International Mathematical Forum, Vol. 7, 2012, no. 43, 2143 - 2156

Factorization of Hurwitz Quaternions

Boyd Coan and Cherng-tiao Perng *

Department of Mathematics
Norfolk State University
700 Park Avenue, Norfolk, VA 23504, USA
bcoan@nsu.edu, ctperng@nsu.edu

Abstract

This is an exposition on Hurwitz quaternions. We first introduce Hurwitz quaternions and show the existence of (one-sided) division algorithm. Using the language of Hurwitz quaternions, we prove Lagrange's Theorem of Four Squares. After that we move on to establish the theory of factorization of Hurwitz quaternions. More precisely we give a detailed explanation on the "unique factorization of Hurwitz quaternions" proposed by Conway and Smith, namely any non-unit Hurwitz quaternion can be factored uniquely, up to a series of *unit-migrations*, *meta-commutations*, and *re-combinations*.

Mathematics Subject Classification: 11A05, 11A51, 16U30

Keywords: Hurwitz quaternions, unique factorization, Lagrange's theorem of four squares

1 Introduction

The investigations done in this note started from reading a proof circulated on the internet regarding Lagrange's Theorem of Four Squares using the "unique factorization" of Hurwitz quaternions. Of course, we know by simple example that there is no uniqueness in the usual sense of factorization. When we did closer investigation on the factorization, we developed some skills, which, albeit elementary, serve to clarify the structure of factorization. Many of these were done before reading Hurwitz's original paper ([3]) and Conway and Smith ([1]). To our knowledge, Hurwitz's presentation of quaternions already contained very detailed analysis of the structure of the factorizations. As far as we know, the concept of "unique factorization of Hurwitz quaternions" was first proposed by Conway and Smith in [1]. This reference contains a chapter describing

*corresponding author, ctperng@nsu.edu

the division algorithm of Hurwitz quaternions and introducing the concepts of unit-migration, meta-commutation, and recombination. Even though most arguments there are clear, some of the remarks are only sketched. Accordingly, we feel that supplying the details is not a bad idea, at least pedagogically. For the purpose of this note which is meant to be as self-contained as possible, there are a few goals we want to achieve. First of all, we will give a proof of Lagrange's Theorem of Four Squares, based on the existence of division algorithm for Hurwitz quaternions. From this, we are led to the factorization of Hurwitz quaternions. We will supply details for the "unique factorization of Hurwitz quaternions" as in the layout given by Conway and Smith.

2 Preliminary Notes

Definition 2.1 *Let $\mathbb{H}(\mathbb{R})$ be the quaternions over the reals. For $q = a + bi + cj + dk \in \mathbb{H}(\mathbb{R})$, we define the conjugate $\bar{q}$ by $\bar{q} = a - bi - cj - dk$. Furthermore, we define norm and trace by the following formulas:*

$$\mathrm{Nm}(q) = q\bar{q} = a^2 + b^2 + c^2 + d^2 \qquad \mathrm{Tr}(a) = q + \bar{q} = 2a.$$

We write $\mathbb{H}(\mathbb{Z})$ for the subring of $\mathbb{H}(\mathbb{R})$ consisting of quaternions with integer components.

More precisely, $\mathbb{H}(\mathbb{R})$ is a ring consisting of elements q of the form $q = a + bi + cj + dk$, where $a, b, c, d \in \mathbb{R}$. Addition is componentwise. For multiplication, we prescribe $\mathbb{R}$ to be the center of $\mathbb{H}(\mathbb{R})$, and the multiplication of the basis elements follows the rules: $i^2 = j^2 = k^2 = -1$ and $ij = -ji = k$ (and hence $jk = -kj = i$, etc.) It can be checked easily that the rule of multiplication is associative.

It is easy to check that

$$\overline{q_1 q_2} = \bar{q}_2 \bar{q}_1$$

and it follows that

$$\mathrm{Nm}(q_1 q_2) = \mathrm{Nm}(q_1) \cdot \mathrm{Nm}(q_2).$$

Definition 2.2 *The set of Hurwitz quaternions $\mathbb{A}$ is a subset of quaternions over half integers, defined as*

$$\mathbb{A} = \left\{ \frac{a + bi + cj + dk}{2} \mid a \equiv b \equiv c \equiv d \pmod 2 \right\}.$$

We say that q is a unit in $\mathbb{A}$ if q is invertible in $\mathbb{A}$, i.e. $\exists q' \in \mathbb{A}$ such that $qq' = q'q = 1$.

To see that $\mathbb{A}$ is a subring of $\mathbb{H}(\mathbb{R})$, it suffices to see that it consists of two cosets under addition, namely $\mathbb{A} = \mathbb{H}(\mathbb{Z}) \sqcup (\mathbb{H}(\mathbb{Z}) + \frac{1+i+j+k}{2})$. Since $\mathbb{A}$ is obviously a (two-sided) $\mathbb{H}(\mathbb{Z})$-module, it is an $\mathbb{A}$-module because $\frac{1+i+j+k}{2} \cdot q \in \mathbb{A}$, for any $q \in \mathbb{A}$: For example, if $q \in \mathbb{A} \setminus \mathbb{H}(\mathbb{Z})$, we may write $q = q_0 + \frac{1-i-j-k}{2}$, where $q_0 \in \mathbb{H}(\mathbb{Z})$. Then $\frac{1+i+j+k}{2} \cdot q = \frac{1+i+j+k}{2} \cdot q_0 + 1 \in \mathbb{A}$.

