LATTICE EMBEDDINGS IN THE COMPOSITION ALGEBRAS

MICHAEL KNOPF, UC BERKELEY

I would like to thank Professor George Bergman for advising this paper, especially for his patient reading and many helpful suggestions.

Abstract. Define a *rational composition algebra* to be a Euclidean Hurwitz algebra, except where the underlying field is $\mathbb{Q}$. I prove a simple characterization of all such algebras. One example is the subring $\mathbb{Q}(i,j) \subset \mathbb{H}$ of quaternions with rational coordinates, which can be identified with $\mathbb{Q}^4$. The Hurwitz integral quaternions $\mathbf{H}$ are a maximal order of algebraic integers in $\mathbb{Q}(i,j)$. If $\mathcal{M}$ is a subset of $\mathbb{R}^n$ with the squared distance between any two points integral, call $\mathcal{M}$ an *integer norm set.* If $\mathcal{M} \subset \mathbb{Q}(i,j)$ is an integer norm set, I prove there is an inner automorphism of $\mathbb{Q}(i,j)$ for which the image of $\mathcal{M}$ lies in $\mathbf{H}$. In particular, every order of algebraic integers in $\mathbb{Q}(i,j)$ is isomorphic to a subring of $\mathbf{H}$. If $\mathcal{M} \subset \mathbb{R}^2$ is an integer norm set, not necessarily in $\mathbb{Q}(i,j)$, there is a positive squarefree integer D such that any triangle formed in $\mathcal{M}$ has area of the form $q\sqrt{D}$ for some $q \in \mathbb{Q}$. I prove that if $D \not\equiv 3 \pmod 4$, $\mathcal{M}$ embeds congruently in $\mathbb{Z}^4$; and if $D \not\equiv 7 \pmod 8$, $\mathcal{M}$ embeds congruently in $\mathbf{H}$. If $D \equiv 7 \pmod 8$, I conjecture that $\mathcal{M}$ embeds congruently in the Kleinian octaves, an order within the octonion algebra. This conjecture would imply that all integer norm sets in $\mathbb{R}^2$ embed in the *Double Hurwitzian Ring* $\mathbf{H} \oplus \mathbf{H}$.

1. Introduction

A well-known problem of Paul Erdös asks for n points in the plane, no three on a line and no four on a circle, for which all pairwise distances are integral. A point set of this kind is said to be in “general position”. In 2008, it was announced that a set of seven such points had been found, having a diameter of 22270 [8]. When coordinates for this heptagon were presented, they had the curious property that each point was of the form $(a, b\sqrt{2002})$ for integers a and b.

This phenomenon is no coincidence. In fact, the number 2002 turns out to be a defining feature of this point set: any 3 of its points form a triangle with area of the form $\frac{z}{4}\sqrt{2002}$, where z is an integer. In general, if $\mathcal{M} \subseteq \mathbb{R}^2$ is a set of points in the plane such that $|x-y|^2 \in \mathbb{Z}$ for all $x, y \in \mathcal{M}$, then there exists a squarefree integer D such that any three points in $\mathcal{M}$ form a triangle of area $\frac{z}{4}\sqrt{D}$ for some integer z. If $\mathcal{M}$ is not collinear, the number D is called the *characteristic* of $\mathcal{M}$ [8]. We call such a set a *planar integer norm set.*

Naturally, the case of $D = 1$ has been of interest, and it has been shown that $\mathcal{M}$ embeds in $\mathbb{Z}^2$ if this holds (when we speak of embeddings, we will always mean congruent embeddings via an isometry) [20, 5, 12, 13]. The general case was explored and it was established that, when the square of every ideal of $\mathcal{O}_{\mathbb{Q}(\sqrt{-D})}$(the maximal order of algebraic integers within $\mathbb{Q}(\sqrt{-D})$) is principal, $\mathcal{M}$ embeds in $\mathcal{O}_{\mathbb{Q}(\sqrt{-D})}$ if it embeds in $\mathbb{Q}(\sqrt{-D})$; conversely, if the square of some ideal is nonprincipal, then there exists such a pointset - a triangle, even - which embeds in $\mathbb{Q}(\sqrt{-D})$ but not in $\mathcal{O}_{\mathbb{Q}(\sqrt{-D})}$. It is natural to consider such lattices as targets for these embeddings, for if $\mathcal{M}$ has characteristic D then it cannot embed in $\mathbb{Q}(\sqrt{-E})$ for any squarefree $E \neq D$ [7], but a simple condition can be given to characterize whether $\mathcal{M}$ embeds in $\mathbb{Q}(\sqrt{-D})$.

This paper investigates the remaining cases of those $\mathcal{M}$ for which no embedding in $\mathcal{O}_{\mathbb{Q}(\sqrt{-D})}$ exists, as well as integer norm sets which are not planar. Clearly, any subset of $\mathcal{O}_{\mathbb{Q}(\sqrt{-D})}$ is an planar integer norm set, nevertheless not all planar integer norm sets can be realized as subsets of one of these orders. Is there a natural lattice that does have this property? I conjecture that the answer is yes, and that the lattice we seek is the double Hurwitzian ring, a sublattice of the integral octonions.

In an effort to keep this paper as self-contained as possible, I have presented all background material necessary to understand the final results. Sections 4, 7, and 8 contain primarily new material; anything

Date: December 10, 2015.

in these sections that has been proven before will be clearly attributed. Section 3 contains an original presentation of some elementary concepts of this theory, which are certainly well-known. Proposition 12 is a key result that I have not found in the literature, but I am certain would also be considered elementary.

2. The Composition Algebras

Note: The appendix contains a collection of laws satisfied in a composition algebra. They are labeled by a letter followed by a number. For instance, the "braid law", which states that $[\alpha\beta, \gamma] = [\beta, \overline{\alpha}\gamma]$ is labeled C1. When one of these relations is used, we will indicate this by placing its label over an equality sign. For example, $[\alpha(\gamma\delta), \beta\nu] \overset{\text{C1}}{=} [\gamma\delta, \overline{\alpha}\beta\nu]$.

Definition 1. An *algebra over a field* is a vector space V, over a field K, equipped with a bilinear, not necessarily associative, multiplication $V \times V \to V$.

In general, an inner product space is usually thought of to have $\mathbb{R}$ or $\mathbb{C}$ as its underlying field. We will do away with this convention, and allow an inner product space to use $\mathbb{Q}$ as its field of scalars. For the purposes of this paper, we adopt the following definition, though outside this discussion this object might instead be called a "Euclidean Hurwitz algebra":

Definition 2. Let V be a finite-dimensional inner product space over a field F, where $F = \mathbb{Q}$ or $F = \mathbb{R}$, with inner product $[\,\cdot\,,\,\cdot\,] : V \times V \to F$. Define a *norm* function $[\,\cdot\,] : V \to F$ by $[\alpha] = [\alpha, \alpha]$. Suppose we define a multiplication making V into a unital algebra A over F. Then A is called a *composition algebra* if the identity

$$[\alpha\beta] = [\alpha]\,[\beta]$$

holds, which is known as the *composition law.* We call a composition algebra A a *rational composition algebra* if $F = \mathbb{Q}$ and a *real composition algebra* if $F = \mathbb{R}$.

We will follow the convention of using Greek letters for elements of a composition algebra and Roman letters for real numbers. We call $[\alpha, 1]$ the *real part* of α, and denote it by $\mathrm{Re}(\alpha)$. We also define a conjugation operator by $\overline{\alpha} = 2[\alpha, 1] - \alpha$. It is verified, in the appendix, that the identities $\overline{\alpha + \beta} = \overline{\alpha} + \overline{\beta}$, $\overline{\alpha \cdot \beta} = \overline{\beta} \cdot \overline{\alpha}$, $\overline{\overline{\alpha}} = \alpha$, and $\alpha\overline{\alpha} = [\alpha]$ are satisfied. If A and B are composition algebras over F, we define an *embedding of A into B* to be an inner product space homomorphism φ such that $\varphi(1) = 1$ and $\varphi(\alpha\beta) = \varphi(\alpha)\varphi(\beta)$ for all $\alpha, \beta \in A$. By saying φ is an inner product space homomorphism, we mean that φ is a linear map satisfying $[\varphi(\alpha), \varphi(\beta)] = [\alpha, \beta]$ for all $\alpha, \beta \in A$. Therefore, an embedding of composition algebras must be injective, since $\varphi(\alpha) = 0$ if and only if $[\varphi(\alpha)] = [\alpha] = 0$, which is equivalent to having $\alpha = 0$. If an embedding of composition algebras is surjective as well, call it an *isomorphism of composition algebras.* This leads us to the following simplification:

Proposition 3. Up to isomorphism, any real composition algebra is the inner product space $\mathbb{R}^n$, with the standard Euclidean inner product, equipped with some bilinear multiplication.

Proof. If A is a composition algebra space over $\mathbb{R}$ of finite dimension n, we can extend $\{1\} \subseteq A$ to a basis of A, then apply the Gram-Schmidt process to obtain an orthonormal basis. It follows that A is isomorphic, as an inner product space, to $\mathbb{R}^n$ with the standard Euclidean inner product. This isomorphism can be chosen to send 1_A to $e_1 \in \mathbb{R}^n$. The linearity of the isomorphism then induces a bilinear multiplication on $\mathbb{R}^n$ satisfying the composition law, making it into an algebra isomorphic to A. □

Obviously, $\mathbb{R}$ itself is a real composition algebra, though the quintessential example is $\mathbb{C}$. Still well-known is the ring of quaternions $\mathbb{H}$, which extends $\mathbb{C}$ by adjoining an orthogonal unit vector j and imposing the relations $i^2 = j^2 = k^2 = ijk = -1$, where $k = ij$. A consequence of this definition is that k is orthogonal to $1, i$, and j, but together these four vectors span all of $\mathbb{H}$.

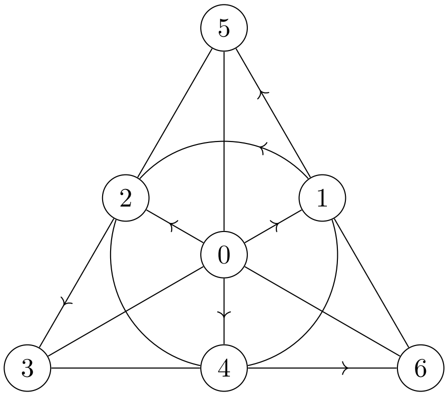
To obtain a final example, we repeat this process, this time adjoining an element orthogonal to $\mathbb{H}$ and defining a multiplication in the following way: denote the basis elements of $\mathbb{H}$ by $i_\infty = 1$, $i_0 = i$, $i_1 = j$, $i_3 = ij$, and call the new orthogonal element i_2. Next, define $i_4 = i_1 i_2$, $i_5 = i_2 i_3$, and $i_6 = i_3 i_4$. These 8 elements are pairwise-orthogonal, and their multiplication is given by the relations

$$\begin{aligned}
&i_n^2 = -1\\
&i_\infty i_n = i_n = i_n i_\infty\\
&i_{n+1} i_{n+2} = i_{n+4} = -i_{n+2} i_{n+1}\\
&i_{n+2} i_{n+4} = i_{n+1} = -i_{n+4} i_{n+2}\\
&i_{n+4} i_{n+1} = i_{n+2} = -i_{n+1} i_{n+4}
\end{aligned}$$

for $0 \leq n \leq 6$, where the indices are taken mod 7. $\mathbb{O}$ fails to be associative. However, it is *alternative*, meaning that $\alpha(\alpha\beta) = \alpha^2\beta$ for all $\alpha, \beta \in \mathbb{O}$. A theorem of Artin states that the subalgebra generated by two elements in an alternative algebra is associative.

Notice that any pair of the elements i_a, i_b, for $a, b \neq \infty$, generate a quaternion subalgebra, since any $r, s \in \mathbb{Z}_7$ differ by either 1,2, or 3 (in absolute value), thus the algebra they generate is determined by the above relations after fixing an appropriate n for the bottom three relations. For example, i_3 and i_5 generate the algebra $\mathbb{R}[i_2, i_3, i_5]$, whose multiplication is found by fixing $n = 1$. Furthermore, all quaternion subalgebras having $\{i_\infty, i_a, i_b, i_c\}$ as a basis over $\mathbb{R}$, for some distinct a, b, and c, arise by fixing some n in these relations. For if c were not the index such that $i_a i_b = \pm i_c$, then the space spanned by $\{i_\infty, i_a, i_b, i_c\}$ would not be closed under multiplication.

The phenomenon just observed can be visualized by labeling the vertices of the Fano plane, as shown below, and identifying each line with the quaternion subalgebra generated by the units corresponding to the nodes it passes through. The direction of each line symbolizes the "positive direction of multiplication." For instance, $i_5 i_2 = i_3$, but $i_2 i_5 = -i_3$ is visualized by the direction of the line connecting 5, 2, and 3.



The above process of extending an algebra by adjoining an orthogonal vector and imposing multiplicative relations that result in a composition algebra is called the Cayley-Dickson construction. A subtly different situation is one in which H is a proper subalgebra of a larger composition algebra. In this case, there is already a natural extension of H found by choosing an element i orthogonal to H and forming the subalgebra $H + iH$. This algebra is unique up to isomorphism, since its multiplication is completely determined by the composition doubling law (D3). We call $H + iH$ the "Dickson double" of H. In light of the following famous theorem, the Cayley-Dickson construction must terminate after three doublings of the base field $\mathbb{R}$. Important details of the proof, borrowed from [3], are relegated to the appendix, but the key ideas are all contained here.

Theorem 4 (Hurwitz)**.** The only real composition algebras are $\mathbb{R}$, $\mathbb{C}$, $\mathbb{H}$, and $\mathbb{O}$.

Sketch of proof. Let Y be a real composition algebra, and suppose it contains a proper sub-algebra X. Then Y contains an element orthogonal to X and thus also contains its Dickson double. In fact, since Y is finite-dimensional it must itself be a Dickson double, for otherwise it would lie strictly between a proper subalgebra and its Dickson double.

Suppose then that $Y = X + i_Y X$, where $X \subsetneq Y$ and $i_Y \in Y$ is a unit vector orthogonal to X. It follows from the composition law alone (see (D3) in the appendix) that

$$(a + i_Y b)(c + i_Y d) \overset{\text{D3}}{=} (ac - d\bar{b}) + i_Y(cb + \bar{a}d)$$

for all $a, b, c, d \in X$. Therefore, we must have, for all $a, b, c, d \in X$,

$$[a + i_Y b]\,[c + i_Y d] = \left[(ac - d\bar{b}) + i_Y(cb + \overline{a}d)\right].$$

Expanding this expression and canceling, we see that $[ac, d\bar{b}] = [cb, \overline{a}d]$, or equivalently $[(ac)b, d] \overset{\text{C1}}{=} [a(cb), d]$, holds for all $a, b, c, d \in X$. This implies the law of associativity for X. Thus, X is an associative composition algebra.

Suppose a real composition algebra is not $\mathbb{R}, \mathbb{C}$, or $\mathbb{H}$. The algebra is unital, and thus properly contains $\mathbb{R}$. By Dickson doubling, it must then contain $\mathbb{C}$, $\mathbb{H}$, and $\mathbb{O}$ as well. If the containment of $\mathbb{O}$ were proper, it would also contain its Dickson double, contradicting that it is a composition algebra because $\mathbb{O}$ is nonassociative. Therefore, the algebra must be $\mathbb{O}$. □

For a more detailed overview of these topics, refer to [3] or the appendix.

