Turkish Journal of Mathematics

http://journals.tubitak.gov.tr/math/

Research Article

Turk J Math
(2023) 47: 1944 – 1954
© TÜBİTAK
doi:10.55730/1300-0098.3474

Involutive automorphisms and derivations of the quaternions

Eyüp KIZIL[1*], **Adriano DA SILVA**[2], **Okan DUMAN**[1]
[1]Department of Mathematics, Yıldız Technical University, İstanbul, Turkiye
[2]Department of Mathematics, University of Tarapaca, Iquique, Chile

Received: 28.05.2023 • **Accepted/Published Online:** 06.09.2023 • **Final Version:** 09.11.2023

Abstract: Let $Q = (\frac{a,b}{\mathbb{R}})$ denote the quaternion algebra over the reals which is by the Frobenius Theorem either split or the division algebra H of Hamilton's quaternions. We have presented explicitly in [4] the matrix of a typical derivation of Q. Given a derivation $d \in Der(H)$, we show that the matrix $D \in M_3(\mathbb{R})$ that represents d on the linear subspace $H_0 \simeq \mathbb{R}^3$ of pure quaternions provides a pair of idempotent matrices $AdjD$ and $-D^2$ that correspond bijectively to the involutary matrix Σ of a quaternion involution σ and present several equations involving these matrices. In particular, we deal with commuting derivations of H and introduce some results to guarantee commutativity. We also mention briefly eigenspace decomposition of a derivation.

Key words: Derivation, quaternion, involution, automorphism

1. Introduction

It is well known by the Frobenius Theorem that a quaternion algebra over the field of reals is either split or the set of Hamilton's quaternions. We have explicitly determined in [4] derivations of such an algebra in their matrix forms and it is well known that any derivation of such an algebra is always inner. Following Hilbert symbol we denote by $Q = (\frac{a,b}{\mathbb{R}})$ the quaternion algebra over $\mathbb{R}$ equipped with the quaternionic multiplication. Since Q is central, its center is $\mathbb{R}$ so that one might consider the decomposition $Q = \mathbb{R} \oplus Q_0$ where Q_0 is the set of all quaternions without scalar part (i.e. pure quaternions) and is identified with $\mathbb{R}^3$.

A linear map $d : Q \to Q$ satisfying the Leibnitz rule is called a derivation for Q and since it must be inner there exists a quaternion $p \in Q$ such that $d = ad(p)$ which means $d(q) = pq - qp$ for every $q \in Q$. It follows at once from the definition that d as a map sends the center of Q to zero and hence the matrix that represents it (w.r.t. the standard quaternionic basis) reduces actually to a 3×3 submatrix, say D. This is because the first row and first column of matrix d are trivial subspaces of $\mathbb{R}^4$. We prove that d distributes the quaternionic multiplication for pure quaternions according to Leibnitz rule. More precisely, we have for every $\mathbf{p}, \mathbf{q}$ in Q_0 both equations $d(\langle \mathbf{p}, \mathbf{q} \rangle) = \langle d\mathbf{p}, \mathbf{q} \rangle + \langle \mathbf{p}, d\mathbf{q} \rangle$ and $d(\mathbf{p} \times \mathbf{q}) = (d\mathbf{p} \times \mathbf{q}) + (\mathbf{p} \times d\mathbf{q})$.

On the other hand, a typical involutive automorphism of $\sigma : Q \to Q$ -as a linear map that is both (anti)-homomorphism and self-inverse- is given by $\sigma_{\mathbf{u}}(q) = -\mathbf{u}q\mathbf{u}$ where $\mathbf{u} \in Q_0$ is a unit vector. A simple computation shows that the matrix, say Σ, that represents $\sigma_{\mathbf{u}}$ (or simply σ) is indeed involutary and a well-

*Correspondence: kizil@yildiz.edu.tr
2010 *AMS Mathematics Subject Classification:* 16W20 , 11R52

known fact from linear algebra says that given an involutary matrix S the mapping $g(S) = (I \pm S)/2$ provides idempotent matrices associated to S. Reciprocally, if A is an idempotent matrix then $f(A) = 2A - I$ results an involutary matrix. In the present context we show that idempotent variants of D that correspond in an bijective way to Σ are the adjoint matrix $AdjD$ of D and $-D^2$. Note that the negative sign here makes the difference since D^2 fails to be idempotent as we emphasize.

It should be also noted that neither derivations nor involutions commute in general. Hence we also provide some simple conditions to ensure commuting derivations. On the other hand, as a real skew-symmetric matrix, D admits either zero or purely imaginary eigenvalues. In fact, $\lambda = 0, \pm \mathrm{i}$ (complex i) are the only eigenvalues of D and hence Q might be also decomposed as $Q = E(0) \oplus E(\mathrm{i}) \oplus E(-\mathrm{i})$ where $E(\lambda) = \{q \in Q : (D - \lambda I)q = 0\}$ is the eigenspace corresponding to the eigenvalue $\lambda \in \{0, \pm\mathrm{i}\}$. In particular, $E(0)$ is spanned by the fixed vector $\mathbf{u}$ while $E(\pm\mathrm{i})$ represents a plane passing through the origin generated by the real and imaginary part of the complex eigenvector $q \pm \mathrm{i}p$ corresponding to $\pm\mathrm{i}$.

The paper is organized as follows: In Section 2, we give a quite brief exposition on real quaternion algebras that will be useful for the rest of the article. Section 3 treats quaternion derivation matrices. We focus on idempotent variants of such a matrix and show in the last section how these variants become closely related to quaternion involutions. We also deal with characteristic polynomial of a quaternion derivation that reveal further interesting insights about quaternion derivations. In the last section 4 we deal with quaternion involutions and show that associated with the matrix of such an involution one might correspond in a bijective manner to a pair of idempotent matrices derived from quaternion derivations.

2. Quaternion algebra

An *algebra* $\mathcal{A}$ over F means a finite-dimensional vector space over F equipped with an associative multiplication with identity 1 that relates to vector addition and scalar multiplication according to appropriate and well-known laws for algebras. We will sometimes refer to an algebra $\mathcal{A}$ over the field F simply as an F-algebra and identify F with the subalgebra $F1$ of $\mathcal{A}$, since the map $r \mapsto r1$ is an isomorphic embedding of F into $\mathcal{A}$. We say that an F-algebra $\mathcal{A}$ is central if its center is F, that is, $Z(\mathcal{A}) = F$.