One verifies directly that $\mathrm{Nm}(q) \in \mathbb{Z}_{\geq 0}$, and $\mathrm{Tr}(q) \in \mathbb{Z}$ for any $q \in \mathbb{A}$. And furthermore, $q \in \mathbb{A}$ is a unit if and only if $\mathrm{Nm}(q) = 1$. It follows that there are precisely 24 units in $\mathbb{A}$:

$$\pm 1, \pm i, \pm j, \pm k, \frac{\pm 1 \pm i \pm j \pm k}{2}.$$

Proposition 2.3 *Considered as left-module (resp. right-module), the ring* $\mathbb{A}$ *has division algorithm with respect to the norm* Nm*: For any nonzero* $a, b \in \mathbb{A}$*, there exist* q *and* r *in* $\mathbb{A}$ *such that*

$$a = qb + r, \text{ where } \mathrm{Nm}(r) < \mathrm{Nm}(b)$$

$$(\text{resp. } a = bq + r, \text{ where } \mathrm{Nm}(r) < \mathrm{Nm}(b)).$$

Proof. Since we will be concerned with left module (or left ideals), we prove the case for left module. The proof for right module is similar.

Given $a, b \in \mathbb{A}$, consider ab^{-1}; approximate ab^{-1} by $q \in \mathbb{H}(\mathbb{Z})$ so that each component of $ab^{-1} - q$ has absolute value less than or equal to $\frac{1}{2}$. Letting $r' = ab^{-1} - q$, we have $\mathrm{Nm}(r') \leq \frac{1}{4} + \frac{1}{4} + \frac{1}{4} + \frac{1}{4} = 1$.

Case 1. If $\mathrm{Nm}(r') < 1$, then multiplying the above equation from the right by b, we have $a = qb + r$, where $r = r'b$ satisfies $\mathrm{Nm}(r) = \mathrm{Nm}(r')\mathrm{Nm}(b) < \mathrm{Nm}(b)$. So we are done in this case.

Case 2. If $\mathrm{Nm}(r') = 1$, then each of the components of r' has absolute value $\frac{1}{2}$, therefore r' is one of the 16 units with denominator 2. By definition of $\mathbb{A}$, $q' = q + r' \in \mathbb{A}$. Hence $ab^{-1} = q + r' = q' \Rightarrow a = q'b + 0$. Clearly $\mathrm{Nm}(0) = 0 < \mathrm{Nm}(b)$, so we are done in this case as well.

□

Corollary 2.4 *Every left ideal* I *of* $\mathbb{A}$ *is of the form* $\mathbb{A}a$ *for some* $a \in I$*. Similarly every right ideal is of the form* $a\mathbb{A}$*.*

Proof. If $I = \{0\}$, $a = 0$. So we may assume $I \neq \{0\}$. In the latter case, pick $0 \neq a \in I$ such that a has least positive norm $\mathrm{Nm}(a)$. It is easy to check by the division algorithm that $I = \mathbb{A}a$. The case of right ideal follows by symmetry.

□

3 Lagrange's Theorem of Four Squares

Lagrange's Theorem of Four Squares states that any positive integer is a sum of the squares of four integers. This was first proven by Lagrange, based on Euler's work on sum of two squares (see comments in [5]). After reading Lagrange's paper, Euler gave a much shorter proof which applied equally well to other related results (loc. cit.). It is remarkable that Euler discovered his famous identity showing that the product of two four squares sum is a four squares sum, before the discovery of quaternions. Even though Euler's original proof is not exactly the one which is widely circulated nowadays (see for example the version presented in [5]), it is fair to attribute most of the credit to Euler (even the present version using quaternions), since it bears so much overlap with Euler's original proof. It appears to us: combining the division algorithm of Hurwitz quaternions (Proposition 2.3), and Lemma 3.1 shown below, the proof of Lagrange's Theorem is nothing but an interesting exercise in algebra. Due to this, perhaps, Hurwitz never mentioned that he proved Lagrange's Theorem of Four Squares in his paper ([4]). (But he did mention Lemma 3.4 below, which certainly implies the theorem of four squares.)

Lemma 3.1 *Let p be a prime number. Then there exist $u, v \in \mathbb{Z}$ such that the congruence relation $1 + u^2 + v^2 \equiv 0 \pmod{p}$ is satisfied. In other words, there exists $q \in \mathbb{H}(\mathbb{Z}) \subset \mathbb{A}$ such that $p \nmid q$ (i.e. p does not divide some component of q), but $p|\mathrm{Nm}(q)$.*

Proof. This can be proved by the *Pigeonhole Principle* as follows.

The case of $p = 2$ being trivial, we may assume that p is odd. It can be checked easily that the following numbers are representatives of distinct residue classes mod p:

$$0^2, 1^2, \cdots, \left(\frac{p-1}{2}\right)^2,$$

from which we derive two lists of residue classes, each of which has $\frac{p+1}{2}$ distinct residue classes:

$$\text{List } A: \qquad 1 + 0^2, 1 + 1^2, \cdots, 1 + \left(\frac{p-1}{2}\right)^2$$

and

$$\text{List } B: \qquad 0^2, -1^2, \cdots, -\left(\frac{p-1}{2}\right)^2.$$

The two lists comprise a total of $p + 1$ residue classes. Since there are only p distinct residue classes, by the Pigeonhole Principle, two of the $p + 1$ residue

classes must coincide. Since the classes either in A or in B are distinct, therefore a class in A equals a class in B, i.e. there exist $0 \leq u, v \leq \frac{p-1}{2}$ such that

$$1 + u^2 \equiv -v^2 \pmod{p},$$

which means

$$1 + u^2 + v^2 \equiv 0 \pmod{p}.$$

In terms of quaternions, this says there exists $q = 1 + ui + vj$ such that $p \nmid q$ but $p|\mathrm{Nm}(q) = 1 + u^2 + v^2$.

