The Quaternions

Algebra: An *(associative) algebra* over a field $\mathbb{F}$ is a vector space over $\mathbb{F}$ which is equipped with a vector product which is associative and distributive.

Normed Algebra: An algebra over $\mathbb{R}$ is *normed* (or is called a *composition algebra*) if $|uv| = |u| \cdot |v|$ for all u, v.

Note: The complex numbers, $\mathbb{C}$, may be viewed as formal linear combinations $x + iy$ where $x, y \in \mathbb{R}$ and i commutes with every real and obeys the rule $i^2 = -1$. The norm of a complex number is $|x + iy| = \sqrt{x^2 + y^2}$ and $\mathbb{C}$ is a 2-dimensional normed vector space over $\mathbb{R}$.

Quaternions: The *Quaternions*, $\mathbb{H}$, are formal linear combinations $x + iy + jz + kw$ where $x, y, w, z \in \mathbb{R}$ and i, j, k commute with every real and satisfy the rules:

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

(it follows from this that $ij = k$, $jk = i$, $ki = j$ and $ji = -k$, $kj = -i$, $ik = -j$). The norm of a quaternion is $|x + iy + jz + kw| = \sqrt{x^2 + y^2 + z^2 + w^2}$ and this gives $\mathbb{Q}$ the structure of a 4-dimensional normed algebra over $\mathbb{R}$.

Octonians: The *Octonians*, $\mathbb{O}$, form an eight dimensional normed (non-associative!) algebra over $\mathbb{R}$ which is based on the geometry of the Fano Plane.

Theorem 1 (Hurwitz) *The only normed algebras over $\mathbb{R}$ are: $\mathbb{C}$, $\mathbb{H}$, and $\mathbb{O}$.*

Theorem 2 (Pfister) *In any field and for any n, the product of two sums of 2^n squares is a sum of 2^n squares.*

Note: There is no contradiction in the above two theorems, as Pfister's result does not yield a suitable composition law.

Actions of $\mathbb{C}$: Let $U = \{z \in \mathbb{C} : |z| = 1\}$, then U acts on $\mathbb{C}$ by the rule that $u \in U$ sends $z \in \mathbb{C}$ to uz. If $u = e^{i\theta}$ then u has the effect of rotating the plane counterclockwise about the origin by an angle of θ. Indeed, this action is isomorphic to SO_2 (rotations fixing 0).

Actions of $\mathbb{H}$: let $q \in \mathbb{H} \setminus \{0\}$ and let q act on $\mathbb{H}$ by the rule $q(x) = qxq^{-1}$. This is a linear map which preserves the norm of each vector, so it must be an isometry of $\mathbb{R}^4$. This mapping fixes $\mathbb{R}$ pointwise, so it fixes the orthogonal subspace $V = \{iy + jz + kw : y, z, w \in \mathbb{R}\}$ setwise. Thus, each $q \in \mathbb{H}$ gives an isometry of $V \cong \mathbb{R}^3$ which fixes 0. In fact, each such isometry is a rotation. This action is not faithful: its kernel is $\mathbb{R} \setminus \{0\}$, but if we quotient by this we get an action isomorphic to SO_3.

Gaussian Numbers: The *Gaussian numbers* are $\{x + iy \in \mathbb{H} : x, y \in \mathbb{Z}\}$. It is immediate that the Gaussian numbers are closed under addition and multiplication. The Gaussian numbers of norm 1, called *units* are $\{1, -1, i, -i\}$ and importantly, every Gaussian number has a unique factorization (up to multiplication by units).

Hurwitz Integral Quaternions: Although a naive extension of the above to Quaternions does not yield a ring with unique factorization, the *Hurwitz Quaternions* given by

$$\{x + iy + jz + kw : x, y, z, w \in \mathbb{Z} \text{ or } x, y, z, w \in \tfrac{1}{2} + \mathbb{Z}\}$$

do form a ring with this property.

Proposition 3 *Let n, m be integers.*

(i) *If n, m are sums of two squares, then nm is a sum of two squares.*

(ii) *If $n, m$are sums of four squares, then nm is a sum of four squares.*

Proof: These follow immediately from the structure of $\mathbb{C}$ and $\mathbb{H}$: for (i) let $n = a^2 + b^2$ and $m = c^2 + d^2$ and set $(a + bi)(c + di) = (f + gi)$. Then $\sqrt{nm} = \sqrt{a^2 + b^2}\sqrt{c^2 + d^2} = \sqrt{f^2 + g^2}$ so $nm = f^2 + g^2$. As similar argument works for (ii). $\square$

Theorem 4 (Fermat (i) and Lagrange (ii))

(i) *Every $n \in \mathbb{N}$ with no prime factor $\equiv 3 \pmod 4$ is a sum of two squares.*

(ii) *Every $n \in \mathbb{N}$ is a sum of four squares.*