Beyond Complex:
An Inspection of Quaternions

Matthew Zaremsky

April 3, 2007

Senior Exercise in Mathematics,
Kenyon College Fall 2006

1 Introduction

The Brougham Bridge in Dublin, Ireland was the site of one of the most well-known examples of spontaneous mathematical inspiration in history. On October 16th, 1843, Sir William Rowan Hamilton suddenly realized in a flash of inspiration the equations that gave structure to his brainchild, the noncommutative *quaternions*. He immediately carved the equations into the stone of the bridge so as not to forget them.[1]

$$i^2 = j^2 = k^2 = ijk = -1.$$

With a mere seven symbols, Hamilton completely described the twisted, noncommutative mathematical structure of the quaternions. This took the notion of the complex numbers to another level: instead of just one square root of -1, the quaternions boasted three distinct square roots of -1. An immediate and obvious consequence of this new structure was the ability to represent 4-space via quaternion basis vectors. Much like the complex numbers can represent the complex plane, using 1 and i as basis vectors, the elements 1, i, j, and k span a complex 4-space.

Hamilton's discovery was much more far-reaching than this simple geometric application shows. The quaternion algebra makes appearances in a large number of mathematical fields, often appearing unexpectedly. In this senior exercise, I will inspect the many manifestations of the quaternion algebra, and tie the various fields together via this common thread. Specifically, I will discuss the fields of representation theory, algebra, number theory, rotational geometry, and quantum physics, and see how each is connected through quaternion mathematics.

2 Normed Composition Algebras

On the way from the complex algebra spanning 2-space to the quaternion algebra spanning 4-space, one would think there should be a similar algebraic structure for 3-space. Since we live in a universe of 3 spatial dimensions, this would be particularly applicable to real-world situations. This algebra of "triads" was actually Hamilton's initial goal. On that fateful October walk across Brougham Bridge, Hamilton was grappling with the many problems arising from the triad operations. We in the 21st century have the luxury

[1] [C]

of hindsight, and now know what Hamilton could not: that a 3-dimensional normed composition algebra is, in fact, impossible to construct. Before this can be proved, we must establish a few definitions and lemmas, but the end result, proven by Adolf Hurwitz, is worth it: normed composition algebras may only have dimension 1, 2, 4, or 8.[2]

Definition 2.1 A *normed composition algebra* is an algebra X with a norm, $|\ |$, that obeys composition. That is, $\forall\ x, y \in X$, $|xy| = |x||y|$.

An algebra is just a vector space over a field $\mathbb{K}$, with the added property of a (possibly nonassociative) multiplicative structure with a multiplicative identity applied to the space. We will use $\mathbb{K} = \mathbb{R}$. Here, a norm is a function into the reals that is positive definite and obeys the triangle inequality. We can also define an inner product $|\ ,\ |$ such that $|x, y| = \frac{1}{2}(|x + y| - |x| - |y|)$. Note that we define the norm so that $|mx| = m^2|x|$ for scalar m. This is like the squared Euclidean norm over $\mathbb{R}^n$, where for any $x = (a_1, a_2, ..., a_n)$, $|x| = a_1^2 + a_2^2 + ... + a_n^2$. Defining the norm this way ensures that $|\ ,\ |$ is positive definite; $|x, x| = \frac{1}{2}(|2x| - 2|x|) = \frac{1}{2}(4|x| - 2|x|) = \frac{1}{2}(2|x|) = |x|$, which is nonnegative, and is zero iff $x = 0$. The benefit of introducing this inner product over the algebra is that we can now designate two vectors x, y as *orthogonal*, in the case that $|x, y| = 0$. With a means of testing orthogonality at our disposal, we can more readily discuss the subspaces of a normed composition algebra. This is vital to the proof of Hurwitz's Theorem.

Definition 2.2 Let Y be a normed composition algebra with $|\ ,\ |$ and let X be an n-dimensional proper subalgebra of Y with unity. Let i be a unit vector in Y such that $|i, x| = 0\ \forall\ x \in X$, i.e. i is orthogonal to all of X. Since X is proper, $dim(X) < dim(Y)$ and such an i must exist. The *Dickson double algebra* of X is $X + iX = \{a + ib \mid a, b \in X\}$.

Since Y is closed under multiplication and addition, $X + iX$ is surely a subalgebra of Y. The norm and inner product still apply to $X + iX$, and composition still holds, so $X + iX$ is a normed composition algebra. But what is its dimension? Is it simply twice the dimension of X? If $|ia, b| = 0$, $\forall a, b \in X$, then this will be the case, since then no basis element of iX will be in X. But we don't yet know enough about the multiplicative structure of generic normed composition algebras to make this claim.

[2][C],p.67

Lemma 2.3 Scaling Laws: $|xy, xz| = |x||y, z|$, $|xz, yz| = |x, y||z|$.

Proof: Let x, y, z be in the normed composition algebra X. Then

$$\begin{aligned}
|xy| + 2|xy, xz| + |xz| &= |xy + xz| && \text{(By definition of } |\ ,\ |) \\
&= |x||y + z| && \text{(By composition)} \\
&= |x|(|y| + 2|y, z| + |z|) && \text{(By definition of } |\ ,\ |) \\
&= |xy| + 2|x||y, z| + |xz| && \text{(By composition)}
\end{aligned}$$

And so $|xy, xz| = |x||y, z|$, since the codomain of $|\ |$ and $|\ ,\ |$ is $\mathbb{R}$. The second Scaling Law, $|xz, yz| = |x, y||z|$, follows similarly.

Lemma 2.4 Exchange Law: $|xy, uz| = 2|x, u||y, z| - |xz, uy|$,
or equivalently, $|xy, uz| + |xz, uy| = 2|x, u||y, z|$.

Proof: Let $w, x, y, z \in X$. Then

$$\begin{aligned}
|xy, wz| + |xz, wy| &= |xy + wy, xz + wz| - |xy, xz| - |wy, wz| \\
&\qquad\qquad \text{(By linearity of } |\ ,\ |) \\
&= |(x + w)y, (x + w)z| - |x||y, z| - |w||y, z| \\
&\qquad\qquad \text{(By Scaling Law)} \\
&= |x + w||y, z| - |x||y, z| - |w||y, z| \quad \text{(By Scaling Law)} \\
&= (|x + w| - |x| - |w|)|y, z| \quad \text{(Distributive Property)} \\
&= 2|x, w||y, z| \quad \text{(By definition of } |\ ,\ |)
\end{aligned}$$

Before the next Lemma can be proven, the notion of conjugates must be introduced. We will define $x^* = 2|x, 1| - x$, where $2|x, 1|$ is really the identity vector in X scaled by $2|x, 1|$. We can see that for $X = \mathbb{C}$, this makes sense. If $x = a + bi$, then $2|x, 1| - x = 2a - (a + bi) = a - bi = x^*$. Also note that for any $x \in X$, $x^* \in X$ by closure of X.

Lemma 2.5 Braid Laws: $|xy, z| = |y, x^*z|$ and $|xy, z| = |x, zy^*|$.

Proof: Let $x, y, z \in X$. Then

$$\begin{aligned}
|xy, z| &= 2|x, 1||y, z| - |xz, y| && \text{(By Exchange Law for } w = 1) \\
&= |y, (2|x, 1| - x)z| && \text{(By linearity and symmetry of } |\ ,\ |) \\
&= |y, x^*z| && \text{(By definition of conjugate)}
\end{aligned}$$

The second Braid Law follows similarly.

Corollary 2.6 The Product Conjugation Law $(xy)^* = y^*x^*$ follows immediately. If we fix t to be any arbitrary element of Y,

$$|t, x| = |tx^*, 1| = |t, x^{**}|, \text{ so } x = x^{**}$$

$$\text{and } |t, (xy)^*| = |txy, 1| = |t, y^*x^*|, \text{ so } (xy)^* = y^*x^*.$$

This works because t was arbitrary.