□

To prove the Theorem of Four Squares, observe that if integers $m > 0, n > 0$ are sum of fours squares then mn is sum of four squares: $m = \mathrm{Nm}(q_1), n = \mathrm{Nm}(q_2) \Rightarrow mn = \mathrm{Nm}(q_1 q_2)$, where $q_1, q_2 \in \mathbb{H}(\mathbb{Z})$. Therefore, it suffices to prove that every prime is a sum of four squares. The case $p = 2$ being trivial, we will work on an odd prime p and first show that $p = \mathrm{Nm}(q)$ for some Hurwitz quaternion. Then we will show that this q can be chosen so that $q \in \mathbb{H}(\mathbb{Z})$, which would conclude the proof.

Proposition 3.2 *Let p be an odd prime. Then p is a sum of four squares.*

Let p be an odd prime number and $q = 1 + ui + vj \in \mathbb{H}(\mathbb{Z})$ such that $p|\mathrm{Nm}(q)$ as in Lemma 3.1.

Claim. $\mathbb{A}p \subsetneq \mathbb{A}p + \mathbb{A}q \subsetneq \mathbb{A}$.
Proof of Claim. First we show the first containment is proper: If $q \in \mathbb{A}p$, we see that $2q \in \mathbb{H}(\mathbb{Z})p$ and hence $p|2$, which is a contradiction.

Now to show that the second containment is proper, it suffices to show that $1 \notin \mathbb{A}p + \mathbb{A}q$: Suppose it were, write $kp + lq = 1$, where $k, l \in \mathbb{A}$. Taking norm on both sides of $lq = 1 - kp$, we see that

$$(lq)(\overline{lq}) = (1 - kp)(1 - \bar{k}p) \Rightarrow lq\bar{q}\bar{l} = 1 - \mathrm{Tr}(k)p + \mathrm{Nm}(k)p^2,$$

i.e.,

$$\mathrm{Nm}(l)\mathrm{Nm}(q) = 1 - \mathrm{Tr}(k)p + \mathrm{Nm}(k)p^2,$$

which implies

$$0 \equiv 1 \pmod{p},$$

a contradiction. Therefore we have proved the Claim.

By Corollary 2.4, $\mathbb{A}p + \mathbb{A}q = \mathbb{A}b$ for some $b \in \mathrm{A}$ with $\mathrm{Nm}(b) \neq 1$. Furthermore, since $\mathbb{A}p \subsetneq \mathbb{A}b$, we have $p = mb$, where $\mathrm{Nm}(m) \neq 1$. Therefore, p is reducible, and $p = \mathrm{Nm}(m)$ (since $p^2 = \mathrm{Nm}(mb) = \mathrm{Nm}(m)\mathrm{Nm}(b)$).

If the above $m \in \mathbb{H}(\mathbb{Z})$, then $p = \mathrm{Nm}(m)$ will be a sum of four squares of integers. Therefore to conclude the proof of the theorem, it suffices to consider the case where $m \in \mathbb{A} \setminus \mathbb{H}(\mathbb{Z})$. We prove in the next lemma that we can get $m' = \delta m \in \mathbb{H}(\mathbb{Z})$ for some unit $\delta \in \mathbb{A}$. Then the theorem would be proven.

□

Lemma 3.3 *For any element $m \in \mathbb{A} \setminus \mathbb{H}(\mathbb{Z})$, we can find $\delta \in \mathbb{A}$ of the form $\frac{\pm 1 \pm i \pm j \pm k}{2}$ such that $\delta m \in \mathbb{H}(\mathbb{Z})$.*

Proof. Given $m = \frac{a+bi+cj+dk}{2} \in \mathbb{A} \setminus \mathbb{H}(\mathbb{Z})$, we have by definition that $a \equiv b \equiv c \equiv d \equiv 1 \pmod 2$. Since a, b, c, d are all odd, we may write further

$$a = 4a_1 + \epsilon_1, b = 4b_1 + \epsilon_2, c = 4c_1 + \epsilon_3, d = 4d_4 + \epsilon_4$$

such that $\epsilon_i = \pm 1$ for $1 \leq i \leq 4$. Then

$$m = 2(a_1 + b_1 i + c_1 j + d_1 k) + \frac{\epsilon_1 + \epsilon_2 i + \epsilon_3 j + \epsilon_4 k}{2}.$$

Letting $\delta_1 := \frac{\epsilon_1 + \epsilon_2 i + \epsilon_3 j + \epsilon_4 k}{2}$, and $\delta = \bar{\delta}_1$, it is easy to check that $\delta m \in \mathbb{H}(\mathbb{Z})$.

□

Lemma 3.4 *Let $h \in \mathbb{A}$ be a nonzero element which is not a unit. Then $h \in \mathbb{A}$ is irreducible $\Leftrightarrow$ $\mathrm{Nm}(h) = p$ for some prime number p.*

Proof. The implication "$\Leftarrow$" is clear.

For the other implication, assume that h is irreducible. Since h is not a unit, we have $\mathrm{Nm}(h) \neq 1$. Let p be any prime factor of $\mathrm{Nm}(h)$.