The following well-known way of constructing a quaternion algebra might be found in many textbook but we refer to [3] and define a quaternion algebra via generators and relations as follows:

Definition 2.1 *An algebra $\mathcal{A}$ over a field F of characteristic not 2 is a quaternion algebra if there is a basis $1, i, j, k$ for $\mathcal{A}$ as an F-vector space such that*

$$i^2 = a, \quad j^2 = b, \quad \text{and} \quad ij = k = -ji \tag{2.1}$$

for some non-zero $a, b \in F$.

It follows from (2.1) that $k^2 = -ab, jk = -bi = -kj$ and $ki = -aj = -ik$. For $0 \neq a, b \in F$ we denote by $Q = (\frac{a,b}{F})$ (Hilbert symbol) the quaternion algebra over F with F-basis $1, i, j, k$ subject to the multiplication (2.1). And by an element (i.e. a quaternion) of Q we will understand $q = r + x_0 i + y_0 j + z_0 k$ with $r, x_0, y_0, z_0 \in F$.

Note that any quaternion algebra with $\mathrm{char}(F) \neq 2$ is given by this way: If $\mathcal{A}$ is a quaternion algebra over F then there exist non-zero $a, b \in F$ such that $\mathcal{A} \simeq (\frac{a,b}{F})$. Since a quaternion algebra is generated by the generators i, j satisfying (2.1), the map that interchanges i and j gives a natural isomorphism $(\frac{a,b}{F}) \simeq (\frac{b,a}{F})$. According to this set up, when $F = \mathbb{R}$, varying the Hilbert symbols we get 4 possibilities: (i) $(\frac{-1,1}{\mathbb{R}})$, (ii) $(\frac{1,-1}{\mathbb{R}})$, (iii) $(\frac{1,1}{\mathbb{R}})$ and (iv) $(\frac{-1,-1}{\mathbb{R}})$. However, up to isomorphism (i) and (ii) means the same algebra and hence we reduce to 3 possibilities. On the other hand, the Frobenius Theorem says that up to isomorphism there are only two real quaternion algebras: $(\frac{1,1}{\mathbb{R}}) \simeq M_2(\mathbb{R})$ the algebra of 2×2-matrices with real entries and $(\frac{-1,-1}{\mathbb{R}}) = H$, the algebra of Hamilton's quaternions. Finally, since $(\frac{1,-1}{\mathbb{R}}) \simeq M_2(\mathbb{R})$ (and hence by transitivity $(\frac{-1,1}{\mathbb{R}}) \simeq (\frac{1,1}{\mathbb{R}})$) it follows that (i)-(ii)-(iii) actually means the same algebra and thus we have indeed only two quaternion algebras over $\mathbb{R}$. It is also clear that a quaternion algebra Q over F is central.

Remark 2.2 *What is considered in [7] as* generalized quaternion algebra *over the real numbers is actually the Definition (2.1) itself with a* $\mathbb{R}$*-basis* e_0, e_1, e_2, e_3 *subject to the multiplication* $e_1^2 = ae_0$, $e_2^2 = be_0$ *and* $e_1e_2 = e_3 = -e_2e_1$ *where* $a = -\alpha$ *and* $b = -\beta$ *for some* $\alpha, \beta \in \mathbb{R} \setminus \{0\}$.

As usual, if $q = r + x_0i + y_0j + z_0k \in Q$ we let $\mathbf{q} = x_0i + y_0j + z_0k$ to stand for its vector part and use the representation $q = r + \mathbf{q}$ whenever it is more convenient for formatting. In particular, if $q \in H = (\frac{-1,-1}{\mathbb{R}})$ then we say q is real if $q \in \mathbb{R}$, and we say q is pure (or imaginary) if $q = x_0i + y_0j + z_0k$. However, the notion of *pure quaternion* is not addressed exclusively to a particular basis and one might define a pure quaternion for a quaternion algebra $Q = (\frac{a,b}{F})$ with $a, b \in F \setminus \{0\}$. In fact, if $q = r + x_0i + y_0j + z_0k \in Q$ is a non-zero element, then $r = 0$ is equivalent to say that $q \notin F$ and $q^2 \in F$.

We denote by Q_0 the linear subspace of $Q = (\frac{a,b}{\mathbb{R}})$ spanned by $\{i, j, k\}$ which consists of only pure quaternions. In particular, we have the set

$$Q_0 \setminus \{0\} = \{q \in Q : q \notin \mathbb{R}, q^2 \in \mathbb{R}\}$$

of non-zero pure quaternions and hence $Q = \mathbb{R} \oplus Q_0$. Given $q = r + x_0i + y_0j + z_0k \in Q$ we define the *quaternionic conjugation map* J on Q by

$$J(q) = \overline{q} = r - x_0i - y_0j - z_0k$$

and the *norm* map N on Q by

$$N(q) = q\overline{q} = \overline{q}q = r^2 - ax_0^2 - by_0^2 + abz_0^2 \in \mathbb{R}.$$

Note that $J(pq) = J(q)J(p)$ and $J(p + q) = J(p) + J(q)$ for every $p, q \in Q$ and we denote the matrix of J by the same letter $J = diag\{1, -I\}$ with I being the identity matrix. One might consider the slightly different versions of the familiar dot and cross product in $\mathbb{R}^3$ as follows:

$$\mathbf{v} \times \mathbf{w} = \det \begin{pmatrix} -bi & -aj & k \\ v_1 & v_2 & v_3 \\ w_1 & w_2 & w_3 \end{pmatrix} \tag{2.2}$$

and

$$\langle \mathbf{v}, \mathbf{w} \rangle = -av_1w_1 - bv_2w_2 + abv_3w_3 \tag{2.3}$$

for $\mathbf{v} = (v_1, v_2, v_3)$, $\mathbf{w} = (w_1, w_2, w_3) \in \mathbb{R}^3$ and $a, b < 0$. Note that $Q = (\frac{a,b}{\mathbb{R}}) \simeq H$ which occurs if and only if $a < 0$ and $b < 0$. Given $p, q \in Q$ the quaternionic multiplication on Q is defined by $pq = rs - \langle \mathbf{p}, \mathbf{q} \rangle + s\mathbf{p} + r\mathbf{q} + \mathbf{p} \times \mathbf{q}$ where $p = r + \mathbf{p}$ and $q = s + \mathbf{q}$ with $r, s \in \mathbb{R}$. In particular, we have the following significant formula for Q_0:

$$\mathbf{pq} = -\langle \mathbf{p}, \mathbf{q} \rangle + \mathbf{p} \times \mathbf{q} \tag{2.4}$$

which simply says the set Q_0 is not closed under multiplication.

