Quaternion Algebras

Arjun Kudinoor (ask2262)
Aswath Suryanarayanan (as5975)
Mateo Maturana (mm5589)

MATH 4042 Modern Algerba 2, Spring 2021

Contents

1 Introduction

In 1843, Irish Mathematician William Rowan Hamilton discovered an interesting way to extend complex number multiplication into four dimensions using what we call quaternions. For background, a complex number is a sum $a+bi$ of real numbers $a, b \in \mathbb{R}$ with the condition that $i^2 = -1$. Addition and multiplication of complex numbers are given by the rules $(a + bi) + (c + di) = (a + c) + (b + d)i$ and $(a + bi)(c + di) = (ac - bd) + (ad + bc)i$.

We observe that we may represent a complex number $a + bi$ as a vector $(a, b) \in \mathbb{R}^2$ with addition and multiplication rules $(a, b) + (c, d) = (a + c, b + d)$ and $(a, b)(c, d) = (ac - bd, ad + bc)$. Hamilton asked if it was possible to extend complex multiplication to multiplication of triples (a, b, c). Although he was unable to do this, in 1843, he found a way to multiply quadruples (a, b, c, d) after abandoning commutativity of these quadruples. This construction is what we call Hamilton's quaternions.

Using Keith Conrad's paper on quaternions algebras [1] as our guide, we seek to extend our knowledge of quaternions in this paper by extending new concepts and constructions from old concepts learnt along the way. In Section 2, we first describe the extension of complex numbers into four dimensional vectors via Hamilton's quaternions. In Section 3, we then extend Hamilton's quaternions to a more general framework of quaternion algebras. And finally in Section 4, we extend quaternions even further into biquaternions to describe quaternion vectors with complex entries.

As an aside, if you want to learn more about Hamilton's contributions to math and physics, you can watch this great music parody video [2].

2 Hamilton's Quaternions

2.1 Properties

Definition. *The quarternions are* $\mathbb{H} = \{a + bi + cj + dk : a, b, c, d \in \mathbb{R}\}$ *We impose the following conditions on multiplication in* $\mathbb{H}$*:*

- $i^2 = j^2 = k^2 = -1$
- $ij = -ji = k, ki = -ik = j, jk = -kj = i$
- $a \in \mathbb{R}$*, commutes with* i, j, k

Although quarternion multiplication is usually non-commutative, multiplication of quarternions with real numbers is commutative.

Remark. *Quarternions with* $a = 0$ *are pure quarternions.*
$(bi + cj + dk)^2 = -b^2 - c^2 - d^2$

Definition. *The conjugate of a quarternion is* $\bar{q} = a - bi - cj - dk$*. It has the following properties (similar to the complex numbers):*

- $\overline{q_1 + q_2} = \overline{q_1} + \overline{q_2}$
- $\overline{q_1 q_2} = \overline{q_2}\,\overline{q_1}$
- *The* ***norm*** *of* q*,* $N(q) = q\,\overline{q} = \overline{q}\,q = a^2 + b^2 + c^2 + d^2$

Definition. *A ring* R *is a division ring if every nonzero element in* R *has a multiplicative inverse.*

For all $q \in \mathbb{H}, q \neq 0$, $\frac{\bar{q}}{N(q)}$ is its inverse. Thus, as every nonzero element in $\mathbb{H}$ has an inverse, it is a division ring. The quarternions are, indeed, a noncommutative division ring, the first of its sort discovered. Furthermore, note that the center $\mathbf{Z}(\mathbb{H}) = \{x \in \mathbb{H} \mid xq = qx, \forall\, q \in \mathbb{H}\} = \mathbb{R}$, since a commutes with q $\forall q \in \mathbb{H}$, only if $a \in \mathbb{R}$.

Theorem 2.1. *(Frobenius) Each division ring* $\mathbb{D}$ *with center* $\mathbb{R}$ *that is finite dimensional as a vector space over* $\mathbb{R}$ *is isomorphic to* $\mathbb{R}$ *or* $\mathbb{H}$*.*

Proof. Proof involves concepts not covered in the algebra course as of yet. However, it is worth mentioning that the essential aspects of the proof are the fundamental theorem of algebra, and the Cayley-Hamilton theorem [3]. □

2.2 Quaternion Rotations

It must be noted that conjugation of a quaternion can take two different meanings - the first being the one mentioned above. The second is (for $q \neq 0$), the mapping $r \mapsto qrq^{-1}$, which we have encountered in group theory and ring theory. This conjugation by quaternions has some notable properties that induce an equivalence to rotations of vectors in $\mathbb{R}^3$. We shall establish (and prove) this rotations of vectors-conjugation by quaternions equivalence.

