A Proof of the Skolem-Noether Theorem for Quaternions

Justin Paul Skycak

January 13, 2015

Abstract

After presenting a historical and abstract algebraic exposition of the quaternions, we prove the Skolem-Noether theorem for quaternions. We conclude with an application of the quaternions to number theory.

Introduction

We begin with a historical background of Hamilton's quaternions and a review of their defining properties. In this paper we show that the quaternions form an algebra, and we prove the Skolem-Noether theorem, for pure quaternions. We show that the result of the theorem gives physical meaning to automorphisms of pure quaternions. Lastly, we present an application of quaternions to number theory.

Hamilton's Discovery of the Quaternions

The quaternions were discovered by William Rowan Hamilton on October 16th, 1843 (Buchmann 2011). Having completed the Theory of Couplets, an algebraic representation of the complex numbers, in 1833, Hamilton set out to form the Theory of Triplets, an algebraic representation of vectors in three-dimensional space. Hamilton suspected that, just as the Theory of Couplets used vectors with a real unit 1 and single imaginary unit, denoted i, to analyze rotations in two dimensions, the Theory of Triplets would use vectors with the real unit and two imaginary units, denoted i and j, to analyze rotations in three dimensions (Buchmann 2011).

However, after ten years of unsuccessful pursuit, a flash of insight came to Hamilton as he strolled with his wife along the Royal Canal in Dublin. Hamilton realized that the tools for analyzing rotations in three dimensions were not themselves three-dimensional. Rather, they were quaternions, four dimensional vectors consisting of a real unit and three imaginary units denoted i, j, and k. Hamilton was so excited by his discovery that he carved the quaternion multiplication rule

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

for his four-dimensional algebra and described his experience by the words

> *"And here dawned on me the notion that we must admit, in some sense, a fourth dimension of space for the purpose of calculating with triples . . . An electric circuit seemed to close, and a spark flashed forth"*

in a letter to his colleague and friend John Graves the very next day (Shipmann). Hence, in honor of Hamilton, we will define $\mathbb{H} := \mathbb{R}^4$ to be the set of quaternions.

Hamilton defined the following binary operations on his quaternions:

Definition Define **real-quaternion multiplication** $\cdot_{RH} : \mathbb{R} \times \mathbb{H} \to \mathbb{H}$ and **quaternion-quaternion addition** $+_{HH} : \mathbb{H} \times \mathbb{H} \to \mathbb{H}$ component-wise as follows:

(i). if r is a real number and $q = (q_0, q_1, q_2, q_3)$ is a quaternion, then

$$r \cdot_{RH} q = (rq_0, rq_1, rq_2, rq_3)$$

(ii). If $q = (q_0, q_1, q_2, q_3)$ and $h = (h_0, h_1, h_2, h_3)$ are quaternions, then

$$q +_{HH} h = (q_0 + h_0, q_1 + h_1, q_2 + h_2, q_3 + h_3)$$

To formalize Hamilton's notation scheme, we define the real and imaginary quaternion units and spaces as follows:

Definition In $\mathbb{H}$, denote the real unit as $1' := (1, 0, 0, 0)$, and denote the imaginary units as $i := (0, 1, 0, 0), j := (0, 0, 1, 0)$, and $k := (0, 0, 0, 1)$.

(i). We denote the space of **real quaternions** $\mathbb{R}_H$ as the span of the real unit $1'$ over $\mathbb{R}$.

(ii). We denote the space of **imaginary quaternions** V^3 as the span of imaginary units i, j, k over $\mathbb{R}$.

