On Quaternions and Octonions

Sujeet Bhalerao

20151115

MTH301

Project supervisor:

Dr. Steven Spallone

February 28, 2018

Quaternions and geometry

Quaternions (denoted by $\mathbb{H}$) are usually represented in the form $a + bi + cj + dk$ where $a, b, c, d \in \mathbb{R}$ and i, j, k satisfy $i^2 = j^2 = k^2 = ijk = -1$. They can be represented as pairs of complex numbers (which themselves can be thought of as pairs of real numbers). The Cayley-Dickson construction uses this representation extensively. The quaternion $a + bi + cj + dk$ corresponds to the complex pair $(a + ib, c + id)$.

Example 1. Multiplication of quaternions is not commutative: $ij = k \neq ji = -k$.

As a vector space over $\mathbb{R}$, $\mathbb{H}$ is isomorphic to $\mathbb{R}^4$. The map $a + ib + jc + dk \mapsto (a, b, c, d)$ is an isomorphism between the two vector spaces.

1.1 O_n and GO_n

Definition 1. A linear map $L : \mathbb{R}^n \to \mathbb{R}^n$ is said to be **orthogonal** (or a **Euclidean congruence**) if $\|Lv\| = \|v\|$ for all $v \in \mathbb{R}^n$.

Example 2. As an example, consider the linear map $L : \mathbb{R}^2 \to \mathbb{R}^2$ given by $L(x, y) = (y, x)$. The matrix representation of L w.r.t the standard basis is

$$L = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.$$

Let $v = \begin{pmatrix} x \\ y \end{pmatrix}$ be an arbitrary element of $\mathbb{R}^2$. We now verify that L satisfies the condition for being orthogonal, that is, $\|Lv\| = \|v\|$.

$$\|Lv\| = \left\| \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} \right\| = \left\| \begin{pmatrix} y \\ x \end{pmatrix} \right\| = \|v\|.$$

Therefore L is orthogonal.

Definition 2. A linear map $L : \mathbb{R}^n \to \mathbb{R}^n$ is a **Euclidean similarity** if there exists $\lambda \in \mathbb{R}_{>0}$ such that $\|Lv\| = \lambda\|v\|$ for all $v \in \mathbb{R}^n$. Then, λ is called the multiplier.

Example 3. We claim that the following matrix L is an example of a Euclidean similarity of $\mathbb{R}^2$

$$L = \begin{pmatrix} 0 & 2 \\ -2 & 0 \end{pmatrix}$$

Let v be any element of $\mathbb{R}^2$. Written as a column vector, we have

$$v = \begin{pmatrix} x \\ y \end{pmatrix}$$

Then , $\|v\| = \sqrt{x^2 + y^2}$.

We now check that there does indeed exist a multiplier λ such that $\|Lv\| = \lambda \|v\|$.

$$\|Lv\| = \left\| \begin{pmatrix} 0 & 2 \\ -2 & 0 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} \right\| = \left\| \begin{pmatrix} 2x \\ -2y \end{pmatrix} \right\| = 2\sqrt{x^2 + y^2} = 2\|v\|.$$

Therefore, L is a Euclidean similarity of $\mathbb{R}^2$ with $\lambda = 2$.

Lemma 1. The following holds for all v, w belonging to a inner product space V over $\mathbb{R}$:

$$\langle v, w \rangle = \frac{\|v + w\|^2 - \|v - w\|^2}{4}$$

Proof. We use the fact that norms and inner products are related by $\langle v, v \rangle = \|v\|^2$ to rewrite the right side of the required identity as

$$\frac{\|v + w\|^2 - \|v - w\|^2}{4}$$

$$= \frac{\langle v + w, v + w \rangle - \langle v - w, v - w \rangle}{4}$$

$$= \frac{\langle v, v \rangle + 2\langle v, w \rangle + \langle w, w \rangle - (\langle v, v \rangle - 2\langle v, w \rangle + \langle w, w \rangle)}{4}$$

$$= \langle v, w \rangle.$$

■

Theorem 2. If a linear map $L\colon \mathbb{R}^n \to \mathbb{R}^n$ is a Euclidean similarity with multiplier λ, then $\langle Lv, Lw\rangle = \lambda^2\langle v, w\rangle$.