3. Automorphisms of $\mathbb{O}$

The Cayley-Dickson construction gives us a method of understanding the automorphism groups of real composition algebras. Let $\{\alpha, \beta, \gamma\} \subset \mathbb{O}$ be a set of unit length vectors such that $\alpha \perp \mathbb{R}$, $\beta \perp \mathbb{R}(\alpha)$, and $\gamma \perp \mathbb{R}(\alpha, \beta)$. In the Cayley-Dickson construction, we could have chosen α to be the vector which extends $\mathbb{R}$ to $\mathbb{C}$, then β to be the vector which extends $\mathbb{C}$ to $\mathbb{H}$, and finally γ to be the vector which extends $\mathbb{H}$ to $\mathbb{O}$. Therefore, the map $i_0 \mapsto \alpha, i_1 \mapsto \beta, i_2 \mapsto \gamma$ induces an automorphism of $\mathbb{O}$.

Conversely, if φ is an automorphism of $\mathbb{O}$, and we let $\alpha = \varphi(i_0), \beta = \varphi(i_1)$, and $\gamma = \varphi(i_2)$, then it is necessarily the case that none of α, β, and γ are in the algebra generated by either of the other two over $\mathbb{R}$. For the algebra generated by any two over $\mathbb{R}$ must be, by the Cayley-Dickson construction, isomorphic to $\mathbb{H}$. If this subalgebra were to contain the third element as well, then it would have to be all of $\mathbb{O}$, and clearly $\mathbb{O}$ cannot be embedded into $\mathbb{H}$, since it has greater dimension. Therefore, $\{\alpha, \beta, \gamma\} \subset \mathbb{O}$ must be a set of unit length vectors such that $\alpha \perp \mathbb{R}$, $\beta \perp \mathbb{R}(\alpha)$, and $\gamma \perp \mathbb{R}(\alpha, \beta)$. Thus, the set of automorphisms of $\mathbb{O}$ is in correspondence with sets of the form $\{\alpha, \beta, \gamma\} \subset \mathbb{O}$ where $[\alpha] = [\beta] = [\gamma] = 1$ and $\alpha \perp \mathbb{R}$, $\beta \perp \mathbb{R}(\alpha)$, and $\gamma \perp \mathbb{R}(\alpha, \beta)$

Similarly, by choosing any two elements $\alpha, \beta \in \mathbb{O}$ of unit length satisfying with $\alpha \perp \mathbb{R}$ and $\beta \perp \mathbb{R}(\alpha)$, we can create an embedding $\mathbb{H} \hookrightarrow \mathbb{O}$ by $i \mapsto \alpha, j \mapsto \beta$. Conversely, any such embedding must be of this form. Therefore, the set of embeddings of $\mathbb{H}$ into $\mathbb{O}$ are in correspondence with sets of the form $\{\alpha, \beta\} \subseteq \mathbb{O}$ where $[\alpha] = [\beta] = 1$, $\alpha \perp \mathbb{R}$, and $\beta \perp \mathbb{R}(\alpha)$. Continuing this reasoning, we see that the set of embeddings of $\mathbb{C}$ into $\mathbb{O}$ is in correspondence with the set of elements of $\mathbb{O}$ of unit length that are orthogonal to $\mathbb{R}$. This establishes the following theorem:

Theorem 5. Let $\mathcal{S}_1, \mathcal{S}_2, \mathcal{S}_3$ be the collections of every subset of $\mathbb{O}$ that is a minimal orthonormal generating set for a subalgebra isomorphic to $\mathbb{C}$, $\mathbb{H}$, or $\mathbb{O}$, respectively. That is, for each $n \in \{1, 2, 3\}$, define

$$\mathcal{S}_n = \{\{\alpha_1, \ldots, \alpha_n\} \subset \mathbb{O} : r, s, t \in \{1, \ldots, n\}, r \notin \{s, t\}, \alpha_r \notin \mathbb{R}(\alpha_s, \alpha_t)\}.$$

The maps $\operatorname{Emb}(\mathbb{C}, \mathbb{O}) \to \mathcal{S}_1$ defined by $\varphi \mapsto \{\varphi(i)\}$, $\operatorname{Emb}(\mathbb{H}, \mathbb{O}) \to \mathcal{S}_2$ defined by $\varphi \mapsto \{\varphi(i_0), \varphi(i_1)\}$, and $\operatorname{Aut}(\mathbb{O}) \to \mathcal{S}_3$ defined by $\varphi \mapsto \{\varphi(i_0), \varphi(i_1), \varphi(i_2)\}$ are bijections.

Corollary 6 (Diassociativity)**.** A subalgebra of $\mathbb{O}$ generated by two elements is associative.

Proof. The subalgebra generated by any two elements of $\mathbb{O}$ is isomorphic to $\mathbb{R}$, $\mathbb{C}$, or $\mathbb{H}$. □

Let A be an algebraic structure with a binary operation and an inverse operator, written additively. Let I be an index set. A *generalized permutation* is an operation on $\prod_{t \in I} A$ of the form

$$\prod_{t \in I} x_i \mapsto \prod_{t \in I} \lambda_t(x_{\sigma^{-1}(t)})$$

where the function $\lambda : I \to \{\mathrm{id}, x \mapsto -x\}$ assigns, to each element $t \in I$, a function λ_t which is either the identity map on A or the inverse map on A, and σ is a permutation of I. Less formally, a generalized permutation is an operation on $\prod_{t \in I} A$ that "permutes components change signs." For a given generalized permutation, we will call λ the *associated sign function* and σ the *associated permutation.* Consider the following example: $(a, b, c) \mapsto (-c, a, b)$ is a generalized permutation on A^3 with associated sign function defined by $1 \mapsto (x \mapsto -x)$, and $2, 3 \mapsto \mathrm{id}$, and associated permutation defined by $1 \to 2 \to 3 \to 1$.

If f and g are two generalized permutations on $\prod_{t\in I} A$, with associated sign functions λ and μ, and associated permutation σ and τ, then $f \circ g$ is a generalized permutation on $\prod_{t\in I} A$ with associated sign function ν, where $\nu_t = \lambda_t \circ \mu_t$ for each $t \in I$, and associated permutation $\sigma\tau = \sigma \circ \tau$. Generalized permutations are clearly invertible. Since function composition is associative, the generalized permutations on $\prod_{t\in I}$ form a group $G \cong \mathbb{Z}_2 \times \mathrm{Perm}(I)$, and the map taking a generalized permutation on $\prod_{t\in I} A$ to its associated permutation is a homomorphism from G to the group of permutations on I.

Let $\Omega = \{\infty, 0, 1, 2, 3, 4, 5, 6\}$, so that $\mathbb{O} \cong \prod_{t\in\Omega} \mathbb{R}$. Every element $\gamma \in \mathbb{O}$ induces left and right multiplication operators L_γ and R_γ on $\mathbb{O}$, defined in the obvious way. If $\gamma = i_r$ for some $r \in \Omega$, then these operators are generalized permutations on $\mathbb{O}$ when it is viewed as $\mathbb{R}^8$. Fix some $r \in \Omega$ and assume M_{i_r} is one of L_{i_r} or R_{i_r}, since the arguments we will use for one apply to both. Note that, for $t \in \Omega$, σ is the permutation associated with M_{i_t} if and only if

$$M_{i_t}\left(\sum_{s\in\Omega} a_s i_s\right) = \sum_{s\in\Omega} a_{\sigma^{-1}(s)} i_s = \sum_{s\in\Omega} a_s i_{\sigma(s)}.$$

If S is a subset of Ω containing r then, by closure under multiplication, M_{i_r} restricts to a generalized permutation on $\mathbb{R}(\{i_t : t \in S\})$ (when it is viewed as a direct product of copies of $\mathbb{R}$). Less obvious is the following fact.

Proposition 7. If S is a 4-element subset of Ω such that $\mathbb{R}(\{i_t : t \in S\}) \cong \mathbb{H}$ and $r \in S^c = \Omega \setminus S$, then $\sigma(S) = S^c$ and $\sigma(S^c) = S$, where σ is the associated permutation of M_{i_r}.

Proof. To see this, first check the claim for $S = \{\infty, 0, 1, 3\}$ and $r = 2$:

$$L_{i_2}(ai_\infty + bi_0 + ci_1 + di_3) = ai_2 - bi_6 - ci_4 + di_5$$
$$R_{i_2}(ai_\infty + bi_0 + ci_1 + di_3) = ai_2 + bi_6 + ci_4 - di_5$$

If S' is another 4-element subset of Ω such that $\mathbb{R}(\{i_t : t \in S'\}) \cong \mathbb{H}$ and $r' \notin S$, then by Theorem 5 there is a permutation τ of Ω taking S' to S (note that this implies $\tau(S'^c) = S^c$ as well) and r' to r that induces an automorphism φ_τ of $\mathbb{O}$, defined by

$$\varphi_\tau\left(\sum_{s\in\Omega} a_s i_s\right) = \sum_{s\in\Omega} a_s i_{\tau(s)}.$$

More formally, we know that $\mathbb{R}(\{i_t : t \in S\}) = \mathbb{R}(i_{t_1}, i_{t_2}) \cong \mathbb{H}$ and $\mathbb{R}(\{i_t : t \in S'\}) = \mathbb{R}(i'_{t_1}, i'_{t_2}) \cong \mathbb{H}$ for some $t_1, t_2, t'_1, t'_2 \in \Omega$ with $t_1 \neq t_2$ and $t'_1 \neq t'_2$. Therefore, the map $i_{t_1} \mapsto i'_{t_1}, i_{t_2} \mapsto i'_{t_2}$ induces an embedding of $\mathbb{R}(\{i_t : t \in S\})$ into $\mathbb{R}(\{i_t : t \in S'\})$. It can then be extended to an automorphism of $\mathbb{O}$ simply by choosing an image for i_r that is orthogonal to $\mathbb{R}(\{i_t : t \in S'\})$, since $i_r \perp \mathbb{R}(\{i_t : t \in S\})$. We know that $i'_r \perp \mathbb{R}(\{i_t : t \in S'\})$, thus i'_r is a valid choice.

φ_τ is also a generalized permutation on $\mathbb{O}$, with associated permutation τ. Also, $\varphi_\tau^{-1} = \varphi_{\tau^{-1}}$ has associated permutation τ^{-1}. We now have the following commutative squares

$$\begin{tikzcd}
\mathbb{O} \arrow[r, "\varphi_\tau"] \arrow[d, "M_{i_{\tau(r)}}"'] & \mathbb{O} \arrow[d, "M_{i_r}"] \\
\mathbb{O} \arrow[r, "\varphi_\tau"'] & \mathbb{O}
\end{tikzcd}
\qquad
\begin{tikzcd}
S' \arrow[r, "\tau"] \arrow[d, "\tau^{-1}\sigma\tau"'] & S \arrow[d, "\sigma"] \\
S'^c \arrow[r, "\tau"'] & S^c
\end{tikzcd}$$

The commutativity of the left diagram follows from

$$\varphi_\tau \circ L_{i_r}(\alpha) = \varphi_\tau(i_r\alpha) = \varphi_\tau(i_r)\varphi_\tau(\alpha) = i_{\tau(r)}\varphi_\tau(\alpha) = L_{i_{\tau(r)}} \circ \varphi_\tau(\alpha)$$

and

$$\varphi_\tau \circ R_{i_r}(\alpha) = \varphi_\tau(\alpha i_r) = \varphi_\tau(\alpha)\varphi_\tau(i_r) = \varphi_\tau(\alpha)i_{\tau(r)} = R_{i_{\tau(r)}} \circ \varphi_\tau(\alpha).$$

The associated permutation of $M_{i_{\tau(r)}} = \varphi_\tau^{-1} \circ M_{i_r} \circ \varphi_\tau$ is $\tau^{-1}\sigma\tau$, which has the desired properties $\tau^{-1}\sigma\tau(S') = S'^c$ and $\tau^{-1}\sigma\tau(S'^c) = S'$. Therefore, the proposition holds for an arbitrary halving set S and $r \in S^c$. □

4. Rational Composition Algebras

An observation regarding rational composition algebras can be made that is similar to Proposition 3.

Lemma 8. Let Q be a rational composition algebra. Then Q has an orthogonal basis, and there is a unique extension of Q to a real composition algebra.

Proof. If V is an inner product space over $\mathbb{Q}$ of finite dimension n, then a modified version of the Gram-Schmidt process produces an orthogonal (not necessarily orthonormal) basis as follows. Choose a basis $\{v_1, \ldots, v_n\}$ for V over $\mathbb{Q}$. Suppose that we have found a pairwise orthogonal list $\{u_1, \ldots, u_k\}$, with $1 \leq k < n$, that spans the same subspace as $\{v_1, \ldots, v_k\}$. Define

$$u_{k+1} = v_{k+1} - \frac{[v_{k+1}, u_1]}{[u_1]} u_1 - \cdots - \frac{[v_{k+1}, u_k]}{[u_k]} u_k.$$

Taking the inner product of u_{k+1} with any of $u_1, \ldots, u_k$ shows that adding u_{k+1} to this list produces a new list that is still pairwise orthogonal. Repeating this process will eventually yield an orthogonal basis. Thus, Q has an orthogonal basis.

Taking an orthogonal basis $\{\beta_1, \ldots, \beta_n\}$ for Q, we may embed Q as a subset of $\mathbb{R}^n$ by the linear map induced by $\beta_j \to \sqrt{[\beta_j]} e_j$, where e_j is the jth standard basis vector in $\mathbb{R}^n$. For now, we will simply identify Q with this subset, noting that the inner product on Q is the restriction of the standard Euclidean inner product to this subset.

The Euclidean distance on $\mathbb{R}^n$, which is the squareroot of Q's norm function, makes Q into a metric space. This metric induces the product metric on $Q \times Q$. Fix a value $\beta \in Q$, and let α_k be a Cauchy sequence in Q. We aim to show that $\alpha_k\beta$ is Cauchy as well, showing that the right multiplication map is continuous. This is obvious if $\beta = 0$, so assume otherwise. Given $\epsilon > 0$, there is some N such that $|\alpha_j - \alpha_k| < \frac{\epsilon}{|\beta|}$ whenever $j, k > N$. From the composition law in Q, we have

$$|\alpha_j\beta - \alpha_k\beta| = |\alpha_j - \alpha_k||\beta| < \epsilon$$

whenever $j, k > N$, and so the result follows. A symmetric argument shows that the left multiplication map is continuous, as well. Therefore, the multiplication map $Q \times Q \to Q$ is continuous, because it is continuous in both of its components.

Since Q is a rational vector space of dimension n embedded in $\mathbb{R}^n$, it is dense in $\mathbb{R}^n$. Thus we may, for any $\alpha, \beta \in \mathbb{R}^n \setminus Q$, take a sequence (α_k, β_k) in $Q \times Q$ converging to (α, β). By the continuity of multiplication, $\alpha_k\beta_k$ is Cauchy, and so converges to some point in $\mathbb{R}^n$. Define the product $\alpha\beta$ to be this point. The composition law holds for α and β because the distance function is continuous, thus

$$|\alpha\beta| = \lim_{k\to\infty} |\alpha_k\beta_k| = \lim_{k\to\infty} |\alpha_k| \lim_{k\to\infty} |\beta_k| = |\alpha||\beta|.$$

We have successfully extended Q to a real composition algebra for which the underlying vector space is $\mathbb{R}^n$. If we had attempted to extend the multiplication in any other way, the resulting multiplication function $\mathbb{R}^n \times \mathbb{R}^n \to \mathbb{R}^n$ could not be continuous. However, the same argument which showed that the multiplication operation on Q is continuous shows that the multiplication on $\mathbb{R}^n$ must, also, be continuous (just change all mentions of Q in the argument to $\mathbb{R}^n$). Therefore, this extension is unique. □

What this lemma shows is that, if Q is a rational composition algebra, it lies within some real composition algebra of the same dimension. Specifically, it must lie within one of the four identified by Hurwitz's Theorem and can be obtained by restricting one of these algebras to a closed subset that forms a $\mathbb{Q}$-vector space.