Recalling Hamilton's rule for quaternion multiplication, we define:

Definition Quaternion-quaternion multiplication is the binary relation $\cdot_{HH} : \mathbb{H} \times \mathbb{H} \to \mathbb{H}$ such that

$$i \cdot_{HH} i = j \cdot_{HH} j = k \cdot_{HH} = i \cdot_{HH} j \cdot_{HH} k = -1'$$

Hamilton's rule for quaternion-quaternion multiplication is a compact way of describing the following table:

$\cdot_{HH}$	$1'$	i	j	k
$1'$	$1'$	i	j	k
i	i	$-1'$	k	$-j$
j	i	$-k$	$-1'$	i
k	k	j	$-i$	$-1'$

To ease notation, we will use the symbol $(\cdot)$ or omit the symbol when we use real-real multiplication, real-quaternion multiplication, and quaternion-quaternion multiplication. Similarly, we will denote both real-real addition and quaternion-quaternion addition by a single symbol $(+)$. In both cases, the intended operation should be clear given the context in which it appears.

Algebra as an Abstract Structure

Before we show that the quaternions comprise an algebra, we need to explain what an algebra is. We will now review some basic abstract algebra that will lead us to the definition of an algebra. We begin with the definitions of monoids and groups.

Definition A **monoid** $N' := (N, \cdot_N)$ is a nonempty set N equipped with a binary operation $(\cdot_N) : N \times N \to N$, called multiplication, such that:

(i). multiplication is closed and associative in N, and

(ii). N contains an identity element 1 such that $n \cdot_N 1 = 1 \cdot_N n = n$ for every $n \in N$.

Definition A **group** $G' := (G, \cdot_G)$ is a nonempty set G equipped with multiplication $(\cdot_G) : G \times G \to G$ such that:

(i). G' is a monoid, and

(ii). every element $g \in G$ has an inverse element $g^{-1} \in G$ such that $g \cdot_G g^{-1} = g^{-1} \cdot_G g = 1$.

We define an **additive group** in the same way as above, except that we replace multiplication $(\cdot_G)$ by addition $(+_G)$, 1 by 0, and g^{-1} by $-g$. The difference between a multiplicative group and an additive group is purely notational.

We now use our definitions of monoids and groups to define a ring.

Definition A **ring** $R' := (R, \cdot_R, +_R)$ is a nonempty set R equipped with multiplication $(\cdot_R) : R \times R \to R$ and addition $(+_R) : R \times R \to R$ such that:

(i). $(R, \cdot_R)$ is a monoid,

(ii). $(R, +_R)$ is an Abelian additive group, and

(iii). multiplication distributes over addition.

We say that R' is a **division ring** if $(R, \cdot_R)$ is a group, and we say that R' is a **commutative ring** if $(R, \cdot_R)$ is an Abelian group.

Finally, we use the three previous definitions to define an algebra over a ring, or an R-algebra.

Definition An **R-algebra** $A' := (G', R', \cdot_{RG}, \cdot_A)$ is an Abelian additive group G', whose elements are called *vectors*, together with a division ring R', whose elements are called *scalars*, and two binary relations $(\cdot_{RG}) : R \times G \to G$, called scalar-vector multiplication, and $(\cdot_A) : G \to G$, called vector-vector multiplication, such that:

(i). scalar-vector multiplication distributes over vector-vector addition.

(ii). vector-vector multiplication is bilinear

An algebra is an **associative algebra** if vector-vector multiplication is associative.

The Quaternion Algebra

We wish to prove that $A_H := (\mathbb{H}, \mathbb{R}, \cdot, +)$ is an $\mathbb{R}$-algebra. We will do this by constructing a simpler $\mathbb{R}$-algebra called $M_2(\mathbb{C})$ and then finding an isomorphism from A_H to $M_2(\mathbb{C})$.

Definition Define $\mathscr{H}$ to be the span over $\mathbb{R}$ of linearly independent matrices $M_{1'} = \begin{bmatrix} 1' & 0 \\ 0 & 1' \end{bmatrix}$, $M_i = \begin{bmatrix} i & 0 \\ 0 & -i \end{bmatrix}$, $M_j = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}$, and $M_k = \begin{bmatrix} 0 & -i \\ -i & 0 \end{bmatrix}$ so that, under normal matrix multiplication, $M_i^2 = M_j^2 = M_k^2 = M_i M_j M_k = -M_{1'}$. Let $M_2(\mathbb{C}) = (\mathscr{H}, \mathbb{R}, \cdot, +)$, where $(\cdot)$ denotes normal matrix or real-matrix multiplication and $(+)$ denotes normal matrix addition.