Definition. *For* $q \in \mathbb{H}^\times$*,* $R_q : \mathbb{H} \mapsto \mathbb{H}$ *is defined by* $R_q(r) = qrq^{-1}\,\forall\, r \in \mathbb{H}$

Proposition. R_q *is a ring automorphism of* $\mathbb{H}$

Proof. We need to prove that R_q is a invertible ring homomorphism (as this is the definition of ring automorphism). $R_q(a + b) = q(a + b)q^{-1} = qaq^{-1} + qbq^{-1} = R_q(a) + R_q(b)$ where $a, b \in \mathbb{H}$. $R_q(ab) = q(ab)q^{-1} = qaq^{-1}qbq^{-1} = R_q(a)R_q(b)$ where $a, b \in \mathbb{H}$. $R_q(1) = qq^{-1} = 1$ So R_q is a ring homomorphism. As $R_{q^{-1}}$ is the inverse of R_q, we have that it is a ring automorphism of $\mathbb{H}$.
If $c \in \mathbb{R}, R_q(ca) = qcaq^{-1} = cqaq^{-1} = cR_q(a)$ as c commutes with $q \in \mathbb{H}^\times$. Therefore this transformation is linear under addition and multiplication by elements in $\mathbb{R} \Rightarrow R_q$ is a linear transformation. □

Proposition. $R_{q_1} \circ R_{q_2} = R_{q_1 q_2}$

Proof. $R_{q_1} \circ R_{q_2}(x) = q_1 q_2 x q_2^{-1} q_1^{-1} = (q_1 q_2) x (q_1 q_2)^{-1} = R_{q_1 q_2}$ □

Proposition. *For q, q' in $\mathbb{H}^\times$, show that $R_q = R_{q'} \Leftrightarrow q' = cq$ for some $c \in \mathbb{R}^\times$*

Proof. $\Leftarrow$: If $q' = cq$, then $R_{q'}(x) = cqxc^{-1}q^{-1} = R_q(x) \forall x \in \mathbb{R}$ as c commutes with q, x.
$\Rightarrow$: If $R_q = R_{q'}$, then $R_q(x) = R_{q'}(x) \forall x \in \mathbb{R}$. Thus, $qxq^{-1} = q'xq'^{-1}$. This implies that, $x = q^{-1}q'xq'^{-1}q = (q^{-1}q')x(q^{-1}q')^{-1}$. But, as R_q is an isomorphism, and thus is injective, $q^{-1}q' = c$ if $c \in \mathbb{H}^\times \Rightarrow q' = cq$ □

Definition. $\mathbb{H}^0 = \mathbb{R}i + \mathbb{R}j + \mathbb{R}k = \{q \in \mathbb{H} \mid Tr(q) = 0\}$*, where* $Tr : \mathbb{H} \mapsto \mathbb{R}$*, and* $Tr(q) = q + \overline{q} = 2a$*, where* $q = a + bi + cj + dk$*.*

Proposition. *Show that $Tr(qq') = Tr(q'q) \forall q \in \mathbb{H}$. Then, show that $R_q(\mathbb{H}^0) = \mathbb{H}^0 \, \forall q \in \mathbb{H}^\times$*

Proof.

1. $q = a + bi + cj + dk, q' = e + fi + gj + hk, qq' = ae - bf - cg - dh +$ terms containing i, j, k. So, $Tr(qq') = qq' + \overline{qq'} = 2(ae - bf - cg - dh)$. We can easily see that we shall get the very same result for $Tr(q'q)$.
2. $\forall x \in \mathbb{H}^0, R_q(x) = qxq^{-1} \Rightarrow Tr(R_q(x)) = Tr(qxq^{-1}) = Tr(qq^{-1}x) = Tr(x) = 0$, as $x \in \mathbb{H}^0$. So, R_q maps every element in $\mathbb{H}^0$ to an element in $\mathbb{H}^0$. Since R_q is injective, $R_q(\mathbb{H}^0) = \mathbb{H}^0 \, \forall q \in \mathbb{H}^\times$.

□

Note that if $Tr(q) = 0$, q is a pure Hamilton's quaternion, and therefore, $q^2 \in \mathbb{R}, q^2 < 0$.
It is very important at this juncture to note that we can identify every element $\mathbb{H}^0$ with $\mathbb{R}^3$ [4]. This is because there is a direct correspondence between $q = bi + cj + dk$ and $(b, c, d) \in \mathbb{R}^3$. So, we have learnt the following:

- R_q is a ring automorphism of $\mathbb{H}$
- $R_{q_1} \circ R_{q_2} = R_{q_1 q_2}$
- For q, q' in $\mathbb{H}^\times$, $R_q = R_{q'} \Leftrightarrow q' = cq$ for some $c \in \mathbb{R}^\times$
- $Tr(qq') = Tr(q'q) \forall q \in \mathbb{H}$ and $R_q(\mathbb{H}^0) = \mathbb{H}^0 \, \forall q \in \mathbb{H}^\times$
- We can identify $\mathbb{H}^0$ with $\mathbb{R}^3$

Due to all the above properties of the ring isomorphism R_q, it can be considered as a method of executing rotations of vectors in $\mathbb{R}^3$. Thus, quaternions - which have only 4 degrees of freedom, compared with the 9 required for matrix-based rotation - are a practical tool in computer graphics, to execute rotations.