Following the same line of argument as in Proposition 3.2, we have

$$\mathbb{A}p \subsetneq \mathbb{A}p + \mathbb{A}h \subsetneq \mathbb{A},$$

where the first containment is proper by the fact that $h \notin \mathbb{A}p$ otherwise h would be reducible.

Then we have $\mathbb{A}p + \mathbb{A}h = \mathbb{A}k$ for some non-unit $k \in \mathbb{A}$, hence we have $h = ak$ for some a which must be a unit. Therefore $p \in \mathbb{A}k = \mathbb{A}h$ which implies $p = bh$ for some b, and it is easy to see that $\mathrm{Nm}(h) = p$.

□

4 Unique Factorization of Hurwitz Quaternions

Motivation. We aim to show "unique factorization" for Hurwitz quaternions. But it can be checked that

$$5 = (1+2i)(1-2i) = (1+2j)(1-2j)$$

are manifestly two different factorizations. How do we justify the uniqueness? We will define an equivalence called "recombination". To justify the uniqueness of factorization, just note that we identify two factorizations if one can be obtained from the other by recombination.
Given a Hurwitz quaternion, we will establish its factorization. If $q = mq'$, where $q, q' \in \mathbb{A}$ and $m \in \mathbb{Z}, m > 1$, then by the above example, at least there are many different ways to factor q, since there are many ways to factor m. To avoid such a situation, we will deal with *primitive quaternions* first, as defined below:

Definition 4.1 *A Hurwitz quaternion q is primitive if q cannot be written as mq' for some $m \in \mathbb{Z}, m > 1$ and some $q' \in \mathbb{A}$. If $q = mq'$ for some $q' \in \mathbb{A}$, then we will write $m|q$.*

Lemma 4.2 *Assume* $\mathrm{Nm}(P) = p$ *is a rational prime. If $p \mid QPB$ and $p \nmid QP$, then $p \mid PB$.*

We give two proofs. (cf. Lemma 3 of [2])
First proof: Consider $\mathbb{A}p + \mathbb{A}QP = \mathbb{A}\alpha$. Clearly $\mathrm{Nm}(\alpha) = 1, p$ or p^2 (because $p = q\alpha$ for some $q \in \mathbb{A} \Rightarrow \mathrm{Nm}(\alpha)|\mathrm{Nm}(p) = p^2$).

We rule out the following two cases:

- $\mathrm{Nm}(\alpha) = p^2 \Rightarrow p = \epsilon\alpha$ (ϵ a unit) $\Rightarrow p \mid QP$, a contradiction.
- $\mathrm{Nm}(\alpha) = 1 \Rightarrow \exists\ x, y$ such that $xp + yQP = 1 \Rightarrow yQP = 1 - xp$, a contradiction again when taking norms mod p.

Therefore $\mathrm{Nm}(\alpha) = p$ and there exist x, y such that $xp+yQP = \alpha$. Substituting $\overline{P}P$ for p into this formula gives

$$(x\overline{P} + yQ)P = \alpha,$$

which shows that $(x\overline{P} + yQ) := \epsilon$ is a unit, hence we may write

$$xp + yQP = \epsilon P$$

$$\Rightarrow xpB + yQPB = \epsilon PB$$

$$\Rightarrow p \mid \epsilon PB,$$

hence $p \mid PB$.

□

Second proof: Consider $\overline{P}\mathbb{A} + B\mathbb{A} = \alpha\mathbb{A}$.
Observe first that $\mathrm{Nm}(\alpha) \mid \mathrm{Nm}(\bar{P}) = p$ (because $\bar{P} = \alpha q$ for some $q \in \mathbb{A}$). Therefore $\mathrm{Nm}(\alpha) = 1$ or p.
Claim: $\alpha \neq 1$ (or any unit).
If $\alpha = 1$, then there exist $x, y \in \mathbb{A}$ such that

$$\overline{P}x + By = 1$$

$$\Rightarrow QP(\overline{P}x + By) = QP$$

$$\Rightarrow p \mid QP, \text{ a contradiction.}$$

Hence $\alpha = \overline{P}\epsilon$ for some unit ϵ and $B = \overline{P}\beta$ for some $\beta \in \mathbb{A}$. Therefore we have $p \mid P\overline{P}\beta = PB$.

□

Lemma 4.3 *Let $m > 0$ be an integer, and $A, B \in \mathbb{A}$ be two Hurwitz quaternions. If $m|AB$ and $(m, \mathrm{Nm}(A)) = 1$, then $m|B$.*

Proof. It is easy to see the following implication from the assumptions:

$$(\bar{A}A, m) = 1 \Rightarrow \exists r, s \in \mathbb{Z} \text{ such that } r\bar{A}A + sm = 1$$

$$\Rightarrow r\bar{A}AB + smB = B$$

$$\Rightarrow m|B, \quad \text{since } m|AB \text{ and } m \text{ is in the center of } \mathbb{A}.$$

Note. By similar argument, we also have the following result:

$$m \mid AB, (m, \mathrm{Nm}(B)) = 1 \Rightarrow m \mid A.$$

Corollary 4.4 $(p, p') = 1, p \mid B, \text{ and } p' \mid B \Rightarrow pp' \mid B$.

Proof. Let $B = pQ$. We have $p' \mid pQ$. It suffices to show that $p' \mid Q$, but this is clear by the lemma.

□

Corollary 4.5 *α, β primitive and $(\mathrm{Nm}(\alpha), \mathrm{Nm}(\beta)) = 1 \Rightarrow \alpha\beta$ is primitive.*

Proof. If not, there exists p such that $p \mid \alpha\beta$. By assumption, p cannot divide $\mathrm{Nm}(\alpha)$ and $\mathrm{Nm}(\beta)$ at the same time.

