POLARIZATION IDENTITIES

CHASE BENDER AND DEBRAJ CHAKRABARTI

ABSTRACT. We prove a generalization of the polarization identity of linear algebra expressing the inner product of a complex inner product space in terms of the norm, where the field of scalars is extended to an associative algebra equipped with an involution, and polarization is viewed as an averaging operation over a compact multiplicative subgroup of the scalars. Using this we prove a general form of the Jordan-von Neumann theorem on characterizing inner product spaces among normed linear spaces, when the scalars are taken in an associative algebra.

1. INTRODUCTION

1.1. **Motivation.** The goal of this article is to present a general version of the *polarization identity* of elementary linear algebra. This well-known identity takes the form

$$\langle x, y \rangle = \frac{1}{4} \left(\|x + y\|^2 + i \|x + iy\|^2 - \|x - y\|^2 - i \|x - iy\|^2 \right), \quad i = \sqrt{-1}, \qquad (1.1)$$

for vectors x, y in a complex inner product space, where the inner product is denoted by $\langle \cdot, \cdot \rangle$ and the induced norm by $\|\cdot\|$. The identity has very important applications in classical Hilbert space theory (e.g. [JvN35, Hal51]). This paper takes the point of view, not unknown in the literature (see [You88, p. 12, Problem 1.10] and [D'A02, pp. 53–54]), that this identity is an instance of a fundamental and ubiquitous process in mathematics, that of averaging over a group (a.k.a. Haar integration). From this point of view, (1.1) is really saying that

$$\langle x, y \rangle = \int_G \|x + gy\|^2 \, g \, dg, \qquad (1.2)$$

where $G = \{\pm 1, \pm i\}$ is the four element cyclic group of complex fourth roots of unity, and the integral is that of the complex valued function $g \mapsto \|x + gy\|^2 \, g$ on the compact group G with respect to the Haar measure of G, normalized to a probability measure. Our generalization of (1.1) (Theorem 1.1 below) will replace the field of complex numbers by an associative algebra $\mathfrak{A}$ over $\mathbb{R}$ equipped with an involution, the inner product with a general Hermitian form, the group G with a compact multiplicative group of unitary elements of $\mathfrak{A}$ (where an element of $\mathfrak{A}$ is unitary if the involution maps it to its inverse).

Several authors have considered the natural problem of obtaining polarization identities for Hermitian forms over scalars other than $\mathbb{R}$ or $\mathbb{C}$. In [Jam70, page 75, Theorem 5] Jamison obtained a polarization identity over the $\mathbb{R}$-algebra of quaternions (and the nonassociative algebra of octonions). In [GR93] Giarrusso and Romano obtained a polarization identity over Clifford numbers. The question has also been studied by Waterhouse ([Wat95]) from a purely algebraic perspective for involutive algebras over very general commutative rings.

Our results here have interesting intersections with the generalized polarization identities obtained by these authors, but emphasize the role of averaging over a group as a key feature of the polarization process of recovering a Hermitian form from its restriction to the diagonal. We also restrict ourselves to algebras over the real numbers $\mathbb{R}$, first, to take advantage of classical integration theory, and second, because of the application to a generalized Jordan-von Neumann theorem (see Theorem 1.3 below). However, it is clear that ideas and results of this paper make sense over other fields, and it would be interesting to look at such generalizations.

1.2. **Polarizable algebras and polarizing subgroups.** Let $\mathfrak{A} = (\mathfrak{A}, *)$ be a *real involutive algebra,* by which we mean a finite dimensional unital associative algebra over $\mathbb{R}$ equipped with an anti-automorphism $\mathfrak{A} \to \mathfrak{A}, \alpha \mapsto \alpha^*$ of order two (the *involution*), i.e., the involution is $\mathbb{R}$-linear, $(\alpha\beta)^* = \beta^*\alpha^*$ and $(\alpha^*)^* = \alpha$ for $\alpha, \beta \in \mathfrak{A}$. The multiplicative identity of $\mathfrak{A}$ will be denoted by $1_{\mathfrak{A}}$ (or simply 1 if confusion is unlikely). We also call real involutive algebras *∗-algebras* for short, and these ∗-algebras will replace the field $\mathbb{C}$ in the generalized polarization identity.

Thought of as a finite dimensional real vector space, a ∗-algebra $\mathfrak{A}$ has a natural linear topology in which the algebraic operations are continuous. We will always endow $\mathfrak{A}$ with this topology, and its subsets with the induced subspace topology. Then the group $\mathfrak{A}^{\times}$ of units of $\mathfrak{A}$ is a locally compact topological group. If G is a compact subgroup of $\mathfrak{A}^{\times}$, then G is a compact topological group, and therefore admits a (simultaneously left and right invariant) Haar measure. which will be always normalized to a probability measure. Given a function $f : G \to V$ taking values in a finite dimensional real vector space V, we can define the integral with respect to Haar measure of f, which we will denote by

$$\int_G f dg \quad \text{or} \quad \int_G f(g) dg \tag{1.3}$$

and can be defined invariantly as the unique vector in the space V satisfying the condition

$$\phi \left(\int_G f dg \right) = \int_G (\phi \circ f) \, dg \tag{1.4}$$

for each linear functional $\phi : V \to \mathbb{R}$, the integral on the right being the classical integral of a real valued function on G with respect to Haar measure. The existence and uniqueness of the integral in (1.3) is easily established by choosing a basis of the vector space V and working in the corresponding coordinates.

An element $u \in \mathfrak{A}$ will be said to be *unitary* if we have $uu^* = 1_{\mathfrak{A}}$, and the collection of all unitary elements

$$\Gamma(\mathfrak{A}, *) = \{u \in \mathfrak{A} : uu^* = 1_{\mathfrak{A}}\}, \tag{1.5}$$

will be called the called the *unitary group* of the algebra $(\mathfrak{A}, *)$. It is therefore a locally compact topological group, and generalizes the circle group $\{|z| = 1\}$ in $\mathbb{C}$.

We will say that a closed subgroup $G \subset \Gamma(\mathfrak{A}, *)$ *generates* the ∗-algebra $\mathfrak{A}$ if $\mathfrak{A}$ is the smallest ∗-subalgebra of $\mathfrak{A}$ containing the group G. It is clear that $\Gamma(\mathbb{C}) = \{|z| = 1\}$ generates $\mathbb{C}$. Notice that since G is closed under the operations of multiplication and involution of $\mathfrak{A}$, it follows that G generates $\mathfrak{A}$ if and only if

$$\text{span}_{\mathbb{R}} G = \mathfrak{A}$$

i.e. G generates $\mathfrak{A}$ also as a vector space. We now make the following definition:

Definition 1.1. Let $(\mathfrak{A}, *)$ be a $*$-algebra. We say that $(\mathfrak{A}, *)$ is *polarizable* if the unitary group $\Gamma(\mathfrak{A}, *)$ is compact and generates $\mathfrak{A}$.

Polarizable algebras will replace the complex numbers in the general polarization identity (1.8) below. A key property of polarizable algebras is that a version of Maschke's theorem holds for them, showing that they are semisimple and leading to a complete classification of these algebras under an appropriate notion of equivalence (see Theorem 1.2 below). We now introduce the groups which will replace, in the general polarization formula, the group G of 4-th roots of unity that appears in (1.1) and (1.2):

Definition 1.2. Let $(\mathfrak{A}, *)$ be a $*$-algebra. A compact subgroup $G \subseteq \Gamma(\mathfrak{A}, *)$ is said to be *polarizing* if G generates $\mathfrak{A}$ as an algebra and

$$\int_G g\, dg = 0, \tag{1.6}$$

where the integral is that of the inclusion function $g : G \to \mathfrak{A}$ of the group G in the vector space $\mathfrak{A}$, and the integral is taken with respect to the (bi-invariant) Haar measure.

The following facts shed some light on the notions introduced in Definitions 1.1 and 1.2:

(a) In a polarizable algebra $(\mathfrak{A}, *)$, the unitary group $\Gamma(\mathfrak{A}, *)$ is polarizable. The condition (1.6) is satisfied for $\Gamma(\mathfrak{A}, *)$ since $-1_{\mathfrak{A}}$, the negative of the identity of the algebra $\mathfrak{A}$, automatically belongs to $\Gamma(\mathfrak{A}, *)$, so we have by Haar invariance:

$$\int_{\Gamma(\mathfrak{A},*)} g\, dg = \int_{\Gamma(\mathfrak{A},*)} (-1_{\mathfrak{A}})g\, dg = -\int_{\Gamma(\mathfrak{A},*)} g\, dg. \tag{1.7}$$

(b) We will see below that (1.6) is satisfied for many groups G (Proposition 3.2).

(c) On the other hand, as soon as a $*$-algebra has a polarizing subgroup (or even a compact subgroup of the unitary group that generates the algebra), it is polarizable (see Proposition 2.4 below).

(d) Finally, each polarizable algebra admits a *finite* polarizing subgroup (see Proposition 5.3) below. It follows that the polarization process is always possible in terms of algebraic formulas such as (1.1) rather than integral formulas such as (5.3), where the integral is over a Lie group of positive dimension.

1.3. **Generalized Polarization identity.** Let $(\mathfrak{A}, *)$ be a $*$-algebra and let X be a left $\mathfrak{A}$-module. By an ($\mathfrak{A}$-valued) *Hermitian form* on X we mean a map $Q : \mathsf{X} \times \mathsf{X} \to \mathfrak{A}$ such that for $x, y, z \in \mathsf{X}$, $\alpha \in \mathfrak{A}$ we have

$$Q(x + y, z) = Q(x, z) + Q(y, z), \quad Q(\alpha x, y) = \alpha Q(x, y), \quad \text{and} \quad Q(x, y)^* = Q(y, x).$$

Then we have the following:

Theorem 1.1. *Let $(\mathfrak{A}, *)$ be a polarizable $*$-algebra. Then there is an element $\kappa \in \mathfrak{A}$ such that whenever X is a left $\mathfrak{A}$-module and $Q : \mathsf{X} \times \mathsf{X} \to \mathfrak{A}$ is a Hermitian form, then we have the polarization identity*

$$Q(x, y) = \kappa \int_G q(x + gy)g\, dg, \quad x, y \in \mathsf{X} \tag{1.8}$$

where $q(x) = Q(x, x)$, $G \subset \Gamma(\mathfrak{A})$ is a polarizing subgroup, and the integral is that of an $\mathfrak{A}$-valued function on G with respect to the normalized Haar measure.

We emphasize that in Theorem 1.1, the constant κ depends only on the (polarizable) $*$-algebra $(\mathfrak{A}, *)$ and not on the particular polarizing group G. This element $\kappa = \kappa(\mathfrak{A}, *)$ will be called the *polarization constant* of $(\mathfrak{A}, *)$, and in Theorem 1.2 below we show how to compute it.

1.4. **More definitions and constructions related to $*$-algebras.** Before we proceed further, we collect a few definitions.

(1) If $(\mathfrak{A}, \sharp)$ is a $*$-algebra, there is a natural way to define an induced involution on the matrix algebra $M_n(\mathfrak{A})$ by setting

$$A \mapsto (A^\sharp)^T, \tag{1.9}$$

where $A^\sharp$ is the matrix obtained from A by applying the involution $\sharp$ to each entry, and B^T is the transpose of the matrix B. We call this involution on $M_n(\mathfrak{A})$ the *involution induced by $\sharp$*.

(2) Each of the real division algebras $\mathbb{D} = \mathbb{R}, \mathbb{C}, \mathbb{H}$ has its own standard involution traditionally called a "conjugation", which is the identity for $\mathbb{R}$, the complex conjugation for $\mathbb{C}$ and the quaternionic conjugation

$$a + ib + jc + kd \mapsto a - ib - jc - kd \tag{1.10}$$

for $\mathbb{H}$. We denote the conjugation operation in each case by $z \mapsto \overline{z}$, following the standard convention. The involution induced by the conjugation map on $\mathbb{D}$ on the algebra $M_n(\mathbb{D})$ will be called the "conjugate-transpose" involution of $M_n(\mathbb{D})$. We will see later that $M_n(\mathbb{D})$ has many other involutions apart from the conjugate-transpose (see Proposition 2.2 below).

(3) In the category of involutive algebras, a morphism is called a $*$-*homomorphism*:

$$\phi : (\mathfrak{A}, *) \to (\mathfrak{B}, \sharp)$$

where ϕ is a homomorphism of unital associative algebras, and preserves the involution, i.e.

$$\phi(\alpha^*) = \phi(\alpha)^\sharp.$$

It is clear what is meant by a $*$-isomorphism, or a $*$-subalgebra.

(4) Given a finite collection $\{(\mathfrak{A}_j, *_j), 1 \leqslant j \leqslant N\}$ of $*$-algebras, we define its $*$-*direct sum* be the direct sum $\bigoplus_{j=1}^N \mathfrak{A}_j$ equipped with the "direct sum involution"

$$(\alpha_1, \ldots, \alpha_N)^* = (\alpha_1^{*_1}, \ldots, \alpha_N^{*_N}), \quad \alpha_j \in \mathfrak{A}_j, 1 \leqslant j \leqslant N.$$

1.5. **Polarization constants.** We now determine the structure of polarizable algebras and use it to compute the polarization constant of an algebra:

Theorem 1.2. *Let $(\mathfrak{A}, *)$ be a $*$-algebra. Then $(\mathfrak{A}, *)$ is polarizable if and only if there is a $*$-isomorphism*

$$\phi : \bigoplus_{j=1}^N (M_{n_j}(\mathbb{D}_j), *) \to (\mathfrak{A}, *), \tag{1.11}$$

where in the left is the $*$-direct sum of a a finite number of matrix algebras over real division rings, each endowed with the "conjugate-transpose" involution. The polarization constant of $(\mathfrak{A}, *)$ is

$$\phi\left(\frac{n_1 \delta_1}{(n_1 - 1)\delta_1 + 2} I_{n_1}, \ldots, \frac{n_j \delta_j}{(n_j - 1)\delta_j + 2} I_{n_j}, \ldots, \frac{n_N \delta_N}{(n_N - 1)\delta_N + 2} I_{n_N}\right), \tag{1.12}$$

where $\delta_j = \dim_{\mathbb{R}}(\mathbb{D}_j) = 1, 2$ or 4 denotes the dimension of the division algebra $\mathbb{D}_j$ as a real vector space and I_{n_j} is the $n_j \times n_j$ identity matrix of $M_n(\mathbb{D}_j)$ for $1 \leqslant j \leqslant N$.

The fact that a polarizable algebra such as $(\mathfrak{A}, *)$ has the above structure (i.e. it is semisimple) allows us to understand the module X and Hermitian form Q of Theorem 1.1 in terms of $\mathfrak{A}$ (see [Lam01]). Since the precise structure of the module X does not play any role in the polarization phenomenon of Theorem 1.1, we do not discuss this further.

1.6. **Generalized Jordan-von Neumann-Jamison theorem.** The Jordan-von Neumann theorem ([JvN35]) solves the problem of geometrically characterizing inner product spaces among normed linear spaces over $\mathbb{C}$ or $\mathbb{R}$: the norm of a normed space $(X, \|\cdot\|)$ arises from an inner product (i.e., there is an inner product $\langle \cdot, \cdot \rangle$ on X such that $\|x\| = \sqrt{\langle x, x \rangle}$ for each $x \in X$) if and only if the *parallelogram identity*

$$\|x + y\|^2 + \|x - y\|^2 = 2 \left(\|x\|^2 + \|y\|^2 \right) \tag{1.13}$$

holds for all $x, y \in X$. In [Jam70], the field of scalars was already extended to the quaternions (and octonions.) Here, we will prove a generalization to Hermitian forms over polarizable algebras. The case of quaternionic scalars was proved in [Jam70].

The analog of the map $x \mapsto \|x\|^2$ occurring in formulas such as (1.1) and (1.13) in the situation of non-commutative scalars from $\mathfrak{A}$ will be called a *quadrance*, i.e., a "squaring", a name inspired by the unorthodox work of Norman J. Wildberger [Wil05].