3. Quaternion derivations

Derivations of an algebra might be useful for exploring the algebraic structure. We have presented in [4] the matrix of an arbitrary derivation of the quaternion algebra $Q = (\frac{a,b}{\mathbb{R}})$ over the reals and our main purpose here is to connect derivations and involutions of Q. Hence, we find it convenient to start with some basic definitions for the sake of clarity.

Definition 3.1 *A linear map $d : \mathcal{A} \to \mathcal{A}$ of an algebra $\mathcal{A}$ satisfying the Leibnitz law $d(xy) = d(x)y + xd(y)$ for all $x, y \in \mathcal{A}$ is called a derivation of $\mathcal{A}$. In particular, associated to an element $x \in \mathcal{A}$ one has an inner derivation $d = ad(x)$ defined by $d(y) = xy - yx$ for every $y \in \mathcal{A}$.*

Denote by $Der(\mathcal{A})$ the vector space of all derivations of $\mathcal{A}$. From now on, we mean by $\mathcal{A}$ the quaternion algebra $Q = (\frac{a,b}{\mathbb{R}})$ unless otherwise explicitly stated. For further references, we quote our earlier result that states a typical derivation of Q in its matrix form as follows:

Lemma 3.2 *(Theorem 3.5,[4]) If d is a derivation of the quaternion algebra $Q = (\frac{a,b}{\mathbb{R}})$ over $\mathbb{R}$, then its matrix (also denoted by d) is of the form $d = diag\{0, D\}$ with D as*

$$D = \begin{pmatrix} 0 & -\frac{b}{a}z & y \\ z & l & ax \\ \frac{1}{b}y & x & l \end{pmatrix}, \tag{3.1}$$

for some $z, y, x, l \in \mathbb{R}$ such that $l = l(b)$ is zero if $b \neq 0$ and non-zero otherwise.

We usually prefer the bold face letters (i.e. $\mathbf{0} = (0, 0, 0) \in \mathbb{R}^3$) to denote 3-vectors in space and combine the scalars z, y, x in D to form $\mathbf{u} = xi + yj + zk$ (in this order). The reason is that Q has only inner derivations and hence given a derivation d there corresponds a 3-vector whose adjoint is equal to d on Q_0. Sometimes we will simply say $\mathbf{u}$ is associated to $D \in M_3(\mathbb{R})$ rather than $d \in Der(Q)$. In particular, when $Q = H$ the matrix D reads as

$$D = \begin{pmatrix} 0 & -z & y \\ z & 0 & -x \\ -y & x & 0 \end{pmatrix} \tag{3.2}$$

and hence $col_1(D) = d(i) = zj - yk$, $col_2(D) = d(j) = -zi + xk$ and $col_3(D) = d(k) = yi - xj$. If Q is split then the columns of D are such that $col_1(D) = d(i) = zj + yk$, $col_2(D) = d(j) = zi + xk$ and $col_3(D) = d(k) = yi - xj$.

It is obvious that different choices of $\mathbf{u}$ result in different inner derivations and once we fix $\mathbf{u} = xi+yj+zk$ and consider $d(q)$ where $d = ad(\mathbf{u})$ and $q = r + x_0 i + y_0 j + z_0 k$ we need to distinguish $\mathbf{u}$ and the vector part $x_0 i + y_0 j + z_0 k$ of q. In Section 4 where we treat quaternion involutions, $\mathbf{u}$ will be additionally chosen with norm $N(\mathbf{u}) = 1$ which is of course not essential for a quaternion derivation.

It should be noted that the above Lemma provides also derivations of (split)semi-quaternions for which b is identically zero. Since the quaternion algebra $Q = (\frac{a,b}{\mathbb{R}})$ is either Hamiltonian or split we restrict our attention to either $a = b = -1$ or $a = -1$, $b = 1$ and hence the diagonal entries of D are all zero here and D is a singular traceless matrix independently from the choice of $a, b \in \mathbb{R} \setminus \{0\}$ and $\mathbf{u} \in \mathbb{R}^3 \setminus \{0\}$. In particular, if $Q \simeq H$ then D is such that $D^T = -D$ which means transpose of a derivation $d \in Der(H)$ is still a derivation, a fact that does not hold in general. If Q is split then D is neither symmetric nor skew-symmetric in general but continues to be a derivation, too.

An observation shows that a derivation $d \in Der(Q)$ might appear as a transpose of another derivation if their associated vectors differ only by the same opposite sign in each coordinate as we prove in the next.

Proposition 3.3 *Let $d_1 = ad(\mathbf{u}_1)$ and $d_2 = ad(\mathbf{u}_2)$ be two derivations of Q for some $\mathbf{u}_1, \mathbf{u}_2 \in Q_0$. Then $d_1 = d_2^T$ (resp. $d_2 = d_1^T$) if and only if $\mathbf{u}_2 = -\mathbf{u}_1$ (resp. $\mathbf{u}_1 = -\mathbf{u}_2$) and this holds if and only if $Q \simeq H$.*

Proof Let $\mathbf{u}_1 = x_1 i + y_1 j + z_1 k$ and $\mathbf{u}_2 = x_2 i + y_2 j + z_2 k$. It follows at once that

$$D_1 = \begin{pmatrix} 0 & -\frac{b}{a} z_1 & y_1 \\ z_1 & 0 & a x_1 \\ \frac{1}{b} y_1 & x_1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & z_2 & \frac{1}{b} y_2 \\ -\frac{b}{a} z_2 & 0 & x_2 \\ y_2 & a x_2 & 0 \end{pmatrix} = D_2^T$$

which occurs if and only if (i) $x_2 = a x_1,\ y_2 = b y_1,\ a z_2 = -b z_1$ and (ii) $x_1 = a x_2,\ y_1 = b y_2,\ a z_1 = -b z_2$. Thus, $D_1 = D_2^T$ (resp. $D_2 = D_1^T$) if and only if $a = b = -1$ which implies in turn $\mathbf{u}_2 = -\mathbf{u}_1$ (resp. $\mathbf{u}_1 = -\mathbf{u}_2$).