We can now answer the question of whether $|ia, b| = 0, \forall a, b \in X$. Taking the inner product, $|ia, b| = |i, ba^*|$ for any $a, b \in X$. Since we chose i to be orthogonal to every vector in X, this is zero. Thus, iX and X have no basis vectors in common and $dim(X + iX) = 2dim(X)$.

Example 2.7 Let Y be the 4-dimensional algebra of quaternions $\mathbb{H}$. The basis elements of this are $1, i, j, k$, and they obey the relations established by Hamilton's famous equations. Let X be the 2-dimensional subset of Y generated by the basis elements 1 and j. Then the second part of the Dickson double algebra of X can be taken to be iX, since $|1, i| = |j, i| = 0$. Under these definitions, $X = \{a + jb | a, b \in \mathbb{R}\}$ and $iX = \{ia + ijb | a, b \in \mathbb{R}\}$. But ij is really k, and so $X + iX = \{a + jb + ic + kd | a, b, c, d \in \mathbb{R}\} = Y$. The quaternion algebra decomposes into two copies of the complex algebra.

So any normed composition algebra with even dimension can be decomposed into normed composition algebras of smaller dimension. It would seem that the converse should be true also. If we have a normed composition algebra, shouldn't we be able to invent a new element i that is orthogonal to everything else, and thus double our algebra? We can in fact do this. Given any algebra Y we can invent an i that is orthogonal to everything in Y and construct $Z = Y + iY$ with twice the dimension of Y. The problem is, there's no guarantee that Z will still be a normed composition algebra. If Y does not have certain important properties, Z will not have the characteristic composition property that every normed composition algebra must have: $|xy| = |x||y| \ \forall x, y \in Z$. Note that the norm and inner product in Z are not equivalent to the norm and inner product in Y. Half the elements of Z are not even in Y. We can, however, work out how these operations should act, along with how conjugation and multiplication should act in Z. Defining a norm and inner product on a Dickson double of a normed composition algebra allows us to ask whether the normed double algebra is also a composition algebra. The answer, as will be shown, is Hurwitz's Theorem.

Let Y be a normed composition algebra and let $Z = Y + iY$ be its Dickson double algebra. We repeatedly use the fact that $|i| = 1$, by definition of i, and that i is orthogonal to every element of Y.

Arithmetic Rules:

1. What is the inner product of two elements of $Y + iY$?
2. How does conjugation work over $Y + iY$?
3. How do elements of $Y + iY$ multiply?

Proof 2.8 (1) Proof that $|a + ib, c + id| = |a, c| + |b, d|$.

Let $a, b, c, d \in Y$. Then

$$\begin{aligned} |a + ib, c + id| &= |a + ib, c| + |a + ib, id| \\ &= |a, c| + |ib, c| + |a, id| + |ib, id| \\ &= |a, c| + |i, cb^*| + |ad^*, i| + |i||b, d| \\ &= |a, c| + |b, d| \end{aligned}$$

The norm is defined as $|x| = |x, x|$, just like before.

Proof 2.9 (2) Proof that $(a + ib)^* = a^* - ib$.

Let $a, b \in Y$. Then

$$\begin{aligned} (a + ib)^* &= 2|a + ib, 1| - a - ib \\ &= 2|a, 1| + 2|ib, 1| - a - ib \\ &= 2|a, 1| - a - ib \\ &= a^* - ib \end{aligned}$$

Note that $i^* = -i$. Also note that $ib = -(ib)^* = -b^*i^* = b^*i$. The step $(ib)^* = b^*i^*$ is due to the Product Conjugation Law.

Proof 2.10 (3) Proof that $(a + ib)(c + id) = (ac - db^*) + i(cb + a^*d)$.

First, $(a + ib)(c + id) = ac + a(id) + (ib)c + (ib)(id)$. Since we don't necessarily have associativity, we don't know many of these terms. We must use the inner product to find $a(id)$, $(ib)c$, and $(ib)(id)$ in the desired forms

$\alpha + i\beta$. The following are three inner product tricks, (IP1), (IP2), and (IP3). Fix t to be an arbitrary element of Z.

(IP1)

$$\begin{aligned} |t, a(id)| = |a(id), t| &= |id, a^*t| \text{ Now use the Exchange Law, so} \\ &= 2|i, a^*||d, t| - |it, a^*d| \\ &= -|it, a^*d| \\ &= |t, i(a^*d)| \end{aligned}$$

Since t was arbitrary, $a(id) = i(a^*d)$.

(IP2)

$$\begin{aligned} |(ib)c, t| &= |ib, tc^*| \\ &= |b^*i, tc^*| \text{ Now use the Exchange Law, so} \\ &= 2|b^*, t||i, c^*| - |b^*c^*, ti| \\ &= -|b^*c^*, ti| \\ &= |(b^*c^*)i, t| \\ &= |(cb)^*i, t| \\ &= |i(cb), t| \end{aligned}$$

Since t was arbitrary, $(ib)c = i(cb)$.

(IP3)

$$\begin{aligned} |(ib)(id), t| &= -|ib, t(id)| \text{ Now use the Exchange Law, so} \\ &= -2|i, t||b(id)| + |i(id), tb| \\ &= |i(id), tb| \\ &= -|id, i(tb)| \\ &= -|i||d, tb| \\ &= -|d, tb| \\ &= |-db^*, t| \end{aligned}$$

Since t was arbitrary, $(ib)(id) = -db^*$.

Returning to $(a + ib)(c + id) = ac + a(id) + (ib)c + (ib)(id)$, we can now say that $(a + ib)(c + id) = ac + i(a^*d) + i(cb) - db^*$. This simplifies to $(a + ib)(c + id) = (ac - db^*) + i(cb + a^*d)$, which is what we want.

Armed with the tools of composition algebra arithmetic, we can ask the question, what is required of Y for $Z = Y + iY$ to be a composition algebra? We know now that it is a normed algebra, but is it a normed composition algebra? What restrictions must be imposed on $a, b, c, d \in Y$ so that $|a + ib||c + id| = |(ac - db^*) + i(cb + a^*d)|$? Can we keep doubling our algebras indefinitely, with no fear of losing the composition property? To find out, we expand both sides of the equality $|a + ib||c + id| = |(ac - db^*) + i(cb + a^*d)|$, via $|x+y| = |x|+|y|+2|x, y|$, and simplify using the tools we've established. The last step is the result of the distributive law.

$$(|a|+|ib|+2|a, ib|)(|c|+|id|+2|c, id|) = |ac|+|db^*|-2|ac, db^*|+|icb|+|ia^*d|+2|icb, ia^*d|$$

$$(|a| + |b|)(|c| + |d|) = |ac| + |db| - 2|ac, db^*| + |cb| + |ad| + 2|cb, a^*d|$$

$$2|ac, db^*| = 2|cb, a^*d|$$

Now we see that, using the Braid Law, $|(ac)b, d| = |a(cb), d|$ for any $a, b, c, d \in Y$. By the principle that $|x, y| = |z, y| \Rightarrow x = z$, it follows that $(ac)b = a(cb) \forall a, b, c \in Y$. Thus, Y must be an associative normed composition algebra.

Result 2.11 *If $Z = Y + iY$ is a normed composition algebra, then Y must be associative.*

Any associative normed composition algebra can be doubled, and still retain its composition property. Also, $Z = Y + iY$ will only have composition if Y is associative. But where did Y come from? Can we construct associative normed composition algebras of any dimension? For any algebra of dimension higher than 1, we can always find a proper nontrivial subspace with lower dimension, and then construct its Dickson double algebra. Thus, unless Y has dimension 1, it must split into $X + iX$ for some X and $i \in Y$. The question now becomes, can X be of any dimension? What are the restrictions on X that ensure Y is associative? We can use the results from the $Z = Y + iY$ case. Since $Y = X + iX$ is a normed composition algebra, (IP2) gives that $(ia)b = i(ba)$ for any $a, b \in X$. Before, Z was not necessarily associative, but here Y *is* associative. Thus, $i(ab) = i(ba)$. Since we chose i to be a unit, we can divide out by i. Thus, $ab = ba$ for all $a, b \in X$ and X is commutative.