Theorem 9. Every rational composition algebra is of the form $\mathbb{Q}$, $\mathbb{Q}(\sqrt{q}i)$, $\mathbb{Q}(\sqrt{q}i, \sqrt{r}j)$, or $\mathbb{Q}(\sqrt{q}i_0, \sqrt{r}i_1, \sqrt{s}i_2)$, where $q, r, s \in \mathbb{Q}$ have squarefree numerators and denominators.

Proof. Let Q be a rational composition algebra of dimension $n = 1, 2, 4$, or 8. In the proof of Lemma 8, we show that Q can be embedded into $\mathbb{R}^n$ with an orthonormal basis of the form $\{\sqrt{q_t}e_t\}_{t\in S}$, where S is an index set of size n. Clearly, we may take the q_t to have squarefree numerators and denominators. Furthermore, we can extend the multiplication on Q to $R = \mathbb{R}(\{\sqrt{q_t}e_t\}_{t\in S})$ in a manner that makes R into a real composition algebra. By Theorem 5, there is an isomorphism of either $\mathbb{R}$, $\mathbb{C}$, $\mathbb{H}$, or $\mathbb{O}$ onto R taking $\{1\}$, $\{1, i\}$, $\{1, i, j\}$, or $\{i_\infty, i_0, i_1, i_2\}$ onto a subset of $\{e_t\}_{t\in S}$. This isomorphism restricts to an isomorphism of $\mathbb{Q}$, $\mathbb{Q}(\sqrt{q}i)$, $\mathbb{Q}(\sqrt{q}i, \sqrt{r}j)$, or $\mathbb{Q}(\sqrt{q}i_0, \sqrt{r}i_1, \sqrt{s}i_2)$ onto $Q = \mathbb{Q}(\{\sqrt{q_t}e_t\}_{t\in S})$ where $q, r, s \in \mathbb{Q}$ have squarefree numerators and denominators. □

5. Orders and Lattices

In working with nonassociative algebras, we often look for weaker forms of the associativity law. One such form is called *power associativity*, which requires any bracketing of the multiplication in a product containing multiple factors of a single element to produce the same result. For example, we should have $x(xx) = (xx)x$ as a result of power associativity. This ensures that exponentiation (with a positive integer exponent) is well-defined, and so polynomials with coefficients in the algebra induce functions on the algebra. If the algebra is also unital, then x^0 can be defined to be 1, and polynomials with integer coefficients induce functions, as well.

We have seen that composition algebras are alternative, which implies they are power associative. They are by definition unital. If α is an element of a composition algebra over F, then α satisfies the polynomial

$$x^2 - 2\operatorname{Re}(\alpha)x + [\alpha] \in F[x]$$

since

$$\alpha^2 - 2\operatorname{Re}(\alpha)\alpha + [\alpha] = \alpha^2 - (\alpha + \overline{\alpha})\alpha + [\alpha] = 0.$$

We call $2\operatorname{Re}(\alpha)$ the *trace* of α. The only case in which α satisfies a linear polynomial with coefficients in F is when $\alpha \in F$, in which case it satisfies $x - \alpha$. There is always a unique monic polynomial over F of minimal degree having α as a root. To avoid trying to generalize the classical theory of polynomials over fields to a context without commutativity or associativity, consider the following ad hoc proof of this fact.

If $\alpha \in F$, clearly the only linear polynomial it satisfies is $x - \alpha$. Otherwise, α satisfies a monic quadratic polynomial $x^2 + ax + b$ (in particular, the one given above). Suppose $x^2 + a'x + b'$ is another. Then

$$\alpha^2 + a\alpha + b = \alpha^2 + a'\alpha + b'$$

so $a\alpha + b = a'\alpha + b'$. If $a \neq a'$, we have $\alpha = \frac{b'-b}{a-a'} \in F$, a contradiction; so $a = a'$. It follows also that $b = b'$. Call this unique monic polynomial the *minimal polynomial* of α over $\mathbb{R}$.

Definition 10. Let Q be a rational composition algebra. A subring $\mathcal{O} \subseteq Q$ is called an *order* of Q if every element $\alpha \in \mathcal{O}$ has integral norm and trace. We call elements of an order *integral.* A *maximal order* is an order that is maximal with respect to inclusion.

Definition 11. A free $\mathbb{Z}$-submodule of $\mathbb{R}^n$, of rank $\leq n$, is called a *lattice* if it has a basis that is linearly independent over $\mathbb{R}$. A lattice is of *full rank* if it spans $\mathbb{R}^n$ over $\mathbb{R}$.

We are about to prove that an order of a rational comosition algebra of dimension n is a lattice in $\mathbb{R}^n$. For the proof of this fact, we will invoke exercise 5 from Chapter III of Lang's Algebra [11], which states that an additive subgroup of $\mathbb{R}^n$ is a free abelian group with at most n generators if every bounded region of $\mathbb{R}^n$ contains only a finite number of elements of M. In the standard proof of the exercise, the generating set is shown to be free by establishing its linear independence over $\mathbb{R}$, meaning that the additive subgroup must be a lattice. We will actually prove something more general than what is currently needed, however the following proposition will later be employed in its full generality.

Proposition 12. Let $\mathcal{M} \subseteq \mathbb{R}^n$ be such that $0 \in \mathcal{M}$ and $[\alpha - \beta] \in \mathbb{Z}$ for all $\alpha, \beta \in \mathcal{M}$. Then the additive group $\mathbb{Z}[\mathcal{M}]$ generated by $\mathcal{M}$ also satisfies $[\alpha - \beta] \in \mathbb{Z}$ for all $\alpha, \beta \in \mathbb{Z}[\mathcal{M}]$, and contains finitely many points in any bounded region of $\mathbb{R}^n$. Therefore, $\mathbb{Z}[\mathcal{M}]$ is a lattice in $\mathbb{R}^n$. In particular, an order of an n-dimensional rational composition algebra is a lattice in $\mathbb{R}^n$.

Proof. Let $\alpha \in \mathbb{Z}[\mathcal{M}]$, so that $\alpha = \sum_{t=1}^{m} \alpha_t$ for some $\alpha_1, \ldots, \alpha_m \in \mathcal{M}$. We have

$$[\alpha] = \left[\sum_{t=1}^{m} \alpha_t\right] = \left[\sum_{t=1}^{m} \alpha_t, \sum_{t=1}^{m} \alpha_t\right] = \sum_{s=1}^{m}\sum_{t=1}^{m} [\alpha_s, \alpha_t] = \sum_{1\leq s\leq t\leq m} 2\,[\alpha_s, \alpha_t]\,.$$

Since $[\alpha_s] = [\alpha_s - 0] \in \mathbb{Z}$ and $[\alpha_s - \alpha_t] = [\alpha_s] + [\alpha_t] - 2\,[\alpha_s, \alpha_t] \in \mathbb{Z}$ for all $s, t \in \mathbb{Z}$, we know $2\,[\alpha_s, \alpha_t] \in \mathbb{Z}$ for all $s, t \in \mathbb{Z}$. Therefore, $[\alpha] \in \mathbb{Z}$. Since α is a subgroup, we know that $\alpha - \beta \in \mathbb{Z}[\mathcal{M}]$ for any $\beta \in \mathbb{Z}[\mathcal{M}]$, thus $[\alpha - \beta] \in \mathbb{Z}$ as well.

Let R be any bounded region of $\mathbb{R}^n$. We aim to show that $\mathbb{Z}[\mathcal{M}] \cap R$ is finite. We may assume R is closed, since R is certainly contained within its closure and hence so is $\mathbb{Z}[\mathcal{M}] \cap R$. Let $\mathcal{C}$ be the set of all open balls in $\mathbb{R}^n$ of radius $\frac{1}{2}$. $\mathcal{C}$ is an open cover of the compact set R, hence it has a finite subcover $\mathcal{C}' \subset \mathcal{C}$ containing $N \in \mathbb{Z}_{>0}$ elements. If $B \in \mathcal{C}'$, then B may contain at most one point of $\mathbb{Z}[\mathcal{M}]$, since we have $[\alpha - \beta] \in \mathbb{Z}$, and thus $|\alpha - \beta| \geq 1$, for all $\alpha, \beta \in \mathbb{Z}[\mathcal{M}]$. Therefore, $\mathbb{Z}[\mathcal{M}] \cap R$ contains at most N points. By the referenced exercise from Lang, we see that $\mathbb{Z}[\mathcal{M}]$ must be a lattice in $\mathbb{R}^n$. □

Some authors require an order to have full rank as a lattice. We will not use this requirement, since it destroys the usefulness of the notion of a suborder. However, even if an order $\mathcal{O}$ does not have full rank, it would have full rank in the subspace $\mathbb{R}\mathcal{O}$ which it spans over $\mathbb{R}$. Therefore, the difference in these definitions is more or less synthetic.

If Q_1 and Q_2 are rational composition algebras, and $\mathcal{O}_1 \subset Q_1$ and $\mathcal{O}_2 \subset Q_2$ are orders, define an *order embedding* to be a map $\mathcal{O}_1 \to \mathcal{O}_2$ which is both a homomorphism of nonassociative rings and an isometry. We will spare ourselves from using the word "homomorphism" to describe such a map because an isometry is always injective. If an embedding exists, we will say that $\mathcal{O}_1$ *embeds* in $\mathcal{O}_2$. If an embedding is also surjective, we may call it an isomorphism of orders. If $\mathcal{O}_1 \subseteq \mathcal{O}_2$, we will say that $\mathcal{O}_1$ is a *suborder* of $\mathcal{O}_2$.

In the following sections, we construct several orders of rational composition algebras. The propositions that follow are stated in [3], but usually without proof, so the proofs are presented here.

Complex Orders. Consider the quadratic field extension $\mathbb{Q}(\sqrt{-D})$ for a positive squarefree integer D. The subring $\mathbb{Z}[\sqrt{-D}]$ forms an order, which is maximal if and only if $D \not\equiv 3 \pmod 4$. If $D \equiv 3 \pmod 4$, then this order is contained in the maximal order $\mathbb{Z}[\omega_D]$, where $\omega_D = \frac{-1+\sqrt{-D}}{2}$. Some equivalent formulations are

$$\mathbb{Z}[\omega_D] = \mathbb{Z}[\sqrt{-D}] \cup \left(\mathbb{Z}[\sqrt{-D}] + \omega_D\right) = \left\{\frac{a + b\sqrt{-D}}{2} \mid a \equiv b \pmod 2\right\}.$$

Some of these maximal orders have been named: the Gaussian integers $\mathbb{Z}[i]$, the Eisenstein integers $\mathbb{Z}[\omega_3]$, and the Kleinian integers $\mathbb{Z}[\omega_7]$. A great deal of information about these rings can be found in [2].

Quaternion Orders. Consider the algebra of quaternions with rational coordinates $\mathbb{Q}[i, j] = \mathbb{Q}(i, j) \subseteq \mathbb{H}$, which is a division ring because the law of composition gives us $\alpha^{-1} = \frac{\overline{\alpha}}{[\alpha]} \in \mathbb{Q}[i, j]$ for any $\alpha \in \mathbb{Q}[i, j]$. The most natural order to consider is the set of *Lipschitz integral quaternions* $\mathbf{L} = \mathbb{Z}[i, j] = \{a + bi + cj + dk \mid a, b, c, d \in \mathbb{Z}\}$, which can be identified via isometry with the $\mathbb{Z}^4$ lattice. However, this naive choice is not maximal, for it sits inside the larger order of *Hurwitz integral quaternions*

$$\mathbf{H} = \mathbb{Z}[i, j, \omega_3] = \left\{\frac{a + bi + cj + dk}{2} \mid a \equiv b \equiv c \equiv d \pmod 2\right\}.$$

It is not hard to check that this order is a subring, and that it is formed from the Lipschitz quaternions by adjoining the element $\frac{1}{2}(-1 + i + j + k)$, which is a primitive cube root of unity and can hence be identified with ω_3. The fact that it is maximal follows from arguments similar to those in the proofs of Lemmas 13 and 14 in the next section, which proves that if α is an element of an order of $\mathbb{Q}(i, j)$ containing $\mathbf{L}$, then either every component of α is an integer or every component is a proper half integer. This also implies that $\mathbf{L}$ and $\mathbb{H}$ are the *only* orders of $\mathbb{Q}(i, j)$ containing $\mathbf{L}$.

Geometrically, $\mathbf{H}$ can be identified via isometry with the lattice $\mathbb{Z}^4 \cup \left(\mathbb{Z}^4 + (\frac{1}{2}, \frac{1}{2}, \frac{1}{2}, \frac{1}{2})\right)$, which is visualized by taking the $\mathbb{Z}^4$ lattice and placing a point at the center of every unit hypercube formed by lattice points. An important fact is that the number of Hurwitz quaternions of norm n is 24 times the sum of the odd divisors of n.

Octonion Orders. Consider the algebra of octonions with rational coordinates $\mathbb{Q}(i_0, i_1, i_2) \subseteq \mathbb{O}$. Again, the naive order $\mathbf{G} = \mathbb{Z}[i_0, i_1, i_2] \cong \mathbb{Z}^8$, called the *Gravesian Octaves*, is not maximal. The following lemmas will narrow down the possibilities for larger orders. Let $\mathcal{O}$ be an order of $\mathbb{Q}(i_0, i_1, i_2)$ containing $\mathbf{G}$. The following two lemmas are from [3].

Lemma 13. Let $\alpha \in \mathcal{O}$. The coordinates of α are all in $\frac{1}{2}\mathbb{Z}$.

Proof. If a_r is the rth coordinate of α, then $2a_r = -2\operatorname{Re}(\alpha \cdot i_r) \in \mathbb{Z}$. □

If $\alpha = a_\infty i_\infty + a_0 i_0 + \cdots + a_6 i_6 \in \mathcal{O}$, then there is a set $S \subseteq \{\infty, 0, 1, 2, 3, 4, 5, 6\}$ such that a_r is a proper half integer if $r \in S$ and a_r is an integer otherwise. We call S the *halving set* of α, and we also define $S^c = \{\infty, 0, 1, 2, 3, 4, 5, 6\} \setminus S$. Note also that if $\mathcal{O}$ contains one element with halving set S, then it contains *every* possible element with halving set S. More formally, it contains the set

$$\{a_\infty i_\infty + \cdots + a_6 i_6 : a_r \in \tfrac{1}{2}\mathbb{Z} \setminus \mathbb{Z} \text{ if } r \in S, a_r \in \mathbb{Z} \text{ if } r \in S^c\}.$$

Therefore, if $\mathcal{O}$ contains an element with halving set S, we say also that S is a halving set of $\mathcal{O}$. For convenience, we will write halving sets simply as lists. For example, instead of writing $\{\infty, 0, 1, 3\}$, we will just write $\infty 013$. We also choose to denote the set $\infty 0123456$ by Ω.

Lemma 14. The size of every halving set of $\mathcal{O}$ is divisible by 4.

Proof. Let α have exactly m components which are half integers. Then, for some odd integers $a_1, \dots, a_m$ and some integers $a_{m+1}, \dots, a_8$, we have

$$[\alpha] = \left(\frac{a_1}{2}\right)^2 + \cdots + \left(\frac{a_m}{2}\right)^2 + a_{m+1}^2 + \cdots + a_8^2 = \frac{a_1^2 + \cdots + a_m^2}{4} + a_{m+1}^2 + \cdots + a_8^2 \in \mathbb{Z}$$

therefore 4 divides $a_1^2 + \cdots + a_m^2$. But each of these terms is congruent to 1 (mod 4), thus 4 divides m. □

We now understand that halving sets of $\mathcal{O}$ always consist of 0, 4, or 8 indices. This means that there are at most $1 + \binom{8}{4}$ possible halving sets, in addition to $\emptyset$, that $\mathcal{O}$ can have. Therefore, $2^{1+\binom{8}{4}}$ is an upper bound for the number of orders of $\mathbb{Q}(i_0, i_1, i_2)$ containing $\mathbf{G}$. However, it is possible that some combinations of halving sets will not result in subrings, and it is also possible that some of the resulting orders will be isomorphic to each other. The remainder of this discussion is dedicated to sorting out these details.