Definition 1.3. If $(\mathfrak{A}, *)$ is a $*$-algebra, and X a left $\mathfrak{A}$-module, a map $q\colon \mathsf{X} \to \mathfrak{A}$ is called a *quadrance* on X if

(1) $q(x) = q(x)^*$ for all $x \in \mathsf{X}$
(2) $q(\alpha x) = \alpha q(x) \alpha^*$ for all $x \in \mathsf{X}, \alpha \in \mathfrak{A}$
(3) For $x, y \in \mathsf{X}$ the map $\mathbb{R} \times \mathfrak{A} \to \mathfrak{A}$ given by

$$(\lambda, \alpha) \mapsto q(\lambda x + \alpha y) \tag{1.14}$$

is continuous.

Notice that the square of a norm on a real or complex vector space is obviously a quadrance. In this case, the vector space acquires a norm-topology, in which the norm is continuous, by the "reverse triangle inequality" $\big| \|x\| - \|y\| \big| \leqslant \|x - y\|$, which is an immediate consequence of the "triangle inequality" $\|x + y\| \leqslant \|x\| + \|y\|$ postulated on norms. Notice that we have not endowed the module X with a topology, but we impose the continuity condition (1.14) on a quadrance q. We show below in Proposition 4.1 that the restriction of a Hermitian form to the diagonal is a quadrance. Conversely we have the following generalization of the Jordan-von Neumann theorem to non-commutative scalars:

Theorem 1.3. *Let $(\mathfrak{A}, *)$ be a polarizable $*$-algebra, let X be a left $\mathfrak{A}$-module, and let q be a quadrance on X. Then there is a Hermitian form Q on X such that $q(x) = Q(x, x)$ if and only if q satisfies the* classical parallelogram identity

$$q(x + y) + q(x - y) = 2(q(x) + q(y)), \tag{1.15}$$

for all $x, y \in \mathsf{X}$. If such a form Q exists, then it is unique.

1.7. **Examples.** In the last section of the paper, we show that group algebras of finite groups over the reals, as well as real Clifford algebras are polarizable, and determine some polarizing subgroups, as well as the polarization constants. This gives examples of concrete polarization identities in new contexts. The case of classical Clifford numbers $\mathsf{C}_{0,n}$ associated to negative definite inner products was considered in [GR93]. We also make a few comments about polarizing subgroups in matrix algebras.

2. STRUCTURE OF POLARIZABLE ALGEBRAS

In this section our goal is to prove the first half of Theorem 1.2, i.e., a $*$-algebra is polarizable if and only if it is isomorphic to a $*$-direct sum of matrix algebras over real division rings, each endowed with the conjugate-transpose involution.

2.1. **Involutions on matrix algebras and compact unitary groups.** The following result is needed to prove the existence of isomorphism (1.11):

Proposition 2.1. *Let* $\mathbb{D} = \mathbb{R}, \mathbb{C}$ *or* $\mathbb{H}$ *be a real division algebra, and let* $\sharp$ *be an involution on* $M_n(\mathbb{D})$. *If the involutive algebra* $(M_n(\mathbb{D}), \sharp)$ *is polarizable then it is* $*$-*isomorphic to* $(M_n(\mathbb{D}), *)$ *where* $*$ *is the conjugate-transpose involution of* $M_n(\mathbb{D})$.

The proof will employ brute force, using a classification of all the involutions of the matrix algebras $M_n(\mathbb{D})$, and a characterization of their unitary groups, and then singling out the ones which have polarizable unitary groups. Since we have not been able to locate a full statement of this classification in the literature, we include it below in Proposition 2.2, and sketch a proof based on the general results in [Sch85] on involutions of matrix algebras.

We begin by recalling some facts and introducing some notation to simplify the presentation of this result.

(1) On the quaternions $\mathbb{H}$, it is known that any involution is either the conjugation (1.10), or is a so-called *nonstandard involution* (see [Rod14, Theorem 2.4.4]): an example of a nonstandard involution is the mapping $x \mapsto \widetilde{x}$ given for $x = x_0 + x_1 i + x_2 j + x_3 k$ by

$$\widetilde{x} = x_0 - x_1 i + x_2 j + x_3 k, \tag{2.1}$$

and any other nonstandard evaluation is conjugate to it. A computation shows that the nonstandard involution (2.1) and the conjugation $x \mapsto \overline{x}$ are related by

$$\widetilde{x} = i\overline{x}i^{-1} = -i\overline{x}i. \tag{2.2}$$

Given a matrix A of quaternions, we denote by $\widetilde{A}$ the matrix obtained by applying the involution $\widetilde{\ }$ to each element of A.

(2) Let $J_1 \in M_2(\mathbb{R})$ be the matrix $J_1 = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ and for each positive integer m let J_m be the $2m \times 2m$ block diagonal matrix with m blocks each equal to J_1:

$$J_m = \mathrm{diag}(J_1, \ldots, J_1).$$

(3) Let p, q be nonnegative integers such that $p + q = n$. We denote by $I_{p,q}$ the diagonal matrix where the first p diagonal entries are +1s and the remaining q entries are -1s:

$$I_{p,q} = \operatorname{diag}(1, \ldots, 1, -1, \ldots, -1).$$

Proposition 2.2. *The rows of the following table give a complete list of nonisomorphic involutions on the algebras $M_n(\mathbb{D}), \mathbb{D} = \mathbb{R}, \mathbb{C}, \mathbb{H}$, and characterize the corresponding unitary groups. More precisely, for $\mathbb{D} = \mathbb{R}, \mathbb{C}$ or $\mathbb{H}$, if $\sharp$ is an involution on the real associative algebra $M_n(\mathbb{D})$, then $(M_n(\mathbb{D}), \sharp)$ is $*$-isomorphic to $(M_n(\mathbb{D}), \flat)$, where $\flat$ is an involution in some row of the table in the column "Involution" associated with the algebra $M_n(\mathbb{D})$ in the first column.*

Algebra	No.	Parameters	Involution	Unitary Group
$M_n(\mathbb{R})$	$1_{p,q}$	$p + q = n, p \geqslant q$	$A \mapsto I_{p,q} A^T I_{p,q}$	$O(p, q) = \{A^T I_{p,q} A = I_{p,q}\}$
	2	$n = 2m$ even	$A \mapsto -J_m A^T J_m$	$Sp(2m, \mathbb{R}) = \{A^T J_m A = J_m\}.$
$M_n(\mathbb{C})$	$3_{p,q}$	$p + q = n, p \geqslant q$	$A \mapsto I_{p,q} A^* I_{p,q}$	$U(p, q) = \{A^* I_{p,q} A = I_{p,q}\}$
	4		$A \mapsto A^T$	$O(n, \mathbb{C}) = \{A^T A = I\}$
	5	$n = 2m$ even	$A \mapsto -J_m A^T J_m$	$Sp(2m, \mathbb{C}) = \{A^T J_m A = J_m\}.$
$M_n(\mathbb{H})$	$6_{p,q}$	$p + q = n, p \geqslant q$	$A \mapsto I_{p,q} A^* I_{p,q}$	$Sp(p, q) = \{A^* I_{p,q} A = I_{p,q}\}$
	7		$A \mapsto \widetilde{A}^T$	$Sp_{\mathrm{NS}}(n) = \{\widetilde{A}^T A = I\}$

The rows numbered $1_{p,q}, 3_{p,q}$ and $6_{p,q}$ each stand for multiple rows (and therefore multiple non $*$-isomorphic $*$-algebras), with a separate row for each "signature" (p, q).

If R is an involution of $M_n(\mathbb{D})$, then the restriction of R to the center $\mathbb{K}$ of $M_n(\mathbb{D})$ is a field automorphism of $\mathbb{K}$ fixing $\mathbb{R}$, which is either the identity, or is of order 2. When $\mathbb{D} = \mathbb{R}$ or $\mathbb{H}$, then $\mathbb{K}$ can be identified with $\mathbb{R}$, so all involutions restrict to the identity. On the other hand, if $\mathbb{D} = \mathbb{C}$, the center $\mathbb{K}$ consists of the complex scalar matrices, so an involution can be either restrict to the identity (a so called involution of the *first kind*), or its restriction to the center $\mathbb{K} \cong \mathbb{C}$ of can be the complex conjugation map (an involution is of the *second kind*).

The following is the special case for the base field $\mathbb{R}$ of a well-known result on the classification of involutions of central simple algebras over a field (see [Sch85, Chapter 8, Theorem 7.4]). The proof is straightforward using the Skolem-Noether characterization of automorphisms of simple algebras, and we refer the reader to [Sch85] for details:

Lemma 2.3. *Let $\mathbb{D} = \mathbb{R}, \mathbb{C}$ or $\mathbb{H}$ and n a positive integer.*

(1) Every involution R on $M_n(\mathbb{D})$ is of the form

$$A^R = U A^S U^{-1}, \quad \text{for all } A \in M_n(\mathbb{D}) \tag{2.3}$$

where

(a) S is the transposition map on $M_n(\mathbb{D})$ if $\mathbb{D} = \mathbb{R}$ or $\mathbb{D} = \mathbb{C}$ and R is of the first kind, and the conjugate-transpose map otherwise, and

(b) U is invertible in $M_n(\mathbb{D})$ and satisfies $U^S = \pm U$.

(2) If $\sharp, \flat$ are involutions on $M_n(\mathbb{D})$, then $(M_n(\mathbb{D}), \sharp)$ and $(M_n(\mathbb{D}), \flat)$ are $*$-isomorphic if and only if the following conditions hold:

(a) If $\mathbb{D} = \mathbb{C}$ then both $\flat$ and $\sharp$ are of the first kind or of the second kind.

(b) If

$$A^\sharp = U A^S U^{-1}, \quad A^\flat = V A^S V^{-1}$$

are the representations of the two involutions given by (2.3) *(with S as in part 1(a)), then we have*

$$V = \lambda W U W^S \tag{2.4}$$

with $\lambda \neq 0$ in the center of $\mathbb{D}$ and W inveritible in $M_n(\mathbb{D})$

Proof of Proposition 2.2. In view of Lemma 2.3, the proof is reduced to the determination of equivalence classes in $M_n(\mathbb{D})$ under the equivalence relation (2.4) (so-called *multiplicative congruence*). For $\mathbb{D} = \mathbb{R}, \mathbb{C}$, wherever possible, we will use classical results in linear algebra which classify matrices up to *congruence* (i.e., with $\lambda = 1$ in (2.4)). In the case of the quaternions, we will need to use facts about spectral theory over $\mathbb{H}$. Once involution is reduced to a normal form, the computation of the unitary group of the last column is straightforward.

The case $\mathbb{D} = \mathbb{R}$. Thanks to Lemma 2.3 each involution $M_n(\mathbb{R})$ is of the form $A \mapsto U A^T U^{-1}$ where $A \mapsto A^T$ is the transposition operation, and $U^T = \pm U$, i.e. U is either symmetric or anti-symmetric . We consider the two cases separately.

(1) *U symmetric.* The eigenvalues of the symmetric and invertible matrix U are real and nonzero, and suppose that U has p positive and $q = n - p$ negative eigenvalues. By the real form of Sylvester's Law of of Inertia ([Her75, Theorem 6.11.1]), the invertible symmetric matrix U is congruent to the matrix $I_{p,q}$, i.e., there is a matrix W such that $I_{p,q} = W U W^T$. If $p \geqslant q$, this shows that $I_{p,q}$ and U are multiplicatively congruent. If $q > p$ then the relation $I_{q,p} = (-1) W U W^T$ holds, showing that U is multiplicatively congruent to $I_{q,p}$. Case $1_{p,q}$ of the table follows, on noting that $I_{p,q}^{-1} = I_{p,q}$.

(2) *U is anti-symmetric.* Using the real spectral theorem, it is not difficult to show that (see [HJ13, Corollary 2.5.11]) $n = 2m$ is even and there is an orthogonal matrix $V \in O(n)$ such that $U = V \operatorname{diag}(r_1 J_1, \ldots, r_m J_1) V^T$, where each $r_j > 0$. Taking $W = V \operatorname{diag}(\sqrt{r_1}, \sqrt{r_1}, \ldots, \sqrt{r_m}, \sqrt{r_m})$, we see that $U = W J_m W^T$, so U is (multiplicatively) congruent to J_m, and consequently by Lemma 2.3, the involution $\sharp$ is equivalent to the involution $A \mapsto J_m A^T J_m^{-1} = -J_m A^T J_m$ of row 2, since $J_m^{-1} = -J_m$.

The case $\mathbb{D} = \mathbb{C}$. Given an involution on $M_n(\mathbb{C})$, it can be either of the first or second kind. We consider these two cases separately.

First suppose that we are given an involution of the first kind on $M_n(\mathbb{C})$, i.e., it acts as the identity on the complex scalar matrices that form the center of $M_n(\mathbb{C})$. Then by Lemma 2.3, such an involution of is of the form $A \mapsto U A^T U^{-1}$ where $A \mapsto A^T$ is the transposition involution on complex matrices and $U^T = \pm U$. Again we consider the two cases:

(1) *U symmetric, i.e. $U^T = U$.* By a classical result of linear algebra (see [HJ13, Theorem 4.5.12]) for the nonsingular complex symmetric matrix U, there is an invertible W such that $W U W^T = I$, which shows that U is (multiplicatively) congruent to the identity matrix I. The case of row 4 follows.

(2) *U is anti-symmetric, i.e. $U^T = -U$.* By an application of the spectral theorem (see [Hua44, Theorem 7, p. 481]) we can show that there is a V such that we have

$$U = V \operatorname{diag}(r_1 J_1, \ldots, r_m J_1) V^T$$

where $n = 2m$ (and hence even) and each $r_j > 0$. Now we take

$$W = V \operatorname{diag}(\sqrt{r_1}, \sqrt{r_1}, \ldots, \sqrt{r_m}, \sqrt{r_m}),$$

and see that $U = W J_m W^T$, so U is (multiplicatively) congruent to J_m, and consequently by Lemma 2.3, we get row 5.

Now suppose that we are given an involution of the second kind on $M_n(\mathbb{C})$, so that by Lemma 2.3, we see that such an involution is of the form $A \mapsto U A^* U^{-1}$, where $A \mapsto A^*$ is the standard conjugate-transpose involution of the algebra $M_n(\mathbb{C})$, and $U^* = \pm U$. We consider the two cases

(1) U *is Hermitian, i.e.* $U^* = U$. This case is similar to the case of row number $1_{p,q}$, using the Hermitian version of Sylvester's Law of Inertia ([HJ13, Theorem 4.5.8]) , which shows that there is a $W \in GL_n(\mathbb{C})$ such that $I_{p,q} = W U W^*$, where p and q are the numbers of positive and negative eigenvalues of the matrix U. If $p < q$ we again write $(-1) W U W^* = I_{q,p}$. This gives row $3_{p,q}$ of the table.

(2) U *is Skew-Hermitian, i.e.* $U^* = -U$ Since $(iU)^* = iU$, by the arguments of the preceding case there is a signature (p, q) and a matrix W such that

$$I_{p,q} = W(iU)W^* = iWUW^*$$

If $p < q$ we again have $I_{q.p} = -iWUW^*$, so we have that U is multiplicatively congruent to one of the matrices $I_{p,q}$ with $p \geqslant q$, and we are again in row $3_{p,q}$.

The case $\mathbb{D} = \mathbb{H}$. We will use the following quaternionic version of the spectral theorem, where the quaternions of the form $a + ib, a, b \in \mathbb{R}$ (i.e. quaternions with vanishing j and k components) are identified with the complex numbers $\mathbb{C}$:

Result: (see [FP03], and cf. [Rod14, Theorem 4.1.12]) *Suppose $U \in M_n(\mathbb{H})$ is a normal matrix, i.e. $U^*U = UU^*$. Then there exists a $V \in Sp(n)$ and a diagonal matrix D with entries in the closed upper half plane in $\mathbb{C} \subset \mathbb{H}$ such that $U = VDV^*$.*

By Lemma 2.3 every involution on $M_n(\mathbb{H})$ is of the form $A \mapsto U A^* U^{-1}$ where $U \in GL_n(\mathbb{H})$ is such that $U^* = \pm U$. In both cases, U is normal so that we can apply the quaternionic spectral theorem as stated above.