Proof. By Lemma 1, we can write

$$\begin{aligned}
\langle Lv, Lw\rangle &= \frac{\|Lv + Lw\|^2 - \|Lv - Lw\|^2}{4} \\
&= \frac{\|L(v + w)\|^2 - \|L(v - w)\|^2}{4} \\
&= \frac{\|\lambda(v + w)\|^2 - \|\lambda(v - w)\|^2}{4} \\
&= \frac{\lambda^2(\|(v + w)\|^2 - \|(v - w)\|^2)}{4} \\
&= \lambda^2\langle v, w\rangle.
\end{aligned}$$

■

Definition 3. The **orthogonal group** O_n is the group of Euclidean congruences of $\mathbb{R}^n$. Equivalently, it is the group of $n \times n$ orthogonal matrices. A proof of this equivalence is given in Theorem 4.

Definition 4. The **general orthogonal group** GO_n is the group of Euclidean similarities of $\mathbb{R}^n$.

Theorem 3. The map $L \mapsto \lambda$ which sends each similarity of $\mathbb{R}^n$ to its multiplier is a homomorphism from GO_n to $\mathbb{R}_{>0}$. The kernel of this map is O_n.

Proof. For the given map to be a homomorphism, it must send the composition of two similarities L_1 and L_2 to the product of their multipliers λ_1 and λ_2. To put it slightly differently, the similarity $L_1 \circ L_2$ must have multiplier $\lambda_1\lambda_2$. This is true because one can write $\|L_1 \circ L_2(v)\| = \|L_1(L_2(v))\| = \lambda_1 \|L_2(v)\| = \lambda_1\lambda_2 \|v\|$.

The kernel of the given map is the set containing all elements of GO_n which have multiplier 1. Therefore, $\|Lv\| = \|v\|, \forall v \in \mathbb{R}^n$ is true for each element L in the kernel. This implies that the kernel is the collection of Euclidean congruences of $\mathbb{R}^n$ which is precisely O_n.

■

Definition 5. If W is a subspace of a vector space V, the codimension of W is defined as

$$\text{codim } W = \dim V - \dim W$$

W is said to be a **hyperplane** in V if codim $W = 1$.

Example 4. Lines and planes are hyperplanes in $\mathbb{R}^2$ and $\mathbb{R}^3$ respectively.

Theorem 4. Let $A : \mathbb{R}^n \to \mathbb{R}^n$ be a linear transformation. The following are equivalent:
1)$AA^T = I$.
2) For all $v \in \mathbb{R}^n$ $\|Av\| = \|v\|$.
3) For all $v, w \in \mathbb{R}^n, \langle Av, Aw\rangle = \langle v, w\rangle$.

Proof. We first prove that statements 2 and 3 are equivalent. Then we show that $1 \implies 2$ and $3 \implies 1$.

We start by proving $3 \implies 2$.
From (3) we have,

$$\begin{aligned} \langle Av, Aw\rangle = \langle v, w\rangle \quad \forall v, w \in \mathbb{R}^n. \\ v = w \implies \langle Av, Av\rangle = \langle v, v\rangle. \\ \implies \|Av\| = \|v\|. \end{aligned}$$

To show the converse, we use Lemma 1 to write

$$\begin{aligned} \langle Av, Aw\rangle &= \frac{\|Av + Aw\|^2 - \|Av - Aw\|^2}{4} \\ &= \frac{\|A(v + w)\|^2 - \|A(v - w)\|^2}{4} \\ &= \frac{\|v + w\|^2 - \|v - w\|^2}{4} \\ &= \langle v, w\rangle. \end{aligned}$$

Now we show $1 \implies 2$.

$$\begin{aligned} \|Av\| &= \sqrt{\langle Av, Av\rangle} \\ &= \sqrt{Av.Av} \\ &= \sqrt{(Av)^\intercal (Av)} \\ &= \sqrt{v^\intercal A^\intercal Av} \\ &= \sqrt{v^\intercal v} \\ &= \|v\|. \end{aligned}$$