Result 2.12 *If $Y = X + iX$ is an associative normed composition algebra, then X must be commutative.*

So any commutative, associative normed composition algebra can be doubled, and still retain its associativity and composition properties. Also, $Y = X + iX$ will only be associative if X is commutative. But we still don't know whether X has a restricted dimension. Can we construct a commutative, associative normed composition algebra of arbitrary dimension? Using the same trick as before, we know we can decompose X into $X = W + iW$ for some $i \in X \backslash W$. What are the restrictions on W? We refer back to the second arithmetic rule, that $ia = a^* i$ for any a. If X is commutative, this is $ia = ia^*$, and so $a = a^*$, for any $a \in W$. So W must have a *trivial conjugation.*

Result 2.13 *If $X = W + iW$ is a commutative, associative normed composition algebra, then W must have trivial conjugation.*

Now we can actually say something about dimension. What are the possible dimensions of W? Since $x^* = x$ for all $x \in W$, $2|x, 1| - x = x$. Thus, $|x, 1| = |x|$ and if x is orthogonal to 1, $|x|$ must be zero. Thus, W has dimension 1.

Theorem 2.14 Hurwitz's Theorem:

$dim(W) = 1$ so $\dim(X) = 2$, $dim(Y) = 4$, and $dim(Z) = 8$. Clearly, X does not have trivial conjugation, since it has dimension greater than 1. But then Y cannot be commutative, and so Z cannot be associative. Therefore, $Z + iZ$ is *not a normed composition algebra.* The only normed composition algebras have dimension 1, 2, 4, and 8, and they are $\mathbb{R}$, $\mathbb{C}$, $\mathbb{H}$, and $\mathbb{O}$.

We can show that these are unique up to isomorphism, since we are dealing with algebras over the reals. We know a normed composition algebra of dimension 1 must simply be $\mathbb{R}$. Since the other three normed composition algebras are constructed via the Dickson doubles of the previous one, it follows that these algebras are all unique up to isomorphism. The algebras of the real numbers, complex numbers, quaternions, and octonions $\mathbb{O} = \mathbb{H} + i\mathbb{H}$ are the *only* normed composition algebras that exist. If we restrict ourselves to examining only associative algebraic structures, so that there is a *ring* structure, then the quaternions are in fact the only nonabelian algebra of this type.

In the course of proving this, we have also established most of quaternion arithmetic! We know now that the quaternions are the Dickson double

algebra of $\mathbb{C}$. Thus, any quaternion q is really $z + iw$ for complex numbers z, w. Note that the "i" contained in z and w, say $z = a + ib$, $w = c + id$, is really "j" in the quaternion sense. This way, $z = a + jb$ and $iw = ia + ijb = ia + kb$, and q is in terms of the right basis elements. We can now use the Arithmetic Rules.

(1): We can take the inner product of two quaternions, q_1 with q_2:

$$|z_1 + iw_1, z_2 + iw_2| = |z_1, z_2| + |w_1, w_2| = a_1a_2 + b_1b_2 + c_1c_2 + d_1d_2.$$

(2): We can find q^*:

$$q^* = z^* - iw = a - jb - ic - kd.$$

(3): Lastly, we can find q_1q_2:

$$\begin{array}{rcl} q_1q_2 & = & (z_1z_2 - w_2w_1^*) + i(z_2w_1 + z_1^*w_2) \\ & = & (a_1a_2 - b_2b_1) + j(a_2b_1 + a_1b_2) \\ & - & (c_1c_2 + d_2d_1) + j(c_2d_1 - c_1d_2) \\ & + & i(a_2c_1 - d_1b_2) + k(c_1b_2 + a_2d_1) \\ & + & i(a_1c_2 - d_2b_1) + k(c_2b_1 + a_1d_2) \end{array}$$

The tools are all established, and we are ready to put these quaternions to use.

3 Quaternionic Representations: the Algebra Structure

Being the basis of a normed composition algebra with operations both of addition and multiplication, the quaternions naturally lend themselves to some sort of matrix representation. We show here that $\mathbb{H}_2^{\mathbb{C}} = \left\{ \begin{pmatrix} z & w \\ -w^* & z^* \end{pmatrix} : z, w \in \mathbb{C} \right\}$ is in fact an isomorphic copy of the normed composition algebra that is associative but not commutative, i.e. the quaternion algebra. Here, the matrix algebras used have the standard matrix addition and multiplication as their operations, and are over the scalar field $\mathbb{R}$.

Proof 3.1 Let $\tilde{i} = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}$, $\tilde{j} = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$, $\tilde{k} = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}$.

We see from the definition that $\tilde{i}, \tilde{j}, \tilde{k} \in \mathbb{H}_2^{\mathbb{C}}$.

Inspecting these elements, we find that

$$\tilde{i}^2 = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix} \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix} = -\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix},$$

$$\tilde{j}^2 = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} = -\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix},$$

$$\tilde{k}^2 = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix} \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix} = -\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \text{ and}$$

$$\tilde{i}\tilde{j}\tilde{k} = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix} \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix} = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix} \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix} = -\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.$$

So these matrices act in the manner expected of the basis elements of the quaternion algebra. To show that this really is a representation of $\mathbb{H}$, however, we must show that $1, \tilde{i}, \tilde{j}, \tilde{k}$ forms a basis of $\mathbb{H}_2^{\mathbb{C}}$. Clearly, these four matrices are linearly independent.

To show that they form a basis, we must show that any $\begin{pmatrix} z & w \\ -w^* & z^* \end{pmatrix} \in \mathbb{H}_2^{\mathbb{C}}$ can be written as a linear combination of $1, \tilde{i}, \tilde{j}, \tilde{k}$.

Let $z, w \in \mathbb{C}$, and let $z = a + bi$, $w = c + di$ for $a, b, c, d \in \mathbb{R}$. Then

$$\begin{aligned} a1 + b\tilde{i} + c\tilde{j} + d\tilde{k} &= a\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} + b\begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix} + c\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} + d\begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix} \\ &= \begin{pmatrix} a+bi & 0 \\ 0 & a-bi \end{pmatrix} + \begin{pmatrix} 0 & c+di \\ -c+di & 0 \end{pmatrix} \\ &= \begin{pmatrix} z & w \\ -w^* & z^* \end{pmatrix} \end{aligned}$$

So $1, \tilde{i}, \tilde{j}, \tilde{k}$ is a basis of $\mathbb{H}_2^{\mathbb{C}}$.

Having established that the quaternion algebra can be represented via 2×2 matrices with complex entries, the natural next question is, can matrices with purely *real* entries represent the quaternions? If $\mathbb{C}$ could be

represented with real matrices, then z and w could be turned into matrices, and $\begin{pmatrix} z & w \\ -w^* & z^* \end{pmatrix}$ would be a matrix with real entries, of possibly higher dimension than before.

Let $\tilde{i} = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$. Then for any $z = a + bi \in \mathbb{C}$, we can represent z by

$$z \mapsto \begin{pmatrix} a & b \\ -b & a \end{pmatrix} = a \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} + b \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix},$$

which is $a + bi$ in matrix form. Thus, returning to our quaternion representation, any $q = a + bi + cj + dk \in \mathbb{H}$ can be represented with a 4-dimensional real-valued matrix

$$\begin{pmatrix} a & b & c & d \\ -b & a & -d & c \\ -c & d & a & -b \\ -d & -c & b & a \end{pmatrix} \in \mathbb{H}_4^{\mathbb{R}}$$

The following table nicely summarizes these results.