(1) U *is quaternionic Hermitian, i.e.* $U^* = U$: Then there exists a $V \in Sp(n)$ such that $V^*UV = D$, a diagonal with values in the upper half plane. Further $D^* = V^*U^*V = V^*UV = D$ and it follows that D is a real diagonal matrix. Applying the argument used to deduce Sylvester's law of inertia from the spectral theorem (see the proof of [Her75, Theorem 6.11.1]), we see that there are $p, q \geqslant 0, p + q = n$ and $W \in GL_n(\mathbb{H})$ such that $I_{p,q} = WUW^*$. Again if $q > p$, we can write $I_{q,p} = (-1)WUW^*$, showing that U is multiplicatively congruent to $I_{p,q}$ for some $p \geqslant q$.

(2) U *is quaternionic skew-Hermitian, i.e.* $U^* = -U$ If $U^* = -U$, then there exists a $V \in Sp(n)$ such that $V^*UV = D$, a diagonal matrix with values in the upper half plane. In this case, however, $D^* = V^*U^*V = -V^*UV = -D$ and it follows that $D = \operatorname{diag}(ir_1, \ldots, ir_n)$ where each $r_j > 0$ is a positive real number. Setting

$$W = V \operatorname{diag}\left(\sqrt{r_1}, \ldots, \sqrt{r_n}\right)$$

yields $U = W(iI)W^*$, so that the the algebra $M_n(\mathbb{H})$ with this involution is $*$-isomorphic to the algebra $(M_n(\mathbb{H}), \sharp)$, where $A^\sharp = (iI)A^*(iI)^{-1} = iA^*i^{-1}$. Denoting the entry in the λ-th row and μ-th column of the matrix A by $(a_{\lambda\mu})$, we see using (2.2) that the (λ, μ)-th entry of iA^*i^{-1} is

$$i \cdot \overline{a_{\mu,\lambda}} \cdot i^{-1} = \widetilde{a}_{\mu,\lambda},$$

where the tilde denotes the nonstandard involution of (2.1). Therefore, we get the invo-
lution $A \mapsto \widetilde{A}^T$ of row (7) of the table (cf. [Rod14, section 3.6]) and it is clear that the
corresponding unitary group is $\{\widetilde{A}^T A = I\}$, which does not seem to have a standard name
in the literature, but perhaps may be called the nonstandard symplectic group $Sp_{\mathrm{NS}}(n)$.

$\hfill\square$

Proof of Proposition 2.1. We will show that if $\sharp$ is not the conjugate-transpose involution
on $M_n(\mathbb{D})$, then the algebra $(M_n(\mathbb{D}), \sharp)$ is not polarizable, i.e., the unitary groups in the
table of Proposition 2.2 except those in rows $1_{n,0}, 3_{n,0}$ and $6_{n,0}$ are not compact or do not
generate $M_n(\mathbb{D})$.

When $n = 1$, and $\mathbb{D} = \mathbb{R}$, the the only possibility is row $1_{1,0}$ so there is nothing to show.
For $\mathbb{D} = \mathbb{C}$ the only possibility (except $3_{1,0}$) is row 4, where the unitary group is

$$\Gamma(M_1(\mathbb{C}), \mathrm{id}) = \{z \in M_1(\mathbb{C}) = \mathbb{C} : z^2 = 1\} = \{\pm 1\}.$$

The linear span of this group is $\mathbb{R}$ and therefore it is not polarizing. For $\mathbb{D} = \mathbb{H}$, the only
possibility we need to consider is 7, where the unitary group is

$$\{a \in \mathbb{H} : \widetilde{a}a = 1_{\mathbb{H}}\}.$$

It is easy to see that a quaternion satisfying this system of four real equations are of the
form $a = \cos\theta + i\sin\theta$ for some $\theta \in \mathbb{R}$. Therefore, the unitary group in this case generates
a subalgebra of $\mathbb{H}$ isomorphic $\mathbb{C}$, and not the whole of $\mathbb{H}$. The result is proved when $n = 1$.

Now let $n \geqslant 2$. In the numbering system of the table in Proposition 2.2, the conjugate
transpose involutions correspond to rows $1_{n,0}$ (for $\mathbb{R}$), $2_{n,0}$ (for $\mathbb{C}$) and $6_{n,0}$ (for $\mathbb{H}$). We
will show that all the other groups in the table are noncompact, thus showing that they
are nonpolarizable. If $n = 2$ and $p = q = 1$, for number $1_{1,1}$ it is well-known that the
group $O(1, 1)$ is not compact, which can be seen for example by looking at the sequence
of matrices

$$\frac{1}{2} \begin{pmatrix} n + \dfrac{1}{n} & n - \dfrac{1}{n} \\[2mm] n - \dfrac{1}{n} & n + \dfrac{1}{n} \end{pmatrix}$$

in $O(1, 1)$ which does not have a limit point. Now since $O(1, 1)$ can be embedded as a
closed subgroup of $O(p, q)$ if $n \geqslant 3$ it follows that $O(p, q)$ is noncompact if $p \geqslant q \geqslant 1$.

The inclusions $O(p, q) \subset U(p, q) \subset Sp(p, q)$ (obtained by extending scalars) show that
rows $3_{p,q}$ and $6_{p,q}$ also have noncompact unitary groups if $p, q \geqslant 1$.

In row no. 4, the group $O(n, \mathbb{C})$ is a complex affine variety in $\mathbb{C}^{n^2} = M_n(\mathbb{C})$ of dimension
equal to that of the Lie algebra $\{A + A^T = 0\}$ which is therefore $\frac{1}{2}n(n-1)$. If $n \geqslant 2$, this
is at least 1, so $O(n, \mathbb{C})$ is noncompact.

The map $f : \mathbb{C} \to \mathbb{H}$ given by $f(x + iy) = x + jy$ is an $\mathbb{R}$-algebra monomorphism, and
satisfies $f(x) = \widetilde{f(x)}$ for each x, where the tilde has the same meaning as in (2.1). We
may therefore define an algebra homomomorphism $f : M_n(\mathbb{C}) \to M_n(\mathbb{H})$ by applying it
elementwise. This maps the group $O(n, \mathbb{C})$ into a closed subgroup of the group $Sp_{\mathrm{NS}}(n) = \{\widetilde{A}^T A = I\}$, which is therefore noncompact.

Using the formula for the inverse of a 2×2 matrix, we see that a matrix $A \in M_2(\mathbb{R})$
satisfies the condition $A^T J_1 A = J_1$ if and only if $\det A = 1$, so $Sp(2, \mathbb{R}) = SL(2, \mathbb{R})$.
The noncompactness of $SL(2, \mathbb{R})$ can be seen, e.g., by looking at the sequence of matrices

$\left\{ \begin{pmatrix} n & 1 \\ n-1 & 1 \end{pmatrix} \right\}$. Using the obvious inclusion of $Sp(2, \mathbb{R})$ in $Sp(2m, \mathbb{R})$ we see that the latter is noncompact for each $m \geqslant 1$. Similarly, the inclusion of $Sp(2m, \mathbb{R})$ in $Sp(2m, \mathbb{C})$ shows that the latter is noncompact. This completes the proof. $\qquad\square$

2.2. **Semisimplicity of polarizable algebras.** We begin with the following simple application of the Weyl averaging trick:

Proposition 2.4. *Let $(\mathfrak{A}, *)$ be an involutive algebra and suppose there is a compact subgroup G of $\Gamma(\mathfrak{A}, *)$ which generates $\mathfrak{A}$. Then*

(1) *there exists an inner product on the $\mathbb{R}$-vector space $\mathfrak{A}$:*

$$\langle \cdot, \cdot \rangle : \mathfrak{A} \times \mathfrak{A} \to \mathbb{R}$$

such that for $\alpha, \beta, \eta \in \mathfrak{A}$ we have

$$\langle \eta \alpha, \beta \rangle = \langle \alpha, \eta^* \beta \rangle. \tag{2.5}$$

(2) *the $*$-algebra $(\mathfrak{A}, *)$ is $*$-isomorphic to a $*$-subalgebra of $(M_n(\mathbb{R}), T)$, were $n = \dim_{\mathbb{R}} \mathfrak{A}$ (as a vector space) and T denotes the transposition involution.*

(3) *the $*$-algebra $(\mathfrak{A}, *)$ is polarizable.*

Proof. (1) Let $\langle \cdot, \cdot \rangle_0 : \mathfrak{A} \times \mathfrak{A} \to \mathbb{R}$ be a real inner product on $\mathfrak{A}$, i.e. a positive-definite, symmetric, bilinear form. Then

$$\langle \alpha, \beta \rangle := \int_G \langle g\alpha, g\beta \rangle_0 \, dg$$

is also an inner product, and by Haar invariance we have for this inner product for each $g \in G$, $\alpha, \beta \in \mathfrak{A}$ that

$$\langle g\alpha, g\beta \rangle = \langle \alpha, \beta \rangle. \tag{2.6}$$

Therefore

$$\langle h\alpha, \beta \rangle = \langle h\alpha, hh^* \beta \rangle = \langle \alpha, h^* \beta \rangle$$

for $\alpha, \beta \in \mathfrak{A}$ and $h \in G$. By the $\mathbb{R}$-bilinearity of the inner product, and the fact that $\mathfrak{A} = \mathrm{span}_{\mathbb{R}} G$ the equality (2.5) follows.

(2) Let

$$\rho : \mathfrak{A} \to \mathrm{End}_{\mathbb{R}}(\mathfrak{A}) \tag{2.7}$$

be the injective $\mathbb{R}$-algebra homomorphism given by $\rho(\alpha)(\beta) = \alpha\beta$. On the endomorphism algebra $\mathrm{End}_{\mathbb{R}}(\mathfrak{A})$ there is an involution $\sharp$ given by taking adjoints with respect to the inner product of part (1) above, i.e. for an $\mathbb{R}$-linear map $A : \mathfrak{A} \to \mathfrak{A}$, the map $A^\sharp : \mathfrak{A} \to \mathfrak{A}$ is characterized by the fact that $\langle A\alpha, \beta \rangle = \langle \alpha, A^\sharp \beta \rangle$. Notice that (2.5) says that for each $\eta \in \mathfrak{A}$, we have $\rho(\eta)^\sharp = \rho(\eta^*)$, i.e., ρ is a $*$-homomorphism from $(\mathfrak{A}, *)$ into $(\mathrm{End}_{\mathbb{R}}(\mathfrak{A}), \sharp)$, which is known to be injective, so that $(\mathfrak{A}, *)$ is isomorphic to a $*$-subalgebra of $(\mathrm{End}_{\mathbb{R}}(\mathfrak{A}), \sharp)$. Now choosing a basis of the $\mathbb{R}$-vector space $\mathfrak{A}$, the algebra $(\mathrm{End}_{\mathbb{R}}(\mathfrak{A}), \sharp)$ is $*$-isomorphic to $(M_n(\mathbb{R}), *)$ and the result follows.

(3) Identifying $\mathrm{End}_{\mathbb{R}}(\mathfrak{A})$ with the matrix algebra $M_n(\mathbb{R})$ by choosing a basis, we see that the map ρ of (2.7)

$$\Gamma(\mathfrak{A}, *) = \rho^{-1}(O(n)),$$

where $O(n)$ is the orthogonal group. Since ρ, being linear and injective, is topologically a proper map, it follows that $\Gamma(\mathfrak{A}, *)$ is compact. Since the subgroup G of $\Gamma(\mathfrak{A}, *)$ generates $\mathfrak{A}$, it follows a fortiori that $\Gamma(\mathfrak{A}, *)$ generates $\mathfrak{A}$. The result follows.

$\qquad\square$

We are now ready to prove the first half of Theorem 1.2, which we state as a separate proposition for convenience. It can be thought of as a version of Maschke's theorem.

Proposition 2.5. *Let $(\mathfrak{A}, *)$ be a polarizable $*$-algebra. Then there is a $*$-isomorphism*

$$\phi : \bigoplus_{j=1}^{N}(M_{n_j}(\mathbb{D}_j), *) \to (\mathfrak{A}, *), \tag{2.8}$$

where in the left is the $*$-direct sum of a a finite number of matrix algebras over real division rings, each endowed with the "conjugate-transpose" involution.

Proof. Let $\mathfrak{j}$ be a left ideal in the algebra $\mathfrak{A}$, and let $\mathfrak{k}$ be the $\mathbb{R}$-linear subspace of $\mathfrak{A}$ which is its orthogonal complement with respect to the inner product of Proposition 2.4, i.e.

$$\mathfrak{k} = \{\alpha \in \mathfrak{A} : \langle \alpha, \beta \rangle = 0, \text{ for each } \beta \in \mathfrak{j}\}.$$

Now, $\mathfrak{k}$ is also a left ideal in the algebra $\mathfrak{A}$, since by (2.5), we have for $\alpha \in \mathfrak{k}$ and $\eta \in \mathfrak{A}$,

$$\langle \eta\alpha, \beta \rangle = \langle \alpha, \eta^*\beta \rangle = 0,$$

for each $\beta \in \mathfrak{j}$ since $\mathfrak{j}$ is a left ideal. It follows that $\mathfrak{A}$ is semisimple as a left module over itself, i.e., it is a semisimple $\mathbb{R}$-algebra. By a famous theorem of Wedderburn (e.g. [Lam01]), the algebra $\mathfrak{A}$ is isomorphic to a direct sum of matrix algebras over $\mathbb{R}$-division algebras. This shows the existence of an isomorphism of $\mathbb{R}$-algebras:

$$\phi : \bigoplus_{j=1}^{N} M_{n_j}(\mathbb{D}_j) \to \mathfrak{A},$$

where for each j, $\mathbb{D}_j$ is one of the three real division algebras.

Let $\sharp$ denote the involution on the algebra $\mathfrak{B} = \bigoplus_{j=1}^{N} M_{n_j}(\mathbb{D}_j)$ obtained by pulling back the involution $*$ of $\mathfrak{A}$ via ϕ, so that ϕ is a $*$-isomorphism of $\mathfrak{B}$ with $\mathfrak{A}$: $\phi(x^\sharp) = \phi(x)^*$. We will now show that the involution $\sharp$ preserves the direct sum structure of $\mathfrak{B}$, i.e., there exists for each j, an involution $\sharp_j$ of $M_{n_j}(\mathbb{D}_j)$ such that

$$(x_1, \ldots, x_N)^\sharp = (x_1^{\sharp_1}, \ldots, x_n^{\sharp_n}),$$

i.e. $\mathfrak{B}$ is the $*$-direct sum of the algebras $(M_{n_j}(\mathbb{D}_j), \sharp_j)$.

For each j, let $\mathfrak{a}_j$ be the image of the algebra $M_{n_j}(\mathbb{D}_j)$ in the direct sum $\mathfrak{B}$ under the canonical inclusion, so that $\mathfrak{a}_j$ is a minimal two-sided ideal in $\mathfrak{B}$. If $\sharp$ does not preserve the direct sum structure of $\mathfrak{B}$, there is a j such that $\sharp$ maps $\mathfrak{a}_j$ to $\mathfrak{a}_k$ for some $k \neq j$ (this follows from the minimality of the two-sided ideals $\mathfrak{a}_\ell$.) Without loss of generality assume that $j = 1, k = 2$ (and therefore $n_1 = n_2$, and $\mathbb{D}_1 = \mathbb{D}_2$). For each positive integer n, consider the element $u_n \in \mathfrak{B}$ given by

$$u_n = \left(nI_1, \frac{1}{n}I_2, I_3, \ldots, I_N\right),$$

where I_j is the identity of $M_{n_j}(\mathbb{D}_j)$. Then it follows that

$$u_n^\sharp = \left(\frac{1}{n}I_1, nI_2, I_3, \ldots, I_N\right)$$

so that $u_n u_n^\sharp$ is the identity element of $\mathfrak{B}$, and consequently $u_n \in \Gamma(\mathfrak{B}, \sharp)$. It follows that $\Gamma(\mathfrak{B}, \sharp)$ is not compact, but since ϕ is a $*$-isomorphism, we have that $\Gamma(\mathfrak{A}, *)$ is also noncompact, which contradicts the assumption that $(\mathfrak{A}, *)$ is polarizable.

Therefore we have $(\mathfrak{B}, \sharp) = \bigoplus_{j=1}^{N} (M_{n_j}(\mathbb{D}_j), \sharp_j)$, a $*$-direct sum, where $\sharp_j$ denotes the restriction of $\sharp$ to $\mathfrak{a}_j$, which can be identified with $M_{n_j}(\mathbb{D}_j)$. Since $(\mathfrak{B}, \sharp)$ is polarizable, it easily follows that each summand $(M_{n_j}(\mathbb{D}_j), \sharp_j)$ is also polarizable. By Proposition 2.1, it follows that each $\sharp_j$ is the conjugate transpose involution.