The proof is completed by showing $3 \implies 1$.
$3 \implies \langle Av, Aw\rangle = \langle v, w\rangle \quad \forall v, w \in \mathbb{R}^n$.

$$\begin{aligned}\langle Av, Aw\rangle &= Av.Aw \\ &= (Av)^\intercal(Aw) \\ &= v^\intercal A^\intercal Aw \\ &= v^\intercal w.\end{aligned}$$

It suffices to show that if $v^\intercal Bw = v^\intercal B'w \; \forall v, w \in \mathbb{R}^n$, then $B = B'$. This implies $AA^\intercal = I$.

Since $v^\intercal Bw = v^\intercal B'w$ is true for all $v, w \in \mathbb{R}^n$,
$(e_i)^\intercal Be_j = (e_i)^\intercal B'e_j$. This gives $b_{ij} = b'_{ij}$. Hence, $B = B'$.

■

Theorem 5. All eigenvalues λ of an orthogonal matrix A satisfy $|\lambda| = 1$.

Proof. Any eigenvalue λ must satisfy $Av = \lambda v$. Since A is an orthogonal matrix, we must have $\|Av\| = \|v\|$. Therefore $\|\lambda v\| = \|v\|$. Since $\|v\|$ is nonzero, $|\lambda| = 1$. ■

Theorem 6. If $L \in GO_n$ with $L(v) = v$, then $L(v^\perp) = v^\perp$.
Here, $v^\perp = \{w \in V : \langle v, w\rangle = 0\}$.

Proof. We show set inclusion both ways.
Suppose $w \in v^\perp$. Then $\langle v, L(w)\rangle = \langle L(v), L(w)\rangle = \lambda^2\langle v, w\rangle = 0$. Therefore, $L(v^\perp) \subset v^\perp$.
To show the reverse inclusion, let $w \in v^\perp$. We must show that $w = L(u)$ for some $u \in v^\perp$.
Observe that $u = L^{-1}(w) \in v^\perp$ since $\langle v, L^{-1}(w)\rangle = \langle L^{-1}(v), L^{-1}(w)\rangle = \lambda^2\langle v, w\rangle = 0$. ■

1.2 Quaternions and 3-dimensional rotations

Theorem 7. There exists a linear map $L : \mathbb{R}^3 \to \mathbb{R}^3$ given by $L(v) = qvq^{-1}$ where q is a quaternion of the form $ai + bj + ck$. Moreover, L is a Euclidean congruence of $\mathbb{R}^3$.

Proof. Consider the linear map $L : \mathbb{R}^4 \to \mathbb{R}^4$ given by $L(v) = q_1vq_2$ where q_1 and q_2 are quaternions. Recall that $\mathbb{H}$ and $\mathbb{R}^4$ are isomorphic. Each element (a, b, c, d) of $\mathbb{R}^4$ can thus be identified with the quaternion $a + bi + cj + dk$. We have, $N(q_1vq_2) = N(q_1)N(v)N(q_2)$ where $N(a + ib + cj + dk) = a^2 + b^2 + c^2 + d^2$. Therefore, $L \in GO_4$ with multiplier $\lambda = \sqrt{N(q_1)N(q_2)}$. If $L(\mathbb{1}) = \mathbb{1}$, by Theorem 5, L must fix the 3-dimensional space perpendicular to $\mathbb{1}$, which contains elements of the form $ai + bj + ck$ (since the inner product with $\mathbb{1}$ must be 0). L fixes $\mathbb{1}$ if $q_2 = q_1^{-1}$. Hence, $L(v) = qvq^{-1}$ fixes a 3-dimensional space perpendicular to $\mathbb{1}$, which is isomorphic to $\mathbb{R}^3$. Also, $L \in O_3$ because $N(qvq^{-1}) = N(v)$. ■

1.3 Reflections in $\mathbb{R}^n$

Lemma 8. Suppose v is a nonzero element of $\mathbb{R}^n$. Let $H = v^\perp$. So $\mathbb{R}^n = \mathbb{R}v \oplus H$. Every element w of $\mathbb{R}^n$ can be written uniquely in the form $w = \lambda v + h$, with $\lambda \in \mathbb{R}$, $h \in H$.