For the split case, it is evident by the signature* $-,+,+$ (resp. $+,-,+$ and $+,+,-$) that $\mathbf{u}_2$ (resp. $\mathbf{u}_1$) is in general not the opposite of $\mathbf{u}_1$ (resp. $\mathbf{u}_2$). □

It is also quite clear that the composition $d_1 d_2$ (resp. $d_2 d_1$) of two derivations d_1 and d_2 of Q may fail to be a derivation and $d_1 d_2$ and $d_2 d_1$ might be different (whenever exist). A simple commuting result is given below:

Proposition 3.4 *Given $\mathbf{u}_1, \mathbf{u}_2 \in Q_0$ and let $d_1 = ad(\mathbf{u}_1)$ and $d_2 = ad(\mathbf{u}_2)$. Then $d_1 d_2 = d_2 d_1$ if and only if $\mathbf{u}_1 \parallel \mathbf{u}_2$.*

Proof Let $\mathbf{u}_1 = x_1 i + y_1 j + z_1 k$ and $\mathbf{u}_2 = x_2 i + y_2 j + z_2 k$. If we write each D_n $(n = 1, 2)$ associated to $\mathbf{u}_n$ and apply standard matrix multiplication we see that $D_1 D_2 = D_2 D_1$ if and only if $x_1 y_2 = x_2 y_1,\ x_1 z_2 = x_2 z_1$ and $y_1 z_2 = y_2 z_1$. However, these conditions define each component of the cross product

$$\mathbf{u}_1 \times \mathbf{u}_2 = -b(y_1 z_2 - y_2 z_1) i + a(x_1 z_2 - x_2 z_1) j + (x_1 y_2 - x_2 y_1) k$$

to be zero and this completes the proof. □

*By the signatures $-,+,+$; $+,-,+$; $+,+,-$ we mean for (a,b) the possibilities $(-1,1)$, $(1,-1)$ and $(1,1)$. Hence, $\mathbf{u}_2 = -\mathbf{u}_1$ (or $\mathbf{u}_1 = -\mathbf{u}_2$) iff the signature is $-,-,-$ that correspond to $(a,b) = (-1,-1)$.

Note that the first column of d spans a trivial subspace of $\mathbb{R}^4$ since $d(1)1 = d(1)i = d(1)j = d(1)k = 0$ for the basis element $1, i, j, k$. To see that the first row $row_1(d)$ of d also consists of only zeros one has to solve the equations (as we have done in [4]) $D(i^2) = D(i)i + iD(i)$, $D(j^2) = D(j)j + jD(j)$ and $D(k^2) = D(k)k + kD(k)$. However, the following Proposition justifies in an alternative way why this should be indeed the case without solving the above equations.

Lemma 3.5 *Let $d \in Der(Q)$. Then d maps the center of Q to zero, that is, derivations of Q are center annihilating.*

Proof An immediate computation shows that $d(1) = d(1 \cdot 1) = d(1)1 + 1d(1)$ and hence $d(1) = 0$ which implies $d(r) = d(r1) = rd(1) = 0$ for every $r \in \mathbb{R} = Z(Q)$. □

Despite its simplicity, Lemma 3.5 might be quite useful to derive some other results. For example, $\langle d\mathbf{p}, \mathbf{q}\rangle + \langle \mathbf{p}, d\mathbf{q}\rangle = 0$ as we prove in the next Proposition and since $d(\langle \mathbf{p}, \mathbf{q}\rangle) = 0$ it seems that d maintains the Leibnitz rule on the product $\langle \cdot, \cdot \rangle$. Since the cross product $\times$ and $\langle \cdot, \cdot \rangle$ together completely determine the quaternionic multiplication for pure quaternions in Q_0 one might ask if d behaves in a similar manner also on the product $\times$. For the one thing, $d(\mathbf{p} \times \mathbf{q}) \neq d\mathbf{p} \times d\mathbf{q}$ if we take $Q = H$ and consider $d = diag\{0, D\}$ with D such that $d(i) = zj - yk$, $d(j) = -zi + xk$ and $d(k) = yi - xj$. It follows that $d(i \times j) = d(k) = yi - xj$ while $d(i) \times d(j) = xzi + yzj + z^2k = z\mathbf{u}$ so that $d(i \times j) \neq d(i) \times d(j)$. Nonetheless, we prove below that d distributes $\times$ according to the Leibnitz rule:

Proposition 3.6 *Let $d \in Der(Q)$. Then $d(\langle \mathbf{p}, \mathbf{q}\rangle) = \langle d\mathbf{p}, \mathbf{q}\rangle + \langle \mathbf{p}, d\mathbf{q}\rangle = 0$ and $d(\mathbf{p} \times \mathbf{q}) = (d\mathbf{p} \times \mathbf{q}) + (\mathbf{p} \times d\mathbf{q}), \forall \mathbf{p}, \mathbf{q} \in Q_0$.*

Proof Let $\mathbf{p} = x_1 i + y_1 j + z_1 k$ and $\mathbf{q} = x_2 i + y_2 j + z_2 k$. By Lemma 3.5 we have $d(\langle \mathbf{p}, \mathbf{q}\rangle) = 0$. On the other hand, $d\mathbf{p} = x_1 d(i) + y_1 d(j) + z_1 d(k)$ and $d\mathbf{q} = x_2 d(i) + y_2 d(j) + z_2 d(k)$ where $d(i), d(j)$ and $d(k)$ are the columns of D as said earlier. It follows that

$$d\mathbf{p} = (yz_1 - y_1 z)i + (x_1 z - xz_1)j + (xy_1 - x_1 y)k$$

and

$$d\mathbf{q} = (yz_2 - y_2 z)i + (x_2 z - xz_2)j + (xy_2 - x_2 y)k.$$

Hence,

$$\langle d\mathbf{p}, \mathbf{q}\rangle = x_2 yz_1 - x_2 y_1 z + x_1 y_2 z - xy_2 z_1 + xy_1 z_2 - x_1 yz_2$$

and

$$\langle \mathbf{p}, d\mathbf{q}\rangle = x_1 yz_2 - x_1 y_2 z + x_2 y_1 z - xy_1 z_2 + (xy_2 z_1 - x_2 yz_1$$

so that $\langle d\mathbf{p}, \mathbf{q}\rangle + \langle \mathbf{p}, d\mathbf{q}\rangle = 0$.