Matrix addition is closed in $\mathscr{H}$, and it is always associative. The zero matrix is the identity element in $\mathscr{H}$. Thus, $(\mathscr{H}, +)$ is a monoid. Furthermore, We know that $(\mathbb{R}, \cdot, +)$ is a field, so it is also a division ring. Also, we know that scalar-matrix multiplication distributes over matrix-matrix addition. Lastly, we know that matrix-matrix multiplication is $\mathbb{R}$ bilinear. Thus, we have that:

Proposition 1. *$M_2(\mathbb{C})$ is an $\mathbb{R}$-algebra.*

We can use this fact to prove the following theorem:

Theorem 2. *A_H is an $\mathbb{R}$-algebra.*

Proof. Let $T : \mathbb{H} \to \mathscr{H}$ be the transformation defined by $T(q) = M_q$ for $q \in \{1', i, j, k\}$. We see that $T(qh) = TqTh$ whenever $q, h \in \{1', i, j, k\}$. But because $M_2(\mathbb{C})$ is $\mathbb{R}$-bilinear, $T(qh) = TqTh$ for any quaternions $q, h \in \mathbb{H}$. Furthermore, since T maps the basis $\{1', i, j, k\}$ to the basis $\{M_{1'}, M_i, M_j, M_k\}$, it is bijective, so T is an isomorphism. Thus, A_H is an $\mathbb{R}$-algebra as well. $\square$

The Skolem-Noether Theorem

The Skolem-Noether Theorem tells about homomorphisms of central simple algebras, so we must first define a central simple algebra and a homomorphism.

Definition A **right ideal** of an algebra A' is a subspace I_R of A' such that $r \cdot_A a \in I_R$ for every $a \in A$ and $r \in I_R$. Similarly, a **left ideal** of an algebra A' is a subspace I_L of A' such that $a \cdot_A \ell \in I_L$ for every $a \in A$ and $\ell \in I_L$. An ideal I is a **two-sided ideal** if it is both a right ideal and a left ideal.

In other words, each element of a two-sided ideal commutes with every element in the algebra. The definition of a simple algebra is a characterization of an algebra's two-sided ideals:

Definition An algebra A' is **simple** if it has no two-sided ideals other than $\{0\}$ and possibly A'.

Note that real quaternions and the zero quaternions are the only quaternions that commute with all other quaternions. Thus, $A_{V^3} := (V^3, \mathbb{R}, \cdot, +)$ is a simple algebra.

The largest two-sided ideal of an algebra is its center. More precisely,

Definition The **center** of an R-algebra A' is the set of all elements $c \in R$ that commute with every element $a \in A$. A simple R-algebra is **central** if its center is R.

Every element of $\mathbb{R}$ commutes with every quaternion. Hence, A_{V^3} is a central simple algebra.

The Skolem-Noether Theorem tells us about homomorphisms of central simple algebras, so we will define a homomorphism between two algebras:

Definition Let S and C be algebras over a ring R. A **homomorphism** from S to C is a bijective linear transformation $T : S \to C$ such that $T(pq) = T(p)T(q)$ for each $p, q \in \mathbb{S}$.

Homomorphisms preserve algebraic structure. In particular,

Proposition 3. *Let S and C be algebras, and let $T : S \to C$ be a homomorphism. Then*

(i) $T(1_S) = 1_C$.
(ii) $T(s^{-1}) = T(s)^{-1}$ for each $s \in S$.