$\square$

2.3. Polarizability of matrix algebras.

In this subsection, we will prove that a finite $*$-direct sum of matrix algebras over division algebras is polarizable. We note some properties of the vector-valued integral (1.3) defined by the condition (1.4):

(1) If $f : G \to V$ is a continuous function on the group G with values in a finite dimensional real vector space V, W is another finite dimensional real vector space and $T : V \to W$ is an $\mathbb{R}$-linear map, then we have:

$$T \left(\int_G f dg \right) = \int_G (T \circ f) \, dg \tag{2.9}$$

where now the integral on the right is the vector-valued integral of a W-valued function on G. The relation (2.9) is easily verified using the defining condition (1.4).

(2) Again, let $f : G \to V$ be a continuous function on the group G with values in a finite dimensional real vector space V. Then we have

$$\int_G f dg \in \operatorname{span}_{\mathbb{R}} (f(G)), \tag{2.10}$$

where $f(G) = \{f(g) : g \in G\} \subset V$ is the image of the map f. To see (2.10), let $W = \operatorname{span}_{\mathbb{R}} (f(G))$, and let $\pi : V \to V/W$ be the quotient map. Then by (2.9),

$$\pi \left(\int_G f dg \right) = \int_G \pi(f(g)) dg = 0,$$

which shows that $\int_G f dg \in W$. With a little more work, one can show that $\int_G f dg$ belongs to the convex hull of $f(G)$, but we do not need this.

We also recall a few definitions. Let $\sigma \in S_n$ be a permutation, i.e., a bijection of $\{1, \ldots, n\}$ with itself. We can associate with σ an $n \times n$ *permutation matrix* P_σ, where the j-th column of P_σ is $e_{\sigma(j)}$ for $1 \leqslant j \leqslant n$, with e_i denoting the $n \times 1$ column matrix with an 1 in the i-th place and 0's everywhere else. It is clear that $P_\sigma e_j = e_{\sigma(j)}$. Given a group H of permutation matrices, we say that it is *transitive* if the corresponding permutations act transitively on the set $\{1, \ldots, n\}$.

Proposition 2.6. *Let $(\mathfrak{A}, \sharp)$ be a $*$-algebra, and let $G \subset \Gamma(\mathfrak{A}, \sharp)$ be a polarizing group. Let $n \geqslant 2$ and let $\Delta_G \subset M_n(\mathfrak{A})$ be the collection of $n \times n$ diagonal matrices with the diagonal entries taken from G:*

$$\Delta_G = \{\operatorname{diag}(g_1, \ldots, g_n) \in M_n(\mathfrak{A}) : g_j \in G\},$$

and let H be a transitive group of permutation matrices in $M_n(\mathfrak{A})$. Then the set

$$\Delta_G H = \{DP : D \in \Delta_G, P \in H\}$$

is a compact subgroup of $(M_n(\mathfrak{A}), *)$ which is polarizing, where $*$ is the involution induced on $M_n(\mathfrak{A})$ by the involution $\sharp$ of $\mathfrak{A}$ as in (1.9).

Proof. It is clear that $\Delta_G \cong G^n$ is a compact group as a Cartesian power of the compact group G and $\Delta_G H$ is compact as a union of finitely many homeomorphic copies of Δ_G. If $D \in \Delta_G$, we can write $D = \operatorname{diag}(g_1, \ldots, g_n)$ for $g_j \in G, 1 \leqslant j \leqslant n$, so that we have

$$D^*D = \operatorname{diag}(g_1^\sharp, \ldots, g_n^\sharp) \cdot \operatorname{diag}(g_1, \ldots, g_n) = \operatorname{diag}(1_\mathfrak{A}, \ldots, 1_\mathfrak{A}).$$

since $G \subset \Gamma(\mathfrak{A}, \sharp)$ by hypothesis. Also, we have for a permutation matrix $P \in M_n(\mathfrak{A})$:

$$P^*P = (P^\sharp)^T P = P^T P = I.$$

It follows that $\Delta_G H$ is a compact subset of the unitary group $\Gamma(M_n(\mathfrak{A}), *)$.

A direct computation shows that for each $\sigma \in S_n$, and $D \in \Delta_G$ we have

$$(P_\sigma)^{-1} D P_\sigma = P_{\sigma^{-1}} D P_\sigma = D' \in \Delta_G \tag{2.11}$$

where D' is a diagonal matrix whose nonzero nonzero entries are a permutation of the diagonal entries of D. More precisely, if $D = \operatorname{diag}(g_1, \ldots, g_n)$ where $g_j \in G$, then $D' = \operatorname{diag}(g_{\sigma(1)}, \ldots, g_{\sigma(n)})$.

The relation (2.11) shows not only that $\Delta_G H$ is a group, but also that Δ_G is normal subgroup of the group $\Delta_G H$. The intersection $\Delta_G \cap H$ consists of diagonal matrices which are permutation matrices and therefore is $\{I\}$. It folows that $\Delta_G H$ is the (internal) semidirect product of the two subgroups Δ_G and H. Since on a semidirect product, the Haar measure is equal to the product measure (e.g. [Nac76, pp. 96ff.]), we have, using Fubini's theorem:

$$\int_{\Delta_G H} g\,dg = \int_H \int_{\Delta_G} DP\,dD\,dP = \left(\int_{\Delta_G} D\,dD \right) \cdot \left(\int_H P\,dP \right) = 0 \cdot \left(\int_H P\,dP \right) = 0,$$

using the fact that G is polarizable so (1.6) holds.

We now show that $\Delta_G H$ generates $M_n(\mathfrak{A})$. Let $E_{i,j}$ be the $n \times n$ matrix with $1_\mathfrak{A}$ in the i-th row and j-th column and zeros everywhere else. First we show that $E_{i,j}$ is in the subalgebra of $M_n(\mathfrak{A})$ generated by the group $\Delta_G H$. For $1 \leqslant j \leqslant n$ and $g \in G$, denote by $D_j(g) \in \Delta_G$ the diagonal matrix with a $1_\mathfrak{A}$ in the j-th place and and g in each other place. Then we clearly have, using (1.6) that $E_{j,j} = \int_G D_j(g)\,dg$. It follows by (2.10) that $E_{j,j}$ is in the algebra generated by Δ_G. Now observe that

$$E_{i,j} e_k = \begin{cases} e_i & k = j \\ 0 & \text{otherwise} \end{cases}.$$

Since H is transitive, by definition there exists a $P \in H$ such that $Pe_j = e_i$, so that

$$PE_{j,j} e_k = \begin{cases} Pe_j = e_i & k = j \\ P(0) = 0 & \text{otherwise} \end{cases}.$$

Hence $PE_{j,j} = E_{i,j}$, so that $\Delta_G H$ generates all of the $E_{i,j}$.

Now we note that αI is generated by $\Delta_G H$ for each $\alpha \in \mathfrak{A}$. Since G generates $\mathfrak{A}$, there exist $g_1, \ldots g_n \in G$ and $\lambda_1, \ldots, \lambda_n \in \mathbb{R}$ so that $\alpha = \sum \lambda_i g_i$. Hence $\alpha I = \sum_{i=1}^n \lambda_i(g_i I)$, where each $g_i I \in \Delta_G$. Writing a matrix $A = (\alpha_{i,j}) \in M_n(\mathfrak{A})$ as

$$A = \sum_{i,j=1}^n (\alpha_{i,j} I) \cdot E_{i,,j}$$

we see that $\Delta_G H$ is a polarizing subgroup of $M_n(\mathfrak{A})$. $\qquad \square$

From this we deduce the following:

Proposition 2.7. *A ∗-algebra which is ∗-isomorphic to a finite ∗-direct sum of matrix algebras over real division algebras, each endowed with the conjugate-transpose involution, is polarizable.*

Proof. From part (3) of Proposition 2.4 it follows that a ∗-algebra is polarizable if and only if it has a compact subgroup of the unitary group whose $\mathbb{R}$-linear span is the whole algebra. In particular, any ∗-algebra which admits a polarizing subgroup is polarizable.

Using this criterion it is easy to see that $\mathbb{R}$, $\mathbb{C}$ and $\mathbb{H}$ are each polarizable if endowed with the standard conjugation operation. Indeed, each of the finite groups $\{\pm 1\}, \{\pm 1, \pm i\}$ and $\{\pm 1, \pm i, \pm j, \pm k\}$ consist of unitary elements in $\mathbb{R}, \mathbb{C}$ and $\mathbb{H}$ respectively and span the respective division algebra.

Therefore, by Proposition 2.6, the ∗-algebra $(M_n(\mathbb{D}), \ast)$, where the involution ∗ is the standard conjugate-transpose operation, is polarizable, where $\mathbb{D}$ is one of $\mathbb{R}, \mathbb{C}, \mathbb{H}$. Notice also that the ∗-direct sum of a finite number of polarizable ∗-algebras is easily seen to be polarizable. Therefore the ∗-direct sum $\bigoplus_{j=1}^{N}(M_{n_j}(\mathbb{D}_j)\ast)$ is polarizable. Finally polarizability is clearly preserved by ∗-isomorphisms, so the result follows. $\qquad\square$

3. Proof of Theorems 1.1 and 1.2

3.1. **Integrals on compact multiplicative groups.** Let $\mathfrak{A}$ be a ∗-algebra and let G be a compact subgroup of $\mathfrak{A}^{\times}$, the group of units (i.e. invertible elements) of $\mathfrak{A}$. For an integer $k \geqslant 0$, we define the k-th *moment* of G to be the element of $\mathfrak{A}$ given by

$$\mu_k(G) = \int_G g^k dg, \tag{3.1}$$

where the integral is that of the $\mathfrak{A}$-valued function $g \mapsto g^k$ taken with respect to the normalized Haar measure of the compact group G, defined as in (1.4). The relation (2.9) will be used repeatedly without further comments in the computations below. We now collect some basic information about moments.

Proposition 3.1. *For each compact subgroup $G \subset \mathfrak{A}^{\times}$ and each integer $k \geqslant 0$, the element $\mu_k(G)$ belongs to the subalgebra $\mathfrak{B}$ of $\mathfrak{A}$ generated by G, and in fact lies in the center of $\mathfrak{B}$, i.e., for each $h \in \mathfrak{B}$, we have $h\mu_k(G) = \mu_k(G)h$.*

Proof. Since G being a group is closed under multiplication in $\mathfrak{A}$, one sees easily that $\mathfrak{B} = \mathrm{span}_{\mathbb{R}}G$, i.e. the algebra $\mathfrak{B}$ generated by G coincides with the linear span of the subset of G of the $\mathbb{R}$-vector space $\mathfrak{A}$. However the integrand of the vector-valued integral (3.1) takes values in the linear subspace $\mathfrak{B}$ of $\mathfrak{A}$, and therefore by (2.10) the value of the integral lies in $\mathfrak{B}$. Now let $h \in G$, then

$$h\mu_k(G)h^{-1} = \int_G hg^k h^{-1}dg = \int_G (hgh^{-1})^k dg = \int_G g^k dg = \mu_k(G),$$

using the invariance of the Haar measure. Therefore, we have for each $h \in G$ that $h\mu_k(G) = \mu_k(G)h$. Since $\mathfrak{B}$ is the collection of real linear combinations of the elements of G, it follows that the same relation holds for $h \in \mathfrak{B}$ as well. $\qquad\square$

We now compute the first and second moments of a group under appropriate hypotheses.

Proposition 3.2. *Let $G \subset \mathfrak{A}^{\times}$ be a compact subgroup and suppose that one of the following hold:*

(a) $-1_{\mathfrak{A}} \in G$,
(b) $G \neq \{1_{\mathfrak{A}}\}$ and the subalgebra $\mathfrak{B}$ of $\mathfrak{A}$ generated by G is simple (i.e. has no nontrivial two sided ideals).

Then we have

$$\mu_1(G) = 0.$$

Proof. If condition (a) holds, then by the invariance of Haar measure

$$\mu_1(G) = \int_G (-1_{\mathfrak{A}})g\,dg = -\mu_1(G).$$

Now, assume (b). If $\mathfrak{B} = \mathbb{R}$, then by the nontriviality of G, we must have $G = \{\pm 1_{\mathfrak{A}}\}$, so that $\mu_1(G) = \frac{1}{2}(1 - 1) = 0$. Assuming therefore that $\mathfrak{B} \neq \mathbb{R}$, since by Proposition 3.1, the element $\mu_1(G)$ is in the center of $\mathfrak{B}$ it follows that the set $\mathfrak{J} = \{h : h\mu_1(G) = 0\}$ is a two sided ideal in $\mathfrak{B}$. Since $\mathfrak{B} \neq \mathbb{R}$, there are two $\mathbb{R}$-linearly independent elements $g_1, g_2 \in G$. If we let $h = g_1 - g_2$, we have $0 \neq h \in \mathfrak{J}$ since

$$h\mu_1(G) = \int_G g_1 g\,dg - \int_G g_2 g\,dg = \int_G g\,dg - \int_G g\,dg = 0.$$

By simplicity of $\mathfrak{B}$, $\mathfrak{J}$ is all of $\mathfrak{B}$. It follows that $\mu_1(G) = 1_{\mathfrak{A}} \cdot \mu_1(G) = 1\mu_1(G) = 0$. $\qquad \square$

The following proposition summarizes the properties of the second moment that we will need in our application:

Proposition 3.3. *Let $(\mathfrak{A}, *)$ be a $*$-algebra, and $G \subset \Gamma(\mathfrak{A}, *)$ be a compact subgroup of unitary elements of $\mathfrak{A}$ that generates $\mathfrak{A}$. Then for each $\alpha \in \mathfrak{A}$, we have*

$$\int_G g\alpha g\,dg = \alpha^* \mu_2(\Gamma(\mathfrak{A}, *)). \tag{3.2}$$

Remark: Thanks to part (3) of Proposition 2.4, we know that the unitary group $\Gamma(\mathfrak{A}, *)$ is compact, and therefore $\mu_2(\Gamma(\mathfrak{A}, *))$ makes sense. Taking $\alpha = 1_{\mathfrak{A}}$ in (3.2), we have the remarkable fact that in a polarizable $*$-algebra $(\mathfrak{A}, *)$:

$$\mu_2(G) = \mu_2(\Gamma(\mathfrak{A}, *)), \tag{3.3}$$

for each compact subgroup G of $\Gamma(\mathfrak{A}, *)$ which generates the algebra $\mathfrak{A}$. For a polarizable algebra $(\mathfrak{A}, *)$ we will denote, by abuse of notation,

$$\mu_2(\mathfrak{A}) = \mu_2(\Gamma(\mathfrak{A}, *)).$$

we refer to the element $\mu_2(\mathfrak{A}) \in \mathfrak{A}$ as the the *second moment* of the polarizable algebra $(\mathfrak{A}, *)$.