2.3 Matrix Representation of Complex Numbers and Quaternions

2.3.1 Matrix Representation of Complex Number

Although we have represented complex numbers above using vectors, we may also represent complex numbers using matrices. Using $\{1, i\}$ (or $\{(1,0), (0,1)\}$ in vector representation) as a basis for $\mathbb{C}$, we wish to find matrices $m_z \in M_2(\mathbb{R})$ that represent complex numbers $z \in \mathbb{C}$ such that $m_z(w) = zw$ for all $z, w \in \mathbb{C}$. This defines a linear map $m_z : \mathbb{C} \to \mathbb{C}$. Additionally, we want these matrices to obey the rules $m_{z+u} = m_z + m_u$, $m_{zu} = m_z \circ m_u$, and $m_1 = \mathbb{I}$, the identity in $M_2(\mathbb{R})$, so that we get a ring homomorphism $\mathbb{C} \to M_2(\mathbb{R})$ defined by $z \mapsto m_z$.

To determine this matrix representation of complex numbers, we note what values our basis vectors $\{1, i\} = \{(1,0), (0,1)\}$ (in $\mathbb{R}^2$ vector notation) will map to when multiplied by an arbitrary complex number $z = (a, b)$, where $a, b \in \mathbb{R}$. Multiplying 1 by z yields $z \cdot 1 = z = (a, b)$, and multiplying

i by z yields $z \cdot i = (-b, a)$. Therefore, $z = a + bi \mapsto \left(\begin{smallmatrix} a & -b \\ b & a \end{smallmatrix}\right) = m_z$ is the ring homomorphism $\mathbb{C} \to M_2(\mathbb{R})$ we were looking for. It is not hard, although lengthy, to check that the above rules for ring homomorphisms hold.

Conjugation and the norm on $\mathbb{H}$ may be described as $[l_{\bar{q}}] = \overline{[l_q]}^T$ and $N(q) = det[l_q]$ respectively.

2.3.2 Matrix Representation of Hamilton's Quaternions

Similarly to the complex numbers case above, let us find a 2×2 matrix representation for Hamilton's quaternions. In this case, the entries of our matrices will not be real numbers, but will instead be complex numbers. Let us examine why this is the case.

Since both $\mathbb{H}$ and $M_2(\mathbb{R})$ have dimension 4, a ring homomorphism between the two rings would imply an ring isomorphism between them. However, we know Hamilton's quaternions are a division ring, whereas real matrices are not a division ring. This is equivalent to stating that nonzero every element $q \in \mathbb{H}$ has a multiplicative inverse $\frac{\bar{q}}{N(q)}$, whereas not every 2×2 real matrix has a multiplicative inverse. So, we cannot draw an isomorphism between invertible quaternions and non-invertible real matrices. Thus, we must find a matrix ring such that a ring homomorphism between $\mathbb{H}$ and that matrix ring is injective and not surjective. Such a matrix ring is the $M_2(\mathbb{C})$, the set of 2×2 matrices with complex entries, as we will see in more detail below.

First, let us choose a basis for our quaternion-vector space over $\mathbb{C}$. If we choose $\{1, j\}$ as our basis, we may represent an arbitrary quaternion $q = a + bi + cj + dk = (a + bi) + j(c - di)$ as a unique vector $(a + bi, c + di) \in \mathbb{C}^2$. So, we may write any quaternion $q \in \mathbb{H}$ as $q = z + jw$ for some $z, w \in \mathbb{C}$. Thus, we may describe $\mathbb{H}$ as a complex vector space under a $\{1, j\}$ basis.

However, when describing $\mathbb{H}$ as a complex vector space we must be careful to note that quaternion multiplication is NOT commutative. Here, we have chosen to represent $\mathbb{H}$ as a right complex vector space, i.e. scalar multiplication of an arbitrary hamiltonian quaternion q by an arbitrary complex number z yields $z \cdot q = qz$.

Definition. *Define the "left multiplication" function $l_q : \mathbb{H} \to \mathbb{H}$ by $l_q(p) = qp$ for all $p \in \mathbb{H}$.*

Proposition. *$q \mapsto l_q$ is an additive and multiplicative embedding $\mathbb{H} \to End_{\mathbb{C}}(\mathbb{H})$.*

Proof. We first check that l_q is a linear function over $\mathbb{C}$. We note that $l_q(p_1 + p_2) = q(p_1 + p_2) = qp_1 + qp_2 = l_q(p_1) + l_q(p_2)$ for all $p_1, p_2 \in \mathbb{H}$. Additionally, $l_q(z \cdot p) = l_q(pz) = q(pz) = (qp)z = z \cdot (qp) = z \cdot l_q(p)$ for all $p \in \mathbb{H}$ and $z \in \mathbb{C}$. Thus, l_q is linear.

Now, we show that l_q functions obey the same additive and multiplicative properties in q as quaternions. $(l_q + l_{q'})(p) = l_q(p) + l_{q'}(p) = qp + q'p = l_{q+q'}(p)$ and $(l_q \circ l_{q'})(p) = q(q'p) = (qq')p = l_{qq'}(p)$. Thus, $l_q + l_{q'} = l_{q+q'}$ and $l_q \circ l'_q = l_{qq'}$, as desired. Additionally, we can recover q from l_q since $l_q(q) = q$.