Now $p \nmid \mathrm{Nm}(\alpha) \Rightarrow p \mid \beta$. And $p \nmid \mathrm{Nm}(\beta) \Rightarrow p \mid \alpha$. This is a contradiction.

□

Lemma 4.6 *Let $M_1, M_2, M_1', M_2' \in \mathbb{A}$. Assume that $M_1M_2 = M_1'M_2'$, where $\mathrm{Nm}(M_i) = \mathrm{Nm}(M_i') \neq 1, i = 1, 2$, and $(\mathrm{Nm}(M_1), \mathrm{Nm}(M_2)) = 1$. Then there exists a unit $\epsilon \in \mathbb{A}$ such that $\epsilon M_2 = M_2'$, i.e.*

$$M_1M_2 = (M_1\epsilon^{-1})(\epsilon M_2) = M_1'M_2',$$

where $M_1\epsilon^{-1} = M_1'$, and $\epsilon M_2 = M_2'$.

Proof. Let $m = \mathrm{Nm}(M_2) = M_2\overline{M}_2$. Then by assumption, $(m, \mathrm{Nm}(M_1')) = 1$.

Now $M_1M_2 = M_1'M_2' \Rightarrow M_1M_2\overline{M}_2 = M_1'M_2'\overline{M}_2$. Therefore $m|M_1'M_2'\overline{M}_2$. Since $(m, \mathrm{Nm}(M_1')) = 1$, Lemma 4.3 implies $m|M_2'\overline{M}_2$, i.e. $M_2'\overline{M}_2 = \epsilon m$, where ϵ must be a unit by norm consideration.

Therefore $M_2'\overline{M}_2 = \epsilon m = \epsilon M_2\overline{M}_2 \Rightarrow M_2' = \epsilon M_2$, and as a result $M_1\epsilon^{-1} = M_1'$.

□

Definition 4.7 *If $Q = P_1P_2\cdots P_n$ is a factorization into irreducible elements, then $Q = P_1'\cdots P_n'$ is obviously another factorization into irreducible elements, with $P_n' = \epsilon_{n-1}P_n$, $P_{n-1}' = \epsilon_{n-2}P_{n-1}\epsilon_{n-1}^{-1}, \cdots, P_2' = \epsilon_1P_2\epsilon_2^{-1}$, and $P_1' = P_1\epsilon_1^{-1}$, where ϵ_i's are units. Following Conway and Smith, we call these two factorizations are differed by* ***unit-migration****.*

Theorem 4.8 *Let Q be a primitive element of $\mathbb{A}$. Let $p_1\cdots p_n$ be a fixed prime factorization of $\mathrm{Nm}(Q)$, i.e. we choose a particular model for factoring $\mathrm{Nm}(Q)$, where the order of p_i's matters. Then Q can be factored as $Q = P_1\cdots P_n$, such that $\mathrm{Nm}(P_i) = p_i$, which is unique up to unit-migration.*

Proof. First of all, we need to show such factorization exists, i.e. $\exists P_1, \cdots, P_n$ such that $Q = P_1\cdots P_n$, where $\mathrm{Nm}(P_i) = p_i$ for each i. We prove this by induction, the case $n = 1$ being trivial.

Assume the result is true for $n-1$, $n \geq 2$.

Let $\mathrm{Nm}(Q) = p_1\cdots p_n$. Then $p_n|\mathrm{Nm}(Q)$. As in the first proof of Lemma 4.2, the left ideal $\mathbb{A}Q + \mathbb{A}p_n = \mathbb{A}P$ is principal. By exactly the same argument, we see that $\mathrm{Nm}(P) = p_n$. Consequently $P_n := P$ is a right factor of Q, i.e. $Q = Q'P_n$, where Q' is necessarily primitive, which has a factorization $Q' = P_1\cdots P_{n-1}$ by the induction hypothesis. Therefore Q has a factorization $Q = P_1\cdots P_n$ satisfying $\mathrm{Nm}(P_i) = p_i$.

To prove the unit-migration, we first remark that the case of $n = 1$ is trivial. For $n = 2$, assume the factorization $Q = P_1P_2 = P_1'P_2'$. Then we have $P_1P_2\overline{P_2} = P_1'P_2'\overline{P_2}$, hence $p_2|P_1'P_2'\overline{P_2} \Rightarrow p_2|P_2'\overline{P_2}$ (by Lemma 4.2 and the primitiveness of Q). Therefore we have $P_2'\overline{P_2} = \epsilon p_2 = \epsilon P_2\overline{P_2}$, hence $P_2' = \epsilon P_2$ and $P_1' = P_1\epsilon^{-1}$, where ϵ is a unit.

By induction, assume $n \geq 3$ and the case of $n-1$ has been proved. If $Q = P_1\cdots P_n = P_1'\cdots P_n'$ such that Q is primitive and $\mathrm{Nm}(P_i) = \mathrm{Nm}(P_i') = p_i$ for each i, then

$$P_1\cdots P_n\bar{P}_n = P_1'\cdots P_n'\bar{P}_n$$

$$\Rightarrow p_n|P_1'\cdots P_n'\bar{P}_n = (P_1'\cdots P_{n-1}')P_n'\bar{P}_n$$

$$\Rightarrow p_n|P_n'\bar{P}_n, \text{ by Lemma 4.2 , since } p_n \nmid Q = (P_1'\cdots P_{n-1}')P_n' \text{ by the primitiveness of } Q$$

$$\Rightarrow P_n'\overline{P}_n = \eta p_n = \eta P_n\overline{P}_n \text{ for some } \eta \in \mathbb{A}$$

$$\Rightarrow P'_n = \eta P_n \text{ and } \eta \text{ is a unit}$$

Letting $\epsilon_{n-1} := \eta$, we have proved that $P'_n = \epsilon_{n-1} P_n$.