	$\mathbb{R}$	$\mathbb{C}$	$\mathbb{H}$	$\mathbb{O}$
$\mathbb{R}$	$\mathbb{R}_1^{\mathbb{R}}$	$\mathbb{C}_2^{\mathbb{R}}$	$\mathbb{H}_4^{\mathbb{R}}$	$\mathbb{O}_8^{\mathbb{R}}$
$\mathbb{C}$		$\mathbb{C}_1^{\mathbb{C}}$	$\mathbb{H}_2^{\mathbb{C}}$	$\mathbb{O}_4^{\mathbb{C}}$
$\mathbb{H}$			$\mathbb{H}_1^{\mathbb{H}}$	$\mathbb{O}_2^{\mathbb{H}}$
$\mathbb{O}$				$\mathbb{O}_1^{\mathbb{O}}$

We have seen that $\mathbb{H}$ can be represented as $\mathbb{H}_2^{\mathbb{C}}$, or as $\mathbb{H}_4^{\mathbb{R}}$, and that $\mathbb{C}$ can be represented as $\mathbb{C}_2^{\mathbb{R}}$. We also claim without proof that the pattern holds for $\mathbb{O}$, the algebra of octonions. This table shows the pattern in the representations of the four normed composition algebras. Each column lists possible matrix representations of a given algebra, with entries from the algebra indicated on the left. In each case, for algebras $\mathbb{A}$ and $\mathbb{B}$, $\mathbb{A}_n^{\mathbb{B}} \subseteq M_n(\mathbb{B})$.

Representing the bases of these algebras as matrices leads to an interesting question: what is the internal structure of the sets of basis matrices? Do they form a group? If so what sort of group? Matrix groups, surely. Before the structure of the *representations* of basis elements can be discussed,

however, we must elucidate the structure of the basis elements themselves, in a generalized form.

4 Generalized Quaternions: the Group Structure

Hamilton's equations determine the algebra of quaternions that is a normed composition algebra, but it is also possible to craft algebras of *generalized quaternions*. These may not be normed composition algebras, but they still will be the basis of *some* algebra. Working out the details of the generalized quaternions also leads us to the underlying *group* structure of the quaternions, where the basis elements form a nonabelian multiplicative group.

We define

$$i^3 = j^2 = k^2 = ijk = -1.$$

This style of presentation is in reverence to Hamilton's style, but it is a bit deceptive. Using "k" makes it seem like there are 3 independent imaginary numbers that all combine in various ways to form -1. But really, we can represent any one of these elements in terms of the other two. For no particular reason, we choose to write k as ij. We could have just as easily called i "$-kj$", or called j "i^2k", but eliminating k is the cleanest option. So we rewrite the equations as

$$i^3 = j^2 = (ij)^2 = -1$$

or even

$$i^3 = j^2 = -1, j^{-1}ij = i^{-1}.$$

This last presentation most clearly shows the group structure of the basis elements. Let

$$Q_3 = \{1, j, i, ij, i^2, i^2j, -1, -j, -i, -ij, -i^2, -i^2j\}$$

be the multiplicative group of basis elements and their additive inverses of the generalized quaternion algebra. To check that this is a group, we check that each element has a (multiplicative) inverse: If we let $Q_3^{-1} = \{x^{-1} \mid x \in Q_3\}$, then

$$Q_3^{-1} = \{1, -j, -i^2, -ij, i, -i^2j, -1, j, i^2, ij, i, i^2j\} = Q_3.$$

Also, we must check that Q_3 is closed, for it to be a group. Since $jij = i^2$, we can see that $ji = -i^2j \in Q_3$ and $ji^2 = -ij \in Q_3$. This fully determines the possible multiplications of powers of j and i, and so the group is in fact closed.

It is no surprise that in this case there is nothing special about the number 3. If we define a set of relations to determine the group Q_n, a similar result should follow.

$$i^n = j^2 = -1, j^{-1}ij = i^{-1}$$

These relations form Q_n, which has elements $1, j, i, ij, i^2, i^2j, ..., i^{n-1}, i^{n-1}j$ and $-1, -j, -i, -ij, -i^2, -i^2j, ..., -i^{n-1}, -i^{n-1}j$. The groups of generalized quaternions have order $4n$. Note that for $n = 1$, $Q_1 = \{\pm 1, \pm j\}$. This is just $\mathbb{Z}_4$, since $Q_1 = \langle j \rangle$ and $|Q_1| = 4$. Any cyclic group of order 4 must be isomorphic to $\mathbb{Z}_4$.

Hamilton's insight about noncommutative possibilities applies to a much broader portion of group theory than Hamilton initially knew. It is easy to lose sight of Hamilton's equations in this sea of possibilities. The generalized quaternions do, however, reduce to Hamilton's quaternions when $n = 2$: $Q_2 = \{\pm 1, \pm j, \pm i, \pm ij\}$. This group is clearly nonabelian, since $ji = -ij$, and has order 8. The only groups of order 8 that are nonabelian are D_4 and Dic_4, the dihedral and dicyclic groups of order 8. Thus, the quaternions must be isomorphic to one of these. It is easy to find out which one by using a simple order argument. In D_4, if we imagine the elements to be symmetric rotations and reflections of a square, surely a reflection will have order 2, as will a rotation of 180. But the only basis element of the quaternion algebra that has order 2 is -1. The identity has order 1, and $\pm i, \pm j, \pm ij$ all have order 4. Thus, $Q_2 = Dic_4$.

There is a useful Latin Square on page 55 of Ledermann that details the structure of the quaternion group. With this chart, it is easy to see that -1

is the only element of order 2, i.e. it is the only nontrivial element whose square is 1.

	1	i	-1	$-i$	j	ij	$-j$	$-ij$
1	1	i	-1	$-i$	j	ij	$-j$	$-ij$
i	i	-1	$-i$	1	ij	$-j$	$-ij$	j
-1	-1	$-i$	1	i	$-j$	$-ij$	j	ij
$-i$	$-i$	1	i	-1	$-ij$	j	ij	$-j$
j	j	$-ij$	$-j$	ij	-1	i	1	$-i$
ij	ij	j	$-ij$	$-j$	$-i$	-1	i	1
$-j$	$-j$	ij	j	$-ij$	1	$-i$	-1	i
$-ij$	$-ij$	j	ij	$-j$	i	1	$-i$	-1

Contrast this with the chart of $D_4 = \langle a, b | a^4 = b^2 = (ba)^2 = 1 \rangle$, on the same page.

	1	a	a^2	a^3	b	ab	a^2b	a^3b
1	1	a	a^2	a^3	b	ab	a^2b	a^3b
a	a	a^2	a^3	1	ab	a^2b	a^3b	b
a^2	a^2	a^3	1	a	a^2b	a^3b	b	ab
a^3	a^3	1	a	a^2	a^3b	b	ab	a^2b
b	b	a^3b	a^2b	ab	1	a^3	a^2	a
ab	ab	b	a^3b	a^2b	a	1	a^3	a^2
a^2b	a^2b	ab	b	a^3b	a^2	a	1	a^3
a^3b	a^3b	a^2b	ab	b	a^3	a^2	a	1

Here, the elements a and a^3 both have order 2. Note, though, that the top-left fourth of each square is the same. Both of these groups contain an isomorphic copy of $\mathbb{Z}_4$, generated by i and a respectively. The difference comes about by virtue of the "b" or "j" element having order 2 or 4. In D_4, $b^2 = 1$, and in Q_2, $j^2 = -1$. This minus sign makes all the difference.

The generalized quaternion groups also provide a basis for generalized quaternion algebras. We know $Q_n = \{\pm 1, \pm j, \pm i, \pm ij, \pm i^2, \pm i^2 j, ..., \pm i^{n-1}, \pm i^{n-1} j\}$. We also know that, since 1 and -1 commute with every element of Q_n and $(-1)^2 = 1$, that $\{1, -1\}$ is a normal subgroup of Q_n. If we consider the factor group $Q'_n = Q_n / \{1, -1\}$, we will have a set with $2n$ elements. We

also have the property that none of the elements of Q'_n are scalar multiples of each other, with scalars taken from $\mathbb{R}$. The move from Q_n to Q'_n ensures this, since in Q_n, $-i = (-1)i$ etc. Thus they span a space of dimension $2n$, the generalized quaternion algebra of dimension $2n$, which we will denote $\mathbb{G}_n$.