On the other hand, if we apply d to the equation in (2.4) and use the fact that $d(r) = 0, \forall r \in \mathbb{R}$ we obtain $d(\mathbf{pq}) = -d(\langle \mathbf{p}, \mathbf{q}\rangle) + d(\mathbf{p} \times \mathbf{q}) = d(\mathbf{p} \times \mathbf{q})$ and hence $(d\mathbf{p})\mathbf{q} + \mathbf{p}(d\mathbf{q}) = d(\mathbf{p} \times \mathbf{q})$. If we write (2.4) for both pairs $d\mathbf{p}, \mathbf{q} \in Q$ and $\mathbf{p}, d\mathbf{q} \in Q$ we get $(d\mathbf{p})\mathbf{q} = -\langle d\mathbf{p}, \mathbf{q}\rangle + d\mathbf{p} \times \mathbf{q}$ and $\mathbf{p}(d\mathbf{q}) = -\langle \mathbf{p}, d\mathbf{q}\rangle + \mathbf{p} \times d\mathbf{q}$. Thus, $(d\mathbf{p})\mathbf{q} + \mathbf{p}(d\mathbf{q}) = -\langle d\mathbf{p}, \mathbf{q}\rangle + d\mathbf{p} \times \mathbf{q} - \langle \mathbf{p}, d\mathbf{q}\rangle + \mathbf{p} \times d\mathbf{q} = d(\mathbf{p} \times \mathbf{q})$ which holds if and only if $\langle d\mathbf{p}, \mathbf{q}\rangle + \langle \mathbf{p}, d\mathbf{q}\rangle = 0$ and $d\mathbf{p} \times \mathbf{q} + \mathbf{p} \times d\mathbf{q} = d(\mathbf{p} \times \mathbf{q})$, as claimed. □

The action of the conjugation map J of Q on $Der(Q)$ is also interesting since any derivation combined on the left or right by J continues to be a derivation. Since the proof is essentially the same if Q is Hamiltonian or split we provide it only in the case $Q \simeq H$ as follows:

Proposition 3.7 *Given $d \in Der(H)$, we have $dJ = Jd = -d$ and, in particular, $DJ = JD = -D$.*

Proof Given $q = r + x_0 i + y_0 j + z_0 k \in H$ and denote by $d = ad(\mathbf{u})$ for some $\mathbf{u} = xi + yj + zk \in H_0$. Since $d(r) = 0$ it follows that $d(q) = x_0 d(i) + y_0 d(j) + z_0 d(k)$ and hence $d(q) = (yz_0 - y_0 z)i + (x_0 z - xz_0)j + (xy_0 - x_0 y)k$. Now, we write

$$(Jd)(q) = (y_0 z - yz_0)i + (xz_0 - x_0 z)j + (x_0 y - xy_0)k.$$

On the other hand,

$$\begin{aligned} (dJ)(q) &= d(r - x_0 i - y_0 j - z_0 k) \\ &= -x_0 d(i) - y_0 d(j) - z_0 d(k) \text{ (and hence } dJ(q) = -d(q)) \\ &= (y_0 z - yz_0)i + (xz_0 - x_0 z)j + (x_0 y - xy_0)k \\ &= (Jd)(q) \end{aligned}$$

which means $dJ = -d = Jd$. Since both $d = diag\{0, D\}$ and $J = diag\{1, -I\}$ are block-diagonal matrices, $dJ = diag\{0, -D\} = Jd$ implies the second assertion. □

Corollary 3.8 *Given $\mathbf{p}, \mathbf{q} \in H$, it follows that $(dJ)(\mathbf{pq}) = (Jd)(\mathbf{pq})$.*

Proof In fact, $(dJ)(\mathbf{pq}) = d(J(\mathbf{q})J(\mathbf{p})) = (dJ)(\mathbf{q})J(\mathbf{p}) + J(\mathbf{q})(dJ)(\mathbf{p})$ while $(Jd)(\mathbf{pq}) = J(d(\mathbf{p})\mathbf{q} + \mathbf{p}d(\mathbf{q})) = J(d(\mathbf{p})\mathbf{q}) + J(\mathbf{p}d(\mathbf{q}))$ and hence $(Jd)(\mathbf{pq}) = J(\mathbf{q})(Jd)(\mathbf{p}) + (Jd)(\mathbf{q})J(\mathbf{p})$ so that $(dJ)(\mathbf{pq}) = (Jd)(\mathbf{pq})$ if and only if $dJ = Jd$ on H. □

Remark 3.9 *If $d \in Der(Q)$ where $Q = (\frac{-1,1}{\mathbb{R}})$, then D is such that $col_1(D) = d(i) = zj + yk$, $col_2(D) = d(j) = zi + xk$ and $col_3(D) = d(k) = yi - xj$ but the same proof above still applies also in the split case.*

We emphasize now that some matrix variants of D become important in what follows and although the condition $N(\mathbf{u}) = 1$ for $\mathbf{u} \in Q_0$ is not essential for D we gain with this simple assumption interesting properties of some variants of D such as $AdjD$, $-D^2$:

$$AdjD = \begin{pmatrix} -ax^2 & xy & -bxz \\ \frac{a}{b}xy & -\frac{1}{b}y^2 & yz \\ xz & -\frac{1}{a}yz & \frac{b}{a}z^2 \end{pmatrix} \tag{3.3}$$

and the matrix

$$-D^2 = \begin{pmatrix} \frac{b}{a}z^2 - \frac{1}{b}y^2 & -xy & bxz \\ -\frac{a}{b}xy & \frac{b}{a}z^2 - ax^2 & -yz \\ -xz & \frac{1}{a}yz & -ax^2 - \frac{1}{b}y^2 \end{pmatrix} \tag{3.4}$$