It is easy to check that

$$\mathbf{K} = \{\tfrac{1}{2}(a_\infty i_\infty + a_0 i_0 + \cdots + a_6 i_6) \mid a_\infty \equiv a_0 \equiv \cdots \equiv a_6 \pmod 2\}.$$

is an order containing $\mathbf{G}$. Its halving sets are $\emptyset$ and Ω, and it can be formed by adjoining $\frac{1}{2}(-i_\infty + i_0 + i_1 + i_2 + i_3 + i_4 + i_5 + i_6)$ to $\mathbf{G}$. The minimal polynomial of this element is $x^2 + x + 2$, which is also the minimal polynomial of the Kleinian integer $\omega_7 = \frac{-1+\sqrt{-7}}{2}$. Because of this, Conway and Smith refer to this order as the *Kleinian integers*, and we can think of it as $\mathbf{K} = \mathbb{Z}[i_0, i_1, i_2, \omega_7]$.

There are exactly seven 4-element sets S for which $\{i_s : s \in S\}$ is the basis of a quaternion subalgebra. They are the sets $\{\infty, n, n+1, n+3\} \pmod 7$ for $0 \leq n \leq 6$, each of which corresponds to one of the lines on the Fano plane. We will soon be interested in situations where such an S occurs as a halving set, so we name these seven 4-element sets the *quaternion halving sets*. Below, we list these sets along with their complements, as well as the sets $\emptyset$ and Ω.

$\emptyset$	$\infty 013$	$\infty 124$	$\infty 235$	$\infty 346$	$\infty 450$	$\infty 561$	$\infty 602$
Ω	2456	0356	0146	0125	1236	0234	1345

Conway and Smith call this collection of 16 sets the ∞-sets for reasons that will soon be explained.

For each of the seven quaternion halving sets S, we define the lattice

$$\{a_\infty i_\infty + a_0 i_0 + \cdots + a_6 i_6 \mid a_s \equiv a_t \pmod 2 \text{ if } s, t \in S \text{ or } s, t \in S^c\}.$$

As modules, these are all isomorphic to $\mathbf{H} \oplus \mathbf{H}$, so we will denote the lattice associated with S by $(\mathbf{H} \oplus \mathbf{H})_S$.

Proposition 15. Let S be a quaternion halving set. $(\mathbf{H} \oplus \mathbf{H})_S$ is a subring of $\mathbb{Q}(i_0, i_1, i_2)$, and is the smallest order containing $\mathbf{G}$ having S or S^c as a halving set. If T is another quaternion halving set, then $(\mathbf{H} \oplus \mathbf{H})_S \cong (\mathbf{H} \oplus \mathbf{H})_T$ as rings.

Proof. It is clear that $(\mathbf{H}\oplus\mathbf{H})_S$ is closed under addition. Now, let $\alpha\in(\mathbf{H}\oplus\mathbf{H})_S$. By Proposition 7, multiplying α by a unit i_r, where $r\in S$, does nothing but permute the components of α in S and possibly change their signs. It does the same to the components in S^c. Multiplying by a unit i_r with $r\notin S$ interchanges the halving set S with its complement, then permutes the components of each and possibly changes signs. More formally, if $r\in S$ then there are permutations σ and τ of Ω for which $\sigma(S)=\tau(S)=S$, $\sigma(S^c)=\tau(S^c)=S^c$, and the following equations hold:

$$\left(\sum_{s\in S}a_s i_s+\sum_{s\in S^c}a_s i_s\right)i_r=\sum_{s\in S}\pm a_s i_{\sigma(s)}+\sum_{s\in S^c}\pm a_s i_{\sigma(s)}$$

$$i_r\left(\sum_{s\in S}a_s i_s+\sum_{s\in S^c}a_s i_s\right)=\sum_{s\in S}\pm a_s i_{\tau(s)}+\sum_{s\in S^c}\pm a_s i_{\tau(s)}$$

Similarly, if $r\in S^c$, then the above equations hold for some σ and τ such that $\sigma(S)=\tau(S)=S^c$ and $\sigma(S^c)=\tau(S^c)=S$. Therefore, αi_r and $i_r\alpha$ both have halving set $\emptyset, S, S^c$, or Ω. Scaling α by an integer can only change its halving set if that integer is even, in which case the set becomes $\emptyset$. Applying these facts along with linearity, we see that multiplying α by a Gravesian integer results in an element with one of these four halving sets.

Next, let $r\in S^c$ and consider the element

$$\gamma=\sum_{s\in S}\frac{1}{2}i_s.$$

Together with the Gravesian integers, γ and $i_r\gamma$ additively generate the double Hurwitzian ring of halving set S. Thus, we need only show that the pairwise products of these two elements are in $\mathbb{R}$. γ is an element of an order isomorphic to the Hurwitz integral quaternions, and so γ^2 has halving set S or Ω (in fact, it has the same halving set as γ). Since $\operatorname{Re}(i_r\gamma)=0$, we have $(i_r\gamma)^2=-[i_r\gamma]=-1$. Because $\mathbb{O}$ is alternative, the subalgebra generated by i_r and γ is associative. Thus, $(i_r\gamma)\gamma=i_r\gamma^2\in(\mathbf{H}\oplus\mathbf{H})_S$ and $\gamma(i_r\gamma)=(-i_r^2)\gamma(i_r\gamma)=i_r(i_r\gamma)^2\in(\mathbf{H}\oplus\mathbf{H})_S$, since we have just confirmed that $\gamma^2,(i_r\gamma)^2\in(\mathbf{H}\oplus\mathbf{H})_S$ and $(\mathbf{H}\oplus\mathbf{H})_S$ is closed under multiplication by the Gravesian integer i_r. This proves that $(\mathbf{H}\oplus\mathbf{H})_S$ is an order. It is clear that it must be the smallest subring containing $\mathbf{G}$ with either of S or S^c as a halving set.

For the last statement, let T be another quaternion halving set. If $S=\infty abc$ and $T=\infty a'b'c'$, where $i_a i_b=i_c$ and $i_{a'}i_{b'}=i_{c'}$, then clearly the map taking i_a to $i_{a'}$ and i_b to $i_{b'}$ extends to a unique ring isomorphism. □

Following Conway and Smith, we call this order the *double Hurwitzian ring*, since it is unique up to isomorphism. As a matter of convenience, define $i_{abcd}=\frac{1}{2}(i_a+i_b+i_c+i_d)$. If the halving set of an integral octonion is an ∞-set, we call it an ∞*-integer.* J. Kirmse had claimed that the ∞-integers form a maximal order. While they do form an additive group, it was later was noticed by Coxeter that they are not closed under multiplication [4]. For instance, $i_{\infty026}i_{\infty013}=i_{0235}$ is not an ∞-integer. Even worse, the product $i_{0235}i_{\infty235}=\frac{1}{4}(-3i_\infty+i_0-i_1+i_2+i_3-i_4+i_5+i_6)$ is not even integral. This blunder has come to be known as "Kirmse's Mistake," and actually appears in several published papers.

Although the ∞-integers do not form an order, there is a simple adjustment that can be made which does result in a subring: for any $n\in\mathbb{Z}_7$, construct the *n-integers* by interchanging ∞ with n in every ∞-set. For instance, the 0-sets are

$\emptyset$	$\infty013$	0124	0235	0346	$\infty045$	0156	$\infty026$
Ω	2456	$\infty356$	$\infty146$	$\infty125$	1236	$\infty234$	1345

Observe that any given pair of these halving sets shares either 0 or 2 elements in common. If they share 2 elements, then the 4 they do not share form another halving set on this list. This implies that the 0-integers are additively closed. Even more tedious to verify is that the products $i_r i_{abcd}$, $i_{abcd}i_r$, and $i_{abcd}i_{efgh}$ are 0-integers if $abcd$ and $efgh$ are 0-sets and $r\in\Omega$. Once this has been confirmed, however, we see that the 0-integers are closed, since they are additively generated by elements of the form i_r and i_{abcd}, where $abcd$ is a 0-set. This leads us to the final proposition of this section:

Proposition 16. The n-integers are a maximal order of $\mathbb{Q}(i_0,i_1,i_2)$ containing the Gravesian integers. All of these orders are isomorphic.

Proof. See [3], section 9.2. □

For a more in depth discussion of this topic, please refer to [3]. An noteworthy fact is that the number of octavian integers of norm n is 240 times the sum of the cubes of the divisors of n.

6. Factorization in Quaternion Orders

Recall the rings $\mathbf{L} = \mathbb{Z}[i,j]$ of Lipschitz quaternions and $\mathbf{H} = \mathbb{Z}[i,j,\omega_3]$ of Hurwitz quaternions. It is not hard to see that, for every point $\alpha \in \mathbb{H}$, we can find a point $\beta \in \mathcal{O}$ such that $[\alpha - \beta] \leq \frac{1}{2}$. This proves the following:

Theorem 17 (Division Algorithm)**.** If $\alpha, \delta \in \mathcal{O}$ and $\delta \neq 0$, then there exists $\beta \in \mathbf{H}$ such that

$$\alpha = \delta\beta + \rho$$

and $[\rho] \leq \frac{1}{2}[\delta]$ (and $\beta' \in \mathcal{O}$ such that $\alpha = \beta'\delta + \rho'$ and $[\rho'] \leq \frac{1}{2}[\delta]$).

From this, it is possible to show that, given any factorization $[\alpha] = p_1 \cdots p_n$ of the norm of some $\alpha \in \mathcal{O}$, there is a Hurwitz factorization $\alpha = \pi_1 \cdots \pi_n$ with $[\pi_t] = p_t$ for each t. The Lipschitz quaternions do not satisfy a division algorithm, namely because the point $\frac{1}{2}(1+i+j+k)$ lies a distance of at least 1 from any lattice point. However, Gordon Pall's paper *Arithmetic of Quaternions* does a wonderful job of attacking factorization in this order using the theory of quadratic forms [15]. The following are Theorem 1 and Theorem 7 from that article, and they will be useful in proving the main theorem of this paper. If the components of a Lipschitz quaternion α are not all divisible by p, then α is called *proper* $\pmod p$.

Theorem 18 (Pall)**.** Let $\alpha \in \mathbf{L}$ be proper $\pmod p$ for an odd prime p, and suppose $p \mid [\alpha]$. Then α has a set of exactly eight left divisors of norm p, which is of the form $\{\pm\delta, \pm\delta i, \pm\delta j, \pm\delta k\}$ for some left divisor δ of α. Likewise, it has a set of exactly eight right divisors, which is of the form $\{\pm\delta, \pm i\delta, \pm j\delta, \pm k\delta\}$ for some right divisor δ of α.

Proof. See [15], Theorem 1. □

Note also that if $2 \mid \alpha$, then α still has both a left and a right Lipschitz divisor of norm 2.

Theorem 19 (Pall)**.** Let p be an odd prime. Suppose that $\alpha, \beta \in \mathbf{L}$ are both proper $\pmod p$, but $p \mid [\alpha], [\beta]$. Then α and β share the same left divisors, or the same right divisors, or both, of norm p, if and only if $p \mid [\alpha, \beta]$.

Proof. See [15], Theorem 7. □

From these theorems, we can now prove an important lemma.

Lemma 20. Let p be prime, and let $S \subseteq \mathbf{L}$. Suppose $p \mid [\alpha_s], [\alpha_s - \alpha_t]$ for all $s, t \in \{1, \ldots, n\}$.

(1) If p is odd, then either all elements of S share set of eight left Lipschitz divisors of norm p, or all elements of S share a set of eight right Lipschitz divisors of norm p.
(2) If $p = 2$, every Hurwitz integer of norm 2 is both a left and a right Hurwitz divisor of each $\alpha \in S$.
(3) Let $\alpha \in \mathbf{H}$. If $4 \mid [\alpha]$, then 2 is a Hurwitz divisor of α.

Proof. Let p be an odd prime, and let T be the subset of all elements in S which are proper $\pmod p$. For any $\alpha_1, \alpha_2 \in S$, we know

$$0 \equiv [\alpha_1 - \alpha_2] \equiv [\alpha_1] + [\alpha_2] - 2[\alpha_1, \alpha_2] \equiv -2[\alpha_1, \alpha_2] \pmod p.$$

Since p is odd, $p \mid [\alpha_1, \alpha_2]$. Therefore, α_1 and α_2 have either the same set of left Lipschitz divisors of norm p or the same set of right Lipschitz divisors of norm p.

We will now show that all elements of T share the same set of left Lipschitz divisors of norm p, or all elements of T share the same set of right Lipschitz divisors of norm p. For each $\alpha \in T$, define $\mathcal{C}^L_\alpha$ to be the set of elements that have the same left divisors of norm p as α, and define $\mathcal{C}^R_\alpha$ to be the set of elements that have the same right divisors of norm p as α. By Theorem 19, we must have $\mathcal{C}^L_\alpha \cup \mathcal{C}^R_\alpha = T$ for all $\alpha \in T$. We may assume T is nonempty, else the statement is vacuous. So let $\alpha \in T$ and suppose, for a contradiction, that either $\mathcal{C}^L_\alpha \neq T$ or $\mathcal{C}^R_\alpha \neq T$. Thus, there is some $\beta \notin \mathcal{C}^R_\alpha$ and some $\gamma \notin \mathcal{C}^L_\alpha$. We must then have $\beta \in \mathcal{C}^L_\alpha$ and $\gamma \in \mathcal{C}^R_\alpha$, and so $\mathcal{C}^L_\alpha = \mathcal{C}^L_\beta$ and $\mathcal{C}^R_\alpha = \mathcal{C}^R_\gamma$. Therefore, $\beta \notin \mathcal{C}^R_\alpha = \mathcal{C}^R_\gamma$ and $\gamma \notin \mathcal{C}^L_\alpha = \mathcal{C}^L_\beta$. This means that

β and γ share no left or right divisors of norm p, a contradiction. Thus, either $\mathcal{C}_\alpha^L = T$ or $\mathcal{C}_\alpha^R = T$, and so either all elements share a set of common left divisors of norm p with α, and thus with each other, or all elements share a set of common right divisors of norm p with α, and thus with each other.

Now, let $\alpha \in S \setminus T$, and let θ be one of the common left or right divisors of all the elements in T of norm p. Since α is not proper $\pmod p$, we know $p \mid \alpha$. Thus, $\alpha = p\beta = \theta(\overline{\theta}\beta)$ and $\alpha = \beta p = (\beta\overline{\theta})\theta$ and so θ is both a left and a right divisor of α of norm p. This completes the proof of (1).

The case of $p = 2$ is more or less trivial if we recall that the number of Hurwitz integers of norm n is 24 times the sum of the odd divisors of n. We know if $2 \mid [\alpha]$, then α has both a left and a right divisor of norm 2. However, there are only 24 Hurwitz integers of norm 2, and they are all both left and right associates of each other. So every Hurwitz integer of norm 2 is both a left and a right divisor of α.

The third statement results immediately from this fact, since if $4 \mid [\alpha]$ then $\alpha = \pi_1\pi_2\alpha'$, where $[\pi_1] = [\pi_2] = 2$. But up to unit multiplication, these divisors are conjugates of each other. Therefore, $2 \mid \alpha$. □

The theory of factorization in these orders admits many fascinating results. However, we are ready to develop the central ideas of this paper. We will return to this factorization theory later, in the wider context of the octavian integers.