Proof. Using the definition of a homomorphism, $T(1_S) = T(1_S \cdot 1_S) = T(1_S)T(1_S)$. Then we must have that (i) $T(1_S) = 1_C$. Thus, for each $s \in S$, we have that $1_C = T(1_S) = T(ss^{-1}) = T(s)T(s^{-1})$, so we must have that (ii) $T(s^{-1}) = T(s)^{-1}$. □

The Skokem-Noether Theorem is:

Theorem 4. ***(Skolem-Noether Theorem)*** *Let S and C be finite-dimensional algebras with S a simple algebra and C a central simple algebra. If f and g are homomorphisms $S \to C$, then there is an element $c \in C$ such that $g(s) = c^{-1}f(s)c$ for each $s \in S$.*

Skolem-Noether Theorem for Inner Automorphisms of Pure Quaternions

In the case that S and C of the Skolem-Noether Theorem are actually the same algebra A, the Skolem-Noether Theorem simplifies to a theorem about homomorphisms from A to itself, also known as automorphisms. We are interested in a particular kind of automorphism: an inner automorphism.

Proposition 5. *Fix $q \in V^3 - \{0\}$, and define $T_q : \mathbb{H} \to \mathbb{H}$ by the rule $T_q(x) = qxq^{-1}$. We call T_q an **inner automorphism** and verify that it is indeed an automorphism.*

Proof. First, we prove that T_q is linear. Let $x \in \mathbb{H}$ and $r \in \mathbb{R}$. Then $T_q(rx) = qrxq^{-1} = rqxq^{-1} = rT_q(x)$. Additionally, let $y \in \mathbb{H}$. Then $T_q(x+y) = q(x+y)q^{-1} = (qx+qy)q^{-1} = qxq^{-1} + qyq^{-1} = T_q(x) + T_q(y)$. Therefore, T_q is linear.

Next, we prove that T_q is bijective. This is proved if we show that $T_q^{-1} = T_{q^{-1}}$. Let $x \in \mathbb{H}$. Then $T_{q^{-1}}(T_q(x)) = q^{-1}(T_q(x))q = q^{-1}qxq^{-1}q = x$. Therefore, $T_q^{-1} = T_{q^{-1}}$.

Lastly, we prove that for each $p, q \in \mathbb{H}$, we have $T(pq) = T(p)T(q)$. Let $x, y \in \mathbb{H}$. Then $T_q(x, y) = qxq^{-1}qyq^{-1} = qxyq^{-1} = T_qxy$. □

We will prove the special case of the Skolem-Noether Theorem for inner automorphisms of the quaternion algebra:

Theorem 6. ***(Skolem-Noether Theorem for Inner Automorphisms)**. Every automorphism $T : V^3 \to V^3$ of the pure quaternion algebra is an inner automorphism. That is, for every $u \in V^3$, there is another quaternion $v \in V^3 - \{0\}$ such that $T(u) = v^{-1}uv$.*

Our proof strategy is as follows: first, we will show that each pure unit quaternion $\hat{v}$ in the unit sphere S^2 of pure quaternions satisfies $\hat{v}^2 = 1$. We will show that every automorphism T of the quaternions satsifies $T(S^2) = S^2$, and that T has a fixed point u. After showing that T preserves norms of quaternions and angles between pure unit quaternions and u, we will see that T is a rotation of unit quaternions about an axis u. It will follow that T rotates V^3 about u. Lastly, we will show that rotations can be written as inner automorphisms.

To show that each pure unit quaternion $\hat{v}$ in the unit sphere satisfies $\hat{v}^2 = -1$, we must first introduce the quaternion norm and the quaternion conjugate.

Lemma 7. *The **quaternion norm**, defined by $||q|| = \sqrt{q_1^2 + q_2^2 + q_3^2 + q_4^2}$ for each quaternion $q = (q_0, q_1, q_2, q_3)$, satisfies $||qh|| = ||q||||h||$ for every $q, h \in \mathbb{H}$.*

Proof. Using the quaternion product, we know that $qh = (q_oh_0 - q_1h_1 - q_2h_2 - q_3h_3) + (q_0h_1 + q_1h_0 + q_2h_3 - q_3h_2)i + (q_0h_2 + q_2h_0 + q_3h_1 - q_1h_3)j + (q_0h_3 + q_3h_0 + q_1h_2 - q_2h_1)k$. It is straightforward to verify that $||qh|| = ||q||||h||$. □