Thus, $q \mapsto l_q$ is an additive and multiplicative embedding $\mathbb{H} \to End_{\mathbb{C}}(\mathbb{H})$. □

Since $q \mapsto l_q$ is an additive and multiplicative embedding $\mathbb{H} \to End_{\mathbb{C}}(\mathbb{H})$, we can examine how the basis $\{1, j\}$ evolves under the left multiplication transformation to derive a 2×2 complex-matrix representation for quaternions. For $q = z + jw$, where $z, w \in \mathbb{C}$, $l_q(1) = z + jw$ and $l_q(j) = zj + jwj$. To write this expression as a linear combination of basis vectors, we examine that for an arbitrary complex number $a + bi$, $(a + bi)j = j(a - bi)$. So, $l_q(j) = zj + jwj = j\bar{z} + jj\bar{w} = -\bar{w} + j\bar{z}$. Therefore, $q = z + jw \mapsto \left(\begin{smallmatrix} z & -\bar{w} \\ w & \bar{z} \end{smallmatrix}\right) = [l_q]$ is the matrix representation we were looking for.

Example. *For example, we can generate the matrices for each of i, j, k quaternions. We note that*

$i = i + j(0)$, $j = 0 + j(1)$, $k = 0 + j(-i)$. *So,*

$$[l_i] = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}, \ [l_j] = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \ [l_k] = \begin{pmatrix} 0 & -i \\ -i & 0 \end{pmatrix}$$

Remark. *The matrices corresponding to i, j, k above look very similar to the Pauli matrices $\sigma_1, \sigma_2, \sigma_3$ used to describe spin in quantum mechanics [5]. In fact, the algebra generated by $\mathbf{1}, i\sigma_1, i\sigma_2, i\sigma_3$ is isomorphic to the quaternions ($1 \mapsto \mathbf{1}, i \mapsto i\sigma_3, j \mapsto i\sigma_2, k \mapsto i\sigma_1$ describes the ring isomorphism) [6].*

3 Quaternion Algberas

3.1 Algebraic Properties

Let us now generalize Hamilton's formulation of the quarternions by considering $a, b, c, d \in F$, where F is a general field. N.B. Previously, we restricted a, b, c, d to $\in \mathbb{R}$. Formally, we define the following: $\mathbb{H}(F) = \{a + bi + cj + dk \mid a, b, c, d \in F\}$

The norm, $N(q)$, and conjugation $\overline{q}$, are defined in the same way as in Section 2.1, and obeys the same properties. Recall that the characteristic of a field, $char(F)$, is defined as the lowest $n \in \mathbb{N}, n \neq 0 \mid n \cdot a = 0 \,\forall\, a \in F$. An interesting sidenote here describes when $\mathbb{H}(F)$ is commutative: if $char(F) = 2$, then $-1 = 1$ in $F \Rightarrow \mathbb{H}(F)$ is commutative, otherwise $-1 \neq 1$, so $\mathbb{H}(F)$ is not commutative.

Furthermore, we can identify fields F such that $\mathbb{H}(F)$ is not a division ring. For example, in $\mathbb{F}_{14} = \mathbb{Z}/14\mathbb{Z}$, we have $N(4i + 6j + 2k) = -4^2 - 6^2 - 2^2 = 0$. This implies that this element in $\mathbb{F}_{14}$ has no defined inverse, and thus $\mathbb{F}_{14}$ is not a division ring.

Definition. *A quarternion algebra over a field F is a ring that is a 4-dimensional vector space over F, with basis $\{1, u, v, uv\}$. It has the following properties:*

- $u^2, v^2 \in F^\times$, $w = uv = -vu$
- *Every $c \in F$ commutes with u, v*
- *We denote this ring by $(a, b)_F$, where $a = u^2, b = v^2$*

$\mathbb{H}(F) = (-1, -1)_F$ *as per this definition as we place $u^2 = v^2 = w^2 = -1$ requirements in order to obtain $u = i, v = j, w = k$.*
In general, u, v, w anti-commute

Definition. *The conjugate of a quaternion $q = a_1 + a_2u + a_3v + a_4w$, is $\overline{q} = a_1 - a_2u - a_3v - a_4w$ and the corresponding norm is $N(q) = q\overline{q} = a_1^2 - a_2^2a - a_3^2b + a_4^2ab$.*

A pure quaternion carries the same meaning here as in Section 2. We can illustrate the behavior of $(a, b)_F$ through the following example in $F = \mathbb{R}$.

