Quaternion Algebras

Edgar Elliott

May 1, 2016

Copyright (C) 2016 Edgar Elliott. Permission is granted to copy, distribute and/or modify this document under the terms of the GNU Free Documentation License, Version 1.3 or any later version published by the Free Software Foundation; with no Invariant Sections, no Front-Cover Texts, and no Back-Cover Texts. A copy of the license is included in the section entitled ”GNU Free Documentation License”.

1 Abstract

In 1843, after many failed efforts to describe a 3-dimensional extension to the complex numbers, William Hamilton realized the solution lay in 4-dimensions, he carved the expression $i^2 = j^2 = k^2 = ijk = -1$ into the stone of a nearby bridge to commemorate the moment and went on to devote his life to studying them. It was his colleague John T. Graves who suggested going further, saying “There is still something in the system which graviels me. I have not yet any clear views as to the extent to which we are at liberty arbitrarily to create imaginaries, and to endow them with supernatural properties...If with your alchemy you can make three pounds of gold, why should you stop there?” Graves was referring to the Octonions, which he went on to study, but his sentiments hold true for the abstraction of quaternion algebras as well. Hamilton was focused on the obviously practical quaternions. I will start by looking at Hamilton’s quaternions before addressing the generalization to other fields.
2 The Real Quaternions

The real quaternions are of the form

\[ \mathbb{H} = \{ a + bi + cj + dk | a, b, c, d \in \mathbb{R} \} \]

Where multiplication follows the rules \( i^2 = j^2 = k^2 = ijk = -1 \) and \( i, j, \) and \( k \) commute with real numbers.

The quaternions form an algebra over the real numbers since they are both a vector field over the reals and a ring under the multiplication rules set forth by Hamilton. Before generalizing to other fields let us look at some properties of the Hamiltonian quaternions.

**Definition:** The conjugate of a quaternion \( q = a + bi + cj + dk \) is given by \( \overline{q} = a - bi - cj - dk \).

It can easily be shown that \( \overline{q} = q \) and \( q_1 + q_2 = \overline{q_1} + \overline{q_2} \). It is also true that \( \overline{q_1 q_2} = \overline{q_2} \overline{q_1} \), it is important to note that the order of multiplication is reversed since quaternion multiplication is not commutative.

**Definition:** The norm \( N(q) \) of a quaternion is given by \( N(q) = q\overline{q} = a^2 + b^2 + c^2 + d^2 \).

Because elements commute with real numbers the norm preserves multiplication.

\[ N(q_1 q_2) = q_1 q_2 \overline{q_1} \overline{q_2} = q_1 q_2 \overline{q_2} \overline{q_1} = q_1 N(q_2) \overline{q_1} = N(q_2) q_1 \overline{q_1} = N(q_2) N(q_1) \]

Every nonzero quaternion has an inverse given by \( \frac{\overline{q}}{N(q)} \) since \( N(q) > 0 \), which means that the quaternions are a division ring. They cannot be a field like \( \mathbb{R} \) and \( \mathbb{C} \) because their multiplication is not commutative.

3 Generalizing

Now we will begin to generalize. We will define a quaternion Algebra \((a, b)_F\) with nonzero \(a, b \in F\) is an algebra over a field \( F \) with an \( i, j, \) and \( k \) such that \( i^2 = a, j^2 = b, \) and \( ij = k = -ji, \) and where \( i, j, \) and \( k \) commute with elements of \( F \). We will also assume that \( \text{char}(F) \neq 2 \).

Under this more general model Hamilton’s quaternions are given by \((-1, -1)_\mathbb{R}, \) and we can confirm this by taking

\[ k^2 = (ij)k = ijj = -iijj = i(-1)(-1) = -1 \]

giving us the rest of the rules Hamilton devised.

We can also create the algebra \((1, 1)_\mathbb{R}\) called the split-quaternions. In the split-quaternions \( i^2 = 1, j^2 = 1, \) and \( k^2 = ijj = -iijj = -(1)(1) = -1 \).