Lemma 8. *Define **conjugate** of a quaternion $q = r + v$, where r is a real quaternion and v is a pure quaternion, as $\overline{q} = r - v$. The quaternion conjugate satisfies $q\overline{q} = ||q||^2$.*

Proof. Multiplying, we have $q\overline{q} = (r+v)(r-v) = r^2 - v^2$. But $v^2 = -v_1^2 - v_2^2 - v_3^2 + (v_2v_3 - v_3v_2)i + (v_3v_1 - v_1v_3)j + (v_1v_2 - v_2v_1)k = -(v_1^2 + v_2^2 + v_3^2)$. Then $q\overline{q} = r^2 + v_1^2 + v_2^2 + v_3^2 = ||q||^2$. □

Lemma 9. *If v, w are pure quaternions, then $vw = -(v \cdot w) + (v \times w)$.*

Proof. Because the quaternion product is $\mathbb{R}$-bilinear, we need only verify the lemma for the imaginary units i, j, k. □

We use the previous three lemmas to prove the following proposition:

Proposition 10. *The unit sphere $S^2 = \{\vec{v} \in V^3 : ||\vec{v}|| = 1\}$ is precisely the set of quaternions $Q = \{q \in \mathbb{H} : q^2 = -1'\}$.*

Proof. We first prove that $Q \subset S^2$. Suppose that $q \in Q$. Then by Lemma 7 we have $||q||^2 = ||q^2|| = ||-1'|| = 1$, so $||q|| = 1$. Furthermore, since $1' = -q^2 = q(-q)$, we have by Lemma 8 that $-q = q^{-1} = \frac{\overline{q}}{||q||^2} = \overline{q}$, so q is pure. Therefore, because q is pure and $||q|| = 1$, we have $q \in S^2$.

Now, we prove that $S^2 \subset Q$. Conversely, suppose that $\hat{v} \in S^2$. Then $\hat{q}$ is pure and $||\hat{v}|| = 1$, so by Lemma 9, $\hat{v}^2 = -(\hat{v} \cdot \hat{v}) + (\hat{v} \times \hat{v}) = -||\hat{v}||^2 = -1$. Therefore, $\hat{v} \in Q$. □

Now we can prove that every automorphism of the quaternion algebra sends S^2 to S^2.

Proposition 11. *If $T : \mathbb{H} \to \mathbb{H}$ is an automorphism of the quaternion algebra, then $T(S^2) = S^2$.*

Proof. Let $\hat{v} \in S^2$. From the previous proposition we know that $\hat{v}^2 = -1$, so $\hat{v}^{-1} = -\hat{v}$. Then $T(\hat{v})^{-1} = T(\hat{v}^{-1}) = T(-\hat{v}) = -T(\hat{v})$, so $T(\hat{v})^{-1} = -T(\hat{v})$. This means $T(\hat{v})^2 = T(\hat{v}) \cdot -T(\hat{v})^{-1} = -1$‘, so $||T(\hat{v})||^2 = 1$. Thus $T(\hat{v}) \in Q = S^2$. □

Our next step is to prove that every automorphism of pure quaternions preserves norms of quaternions and angles between quaternions. First, we'll prove that every automorphism of pure quaternions preserves norms.

Lemma 12. *Let $T : \mathbb{H} \to \mathbb{H}$ be an automorphism. Then for every quaternion q, we have that $T(\overline{q}) = \overline{T(q)}$.*

Proof. Let $q = r + v$ be a quaternion with $r \in \mathbb{R}$ and $v \in V^3$. We have that $\overline{T(q)} = \overline{T(r+v)} = \overline{T(r) + T(v)}$. But $T(r) \in \mathbb{R}$ and $T(v) \in \mathbb{V}^{\not\in}$, so $\overline{T(r) + T(v)} = T(r) - T(v) = T(r - v) = T(\overline{q})$. That is, $\overline{T(q)} = T(\overline{q})$. □