Example. $(-\pi, -e)_\mathbb{R} = \mathbb{R} + \mathbb{R}u + \mathbb{R}v + \mathbb{R}w$, *where $u^2 = -\pi, v^2 = -e, w^2 = -\pi e$. The norm of $q = a_1 + a_2u + a_3v + a_4w$, is $a_1^2 - a_2^2\pi - a_3^2e + a_4^2\pi e$.*

Theorem 3.1. *$q \in (a, b)_F$ has two-sided inverse in $(a, b)_F \Leftrightarrow N(q) \neq 0$*

Proof. If q has a two-sided inverse, q', then $qq' = 1 \Rightarrow N(q)N(q') = 1 \Rightarrow N(q) \in F^\times, N(q) \neq 0$. If $N(q) \neq 0$, then $N(q) \in F^\times \Rightarrow \frac{\overline{q}}{N(q)}$ is the two-side inverse of q. □

Theorem 3.2. *$a, p \in \mathbb{Z}, p$ odd prime such that if $a \equiv c(\mathrm{mod} p)$, then $\nexists k \mid c = k^2$. Then $(a, p)_\mathbb{Q}$ is a division ring.*

Proof. From the previous theorem, note that $(a,p)_{\mathbb{Q}}$ is a division ring $\Leftrightarrow N(q) \neq 0 \,\forall\, q \neq 0$. We shall prove that $(a,p)_{\mathbb{Q}}$ is a division ring by establishing that in $(a,p)_{\mathbb{Q}}, N(q) = 0 \Rightarrow q = 0$.

$q = y_1 + y_2 u + y_3 v + y_4 w$, so $N(q) = y_1^2 - ay_2^2 - py_3^2 + apy_4^2 = 0 \Rightarrow y_1^2 - ay_2^2 = p(y_3^2 - ay_4^2) \Rightarrow ay_2^2 \equiv y_1^2 (\text{mod} p)$.

If $y_1 \equiv k(\text{mod} p)$ (where $k \neq 0$), $y_1^2 \equiv k^2(\text{mod} p) \Rightarrow ay_2^2 \equiv k^2(\text{mod} p)$. However, along the same lines, if we consider $y_2 \equiv l(\text{mod} p)$ (where $l \neq 0$), then, $y_2^2 \equiv l^2(\text{mod} p)$. But this would then imply that $\exists m \mid a \equiv m^2(\text{mod} p)$. This is because both ay_2^2 and y_2^2 modulo p give whole squares. But $\exists m \mid a \equiv m^2(\text{mod} p)$ violates our assumption in the problem statement. So, $y_1 \equiv 0(\text{mod} p) \Rightarrow p \mid y_1$ and thus, $p^2 \mid y_1^2$.

Now, we have that $y_1^2 - ay_2^2 = p(y_3^2 - ay_4^2)$, and that $p \mid y_1^2$ and $p \mid p(y_3^2 - ay_4^2)$. So, this implies, $p \mid ay_2^2$. But p does not divide a. So, $p \mid y_2^2$. As y_1^2, y_2^2 are squares of integers, $p^2 \mid y_1^2, y_2^2 \Rightarrow p^2(y_5^2 - ay_6^2) = p(y_3^2 - ay_4^2) \Rightarrow p(y_5^2 - ay_6^2) = (y_3^2 - ay_4^2)$. where $py_5 = y_1, py_6 = y_2$. If we repeat this process for y_3, y_4, and then for y_5, y_6, and so on, we notice that y_1, y_2, y_3, y_4 can be divided by infinitely high powers of p. This is only possible if $y_1 = y_2 = y_3 = y_4 = 0$. Hence we obtain that $q = 0$. Hence proved. $\square$

As an example, consider $(5,3)_{\mathbb{Q}} \Rightarrow a = 5, p = 3$. Here, $5 \equiv 2(\text{mod} 3)$ and 2 is not a whole square. This theorem establishes that $(5,3)_{\mathbb{Q}}$ is a division ring. In $(5,3)_{\mathbb{Q}}$, $q = y_1 + y_2 u + y_3 v + y_4 w, u^2 = 5, v^2 = 3, w^2 = -15$ and $N(q) = y_1^2 - 5y_2^2 - 3y_3^2 + 15y_4^2$. From this theorem (and proof), we can also conclude that if $N(q) = 0, q = 0$.

3.2 Matrix Representation of Real Quaternion Algebras

Let us now represent quaternion algebras in matrix form. For simplicity, let us examine $(a,b)_{\mathbb{R}}$, the quaternion algebra over the reals. In $(a,b)_{\mathbb{R}}$, we can write a quaternion q as $q = n + ru + sv + tw = (n + ru) + v(s - tu)$, where $n, r, s, t \in \mathbb{R}$ and $u^2 = a, v^2 = b, uv = -vu = w$. Thus, if we define $\mathbb{U} = Span\{1, u\}$ over $\mathbb{R}$, we may write q as a vector in the right-multiplicative vector space $\mathbb{V} = Span\{1, v\}$ over $\mathbb{U}$ as $q = z + vx$ for some $z, x \in \mathbb{U}$. Using the same left-multiplication transformation as in Section 2.3.2, we may derive a ring homomorphism $q \to [l_q]$ that allows us to represent quaternions in (a,b) using matrices in $M_2(\mathbb{U})$.

