm{End}(U) \times \mathrm{End}(V)^{\mathrm{op}}$, they do not completely settle the matter.

Fix a field k, any bimap $\circ: U \times V \to W$, where U, V and W are finite-dimensional k-spaces, and ordered bases $\mathcal{X}$ and $\mathcal{Y}$ for U and V respectively.

For each $\varphi \in W^* = \hom_k(W, k)$, let $M(\circ^\varphi)$ denote the *Gram matrix* of the k-bilinear form $\circ^\varphi$, whose (x, y)-entry ($x \in \mathcal{X}$, $y \in \mathcal{Y}$) is $(x \circ y)\varphi \in k$. The *Gram representation* of $\circ$ is then defined as

$$W^\circ = \{M(\circ^\varphi) : \varphi \in W^*\} \leqslant \mathbb{M}_{a \times b}(k), \tag{3.13}$$

where $a = \dim_k U$ and $b = \dim_k V$. Observe that $(f, g; h) \in \mathrm{Aut}(\circ)$ if, and only if, the matrices (F, G) corresponding to (f, g) satisfy the condition

$$FW^\circ G = W^\circ. \tag{3.14}$$

Now define

$$A = \left\{ \left(\begin{bmatrix} a1_U & Z \\ 0 & b1_V \end{bmatrix}, \begin{bmatrix} a1_U & 0 \\ Z^t & b1_V \end{bmatrix} \right) : a, b \in k, \ Z \in W^\circ \right\} \leqslant \mathbb{M}_{a+b}(k) \times \mathbb{M}_{a+b}(k).$$

Then $J = J(A) = \left\{ \left(\begin{bmatrix} 0 & Z \\ 0 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 0 \\ Z^t & 0 \end{bmatrix} \right) : Z \in W^\circ \right\}$, so

$$N(S; J) = \left\{ \left(\begin{bmatrix} F & 0 \\ 0 & G \end{bmatrix}, \begin{bmatrix} F^{-t} & 0 \\ 0 & G^{-t} \end{bmatrix} \right) : F \in \mathrm{GL}(a, k), G \in \mathrm{GL}(b, k) \right\}, \text{ and}$$

$$N(S) \cap N(A) = \left\{ \left(\begin{bmatrix} F & 0 \\ 0 & G^{-t} \end{bmatrix}, \begin{bmatrix} F^{-t} & 0 \\ 0 & G \end{bmatrix} \right) : FW^\circ G = W^\circ \right\} \cong \mathrm{Aut}(\circ).$$

Thus, in order to construct $N(S) \cap N(A)$ from $N(S; J)$, one must solve a generic stabilizer problem of the form $FW^\circ G = W^\circ$.

4. Pseudo-isometries and ∗-normalizers

In this section we consider bimaps that have a certain form of symmetry. We say that $\circ \colon V \times V \to W$ is *Hermitian* if there exists $\theta \in \mathrm{Aut}(W)$ such that, for all $u, v \in V$, $u \circ v = (v \circ u)^\theta$. Hermitian bimaps, which include the more familiar reflexive forms, were studied in [4], where the groups

$$
\begin{aligned}
\mathrm{Isom}(\circ) &= \{ f \in \mathrm{Aut}(V) \colon \forall u, v \in V, \ uf \circ vf = (u \circ v) \} \\
&= \{ f \colon (f, g; h) \in \mathrm{Aut}(\circ), \ f = g \text{ and } h = 1 \}
\end{aligned}
\tag{4.1}
$$

of *isometries* of $\circ$ were described, and then used to construct intersections of classical groups. However, there are crucial applications of Hermitian bimaps – notably to automorphism groups of p-groups (see Section 5) – that involve a broader (but still restricted) type of autotopism, called a *pseudo-isometry*. We therefore study the group of all pseudo-isometries, namely

$$
\begin{aligned}
\Psi\mathrm{Isom}(\circ) &= \left\{ (f; \hat{f}) \in \mathrm{Aut}(V) \times \mathrm{Aut}(W) \colon \forall u, v \in V, \ uf \circ vf = (u \circ v)^{\hat{f}} \right\} \\
&= \{ (f; h) \colon (f, g; h) \in \mathrm{Aut}(\circ), \ f = g \}.
\end{aligned}
\tag{4.2}
$$