7. Integer Norm Sets

Definition 21. An *integer norm set* is a subset $\mathcal{M} \subset \mathbb{R}^n$ containing 0 such that $[\alpha - \beta] = |\alpha - \beta|^2 \in \mathbb{Z}$ for all $\alpha, \beta \in \mathcal{M}$. We called $\mathcal{M}$ *planar* if the dimension of the subspace it spans over $\mathbb{R}$ is ≤ 2. If this dimension is 1, we also call $\mathcal{M}$ *collinear.* If X is a subset of $\mathbb{R}^m$ for some m, an *embedding* of $\mathcal{M}$ into X is an isometry $\phi : \mathcal{M} \to \mathbb{R}^m$ such that $\phi(\mathcal{M}) \subseteq X$.

Note that, if we did away with the constraint that an integer norm set contain 0, the resulting differences would be only technical, since a set can always be translated so that one point lies at the origin. A planar integer norm set $\mathcal{M}$ can always be embedded in $\mathbb{C}$, and so we will always treat such an $\mathcal{M}$ as a subset of $\mathbb{C}$. Consider a nondegenerate triangle T with sidelengths a, b, and c. Heron's formula states that the area of T is

$$\begin{aligned} A &= \frac{1}{4}\sqrt{(a+b+c)(a+b-c)(a-b+c)(-a+b+c)} \\ &= \frac{1}{4}\sqrt{-a^4 - b^4 - c^4 + 2(a^2b^2 + a^2c^2 + b^2c^2)}. \end{aligned}$$

Therefore, if $a^2, b^2, c^2 \in \mathbb{Z}$ then the area is of the form $A = \frac{z}{4}\sqrt{D}$ for some squarefree integer D. We call this integer the *characteristic* of the triangle. If $\{0, \alpha, \beta\}$ is an integer norm set, define its area to be the area of the triangle formed by $0, \alpha$, and β, and define its characteristic to be the characteristic of this triangle.

Since an integer norm set $\mathcal{M} \subset \mathbb{R}^n$ satisfies the hypotheses of 12, we know that the additive subgroup $\mathbb{Z}[\mathcal{M}]$ of $\mathbb{R}^n$ generated by $\mathcal{M}$ is a lattice in $\mathbb{R}^n$, and that it, too, is an integer norm set. We will call a basis for $\mathbb{Z}[\mathcal{M}]$ simply a *basis for $\mathcal{M}$*.

Proposition 22. Let $\mathcal{M}$ be a noncollinear planar integer norm set. All nondegenerate triangles formed in $\mathbb{Z}[\mathcal{M}]$ have the same characteristic. If $\{\alpha, \beta\} \subseteq \mathcal{M}$ is a basis for $\mathcal{M}$, then every nondegenerate triangle formed in $\mathcal{M}$ has area at least that of $\{0, \alpha, \beta\}$. In particular, the areas of the triangles formed by any two bases of $\mathcal{M}$ with the origin are equal.

Proof. Let $\{\alpha, \beta\}$ be a basis for $\mathcal{M}$, and let D be the characteristic of $\{0, \alpha, \beta\}$. Suppose $\{0, \gamma, \delta\} \subset \mathbb{Z}[\mathcal{M}]$ forms another nondegenerate triangle. The area of $\{0, \gamma, \delta\}$ is $\frac{1}{2}||\lambda||$, where λ is the linear operator defined by $1 \mapsto \gamma, i \mapsto \delta$, and $||\lambda||$ is the absolute value of its determinant. We know that the linear operator μ defined by $\alpha \mapsto \gamma$, $\beta \mapsto \delta$ has integral determinant, since it is a $\mathbb{Z}$-module homomorphism. The absolute value of the determinant of the linear operator ν defined by $1 \mapsto \alpha$, $i \mapsto \beta$ is $\frac{z}{2}\sqrt{D}$ for some integer z (since it is twice the area of $\{0, \alpha, \beta\}$). Since $\lambda = \mu \circ \nu$, the area of $\{0, \gamma, \delta\}$ is

$$\frac{1}{2}||\lambda|| = \frac{1}{2}||\mu|| \cdot ||\nu|| = \frac{||\mu||z}{4}\sqrt{D}.$$

Since $||\mu|| \in \mathbb{Z}_{\geq 0}$, we know this quantity as at least $\frac{z}{4}\sqrt{D}$ (it is certainly not 0 because γ and δ are linearly independent). Thus, if $\{\gamma, \delta\}$ were also a basis, the area of $\{0, \gamma, \delta\}$ would be at least that of $\{0, \alpha, \beta\}$. This argument is symmetric, however, so the area of $\{0, \alpha, \beta\}$ is at least that of $\{0, \gamma, \delta\}$ as well. Thus, these areas must be equal. □

If $\mathcal{M}$ is a noncollinear planar integer norm set, we define the characteristic of $\mathcal{M}$ to be the characteristic of any triangle formed in $\mathcal{M}$. If $\mathcal{M}$ is collinear, then the characteristic of $\mathcal{M}$ is undefined. Any integer norm triangle formed in $\mathbb{Q}(\sqrt{-D})$ necessarily has characteristic D, since its area will be of the form

$$\frac{1}{2}\left|\begin{pmatrix} a & c \\ b\sqrt{D} & d\sqrt{D} \end{pmatrix}\right| = \frac{ad - bc}{2}\sqrt{D}$$

and so it is natural to ask whether a planar integer norm set $\mathcal{M}$ of characteristic D can be embedded in $\mathbb{Q}(\sqrt{-D})$. This question is not difficult to answer.

Proposition 23. Let $\mathcal{M} \subset \mathbb{C}$ be an integer norm set with characteristic D or of undefined characteristic. $\mathcal{M}$ embeds in $\mathbb{Q}(\sqrt{-D})$ if and only if there is a rotation ϕ about the origin such that $\phi(\alpha) \in \mathbb{Q}(\sqrt{-D})$ for some nonzero $\alpha \in \mathcal{M}$.

Proof. See [7], Proposition 3. □

In the cited paper, the above theorem is actually stated for the case where $\mathcal{M}$ is finite and no degenerate triangle can be formed by any 3 points in $\mathcal{M}$. However, the statement easily extends to the general case. Suppose $\mathcal{M} \subset \mathbb{C}$ is an integer norm set, and that there is an element $\alpha \in \mathcal{M}$ such that $\phi(\alpha) \in \mathbb{Q}(\sqrt{-D})$. If $\beta \in \mathcal{M}$ is not collinear with α, then by the proposition, ϕ embeds $\{0, \alpha, \beta\}$. Thus, ϕ embeds every point of $\mathcal{M}$ that is not collinear with α. Consider now the case of a point γ collinear with α. Letting $\{\delta\}$ be a basis for $\mathbb{Z}[\{\alpha, \gamma\}]$, we see that α and γ must be integer multiples of δ. Therefore, $\gamma = c\alpha$ for some rational number c. Thus, $\phi(\gamma) = c\phi(\alpha) \in \mathbb{Q}(\sqrt{-D})$. So ϕ necessarily embeds all of $\mathcal{M}$.

More interesting is the question of whether $\mathcal{M} \subseteq \mathbb{Q}(\sqrt{-D})$ can be embedded in $\mathcal{O}_{\mathbb{Q}(\sqrt{-D})}$. The answer to this question is more complicated. For now, assume $\mathcal{M}$ is finite and that no degenerate triangle can be formed in its points. Given an ideal $\mathfrak{m}$ of $\mathbb{Q}(\sqrt{-D})$, the set $\overline{\mathfrak{m}} = \{\overline{\alpha} \mid \alpha \in \mathfrak{m}\}$ also forms an ideal, called the conjugate of $\mathfrak{m}$. Also, the product $\mathfrak{m}\overline{\mathfrak{m}}$ will be principal, and any of its generators will have the same norm. Thus, we define $[\mathfrak{m}]$ to be the norm of any generator of $\mathfrak{m}$. Both the conjugation and norm operators distribute over ideal multiplication. It turns out that, if $\mathcal{M}$ is written as $\{0, \frac{\alpha_1}{r}, \ldots, \frac{\alpha_n}{r}\}$ with $r \in \mathbb{Z}^+$ as small as possible, then $(r) = \mathfrak{m}\overline{\mathfrak{m}}$ and $(\alpha_t) = \mathfrak{m}^2\mathfrak{a}_t$ for some ideals $\mathfrak{m}, \mathfrak{a}_1, \ldots, \mathfrak{a}_n \subseteq \mathcal{O}_{\mathbb{Q}(\sqrt{-D})}$, where $\mathfrak{m} \neq \overline{\mathfrak{m}}$. In this language, the following theorem answers this question.

Theorem 24. A finite integer norm set $\mathcal{M} \subset \mathbb{Q}(\sqrt{-D})$ containing no degenerate triangles embeds in $\mathcal{O}_{\mathbb{Q}(\sqrt{-D})}$ if and only if there is an ideal $\mathfrak{b}$ such that $\mathfrak{b} \mid \mathfrak{a}_1 + \cdots + \mathfrak{a}_n$ and $\mathfrak{m}^2\mathfrak{b}^2$ is principal. In particular, $\mathcal{M}$ embeds in $\mathcal{O}_{\mathbb{Q}(\sqrt{-D})}$ if the square of every ideal is principal.

Proof. See [7], Theorem 1. □

In the case that $\mathcal{M}$ is *primitive*, meaning the greatest common divisor of $\{[\alpha - \beta] \mid \alpha, \beta \in \mathcal{M}\}$ is 1, we will have $\mathfrak{c}_1 + \cdots + \mathfrak{c}_n = 1$. Therefore, the condition reduces to having $\mathfrak{a}^2$ be principal (see [7], Theorem 2). Further, in the case where $\mathcal{O}_{\mathbb{Q}(\sqrt{-D})}$ is a PID, we have an even stronger statement, which requires no assumption that $\mathcal{M}$ embeds first in $\mathbb{Q}(\sqrt{-D})$.

Proposition 25. Suppose $\mathcal{M} \subseteq \mathbb{C}$ is primitive of characteristic D, and that $\mathcal{O}_{\mathbb{Q}(\sqrt{-D})}$ is a PID. Then $\mathcal{M}$ embeds in $\mathcal{O}_{\mathbb{Q}(\sqrt{-D})}$.

Proof. See [7], Theorem 3. □

Again, this last proposition is actually stated in [7] under the hypothesis that $\mathcal{M}$ is finite and noncollinear, and no degenerate triangles can be formed in its points. However, the proof of the theorem can easily be seen not to apply also to the case where $\mathcal{M}$ is of the form $\{0, \alpha\}$. Additionally, our next theorem shows that all of these conditions are unnecessary, since an infinite primitive integer norm set is always generated by a primitive basis $\mathcal{B}$, meaning that the elements of the set $\{[\alpha - \beta] : \alpha \in \mathcal{B},$ and $\beta \in \mathcal{B}$ or $\beta = 0\}$ are relatively prime.

Theorem 26. Let $\mathcal{M} \subset \mathbb{R}^n$ be any integer norm pointset, and let $\mathcal{B}$ be a basis for $\mathcal{M}$. If A is an additive subgroup of $\mathbb{R}^m$, then $\mathcal{M}$ embeds in A if and only if $\mathcal{B} \cup \{0\}$ embeds in A.

Proof. $\mathcal{M}$ and $\mathcal{B} \cup \{0\}$ additively generate each other, therefore an embedding of either one of them must generate an embedding of the other. □

Returning to the general case, if there is an ideal of $\mathcal{O}_{\mathbb{Q}(\sqrt{-D})}$ whose square is nonprincipal, then we are able to construct an integer norm triangle in $\mathbb{Q}(\sqrt{-D})$ (in fact, with two sides integral) that does *not* embed in $\mathcal{O}_{\mathbb{Q}(\sqrt{-D})}$. Thus, the statement "every $\mathcal{M} \subseteq \mathbb{Q}(\sqrt{-D})$ embeds in $\mathcal{O}_{\mathbb{Q}(\sqrt{-D})}$" is equivalent to "the square of every ideal of $\mathcal{O}_{\mathbb{Q}(\sqrt{-D})}$ is principal," which is in turn equivalent to the ideal class group $C(\mathcal{O}_{\mathbb{Q}(\sqrt{-D})})$ being a direct sum of cyclic groups of order 2 (see [7], Proposition 4). However, assuming the Generalized Riemann Hypothesis, there are only 65 square-free integers D for which the class group has this structure [7]. Therefore, we have an embedding theorem that characterizes almost none of the integer norm sets in existence.

Further, there is an entire class of integer norm sets which do not even embed in $\mathbb{Q}(\sqrt{-D})$. For instance, consider a triangle with sides $\sqrt{2}$, $\sqrt{5}$, and $\sqrt{7}$, which has characteristic 10. If this triangle were to embed in $\mathbb{Q}(\sqrt{-10})$, then by our embedding theorem it would have to embed in $\mathbb{Z}[\sqrt{-10}]$ as well, since the class group of this ring is $\mathbb{Z}_2$. However, $a^2 + 10b^2 = 2$ has no integer solutions, so this is impossible. If $\mathcal{M}$ is a planar integer norm pointset of characteristic D or undefined characteristic, we cannot in general be sure whether $\mathcal{M}$ embeds in $\mathbb{Q}(\sqrt{-D})$. However, the following proposition will help us determine this in certain cases.

Theorem 27. Let D be a positive squarefree integer. The following are equivalent.

(1) For all positive integers n, $\mathbb{Q}(\sqrt{-D})$ contains an element of norm n only if $\mathcal{O}_{\mathbb{Q}(\sqrt{-D})}$ does as well.
(2) $C(\mathcal{O}_{\mathbb{Q}(\sqrt{-D})}) \cong \mathbb{Z}_2^k$ for some $k \geq 0$.

Proof. We begin with $2 \implies 1$. Suppose $C(\mathcal{O}_{\mathbb{Q}(\sqrt{-D})}) \cong \mathbb{Z}_2^k$. If $\alpha \in \mathbb{Q}(\sqrt{-D})$ has norm n, then $\mathcal{M} = \{0, \alpha\}$ is an integer norm set and therefore embeds in $\mathcal{O}_{\mathbb{Q}(\sqrt{-D})}$. The image of α under this embedding must be an element of $\mathcal{O}_{\mathbb{Q}(\sqrt{-D})}$ of norm n.