We can create other algebras, for example: \((x, x + 1)_{GF(9)}\) where \( i^2 = x, j^2 = x + 1, \) and \( k^2 = x + 2 \). Interestingly this algebra has zero divisors since \( (0 + i + j + k)^2 = 0 \).

Other things that must be generalized include the norm and conjugation. Both of these can be generalized to an arbitrary field fairly easily since they only rely on the existence of additive inverses. Multiplicative inverses also exist for all elements with \( N(q) \neq 0 \) since they are still defined as \( \frac{q}{N(q)} \).
4 Isomorphism of Algebras

The question now is, how do we know when two quaternion algebras are actually different from one another.

**Definition:** An isomorphism between quaternion algebras is a ring isomorphism \( f : A \to B \) such that \( f(c) = c \) for all \( c \in F \).

**Theorem:** For all \( a \neq 0 \) in a field \( F \), the quaternion algebra \((a, 1)_F \cong M_2(F)\), which is the algebra of \( 2 \times 2 \) matrices over \( F \). We start by mapping

\[
1 \to \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \quad i \to \begin{bmatrix} 0 & 1 \\ a & 0 \end{bmatrix}, \quad j \to \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}, \quad k \to \begin{bmatrix} 0 & -1 \\ a & 0 \end{bmatrix}
\]

Since \( \text{char}(F) \neq 2 \) we know \( 1 \neq -1 \) so these four matrices are linearly independent and

\[
x_1 + x_2i + x_3j + x_4k \to \begin{bmatrix} (x_1 + x_3) & (x_2 - x_4) \\ a(x_2 + x_4) & (x_1 - x_3) \end{bmatrix}
\]

Since the four matrices we created are linearly independant and \( \dim M_2(F) = 4 \) we know this is a bijection. We can check easily that multiplication is preserved, confirming that its a ring isomorphism. We know that our mapping takes the “scalar term” of the original algebra to multiples of the identity matrix which satisfies the second requirement of our definition, making this mapping an isomorphism. Through similar procedures we can also show that \((a, c^2)_F \cong M_2(F)\) and \((a, -a)_F \cong M_2(F)\).

We have a formal definition of an isomorphism between quaternion algebras. However, there exists a more practical way to determine an isomorphism between two quaternion algebras.

**Definition:** A quaternionic basis of \((a, b)_F\) is a set \(\{1, e_1, e_2, e_1e_2\}\) such that \(e_1^2, e_2^2 \in F\), \(e_1^2, e_2^2 \neq 0\) and \(e_1e_2 = -e_2e_1\).

Any quaternionic basis that can be constructed in a given quaternion algebra will reveal an isomorphism to another algebra with that basis as its defining basis. It is easy to see that \(\{1, i, j, ij\}\) is a basis, as well as \(\{1, j, i, ji\}\), \(\{a, i, ij, -j\}\) and other simple rearrangements of \(i, j,\) and \(k\) are also bases, meaning that \((a, b)_F \cong (b, a)_F \cong (a, -ab)_F\), along with all other obvious permutations of values when constructing an algebra.

Another form of quaternion algebra that is isomorphic to \(M_2(F)\) is any algebra where \(b = x^2 - ay^2\) for \(x, y \in F\). We can construct a basis for \((a, b)_F\) of the form like \(\{1, i, jx + ky, (i)(jx + ky)\}\). This is a basis of \((a, b)_F\), and

\[
(jx + ky)^2 = j^2x^2 + jkxy + kjxy + k^2y^2 = bx^2 - aby^2 = b(x^2 - ay^2) = b^2
\]

so \((a, b)_F \cong (a, b^2)_F \cong M_2(F)\).