A natural question arises. Do Hamilton's quaternions produce the only normed composition algebra among the algebras with generalized quaternion bases? Is $\mathbb{G}_2 = \mathbb{H}$ the only $\mathbb{G}_n$ that is a normed composition algebra? It is perfectly believable that for $n > 4$, $\mathbb{G}_n$ is not a normed composition algebra. The algebra basis is $\{1, j, i, ij, ..., i^{n-1}, i^{n-1}j\}$, so for $n > 4$ the algebra has dimension larger than 8. Hurwitz has proven that no normed composition algebras exist with such high dimensions. We also know that $n = 3$ won't work, since normed composition algebras can't have dimension 6. But the $n = 1$ and $n = 4$ cases are puzzling; couldn't $\mathbb{G}_1 \cong \mathbb{C}$ or $\mathbb{G}_4 \cong \mathbb{O}$? Surely the basis of $\mathbb{G}_1$ has two elements, $\{1, j\}$, and the basis of $\mathbb{G}_4$ has eight elements, $\{1, j, i, ij, i^2, i^2j, i^3, i^3j\}$.

As a matter of fact, $\mathbb{G}_1$ is isomorphic to $\mathbb{C}$, since the basis of $\mathbb{G}_1$ is just $\{1, j\} \cong \{1, i\}$ where i is the standard imaginary number in $\mathbb{C}$. It's a bit strange to call Q_1 a generalized quaternion group though, considering it's abelian. The whole point of Hamilton's quaternions was that it was a noncommutative, yet still fully structured, mathematical construct. We ask then instead, which of the generalized quaternions are nonabelian and produce normed composition algebras? Clearly Q_2 does, since $\mathbb{G}_2 = \mathbb{H}$ (not even an isomorphism, this is an *equality*). But what about Q_4? Is $\mathbb{G}_4 \cong \mathbb{O}$?

A single counterexample is sufficient to disprove a conjecture. Therefore, if we can find two elements whose norms do not compose over multiplication, $\mathbb{G}_4$ will not be a normed composition algebra. Consider $(1 + i), (i^2 + i^3) \in \mathbb{G}_4$. Recall that Q_4 is defined via $i^4 = j^2 = (ij)^2 = -1$. If $\mathbb{G}_4$ were a normed composition algebra, then $|(1 + i)||(i^2 + i^3)|$ would have to be equal to $|(1 + i)(i^2 + i^3)| = |i^2 + 2i^3 - 1|$. But $|(1 + i)||(i^2 + i^3)| = (2)(2) = 4$ whereas $|i^2 + 2i^3 - 1| = 6$. The norms of these algebra elements do not compose over multiplication, and so $\mathbb{G}_4$ cannot be a normed composition algebra. Since Q_4 is the only generalized quaternion group of order 16, this also tells us that the octonions are not a generalized quaternion algebra. Another obvious reason for this is that the basis elements of the octonions are not associative. Since for any n, Q_n is a group by definition, it must be associative and the octonions cannot be a generalized quaternion algebra.

5 Geometric Applications of Quaternions

[3] We now return to the representation $\mathbb{H}_2^{\mathbb{C}}$ of the quaternions. Since we know that the quaternions have a group structure, and that they have matrix representations, it would seem that they should thus be isomorphic to some matrix group. Since representations are homomorphisms, the group structure can be entirely determined by inspecting the representations of the basis elements $\tilde{i}, \tilde{j}, \tilde{k}$. Whatever matrix group $\mathbb{H}_2^{\mathbb{C}}$ is isomorphic to, we know it is generated by $\tilde{i}, \tilde{j}, \tilde{k}$, since i, j, and k can generate the quaternion group. Thus we can write down an arbitrary element $\tilde{q} = x\tilde{i} + y\tilde{j} + z\tilde{k} + t\tilde{1}$ of $\mathbb{H}_2^{\mathbb{C}}$, where $x, y, z, t \in \mathbb{R}$, and

$$\tilde{i} = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix} \quad \tilde{j} = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \quad \tilde{k} = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix} \quad \tilde{q} = \begin{pmatrix} x+yi & z+ti \\ -z+ti & x-yi \end{pmatrix}.$$

Thanks to the matrix nature of $\tilde{q}$, we can readily find the determinant, and thus consider the subset of possibilities such that the determinant is 1. Let $1 = |\tilde{q}| = x^2+y^2+z^2+t^2$, so x, y, z, t are real numbers such that the sum of their squares is 1. Given this condition, we can also show that matrices of this form are unitary, i.e. their hermitian conjugate (conjugate transpose $\dagger$) is their inverse.

$$\begin{aligned} \tilde{q}^\dagger \tilde{q} &= \begin{pmatrix} x-yi & -z-ti \\ z-ti & x+yi \end{pmatrix} \begin{pmatrix} x+yi & z+ti \\ -z+ti & x-yi \end{pmatrix} \\ &= \begin{pmatrix} x^2+y^2+z^2+t^2 & xz+yt-xz-yt \\ zx+yt-xz-yt & z^2+t^2+x^2+y^2 \end{pmatrix} \\ &= \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \end{aligned}$$

$$\begin{aligned} \tilde{q}\tilde{q}^\dagger &= \begin{pmatrix} x+yi & z+ti \\ -z+ti & x-yi \end{pmatrix} \begin{pmatrix} x-yi & -z-ti \\ z-ti & x+yi \end{pmatrix} \\ &= \begin{pmatrix} x^2+y^2+z^2+t^2 & -xz-yt+zx+ty \\ -zx+yt+xz-ty & z^2+t^2+x^2+y^2 \end{pmatrix} \\ &= \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \end{aligned}$$

[3] [B]

So $\tilde{q}$ is unitary and has determinant 1. This is the very requirement for being in the *special unitary group* SU_2! But can every element of SU_2 be expressed in the quaternionic form? If so, then it will be true that $SU_2 \cong (\mathbb{H}_2^{\mathbb{C}})^{\times}$, the multiplicative group of the complex representation for the quaternion algebra.

Let $A \in SU_2$. So $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$, $a, b, c, d \in \mathbb{C}$, where $ad - bc = 1$ and $A^{\dagger} = A^{-1}$. But then $\begin{pmatrix} a^* & c^* \\ b^* & d^* \end{pmatrix} = \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$ and so $d = a^*$ and $c = -b^*$.

But then $A = \begin{pmatrix} a & b \\ -b^* & a^* \end{pmatrix}$ which was exactly the form of matrices in $\mathbb{H}_2^{\mathbb{C}}$. We conclude that $SU_2 \cong (\mathbb{H}_2^{\mathbb{C}})^{\times}$.

So the normal quaternions, those that have norm 1, can represent the special unitary group. But what does this entail? What does SU_2 do that makes this a useful representation? The key lies in the relationship between SU_2 and SO_3, the special orthogonal group of 3×3 matrices. Orthogonal groups are those for which the transpose of each matrix element is also that matrix's inverse. Note that these differ from unitary groups in that the inverse of an element is its transpose, not its conjugate transpose. As might be expected, the *special* orthogonal groups are those for which every element has determinant 1. The thing about SO_3 that is important for our purposes here is that it is the group of rotations about the origin in the xyz-plane.

We represent a vector in 3-space by a quaternion $v = ai + bj + ck$, where a, b, c are real numbers. This is strikingly similar to $\hat{i}, \hat{j}, \hat{k}$ from vector analysis. Then conjugating v by any of the unit quaternions will yield:

$$-ivi = -i(ai + bj + ck)i = ai - bj - ck,$$
$$-jvj = -j(ai + bj + ck)j = -ai + bj - ck,$$
$$-kvk = -k(ai + bj + ck)k = -ai - bj + ck.$$

These are rotations! Conjugating by i is a 180° rotation about the x-axis. Conjugating by j is the same, about the y-axis, and k corresponds to the z-axis. Since we have a mapping between the quaternions and SU_2, we now also have the mapping between SU_2 and the group of 3-dimensional rotations.