Proof. For each $h \in G$ we have, by an application of Haar invariance, that

$$\int_G ghg\,dg = h^*h \int_G ghg\,dg = h^* \int_G (hg)^2\,dg = h^* \int_G g^2\,dg = h^*\mu_2(G),$$

using the fact that $hh^* = 1_{\mathfrak{A}}$. Since $\operatorname{span}_{\mathbb{R}} G = \mathfrak{A}$, we can write each $\alpha \in \mathfrak{A}$ as a finite sum $\alpha = \sum \lambda_j h_j$ for $h_1, \ldots, h_n \in G$ and $\lambda_1, \ldots, \lambda_n \in \mathbb{R}$. Hence

$$\int_G g\alpha g\,dg = \sum_{j=1}^n \lambda_j \int_G gh_j g\,dg = \sum_{j=1}^n \lambda_j h_j^* \int_G g^2\,dg = \alpha^*\mu_2(G). \tag{3.4}$$

To complete the proof we need to establish the relation (3.3). This is obtained from the following computation:

$$\mu_2(G) = \mu_2(G) \cdot \int_{\Gamma(\mathfrak{A},*)} d\gamma = \int_{\Gamma(\mathfrak{A},*)} \gamma\gamma^*\mu_2(G)d\gamma$$

$$= \int_{\Gamma(\mathfrak{A},*)} \gamma \cdot \left(\int_G g\gamma g dg\right) d\gamma \qquad\qquad \text{using (3.4)}$$

$$= \int_{\Gamma(\mathfrak{A},*)} \int_G (\gamma g)^2 dg d\gamma = \int_G \int_{\Gamma(\mathfrak{A},*)} (\gamma g)^2 d\gamma dg$$

$$= \int_G \int_{\Gamma(\mathfrak{A},*)} \gamma^2 d\gamma dg \qquad\qquad \text{by Haar invariance on } \Gamma(\mathfrak{A}, *)$$

$$= \int_G \mu_2(\Gamma(\mathfrak{A}, *))dg = \mu_2(\Gamma(\mathfrak{A}, *)).$$

$\square$

3.2. The key computation.
We begin with the following consequence of the computations of Section 3.1:

Proposition 3.4. *Let $\mathfrak{A}$ be a $*$-algebra and let $G \subset \Gamma(\mathfrak{A}, *)$ be a compact subgroup which generates the algebra $\mathfrak{A}$. Then for each left $\mathfrak{A}$-module X, and each Hermitian form $Q : \mathsf{X} \times \mathsf{X} \to \mathfrak{A}$, we have*

$$\int_G q(x + gy)g dg = (q(x) + q(y)) \cdot \mu_1(G) + Q(x,y) \cdot (1_{\mathfrak{A}} + \mu_2(\Gamma(\mathfrak{A}, *))), \qquad (3.5)$$

where $x, y \in \mathsf{X}$, and we set

$$q(x) = Q(x, x), \quad x \in \mathsf{X}.$$

Proof. For $x, y \in \mathsf{X}$ and $g \in G \subset \mathfrak{A}$ we have

$$q(x + gy) = Q(x + gy, x + gy)$$
$$= Q(x, x) + Q(x, gy) + Q(gy, x) + Q(gy, gy)$$
$$= q(x) + Q(x, y)g^* + gQ(y, x) + gq(y)g^*.$$

Therefore, multiplying on the right by g and integrating on G with respect to Haar measure we have

$$\int_G q(x + gy)g dg = A + B + C + D,$$

where

$$A = \int_G q(x)g dg = q(x)\mu_1(G),$$

$$B = \int_G Q(x, y)g^* g dg = \int_G Q(x, y)dg = Q(x, y)\int_G dg = Q(x, y),$$

$$C = \int_G gQ(y, x)g dg = Q(y, x)^* \int_G g^2 dg = Q(y, x)^*\mu_2(\Gamma(\mathfrak{A}, *)) \quad \text{by (3.2) and (3.3)}$$
$$= Q(x, y)\mu_2(\Gamma(\mathfrak{A}, *)).$$

and

$$D = \int_G gq(y)g^* g\,dg = \left(\int_G g\,dg \right) q(y) = \mu_1(G)q(y) = q(y)\mu_1(G),$$

where in the last step we use the fact that $\mu_1(G)$ lies in the center of $\mathfrak{A}$ (see Proposition 3.1 above). Combining these equations, the result follows. $\qquad\square$

3.3. Second moments of matrix algebras.

Proposition 3.5. *Let $(\mathfrak{A}, \sharp)$ be a polarizable algebra, and endow the matrix algebra $M_n(\mathfrak{A})$ with the involution $*$ given by $A \mapsto A^* = (A^\sharp)^T$ induced by $\sharp$ as in (1.9). Then by Proposition 2.6, the $*$-algebra $(M_n(\mathfrak{A}), *)$ is polarizable. The second moment of this algebra is given by:*

$$\mu_2(M_n(\mathfrak{A})) = \frac{1}{n} \cdot \mu_2(\mathfrak{A})I, \tag{3.6}$$

where I is the identity matrix of $M_n(\mathfrak{A})$.

Proof. Let $\Delta := \Delta_{\Gamma(\mathfrak{A},\sharp)}$ be the collection of diagonal matrices in $M_n(\mathfrak{A})$ with entries from the unitary group $\Gamma(\mathfrak{A}, \sharp)$ as in proposition 2.6. Let H be the cyclic group of permutation matrices in $M_n(\mathfrak{A})$ corresponding to the n-cycle $\sigma = (1, 2, \ldots, n) \in S_n$, i.e.

$$H = \{P_{\sigma^k} : 0 \leqslant k \leqslant n - 1\},$$

where for $\tau \in S_n$, P_τ is the permutation matrix such that $P_\tau e_i = e_{\tau(i)}$, where e_j is the column vector with 1 in the j-th row and zeroes everywhere else.

A computation analogous to that in (2.11) shows that for $D = \mathrm{diag}(g_1, \ldots, g_n) \in \Delta$ (with $g_j \in \Gamma(\mathfrak{A}, \sharp)$) and $P_{\sigma^k} \in H$ we have

$$DP_{\sigma^k}DP_{\sigma^k} = P_{\sigma^{2k}}D''D'$$

where

$$D' = \mathrm{diag}\left(g_{\sigma^k(1)}, \ldots, g_{\sigma^k(n)}\right), \quad D'' = \mathrm{diag}\left(g_{\sigma^{2k}(1)}, \ldots, g_{\sigma^{2k}(n)}\right) \in \Delta_G.$$

Therefore we have (with e_1^T the row vector with 1 in the first slot and zeroes everywhere else):

$$\begin{aligned}
e_1^T DP_{\sigma^k}DP_{\sigma^k}e_1 &= e_1^T P_{\sigma^{2k}}D''D'e_1 \\
&= e_1^T P_{\sigma^{2k}}D''g_{\sigma^k(1)}e_1 \\
&= e_1^T P_{\sigma^{2k}}g_{\sigma^{2k}(1)}g_{\sigma^k(1)}e_1 \\
&= e_1^T g_{\sigma^{2k}(1)}g_{\sigma^k(1)}e_{\sigma^{2k}(1)} \\
&= \begin{cases} g_1 g_{\sigma^k(1)} & \text{if } \sigma^{2k} = \mathrm{id} \\ 0 & \text{otherwise.} \end{cases}
\end{aligned}$$

By proposition 3.1 the element $\mu_2(M_n(\mathfrak{A}))$ is in the center of $M_n(\mathfrak{A})$. It is not difficult to see that the center of $M_n(\mathfrak{A})$ consists of matrices of the form zI, where z belongs to the center of $\mathfrak{A}$ and I is the identity matrix of $M_n(\mathfrak{A})$ Therefore there is a z in the center of $\mathfrak{A}$ such that $\mu_2(M_n(\mathfrak{A})) = zI$. We have

$$z = e_1^T \mu_2(M_n(\mathfrak{A}))e_1 = \int_H \int_\Delta e_1^T DPDPe_1\,dD\,dP$$

$$= \frac{1}{n} \sum_{k=0}^{n-1} \int_\Delta e_1^T D P_{\sigma^k} D P_{\sigma^k} e_1 dD = \frac{1}{n} \sum_{\substack{\sigma^{2k}=\mathrm{id} \\ 0 \leqslant k \leqslant n-1}} \int_\Delta g_1 g_{\sigma^k(1)} dD$$

$$= \frac{1}{n} \sum_{\substack{\sigma^{2k}=\mathrm{id} \\ 0 \leqslant k \leqslant n-1}} \int_{\Gamma(\mathfrak{A},\sharp)} \cdots \int_{\Gamma(\mathfrak{A},\sharp)} g_1 g_{\sigma^k(1)} dg_1 \ldots dg_n$$

$$= \frac{1}{n} \left(\int_{\Gamma(\mathfrak{A},\sharp)} \cdots \int_{\Gamma(\mathfrak{A},\sharp)} g_1^2 dg_1 \ldots dg_n + \sum_{\substack{\sigma^{2k}=\mathrm{id} \\ 1 \leqslant k \leqslant n-1}} \int_{\Gamma(\mathfrak{A},\sharp)} \cdots \int_{\Gamma(\mathfrak{A},\sharp)} g_1 g_{\sigma^k(1)} dg_1 \ldots dg_n \right)$$

$$= \frac{1}{n} \left(\int_{\Gamma(\mathfrak{A},\sharp)} g_1^2 dg_1 + \sum_{\substack{\sigma^{2k}=\mathrm{id} \\ 1 \leqslant k \leqslant n-1}} \int_{\Gamma(\mathfrak{A},\sharp)} \int_{\Gamma(\mathfrak{A},\sharp)} g_1 g_{\sigma^k(1)} dg_1 dg_{\sigma^k(1)} \right)$$

$$= \frac{1}{n} \left(\mu_2(\mathfrak{A}) + \sum_{\substack{\sigma^{2k}=\mathrm{id} \\ 1 \leqslant k \leqslant n-1}} \left(\int_{\Gamma(\mathfrak{A},\sharp)} g_1 dg_1 \right) \left(\int_{\Gamma(\mathfrak{A},\sharp)} g_{\sigma^k(1)} dg_{\sigma^k(1)} \right) \right)$$

$$= \frac{1}{n} \mu_2(\mathfrak{A}),$$

using in the last line the property (1.6) of polarizable subgroups such as $\Gamma(\mathfrak{A}, \sharp)$. $\qquad \square$

To use the above, we need to know the second moment of the algebra $(\mathfrak{A}, \sharp)$. We now do this for the division algebras.

Proposition 3.6. *Let $\mathbb{D}$ be a real division algebra, thought of as a $*$-algebra with the standard conjugate-transpose involution. Then we have*

$$\mu_2(\mathbb{D}) = \frac{2}{\delta} - 1, \quad \delta = \dim_\mathbb{R} \mathbb{D} = 1, 2, \text{ or } 4. \tag{3.7}$$

Consequently, for the $*$-algebra $(M_n(\mathbb{D}), *)$, we have

$$\mu_2(M_n(\mathbb{D})) = \frac{1}{n} \left(\frac{2}{\delta} - 1 \right) I_n, \tag{3.8}$$

where I_n is the $n \times n$ identity matrix.

Proof. We use the relation (3.3) to compute the second moments in (3.7). When $\mathbb{D} = \mathbb{R}$, the trivial multiplicative subgroup $G = \{1\}$ is compact, contained in the unitary group, and generates the algebra $\mathbb{D}$ over $\mathbb{R}$, so we have

$$\mu_2(\mathbb{R}) = \mu_2(G) = 1 = \frac{2}{\dim_\mathbb{R} \mathbb{R}} - 1.$$

When $\mathbb{D} = \mathbb{C}$, we can take G to be the group $\{\pm 1, \pm i\}$ fourth roots of 1. Then we have

$$\mu_2(\mathbb{C}) = \frac{1}{4} \left(1^2 + (-1)^2 + i^2 + (-i)^2 \right) = \frac{1}{4}(1 + 1 + (-1) + (-1)) = 0 = \frac{2}{\dim_\mathbb{R} \mathbb{C}} - 1$$

verifying the assertion.

When $\mathbb{D} = \mathbb{H}$, the 8 element "quaternion group" $G = \{\pm 1, \pm i, \pm j, \pm k\}$ is compact and spans $\mathbb{H}$ over $\mathbb{R}$. We therefore have

$$
\begin{aligned}
\mu_2(\mathbb{H}) &= \frac{1}{8}\left(1^2 + (-1)^2 + i^2 + (-i)^2 + j^2 + (-j)^2 + k^2 + (-k)^2\right) \\
&= \frac{1}{8}(1 + 1 - 1 - 1 - 1 - 1 - 1 - 1) = -\frac{1}{2} = \frac{2}{\dim_{\mathbb{R}} \mathbb{H}} - 1,
\end{aligned}
$$

verifying (3.7) in all cases. The formula (3.8) now follows using Proposition 3.5.   □

3.4. **End of proof of Theorems 1.1 and 1.2.** We have now assembled all the ingredients to prove these two results, which we will prove simultaneously. As in Theorem 1.1, let $(\mathfrak{A}, *)$ be a polarizable $*$-algebra, and let $G \subset \Gamma(\mathfrak{A}, *)$ be a polarizing subgroup, and let Q, q and X also have the same meaning as in the statement of that theorem. By hypothesis (1.6) we have, using the computation (3.5), that for $x, y \in \mathsf{X}$ we have:

$$
\int_G q(x + gy)g\,dg = Q(x, y) \cdot (1_{\mathfrak{A}} + \mu_2(\mathfrak{A})), \tag{3.9}
$$

so to complete the proof of Theorem 1.1 we need to show that the element

$$
1_{\mathfrak{A}} + \mu_2(\mathfrak{A}) \tag{3.10}
$$

of $\mathfrak{A}$ is a unit of the ring $\mathfrak{A}$, i.e., it is invertible, and its inverse is the polarization constant κ of the algebra $(\mathfrak{A}, *)$, i.e.

$$
\kappa = \kappa(\mathfrak{A}, *) = (1_{\mathfrak{A}} + \mu_2(\mathfrak{A}))^{-1}. \tag{3.11}
$$

By Proposition 2.5, the $*$-isomorphism ϕ of (1.11) exists if $(\mathfrak{A}, *)$ is polarizable, and by Proposition 2.7 if ϕ exists, then $(\mathfrak{A}, *)$ is polarizable. To complete the proof of Theorem 1.2, we need to show that the multiplicative inverse of the element (3.10) is given by the formula (1.12).

Thanks to the invariance of the problem under $*$-isomorphisms, it is clear that we only need to consider the case where $(\mathfrak{A}, *)$ is already a $*$-direct sum of the matrix algebras $(M_n(\mathbb{D}_j), *)$ where the involution is the conjugate-transpose involution, i.e. the map ϕ of (1.11) is the identity. In this case the element (3.10) is given by

$$
\begin{aligned}
1_{\mathfrak{A}} + \mu_2(\mathfrak{A}) &= 1_{\mathfrak{A}} + (\mu_2(M_{n_1}(\mathbb{D}_1))I_1, \ldots, \mu_2(M_{n_N}(\mathbb{D}_N)I_N)) \\
&= ((1 + \mu_2(M_{n_1}(\mathbb{D}_1))I_1, \ldots, (1 + \mu_2(M_{n_N}(\mathbb{D}_N))I_N) \\
&= \left(\left(1 + \frac{1}{n_1}\left(\frac{2}{\delta_1} - 1\right)\right)I_1, \ldots, \left(1 + \frac{1}{n_N}\left(\frac{2}{\delta_N} - 1\right)\right)I_N\right).
\end{aligned}
$$

Now since for each j we have $\delta_j \leqslant 4$ and $n_j \geqslant 1$, therefore

$$
1 + \frac{1}{n_j}\left(\frac{2}{\delta_j} - 1\right) \geqslant \frac{1}{2}.
$$

It follows that the element (3.10) is invertible, thus competing the proof of Theorem 1.1. It also follows that its inverse is

$$
(1_{\mathfrak{A}} + \mu_2(\mathfrak{A}))^{-1} = \left(\frac{n_1\delta_1}{(n_1 - 1)\delta_1 + 2}I_{n_1}, \ldots, \frac{n_j\delta_j}{(n_j - 1)\delta_j + 2}I_{n_j}, \ldots, \frac{n_N\delta_N}{(n_N - 1)\delta_N + 2}I_{n_N}\right),
$$

completing the proof of Theorem 1.2.

4. Quadrances and Hermitian forms

4.1. **Quadrances arising from Hermitian forms.**

Proposition 4.1. *If Q is a Hermitian form on a left $\mathfrak{A}$-module X, then the diagonal restriction*

$$q : \mathsf{X} \to \mathfrak{A}, \quad q(x) = Q(x, x), \ \text{where} \ x \in \mathsf{X}$$

is a quadrance, and the generalized parallelogram identity *holds: for a compact subgroup $H \subseteq \mathfrak{A}^\times$ such that*

- *(a) $q(hx) = q(x)$ for all $h \in H$, and*
- *(b) $\mu_1(H) = 0$*

hold, we have for $x, y \in X$,

$$q(x) + q(y) = \int_H q(x + hy)dh. \tag{4.1}$$

Notice that any real $*$-algebra always has a subgroup H of $\mathfrak{A}^\times$ that satisfies the hypotheses of the above proposition. This is the two element subgroup $H = \{\pm 1_{\mathfrak{A}}\}$ for which (4.1) becomes the *classical parallelogram identity* (1.15) which reduces to (1.13) for inner product spaces over $\mathbb{C}$.