Both matrices $AdjD$ and $-D^2$ (not D^2) are (singular) idempotent (See Theorem 3.10 below) and correspond to a certain involutory matrix. In the present context, this involutory matrix is precisely the matrix of a quaternion involution, the subject of the next section. Since it is quite tedious to perform some elementary matrix operations with $AdjD$, $-D^2$ such as standard multiplication, power, etc we refer the reader to linear algebra packages available on the web[†]. Since Q is either H or split we will content ourselves with one of these (or both) cases.

Theorem 3.10 *Let $\mathbf{u} \in H_0$ be such that $N(\mathbf{u}) = 1$ and let D be the matrix in (3.2). It follows that both $A = AdjD$ and $B = -D^2$ are (singular) symmetric idempotent matrices such that $AB = BA = O$ (zero matrix). Moreover,* $\operatorname{rank}(AdjD) = Tr(AdjD) = 1$, $\operatorname{rank}(-D^2) = Tr(-D^2) = 2$ *(resp.* $\operatorname{rank}(D^2) = 2$*) and hence* $\operatorname{rank}(D) = 2$.

Proof If we set $a = b = -1$ in (3.3) and (3.4) (and use $N(\mathbf{u}) = x^2 + y^2 + z^2 = 1$ to simplify diagonal entries of $\pm D^2$) we find the matrices A and $-B$ as

$$A = \begin{pmatrix} x^2 & xy & xz \\ xy & y^2 & yz \\ xz & yz & z^2 \end{pmatrix} \quad \text{and} \quad -B = \begin{pmatrix} x^2-1 & xy & xz \\ xy & y^2-1 & yz \\ xz & yz & z^2-1 \end{pmatrix} = D^2$$

from which the eq. $-B = A - I$ (or $I - A = B$) follows. It is straightforward to check that $AA = A$ for which the assumption $N(\mathbf{u}) = 1$ is indispensable. It is also evident that B is idempotent since

$$BB = (I - A)(I - A) = I - 2A + AA = I - 2A + A = I - A = B.$$

Remember that the identity matrix I is the only non-singular idempotent matrix and adjoint matrix of a singular matrix (i.e. D itself) is always singular. Hence both A and B are singular idempotent matrices. It should be noted that $-B = D^2$ fails to be idempotent since $(-B)(-B) = (A - I)(A - I) = I - A = B$.

If we multiply $I - A = B$ by A on the right we get $IA - AA = BA$ and hence $A - A = O = BA$. The same way, we multiply $I - A = B$ by A on the left and stay with $AI - AA = AB$ so that $A - A = O = AB$.

It is well known that trace of an idempotent matrix equals its rank. A simple observation at this point shows that $TrA = 1$ and $TrB = 2TrA = 2$ so that $\operatorname{rank}(A) = 1$ and $\operatorname{rank}(B) = 2$ as soon as we assume $N(\mathbf{u}) = 1$. That $\operatorname{rank}(D) = 2$ follows from the fact[‡] that $2 = \operatorname{rank}(DD) \leq \operatorname{rank}(D) < 3$. □

Remark 3.11 *1) It is well known (See Section 3.12 in [1]) that given a pair of idempotent matrices $A, B \in M_n(\mathbb{R})$ then $A + B = I$ if and only if $AB = BA = O$ and* $\operatorname{rank}(A) + \operatorname{rank}(B) = n$. *By Theorem 3.10, we already have $AdjD + (-D^2) = I$ which is in accordance with the rank criteria* $\operatorname{rank}(AdjD) + \operatorname{rank}(-D^2) = 3$.

2) The validity of $AdjD + (-D^2) = I$ also follows by Cayley-Hamilton Theorem. In fact, the characteristic polynomial $\mathbf{p}_D(t) = -t^3 - t$ of D (See the eq. (3.5) below) has no constant term (since $\det D = 0$*) and one might obtain a formula for the adjoint that depends only on D and the coefficients of $\mathbf{p}_D(t)$ which can be explicitly represented in terms of traces of powers of D using complete exponential Bell polynomials. The resulting formula for D is*

$$AdjD = \frac{1}{2}\left[(TrD)^2 - Tr(D^2)\right] I - (TrD)D + D^2$$

[†] https://www.symbolab.com/solver/matrix-calculator

[‡] $\operatorname{rank}(XY) \leq \min\{\operatorname{rank}(X), \operatorname{rank}(Y)\}$

and hence $AdjD = \frac{1}{2}(0^2 - (-2))I - 0D + D^2 = I + D^2$ *as soon as we assume* $N(\mathbf{u}) = 1$.

3) Observe that the columns of $A = AdjD$ *appear as* $col_1(A) = x\mathbf{u}^T$, $col_2(A) = y\mathbf{u}^T$ *and* $col_3(A) = z\mathbf{u}^T$. *If we put* $\mathbf{v} = \mathbf{w} = \mathbf{u}^T$ *where* $\mathbf{u} = (x, y, z) \in \mathbb{R}^3$, *then* $\mathbf{w}^T\mathbf{v} = \mathbf{u}\mathbf{u}^T = N(\mathbf{u}) = 1$ *and* $AdjD = \mathbf{v}\mathbf{w}^T$. *This also justifies in an alternative way that* $\operatorname{rank}(AdjD) = 1$. *See Section 3.12 in [1] on facts about idempotent matrices.*

Note that if Q is split, then the matrices $A = AdjD$ and $-B = D^2$ are

$$A = \begin{pmatrix} x^2 & xy & -xz \\ -xy & -y^2 & yz \\ xz & yz & -z^2 \end{pmatrix} \quad -B = \begin{pmatrix} x^2-1 & xy & -xz \\ -xy & -y^2-1 & yz \\ xz & yz & -z^2-1 \end{pmatrix}$$

It follows that $-B = A - I$ and hence $I - A = B = -D^2$ such that $AA = A$ and $BB = B$ again due to the assumption $N(\mathbf{u}) = x^2 - y^2 - z^2 = 1$. We will see later on that the idempotent matrices $Adj(D)$ and $-D^2$ are in bijection with the matrix of a quaternion involution. That is, $Adj(D) \longleftrightarrow \Sigma \longleftrightarrow -D^2$ where $AdjD = (I + \Sigma)/2$ and $-D^2 = (I - \Sigma)/2$ and $\Sigma\Sigma = I$ (i.e. Σ is an involutary matrix).