Quaternions have another application to 3-dimensional geometry: taking the cross product. If we have vectors u, v in the quaternion form $u = ai +$

$bj + ck$, $v = di + ej + fk$, we can compute their product thanks to the arithmetic rules.

$$uv = (-ad - be - cf) + i(bf - ce) + j(cd - af) + k(ae - bd).$$

If we take the imaginary part of this, we have a vector equivalent to $u \times v$. Thinking of u and v now in $\mathbb{R}^3$,

$$u \times v = \begin{vmatrix} \hat{i} & \hat{j} & \hat{k} \\ a & b & c \\ d & e & f \end{vmatrix} = \begin{pmatrix} bf - ce \\ cd - af \\ ae - bd \end{pmatrix}.$$

There is a clear mapping from $\mathbb{R}^3$ to $\mathbb{H}\backslash\text{span}\{1\}$. Addition maps to addition, and the cross product in $\mathbb{R}^3$ maps to a sort of skewed multiplication in $\mathbb{H}\backslash\text{span}\{1\}$. (This really should be written $(\mathbb{H}\backslash\text{span}\{1\}) \cup \{\mathbf{0}\}$ but we call it $\mathbb{H}\backslash\text{span}\{1\}$ here for brevity's sake). Hamilton's original goal is realized! The complex numbers can describe 2-space, and the quaternions can describe 3-space. There is no need for the "triad" algebra that Hamilton could not find, and which we now know does not even exist. The three-dimensional space $\mathbb{H}\backslash\text{span}\{1\}$ is not closed under multiplication, but it is closed under the operation $\text{Im}(uv)$ and under addition. Thus, it is a group under addition, with a closed multiplication. This multiplication acts like the cross product though, and so it is not associative. Since the only nonassociative normed composition algebra is $\mathbb{O}$, which has dimension 8, we know that $\mathbb{H}\backslash\text{span}\{1\}$ is not a normed composition algebra. So Hurwitz is still right, and there are no normed composition algebras of dimension 3; no triads. But the quaternions are capable of doing exactly that function intended for Hamilton's triads: modelling transformations in $\mathbb{R}^3$, just like $\mathbb{C}$ models $\mathbb{R}^2$.

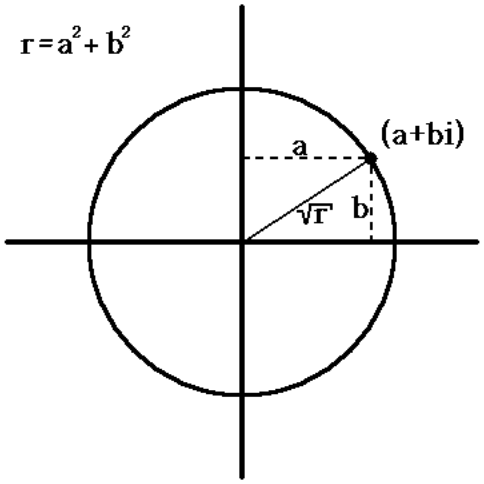
6 Quaternions in Number Theory

Algebra and Number Theory are closely tied, and many algebraic structures exhibit number theoretic properties. The quaternions are no exception. Up until now we have thought of the normed composition algebras as being over some field K, where K is either $\mathbb{R}$ or $\mathbb{C}$. This means that any element q of a normed composition algebra X can be written as a linear combination of basis elements $q = a_1x_1 + a_2x_2 + ... + a_nx_n$ where $a_i \in K$ $\forall i$ and $\{x_i\}_i$

is a basis of X. It is also possible to discuss algebras over a ring, and a well-known example involving $\mathbb{C}$ extends to $\mathbb{H}$ in an intuitive way.

The Gaussian integers are complex numbers with integer coefficients. The set of all Gaussian integers is a $\mathbb{Z}$-*algebra*, an algebra over the ring $\mathbb{Z}$, with basis $\{1, i\}$. Unlike K-algebras, such as $\mathbb{C}$ or $\mathbb{H}$ over a field K, the Gaussian integers do not furnish their scalars with multiplicative inverses. They do, however, have the same norm $|\ |$ and inner product $|\ ,\ |$ as $\mathbb{C}$. Thus, for $a + bi$ and $c + di$ in the Gaussian integers $\mathbb{Z}[i]$, $|a + bi| = a^2 + b^2$ and $|a + bi, c + di| = \frac{1}{2}(|a + bi + c + di| - |a + bi| - |c + di|) = ac + bd$. Note that both of these are integers, and that for any $z \in \mathbb{Z}[i]$, $|z|$ is the sum of two squares of integers.

The Gaussian integers can be used in this way to determine whether a given integer can be represented as the sum of two squares. We draw a circle in the complex plane, centered at 0 and with real radius $\sqrt{r}$ for some integer r. By the Pythagorean Theorem, any Gaussian integer lying on the circle implies that r is the sum of two squares, namely $r = a^2 + b^2$.



A similar phenomenon happens in the algebra of integer quaternions, $\mathbb{H}(\mathbb{Z})$. For any $q = a + bi + cj + dk \in \mathbb{H}(\mathbb{Z})$, $|q| = a^2 + b^2 + c^2 + d^2$. Since $a, b, c, d \in \mathbb{Z}$, this number $|q|$ is the sum of four squares. In the Gaussian integers, there are certain norms which never occur. The number 3, for instance, is not the norm of a Gaussian integer, since the only way to write 3 as the sum of two nonnegative integers is 3=0+3 or 3=1+2, but 2 and 3

are not squares. In the integer quaternions, however, *every* natural number is the norm of some algebra element. Every natural number can be written as the sum of four squares. Before this can be proven, we must establish a theorem about sums of two squares, i.e. possible norms of Gaussian integers.

Theorem 6.1 Proven by Euler in 1793:
For p an odd prime, $p = a^2 + b^2$ for $a, b \in \mathbb{N} \cup \{0\}$ iff $p \equiv_4 1$.

Proof: Let $p = a^2 + b^2$ as defined above. Since $\mathbb{F}_p$ is a field, a has a multiplicative inverse. Thus, $a^2 + b^2 \equiv_p 0$ implies that $1 + (b/a)^2 \equiv_p 0$ and $x^2 = -1$ has a solution modulo p. Thus, $\exists\ x \in \mathbb{F}_p$ such that $x = -x^{-1}$. Is x unique? Suppose $x^2 = y^2 = -1$. Then $x^2 - y^2 = 0$ and $(x + y)(x - y) = 0$. Since this is a field, either $x = y$ or $x = -y$. So the solution to $x^2 + 1 = 0$ is unique up to additive inverse.

We now consider a means of partitioning $\mathbb{F}_p$. Let α be in the equivalence class $A_\alpha \subseteq \mathbb{F}_p$ if α is the additive or multiplicative inverse of some element in A_α. For example, A_0 only has one element, namely 0, since it is its own additive inverse and it has no multiplicative inverse. Similarly, $A_1 = A_{-1} = \{1, -1\}$ since 1 and -1 are additive inverse and are respectively their own multiplicative inverse. Because of uniqueness of inverses, these equivalence classes fully partition $\mathbb{F}_p$. Let $\chi, -\chi$ be the only solutions to $x^2 + 1 = 0$ in $\mathbb{F}_p$. Then $A_\chi = \{\chi, -\chi\}$, since $\chi = -\chi^{-1}$. Note that 0 is the only element that is its own additive inverse, and 1, -1 are the only elements that are their own multiplicative inverse, since p is odd. Also, if some element x obeys $x = -x^{-1}$, it must be either χ or χ. Thus, every element α in $\mathbb{F}_p$ that is not 0, 1, -1, χ, or $-\chi$ obeys $|A_\alpha| = 4$.