Proof. For $x \in \mathsf{X}, \alpha \in \mathfrak{A}$ we have $Q(x, x)^* = Q(x, x)$, i.e. $q(x)^* = q(x)$, and $Q(\alpha x, \alpha x) = \alpha Q(x, x)\alpha^*$, i.e. $q(\alpha x) = \alpha q(x)\alpha^*$, thus verifying the first two conditions in the definition of a quadrance (Definition 1.3 above). For $x, y, \in \mathsf{X}, \lambda \in \mathbb{R} = \mathbb{R} \cdot 1_{\mathfrak{A}}, \alpha \in \mathfrak{A}$, we have

$$\begin{aligned}
q(\lambda x + \alpha y) &= Q(\lambda x + \alpha y, \lambda x + \alpha y) \\
&= Q(\lambda x, \lambda x) = Q(\lambda x, \alpha y) + Q(\alpha y, \lambda x) + Q(\alpha y, \alpha y) \\
&= \lambda^2 q(x) + \lambda Q(x, y)\alpha^* + \alpha Q(y, x)\lambda + \alpha q(y)\alpha^*.
\end{aligned}$$

Since multiplication in $\mathfrak{A}$ is continuous, it follows that the mapping (1.14) is continuous. This shows that q is a quadrance.

For $x, y \in X$ a computation yields (4.1):

$$\begin{aligned}
\int_H q(x + hy)dh &= \int_H Q(x + hy, x + hy)dh \\
&= \int_H q(x)dh + \int_H q(hy)dh + \int_H Q(x, hy)dh + \int_H Q(hy, x)dh \\
&= \int_H q(x)dh + \int_H q(y)dh + Q(x, y)\int_H h^* dh + \left(\int_H h\, dh\right)Q(y, x) \\
&= q(x) + q(y),
\end{aligned}$$

where $\int_H h^* dh = \left(\int_H h\, dh\right)^* = 0$ by $\mathbb{R}$-linearity of $*$.

$\square$

Remark: It would be very interesting to know if the classical parallelogram identity (1.15) can be replaced in Theorem 1.3 by a generalized parallelogram identity with respect to some other compact group $H \subset \mathfrak{A}^\times$.

4.2. **Polarization of quadrances and proof of Theorem 1.3.** The proof of Theorem 1.3 consists of applying the operation on the right hand side of (1.8) to the given quadrance, and showing that the resulting function is a Hermitian form. The following is the first step in the argument:

Proposition 4.2. *Let $(\mathfrak{A}, *)$ be a polarizable $*$-algebra and let X be a left $\mathfrak{A}$-module. Let $q \colon \mathsf{X} \to \mathfrak{A}$ be a quadrance on X and let $G \subset \Gamma(\mathfrak{A})$ be a polarizing subgroup. Define $Q_G \colon \mathsf{X} \times \mathsf{X} \to \mathfrak{A}$ by*

$$Q_G(x, y) = \kappa \cdot \int_G q(x + gy) g \, dg, \tag{4.2}$$

where κ is the polarization constant of $(\mathfrak{A}, *)$. Then Q_G satisfies the following properties, for all $x, y \in \mathsf{X}$:

(a) $Q_G(x, x) = q(x)$.
(b) $Q_G(x, y)^* = Q_G(y, x)$.
(c) $Q_G(hx, y) = h Q_G(x, y)$ for all $h \in G$.
(d) $Q_G(x, 0) = 0$.

Proof.   (a) We compute

$$Q_G(x, x) = \kappa \cdot \int_G q((1 + g)x) g \, dg = \kappa \cdot \int_G (1 + g) q(x) (1 + g)^* g \, dg$$

$$= \kappa \cdot \left(q(x) \int_G g \, dg + q(x) \int_G dg + \int_G g q(x) g \, dg + \left(\int_G g \, dg \right) q(x) \right)$$

$$= \kappa \cdot (q(x) + q(x)^* \mu_2(\mathfrak{A})) = \kappa \cdot (1_{\mathfrak{A}} + \mu_2(\mathfrak{A})) q(x) = q(x),$$

using the facts that $q(x)^* = q(x)$ and $\mu_1(G) = 0$,

(b) We see from the formula (1.12) that the polarization constant κ satisfies $\kappa^* = \kappa$ and lies in the center of $\mathfrak{A}$. Therefore we can compute:

$$Q_G(x, y)^* = \kappa \cdot \int_G (q(x + gy) g)^* \, dg = \kappa \cdot \int_G g^* q(x + gy) \, dg$$

$$= \kappa \cdot \int_G q(g^* x + y) g^* \, dg = \kappa \cdot \int_G q(gx + y) g \, dg$$

$$= Q_G(y, x).$$

(c) This follows by an application of Haar invariance, and the properties of κ used in the previous part:

$$Q_G(hx, y) = \kappa \cdot \int_G q(hx + gy) g \, dg = \kappa \cdot \int_G h q(x + h^* gy) h^* g \, dg$$

$$= \kappa \cdot h \int_G q(x + h^* gy) h^* g \, dg = h \kappa \cdot \int_G q(x + gy) g \, dg$$

$$= h Q_G(x, y).$$

(d) We have: $Q_G(x, 0) = \kappa \cdot \int_G q(x) g \, dg = 0.$

$\square$

Proof of Theorem 1.3. Let G be a polarizing subgroup of $\Gamma(\mathfrak{A}, *)$ (for example, we could take G to be $\Gamma(\mathfrak{A}, *)$ itself). Define the map $Q_G : \mathsf{X} \times \mathsf{X} \to \mathfrak{A}$ by the formula (4.2). We will prove that Q_G is a Hermitian form on X; by part (a) of Proposition 4.2, the result would

follow if we can also show uniqueness: if Q is a Hermitian form such that $Q(x, x) = q(x)$, then we have $Q = Q_G$. But by the polarization identity 1.8 of Theorem 1.1 we have for $x, y \in \mathsf{X}$ that

$$Q(x, y) = \kappa \cdot \int_G q(x + gy)gdg = Q_G(x, y).$$

Thanks to the properties of Q already established in Proposition 4.2, it is enough to show that Q_G is $\mathfrak{A}$-linear in the first argument. For any $x, y \in \mathsf{X}$ we have

$$
\begin{aligned}
Q_G(2x, y) &= \kappa \cdot \int_G q(x + x + gy)gdg \\
&= \kappa \cdot \int_G (2(q(x) + q(x + gy)) - q(gy))gdg \\
&= \kappa \cdot \left(2 \int_G q(x)gdg + 2 \int_G q(x + gy)gdg - \int_G gq(y)dg \right) \\
&= 2\kappa \cdot \int_G q(x + gy)gdg \\
&= 2Q_G(x, y),
\end{aligned}
$$

where we have used the parallelogram identity (1.15) to get the second equality. Using part (b) of Proposition 4.2 we have:

$$Q_G(x, 2y) = Q_G(2y, x)^* = 2Q_G(y, x)^* = 2Q_G(x, y). \tag{4.3}$$

Now, for $x, y, z \in \mathsf{X}$ we have using the classical parallelogram identity (1.15) that

$$
\begin{aligned}
Q_G(x, z) + Q_G(y, z) &= \kappa \cdot \int_G (q(x + gz) + q(y + gz))gdg \\
&= \kappa \cdot \int_G \frac{1}{2}(q(x + y + 2gz) + q(x - y))gdg \\
&= \frac{1}{2}\kappa \cdot \int_G q(x + y + g(2z))gdg + \frac{1}{2}\kappa \cdot q(x - y) \cdot \int_G gdg \\
&= \frac{1}{2}Q_G(x + y, 2z),
\end{aligned}
$$

and so, by (4.3), it follows that $Q_G(x, z) + Q_G(y, z) = Q_G(x + y, z)$ for all $x, y, z \in X$. From this we deduce easily that $Q_G(\cdot, z)$ is $\mathbb{Q}$-homogeneous, i.e. for $\lambda \in \mathbb{Q}$ we have

$$Q(\lambda x, y) = \lambda Q(x, y). \tag{4.4}$$

To extend (4.4) to the situation when $\lambda \in \mathbb{R}$, fix $x, y \in \mathsf{X}$ and $\lambda \in \mathbb{R}$ and let $\{\lambda_n\}$ be a sequence in $\mathbb{Q}$ converging to λ. Let $\{F_n\}$ is the sequence of $\mathfrak{A}$-valued functions on G given by $F_n(g) = q(\lambda_n x + gy)g$. Since the $\mathfrak{A}$-valued function $(\xi, g) \mapsto q(\xi x + gy)g$ is uniformly continuous on the compact space $[\lambda - 1, \lambda + 1] \times G$, it follows that $F_n \to F$ uniformly on G where $F(g) = q(\lambda x + gy)g$. Therefore

$$
\begin{aligned}
\lambda Q_G(x, y) &= \lim_{n \to \infty} \lambda_n Q_G(x, y) = \lim_{n \to \infty} Q_G(\lambda_n x, y) = \kappa \cdot \lim_{n \to \infty} \int_G q(\lambda_n x + gy)gdg \\
&= \kappa \cdot \int_G q(\lambda x + gy)gdg \quad \text{by uniform convergence} \\
&= Q_G(\lambda x, y).
\end{aligned}
$$

Finally, letting $\alpha = \sum_{i=1}^{m} \lambda_i g_i \in \mathfrak{A}$ for some $\lambda_1, \ldots, \lambda_m \in \mathbb{R}$ and $g_1, \ldots, g_m \in G$ we have

$$Q_G(\alpha x, y) = Q_G(\sum_{i=1}^{m} \lambda_j g_j x, y) = \sum_{i=1}^{m} \lambda_i g_i Q_G(x, y) = \alpha Q_G(x, y)$$

completing the proof that Q_G is a Hermitian form. We have already proved uniqueness above. $\square$

5. Some Examples

5.1. **The three real division algebras.** We illustrate Theorems 1.1 and 1.2 by classifying all the polarizing subgroups of $\mathbb{R}, \mathbb{C}$ and $\mathbb{H}$, and therefore obtaining all polarization formulas for Hermitian forms defined on vector spaces over these scalars. By (3.7), the polarization constants of the algebras (made into $*$-algebras with the usual conjugation operations), are

$$\kappa(\mathbb{D}) = (1 + \mu_2(\mathbb{D}))^{-1} = \left(1 + \left(\frac{2}{\dim_{\mathbb{R}}(\mathbb{D})} - 1\right)\right)^{-1} = \frac{1}{2} \dim_{\mathbb{R}} \mathbb{D} = \begin{cases} \frac{1}{2} & \text{if } \mathbb{D} = \mathbb{R} \\ 1 & \text{if } \mathbb{D} = \mathbb{C} \quad (5.1) \\ 2 & \text{if } \mathbb{D} = \mathbb{H}. \end{cases}$$

5.1.1. *The real numbers.* In this case the unitary group is $\Gamma(\mathbb{R}, \mathrm{id}) = \{x \in \mathbb{R} : x^2 = 1\} = \{\pm 1\}$. Therefore the only polarizing subgroups of the reals is the group $\{\pm 1\}$. The polarization formula for a Hermitian form Q on a real vector space is (which in this situation is simply a bilinear form):

$$Q(x, y) = \kappa \int_{\{\pm 1\}} q(x + gy) g \, dg = \frac{1}{2} \left(\frac{1}{2} \cdot q(x + y) + \frac{1}{2} \cdot q(x - y) \cdot (-1)\right)$$
$$= \frac{1}{4} \left(q(x + y) - q(x - y)\right).$$

Of course, at the bottom, after diagonalizing the bilinear form, this is nothing but the identity $xy = \frac{1}{4} \left((x + y)^2 - (x - y)^2\right)$ for real numbers.

5.1.2. *Locus classicus: complex numbers.* For $(\mathbb{C}, \mathrm{conj})$, the unitary group is $\Gamma(\mathbb{C}, \mathrm{conj}) = \{z \in \mathbb{C} : |z| = 1\} = U(1)$. Any compact subgroup of this one dimensional Lie group is either a finite subgroup, or the whole of $U(1)$. It is easy to see that a finite subgroup of $U(1)$ is a cyclic group $G_N = \{\omega^j : 0 \leq j \leq N - 1\}$ generated by the primitive N-th root of unity $\omega = \exp\left(\frac{2\pi i}{N}\right)$. Notice that $\mathrm{span}_{\mathbb{R}} G_N = \mathbb{C}$ if and only if $N \geq 3$. It is clear also that $\mathrm{span}_{\mathbb{R}} U(1) = \mathbb{C}$, and thanks to part (b) of Proposition 3.2, condition (1.6) holds for both G_N and $U(1)$. It follows that any polarizing subgroup of $\mathbb{C}$ is either $U(1)$ or G_N for $N \geq 3$.

For the group G_N, we obtain the "N-th root polarization identity" ([You88, p. 12, Problem 1.10] or [D'A02, pp. 53–54])

$$Q(x, y) = \frac{1}{N} \sum_{k=0}^{N-1} q(x + \omega^k y) \omega^k, \quad \omega = e^{\frac{2\pi i}{N}}, \text{ where } N \geq 3, \quad (5.2)$$

of which (1.1) is the special case for $N = 4$ and $Q = \langle \cdot, \cdot \rangle$. For the polarizing group $G = U(1)$ we obtain the "integral polarization identity"

$$Q(x, y) = \frac{1}{2\pi} \int_0^{2\pi} q(x + e^{i\theta} y) e^{i\theta} d\theta, \quad (5.3)$$

which can also be obtained from (5.2) as the limit when $N \to \infty$, by interpreting its right hand side as a Riemann sum of the integral on the right hand side of (5.3). Notice that this passage to the limit is possible only because in the generalized polarization identity (1.8), the constant κ depends only on the algebra of scalars $\mathfrak{A}$ and not on the polarizing group G.

5.1.3. *The quaternions.* Just as with the complex numbers, there is an abundant supply of polarizing subgroups in the quaternions:

Proposition 5.1. *A subgroup of $\mathbb{H}^{\times}$ is polarizing if and only if it is compact and non-abelian.*

Proof. Let G be a compact subgroup of $\mathbb{H}^{\times}$. The map $\mathbb{H}^{\times} \to \mathbb{R}^{+}$ given by $x \mapsto \|x\|$ is a continuous homomorphism of the group of nonzero quaternions under multiplication to the group of positive real numbers under multiplication, and therefore the image of a compact subgroup G of $\mathbb{H}\backslash\{0\}$ is a compact subgroup of $\mathbb{R}^{+}$, i.e., $\{1\}$, so that $G \subset Sp(1)$.

Now suppose that G is polarizing in $\mathbb{H}$, so in particular G generates $\mathbb{H}$. Since $\mathbb{H}$ is not commutative, it follows that G must be nonabelian.

For the converse assume that G is nonabelian, and let $\mathfrak{B}$ be the subalgebra of $\mathbb{H}$ generated by the group G. Then $\mathfrak{B}$ (with the involution induced from $\mathbb{H}$) is noncommutative and polarizable, since it is generated by a compact nonabelian subgroup $G \subset \Gamma(\mathfrak{B}, \mathrm{conj})$ of unitary elements (see Proposition 2.4). Then by Theorem 1.2, the algebra $\mathfrak{B}$ is isomorphic to $\bigoplus_{j=1}^{N} M_{n_j}(\mathbb{D}_j)$ for some real division algebras $\mathbb{D}_j$ and positive integers n_j. Therefore, if $\delta_j = \dim_{\mathbb{R}}(\mathbb{D}_j) \in \{1, 2, 4\}$ we will have $1 \leqslant \sum_{j=1}^{N} \delta_j n_j^2 \leqslant 3$. It follows that $\mathfrak{B}$ is isomorphic as an algebra to one of

$$\mathbb{R}, \mathbb{R} \oplus \mathbb{R}, \mathbb{C}, \mathbb{R} \oplus \mathbb{R} \oplus \mathbb{R}, \mathbb{R} \oplus \mathbb{C},$$

each of which is commutative. Since $\mathbb{H}$ is not commutative, this shows that $\mathfrak{B} = \mathbb{H}$. Since $\mathbb{H}$, being a division ring, is simple, the condition (1.6) now follows from part (b) of Proposition 3.2.