For the $1 \implies 2$, suppose the class group does not take this form, so that there is some ideal $\mathfrak{m} \subset \mathcal{O}_{\mathbb{Q}(\sqrt{-D})}$ whose square is not principal. Since $\mathcal{O}_{\mathbb{Q}(\sqrt{-D})}$ is a Dedekind domain, there exists a prime ideal $\mathfrak{p}$ such that $\mathfrak{m}^2\mathfrak{p} = (\alpha)$ is principal. Let $r = [\mathfrak{m}]$. Since $\mathfrak{m} \neq (1)$, we know $r > 1$. We also have

$$\left[\frac{\alpha}{r}\right] = \frac{[\mathfrak{m}]^2\,[\mathfrak{p}]}{[\mathfrak{m}]^2} = [\mathfrak{p}] \in \mathbb{Z}$$

Now suppose, for a contradiction, that $\mathcal{O}_{\mathbb{Q}(\sqrt{-D})}$ does contain an element of norm $n = [\mathfrak{p}]$. This element, along with the origin, would give an embedding of $\{0, \frac{\alpha}{r}\}$, and thus, by Theorem 24, there exists some ideal $\mathfrak{b}$ dividing $\mathfrak{p}$ such that $\mathfrak{m}^2\mathfrak{b}^2$ is principal. Since $\mathfrak{p}$ is prime, either $\mathfrak{b} = (1)$ or $\mathfrak{b} = \mathfrak{p}$. Since $\mathfrak{m}^2\mathfrak{b}^2$ is principal but $\mathfrak{m}^2$ is not, $\mathfrak{b}$ cannot be (1). On the other hand, if $\mathfrak{b} = \mathfrak{p}$, then both $\mathfrak{m}^2\mathfrak{p}$ and $\mathfrak{m}^2\mathfrak{p}^2 = \mathfrak{m}^2\mathfrak{b}^2$ are principal, thus so is $\mathfrak{m}^2 = (\mathfrak{m}^2\mathfrak{p})^2/(\mathfrak{m}^2\mathfrak{p}^2)$, a contradiction. □

Suppose, for some positive squarefree D, that the class group of $\mathbb{Q}(\sqrt{-D})$ is $C(\mathcal{O}_{\mathbb{Q}(\sqrt{-D})}) \cong \mathbb{Z}^k$ for some $k \geq 0$. What the first statement says, in other words, is that if $D \not\equiv 3 \pmod 4$, then $a^2 + Db^2 = n$ has an integer solution if and only if it has a rational solution, and if $D \equiv 3 \pmod 4$, then $a^2 + Db^2 = 4n$ has an integer solution with $a \equiv b \pmod 2$ if and only if it has a rational solution. On the other hand, if $C(\mathcal{O}_{\mathbb{Q}(\sqrt{-D})})$ is not of the form $\mathbb{Z}_2^k$, then there exists some positive integer n such that $a^2 + Db^2 = n$ has a rational solution but no integer solution if $D \not\equiv 3 \pmod 4$, and $a^2 + Db^2 = 4n$ has a rational solution but no integer solution with $a \equiv b \pmod 2$ if $D \equiv 3 \pmod 4$.

If $\mathcal{M}$ is a planar integer norm set with characteristic D or undefined characteristic, then checking whether $\mathcal{M}$ embeds in $\mathbb{Q}(\sqrt{-D})$ can be done by taking any element of $\mathcal{M}$, letting n be its norm, and searching for integer solutions to one of these two equations. This is a process that can always be done in a finite number of steps, since any solution to one of these equations will have $-\sqrt{4n} \leq a, b \leq \sqrt{4n}$.

8. Embeddings in 4 and 8 Dimensions

The proof of Theorem 24 relies heavily on the composition law in $\mathbb{C}$ and factorization properties of orders of the form $\mathcal{O}_{\mathbb{Q}(\sqrt{-D})}$. This suggests looking for embeddings of planar integer norm sets in orders of other rational composition algebras. The work of Jan Fricke [5] and Marshall and Perlis [13], who employ the factorization theory of the Lipschitz quaternions to prove that all Heronian tetrahedra embed in $\mathbb{Z}^4$, is also inspirational. The next proposition is also an encouraging result. We will not use it to build any further results, but it is still worth proving here.

Recall the definitions $\mathbf{L} = \mathbb{Z}[i, j]$ (the Lipschitz quaternions), $\mathbf{H} = \mathbb{Z}[i, j, \omega_3]$ (the Hurwitz quaternions), and $\mathbf{K} = \mathbb{Z}[i_0, i_1, i_2, \omega_7]$ (the Kleinian integers). Also, recall the definition $\omega_D = \frac{-1+\sqrt{-D}}{2}$.

Proposition 28. Let D be a positive squarefree integer. When we say "embeds," we are speaking of an order embedding, not just a integer norm set embedding.

(1) $\mathcal{O}_{\mathbb{Q}(\sqrt{-D})}$ embeds in $\mathbf{L}$ if and only if $D \not\equiv 3 \pmod 4$.
(2) $\mathcal{O}_{\mathbb{Q}(\sqrt{-D})}$ embeds in $\mathbf{H}$, but not in $\mathbf{L}$, if and only if $D \equiv 3 \pmod 8$.
(3) $\mathcal{O}_{\mathbb{Q}(\sqrt{-D})}$ embeds in $\mathbf{K}$, but not in $\mathbf{H}$, if and only if $D \equiv 7 \pmod 8$.

Proof. Suppose $D \not\equiv 3 \pmod 4$. D cannot be of the form $4^a(8b + 7)$, thus by Legendre's Theorem is expressible as a sum of three squares. So let $\delta = xi + yj + zk$ with $[\delta] = x^2 + y^2 + z^2 = D$. The map $\sqrt{-D} \mapsto \delta$ gives an embedding $\mathcal{O}_{\mathbb{Q}(\sqrt{-D})} \to \mathbb{Z}[i, j]$. For the converse, note that if $D \equiv 3 \pmod 4$ then the image δ of ω_D would need to satisfy $[\delta, 1] = [\omega_D, 1] = -\frac{1}{2}$, however no Lipschitz integer has a non-integral real part.

Next, suppose $D \equiv 3 \pmod 8$. Again, we can express D as $x^2 + y^2 + z^2$. However, now $\mathcal{O}_{\mathbb{Q}(\sqrt{-D})}$ is generated by $\omega_D = \frac{-1+\sqrt{-D}}{2}$, so let $\delta = \frac{1}{2}(-1 + xi + yj + zk)$. In order for δ to be a Hurwitz integer, we need x, y and z to be odd. Since the sum of their squares is odd, the only other possibility is that one is odd and the other two are even, meaning

$$D = (2l)^2 + (2m)^2 + (2n + 1)^2 = 4(l^2 + m^2 + n^2 + n) + 1 \equiv 3 \pmod 8$$

which is a contradiction. So δ is a Hurwitz integer, thus the map $\omega_D \mapsto \delta$ gives the embedding. All that must be checked is that $[\delta] = [\omega_D] = \frac{1+D}{2}$ and $[\delta, 1] = [\omega_D, 1] = \frac{1}{2}$ hold, which they do.

Finally, suppose $D \equiv 7 \pmod 8$. Then $D-4$ can be written as a sum of three squares $x^2+y^2+z^2$. By the same argument as before, x, y and z must all be odd. Letting $\delta = \frac{1}{2}(-i_\infty + i_0 + i_1 + i_2 + i_3 + xi_4 + yi_5 + zi_6)$ gives an embedding $\omega_D \mapsto \delta$.

For the converse, we need only prove that if $D \equiv 7 \pmod 8$ then $\mathcal{O}_{\mathbb{Q}(\sqrt{-D})}$ is not a subring of the Hurwitz quaternions. Suppose the contrary, so that the image of ω_D is δ under some embedding. Then $[\delta, 1] = [\omega_D, 1] = -\frac{1}{2}$, and so $\delta = \frac{1}{2}(-1 + xi + yj + zk)$ for some odd integers x, y, and z. Since $[\delta] = [\omega_D]$, we have $D = x^2 + y^2 + z^2$. But $D \equiv 7 \pmod 8$, and hence cannot be written as a sum of three squares. □

We immediately obtain a corollary:

Corollary 29. Let $\mathcal{M}$ be a planar integer norm set with characteristic D, and suppose $\mathcal{O}_{\mathbb{Q}(\sqrt{-D})}$ is a PID.

(1) If $D \not\equiv 3 \pmod 4$, then $\mathcal{M}$ embeds in the Lipschitz quaternions $\mathbf{L}$.
(2) If $D \equiv 3 \pmod 8$, then $\mathcal{M}$ embeds in the Hurwitz quaternions $\mathbf{H}$.
(3) If $D \equiv 7 \pmod 8$, then $\mathcal{M}$ embeds in the Kleinian octaves $\mathbf{K}$.

Proof. Let d be the greatest common divisor of the norms of the pairwise differences of elements of $\mathcal{M}$, so that $\frac{1}{\sqrt{d}}\mathcal{M}$ is a primitive integer norm set. By Proposition 28, $\frac{1}{\sqrt{d}}\mathcal{M}$ embeds in $\mathcal{O}_{\mathbb{Q}(\sqrt{-D})}$, and so by the previous theorem also embeds in the specified order. Each of these orders contains the Lipschitz integers $\mathbf{L}$, which in turn contain an element of any given norm (by Lagrange's four square theorem). Scaling this embedded primitive pointset by an element of norm d produces an embedding of $\mathcal{M}$ in the desired order. □

There are only nine such numbers D for which $\mathcal{O}_{\mathbb{Q}(\sqrt{-D})}$ is a PID. These are 1, 2, 3, 7, 11, 19, 43, 67, and 163, and are called Heegner numbers. Still, this corollary begs the question of whether the condition that

D is a Heegner number can be done away with. Our first step will be to establish a powerful embedding theorem regarding orders of $\mathbb{Q}(i,j)$.

Suppose $\alpha \in \mathbb{Q}(i,j)$. We can definitely write α as $\alpha = \beta^{-1}\alpha'$ for some $\alpha', \beta \in \mathbf{L}$, since we could at least write out the coordinates of α and take β to be the least common denominator of each entry. If $\beta \in \mathbf{L}$ is any such number, let us call it a *denominator* of α. If we are discussing a particular representation of α as $\beta^{-1}\alpha'$, we may refer to β as *the* denominator. Obviously, this is not meant to imply that there is a unique choice of denominator for α. The article "the" is only being used to refer to the specific choice being used at that moment. If $\mathcal{M}$ is a finite integer norm set, then we may express $\mathcal{M}$ as

$$\mathcal{M} = \{0, \beta^{-1}\alpha_1, \ldots, \beta^{-1}\alpha_n\}.$$

In this case, let us call β a denominator of $\mathcal{M}$.

Theorem 30. Let $\mathcal{M} \subset \mathbb{Q}(i,j) \cong \mathbb{Q}^4$ be an integer norm pointset (not necessarily planar).

(1) $\mathbb{Z}[\mathcal{M}]$ embeds in the Hurwitz integral quaternions $\mathbf{H}$.
(2) If some finite generating set for $\mathbb{Z}[\mathcal{M}]$ has a denominator with odd norm, then $\mathbb{Z}[\mathcal{M}]$ embeds in $\mathbf{L}$.

The stated embedding can be achieved by an inner automorphism of $\mathbb{Q}(i,j)$. Thus, this is an order embedding, rather than just a integer norm set embedding.

Proof. It suffices to show that a finite generating set for $\mathcal{M}$ embeds in the stated spaced, since its embedding will then additively generate an embedding of the lattice $\mathbb{Z}[\mathcal{M}]$. Thus, we may assume $\mathcal{M}$ is finite. Express $\mathcal{M}$ as

$$\mathcal{M} = \{0, \beta^{-1}\alpha_1, \ldots, \beta^{-1}\alpha_n\}$$

with $\alpha_1, \ldots, \alpha_n, \beta \in \mathbf{L}$. Since $\mathcal{M}$ is assumed to be an integer norm set, we know that $[\beta] \mid [\alpha_s], [\alpha_s - \alpha_t]$ for all s, t. Our goal is to show that, if β has an odd divisor of norm p, then we can rewrite this set as $\mathcal{M} = \{0, \beta'^{-1}\alpha_1', \ldots, \beta'^{-1}\alpha_n'\}$ where $[\beta'] < [\beta]$. Hence, by induction, $\mathcal{M}$ can be written in this form where the norm of β is a power of 2.

Suppose that $[\beta]$ has an odd prime divisor p. By Lemma 4, $\beta, \alpha_1, \ldots, \alpha_n$ all share either a left or a right divisor π of norm p. If π is a common left divisor, then π^{-1} is a right divisor of β^{-1}, and so each point $\beta^{-1}\alpha_s$ is of the form

$$(\beta'^{-1}\pi^{-1})(\pi\alpha_s').$$

Thus, π can simply be canceled from each product, reducing the norm of β, as desired. Otherwise, we have $\beta = \beta'\pi$ and $\alpha = \alpha'\pi$. Therefore, the rotation of $\mathbb{H}$ given by $\gamma \mapsto \pi\gamma\pi^{-1}$ gives a new embedding of $\mathcal{M}$ with a smaller denominator than before.

If $[\beta]$ was odd, then this process has produced an embedding of $\mathcal{M}$ in $\mathbf{L}$. Otherwise, we have reduced ourselves to the case where $[\beta] = 2^v$ for some $v \geq 1$. If v is even, then by Lemma 4 we know that $\beta, \alpha_1, \ldots, \alpha_n$ are divisible by $2^{v/2}$, so canceling these factors leaves us with an embedding in $\mathbf{H}$. Otherwise, we may cancel factors of 2 until $[\beta] = 2$. At this point, we apply Lemma 4 again to find a common Hurwitz right divisor of $\beta, \alpha_1, \ldots, \alpha_n$ of norm 2, then apply the rotation to retrieve a new embedding, which lies in $\mathbf{H}$.

If the elements used in the successive isometries were $\pi_1, \ldots, \pi_m$, then letting $\sigma = \pi_m \cdots \pi_1$ we see that the embedding was achieved by the inner automorphism $\gamma \mapsto \sigma\gamma\sigma^{-1}$ of $\mathbb{Q}(i,j)$. □

An algorithm similar to this was first described by Jan Fricke [5] in the context of the Gaussian integers, and was later replicated by several others [7, 12, 13]. Lemma 5, which we have proven based on the work of Gordon Pall, is crucial. In fact, I conjecture that a similar lemma holds in the broader case of the octavian integers, which I state in the next section.

When we had previously looked at orders of $\mathbb{Q}(i,j)$, we had only considered those orders which contained the Lipschitz quaternions $\mathbf{L}$. However, any order of $\mathbb{Q}(i,j)$ is an integer norm pointset, therefore this theorem immediately gives us a characterization of all orders of $\mathbb{Q}(i,j)$.

Corollary 31. Up to isomorphism, every order of $\mathbb{Q}(i,j)$ is a suborder of $\mathbf{H}$. If the generating set of an order of $\mathbb{Q}(i,j)$ can be written with a denominator of odd norm, then it is isomorphic to a suborder of $\mathbf{L}$, as well.

We will now move on to consider planar integer norm sets.

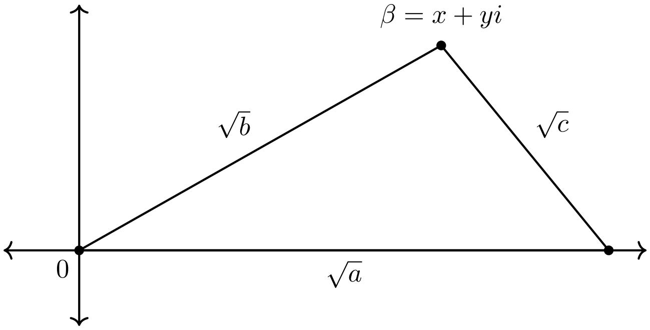
Proposition 32. Let $\mathcal{M}$ be a planar integer norm set.

(1) If the characteristic of $\mathcal{M}$ is undefined, or if it has characteristic $D \not\equiv 7 \pmod 8$, then $\mathcal{M}$ embeds in $\mathbb{Q}(i,j) \cong \mathbb{Q}^4$.
(2) If the characteristic of $\mathcal{M}$ is $D \equiv 7 \pmod 8$, then $\mathcal{M}$ embeds in $\mathbb{Q}(i_0, i_1, i_2) \cong \mathbb{Q}^8$.

Proof. Let Q be the space we claim $\mathcal{M}$ can be embedded in, meaning $Q = \mathbb{Q}(i,j)$ if $\mathcal{M}$ has undefined characteristic or characteristic $D \not\equiv 7 \pmod 8$, and $Q = \mathbb{Q}(i_0, i_1, i_2)$ otherwise. Also, let $R = \mathbb{R}Q$, so that $R = \mathbb{H}$ or $R = \mathbb{O}$, depending on the value of $D \pmod 8$. It is possible to rotate $\mathcal{M}$ in $\mathbb{C}$ so that one of its points $\sqrt{a} + 0i$ lies on the positive real axis (recall we have assumed that $\mathcal{M}$ contains the origin), so assume $\mathcal{M}$ is situated in this way.