As in the case of a general bimap, we propose to study Hermitian bimaps by factoring through an associated tensor product. In view of that, and of the specific applications we have in mind, we restrict our attention to bimaps that are either *symmetric* ($u \circ v = v \circ u$ for all $u, v \in V$), or *alternating* ($v \circ v = 0$ for all $v \in V$). The tensor products associated to symmetric and alternating bimaps are equipped with the same symmetry property, and we denote them $\wedge^+$ and $\wedge^-$, respectively.

Once again, we form tensors over the adjoint algebra, $\mathrm{Adj}(\circ)$, of the bimap $\circ$. The symmetric nature of $\circ$ means that $(x, y) \in \mathrm{Adj}(\circ)$ if, and only if, $(y, x) \in \mathrm{Adj}(\circ)$. If, in addition, $\circ$ is nondegenerate, then y is uniquely determined by x. Hence $x^* := y$ defines an anti-automorphism of $\mathrm{Adj}(\circ)$ of order at most 2, giving it the structure of a ∗-ring. If $A \subseteq \mathrm{End}(V)$ is a ∗-ring, then the normalizer of A in (3.1) becomes

$$N^*(A) = \{ g \in \mathrm{Aut}(V) \colon (y^g)^* = (y^*)^g \in S \text{ for all } y \in A \}. \tag{4.3}$$

4.1. Proof of Theorem 1.5

We now prove our analogue of Theorem 1.3 for symmetric and exterior tensor products.

Proof. If $\circ \colon V \times V \to W$ is nondegenerate symmetric or alternating then $\circ$ factors through $\wedge^{\pm}_{\mathrm{Adj}(\circ)}$. To be equivalent to a tensor product, $\hat{\circ} \colon V \wedge_{\mathrm{Adj}(\circ)} V \to W$ must be an isomorphism.

Now suppose that $\circ = \wedge^{\pm}_A$ for a ∗-algebra $A \leqslant \mathrm{End}(V)$. Let $\varphi \in N^*(\mathrm{Adj}(\wedge_S))$, so that $(\varphi, \varphi) \in N(\mathrm{Adj}(\wedge_S))$. As in Theorem 3.2, there is an induced linear mapping $\hat{\varphi} \in \mathrm{Aut}(V \otimes_S V)$ defined by $(u \otimes v)^{\hat{\varphi}} = u\varphi \otimes v\varphi$. This map also satisfies $(u \wedge u)^{\hat{\varphi}} = 0$, so we can induce $\hat{\varphi}$ on $V \wedge_S V$. Now $(\varphi, \hat{\varphi}) \in \Psi \mathrm{Isom}(\wedge^{\pm}_S)$, and we see that $N^*(\mathrm{Adj}(\wedge^{\pm}_S)) \subseteq \Psi \mathrm{Isom}(\wedge^{\pm}_S)|_{\mathrm{Aut}(V)}$. $\square$

4.2. ∗-algebra normalizers

Theorem 1.5 demonstrates that pseudo-isometries of alternating tensor products are essentially ∗-normalizers of the adjoint ring of the tensor product. We now give a structural description of the ∗-normalizer of an algebra of matrices; in Section 4.3 we describe an algorithm to construct this group.

We adapt the notation set up in Section 3.2 to ∗-algebras. Let $A \leqslant \mathbb{M}_d(k)$ be a ∗-algebra, where $k = 2k$ is a field (we exclude fields of characteristic 2). By a result of Taft [22], A possesses a ∗-*invariant* (semisimple) complement, S, to its Jacobson radical $J = J(A)$.