We write the disjoint union $\mathbb{F}_p = A_0 \cup A_1 \cup A_\chi \cup A$ where A is just the union of the equivalence classes not accounted for in $A_0 \cup A_1 \cup A_\chi$. So $p = |A_0| + |A_1| + |A_\chi| + |A|$. Since $|A_\alpha| = 4$ for all α in A, 4 divides $|A|$. Thus, $p \equiv_4 (|A_0| + |A_1| + |A_\chi|) = (1 + 2 + 2) \equiv_4 1$. So for any odd prime p, if p is the sum of two squares, then $p \equiv_4 1$.

We must now show the only-if part, and we proceed by contraposition. Suppose p is not the sum of two squares. Thus, it is not the norm of any Gaussian integer. Note that for $p \in \mathbb{Z}[i]$, $|p| = p^2$. Thus, if p were not prime, and instead decomposed into non-unit Gaussian integers σ, τ, then $p^2 = |\sigma||\tau|$ would be impossible since p cannot be the norm of any Gaussian integer. We conclude that p is prime in $\mathbb{Z}[i]$. Now suppose that $x^2 + 1 = 0$ has a solution y in $\mathbb{F}_p$. Then p divides $y^2 + 1$. Thinking in terms of Gaussian

integers, $y^2 + 1 = (y + i)(y - i)$, and p must divide either $(y + i)$ or $(y - i)$ since it is prime. This is impossible though, since p is a real number and $(y + i)$, $(y - i)$ both have an imaginary component with magnitude 1. We now know that if p is not the sum of two squares, then $x^2 + 1 = 0$ has no solution in $\mathbb{F}_p$. Thus, there is no element χ in $\mathbb{F}_p$ such that $\chi = -\chi^{-1}$ and $|A_\alpha| = 4$ for all α other than 0, 1, and -1. Using the method from earlier, $p \equiv_4 (|A_0| + |A_1|) = (1 + 2) = 3$. So if p is not the sum of two squares, then it is not true that $p \equiv_4 1$.[4]

This result leads immediately to a fact about integer quaternions. If p is the sum of two squares, it is certainly also the sum of four squares, since $0^2 = 0$. Thus, any odd prime $p \equiv_4 1$ is the norm of some quaternion. To prove the much stronger theorem, that *any* natural number is the norm of some quaternion, requires more work.

Lemma 6.2 We prove that $x^2 + y^2 + 1 \equiv_p 0$, where p is any odd prime, has a solution. There are $\frac{p+1}{2}$ squares in $\mathbb{F}_p$, counting 0, since the square of any element is also the square of its additive inverse. Because of this, only half of the nonzero elements are squares. Since there are $\frac{p+1}{2}$ squares, there are also $\frac{p+1}{2}$ elements of the form $x^2 + 1$, and $\frac{p+1}{2}$ elements of the form $-y^2$. Now, the number of elements of either of these forms would be $\frac{p+1}{2} + \frac{p+1}{2} = p + 1$, which is more elements than fit in $\mathbb{F}_p$, unless at least one element could be represented in either form. Thus, $\exists \alpha \in \mathbb{F}_p$ such that $\alpha = x^2 + 1 = -y^2$ for some $x, y \in \mathbb{F}_p$. Thus, $x^2 + y^2 + 1 = 0$ has a solution in $\mathbb{F}_p$.

Theorem 6.3 For any odd prime p, there exists a quaternion with norm p. Since $x^2 + y^2 + 1 = 0$ has a solution in $\mathbb{F}_p$, the quaternion $q = 1 + ix + jy$ has a norm divisible by p. Say $|q| = np$. We know that p does not, however, divide q itself, since q has a trivial coefficient on the unity basis vector. Since $\mathbb{Z}(\mathbb{H})$ is a ring with unique factorization just like the Gaussian integers, q decomposes into prime quaternions $\alpha_1\alpha_2...\alpha_k$. Since $\mathbb{Z}(\mathbb{H})$ has a norm that obeys composition, $|\pi_1||\pi_2|...|\pi_k| = |q| = np$ and at least one of the π_i has norm p.

In the Gaussian integers, the only odd primes that were the norm of some element were those congruent to 1 (mod 4). Now, in the integer quaternions, *every* odd prime is the norm of some element. Also note that $2 = |1 + i|$ and

[4][D],p.42

so every prime is the norm of some quaternion. It immediately follows that *every natural number* is in fact the norm of a quaternion.

Theorem 6.4 Let $n \in \mathbb{N}$. Let n have prime factorization $n = 2^{r_0}p_1^{r_1}p_2^{r_2}\dots p_k^{r_k}$. Then each prime factor is the norm of some quaternion. Since $\mathbb{H}$ is a normed composition algebra and $\mathbb{Z}(\mathbb{H}) \leq \mathbb{H}$, the product of all the norms must itself be the norm of some quaternion. Thus, every natural number is the norm of an integer quaternion.[5]

This really is an amazing result. Every natural number is the norm of at least one element of $\mathbb{Z}(\mathbb{H})$. The natural next question to ask is, how many? At least one? Do the quaternion integers with norm n number, say, seven? Two million? In Davidoff et al, a proof is presented that the number of integer quaternions with norm n is equal to eight times the sum of the divisors of n.[6] Thus, $n = 1$ has eight integer quaternions for which it is the norm, namely $1, i, j, k, -1, -i, -j, -k$. Moving up to $n = 2$, there exist $8(2 + 1) = 24$ distinct integer quaternions. This is a much larger number than one might have expected prior to learning these theorems, but a quick inspection shows it to be true. The elements with norm 2 are

$$\pm(1 + i), \pm(1 + j), \pm(1 + k), \pm(i + j), \pm(i + k), \pm(j + k),$$

$$\pm(1 - i), \pm(1 - j), \pm(1 - k), \pm(i - j), \pm(i - k), \pm(j - k),$$

and so we see that this theorem really does work in this case. The quaternions are certainly not the useless parlor trick that Hamilton's decriers claimed them to be!

7 Quaternion Quantum Mechanics

When Hamilton first presented his idea to the mathematical community, it was regarded with not a small amount of derision. Many mathematicians were wary of the noncommutative nature of this new structure and thought that there must be something wrong with it. Nobody could tell what was wrong, and that just made them even more averse to the idea of accepting

[5] [D],p.57-67
[6] [D],p.52

quaternions as a legitimate mathematical structure. Group theory was not yet fully established, and the concept that operations can be noncommutative was hazy. If Hamilton were alive today, then, he would be overjoyed to see how his invention has permeated the scientific community. Quaternions are used in applied mathematics to an extent that would puzzle, if not infuriate Hamilton's rivals and naysayers from the pre-group theory era of mathematics.

According to the preface of John H. Conway's "On Quaternions and Octonions," quaternions have found abundant application in the technology of controlling spacecraft, and in the programming of video games. They also have applications in any sort of physics that involves rotations, for obvious reasons. Why use bulky matrices when quaternions work too?

Perhaps the most interesting application of quaternions is in the field of quantum mechanics. If we return to the section on quaternions in algebra, we find that $\mathbb{H}$ can be represented by 2×2 matrices with complex coefficients. Specifically, $\tilde{i} = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}$, $\tilde{j} = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$, and $\tilde{k} = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}$. We now compare these representations to the Pauli operators, three operators over a 2-dimensional Hilbert space $\mathcal{H}$ with representations $\mathbf{X} = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$, $\mathbf{Y} = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}$, and $\mathbf{Z} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$.[7]

Performing various matrix multiplications, we find that $\mathbf{XY} = i\mathbf{Z}$, $\mathbf{YZ} = i\mathbf{X}$, $\mathbf{ZX} = i\mathbf{Y}$, and these multiplications are all anticommutative, so $\mathbf{XY} = -\mathbf{YX}$, etc. This is strikingly reminiscent of the quaternions! In fact, if we look at $\tilde{i}, \tilde{j}, \tilde{k}$ above, we can write down three equalities.

$$i\tilde{i} = \mathbf{X}, i\tilde{j} = \mathbf{Y}, i\tilde{k} = \mathbf{Z}$$

Note that $\mathbf{XY} = i\tilde{i}i\tilde{j} = -\tilde{i}\tilde{j} = -\tilde{k} = i\mathbf{Z}$, just like it should be. Other operations follow similarly.