Proposition 13. *Suppose that $T : \mathbb{H} \to \mathbb{H}$ is an automorphism. Then for every nonzero quaternion q, we have that $||Tq|| = ||q||$.*

Proof. Because $T(q^{-1}) = T(q)^{-1}$, we know $\frac{T(\overline{q})}{||q||^2} = \frac{\overline{T(q)}}{||T(q)||^2}$. But $T(\overline{q}) = \overline{T(q)}$, so we must have $||T(q)|| = ||q||$. □

Proposition 14. *If u, v are pure quaternions, and $T : V^3 \to V^3$ is an automorphism, then $T(u \cdot v) = Tu \cdot Tv$ and $T(u \times v) = Tu \times Tv$, where $(\cdot)$ is the vector dot product and $(\times)$ is the vector cross product.*

Now, we'll prove that every automorphism of pure quaternions preserves angles between quaternions.

Proof. Using Lemma 7, $-T(u \cdot v) + T(u \times v) = T(uv)$. We know that $T(uv) = TuTv$ and Tu, Tv are both pure quaternions, so $-T(u \cdot v) + T(u \times v) = -(Tu \cdot Tv) + (Tu \times Tv)$. But $-T(u \cdot v)$ and $-(Tu \cdot Tv)$ are both real quaternions while $T(u \times v)$ and $Tu \times Tv$ are both pure quaternions, so we must have $T(u \cdot v) = Tu \cdot Tv$ and $T(u \times v) = Tu \times Tv$. □

By finding a fixed point of T, we find the axis of rotation for T. We proceed with the proof of the fixed point.

Proposition 15. *If $T : S^2 \to S^2$ is an automorphism, then it has a fixed point. That is, there is a $z \in S^2$ such that $Tz = z$.*

Proof. Let $\{u, v, w\}$ be a right-handed orthonormal basis of pure quaternions, and let $Tu = (a_{11}, a_{21}, a_{31})$, $Tv = (a_{12}, a_{22}, a_{32})$, and $Tw = (a_{13}, a_{23}, a_{33})$ so that A is matrix of T relative to this basis. Using the vector triple product, we have that $\det A^T = Tu \cdot Tv \times Tw = Tu \cdot T(v \times w) = Tu \cdot Tu = T(u \cdot u) = T(||u||^2) = T(1) = 1$. Thus, the product of the eigenvalues of A is 1.

However, we know that the eigenvalues are the roots of the equation $0 = \det A - \lambda I$, so any complex eigenvalues come in conjugate pairs. Thus, at least one of the eigenvalues is 1. The eigenvector z corresponding to this eigenvalue satisfies $Tz = z$ and is thus a fixed point of T. □

Hence, every automorphism of pure unit quaternions is a rotation of pure unit quaternions about a fixed axis. We will generalize this finding for unit pure quaternions to all pure quaternions:

Proposition 16. *Every automorphism $T : V^3 \to V^3$ is a rotation of V^3 about a fixed axis z.*

Proof. We know that every automorphism $T : S^2 \to S^2$ is a rotation of S^2 about a fixed axis z. Every pure quaternion v can be written as $v = ||v||\hat{v}$, a scalar multiple of a pure unit quaternion. Then $T(v) = T(||v||\hat{v}) = ||v||T(\hat{v})$. But $T(\hat{v})$ is a rotation of $\hat{v}$ about a fixed axis z, and $||v||T(\hat{v})$ has the same direction as $T(\hat{v})$. □

It remains to show that every automorphism that rotates quaternions about a fixed axis can be written as an inner automorphism.

Proposition 17. *Let q be a unit quaternion given by $q = c + su$, where $u \in S^2$, $c = \cos\theta$, and $s = \sin\theta$ with $\theta \in [0, \pi]$. Then $T_q : V^3 \to V^3$, as defined previously, is the rotation about the axis u through 2θ radians counterclockwise.*

Proof. We must show that (i) $T_q u = u$, and also that whenever $||v|| = 1$ and $v \in u^\perp$, we have (ii) $T_q v = \cos 2\theta v + \sin 2\theta w$ and (iii) $T_q w = -\sin 2\theta v + \cos 2\theta w$ where $w = u \times v$. Note that because $||q|| = 1$ we have $q^{-1} = \overline{q}$, so $T_q(x) = qxq^{-1} = qx\overline{q}$.