We also require $\mathcal{E}$ to consist of ∗-invariant central-primitive idempotents. This set is obtained from $\mathcal{E}_0$, the set of central-primitive idempotents of the *ring* A (ignoring ∗ temporarily) as follows. Put $\mathcal{I}_0 = \{ e \in \mathcal{E}_0 \colon e^* = e \}$ and $\mathcal{J}_0 = \{ e + e^* \colon e \in \mathcal{E}_0 - \mathcal{I}_0 \}$. Then $\mathcal{E} := \mathcal{I}_0 \cup \mathcal{J}_0$ is the desired set of ∗-invariant central-primitive idempotents. In particular, eSe is a minimal ∗-ideal, for every $e \in \mathcal{E}$.

Our initial partition of idempotents is a little more refined than for ordinary rings, as we now explain.

Each simple ∗-algebra has an associated pair $(d, \mathcal{O})$ of parameters, where d is a positive integer, and $\mathcal{O}$ is a ∗-algebra whose non-trivial ∗-invariant elements are invertible. Osborn has classified such rings $\mathcal{O}$ and so we refer these as *Osborn*

pseudo-division algebras [20]. To avoid confusion, we denote the involution in $\mathcal{O}$ as $s \mapsto \bar{s}$. Define the usual Hermitian $\mathcal{O}$-forms as bimaps $\bullet \colon \mathcal{O}^d \times \mathcal{O}^d \to \mathcal{O}$ where for some $M = \overline{M}^t \in \mathbb{M}_d(\mathcal{O})$,

$$(\forall u, v \in \mathcal{O}^d) \qquad u \bullet v = uM\bar{v}^t. \tag{4.4}$$

Fix $e \in \mathcal{E}$. As shown in [24, Section 4.5], there is a unique Osborn division algebra $\mathcal{O}_e$, a rank d_e, and a nonsingular $M_e = \overline{M_e}^t \in \mathbb{M}_{d_e}(\mathcal{O}_e)$ such that

$$eSe \cong \mathrm{Adj}(\bullet \colon \mathcal{O}_e^{d_e} \times \mathcal{O}_e^{d_e} \to \mathcal{O}_e) \cong \langle \mathbb{M}_{d_e}(\mathcal{O}_e), X \mapsto M_e \overline{X}^t M_e^{-1} \rangle$$

$$(eSe)^{\#} = \{x \in eTe^{\times} : xx^* = 1\} = \mathrm{Isom}(\bullet \colon \mathcal{O}_e^{d_e} \times \mathcal{O}_e^{d_e} \to \mathcal{O}_e)$$

$$= \{g \in \mathrm{GL}_{d_e}(\mathcal{O}_e) : gM_e\bar{g}^t = M_e\}.$$

Define S-submodules $X_0, \ldots, X_c$ of V as in (3.4), where $VJ^i = X_i \oplus \cdots \oplus X_c$ for each $0 \leqslant i \leqslant c$.

We can now define our equivalence relation $\sim$ on $\mathcal{E}$, where $e \sim e'$ if, and only if, eSe and $e'Se'$ are isomorphic as $*$-rings (that is, $d_e = d_{e'}$ and $\mathcal{O}_e$ and $\mathcal{O}_{e'}$ are isomorphic algebras) and, for all $i \in \{0, \ldots, c\}$, $\dim X_i e = \dim X_i e'$.

The following is our $*$-analogue of Theorem 3.10.

Theorem 4.5. *Let A be a $*$-subalgebra of* $\mathrm{End}(V)$. *Let* $J = J(A)$ *be the Jacobson radical of A, and S a semisimple $*$-invariant complement to J in A. Let $\mathcal{E}$ be the set of $*$-invariant central-primitive idempotents of S. Then the following hold.*

(i) $N^*(A) = \langle \{z + \sqrt{1 + z^2} : z \in J, z^* = -z\}, N^*(S) \cap N^*(A) \rangle$.

(ii) $N^*(S) \cap N^*(A) = \mathrm{Stab}_{N^*(S)}(J^-) \cap \mathrm{Stab}_{N^*(S)}(J^+)$.