Now $P_1 \cdots P_n = P'_1 \cdots P'_n = P'_1 \cdots P'_{n-1} \epsilon_{n-1} P_n \Rightarrow P_1 \cdots P_{n-1} = P'_1 \cdots P'_{n-1} \epsilon_{n-1}$. Hence by induction hypothesis, there exist units $\epsilon_1, \cdots, \epsilon_{n-2}$ such that

$$P'_1 = P_1 \epsilon_1^{-1}, P'_2 = \epsilon_1 P_2 \epsilon_2^{-1}, \cdots, P'_{n-1} \epsilon_{n-1} = \epsilon_{n-2} P_{n-1}.$$

Therefore we have shown the existence of units $\epsilon_1, \cdots, \epsilon_{n-1}$ such that

$$P'_1 = P_1 \epsilon_1^{-1}, P'_2 = \epsilon_1 P_2 \epsilon_2^{-1}, \cdots, P'_{n-1} = \epsilon_{n-2} P_{n-1} \epsilon_{n-1}^{-1} \text{ and } P'_n = \epsilon_{n-1} P_n,$$

which is the desired result for the case of n.

□

Corollary 4.9 *Assume PQ satisfies $\mathrm{Nm}(PQ) = pq$, where p and q are distinct primes, $\mathrm{Nm}(P) = p$ and $\mathrm{Nm}(Q) = q$. Then modeled on qp, PQ can be factored as $Q'P'$ with $\mathrm{Nm}(Q') = q$, and $\mathrm{Nm}(P') = p$, unique up to unit-migration.*

Proof. By Corollary 4.5, PQ is primitive. Hence we can apply Theorem 4.8 under the model qp to conclude.

□

Definition 4.10 *Following Conway and Smith, we call this above situation "**meta-commutation**".*

Question. Let $p \mid Q$ and $Q = P_1 P_2 \cdots P_n$ be any factorization. Does it necessarily imply that there exists an adjacent pair P_{i-1}, P_i such that $p | P_{i-1} P_i$, i.e. $P_i = \overline{P}_{i-1} \epsilon$ for some unit ϵ and $2 \leq i \leq n$? For convenience let's call such situation a *fusion*.

This answer is No, as shown by the following

Example. Let QPP' (where $P' = \overline{P}$) be a factorization modeled on qp^2. We know by meta-commutation that QP can be factored as $P''Q'$ modeled on pq. Clearly the factorization $P''Q'P'$ (which is modeled on pqp) does not allow fusion.

Definition 4.11 *A quaternion $Q \in \mathbb{A}$ is said to be p-pure if $\mathrm{Nm}(Q) = p^n$ for some integer $n \geq 1$ and some prime number p.*

Proposition 4.12 *If Q is p-pure, $\mathrm{Nm}(Q) = p^n$ for some $n \geq 2$, and $p | Q = P_1 P_2 \cdots P_n$, where $P_1 P_2 \cdots P_n$ is a factorization, then there exists a fusion, i.e. $p | P_{i-1} P_i$ for some $2 \leq i \leq n$.*

Proof. This is a direct consequence of Lemma 4.2. More precisely, if $p|P_{n-1}P_n$, we are done. If $p \nmid P_{n-1}P_n$, let i be the smallest index such that $p \nmid P_i \cdots P_n$ (clearly $i \geq 2$). Then we have $p|P_{i-1}P_i \cdots P_n$, and $p \nmid P_i \cdots P_n$ which implies $p|P_{i-1}P_i$ by Lemma 4.2.

□

Lemma 4.13 *Let* $Q = M_1M_2 \cdots M_r = M_1'M_2' \cdots M_r'$, *where* $\mathrm{Nm}(M_i) = \mathrm{Nm}(M_i')$ *for* $i = 1, \cdots, r$. *Assume further that the prime factors of* $\mathrm{Nm}(M_i)$ *are mutually co-prime, namely* $(\mathrm{Nm}(M_i), \prod_{j \neq i} \mathrm{Nm}(M_j)) = 1$ *for each* i. *Then there exist units* $\epsilon_1, \cdots, \epsilon_{r-1}$ *such that*

$$M_r' = \epsilon_{r-1}M_r, M_{r-1}' = \epsilon_{r-2}M_{r-1}\epsilon_{r-1}^{-1}, \cdots, M_1' = M_1\epsilon_1^{-1}.$$

Proof. This follows easily from Lemma 4.6 by induction.

□

To derive a useful corollary from Lemma 4.13, we make the following definition and observation.

Definition 4.14 *Let* $Q \in \mathbb{A}$ *be a nonunit. Let* $\mathrm{Nm}(Q) = p_1^{k_1} \cdots p_r^{k_r}$, *where* $p_1 < \cdots < p_r$ *and* $k_i \geq 1$ *for* $i = 1, \cdots, r$. *We will call this the standard model for* Q.

Observation. For every factorization of Q modeled on the standard model, we can associate a factorization in blocks, i.e. $Q = M_1M_2 \cdots M_r$, where each M_i is a p_i-pure quaternion of norm $p_i^{k_i}, i = 1, \cdots, r$. This is clear, since given any factorization of Q modeled on the standard model, we can simply multiply all the factors of norm p_i and call the result M_i.