Definition 6. The reflection s_v of $\mathbb{R}^n$ determined by v is defined as $s_v(w) = (-\lambda)v + h$, for w as in Lemma 8.

Example 5. Pick

$$v = e_2 = \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix} \in \mathbb{R}^3.$$

Since e_1 and e_2 belong to $v^\perp$, the matrix form of s_{e_2} is

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

.

We now prove a few theorems about reflections.

Theorem 9. The eigenvalues of a reflection are $\pm$ 1.

Proof. For any eigenvalue β and eigenvector $w = \lambda v + h$ of s_v we must have $s_v(w) = \beta w$, i.e., $-\lambda v + h = \beta\lambda v + \beta h$. Rearranging this equation and using the fact that v and h are perpendicular gives us the desired result. ■

Theorem 10. The -1 eigenspace is $\mathbb{R}v$, and $+1$ eigenspace is H.

Proof. The elements of the -1 eigenspace must satisfy $s_v(w) = -w$. Therefore, we have $-\lambda v + h = -\lambda v - h$ which gives $h = 0$. w is thus of the form λv which clearly lies in $\mathbb{R}v$. Similarly, the elements of the $+1$ eigenspace satisfy $s_v(w) = w$, which gives $\lambda = 0$ and thus $w = h$, for some h in H. Hence H is the $+1$ eigenspace. ■

Theorem 11. For any reflection s_v, $s_v^2 = \mathbb{1}$.

Proof. Suppose $w = \lambda v + h$ for some $\lambda \in \mathbb{R}$ and $h \in v^\perp$. Then $s_v^2(w) = s_v(s_v(\lambda v + h)) = s_v(-\lambda v + h) = (\lambda v + h) = w$. ■

Theorem 12. Reflections are orthogonal.

Proof. We use Theorem 4 to show they preserve inner products and hence are orthogonal. We have

$$\begin{aligned} \langle s_v(w_1), s_v(w_2)\rangle &= \langle -\lambda_1 v_1 + h_1, -\lambda_2 v_2 + h_2\rangle \\ &= \langle -\lambda_1 v_1 + h_1, -\lambda_2 v_2 + h_2\rangle \\ &= \lambda^2\langle v_1, v_2\rangle + (-\lambda)\langle v_1, h_2\rangle + (-\lambda)\langle h_1, v_2\rangle + \langle h_1, h_2\rangle \\ &= \lambda^2\langle v_1, v_2\rangle + \langle h_1, h_2\rangle \\ &= \langle w_1, w_2\rangle. \end{aligned}$$

We use the fact that v_1 and v_2 are perpendicular to h_2 and h_1 respectively. ■

Quaternions and number theory

2.1 Euclidean algorithm for rational integers

We begin by recalling the Euclidean algorithm for rational integers before moving on to the Gaussian integers. Throughout this section, the word 'integer' denotes a rational integer. The Euclidean algorithm is a method for computing the gcd of two numbers a and b. The division algorithm states that given any two integers a and nonzero b with $a > b$, there exist unique integers q and r such that $a = bq + r$ such that $0 \leq r < b$. If the remainder r obtained using the division algorithm is non-zero, we apply the division algorithm to b and r to get

$$b = rq_1 + r_1 \text{ with } 0 \leq r_1 < r.$$

This process can be repeated with r and r_1, r_1 and r_2 and so on until one obtains, for some n, $r_{n+1} = 0$. This will eventually occur because $r_1, r_2, r_3...$ is a strictly decreasing sequence of integers bounded below by zero. The last steps of the algorithm will look like:

$$\begin{aligned} &\vdots \\ r_{n-2} &= r_{n-1}q_n + r_n \\ r_{n-1} &= r_n q_{n+1} + 0. \end{aligned}$$

Lemma 13. Let $a, b, q, r \in \mathbb{Z}$ such that $a = bq + r$. Then $\gcd(a, b) = \gcd(b, r)$.