$\square$

Therefore the task of classifying all polarizing subgroups of the quaternions (and therefore finding all quaternionic polarization identities) is reduced to the classification of closed nonabelian subgroups of $Sp(1)$. Notice that if G is a polarizing subgroup in a noncommutative polarizable algebra $(\mathfrak{A}, *)$, then any subgroup H of the unitary group which is conjugate to G (i.e., there is a $\gamma \in \Gamma(\mathfrak{A}, *)$ such that $H = \gamma G \gamma^{-1}$) is clearly also polarizing. Therefore it will be sufficient to classify polarizing subgroups up to conjugacy.

Proposition 5.2. *A subgroup of $\Gamma(\mathbb{H}, \mathrm{conj}) = Sp(1)$ is polarizing if and only if it is one of the following:*

(1) The full group $Sp(1)$.

(2) A subgroup conjugate to the group

$$\{\cos\theta + i\sin\theta : 0 \leqslant \theta \leqslant 2\pi\} \cup \{j\cos\phi + k\sin\phi : 0 \leqslant \phi \leqslant 2\pi\}, \tag{5.4}$$

a Lie group isomorphic to $O(2)$.

(3) A finite subgroup of $\mathbb{H}$ conjugate to one of the groups in the following table, where

$$\omega = \frac{1}{2}\left(-1 + i + j + k\right),$$

and the last row corresponds to an infinity of groups, one for each integer $n \geqslant 2$.

Traditional name	Order	Generators
Binary tetrahedral ($2A_4$)	24	$\langle \omega, i \rangle$
Binary octahedral ($2S_4$)	48	$\left\langle \omega, \frac{1}{\sqrt{2}}(j+k) \right\rangle$
Binary icosahedral ($2A_5$)	120	$\left\langle \omega, \frac{1}{2}i + \frac{\sqrt{5}-1}{4}j + \frac{\sqrt{5}+1}{4}k \right\rangle$
Binary dihedral ($2D_{2n}$)	$4n$	$\left\langle \cos\left(\frac{\pi}{n}\right) + \sin\left(\frac{\pi}{n}\right)i, j \right\rangle$
	($n \geqslant 2$ an integer)	

Proof. The simply connected Lie group $Sp(1)$ is geometrically the three dimensional sphere S^3 in $\mathbb{R}^4$ and is isomorphic to $SU(2)$. Its Lie algebra L can therefore be identified with the tangent space to S^3 at $(1,0,0,0)$ and therefore to the space of purely vector quaternions $\mathbb{R}^3 = \{x_1 i + x_2 j + x_3 k : x_1, x_2, x_3 \in \mathbb{R}\}$. The Lie bracket on L is

$$[X,Y] = XY - YX = (-\langle X, Y \rangle + X \times Y) - (-\langle Y, X \rangle + Y \times X) = 2(X \times Y),$$

where $\times$ denotes the cross product on $\mathbb{R}^3$ and $\langle \cdot, \cdot \rangle$ is the inner product. This Lie algebra L cannot have a subalgebra of dimension 2, since as soon as we have in the subalgebra two linearly independent vectors u, v, their Lie bracket $2(u \times v)$ is another vector linearly independent of u and v. Therefore a polarizing subgroup G of $Sp(1)$ can be of dimension 3, 1 or 0 (i.e. finite). The only Lie subalgebra of L of dimension 3 is L itself, and the corresponding subgroup of $Sp(1)$ is $Sp(1)$, which is polarizing as the unitary group of $\mathbb{H}$.

Now let G be a polarizing subgroup of $Sp(1)$ of dimension 1, and let G^0 be its identity component. Then there is a purely vector quaternion $u \in L$ with $\|u\| = 1$ such that $G^0 = \{\exp(\theta u) : \theta \in \mathbb{R}\}$. Since $u^2 = -1$, it follows that $\exp(\theta u) = \cos\theta + (\sin\theta)u$. Since G^0 is abelian, $G \neq G^0$. Let $z \in G \backslash G^0$, so that, since G^0 is a normal subgroup of G we have $zG^0z^{-1} = G^0$. Therefore for each $\theta \in \mathbb{R}$ there is a $\phi \in \mathbb{R}$ such that $z\exp(\theta u)z^{-1} = \exp(\phi u)$. By looking at the scalar and vector parts, we see that $\cos\theta = \cos\phi$ and $(\sin\theta)zuz^{-1} = (\sin\phi)u$. The first equation gives $\theta = \pm\phi \mod 2\pi$, which when substituted into the second gives $zuz^{-1} = \pm u$. Recall that for a unit quaternion $z \in Sp(1)$, the map $\mathbb{R}^3 = \operatorname{Im}\mathbb{H} \ni w \mapsto zwz^{-1}$ is a rotation of $\mathbb{R}^3$ whose axis is spanned by the vector part $\operatorname{Im} z \in \mathbb{R}^3$ of z. Therefore, if $zuz^{-1} = u$, then $z = \cos\alpha + (\sin\alpha)u$ for some $\alpha \in \mathbb{R}$, which means that $z \in G^0$ which contradicts $z \notin G^0$. Therefore we must have $zuz^{-1} = -u$. This means that the rotation $w \mapsto zwz^{-1}$ of $\mathbb{R}^3$ has for axis a unit vector $v \in \mathbb{R}^3$ orthogonal to u and has angle of rotation π, so that $z = \cos\left(\frac{\pi}{2}\right) + \sin\left(\frac{\pi}{2}\right)v = v$. Therefore each element of $G \backslash G^0$ is a unit vector of $\operatorname{Im}(\mathbb{H})$ orthogonal to u. If $v \in G \backslash G^0$, notice that each element of the coset $G^0 v = \{(\cos\theta)v + (\sin\theta)uv : \theta \in \mathbb{R}\}$ is a unit vector of $\operatorname{Im}(\mathbb{H})$ orthogonal to u, therefore

$$G = \{\cos\theta + (\sin\theta)u : 0 \leqslant \theta \leqslant 2\pi\} \cup \{(\cos\phi)v + (\sin\phi)uv : 0 \leqslant \phi \leqslant 2\pi\}.$$

There is an element $A \in SO(3)$ which maps the ordered basis $\{u, v, uv = u \times v\}$ into the standard basis $\{i, j, k\}$. Thanks to the double covering $Sp(1) \to SO(3)$ then there is an $\gamma \in Sp(1)$ such that for each $w \in \mathbb{R}^3 = \operatorname{Im}(\mathbb{H})$ we have $Aw = \gamma w \gamma^{-1}$. It follows that $\gamma G \gamma^{-1}$ is the group of (5.4).

Finite multiplicative subgroups of $\mathbb{H}^\times$ can be classified up to conjugacy by using the double cover $Sp(1) \to SO(3)$ and then using the well-known classical classification of the finite subgroups of rotations of three dimensional space (see, e.g., [CS03, p. 33]). Using

this classification one obtains the complete list of nonabelian finite subgroups of $\mathbb{H}^\times$ in the table above, and therefore of finite polarizing subgroups of $\mathbb{H}$:

$\square$

Remarks:

(1) A special case of the quaternionic polarization formula was obtained in the unpublished PhD thesis [Jam70, Theorem 5, p. 75]. This corresponds to the group $2D_4$ in the last row of the table, which is the 8 element "quaternion group" $\langle i, j \rangle = \{\pm 1, \pm i, \pm j, \pm k\}$. and a positive definite inner product on a quaternionic vector space. This formula over the quaternion group is also contained in [GR93], which proves an analogous formula for Clifford numbers.

(2) The finite groups above are closely connected with regular polyhedra and other highly symmetric solids in $\mathbb{R}^3$, just as the complex polarization formula (5.2) is associated to a regular N-gon, and the integral version (5.3) is associated to the circle. Recall that there is a covering map of two sheets $\Phi : Sp(1) \to SO(3)$ given by $\Phi(z)(x) = zxz^{-1}$ for $x \in \mathbb{R}^3$ identified with the purely vector quaternions. Under this map, each of the polarizing groups above is mapped to a subgroup of $SO(3)$ which is the rotational symmetry group of a well-known three dimensional figure. For $Sp(1)$, we get $SO(3)$, which is the symmetry group of the unit sphere $S^2 \subset \mathbb{R}^3$. The group (5.4) maps under Φ to the symmetry group of a cylinder. The finite groups in the table map under Φ to the symmetry groups of the Platonic solids (as recognized in the traditional names of these groups.) On the other hand, the convex hull in $\mathbb{H}$ of the groups $2A_4$ and $2A_5$ are themselves 4 dimensional regular polytopes called a 24-cell and 120-cell respectively.

As a consequence of the classification of polarizing subgroups of the division algebras we have the following:

Proposition 5.3. *Let $(\mathfrak{A}, *)$ be a polarizable algebra. Then there is a finite polarizing subgroup $G \subset \Gamma(\mathfrak{A}, *)$.*

Proof. By Theorem 1.2, it suffices to show that the $*$-direct sum $\bigoplus_j^N (M_{n_j}(\mathbb{D}_j), *)$ admits a finite polarizing subgroup. For this we need to show that each matrix algebra $(M_{n_j}(\mathbb{D}_j), *)$ has a polarizing subgroup G_j which is finite, since then the product $G_1 \times \cdots \times G_N$ is clearly a polarizing subgroup of the direct sum $\bigoplus_j^N (M_{n_j}(\mathbb{D}_j), *)$. Now we saw above that each of the division algebras $\mathbb{R}, \mathbb{C}, \mathbb{H}$ has a finite polarizing subgroup (and infinitely many of them for $\mathbb{C}$ and $\mathbb{H}$.) It now follows by Proposition 2.6 that whenever $\mathbb{D}$ has a finite polarizing subgroup G, the matrix algebra $M_n(\mathbb{D})$ has a finite polarizing subgroup $\Delta_G H$ of cardinality $|G|^n |H|$. Therefore each $(M_{n_j}(\mathbb{D}_j), *)$ has a finite polarizing subgroup and the result follows. $\square$

5.2. **Group algebras.** Let G be a finite group, and let $\mathfrak{A} = \mathbb{R}[G]$ be its real group algebra. Recall that this consists of formal linear combinations $\sum_{g \in G} a_g g$, where $a_g \in \mathbb{R}$, with the natural $\mathbb{R}$-linear structure and a bilinear, associative multiplication induced by the multiplication operation of the group G. We can define an involution $*$ on $\mathfrak{A}$ by the $\mathbb{R}$-linear extension of the inversion operation on the group G:

$$\left(\sum_{g \in G} a_g g \right)^* = \left(\sum_{g \in G} a_g g^{-1} \right),$$

which is an involution since $(gh)^* = (gh)^{-1} = h^{-1}g^{-1} = h^*g^*$. The identity $1_{\mathfrak{A}}$ of the algebra $\mathfrak{A}$ is clearly $1 \cdot e_G$, where e_G is the identity element of the group G.

Identifying $g \in G$ with the element $1 \cdot g \in \mathbb{R}[G]$ we see that $G \subset \Gamma(\mathbb{R}[G], *)$, since for $g \in G$, we have $gg^* = gg^{-1} = e_G$. It follows that G is a compact subgroup of the unitary group of $\mathbb{R}[G]$ which generates it as an algebra, and consequently $\mathbb{R}[G]$ is polarizable, thanks to Proposition 2.4. The group

$$\{(\pm 1)g : g \in G\} \subset \Gamma(\mathbb{R}[G], *)$$

isomorphic to $\mathbb{Z}_2 \times G$ contains $-1 \cdot e_g$, hence is a polarizing group in $\mathbb{R}[G]$ by Proposition 3.2. Theorem 1.2 in this case reduces to the classical Maschke's theorem (semisimplicity of the group algebra). The polarization constant of $\mathbb{R}[G]$ can be computed in terms of the representation theory of the group G. We introduce the following notation:

- $\mathrm{Irr}(G)$ is the set of irreducible complex characters of G,
- $\deg \chi = \chi(e_G)$ is the degree of $\chi \in \mathrm{Irr}(G)$, i.e. the dimension of the vector space on which the representation affording χ is defined, and
- for $\chi \in \mathrm{Irr}(G)$, $s(\chi)$ denotes the Frobenius-Schur indicator of χ. Recall that this is respectively $1, 0$ or -1 according to whether the representation affording χ is real, complex or quternionic.

Proposition 5.4. *Then*

$$\kappa(\mathbb{R}[G], *) = \frac{1}{|G|} \sum_{g \in G} \left(\sum_{\chi \in \mathrm{Irr}(G)} \frac{(\deg \chi)^2 \cdot \overline{\chi(g)}}{\deg \chi + s(\chi)} \right) \cdot g. \tag{5.5}$$

Notice that if $\chi \in \mathrm{Irr}(G)$ is afforded by a quaternionic representation, we must have $\deg \chi \geqslant 2$. Therefore in all cases we have $\deg \chi + s(\chi) \geqslant 1$. It is also not difficult to see that the coefficient of each $g \in G$ in the sum on the right hand side of (5.5) is real valued.

Proof. Let

$$r_2(g) = \left| \{x \in G : x^2 = g\} \right|$$

be the number of square roots of the element g in the group G. Then with respect to the inner product $(\phi, \psi) = \frac{1}{|G|} \sum_{g \in G} \phi(g)\overline{\psi(g)}$ on the space of complex-valued functions on G, we have for $\chi \in \mathrm{Irr}(G)$

$$(r_2, \chi) = \frac{1}{|G|} \sum_{g \in G} r_2(g)\overline{\chi(g)} = \frac{1}{|G|} \sum_{g \in G} \overline{\chi(g^2)} = \overline{s(\chi)} = s(\chi),$$

where we use the representation $s(\chi) = \frac{1}{|G|} \sum_{g \in G} \chi(g^2)$ and the fact that s is real valued. Since $r_2 : G \to \mathbb{C}$ is a class function, which corresponds to the fact (Proposition 3.1) that $\mu_2(G)$ is in the center of $\mathbb{R}[G]$, and since $\mathrm{Irr}(G)$ is an orthonormal basis of the class functions with respect to the inner product $(\cdot, \cdot)$ defined above, we can write

$$r_2 = \sum_{\chi \in \mathrm{Irr}(G)} (r_2, \chi)\chi = \sum_{\chi \in \mathrm{Irr}(G)} s(\chi)\chi. \tag{5.6}$$

Since G is a compact (even finite) subgroup of the algebra $\mathfrak{A} = \mathbb{R}[G]$ generating it as an algebra, the second moment of $\mathfrak{A}$ can be computed using (3.3):

$$\mu_2(\mathbb{R}[G]) = \mu_2(G) = \frac{1}{|G|} \sum_{g \in G} g^2 = \frac{1}{|G|} \sum_{g \in G} r_2(g)g,$$

$$= \frac{1}{|G|} \sum_{g \in G} r_2(g^{-1})g, \quad \text{since } r_2(g) = r_2(g^{-1})$$

$$= \frac{1}{|G|} \sum_{g \in G} \left(\sum_{\chi \in \text{Irr}(G)} s(\chi)\chi(g^{-1}) \right) g \quad \text{using (5.6).}$$

$$= \sum_{\chi \in \text{Irr}(G)} \frac{s(\chi)}{\deg \chi} \cdot \epsilon_\chi,$$

where for $\chi \in \text{Irr}(G)$, we set

$$\epsilon_\chi = \frac{\deg \chi}{|G|} \sum_{g \in G} \chi(g^{-1})g. \tag{5.7}$$

It is known (see [Isa76, Chapter 2]) that the collection of elements $\{\epsilon_\chi : \chi \in \text{Irr}(G)\} \subset \mathbb{R}[G]$ form a complete set of primitive orthogonal idempotents in the commutative ring $Z(\mathbb{R}[G])$, the center of $\mathbb{R}[G]$, i.e. they satisfy

$$\epsilon_\chi^2 = \epsilon_\chi, \quad \epsilon_\chi \epsilon_\lambda = 0 \quad \text{for } \chi, \lambda \in \text{Irr}(G), \chi \neq \lambda, \quad \text{and} \quad \sum_{\chi \in \text{Irr}(G)} \epsilon_\chi = 1_{\mathbb{R}[G]}.$$

Therefore by (3.11) we have

$$\kappa(\mathbb{R}[G], *) = \left(1_{\mathbb{R}[G]} + \mu_2(G) \right)^{-1}$$

$$= \left(\sum_{\chi \in \text{Irr}(G)} \epsilon_\chi + \sum_{\chi \in \text{Irr}(G)} \frac{s(\chi)}{\deg \chi} \cdot \epsilon_\chi \right)^{-1}$$

$$= \left(\sum_{\chi \in \text{Irr}(G)} \left(1 + \frac{s(\chi)}{\deg \chi} \right) \epsilon_\chi \right)^{-1}$$

$$= \sum_{\chi \in \text{Irr}(G)} \frac{\deg \chi}{\deg \chi + s(\chi)} \cdot \epsilon_\chi.$$

Substituting ϵ_χ from (5.7) leads to the formula (5.5). $\qquad \square$

5.3. Clifford algebras.

For nonnegative integers p, q, let $\mathsf{C}_{p,q}$ be the real Clifford algebra of signature (p, q) (see [LM89]). Recall that this is a $*$-algebra over $\mathbb{R}$ of dimension 2^{p+q} generated by the $p + q$ elements $\{e_i : 1 \leqslant i \leqslant p + q\}$ satisfying the relations

$$e_i^2 = 1 \quad \text{for } 1 \leqslant i \leqslant p, \quad e_j^2 = -1 \quad \text{for } p \leqslant j \leqslant p + q, \quad e_i e_j = -e_j e_i \quad \text{for } i \neq j.$$

The involution of $\mathsf{C}_{p,q}$ is determined by $e_i^* = e_i, 1 \leqslant i \leqslant p$ and $e_i^* = -e_i, p + 1 \leqslant i \leqslant p + q$. If for $I = \{i_1 < \cdots < i_r\} \subseteq \{1, \ldots, p + q\}$ we set

$$e_I = e_{i_1} e_{i_2} \ldots e_{i_r}$$

then $e_I^* = e_{i_r}^* e_{i_{r-1}}^* \ldots e_{i_1}^*$. It is easy to see that

$$G_{p,q} = \{\pm e_I : I = \{i_1 < \cdots < i_r\} \subseteq \{1, \ldots, p + q\}\}$$

is a finite subgroup of $\Gamma(\mathsf{C}_{p,q}, *)$ which generates $\mathsf{C}_{p,q}$. Therefore by part 3 of Proposition 2.4 the algebra $\mathsf{C}_{p,q}$ is polarizable. We now find its polarization constant.