Choose a Lipschitz quaternion α of norm a. If $\mathcal{M}$ has characteristic $D \not\equiv 7 \pmod 8$, we can also find a purely imaginary Lipschitz quaternion δ of norm D by expressing D as a sum of three squares. Otherwise, if $\mathcal{M}$ has characteristic $D \equiv 7 \pmod 8$, we can express D as a sum of four squares $a^2 + b^2 + c^2 + d^2$ and let $\delta = ai_0 + bi_1 + ci_2 + di_3$ be a Gravesian integer. If the characteristic of $\mathcal{M}$ is undefined, let $D = 1$ and $\delta = i$. Notice that we have $[\alpha\delta, \alpha] \overset{\text{M2}}{=} [\alpha]\,[\delta, 1] = 0$, thus $\alpha\delta$ and α are orthogonal.

Define a linear map $\varphi : \mathbb{C} \to R$ by $1 \mapsto \frac{\alpha}{\sqrt{a}}$ and $i \mapsto \frac{\alpha\delta}{\sqrt{aD}}$. Clearly, φ is an isometry, and $\varphi(\sqrt{a}) = \alpha$. If γ was a point of $\mathcal{M}$ also lying on the real axis, then the discussion following the statement of Proposition 23 proves that $\gamma = c\alpha$ for some rational number c. Thus, $\varphi(\gamma) = c\varphi(\alpha) \in Q$.



Assuming the characteristic D of $\mathcal{M}$ is defined, let $\beta = x + yi \in \mathcal{M}$ be any point of $\mathcal{M}$ not on the real axis. The area of the triangle formed by α and β with the origin is of the form $\frac{z}{4}\sqrt{D}$ for some positive integer z. The above figure is just one possible configuration this triangle may have. However, β could potentially lie to the right of $\sqrt{a}$ or even in another quadrant. Still, regardless of where β lies, the following system holds:

$$b = x^2 + y^2, \qquad c = (x - \sqrt{a})^2 + y^2, \qquad y^2 = \frac{z^2 D}{4a}$$

The first two equations come only from the Pythagorean theorem and the last from the standard formula for the area of a triangle. From these, we deduce

$$x = \frac{a + b - c}{2\sqrt{a}} \qquad y = \pm\frac{z\sqrt{D}}{2\sqrt{a}}$$

The first equality is obtained by manipulating the first two equations given just prior to these. Therefore,

$$\varphi(\beta) = \frac{a+b-c}{2\sqrt{a}}\frac{\alpha}{\sqrt{a}} \pm \frac{z\sqrt{D}}{2\sqrt{a}}\frac{\alpha\delta}{\sqrt{aD}} = \frac{a+b-c}{2a}\alpha \pm \frac{z}{2a}\alpha\delta \in Q.$$

Since β was an arbitrary point of $\mathcal{M}$ not on the real axis, φ embeds the entire set $\mathcal{M}$ into Q. □

We will need one final lemma before proving the main theorem.

Lemma 33. Let T be a triangle of characteristic D with sidelengths $\sqrt{a}$, $\sqrt{b}$, and $\sqrt{c}$, and suppose $D \not\equiv 3 \pmod 4$. Then $a + b - c$ is even, and when the area of T is written as $\frac{z}{4}\sqrt{D}$, z is even as well.

Proof. Suppose $a+b-c$ is odd. Then either one or all three of these terms are odd. By Heron's formula, we have

$$z^2D = -(a^2+b^2+c^2)+2(ab+ac+bc).$$

If a is odd but b and c are even, then $-(a^2+b^2+c^2) \equiv 3 \pmod 4$ and $2(ab+ac+bc) \equiv 0 \pmod 4$. If a, b, and c are all odd, then $-(a^2+b^2+c^2) \equiv 1 \pmod 4$ and $2(ab+ac+bc) \equiv 2 \pmod 4$. Either way, we have $z^2D \equiv 3 \pmod 4$. Since $z^2 \equiv 0$ or $1 \pmod 4$, we must have $D \equiv 3 \pmod 4$ since $z^2 \equiv 0$ would be a contradiction.

Now, assuming $D \not\equiv 3 \pmod 4$, we now know that $a+b-c$ is even, and thus either one of the terms is even or all of them are. By a similar analysis, one checks that z^2D is divisible by 4. D being squarefree, this means that z^2 and therefore z is even. □

Theorem 34. Let $\mathcal{M}$ be a planar integer norm set with characteristic D.

(1) If $D \not\equiv 7 \pmod 8$, then $\mathcal{M}$ embeds in $\mathbf{H}$.
(2) If $D \not\equiv 3 \pmod 4$ then $\mathcal{M}$ embeds in $\mathbf{L}$.

Proof. In both of these situations, Proposition 32 ensures that $\mathcal{M}$ embeds in $\mathbb{Q}(i,j)$. Therefore, by Theorem 30 we know that $\mathcal{M}$ embeds in $\mathbf{H}$ in both cases. Now, suppose that $D \not\equiv 3 \pmod 4$. We may assume $\mathcal{M}$ is finite, since it certainly has a finite generating set. We will also, for now, begin with the assumption that $\mathcal{M}$ is primitive. From Theorem 30, we realize it suffices to show that, in the embedding of $\mathcal{M}$ in $\mathbb{Q}(i,j)$ found in Proposition 32, the denominator of every point was odd. Recall from the proof of Proposition 6 that one point of the embedding was some $\alpha \in \mathbf{L}$, and that every point γ not lying on a line through α and the origin took the form

$$\gamma = \frac{a+b-c}{2a}\alpha \pm \frac{z}{2a}\alpha\delta$$

where $a=[\alpha]$, $b=[\gamma]$, $c=[\alpha-\gamma]$, and $\delta \in \mathbf{L}$. Further, α could be taken to be the image under the embedding of any arbitrary point in $\mathcal{M}$.

Since we are for now assuming $\mathcal{M} \subseteq \mathbb{C}$ to be primitive, there must be at least some pair $\alpha', \eta \in \mathcal{M}$ for which $[\alpha'-\eta]$ is odd. Translate and rotate $\mathcal{M}$ so that η lies at the origin and α' lies on the real axis. Then $a=[\alpha']$ is odd, and we may proceed to embed $\mathcal{M}$ in $\mathbb{Q}(i,j)$ with this α' as our choice for α.

If β is some point of the embedding which lies on the line passing through α and the origin, then $\beta = \frac{\sqrt{[\beta]}}{\sqrt{[\alpha]}}\alpha$. Since $\mathbb{Z}[\{\alpha,\beta\}]$ is generated by a single element, we know β is a rational multiple of α. Therefore, $\frac{\sqrt{[\beta]}}{\sqrt{[\alpha]}}$ must be rational, and so there is a positive squarefree integer E such that $[\alpha]=r^2E$ and $[\beta]=s^2E$. r must be odd because $[\alpha]$ is assumed to be odd, and thus the denominator of β is odd because $\beta = \frac{s}{r}\alpha$.

Now, suppose γ is a point not on a line through the embedded image of α and the origin. The triangle formed by α and γ with the origin has characteristic $D \not\equiv 3 \pmod 4$. Thus, by Lemma 33, $a+b-c$ and z are both even in the expression

$$\frac{\frac{1}{2}(a+b-c\pm z\delta)\alpha}{a}$$

hence both the numerator and denominator are in $\mathbf{L}$. Thus, all points have odd denominators, so $\mathcal{M}$ embeds in $\mathbf{L}$.

If $\mathcal{M}$ is not primitive, then scale $\mathcal{M}$ down by some factor $\frac{1}{\sqrt{d}}$ to obtain a primitive integer norm set, which we may then embed in $\mathbf{L}$. Now, left multiply this embedding of $\frac{1}{\sqrt{d}}\mathcal{M}$ by any Lipschitz quaternion of norm d to retrieve an embedding of the original pointset in $\mathbf{L}$. □

The only remaining characteristics to consider are those congruent to $7 \pmod 8$. It is most definitely not true that these pointsets embed in the Hurwitz quaternions. However, I have a conjecture.

Conjecture 35. If the characteristic of a planar integer norm set is congruent to $7 \pmod 8$, then it embeds in the Kleinian octaves.

I have verified this conjecture for all primitive integer norm triangles with a maximum diamater of $\sqrt{67}$ and maximum characteristic of 87. This means that all planar integer norm sets with characteristic ≤ 87 and a basis forming a triangle with diameter $\leq \sqrt{67}$ embed in the Kleinian octaves. If this were to hold, it would mean that every integer norm triangle embeds in the double Hurwitzian ring, since this is the lattice generated by the Hurwitz integers together with the Kleinian octaves. There are many possible approaches to proving this conjecture. The following example is worth presenting, in case the method used can be generalized.

Proposition 36. Let T be an isosceles triangle with sidelengths $\sqrt{a}, \sqrt{b}, \sqrt{b}$ for positive integers $a < b$. Then T embeds in the double Hurwitz ring.

Proof. By Theorem 34, the equilateral triangle with common sidelength $\sqrt{a}$ embeds in $\mathbb{H}$ as $\{0, \alpha, \beta\}$, since all equilateral triangles have characteristic 3. Let $\gamma \in \mathbb{H}$ be any element of norm $b - a$. Then $\{0, \alpha + i_2\gamma, \beta + i_2\gamma\}$ is an embedding of T, because

$$[(\alpha + i_2\gamma) - (\beta + i_2\gamma)] = [\alpha - \beta] = a$$

and

$$[\alpha + i_2\gamma] = [\alpha] + [\gamma] = a + (b - a) = b = [\beta] + [\gamma] = [\beta + i_2\gamma]\,.$$

□

This method entails partitioning the norms of the pairwise differences of a pointset in a way that forms two integer norm sets, neither of characteristic 7 (mod 8), then embedding the two sets into two orthogonal copies of the Hurwitz integers. Another path to proving this conjecture might require using a proof similar to that of Theorem 34. This would require us to first understand the nature of factorization in the orders of $\mathbb{Q}(i_0, i_1, i_2)$ containing $\mathbf{G}$.

Unfortunately, the foundation of factorization in these orders has not yet been laid out, as it has been for the Lipschitz and Hurwitz quaternions by Pall and others. For the Hurwitz quaternions, we have a division algorithm that we can use along with associativity to prove several familiar facts regarding factorization. In Pall's paper, he relies heavily on the theory of quadratic forms to prove his results regarding the Lipschitz quaternions, which do not satisfy the division algorithm. However, I imagine the complicated system of halving sets in these 8-dimensional orders could cause this coordinate-driven approach to become complicated quickly. The following conjecture is based more on intuition than experimentation.

Conjecture 37. Every integer norm set in $\mathbb{Q}^8$ embeds in the octavian integers.

9. Factorization in the Octavian Integers

From here on, let $\mathcal{O}$ denote the octavian integers. It can be shown that every point of $\mathbb{R}^8$ lies within $\frac{1}{\sqrt{2}}$ unit of an octavian integer [4]. As usual, this implies that the octavian integers also satisfy the division algorithm as stated in Theorem 2. The lack of associativity in $\mathbb{O}$ prevents this theorem from being employed in the usual way to compute common divisors of maximal norm. However, a clever algorithm due to Rehm allows us to compute all divisors of an element rather efficiently. The following proof is from his paper [18].

Theorem 38 (Rehm's Algorithm)**.** Let $\alpha \in \mathcal{O}$, and suppose $[\alpha] = mn$. Then α has a left and a right divisor of norm m.

Proof. Induct on n. This is clear if $m = 0$, so assume otherwise. We may write

$$\alpha = m\delta + \rho$$

with $[\rho] \leq \frac{m^2}{2}$. Also,

$$[\rho] = [\alpha] + m^2\,[\delta] - 2m\,[\delta, \alpha]$$

and m divides each term on the righthand side, therefore m divides $[\rho]$. So, if $\frac{m^2}{2} < mn$, then we know $[\rho] = mn'$ for some $n' < n$, hence by the inductive hypothesis we can write $\rho = \theta\gamma$ with $[\theta] = m$. Thus,

$$\alpha = m\delta + \rho = (\theta\overline{\theta})\delta + \theta\gamma = \theta(\overline{\theta}\delta) + \theta\gamma = \theta(\overline{\theta}\delta + \gamma)$$

and so α has a lefthand divisor of norm m, as desired. Note here that we have used the fact that $\mathbb{O}$ is alternative in order to complete this factorization. Since $\overline{\theta}$ is in the algebra generated by δ and θ, we have $(\theta\overline{\theta})\delta = \theta(\overline{\theta}\delta)$. Finally, factoring ρ with a righthand factor of norm m similarly gives a factorization of α with a righthand factor of norm m.

It will not always be the case that $\frac{m^2}{2} < mn$. If this does not happen, then we can instead factor α as

$$\alpha = \delta' n + \rho'$$

with $[\rho'] \leq \frac{n^2}{2}$. We must now have $\frac{n^2}{2} < mn$, and so $\rho = \gamma'\theta'$ with $[\theta'] = n$. Thus,

$$\alpha = (\delta'\overline{\theta'} + \gamma')\theta'$$

is a factorization where the lefthand factor has norm m. We produce a righthand factor in a similar manner. □

If this algorithm is carried out in more detail, it can actually be shown that the set of lefthand (resp. righthand) divisors of α of norm m, if α is coprime to m, is geometrically similar to the set of 240 octavian units. More formally, there are isometries ϕ_L and ϕ_R of $\mathbb{O}$ such that the set of lefthand (resp. righthand) divisors of α of norm m is the image of the set of all 240 octavian units under the map $m \cdot \phi_L$ (resp. $m \cdot \phi_R$). Furthermore, if we let d be the greatest common rational divisor of α, m, and n, then the sets of left and right divisors of α of norm m are geometrically similar to the set of all elements of norm d [3]. Regarding the common divisors of two elements, all I have to offer is the following conjecture.

Conjecture 39. Let α and β be octavian integers such that $p \mid [\alpha], [\beta], 2[\alpha, \beta]$ for some prime p. Then α and β share either a left or a right divisor of norm p.

Suppose α and β satisfy the hypothesis of this conjecture. If either of α or β is divisible by p, this conjecture is obviously true. For if $p \mid \alpha$ and θ is a left divisor of β of norm p, then $\alpha = p\alpha' = (\theta\overline{\theta})\alpha' = \theta(\overline{\theta}\alpha')$ has a left divisor of θ as well. Therefore, the only case with any substance is that where both α and β are proper $\pmod p$. It cannot be said, as it can in the case of the Lipschitz quaternions, that α and β actually share all of their left or right divisors. Consider the following counterexample, also given in vector notion.

$$\begin{aligned} \alpha' &= (1,1,0,0,0,0,0,1) = i_\infty + i_0 + i_6 \\ \beta' &= (0,1,0,0,1,2,0,1) = i_0 + i_3 + 2i_4 + i_6 \\ \theta &= (2,2,3,6,4,2,0,8) = 2i_\infty + 2i_0 + 3i_1 + 6i_2 + 4i_3 + 2i_4 + 8i_6 \end{aligned}$$

Let $\alpha = \theta\alpha'$ and $\beta = \theta\beta'$. We have $[\alpha'] = 3$, $[\beta'] = 7$, and $[\theta] = 137$. Clearly, 137 divides $2[\alpha, \beta] = 2[\theta][\alpha', \beta']$. However, α and β share no common right divisors of norm 137, and θ and $-\theta$ are their only common left divisors. Examples like this seem to become more likely when p is large relative to $[\alpha]$ and $[\beta]$.