It will be important later that nonzero elements of the form \(x^2 - ay^2\) actually form a group under multiplication called the norm subgroup associated to \(a\) or \(N_a\). Because \(1 = 1^2 - a0^2\) they have the multiplicative identity and because

\[
(x^2 - ay^2)(w^2 - az^2) = (xw + ayz)^2 - a(xz + wy)^2
\]
They have additive closure. Inverse elements are also in the group since
\[
\frac{1}{x^2 - ay^2} = \frac{x^2 - ay^2}{(x^2 - ay^2)^2} = \frac{x}{x^2 - ay^2} = \frac{a}{x^2 - ay^2}.
\]

**Theorem:** If \( A = (a, b) \) is a quaternion algebra over \( \mathbb{R} \), then either \( A \cong (-1, -1) \) or \( A \cong (1, 1) \). That is, either \( A \) is isomorphic to the Hamiltonian quaternions or \( A \) is isomorphic to the split-quaternions.

**Proof:** Take \((a, b)\) to have a quaternionic basis \( \{1, w, v, wv\} \) where \( w^2 = a, v^2 = b \) and \((wv)^2 = -ab\). If \( a, b < 0 \) then in the Hamiltonian quaternions one can define a basis \( \{1, \sqrt{-a}i, \sqrt{-b}j, \sqrt{ab}ij\} \) which is the same basis. This indicates that there is an isomorphism with the Hamiltonian quaternions. In the case where \( a, b > 0 \), WLOG since we have shown that rearranging \( a, b \), and \(-ab\) is an isomorphism, using the basis of the split-quaternions one can construct \( \{1, \sqrt{a}i, \sqrt{b}j, \sqrt{ab}ij\} \) which indicates the existence of an isomorphism between \( A \) and the split-quaternions.

**Theorem:** There is only one quaternion algebra over \( \mathbb{C} \) which is isomorphic to \( M_2(\mathbb{C}) \).

**Proof:** This is easy to show since for any \( b \in \mathbb{C} \) there exists an element such that \( b = c^2 \) and we know that \((a, c^2)\) does not have a division ring if and only if \( b \notin \mathbb{C} \).

**Theorem:** A quaternion algebra that is not a division ring is isomorphic to \( M_2(F) \).

**Proof** We already know that all quaternion algebras of the form \((a, c^2)\) and by isomorphism those of the form \((c^2, b)\) are isomorphic to \( M_2(F) \). So we can assume that neither \( a \) nor \( b \) are squares. If we assume that we do not have a division ring then we must have some nonzero element without a multiplicative inverse. We have already established that inverses exist for all \( q \) where \( N(q) \neq 0 \) so there must exist some \( q \) such that
\[
N(q) = x_1^2 - ax_2^2 - bx_3^2 + abx_4^2 = 0
\]
where the \( x_i \)'s are not all zero. Therefore \( x_1^2 - ax_2^2 = bx_3^2 - abx_4^2 \). Since \( a \) is not a square \( x_1^2 - ax_2^2 \neq 0 \), since if \( x_3^2 - ax_4^2 = 0 \) then either \( x_3 = 0 \), meaning \( x_3 = 0 \) or the equation can be rearranged to form \( a = \frac{x_3^2}{x_4^2} \) showing that \( a \) is a square, which is a contradiction. If both \( x_3^2 = 0 \) and \( x_4^2 = 0 \) then \( x_1^2 - ax_2^2 = 0 \) which is of a similar case. If both expressions are 0 then either all the \( x_i \)'s are 0 or \( a \) is a square. Either is a contradiction so neither expression can be zero, meaning that we can rearrange the entire expression into \( b = \frac{x_1^2 - ax_2^2}{x_4^2 - ax_4^2} \), which because we have shown that \( N_a \) is a group, means that \( b \in N_a \) therefore \( b = x^2 - ay^2 \) and by an earlier theorem \((a, b) \cong M_2(F)\).

**Theorem:** Over a field \( F, H(F) = (-1, -1) \) is a division ring if and only if \(-1 \neq x^2 + y^2 \) for \( x, y \in F \).

**Proof** If \(-1 = x^2 + y^2 \) for \( x, y \in F \) then \(-1 = x^2 - y^2 \) so \( H(F) \cong M_2(F) \) and is therefore not a division ring. If \( H(F) \) is not a division ring then \( H(F) \cong M_2(F) \) by the previous theorem. Therefore if either is not true then the other must also not be true.
So now we know that the structure of a quaternion algebra over a field $F$ can either be a division ring, or it can be isomorphic to $M_2(F)$. Over $\mathbb{R}$ there are exactly two quaternion algebras, over $\mathbb{C}$ there is only one. There are infinitely many non-isomorphic quaternion algebras over $\mathbb{Q}$, the proof of which involves primes congruent to 3 mod 4, and all but one of them are division rings.