We examine what happens when l_q acts on the $\{1, v\}$ basis of $\mathbb{V}$. $l_q(1) = q = z + vx$ and $l_q(v) = qv = zv + vxv = v\bar{z} + vv\bar{x} = b\bar{x} + v\bar{x}$. Here, we have used the fact that $xv = (c + du)v = v(c - du) = v\bar{x}$ for all $x = c + du \in \mathbb{U}$. Thus, $q \mapsto [l_q] = \begin{pmatrix} z & b\bar{x} \\ x & \bar{z} \end{pmatrix}$ is the ring homomorphism we desire.

Example. *Let us calculate the matrix representations for quaternions u, v, w.*

$$[l_u] = [l_{u+0}] = \begin{pmatrix} u & 0 \\ 0 & -u \end{pmatrix} = \begin{pmatrix} \sqrt{a} & 0 \\ 0 & -\sqrt{a} \end{pmatrix}$$

$$[l_v] = [l_{0+1v}] = \begin{pmatrix} 0 & b \\ 1 & 0 \end{pmatrix}$$

$$[l_w] = [l_{0+uv}] = \begin{pmatrix} 0 & -bu \\ u & 0 \end{pmatrix} = \begin{pmatrix} 0 & -b\sqrt{a} \\ \sqrt{a} & 0 \end{pmatrix}$$

Note that $[l_u]^2 = a\mathbf{1}$, $[l_v]^2 = b\mathbf{1}$, $[l_u][l_v] = [l_w]$, as desired. Thus, for a quaternion $q = n + ru + sv + tw$, we can represent it using the matrix $\begin{pmatrix} n + r\sqrt{a} & b(s - t\sqrt{a}) \\ s + t\sqrt{a} & n - r\sqrt{a} \end{pmatrix}$

3.3 Quaternion-Matrix Isomorphisms

We now move to isomorphisms between Quaternion Algebras. An isomorphism between two quaternion algebras A and A' over a field F is a ring isomorphism $f : A \to A'$ that fixes the elements of F. i.e. $f(c) = c$ for all $c \in f$.

Definition. *A basis of $(a, b)_F$ having the form $1, e_1, e_2, e_1e_2$ where $e_1^2 \in F^\times, e_2^2 \in F^\times$, and $e_1e_2 = -e_2e_1$ is called a quaternionic basis of $(a, b)_F$.*

Example. *The basis $\{1, u, v, w\}$ of $(a, b)_F$ is a quaternionic basis.*

Definition. *We call $M_2(F)$, or a quaternion algebra isomorphic to $M_2(F)$, a trivial or split quaternion algebra over F. If $(a, b)_F \ncong M_2(F)$, we say $(a, b)_F$ is a non-split quaternion algebra.*

For example, we can relate this defintion to quaternion algebras over $\mathbb{Q}$.

Definition. *Let $a, b \in \mathbb{Q}^\times$. Then, $(a, b)_\mathbb{Q}$ splits over $\mathbb{R}$ if $(a, b)_\mathbb{R} \cong M_2(\mathbb{R})$. Otherwise, $(a, b)_\mathbb{Q}$ is non-split over $\mathbb{R}$ if $(a, b)_\mathbb{R} \ncong M_2(\mathbb{R})$.*

Theorem 3.3. *Let $a \in F^\times$. Then, $(a, 1)_F$ splits over F, i.e. $(a, 1)_F \cong M_2(F)$*

Proof. Let the basis of $(a, 1)_F$ be $\{1, u, v, w\}$. Recall that $u^2 = a, v^2 = 1, u \cdot v = w$. Then, we can send the basis of $(a_1)_F$ to $M_2(F)$ as follows.

$$1 \mapsto \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, u \mapsto \begin{pmatrix} 0 & 1 \\ a & 0 \end{pmatrix}, v \mapsto \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, w \mapsto u \cdot v = \begin{pmatrix} 0 & -1 \\ a & 0 \end{pmatrix}$$

Similarly to the example at the end of 3.2, for a quaternion $q = x_0 + x_1u + x_2v + x_2w$, we can represent it using the matrix $\left(\begin{smallmatrix} x_0+x_2 & x_1-x_3 \\ a(x_1+x_3) & x_0-x_2 \end{smallmatrix}\right)$. Therefore, we can have a mapping

$$x_0 + x_1u + x_2v + x_3w \mapsto \begin{pmatrix} x_0 + x_2 & x_1 - x_3 \\ a(x_1 + x_3) & x_0 - x_2 \end{pmatrix}$$