Proof. We show that $\gcd(a, b)$ and $\gcd(b, r)$ are divisors of each other.
By definition of gcd, we have that $\gcd(a, b) \mid a$, $\gcd(a, b) \mid b$. Therefore, $\gcd(a, b) \mid r$. By the definition of gcd (again), we have $\gcd(a, b) \mid \gcd(b, r)$. Nearly identical reasoning gives us $\gcd(b, r) \mid \gcd(a, b)$. Thus we have $\gcd(a, b) = \gcd(b, r)$. ■

Claim. $\gcd(a, b) = r_n$.

Proof. By Lemma 13, we have that $\gcd(a, b) = \gcd(b, r) = \gcd(r, r_1) = ... = \gcd(r_{n-1}, r_n) = \gcd(r_n, 0) = r_n$. ■

We state a few definitions to get started on the general notion of an 'integer'.

Definition 7. A **Gaussian integer** is a complex number of the form $a + bi$ where a and b are rational integers.

Definition 8. An **Eisenstein integer** is a complex number of the form $a + b\omega$ where a and b are rational integers and $w = \frac{-1+i\sqrt{3}}{2}$.

Definition 9. A **Kleinian integer** is a complex number of the form $a + b\lambda$ where a and b are rational integers and $\lambda = \frac{-1+i\sqrt{7}}{2}$.

Definition 10. A **Hurwitz integer** is a quaternion of the form $a + bi + cj + dk$ where a, b, c, d are all rational integers or all multiples of $\frac{1}{2}$.

Definition 11. A **Lipschitz integer** is a quaternion of the form $a + bi + cj + dk$ where a, b, c, d are all rational integers.

2.2 Gaussian integers

The Gaussian integers are denoted by $\mathbb{Z}[i]$.
A few pertinent definitions from ring theory are stated before we study $\mathbb{Z}[i]$.
Let R be a commutative ring.

Definition 12. An element x of R is said to be a **unit** if there exists a $y \in R$ such that $xy = 1_R$.

Definition 13. Two elements $x, y \in R$ are said to be **associates** if there exists a unit u such that $x = uy$.

Definition 14. A nonzero element $x \in R$ is said to be **irreducible** if $x = yz$implies y or z is a unit.

Definition 15. A nonzero element $x \in R$ is said to be **prime** if x is not a unit and $x \mid yz \implies x \mid y$ or $x \mid z$.

Primes and irreducibles in a ring are not always the same.

Example 6. Consider the ring $\mathbb{Z}[\sqrt{-5}]$. We show that $3 \in \mathbb{Z}[\sqrt{-5}]$ is irreducible but not prime. $3 \mid (2+\sqrt{-5})(2-\sqrt{-5})$ but it does not divide either of the two factors. Therefore 3 is not prime. We show 3 is irreducible: suppose $3 = pq$. Then applying norm gives us $9 = N(p)N(q)$. Since $N(a+b\sqrt{-5}) = a^2 + 5b^2 = 3$ has no solutions, one of p or q must be a unit.

Definition 16. The norm of a Gaussian integer $a + bi$ is defined as $N(a + bi) = a^2 + b^2$.

It is clear that the norm of any nonzero Gaussian integer is a positive integer.

Theorem 14. The following statements are equivalent:
1) $u \in \mathbb{Z}[i]$ is a unit.
2) $N(u) = 1$.

Proof. Suppose $u \in \mathbb{Z}[i]$ is a unit. Therefore, there exists $y \in \mathbb{Z}[i]$ such that $uy = 1$. Hence $N(uy) = 1$. By multiplicativity of norm, $N(u)N(y) = 1$. Since each of $N(u)$ and $N(y)$ are positive integers, we must have $N(y) = N(u) = 1$.
Conversely, suppose that $N(u) = 1$. By definition of norm, $u\bar{u} = 1$. Since $\bar{u} \in \mathbb{Z}[i]$, u is a unit. ■

Theorem 15. There are four units in the Gaussian integers, namely 1, -1, i, $-i$.