We end this section with a few comments regarding the characteristic polynomial of a derivation since it might be useful for further purposes to deal with eigenspaces of a derivation. For it, we ignore the center of derivations and focus directly on decomposition of Q_0 through the matrix D in its general form as in (3.1).

Assume that $\mathbf{u} = xi + yj + zk \in Q_0$ associated to D is of norm $N(\mathbf{u}) = 1$. Then a simple computation shows that the monic polynomial $\mathbf{p}(\lambda) = -\lambda^3 + c_1\lambda^2 + c_2\lambda + c_3$ of D where $c_1 = c_3 = 0$ since $TrD = \det D = 0$ and the unique non-zero coefficient is $-c_2 = Tr(AdjD) = -ax^2 - \frac{1}{b}y^2 + \frac{b}{a}z^2$ which is equal to 1 no matter if Q is H or split. In fact, it is either $Tr(AdjD) = x^2 + y^2 + z^2$ (i.e. $a = b = -1$) or $Tr(AdjD) = x^2 - y^2 - z^2$ (i.e. $a = -b = -1$) and both correspond to the norm on Q. Hence the characteristic polynomial of D reduces to

$$\mathbf{p}(\lambda) = -\lambda^3 - Tr(AdjD)\lambda = -\lambda^3 - \lambda. \tag{3.5}$$

It follows that $\lambda = 0$ and $\lambda = \pm\mathrm{i}$ (complex i) are the only eigenvalues of D with algebraic multiplicity $\mu(0) = \mu(\pm\mathrm{i}) = 1$. To obtain much sharper results we now suppose $Q \simeq H$. Then it is well known that one might decompose H_0 as

$$H_0 = E(0) \bigoplus_{\lambda=\pm\mathrm{i}} E(\lambda)$$

where $E(\lambda) = \{\mathbf{v} \in H_0 : (D - \lambda I)\mathbf{v} = 0\}$ stands for the corresponding eigenspaces. Neither of the subspaces $E(0)$ and $E(\pm\mathrm{i})$ is trivial and $\dim E(0) = 1$ while $\dim E(\pm\mathrm{i}) = 2$. In fact, that $\det D = 0$ provides non-trivial solutions of the linear homogeneous system $D\mathbf{v} = 0$ and $\dim E(0) = 1$ might be confirmed by $rank\,(D) + \dim\ker(D) = 3$ where $\operatorname{rank}(D) = 2$. On the other hand, the assumption $N(\mathbf{u}) = 1$ implies

$$\det(D \pm \mathrm{i}I) = \mp(x^2 + y^2 + z^2 - 1)\mathrm{i} = 0\mathrm{i} = 0$$

which means $(D \pm \mathrm{i}I)\mathbf{v} = 0$ also admits non-trivial solutions such that $\dim E(\pm\mathrm{i}) = \dim H_0 - \dim E(0) = 2$.

Given any $\mathbf{v} = x'i + y'j + z'k \in H_0$. Then $D\mathbf{v} = 0$ if and only if $x' = \frac{xz'}{z}, y' = \frac{yz'}{z}$ $(z \neq 0)$ and $z' \in \mathbb{R}$, that is, $E(0) = \langle \mathbf{u} \rangle$ since any element of this subspace is the multiple $k\mathbf{u}$ with $k = z'/z$ for $z \neq 0$. Since complex eigenvectors come in conjugate it is enough to look at one of the complex eigenvectors, for instance, $\mathbf{v} = q + \mathrm{i}\mathbf{p}$ that corresponds to $\lambda = \mathrm{i}$. We claim that the plane passing through the origin generated by $Re(\mathbf{v}) = q$ and

$Im(\mathbf{v}) = \mathbf{p}$ is the eigenspace $E(\mathrm{i})$ on which $\mathbf{u}$ acts as a normal vector. Note that $D(q+\mathrm{i}\mathbf{p}) = \mathrm{i}(q+\mathrm{i}\mathbf{p}) = -\mathbf{p}+\mathrm{i}q$ implies $D(q) + \mathrm{i}D(\mathbf{p}) = -\mathbf{p} + \mathrm{i}q$ which occurs if and only if $D(q) = -\mathbf{p}$ and $D(\mathbf{p}) = q$. This is also equivalent to say $D^2q = -D\mathbf{p} = -q$ and $D^2\mathbf{p} = Dq = -\mathbf{p}$ (resp. $Bq = q$ and $B\mathbf{p} = \mathbf{p}$ with $B = -D^2$).

Hence, the components of $\mathbf{v} = q + \mathrm{i}\mathbf{p}$ belong to the -1-eigenspace of D^2 (resp. $+1$-eigenspace of $-D^2$) for which $\lambda = -1$ (resp. $\lambda = 1$) is the unique non-zero eigenvalue with the algebraic multiplicity $\mu(-1) = 2$ (resp. $\mu(1) = 2$).

The geometry between $E(0)$ and $E(\mathrm{i})$ (resp. $E(-\mathrm{i})$) might be clearly viewed for particular matrices $D_1 = ad(i), D_2 = ad(j)$ and $D_3 = ad(k)$ that actually combine D. For instance, D_2 has the same characteristic polynomial $\mathbf{p}(\lambda) = -\lambda^3 - \lambda$ of D and we have the xz-plane $E_2(\mathrm{i}) = \langle(0,0,1) + (1,0,0)\mathrm{i}\rangle$ whose normal vector is $\mathbf{u} = j$. For $D = xD_1 + yD_2 + zD_3$ and $\mathbf{u} = xi + yj + zk$ we conclude that $E(\pm\mathrm{i})$ is a plane passing from the origin such that its normal vector is parallel to $\mathbf{u}$.