(iii) *For each $e \in \mathcal{E}$ there is a positive integer d_e, a finite-dimensional Osborn pseudo-division k-algebra $\mathcal{O}_e$, and an Hermitian $\mathcal{O}$-form $\bullet_e \colon \mathcal{O}_e^{d_e} \times \mathcal{O}_e^{d_e} \to \mathcal{O}_e$ such that $eSe \cong \mathrm{Adj}(\bullet_e)$ (as $*$-algebras) and*

$$\prod_{e \in \mathcal{E}} \mathrm{Isom}(\bullet_e) \leqslant N^*(S) \cap N^*(A) \leqslant \mathrm{Stab}_{N^*(S)}(VJ^i).$$

(iv) *Let $\mathcal{F} = \{\sum_{e \sim e'} e' : e \in \mathcal{E}\}$. Then $N(S; J) = \prod_{f \in \mathcal{F}} N(fSf; J)$, where*

$$N(fSf; J) = \mathrm{Stab}_{N^*(fTf)}(\{VJ^if : 0 \leqslant i \leqslant c\}).$$

(v) *Let $f \in F$, and suppose $f = \sum_{e' \sim e} e'$ for some $e \in \mathcal{E}$. Put $d_f = d_e$, $\mathcal{O}_f = \mathcal{O}_e$, $r_f = |\{e' \in \mathcal{E} : e' \sim e\}|$, and $d_f m_i(f) = \mathrm{rank}_{\mathcal{O}_e} VJ^i e/VJ^{i+1}$. Then*

$$\mathrm{Stab}_{N^*(fTf)}(UJ^if, fJ^iV) = \left(\Psi\mathrm{Isom}(\bullet_e) \otimes_k \prod_{j=0}^{c} \mathrm{GL}_{m_i(f)}(k) \right) \wr S_{r_f}.$$

Proof. For (i), let $\varphi \in N^*(A)$. Since S^{φ} is a $*$-invariant complement to J in A, and $U = \{z + \sqrt{1 + z^2} : z \in J^-\}$ acts transitively on the set of all such complements, there exists $u \in U$ such that $S^{\varphi u} = S$ [4, Theorem 1.1]. It follows that $\varphi u \in \mathrm{Stab}_{N^*(S)}(J^-) \cap \mathrm{Stab}_{N^*(S)}(J^+)$, and the result follows.

For (ii), note that $\varphi \in N^*(S)$ lies in $N^*(A)$ if, and only if, φ stabilizes J and commutes with the involution on J. The condition is equivalent to φ stabilizing J^+ and J^-. For, if φ stabilizes J^+ and J^-, and $z = z^+ + z^-$ with $z^{\pm} \in J^{\pm}$, then

$$(z^{\varphi})^* = ((z^+ + z^-)^{\varphi})^* = ((z^+)^{\varphi})^* + ((z^-)^{\varphi})^* = (z^+)^{\varphi} - (z^-)^{\varphi}.$$

On the other hand, if $z \in J^{\epsilon}$, say, with $z^{\varphi} \notin J^{\epsilon}$, then $(z^*)^{\varphi} = \epsilon z^{\varphi} \neq (z^{\varphi})^*$.

For (iii)–(v) the proofs are essentially the same as that of Theorem 3.10 except that $N^*(eSe) \cong \Psi\mathrm{Isom}(\bullet_e) \otimes \mathrm{GL}_{m_i(e)}(k)$, where $\bullet_e \colon \mathcal{O}_e^{d_e} \times \mathcal{O}_e^{d_e} \to \mathcal{O}_e$ [24, Corollary 4.30]. $\square$

4.3. An algorithm to construct $N^*(A)$

Most of the machinery needed to provide an algorithmic version of Theorem 4.5 was developed in [4].

First, procedures for decomposing S as a direct sum of minimal $*$-ideals, and for identifying the simple type of these ideals, are given in [4, Theorem 4.1].