Corollary 4.15 *Any two factorizations in blocks associated with the corresponding factorizations of* $Q \in \mathbb{A}$ *modeled on the standard model are related by a unit-migration described in Lemma 4.13. Consequently, given two factorizations of* Q *modeled on the standard model, one can exert a unit-migration such that the associated factorizations in blocks agree.*

Definition 4.16 *Let* p *be a prime number. Then* $p = P_1\overline{P_1}$ *for some irreducible* $P_1 \in \mathbb{A}$. *If* $P_2 \in \mathbb{A}$ *satisfies* $\mathrm{Nm}(P_2) = p$, *then* $P_1\overline{P_1} = P_2\overline{P_2}$. *More generally, given* $\mathrm{Nm}(P_1) = \mathrm{Nm}(P_2) = p$, *we say that* $P_1\overline{P_1}\epsilon \to P_2\overline{P_2}\epsilon$ *is a process of* ***re-combination****, where we intentionally allow the appearance of a unit* ϵ.

Lemma 4.17 *Let* Q *be* p*-pure,* $Q = P_1P_2 \cdots P_n$ *and* $p|Q$. *Then after a series of re-combinations and unit-migrations, one arrives at the case when* $p|P_1P_2$. *If* $n > 2$, *by one more unit-migration if necessary, one may assume that* $p = P_1P_2$.

Proof. We prove this by induction, the case $n = 2$ being trivial.

Assume the case $n-1$ ($n \geq 3$) is true, and prove for the case n.

If $Q = (P_1 \cdots P_{n-1})P_n$, we may assume that $p \nmid P_1 \cdots P_{n-1}$, otherwise the result is clear by induction hypothesis.

Now if $p \nmid P_1 \cdots P_{n-1}$, then we have $p|P_{n-1}P_n$ (say $P_{n-1}P_n = \epsilon p \Rightarrow \epsilon^{-1}P_{n-1}P_n = p = \overline{P_n}P_n$) by Lemma 4.2. But then

$$Q = (P_1 \cdots P_{n-2})(P_{n-1}P_n) = P_1 \cdots \underline{P_{n-2}\epsilon} \ \cdot \underline{\epsilon^{-1}P_{n-1}}P_n$$

(underlined factors denote new factors after a unit-migration)

$$= P_1 \cdots P'_{n-2}(\overline{P_n}P_n) \text{ (renaming } P_{n-2}\epsilon \text{ by } P'_{n-2} \text{ and } \epsilon^{-1}P_{n-1} \text{ by } \overline{P_n})$$

$$= P_1 \cdots P'_{n-2}(\overline{P'_{n-2}}P'_{n-2}) \text{ (by recombination } \overline{P_n}P_n \to \overline{P'_{n-2}}P'_{n-2})$$

Since $p|P_1 \cdots P'_{n-2}\overline{P'_{n-2}}$, we have reduced to the case $n-1$, therefore by induction hypothesis, we are done.

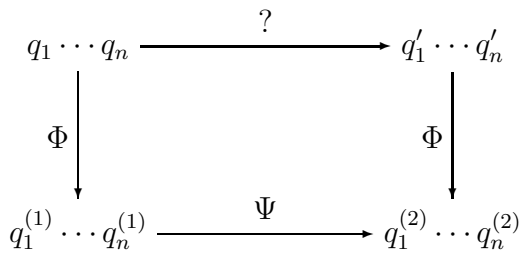
For the last statement, assume $n > 2$, $Q = P_1P_2P_3 \cdots P_n$ and we already have $p|P_1P_2$. Then $P_1P_2 = p\epsilon$ for some unit ϵ. Now we can write $Q = P_1P_2P_3 \cdots P_n = P_1(P_2\epsilon^{-1})(\epsilon P_3) \cdots P_n$. Therefore by this latter unit-migration, we have achieved the result $p = P_1(P_2\epsilon^{-1})$.

□

Now that we have introduced the notions of unit-migration, meta-commutation and recombination, we are ready to state the following

Theorem 4.18 *Let $q \in \mathbb{A}$ be a non-unit Hurwitz quaternion and $q = q_1 \cdots q_n = q'_1 \cdots q'_n$ be two factorizations into irreducible factors. Then $q_1 \cdots q_n$ and $q'_1 \cdots q'_n$ are related by a series of unit-migrations, meta-commutations, and re-combinations, i.e. one is obtained from the other by applying a series of the above operations.*

Proof. First we exhibit the following diagram, where Φ (the two Φ's are in general distinct, but we use the same letter for simplicity) means a series of steps consisting of meta-commutations leading to the the standard models $q_1^{(1)} \cdots q_n^{(1)}$ and $q_1^{(2)} \cdots q_n^{(2)}$, where the prime factors are ordered.



We need to specify the process of Ψ: It consists of two stages. First by the Corollary 4.15, there exists a unit-migration such that the two associated factorizations of q in blocks (of factors whose norms are of the form $p_i^{n_i}$, where the rational primes p_i and p_j are distinct if $i \neq j$) coincide. Therefore as the second stage of Ψ it remains to show that any two factorizations of a p-pure quaternion are related by the two series of processes, namely unit-migrations and recombinations, which we will do in the following proposition. Observe that all the processes are invertible, hence the first factorization reaches the second one by composing Φ, Ψ and Φ^{-1}.