10. Appendix: Consequences of the Composition Law

Recall the defining feature of a composition algebra A is that the norm is multiplicative. We have also defined two other symbols, namely the conjugation operator

$$\overline{\alpha} = 2\,[\alpha, 1] - \alpha$$

and, $\alpha \neq 0$, the inverse operator

$$\alpha^{-1} = \frac{\overline{\alpha}}{[\alpha]}.$$

We will soon see that this operator does in fact give an inverse. The norm can be related to the inner product by

$$[\alpha, \beta] = \frac{[\alpha+\beta] - [\alpha] - [\beta]}{2}.$$

From the axioms of a composition algebra alone, we are able to determine several useful properties. In listing these laws below, I adhere to the naming conventions established by Conway and Smith whenever possible. The proofs of these laws taken from their book [3], with some minor adjustments. In situations where a proposition involves a statement involving a left multiplication as well as a symmetric version of the statement using right multiplication, I will only prove one of the statements, since the proof of the other would be redundant. Note that $\alpha = \beta$ if and only if $[\alpha, \omega] = [\beta, \omega]$ for all ω, since the only vector orthogonal to the entire space is 0.

10.1. The Multiplication Laws.

(M1) **The Composition Law:** $[\alpha\beta] = [\alpha]\,[\beta]$

(M2) **The Scaling Laws:** $[\alpha\beta, \alpha\gamma] = [\alpha]\,[\beta, \gamma]$ and $[\beta\alpha, \gamma\alpha] = [\beta, \gamma]\,[\alpha]$

Proof. $[\alpha\beta, \alpha\gamma] = \dfrac{[\alpha\beta + \alpha\gamma] - [\alpha\beta] - [\alpha\gamma]}{2} \overset{\text{M1}}{=} [\alpha]\,\dfrac{[\beta+\gamma] - [\beta] - [\gamma]}{2} = [\alpha]\,[\beta, \gamma]\,.$ □

(M3) **The Exchange Law:** $[\alpha\beta, \gamma\delta] = 2\,[\alpha, \gamma]\,[\beta, \delta] - [\alpha\delta, \gamma\beta]$.

Proof. We have

$$\begin{aligned}
[\alpha\beta, \alpha\delta] + 2\,[\alpha, \gamma]\,[\beta, \delta] + [\gamma\beta, \gamma\delta] &\overset{\text{M2}}{=} ([\alpha] + 2\,[\alpha, \gamma] + [\gamma])\,[\beta, \delta] \\
&= [\alpha + \gamma]\,[\beta, \delta] \\
&\overset{\text{M2}}{=} [(\alpha+\gamma)\beta, (\alpha+\gamma)\delta] \\
&= [\alpha\beta, \alpha\delta] + [\alpha\beta, \gamma\delta] + [\gamma\beta, \alpha\delta] + [\gamma\beta, \gamma\delta]
\end{aligned}$$

thus

$$\begin{aligned}
[\alpha\beta, \gamma\delta] &= ([\alpha\beta, \alpha\delta] + [\alpha\beta, \gamma\delta] + [\gamma\beta, \alpha\delta] + [\gamma\beta, \gamma\delta]) - ([\alpha\beta, \alpha\delta] + [\gamma\beta, \alpha\delta] + [\gamma\beta, \gamma\delta]) \\
&= ([\alpha\beta, \alpha\delta] + 2\,[\alpha, \gamma]\,[\beta, \delta] + [\gamma\beta, \gamma\delta]) - ([\alpha\beta, \alpha\delta] + [\gamma\beta, \alpha\delta] + [\gamma\beta, \gamma\delta]) \\
&= 2\,[\alpha, \gamma]\,[\beta, \delta] - [\alpha\delta, \gamma\beta]\,.
\end{aligned}$$

□

10.2. The Conjugation Laws.

(C1) **The Braid Laws:** $[\alpha\beta, \delta] = [\beta, \overline{\alpha}\delta]$ and $[\alpha, \beta\delta] = \left[\overline{\beta}\alpha, \delta\right]$

Proof. We make the substitution $\gamma = 1$ in M3:

$$[\beta, \overline{\alpha}\delta] = [\beta, (2\,[\alpha, 1] - \alpha)\delta] = 2\,[\alpha, 1]\,[\beta, \delta] - [\beta, \alpha\delta] \overset{\text{M3}}{=} [\alpha\beta, \delta]\,.$$

□

(C2) **Biconjugation:** $\overline{\overline{\alpha}} = \alpha$

Proof. For all $\omega \in A$,

$$[\alpha, \omega] \overset{\text{C1}}{=} [1, \overline{\alpha}\omega] \overset{\text{C1}}{=} \left[\overline{\overline{\alpha}}, \omega\right].$$

□

(C3) **Product Conjugation:** $\overline{\alpha\beta} = \overline{\beta}\,\overline{\alpha}$

Proof. For all $\omega \in A$,

$$\left[\overline{\beta}\overline{\alpha}, \omega\right] = [\overline{\alpha}, \beta\omega] = [\overline{\alpha}\ \overline{\omega}, \beta] = [\overline{\omega}, \alpha\beta] = \left[\overline{\omega}\overline{\alpha\beta}, 1\right] = \left[\overline{\alpha\beta}, \omega\right]$$

where every equality follows from C1. □

(C4) **Equivalent Definition of Norm:** $[\alpha] = \alpha\overline{\alpha}$

Proof. For all $\omega \in A$,

$$[\alpha\overline{\alpha}, \omega] \overset{\text{C1}}{=} [\alpha, \alpha\omega] \overset{\text{M2}}{=} [\alpha]\,[1, \omega] = [[\alpha]\,, \omega]\,.$$

□

From this last law, it also becomes clear that our inverse operator truly outputs the multiplicative inverse of its argument. We also have $[\overline{\alpha}] = [\overline{\alpha}, \overline{\alpha}] \overset{\text{C1}}{=} [1, \alpha\overline{\alpha}] \overset{\text{C4}}{=} [1, [\alpha]] \overset{\text{M2}}{=} [1, 1]\,[\alpha] = [\alpha]$.

10.3. The Semi-Associativity Laws.

(S1) **Inverse Laws:** $\overline{\alpha}(\alpha\beta) = [\alpha]\,\beta = (\beta\alpha)\overline{\alpha}$ and $\alpha^{-1}(\alpha\beta) = \beta = (\beta\alpha)\alpha^{-1}$

Proof. For all $\omega \in A$,

$$[\overline{\alpha}(\alpha\beta), \omega] \overset{\text{C1}}{=} [\alpha\beta, \alpha\omega] \overset{\text{M2}}{=} [\alpha]\,[\beta, \omega] = [[\alpha]\,\beta, \omega] \overset{\text{C4}}{=} [(\alpha\overline{\alpha})\beta, \omega]\,.$$

The latter statement results from dividing the former by $[\alpha]$. □

(S2) **Alternative Laws:** $\alpha(\alpha\beta) = \alpha^2\beta$ and $(\alpha\beta)\beta = \alpha\beta^2$

Proof.

$$\begin{aligned}
\alpha(\alpha\beta) &= 2\,[\alpha, 1]\,\alpha\beta - (2\,[\alpha, 1]\,\alpha\beta - \alpha(\alpha\beta)) \\
&= 2\,[\alpha, 1]\,\alpha\beta - \overline{\alpha}(\alpha\beta) \\
&\overset{\text{S1}}{=} 2\,[\alpha, 1]\,\alpha\beta - (\overline{\alpha}\alpha)\beta \\
&= 2\,[\alpha, 1]\,\alpha\beta - ((2\,[\alpha, 1] - \alpha)\alpha)\beta \\
&= \alpha^2\beta
\end{aligned}$$

□

(S3) **Moufang Laws:** $(\alpha\beta)(\gamma\alpha) = (\alpha(\beta\gamma))\alpha = \alpha((\beta\gamma)\alpha)$

Proof. For all $\omega \in A$,

$$\begin{aligned}
[(\alpha\beta)(\gamma\alpha), \omega] &\overset{\text{C1}}{=} [\alpha\beta, \omega(\overline{\gamma\alpha})] \\
&\overset{\text{C3}}{=} [\alpha\beta, \omega(\overline{\alpha}\ \overline{\gamma})] \\
&\overset{\text{M3}}{=} 2\,[\alpha, \omega]\,[\beta, \overline{\alpha}\ \overline{\gamma}] - [\alpha(\overline{\alpha}\ \overline{\gamma}), \omega\beta] \\
&\overset{\text{C1}}{=} 2\,[\alpha, \omega]\,[\beta\gamma, \overline{\alpha}] - [\overline{\alpha}\ \overline{\gamma}, \overline{\alpha}(\omega\beta)] \\
&\overset{\text{M2}}{=} 2\,[\alpha, \omega]\,[\beta\gamma, \overline{\alpha}] - [\alpha]\,\left[\overline{\gamma}\ \overline{\beta}, \omega\right] \\
&\overset{\text{C3}}{=} \left[2\,[\beta\gamma, \overline{\alpha}]\,\alpha - [\alpha]\,\overline{\beta\gamma}, \omega\right]
\end{aligned}$$

thus $(\alpha\beta)(\gamma\alpha) = 2\,[\beta\gamma, \overline{\alpha}]\,\alpha - [\alpha]\,\overline{\beta\gamma}$. Therefore, this expression is a function of the product $\beta\gamma$, and does not depend on the individual factors β and γ. Thus, we may replace β with $\beta\gamma$ and γ with 1 (or vice versa), giving the result. □

10.4. **The Doubling Laws.** Let H be a subalgebra of A, let $i \in H$ be a unit vector orthogonal to A, and let $\alpha, \beta, \gamma, \delta \in H$.

(D1) **Inner-Product Doubling:** $[\alpha + i\beta, \gamma + i\delta] = [\alpha, \gamma] + [\beta, \delta]$

Proof.

$$\begin{aligned}[\alpha + i\beta, \gamma + i\delta] &\overset{\text{M2}}{=} [\alpha, \gamma] + [\alpha, i\delta] + [i\beta, \gamma] + [i]\,[\beta, \delta] \\ &\overset{\text{C1}}{=} [\alpha, \gamma] + \left[\alpha\overline{\delta}, i\right] + \left[i, \gamma\overline{\beta}\right] + [i]\,[\beta, \delta] \\ &= [\alpha, \gamma] + [\beta, \delta]\,.\end{aligned}$$

□

(D2) **Conjugation Doubling:** $\overline{\alpha + i\beta} = \overline{\alpha} - i\beta$

Proof.

$$\overline{\alpha + i\beta} = 2\,[\alpha, 1] + 2\,[i\beta, 1] - \alpha - i\beta \overset{\text{C1}}{=} \overline{\alpha} - i\beta - 2\left[i, \overline{\beta}\right] = \overline{\alpha} - i\beta$$

□

Note that this also gives us $i\beta = -\overline{i\beta} = -\overline{\beta}\overline{i} = -\overline{\beta}(-i) = \overline{\beta}i$.

(D3) **Composition Doubling:** $(\alpha + i\beta)(\gamma + i\delta) = (\alpha\gamma - \delta\overline{\beta}) + i(\gamma\beta + \overline{\alpha}\delta)$

Proof. Expanding gives

$$(\alpha + i\beta)(\gamma + i\delta) = \alpha\gamma + (i\beta)\gamma + \alpha(i\delta) + (i\beta)(i\delta).$$

We evaluate the final three terms:

$$[(i\beta)\gamma, \omega] \overset{\text{C1}}{=} [i\beta, \omega\overline{\gamma}] \overset{\text{D2}}{=} \left[\overline{\beta}i, \omega\overline{\gamma}\right] \overset{\text{M3}}{=} 0 - \left[\overline{\beta}\ \overline{\gamma}, \omega i\right] \overset{\text{C1,D2}}{=} \left[(\overline{\beta}\ \overline{\gamma})i, \omega\right] \overset{\text{D2}}{=} [i(\gamma\beta), \omega]$$

$$[\alpha(i\delta), \omega] \overset{\text{C1}}{=} [i\delta, \overline{\alpha}\omega] \overset{\text{M3}}{=} 0 - [i\omega, \overline{\alpha}\delta] \overset{\text{C1}}{=} [\omega, i(\overline{\alpha}\delta)] = [i(\overline{\alpha}\delta), \omega]$$

$$[(i\beta)(i\delta), \omega] \overset{\text{C1,D2}}{=} -[i\beta, \omega(i\delta)] \overset{\text{M3}}{=} 0 + [i(i\delta), \omega\beta] \overset{\text{S2}}{=} -[\delta, \omega\beta] \overset{\text{C1}}{=} \left[-\delta\overline{\beta}, \omega\right]$$

This gives

$$(\alpha + i\beta)(\gamma + i\delta) = \alpha\gamma + i(\gamma\beta) + i(\overline{\alpha}\delta) - \delta\overline{\beta} = (\alpha\gamma - \delta\overline{\beta}) + i(\gamma\beta + \overline{\alpha}\delta).$$

□

References

[1] Boyd Coan and Cherng-tiao Perng. Factorization of Hurwitz quaternions. *International Mathematical Forum*, 7(43):2143–2156, 2012.

[2] Harvey Cohn. *Advanced Number Theory*. Dover, 1980.

[3] J.H. Conway and D.A. Smith. *On Quaternions and Octonions*. Ak Peters Series. Taylor & Francis, 2003.

[4] H. S. M. Coxeter. Integral Cayley numbers. *Duke Math Journal*, pages 561–578, 1946.

[5] Jan Fricke. On Heronian simplices and integer embedding. *arXiv:math/0112239 [math.NT]*, 21 Dec 2001.

[6] Richard Guy. *Unsolved Problems in Number Theory*. Springer, 3rd edition, 2004.

[7] Michael Knopf, Jesse Milzman, Derek A. Smith, Dantong Zhu, and Dara Zirlin. *Lattice Embeddings of Planar Pointsets*, preprint. 2015.

[8] Tobias Kreisel and Sascha Kurz. There are integral heptagons, no three points on a line, no four on a circle. *Discrete and Computational Geometry*, 39:786–790, 2008.

[9] Sascha Kurz. On the characteristic of integral point sets in $\mathbb{E}^m$. *Journal of Combinatorics*, 36:241–248, 2006.

[10] Sascha Kurz, Landon Noll, Randall Rathbun, and Chuck Simmons. Constructing 7-clusters. *Serdica Journal of Computing*, 8:47–70, 2014.

[11] Serge Lang. *Algebra*. Addison-Wesley, Menlo Park Cal.

[12] Fred Lunnon. Lattice embedding of Heronian simplices. *arXiv:1202.3198v2 [math.MG]*, 1 July 2012.

[13] Susan Marshall and Alexander Perlis. Heronian tetrahedra are lattice tetrahedra. *The American Mathematical Monthly*, 120(2):140–149, February 2013.

[14] Landon Noll and David Bell. n-clusters for $1 < n < 7$. *Mathematics of Computation*, 53:439–444, 1989.

[15] Gordon Pall. On the arithmetic of quaternions. *Transactions of the American Mathematical Society*, 47(3):487–500, 1940.

[16] Gordon Pall. Factorization of Cayley numbers. *Journal of Number Theory*, 2:74–90, 1970.

[17] Cherng-tiao Perng. *Factorizaton of Lipschitz quaternions*, preprint. 2011.

[18] H. P. Rehm. Prime factorization of integral Cayley octaves. *Annales de la Facultè des Sciences de Toulouse*, 2:271–289, 1993.

[19] PJ Weinberger. Exponents of the class groups of complex quadratic fields. *Acta Arithmetica*, 22:117–124, 1973.

[20] Paul Yiu. Heronian triangles are lattice triangles. *The American Mathematical Monthly*, 108(3):261–263, March 2001.