The algorithm for Theorem 4.5 is almost identical to its counterpart for Theorem 3.10. The only essential difference is that, instead of generators for $\mathrm{GL}(d_i, K_i)$, we must choose suitable generators for $\Psi\mathrm{Isom}(\bullet_e)$. Those groups are, however, all (conformal) classical groups, and it is elementary to write down small generating sets for them (see [4, Section 5.4]).

For (ii), an algorithmic version of Taft's decomposition is given in [4, Proposition 4.3]. The unipotent radical $\{z + \sqrt{1 + z^2} : z \in J^-\}$ is constructed in [4, Section 5.2] using a power series. Finally, the remarks we made about stabilizing the radical in Section 3.3 apply equally in this setting.

We conclude this section with an analogue of Theorem 3.12 for $*$-rings.

Theorem 4.6. *There is a polynomial-time Las Vegas algorithm that, given a semisimple $*$-subalgebra, A, of* $\mathrm{End}(V)$, *where V is a finite-dimensional vector space over a finite field of odd characteristic, constructs generators for $N^*(A)$.*

5. Applications

We conclude the paper with a brief discussion of several algorithmic problems of interest whose solution relies on our ability to compute and understand $\text{Aut}(\circ)$.

5.1. Automorphisms of p-groups

The relationship between nilpotent groups and algebras extends back to the 1930's and has evolved to handle ever larger families of groups; for a survey see [23, Section 5]. The typical method is to relate commutation $[x, y] = x^{-1}y^{-1}xy$ in a group G to a distributive product. Through specific correspondences of Baer, and of Kaloujnine, Lazard, and Mal'cev, automorphisms of G are seen to induce autotopisms of a distributive product. We make this precise for the more elementary setting: the Baer correspondence [2]. Further details are given in [24, Section 3].

Let G be a group, $G' = \langle [x, y] = x^{-1}y^{-1}xy : x, y \in G \rangle$ its *commutator subgroup*, and $Z = Z(G) = \{x \in G : [x, G] = 1\}$ its *center*. Suppose that $G' \leqslant Z$. If $V = G/Z$ and $W = G'$, with operations written additively, then $\circ : V \times V \to W$, with $xZ \circ yZ := [x, y]$ for all $x, y \in G$, is a well-defined bimap. Also, since $v \circ v = 0$ for all $v \in V$, we see that $\circ$ is *alternating*. Hence $\circ$ factors uniquely through $\wedge : V \times V \to V \wedge V = V \otimes V / \langle v \otimes v : v \in V \rangle$.

For convenience, let us assume that G is a finite p-group, so V and W are now finite-dimensional k-spaces, where $k = \text{GF}(p)$. Each $\alpha \in \text{Aut}(G)$ restricts to an automorphism $w^{\hat{\varphi}} = w\alpha$ on W, and induces an automorphism $(xZ)\varphi = x\alpha Z$ on V. Furthermore, the pair $(\varphi; \hat{\varphi})$ is a pseudo-isometry of $\circ$. This establishes a homomorphism from $\text{Aut}(G)$ to the group $\Psi\text{Isom}(\circ)$ of all pseudo-isometries of $\circ$. In some important settings (for instance when $G^p = 1$) the image of $\text{Aut}(G)$ is all of $\Psi\text{Isom}(\circ)$ [24, Proposition 3.8].

In the absence of more refined strategies, $\Psi\text{Isom}(\circ)$ is typically constructed "by brute-force", meaning that one simply computes the stabilizer of $\ker \hat{\circ}$ under the natural action of $\text{GL}_k(V)$ on $V \wedge V$, sending $u \wedge v \mapsto ug \wedge vg$, for $g \in \text{GL}_k(V)$. The limitations are obvious: the action of $\text{GL}_k(V)$ on $V \wedge V$ can have orbits that are far too large for effective computation. Moreover, the results give no hint of structure.