5 Octonion algebras

I mentioned at the beginning of this paper John Graves and his octonions. They too create a general algebra over a field, but those algebras are severely less studied due to their lack of the associative property, making them more difficult to approach, as well as reducing their potential applications.

**Definition:** The octonions are numbers of the form

$$\mathbb{O} = \{a_0 + a_1e_1 + a_2e_2 + a_3e_3 + a_4e_4 + a_5e_5 + a_6e_6 + a_7e_7 | a_i \in \mathbb{R}\}$$

Where $e_i^2 = -1$ for all $e_i$, the $e_i$’s commute with real numbers, and the $e_i$’s multiply with one another following an extensive set of rules which can most succinctly be described by a diagram called the Fano plane. For any three elements on a line $e_a, e_b,$ and $e_c$ the expression $e_ae_b = e_c = -e_be_a$ holds.

While the multiplication is not commutative or associative, it does obey all forms of the Moufang identity, given by $(z(x(zy))) = (((zx)z)y)$. They still have a conjugation

$$\overline{q} = a_0 - a_1e_1 - a_2e_2 - a_3e_3 - a_4e_4 - a_5e_5 - a_6e_6 - a_7e_7$$
and a norm

\[ N(q) = q\bar{q} = \bar{q}q = a_0^2 + a_1^2 + a_2^2 + a_3^2 + a_4^2 + a_5^2 + a_6^2 + a_7^2 \]

Their norm does preserve multiplication, meaning they are still a composition algebra. And their norm also gives rise to a multiplicative inverse of every octonion \( q \) equal to \( \frac{\bar{q}}{N(q)} \).

An interesting thing to note about the octonions is that, unlike the quaternions, which can be represented as a matrix algebra, the octonions cannot since matrix multiplication is associative and octonion algebra is not. The octonions can be represented by a mathematical object called a Zorn vector matrix, which is a \( 2 \times 2 \) matrix over \( \mathbb{R} \) except two of the entries in the matrix contain vectors of dimension 3. Addition is performed componentwise while multiplication is given by

\[
\begin{bmatrix}
a & u \\
v & b \\
\end{bmatrix}
\begin{bmatrix}
c & w \\
x & d \\
\end{bmatrix} =
\begin{bmatrix}
ac + u \cdot x & aw + d u - v \times x \\

c v + b x + u \times w & bd + v \cdot w \\
\end{bmatrix}
\]

Where \( \cdot \) and \( \times \) are vector dot and cross products. Regardless of its actual utility it is certainly an interesting construction.

Generalizing from the octonions to octonion algebras can be done, but unless \( N(e_i) = 1 \) for all \( i \) it is not as simple as choosing a few values and allowing the rest to be defined by the multiplication. The aforementioned octonions \((-1, -1, -1)_{\mathbb{R}}\) and the split octonions \((1, 1, 1)_{\mathbb{R}}\) are examples of octonion algebras. Defining others and determining if they are isomorphic to an existing octonion algebra is much more complicated than the same task for quaternions. But it would likely make use of the following theorem

**Theorem** If \( e_1, e_2 \) are two distinct nonreal elements of an octonion algebra, then \( \{1, e_1, e_2, e_1 e_2\} \) is a quaternion subalgebra. This can easily be shown by the definition of the multiplication on an octonion algebra.

While quaternions and quaternion algebras have lots of applications due to their connections to three-dimensional rotations, the octonions have significantly less. I found one paper that said octonion algebras could be used to develop fully homomorphic encryption schemes. However, reviews of the paper indicated that it had some serious problems.

Beyond octonion algebras there are no more composition algebras. Sedenion algebras and beyond lack the alternative property, which means that their norm does not preserve multiplication, which is a characteristic of composition algebras.

**References**