Let $\phi : (a, b)_F \to M_2(F)$ be defined by this mapping. Let $q_1 = x_0 + x_1u + x_2v + x_3w, q_2 = y_0 + y_1u + y_2v + y_3w$ be quaternions. Then,

$$\begin{aligned} \phi(q_1) = \phi(q_2) &\implies \begin{pmatrix} x_0 + x_2 & x_1 - x_3 \\ a(x_1 + x_3) & x_0 - x_2 \end{pmatrix} = \begin{pmatrix} y_0 + y_2 & y_1 - y_3 \\ a(y_1 + y_3) & y_0 - y_2 \end{pmatrix} \\ &\implies x_0 + x_2 = y_0 + y_2, x_0 - x_2 = y_0 - y_2, \\ &\qquad a(x_1 + x_3) = a(y_1 + y_3), x_1 - x_3 = y_1 - y_3 \\ &\implies x_0 = y_0, x_1 = y_1 \\ &\implies x_2 = y_2, x_3 = y_3 \\ &\implies x_0 + x_1u + x_2v + x_3w = q_0 + q_1u + q_2v + q_3w \\ &\implies q_1 = q_2 \end{aligned}$$

Therefore, ϕ is injective. However, since $\dim(a_1)_F = \dim M_2(F) = 4$, ϕ is also surjective so it is bijective. We can easily see that $\phi(1) = 1$ and $\phi(q_1 + q_2) = \phi(q_1) + \phi(q_2)$. We can also show that $\phi(q_1q_2) = \phi(q_1)\phi(q_2)$, but due to the length, this part is omitted. Thus, ϕ is a ring isomorphism so $(a_1)_F \cong M_2(F)$. ☐

Theorem 3.4. *Let $a, b \in F^\times$. Then, $(a, b)_F \cong (ac^2, bd^2)_F$ for all $c, d \in F^\times$.*

Proof. The ring $(ac^2, bd^2)_F$ has a quaternionic basis $\{1, cu, dv, (cu)(dv)\}$ for arbitrary $c, d \in F^\times$. This is because $(cu)^2 = ac^2 \in F^\times$, $(dv)^2 = bd^2 \in F^\times$, $(cu)(dv) = -(dv)(cu)$, and the basis vector set is linearly independent (since each basis vector is a scaled version of the corresponding vector in the $\{1, u, v, uv\}$ basis). We note that since $(cu)^2 = ac^2$ and $(dv)^2 = bd^2$, $\{1, cu, dv, (cu)(dv)\}$ is also a quaternionic basis for $(ac^2, bd^2)_F$. Thus, $(a, b)_F \cong (ac^2, bd^2)_F$ for all $c, d \in F^\times$. ☐

Corollary 3.4.1. *$(a,1)_F \cong (a,b^2)_F$ for all $a,b \in F^\times$*

Proof. We note that $1,a,b \in F^\times$. So, by Theorem 3.4, $(a,1)_F \cong (a\cdot 1^2, 1\cdot b^2)_F \cong (a,b^2)_F$. $\square$

Definition. *Let $a \in F^\times$. Define $N_a = N_a(F)$ to be the set of all nonzero $x^2 - ay^2$ where $x,y \in F$.*

Theorem 3.5. *If $b \in N_a$, then $(a,b)_F \cong M_2(F)$.*

Proof. Since $b \in N_a, b = x^2 - ay^2$ for some $x,y \in F$, where $a \in F^\times$. Consider the set $B = \{1, u, xv + yw, u(xv+yw)\}$. Observe that $u(xv+yw) = uxv + uyw = xw + u^2yv = xw + ayv$. Then, we want to change the basis from v,w to $xw + ayv$. We see that

$$\begin{pmatrix} x & y \\ ay & x \end{pmatrix}\begin{pmatrix} v \\ w \end{pmatrix} = \begin{pmatrix} xv + yw \\ ayv + xw \end{pmatrix}$$

so $\left(\begin{smallmatrix} x & y \\ ay & x \end{smallmatrix}\right)$ is the change of basis matrix with nonzero determinant $\det\left(\begin{smallmatrix} x & y \\ ay & x \end{smallmatrix}\right) = x^2 - ay^2 = b \neq 0$.

So, the four elements of B are linearly independent ([7], Theorem 3.6) in F so it is a basis of $(a,b)_F$. Also, $(xv+yw)^2 = bx^2 - aby^2 = b(x^2 - ay^2) = b^2$. Additionally, u and $xv + yw$ anticommute so the basis is also quaternionic. Since $u^2 = a$ and $(xv+yw)^2 = b^2$, B is also a basis for (a,b^2). Thus, $(a,b)_F \cong (a,b^2)_F$. Also, by Corollary 3.4.1, $(a,b^2)_F \cong (a,1)_F$ and by Theorem 3.3, $(a,1) \cong M_2(F)$. Thus, $(a,b^2)_F \cong (a,b^2)_F \cong (a,1) \cong M_2(F)$. $\square$

4 Biquaternions

Definition. *Biquaternions are the quaternion algebra $(-1,-1)_\mathbb{C} = \{q = a+bi+cj+dk \mid a,b,c,d \in \mathbb{C}, i^2 = j^2 = -1, ij = k\}$. In other words, biquaternions are Hamilton's quaternions with complex coefficients.*

4.1 Algebraic Properties of Biquaternions

An interesting property of biquaternions is conjugation: Since the coefficients of biquaternions are complex numbers themselves, they too will have complex conjugates. So, biquaternions have two different types of conjugation [8].