One way to finesse the problem is to factor $\circ$ through the possibly smaller space $V \wedge_A V$, where $A = \text{Adj}(\circ)$. This helps in two ways. First, the natural group that acts on $V \wedge_A V$, namely the group $\Psi\text{Isom}(\wedge_A)$ of pseudo-isometries of the bimap $\wedge_A$, is no longer all of $\text{GL}_k(V)$, and may be a significantly smaller subgroup. Second, the space $V \wedge_A V$ may have much smaller dimension than $V \wedge V$. Therefore finding $\Psi\text{Isom}(\circ)$ as a stabilizer in $\Psi\text{Isom}(\wedge_A)$ of $\ker \hat{\circ} \leqslant V \otimes_A V$ will often be substantially easier. Not surprisingly, this approach to computing $\text{Aut}(G) \cong \Psi\text{Isom}(\circ)$ is most effective in situations where $A = \text{Adj}(\circ)$ is large or $V \wedge_A V$ is small. Both of those desirable conditions are met, for instance, when $|G'| = p^2$, a particularly nice case that is handled separately in [6].

The general method we have outlined above constitutes one part of a comprehensive new strategy to construct generators for the automorphism group of p-group of class 2 and exponent p. This strategy is currently being developed jointly by the authors and E.A. O'Brien [3].

5.2. Quadratic stabilizer

Autotopism groups provide a natural context for the general problem of stabilizing a subspace of rectangular matrices.

The familiar *linear stabilizer problem* starts with a field k, a positive integer a, and subspace $W \leqslant k^a$; and asks for $\text{Stab}(W) = \{x \in \text{GL}(a, k) : Ux = U\}$. By simply writing $k^a = X \oplus U$ we find that

$$\text{Stab}(W) = \left\{ \begin{bmatrix} A & B \\ 0 & C \end{bmatrix} : A \in \text{GL}(X), B \in \text{hom}(X, U), C \in \text{GL}(U) \right\}.$$

So this linear stabilizer problem is elementary to solve.

The *quadratic stabilizer problem* concerns a field k, positive integers a, b, and a subspace $W \leqslant \mathbb{M}_{a \times b}(k)$. The goal is to describe the group

$$\text{Stab}(W) = \{(x, y) \in \text{GL}(a, k) \times \text{GL}(b, k) : xWy^t = W\}. \tag{5.1}$$

The related *Hermitian stabilizer problem* has the tighter constraints that $a = b$ and that for all $w \in W$, $w = \varepsilon \, \overline{w}^t$ for some $\varepsilon \in \{\pm 1\}$, and some (possibly identity) field automorphism $s \mapsto \bar{s}$ on k. The problem is then to describe the group

$$H\text{Stab}(W) = \{x \in \text{GL}(a, k) : xW\bar{x}^t = W\}. \tag{5.2}$$

The quadratic and Hermitian stabilizer problems are known to be hard problems. It is no surprise that the reverse construction to Section 3.4 shows that the quadratic stabilizer problem is the problem of constructing $\text{Aut}(\circ)$.

The introduction of tensor products (other than with k) is new to the this topic. Similar to the improvements made for automorphisms of p-groups in Section 5.1, knowledge of $\text{Aut}(\otimes_S)$ reduces the work needed to compute $\text{Stab}(W)$.