(i). $T_q u = (s + cu)u(c - su) = c^2u - csu^2 + scu^2 - s^2u^3 = c^2u - s^2u^3$. But $u^2 = -1$, so $T_q u = (c^2 + s^2)u = u$.

(ii). $T_q v = (c+su)v(c-su) = c^2v - csvu + scuv - s^2uvu$. But $u \perp v$, so $uvu = (u \times v)u = wu = wxu$. But the right hand rule tells us $w \times u = v$, so $uvu = v$. Then we have $T_q v = (c^2 - s^2)v - csvu + scuv$. But $vu = v \times u = -u \times v = -w$, so $T_q v = (c^2 - s^2)v + 2csw = \cos 2\theta v + \sin 2\theta w$.

(iii). $T_q w = T_q u T_q v = u(\cos 2\theta + \sin 2\theta w) = \cos 2\theta w - \sin 2\theta v$ by the right hand rules. □

Finally, we prove Theorem 6.

Proof. (Theorem 6) Proposition 16 tells us that every automorphism $T : V^3 \to V^3$ is a rotation of V^3 about a fixed axis z. However, by Proposition 17, any fixed-axis rotation can be represented by an inner automorphism $T_q : V^3 \to V^3$ defined by $T_q(x) = qxq^{-1}$. Thus, every automorphism of the pure quaternion algebra can be written as an inner automorphism. □

The Hurwitz Quaternions: An Application of Quaternions to Number Theory

We are going to use quaternions to prove that for every prime number p, some multiple of p can be written as the sum of 1 and the square of two integers. To do this, we turn to the Hurwitz quaternions.

Definition We define the **Hurwitz quaternions** to be the set $\mathbb{A} = \{a + bi + cj + dk : a, b, c, d \in \mathbb{Z} \text{ or } a, b, c, d \in \mathbb{Z} + 1/2\}$.

The Hurwitz quaternions are useful because the balls of radius $\frac{1}{2}$ around all Hurwitz quaternions cover $\mathbb{H}$ entirely. More precisely,

Proposition 18. *For any quaternion q, there is a Hurwitz quaternion $a \in \mathbb{A}$ such that $||q - a|| < 1$.*

Proof. Since $||(\frac{1}{2}, \frac{1}{2}, \frac{1}{2}, \frac{1}{2})|| = 1$, every Hurwitz quaternion is within 1 unit of another Hurwitz quaternion. □

Furthermore,

Proposition 19. *The Hurwitz quaternions form a ring.*

Proof. It is easy to see that the Hurwitz quaternions are closed under addition, so we will turn to multiplication. Noting that Hurwitz quaternions are precisely those that are sums of integer multiples of $\frac{1'+i+j+k}{2}$, i, j, k, we consider the product

$$\left[A\left(\tfrac{1'+i+j+k}{2}\right)+Bi+Cj+Dk\right]\left[A'\left(\tfrac{1'+i+j+k}{2}\right)+B'i+C'j+D'k\right],$$

where $A, A', B, B', C, C', D, D'$ are all integers. After algebraic manipulation, the product simplifies to

$$\begin{aligned}
&-\left(BB'+CC'+DD'+\tfrac{AB'+BA'}{2}+\tfrac{AC'+CA'}{2}+\tfrac{AD'+DA'}{2}+\tfrac{1}{2}\right)1'\\
&+\left(CD'-DC'+\tfrac{AB'+BA'}{2}+\tfrac{AC'+CA'}{2}+\tfrac{AD'+DA'}{2}+\tfrac{1}{2}\right)i\\
&+\left(DB'-BD'-\tfrac{AB'+BA'}{2}+\tfrac{AC'+CA'}{2}-\tfrac{AD'+DA'}{2}+\tfrac{1}{2}\right)j\\
&+\left(BC'-CB'+\tfrac{AB'+BA'}{2}-\tfrac{AC'+CA'}{2}+\tfrac{AD'+DA'}{2}+\tfrac{1}{2}\right)k.
\end{aligned}$$