Definition. *For an arbitrary biquaternion $q = a + bi + cj + dk$, we may define complex conjugates $\bar{q} = a - bi - cj - dk$ and $q^* = \bar{a} + \bar{b}i + \bar{c}j + \bar{d}k$.*

Here, if $z = a + bh, \bar{z} = a - bh$, where $z \in \mathbb{C}, a,b \in \mathbb{R}$ and $h^2 = -1$. Some notable properties of biquaternions:

- $(pq)^* = q^*p^*$, $\bar{pq} = \bar{p}\bar{q}$, $\bar{q^*} = \bar{q}^*$
- If $qq^* \neq 0$, we can define an inverse for each biquaternion with: $q^{-1} = q^*(qq^*)^{-1}$ as $qq^{-1} = (qq^*)(qq^*)^{-1} = 1$ and $q^{-1}q = ((q^*)^*(qq^*)^{-1*})^*q^* = (qq^*)^{-1}qq^* = 1$

4.2 Matrix Representation of Biquaternions

We note that in Section 2.3.2, the ring homomorphism $q = a + bi + cj + dk = z + jw \mapsto [l_q] = \left(\begin{smallmatrix} z & -\bar{w} \\ w & \bar{z} \end{smallmatrix}\right) = \left(\begin{smallmatrix} a+bi & -(c+di) \\ c-di & a-bi \end{smallmatrix}\right)$ gives us a matrix representation for Hamilton's quaternions with real coefficients $a,b,c,d \in \mathbb{R}$. However, we would like to extend this representation to complex coefficients $a,b,c,d \in \mathbb{C}$.

We observe that i here does not refer to the imaginary unit $\sqrt{-1} \in \mathbb{C}$, but is rather one of the quaternion basis vectors for $(-1,-1)_\mathbb{C}$, the biquaterinons. So, we will instead use h (motivated by Hamilton's own use of h) to represent the imaginary unit $\sqrt{-1} \in \mathbb{C}$. Hence, a representation matrix for an arbitrary biquaternion may be obtained from the ring homomorphism

$$q = a + bi + cj + dk \mapsto \begin{pmatrix} a+bh & -(c+dh) \\ c-dh & a-bh \end{pmatrix} = [l_q].$$

This representation also makes sense because if we choose matrix representations $[l_1] = \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)$, $[l_i] = \left(\begin{smallmatrix} h & 0 \\ 0 & -h \end{smallmatrix}\right)$, $[l_j] = \left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)$, $[l_k] = \left(\begin{smallmatrix} 0 & -h \\ -h & 0 \end{smallmatrix}\right)$, for the biquaternion basis $1, i, j, k$, then $[l_i]^2 = [l_j]^2 = -\mathbf{1}$, $[l_i][l_j] = [l_k]$. And for a quaternion $q = a+bi+cj+dk$, we get the matrix $\left(\begin{smallmatrix} a+bh & -(c+dh) \\ c-dh & a-bh \end{smallmatrix}\right) = [l_q]$, as desired above.

We can use this representation to prove the following proposition:

Proposition. $(-1,-1)_{\mathbb{C}} \cong M_2(\mathbb{C})$

Proof. Using notation from Section 3.3, we note that $-1 \in N_{-1} = \{\text{Nonzero } x^2-(-1)y^2 \mid x, y \in \mathbb{C}\}$ since $-1 = (\frac{i}{\sqrt{2}})^2 - (-1)(\frac{i}{\sqrt{2}})^2$. Thus, by Theorem 3.5, $(-1,-1)_{\mathbb{C}} \cong M_2(\mathbb{C})$. $\square$

In fact, $m : (-1,-1)_{\mathbb{C}} \to M_2(\mathbb{C})$ defined by $m(q) = m(a+bi+cj+dk) = \left(\begin{smallmatrix} a+bh & -(c+dh) \\ c-dh & a-bh \end{smallmatrix}\right) = [l_q]$ is an isomorphism from $(-1,-1)_{\mathbb{C}}$ to $M_2(\mathbb{C})$.

References

[1] Keith Conrad. *Quaternion Algebras*. URL: https://kconrad.math.uconn.edu/blurbs/ringtheory/quaternionalg.pdf.

[2] A Capella Science. *William Rowan Hamilton (Science YouTuber Collab)*. URL: https://www.youtube.com/watch?v=SZXHoWwBcDc.

[3] Wikipedia. *Frobenius theorem (real division algebras)*. URL: https://en.wikipedia.org/wiki/Frobenius_theorem_(real_division_algebras).

[4] William Goldman. *Quaternions and Euclidean 3-space*. URL: http://math.umd.edu/~wmg/quaternions.pdf.

[5] Wikipedia. *Pauli Matrices*. URL: https://en.wikipedia.org/wiki/Pauli_matrices.

[6] Wikipedia. *Pauli Matrices, Quaternions*. URL: https://en.wikipedia.org/wiki/Pauli_matrices#Quaternions.

[7] Tom M. Apostol. *Calculus*. Vol. II.

[8] Wikipedia. *Biquaternions*. URL: https://en.wikipedia.org/wiki/Biquaternion.