4. Quaternion involutions

An automorphism of $Q = (\frac{a,b}{\mathbb{R}})$ is a bijective map on Q that preserves the algebraic structure of Q. An (anti)-automorphism is the same, except that it reverses the multiplicative structure, as in part (i) of the following definition.

Definition 4.1 *A map $\sigma : Q \to Q$ is called an involution of the first kind if it is a linear map satisfying for all $p, q \in Q$, (i) $\sigma(pq) = \sigma(q)\sigma(p)$, and (ii) $\sigma(\sigma(q)) = q$ for all q in Q. Alternatively put, an involution is an involutive (anti)-automorphism.*

We state the following simple Proposition, [6], without proof.

Proposition 4.2 *If $\sigma : Q \to Q$ is an automorphism (resp. (anti)-automorphism) then σ is the identity on $\mathbb{R}$ and maps Q_0 onto itself.*

As is said earlier, a quaternion algebra $Q = (\frac{a,b}{\mathbb{R}})$ is either $M_2(\mathbb{R})$ or $Q \simeq H$. Hence, involutions of $Q = (\frac{a,b}{\mathbb{R}})$ might be mainly considered in two categories: split and Hamilton's quaternions. In fact, we have characterized in [5],[6] that all involutive automorphisms and (anti)-automorphisms (for H and split case) arise in terms of inner automorphisms (and eigenspace decomposition). Thus, in what follows we constrain our attention only to involution matrices of either reel or split quaternions.

We start fixing Q as H and selecting $\mathbf{u} = xi + yj + zk \in H_0$ such that $N(\mathbf{u}) = 1$. Denote by $\sigma : H \to H$ the involution defined by $\sigma(q) = -\mathbf{u}q\mathbf{u}$. We remember that σ keeps the center of H invariant and hence the first row and the first column of σ in its matrix form is the quaternion $1 + 0i + 0j + 0k$, that is, $\sigma = diag\{1, \Sigma\}$ is a block-diagonal matrix with

$$\Sigma = \begin{pmatrix} 2x^2 - 1 & 2xy & 2xz \\ 2xy & 2y^2 - 1 & 2yz \\ 2xz & 2yz & 2z^2 - 1 \end{pmatrix} \tag{4.1}$$

such that $col_1(\Sigma) = \sigma(i), col_2(\Sigma) = \sigma(j)$ and $col_3(\Sigma) = \sigma(k)$.

Remark 4.3 *If we consider instead an (anti)-involution $q \mapsto -\mathbf{u}\bar{q}\mathbf{u}$, then it will appear $-\Sigma$.*

We quote without proof the following well-known fact that fits well here:

Lemma 4.4 *If $A \in M_n(\mathbb{R})$ is idempotent, then $S = 2A - I$ is involutary. Conversely, if $S \in M_n(\mathbb{R})$ is involutary, then $A_1 = \frac{1}{2}(I + S)$ and $A_2 = \frac{1}{2}(I - S)$ are idempotent. Hence, $SA_n = \pm A_n$ $(n = 1, 2)$ and the mapping $f(A) = 2A - I$ from the idempotent matrices to involutary matrices is a bijection.*

In the present context, we reveal that idempotent matrices that correspond to an involutary matrix are the idempotent matrices $AdjD$ and $-D^2$ and the matrix Σ above. This way one might establish a relationship between quaternion derivation and quaternion involution matrices for real quaternion algebras. Hence we end our exposition by introducing the following remarkable

Theorem 4.5 *Let D and Σ be as in (3.2) and (4.1), respectively. Then $\Sigma\, AdjD = AdjD$ and $\Sigma D^2 = -D^2$.*

Proof If we compare the matrices Σ and $AdjD$ we immediately write $\Sigma = 2AdjD - I$ and hence $AdjD = \frac{1}{2}(I + \Sigma)$. The same way we obtain $\Sigma = I + 2D^2$ so that $-D^2 = \frac{1}{2}(I - \Sigma)$. Then it follows at once that

$$\Sigma\, Adj(D) = \frac{1}{2}\Sigma(I + \Sigma) = \frac{1}{2}(\Sigma I + \Sigma\Sigma) = \frac{1}{2}(\Sigma + I) = AdjD$$

and $\Sigma(-D^2) = \frac{1}{2}\Sigma(I - \Sigma) = -\frac{1}{2}(I - \Sigma) = -(-D^2) = D^2$ (and hence $\Sigma D^2 = -D^2$). □

It is known that (ref. Skolem-Noether Theorem) any automorphism of central simple algebras (abrev. CSA) is inner and the same is also true for derivations. From the beginning, our main purpose was to connect inner derivations with involutive inner automorphisms of quaternions that obviously form a subclass of CSA. Hence, the preceding theorem provides an interesting connection in this sense.

References

[1] Bernstein, D. Matrix mathematics: Theory, facts and formulas. UK : Princeton University Press, 2009

[2] Ell TA, Sangwine SJ. Quaternion involutions and (anti)-involutions. Computers and Mathematics with Applications. 2007; 53:137-143. https://doi.org/10.1016/j.camwa.2006.10.029

[3] J Voight. Quaternion Algebras. NY, USA: Springer Graduate Texts in Mathematics, 2021

[4] Kizil E, Alagöz Y. Derivations of generalized quaternion algebra, Turkish Journal of Mathematics, 2019; 43 (5): 2649-2657. https://doi.org/10.3906/mat-1905-86

[5] Kizil E, J Lawson. A new eigenspace characterization of split-quaternion involutions. Linear and Multilinear Algebra, 2021; 69: 1981-1988. https://doi.org/10.1080/03081087.2021.1881032

[6] Lawson J, Kizil E. Characterizations of automorphic and (anti)-automorphic involutions of the quaternions. Linear and Multilinear Algebra, 2021; 69: 1975-1980. https://doi.org/10.1080/03081087.2020.1758021

[7] Mamagani A, Jafari M. On properties of generalized quaternion algebra. Journal of Novel Applied Sciences, 2013.