- If each of $\{\frac{AB'+BA'}{2}, \frac{AC'+CA'}{2}, \frac{AD'+DA'}{2}\}$ is in $\mathbb{Z}$, then the product is a Hurwitz quaternion whose entries are all in $\mathbb{Z}$.
- If two of $\{\frac{AB'+BA'}{2}, \frac{AC'+CA'}{2}, \frac{AD'+DA'}{2}\}$ are in $\mathbb{Z}$ and the other is in $\mathbb{Z}+\frac{1}{2}$, then the product is a Hurwitz quaternion whose entries are all in $\mathbb{Z}+\frac{1}{2}$.
- If one of $\{\frac{AB'+BA'}{2}, \frac{AC'+CA'}{2}, \frac{AD'+DA'}{2}\}$ is in $\mathbb{Z}$ and the other two are in $\mathbb{Z}+\frac{1}{2}$, then the product is Hurwitz quaternion whose entries are all in $\mathbb{Z}$.
- If each of $\{\frac{AB'+BA'}{2}, \frac{AC'+CA'}{2}, \frac{AD'+DA'}{2}\}$ is in $\mathbb{Z}+\frac{1}{2}$, then the product is a Hurwitz quaternion whose entries are all in $\mathbb{Z}+\frac{1}{2}$.

Lastly, the additive $(0,0,0,0)$ and multiplicative $(1,0,0,0)$ identity quaternions are both Hurwitz quaternions, and, given any Hurwitz quaternion q, its multiplicative inverse $\frac{\overline{q}}{||q||}$ is a Hurwitz quaternion. □

The coming proof makes use of the following lemma.

Lemma 20. *Given $q \in \mathbb{A}$ and $d \in \mathbb{A}^*$, there exist $a, r \in \mathbb{A}$ so that $||q - da|| < ||d||$.*

Proof. It was previously shown that for every $q' \in \mathbb{H}$, there is an $a \in \mathbb{A}$ such that $||q' - a|| < 1$. Choose $q' = d^{-1}q$. Then $||d^{-1}q - a|| < 1$, so $||q - da|| < ||d||$. □

Now we present an application of quaternions to number theory.

Theorem 21. *Suppose p is a prime number. Then there are integers m, n such that $m^2+n^2+1 \equiv 0 \mod p$.*

Proof. When $p = 2$, we see that $0^2 + 1^2 + 1 = 0 \mod p$. Every even number that is greater than 2 is not prime, so we can assume that p is odd. Let $S = \{0, 1, 2, ..., \frac{p-1}{2}\}$, and let $S' = \{[x^2] : x \in S\}$, where $[x^2]$ refers to the equivalence class of $x^2 \mod p$. Note that $|S'| = |S| = \frac{p+1}{2}$. Let $S'' = \{-1 - [x^2] : x \in S\}$. Note that $|S'| = |S|$, so $|S''| = \frac{p+1}{2}$. Then $|S'| + |S''| = p + 1$. But there are only p equivalence classes modulo p, so S' and S'' overlap by a single element. That is to say, there are integers m, n such that $m^2 \equiv -1 - n^2 \mod p$, or equivalently, $m^2 + n^2 + 1 \equiv 0 \mod p$. □

Further Applications of Quaternions

I'm looking for another straightforward yet interesting application of quaternions to include here.

Conclusion

Acknowledgements

References

Buchmann, A.: A Brief History of Quaternions and of the Theory of Holomorphic Functions of Quaternionic Variables. *arXiv:1111.6088* (2011).

Shipmann, B.: Historical Pathway: Hamilton's Quaternions. *Active Learning Materials for a First Course in Real Analysis.*