Proposition 4.19 *Let Q be a p-pure quaternion of norm $\mathrm{Nm}(Q) = p^n, n \geq 1$. Then any two factorizations of Q are related by a series of unit-migrations and recombinations.*

Proof. If Q is primitive, then by Theorem 4.8, any two factorizations are related by unit-migration. We will prove the general case by induction on n. The case $n = 1$ is trivial. For $n = 2$, the result is clear if Q is primitive, therefore we let $Q = P_1P_2 = P_1'P_2'$, and $p|Q$. Clearly we have $Q = p\epsilon$ for some unit ϵ, so we may write $P_1P_2 = p\epsilon = P_1\overline{P_1}\epsilon$ (resp. $P_1'P_2' = p\epsilon = P_1'\overline{P_1'}\epsilon$), therefore $P_2 = \overline{P_1}\epsilon$ (resp. $P_2' = \overline{P_1'}\epsilon$) and $P_1P_2 = P_1\overline{P_1}\epsilon = P_1'\overline{P_1'}\epsilon = P_1'P_2'$ is a recombination (see Definition 4.16). Assume $n > 2$ and the case of smaller n has been established. Let $p|Q$ (otherwise the result is clear by Theorem 4.8)), and $Q = P_1P_2\cdots P_n = P_1'P_2'\cdots P_n'$ be two factorizations. Following the diagram as in the proof of Theorem 4.18 and using Lemma 4.17, let Φ (under the same name) be two series of recombinations and unit-migrations bringing each of the two factorizations to a form such that $P_1P_2 = p = P_1'P_2'$. The remaining factors $P_3\cdots P_n = P_3'\cdots P_n'$ are related by a series Ψ_1 of recombinations and unit-migrations by the induction hypothesis. But it is clear that $P_1P_2 = P_1'P_2' = p$ (call this Ψ_2) is a recombination. By composing Φ, Ψ_1, Ψ_2 and Φ^{-1}, the original two factorizations $P_1P_2\cdots P_n$ and $P_1'P_2'\cdots P_n'$ are related by a series of recombinations and unit-migrations.

□

With the above proposition, the proof of Theorem 4.18 is complete.

To conclude, let's illustrate Theorem 4.18 by the following

Example. Consider the two factorizations (A) and (B) of $9 - 3i - 15j$:

$$\left(\frac{-1+i+3j-k}{2}\right)\cdot(2+i)\cdot\left(\frac{-1+3i+j+k}{2}\right)\cdot(2+i+j+k) \qquad \text{(A)}$$

and

$$(1+i+j)\cdot(1-i-j)\cdot\left(\frac{-3+i-3j+k}{2}\right)\cdot\left(\frac{1-i+5j+k}{2}\right) \qquad \text{(B).}$$

Starting from (A), we describe a process to reach (B).

Step 1. Meta-commutation of the middle two factors:

$$\left(\frac{-1+i+3j-k}{2}\right)\cdot(2+i)\cdot\left(\frac{-1+3i+j+k}{2}\right)\cdot(2+i+j+k)$$
$$=\left(\frac{-1+i+3j-k}{2}\right)\cdot\left(\frac{-1+i-j-3k}{2}\right)\cdot(j-2k)\cdot(2+i+j+k).$$

Step 2. Unit-migration with $\epsilon_1=1, \epsilon_2=-i$, and $\epsilon_3=\frac{1-i+j+k}{2}$:

$$\left(\frac{-1+i+3j-k}{2}\right)\epsilon_1^{-1}\cdot\epsilon_1\left(\frac{-1+i-j-3k}{2}\right)\epsilon_2^{-1}\cdot\epsilon_2(j-2k)\epsilon_3^{-1}\cdot\epsilon_3(2+i+j+k)$$

$$=\left(\frac{-1+i+3j-k}{2}\right)\cdot\left(\frac{-1-i-3j+k}{2}\right)\cdot\left(\frac{-3+i-3j+k}{2}\right)\cdot\left(\frac{1-i+5j+k}{2}\right)$$

Step 3. Recombination $\left(\frac{-1+i+3j-k}{2}\right)\cdot\left(\frac{-1-i-3j+k}{2}\right)=(1+i+j)(1-i-j)=3$:

$$\left(\frac{-1+i+3j-k}{2}\right)\cdot\left(\frac{-1-i-3j+k}{2}\right)\cdot\left(\frac{-3+i-3j+k}{2}\right)\cdot\left(\frac{1-i+5j+k}{2}\right)$$

$$=(1+i+j)\cdot(1-i-j)\cdot\left(\frac{-3+i-3j+k}{2}\right)\cdot\left(\frac{1-i+5j+k}{2}\right).$$

References

[1] John H. Conway & Derek A. Smith, *On Quaternions And Octonions: Their Geometry, Arithmetic, And Symmetry*, A K Peters, Limited, 2003

[2] L. E. Dickson, On the Theory of Numbers and Generalized Quaternions, *American Journal of Mathematics,* Vol. **46**, No. 1 (Jan., 1924), p.1-16

[3] L. Euler, Novae demonstrationes circa resolutionem numerorum in quadrata, *Nova acta eruditorum* (1773), p.193-211, E445 in the Enestr̈om index.

[4] A. Hurwitz, Über die Zahlentheorie der Quaternionen, *Nachrichten von der k. Gesellschaft der Wissenschaften zu Göttingen, Mathematisch-physikalische Klasse,* 1896, S. 313-340

[5] A. Weil, *Number Theory, An approach through history from Hammurapi to Legendre*, Birkhäuser, Boston, 1983.

Received: April, 2012