Proposition 5.5. $\kappa(\mathsf{C}_{p,q}) = \dfrac{1}{1 + 2^{-\frac{p+q-1}{2}} \cos\left(\frac{p-q-1}{4}\pi\right)}$

Proof. Suppose that $I = \{i_1 < \cdots < i_k\} \subseteq \{1, \ldots, p+q\}$, so that $|I| = k$. Assume that $|I \cap \{1, \ldots, p\}| = \ell$. Then

$$\begin{aligned}
e_I^2 &= e_{i_1} \cdots e_{i_\ell} e_{i_{\ell+1}} \cdots e_{i_k} \cdot e_{i_1} \cdots e_{i_\ell} e_{i_{\ell+1}} \cdots e_{i_k} \\
&= (-1)^{k-1} \cdots (-1)^1 e_{i_1}^2 \cdots e_{i_\ell}^2 e_{i_{\ell+1}}^2 \cdots e_{i_k}^2 \\
&= (-1)^{\frac{k(k-1)}{2}} (-1)^{k-\ell} \\
&= (-1)^{\frac{k(k+1)}{2}} (-1)^\ell.
\end{aligned}$$

For such an I there are $\binom{p}{\ell}$ possibilities for $I \cap \{1, \cdots, p\}$ and $\binom{q}{k-\ell}$ possibilities for $I \setminus \{1, \cdots, p\}$. Hence there are $\binom{p}{\ell}\binom{q}{k-\ell}$ such I and

$$\mu_2(\mathsf{C}_{p,q}) = \mu_2(G_{p,q}) = \frac{1}{2^{p+q}} \sum_I e_I^2 = \frac{1}{2^{p+q}} \sum_{k=0}^{p+q} (-1)^{\frac{k(k+1)}{2}} \sum_{\ell=0}^{k} \binom{p}{\ell}\binom{q}{k-\ell}(-1)^\ell.$$

Next observe that $(-1)^{\frac{k(k+1)}{2}}$ is periodic in k with period 4. The equality $(-1)^{\frac{k(k+1)}{2}} = \mathrm{Re}((1+i)i^k)$ is easily verified by periodicity. From this we get

$$\begin{aligned}
\mu_2(\mathsf{C}_{p,q}) &= \frac{1}{2^{p+q}} \mathrm{Re}\left((1+i) \sum_{k=0}^{p+q} i^k \sum_{\ell=0}^{k} \binom{p}{\ell}\binom{q}{k-\ell}(-1)^\ell \right) \\
&= \frac{1}{2^{p+q}} \mathrm{Re}\left((1+i)\left(\sum_{r=0}^{p} \binom{p}{r}(-1)^r i^r \right)\left(\sum_{s=0}^{q} \binom{q}{s} i^s \right) \right) \\
&= \frac{1}{2^{p+q}} \mathrm{Re}\left((1-i)^p (1+i)^{q+1} \right) \\
&= \frac{2^{\frac{p+q+1}{2}}}{2^{p+q}} \mathrm{Re}\left(e^{-p\pi i/4} e^{(q+1)\pi i/4} \right) \\
&= \frac{1}{2^{\frac{p+q-1}{2}}} \cos\left(\frac{p-q-1}{4}\pi \right).
\end{aligned}$$

The result follows by (3.11). $\qquad\square$

For the algebras $\mathsf{C}_{0,q}$, the polarization identity corresponding to the group $G_{0,q}$ was found in [GR93]. The case $q = 2$ (quaternions) was already done in [Jam70].

5.3.1. *Matrix algebras.* A simple special case of Theorem 1.2 is that that the matrix algebras $M_n(\mathbb{D})$ where $D = \mathbb{R}, \mathbb{C}, \mathbb{H}$ with the conjugate-transpose involution are polarizable, and the polarization constant is $\kappa = \frac{n\delta}{(n-1)\delta+2} I_n$, where $\delta = \dim_\mathbb{R} \mathbb{D}$. Here we note some further information about polarizing subgroups of $M_n(\mathbb{R})$ and $M_n(\mathbb{C})$ obtained by using the classical theorem of Burnside that a subgroup of $GL_n(\mathbb{C})$ spans $M_n(\mathbb{C})$ over $\mathbb{C}$ if and only if the natural representation of G on $\mathbb{C}^n$ by matrix multiplication is irreducible (see e.g. [Lan02]):

Proposition 5.6. *(1) A compact subgroup G of $\Gamma(M_n(\mathbb{R})) = O(n)$ is polarizing in $M_n(\mathbb{R})$ if and only if $G \neq \{I_n\}$ and the natural representation of G on $\mathbb{C}^n$ is irreducible.*

(2) A compact subgroup G of $\Gamma(M_n(\mathbb{C})) = U(n)$ is polarizing in $M_n(\mathbb{C})$ if and only if $G \neq \{I_n\}$, the natural representation of G on $\mathbb{C}^n$ is irreducible and $iI_n \in \mathrm{span}_{\mathbb{R}} G$ where I_n is the identity in $M_n(\mathbb{C})$.

Proof. Suppose that G is polarizing in $M_n(\mathbb{R})$. Then $\mu_1(G) = 0$ implies that G is non-trivial. Since G generates $M_n(\mathbb{R})$ as a real algebra it follows that G generates $M_n(\mathbb{C})$ as a complex algebra. Thus Burnside's theorem implies that the natural action of G on $\mathbb{C}^n$ is irreducible.

Conversely, if G acts irreducibly on $\mathbb{C}^n$, then G generates $M_n(\mathbb{C})$ as a complex algebra by Burnside's theorem. Since the matrices have real entries, G generates $M_n(\mathbb{R})$ as a real algebra. Then by part (b) of Proposition 3.2, $\mu_1(G) = 0$. Therefore G is polarizing in $M_n(\mathbb{R})$

Now suppose that G is polarizing in $M_n(\mathbb{C})$. Again, $\mu_1(G) = 0$ implies that G is nontrivial. Since G generates $M_n(\mathbb{C})$ as a real algebra, i.e. $\mathrm{span}_{\mathbb{R}} G = M_n(\mathbb{C})$, it follows that $iI_n \in \mathrm{span}_{\mathbb{R}} G$. It follows that $M_n(\mathbb{C}) = \mathrm{span}_{\mathbb{R}} G = \mathrm{span}_{\mathbb{C}} G$, and so Burnside's theorem says that the natural action of G on $\mathbb{C}^n$ is irreducible.

Conversely, suppose that G is nontrivial, the natural representation of G on $\mathbb{C}^n$ is irreducible, and $iI_n \in \mathrm{span}_{\mathbb{R}} G$. Burnside's theorem yields that G generates $M_n(\mathbb{C})$ as a complex algebra, i.e. $\mathrm{span}_{\mathbb{C}} G = M_n(\mathbb{C})$. But as was noted above, the fact that $iI_n \in \mathrm{span}_{\mathbb{R}} G$ implies that $\mathrm{span}_{\mathbb{R}} G = \mathrm{span}_{\mathbb{C}} G = M_n(\mathbb{C})$. Then again Proposition 3.2 shows that $\mu_1(G) = 0$. Therefore G is polarizing in $M_n(\mathbb{C})$. $\qquad\square$

As a result we have the following:

Proposition 5.7. *The group $SO(n)$ (resp. $SU(n)$) is polarizing in $M_n(\mathbb{R})$ (resp. $M_n(\mathbb{C})$) if and only if $n \geqslant 3$.*

Proof. If $n = 1, 2$ it is clear that $SO(n)$ (resp. $SU(n)$) fails to span the algebra $M_n(\mathbb{R})$ (resp. $M_n(\mathbb{C})$): note that $SO(2)$ (resp. $SU(2)$) generates an algebra isomorphic to $\mathbb{C}$ (resp. $\mathbb{H}$). Also it is not difficult to show that the natural representation of $SO(n)$ on $\mathbb{C}^n$ is irreducible using Schur's lemma. The same holds for $SU(n)$ as it contains $SO(n)$. To complete the proof we only need to verify that $iI_n \in \mathrm{span}_{\mathbb{R}}(SU(n))$ for $n \geqslant 3$.

If $n = 4k$ for some $k \geqslant 1$, then in fact $iI_n \in SU(n)$. If $n = 4k + 1$ for some $k \geqslant 1$, consider the diagonal matrices $D_\ell \in M_{4k+1}(\mathbb{C})$ with a 1 in the ℓ-th entry and an i in each other entry. Each of these is in $SU(4k + 1)$ and $D_\ell - D_\ell^{-1}$ is the diagonal matix with a 0 in the ℓ-th entry and $2i$ in each of the other entries. Thus

$$iI_{4k+1} = \frac{1}{8k} \sum_{\ell=1}^{4k+1} (D_\ell - D_\ell^{-1}) \in \mathrm{span}_{\mathbb{R}} SU(4k + 1).$$

A similar argument can be used to show that $iI_{4k+3} \in \mathrm{span}_{\mathbb{R}} SU(4k + 3)$ for $k \geqslant 0$ by considering the diagonal matrices $D_\ell \in SU(4k + 3)$ with a -1 in the ℓ-th entry and an i in each other entry. Thus

$$iI_{4k+3} = \frac{1}{2(4k + 2)} \sum_{\ell=1}^{4k+3} (D_\ell - D_\ell^{-1}) \in \mathrm{span}_{\mathbb{R}} SU(4k + 3).$$

For $n = 4k + 2$, $k \geqslant 1$, a further modification is needed. In this case we consider the diagonal matrices $D_{k,\ell} \in SU(4k+2)$ with a 1 in the k-th and ℓ-th entries and an i in each other entry for $1 \leqslant k < \ell \leqslant n$. Then there are $n(n-1)/2 = (4k+2)(4k+1)/2$ summands $D_{k,\ell} - D_{k,\ell}^{-1}$, and $n - 1 = 4k + 1$ of them have a 0 in a given entry and a $2i$ in each other entry. Thus

$$iI_{4k+2} = \frac{1}{4k(4k+1)} \sum_{1 \leqslant k < \ell \leqslant n} (D_{k,\ell} - D_{k,\ell}^{-1}) \in \mathrm{span}_{\mathbb{R}} SU(4k+2).$$

$\square$

References

[CS03]   John H. Conway and Derek A. Smith. *On quaternions and octonions: their geometry, arithmetic, and symmetry.* A K Peters, Ltd., Natick, MA, 2003.

[D'A02] John P. D'Angelo. *Inequalities from complex analysis*, volume 28 of *Carus Mathematical Monographs*. Mathematical Association of America, Washington, DC, 2002.

[FP03]   Douglas R. Farenick and Barbara A. F. Pidkowich. The spectral theorem in quaternions. *Linear Algebra Appl.*, 371:75–102, 2003.

[GR93]   Dante M. Giarrusso and Joseph D. Romano. A polarization formula for Clifford modules. *Linear and Multilinear Algebra*, 35(3-4):191–194, 1993.

[Hal51] Paul R. Halmos. *Introduction to Hilbert Space and the theory of Spectral Multiplicity.* Chelsea Publishing Company, New York, N. Y., 1951.

[Her75] I. N. Herstein. *Topics in algebra.* Xerox College Publishing, Lexington, Mass.-Toronto, Ont., second edition, 1975.

[HJ13]   Roger A. Horn and Charles R. Johnson. *Matrix analysis.* Cambridge University Press, Cambridge, second edition, 2013.

[Hua44] Loo-Keng Hua. On the theory of automorphic functions of a matrix variable. II. The classification of hypercircles under the symplectic group. *Amer. J. Math.*, 66:531–563, 1944.

[Isa76] I. Martin Isaacs. *Character theory of finite groups.* Pure and Applied Mathematics, No. 69. Academic Press [Harcourt Brace Jovanovich, Publishers], New York-London, 1976.

[Jam70] James Edward Jamison. *Extension of some theorems of complex functional analysis to linear spaces over the Quaternions and Cayley numbers.* ProQuest LLC, Ann Arbor, MI, 1970. Thesis (Ph.D.)–University of Missouri - Rolla.

[JvN35] P. Jordan and J. von Neumann. On inner products in linear, metric spaces. *Ann. of Math. (2)*, 36(3):719–723, 1935.

[Lam01] T. Y. Lam. *A first course in noncommutative rings*, volume 131 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, second edition, 2001.

[Lan02] Serge Lang. *Algebra*, volume 211 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, third edition, 2002.

[LM89]   H. Blaine Lawson, Jr. and Marie-Louise Michelsohn. *Spin geometry*, volume 38 of *Princeton Mathematical Series*. Princeton University Press, Princeton, NJ, 1989.

[Nac76] Leopoldo Nachbin. *The Haar integral.* Robert E. Krieger Publishing Co., Huntington, N.Y., 1976. Translated from the Portuguese by Lulu Bechtolsheim, Reprint of the 1965 edition.

[Rod14] Leiba Rodman. *Topics in quaternion linear algebra.* Princeton Series in Applied Mathematics. Princeton University Press, Princeton, NJ, 2014.

[Sch85] Winfried Scharlau. *Quadratic and Hermitian forms*, volume 270 of *Grundlehren der mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]*. Springer-Verlag, Berlin, 1985.

[Wat95] William C. Waterhouse. Polarization formulas over separable algebras. *J. Algebra*, 173(2):271–280, 1995.

[Wil05] N. J. Wildberger. *Divine proportions.* Wild Egg, Kingsford, 2005. Rational trigonometry to universal geometry.

[You88] Nicholas Young. *An introduction to Hilbert space.* Cambridge Mathematical Textbooks. Cambridge University Press, Cambridge, 1988.

DEPARTMENT OF MATHEMATICS, CENTRAL MICHIGAN UNIVERSITY, MT. PLEASANT, MI 48859, USA

Email address: chakr2d@cmich.edu

DEPARTMENT OF MATHEMATICS, CENTRAL MICHIGAN UNIVERSITY, MT. PLEASANT, MI 48859, USA

Email address: chakr2d@cmich.edu