References

[1] E. Artin, Geometric Algebra, Interscience Publishers, Inc, New York–London, 1957, MR0082463 (18,553e).
[2] R. Baer, Groups with abelian central quotient group, Trans. Amer. Math. Soc. 44 (3) (1938) 357–386. MR1501972.
[3] P.A. Brooksbank, E.A. O'Brien, J.B. Wilson, Computing automorphism groups of p-groups (in preparation).
[4] P.A. Brooksbank, J.B. Wilson, Computing isometry groups of Hermitian maps, Trans. Amer. Math. Soc. 364 (2012) 1975–1996.
[5] P.A. Brooksbank, J.B. Wilson, Intersecting two classical groups, J. Algebra 353 (1) (2012) 286–297.
[6] P.A. Brooksbank, J.B. Wilson, The nilpotent groups of co-rank 2, preprint.
[7] A.M. Cohen, G. Ivanyos, D.B. Wales, Finding the radical of an algebra of linear transformations, in: Algorithms for Algebra (Eindhoven, 1996), J. Pure Appl. Algebra 117/118 (1997) 177–193. MR1457838 (98h:16026).
[8] C.W. Curtis, I. Reiner, Methods of Representation Theory. Vol. I, John Wiley & Sons Inc., New York, 1981, With applications to finite groups and orders; Pure and Applied Mathematics; A Wiley-Interscience Publication. MR632548 (82i:20001).
[9] B.A. Davey, H.A. Priestley, Introduction to Lattices and Order, 2nd ed., Cambridge University Press, New York, 2002, MR1902334 (2003e:06001).
[10] W. Eberly, M. Giesbrecht, Efficient decomposition of associative algebras over finite fields, J. Symbolic Comput. 29 (2000) 441–458.
[11] Graham Higman, Enumerating p-groups. I. Inequalities, Proc. London Math. Soc. (3) 10 (1960) 24–30. MR0113948 (22 #4779).
[12] D. Holt, S. Rees, J. Austral. Math. Soc. (Series A) 57 (1994) 1–16.
[13] G. Ivanyos, Fast randomized algorithms for the structure of matrix algebras over finite fields (extended abstract), in: Proceedings of the 2000 International Symposium on Symbolic and Algebraic Computation (St. Andrews), ACM, New York, 2000, pp. 175–183. (electronic). MR1805121.
[14] G. Ivanyos, K. Lux, Treating the exceptional cases of the MeatAxe, Experiment. Math. 9 (3) (2000) 373–381. MR1795309 (2001j:16067).
[15] G. Ivanyos, L. Rónyai, Quaternion algebras, in: Some Tapas of Computer Algebra, in: Algorithms Comput. Math., vol. 4, Springer, Berlin, 1999, pp. 311–314. MR1679932.
[16] N. Jacobson, Basic Algebra. II, 2nd ed., W.H. Freeman and Company, New York, 1989, MR1009787 (90m:00007).
[17] M.L. Lewis, J.B. Wilson, Isomorphism in expanding families of indistinguishable groups, Groups Complex. Cryptol. 4 (2012) 73–110.
[18] E.M. Luks, Permutation groups and polynomial-time computation, in: Groups and Computation, New Brunswick, NJ, 1991, in: DIMACS Ser. Discrete Math. Theoret. Comput. Sci., vol. 11, Amer. Math. Soc., Providence, RI, 1993, pp. 139–175. MR1235801 (94h:20005).
[19] Yu.A. Neretin, An estimate for the number of parameters defining an n-dimensional algebra, Izv. Akad. Nauk SSSR Ser. Mat. 51 (2) (1987) 306–318, 447 (in Russian); English transl., Math. USSR-Izv. 30 (1988), no. 2, 283–294. MR896999 (88i:17001).
[20] J.M. Osborn, Jordan algebras of capacity two, Proc. Natl. Acad. Sci. USA 57 (1967) 582–588. MR0215892 (35 #6727).
[21] L. Rónyai, Computations in associative algebras, in: Groups and Computation, New Brunswick, NJ, 1991, in: DIMACS Ser. Discrete Math. Theoret. Comput. Sci., vol. 11, Amer. Math. Soc., Providence, RI, 1993, pp. 221–243. MR1235805 (94g:68059).
[22] E.J. Taft, Invariant Wedderburn factors, Illinois J. Math. 1 (1957) 565–573.
[23] R.B. Warfield Jr., Nilpotent groups, in: Lecture Notes in Mathematics, vol. 513, Springer-Verlag, Berlin, 1976, MR0409661 (53 #13413).
[24] J.B. Wilson, Decomposing p-groups via Jordan algebras, J. Algebra 322 (8) (2009) 2642–2679. MR2559855 (2010i:20016).
[25] J.B. Wilson, Division, adjoints, and dualities of bilinear maps, Comm. Algebra 41 (2013) http://dx.doi.org/10.1080/00927872.2012.660668.