So the quaternions provide a straightforward way of combining Pauli matrices. Say we want to find the matrix associated with $\mathbf{M} = \mathbf{YXXZXYZYXY}$. One way would be to multiply ten matrices together. Another, much less

[7] [S]

mind-numbing way would be to use the quaternion representation.

$$\begin{aligned}
\mathbf{M} &= i\tilde{j}i\tilde{i}i\tilde{i}k\tilde{i}i\tilde{j}i\tilde{k}i\tilde{j}i\tilde{i}i\tilde{j} \\
&= i^{10}\tilde{j}\tilde{i}\tilde{i}\tilde{k}\tilde{i}\tilde{j}\tilde{k}\tilde{j}\tilde{i}\tilde{j} \\
&= -(-\tilde{k})(-\tilde{j})(\tilde{k})(-\tilde{i})(\tilde{k}) \\
&= -\tilde{i}\tilde{j}\tilde{k} \\
&= \mathbf{1}
\end{aligned}$$

Thanks to the quaternions, we now know that $\mathbf{YXXZXYZYXY}\,|\psi\rangle = |\psi\rangle$ for any $|\psi\rangle \in \mathcal{H}$.

The quaternions are useful in this way for representing various operators over Hilbert spaces, but they also have another quantum mechanical use. Typically in physics, we work over the complex numbers. The Schrödinger equation for example is $H\,|\psi\rangle = i\hbar\frac{d}{dt}\,|\psi\rangle$. Note the imaginary number i on the right side. But since $\mathbb{C}$, written as $\mathbb{C} \cong \text{span}\{1, j\}$, is a subalgebra of $\mathbb{H}$, we could just as easily do quantum mechanics over the quaternions. The Schrödinger equation would then be written $H\,|\psi\rangle = j\hbar\frac{d}{dt}\,|\psi\rangle$. We could also generalize the equation by using a general operator η such that $\eta^2 = \mathbf{-1}$ and $H\,|\psi\rangle = \hbar\eta\frac{d}{dt}\,|\psi\rangle$.[8] Note that despite being potentially quaternionic, we will see that η still commutes with H. This way, all the physics that falls out of the Schrödinger equation will still hold. This is a good thing, since essentially *all of physics* falls out of the Schrödinger equation. We would not want to contradict all of physics.

The advantage to using $\mathbb{H}$ instead of $\mathbb{C}$ in quantum mechanics is that since $\mathbb{C}$QM falls out of $\mathbb{H}$QM, we know that $\mathbb{H}$QM can only be better. Finkelstein et al detail a number of consequences of $\mathbb{H}$QM in the paper "Foundations of Quaternion Quantum Mechanics" in the Journal of Mathematical Physics, March-April, 1962. The scope of many of these consequences is well beyond this paper, but suffice it to say that, as in many circumstances, the general case of the system is the stronger one. Just like classical mechanics falls out of quantum mechanics, or out of relativity theory, complex quantum mechanics falls out of quaternion quantum mechanics.

There is one upshot of $\mathbb{H}$QM that we outline here. The operator η is just i in complex QM, but what do we know about it in quaternion QM? We rewrite the Scrödinger equation as $\frac{d}{dt}\,|\psi\rangle = -\eta H\,|\psi\rangle$. Now, we know from standard QM that the derivative applied to a state is an antihermitian

[8] [F]

operator. We thus know that there is some $G = -G^\dagger$ such that $\frac{d}{dt}|\psi\rangle = G|\psi\rangle$ and G must equal $-\eta H$. Taking the hermitian conjugate of this, $-G = H\eta$ and so H and η must commute.

Definition 7.1 Define the absolute value of an operator B by $|B| = (B^\dagger B)^{1/2}$.

What does this function do? We inspect the diagonal form of the operator, where it is written as the sum of its eigenvalues times their corresponding eigenvectors.

$$\begin{aligned}
|B| &= \left|\sum_k \lambda_k |k\rangle\langle k|\right| \\
&= \left(\left(\sum_j \lambda_j^* |j\rangle\langle j|\right)\left(\sum_k \lambda_k |k\rangle\langle k|\right)\right)^{1/2} \\
&= \left(\sum_k \lambda_k^*\lambda_k |k\rangle\langle k|\right)^{1/2} \\
&= \left(\sum_k |\lambda_k|^2 |k\rangle\langle k|\right)^{1/2} \\
&= \sum_k |\lambda_k| |k\rangle\langle k|
\end{aligned}$$

The absolute value function just finds the absolute value, in the sense we're used to, of the eigenvalues in the diagonal decomposition. Thanks to this form, we see that if two operators commute, that is if they can be thought of over each other's eigenbasis, then their absolute values commute.

We can now inspect the absolute value of $G = -\eta H$. Since η and G are antihermitian, H is hermitian, and η and H commute,

$$|G| = (G^\dagger G)^{1/2} = (H^\dagger(-\eta)^\dagger(-\eta)H)^{1/2} = (-\eta^2 H^2)^{1/2} = (|\eta|^2|H|^2)^{1/2}.$$

Now, since $|\eta|$ and $|H|$ commute, and $H = |H|$ because H is positive, this is $|G| = |\eta|H$. Also, since we defined $\eta^2 = \mathbf{-1}$, we know that $|\eta| = (\eta^\dagger\eta)^{1/2} = (-(-1))^{1/2} = 1$. So $H = |G|$. Now to find η in terms of G, note that $\eta^2 = \mathbf{-1}$ implies that $\eta^{-1} = -\eta$. Thus, $G = -\eta H = -\eta|G|$ implies that $\eta = |G|G^{-1}$. It is assumed in the paper that G has an inverse, so we leave it at that.

We now have η in terms of the differential operator G. It is no longer a mysterious quaternionic operator, provided we know G. Note that in

standard quantum mechanics, one definition of H is as iG. This clearly falls out of the quaternion case, setting $\eta = i$. The power of quaternion quantum mechanics is summed up in the abstract of Finkelstein et al: "This is the most general kind of quantum mechanics possessing the same kind of calculus of assertions as conventional quantum mechanics."[9] This generality is what makes $\mathbb{H}$QM, not only feasible, but perhaps even preferable in certain cases.

8 Conclusion

We have shown the applications of the quaternion algebra in representation theory, group theory, geometry, number theory, and quantum mechanics. Quaternions can represent rotations in 3-space, act as elements of a finite nonabelian group, determine square decompositions of any natural number, and generalize problems in quantum mechanics. They can provide a simple shortcut to finding a cross product, serve as a basis of 4-space, and are even equivalent to the quantum mechanically ubiquitous Pauli operators. Sir William Rowan Hamilton would be proud to know that the insight he had while walking across the Brougham Bridge would prove to be so fruitful for the generations to come.

[9] [F]

REFERENCES

[B] Baker, Andrew. Matrix Groups: An Introduction to Lie Group Theory. Great Britain: Springer, 2002.

[C] Conway, John H. and Derek A. Smith. On Quaternions and Octonions. Natick, MA: A K Peters, Ltd, 2003.

[D] Davidoff, Giuliana, Peter Sarnak, and Alain Valette. Elementary Number Theory, Group Theory, and Ramanujan Graphs. Cambridge: Cambridge University Press, 2003.

[F] Finkelstein, David, Josef M. Jauch, Samuel Schiminovich, and David Speiser. "Foundations of Quaternion Quantum Mechanics." Journal of Mathematical Physics 3.2 (March-April 1962): 207-220.

[L] Ledermann, Walter. Introduction to the Theory of Finite Groups. Edinburgh and London: Oliver and Boyd, 1961.

[S] Schumacher, Benjamin W. and Michael Westmoreland. Quantum Processes, Systems, and Information. Cambridge: Cambridge University Press, 2006.

"[T]hough beautifully ingenious, [quaternions] have been an unmixed evil to those who have touched them in any way..." – Lord Kelvin, 1892. (Quote taken from Wikipedia.org)