Proof. By Theorem 14, every unit has norm 1. If $u = a + bi$ is a unit, $a^2 + b^2 = 1$. The number of solutions (a, b) to this equation are precisely four: $(1, 0)$, $(0, 1)$, $(-1, 0)$, $(0, -1)$. These correspond to 1, -1, i, $-i$. ■

Theorem 16. The division algorithm for Gaussian integers states that if Z and z are two Gaussian integers, then there are Gaussian integers Q and R such that $N(R) < N(z)$ and $Z = zQ + R$.

Proof. Let $Zz^{-1} = x + yi$. Define $Q = X + Yi$ to be the closest Gaussian integer to $x + yi$ and $R = Z - zQ$. We will thus have $|X - x| \leq 1/2$ and $|Y - y| \leq 1/2$. It remains to show that $N(R) < N(z)$. Observe that $N(Rz^{-1}) = N(Zz^{-1} - Q) = (x - X)^2 + (y - Y)^2 \leq \frac{1}{4} + \frac{1}{4} = \frac{1}{2}$. Therefore $N(R) \leq \frac{1}{2}N(z)$. This completes the proof.

■

Note that the Gaussian integers Q and R obtained in the division algorithm need not be unique.

Example 7. For example, if we have $Z = 3 + 3i$ and $z = 2 + 0i$, we can write $3 + 3i = 2(2 + 2i) + (-1 - i)$ and $3 + 3i = 2(1 + i) + (1 + i)$. In each case we have $N(-1 - i) = N(1 + i) = 2 \leq 4 = N(2)$. Therefore, these satisy the criterion for Q and R in the divison algorithm.

2.3 Integral quaternions

We now extend the notion of an integer to the quaternions in the form of Hurwitz integers (denoted $\mathbb{H}_\mathbb{Z}$).

Definition 17. The norm of a Hurwitz integer is defined as $N(a + bi + cj + dk) = a^2 + b^2 + c^2 + d^2$.

Theorem 17. The Hurwitz integers form an abelian group under addition.

Proof. The identity is 0. The inverse of $a + bi + cj + dk$ is $-a - bi - cj - dk$. The group operation is clearly associative. The sum of two Lipschitz integers is also a Lipschitz integer. The sum of a Hurwitz (but not Lipschitz) integer and a Lipschitz integer is again a Hurwitz (but not Lipschitz) integer. The sum of two Hurwitz integers with half integer coordinates is a Lipschitz integer. This shows closure of $\mathbb{H}_\mathbb{Z}$ under $+$ and completes the proof. ■

Theorem 18. The norm of any nonzero Hurwitz integer is a positive integer.

Proof. The norm of a nonzero Lipschitz integer $a + bi + cj + dk$ is clearly a positive integer. We consider the remaining case where $a + bi + cj + dk$ is a Hurwitz integer with a, b, c, $d \in \mathbb{Z} + \frac{1}{2}$. One can rewrite $a + bi + cj + dk$ as $\frac{p_1 + p_2 i + p_3 j + p_4 k}{2}$ with each p_i odd. Therefore $N(a + bi + cj + dk) = \frac{p_1^2 + p_2^2 + p_3^2 + p_4^2}{4}$. Since $p_i s$ are odd, $p_i^2 \equiv 1 \pmod 4$. Thus we have $p_1^2 + p_2^2 + p_3^2 + p_4^2 \equiv 0 \pmod 4$. Hence $\frac{p_1^2 + p_2^2 + p_3^2 + p_4^2}{4}$ is a positive integer. ■

2.4 Primes and units

Theorem 19. The following statements are equivalent:
1) $u \in \mathbb{H}_\mathbb{Z}$ is a unit.
2) $N(u) = 1$.

Proof. Suppose $u \in \mathbb{H}_\mathbb{Z}$ is a unit. Therefore, there exists $y \in \mathbb{H}_\mathbb{Z}$ such that $uy = 1$. Hence $N(uy) = 1$. By multiplicativity of norm, $N(u)N(y) = 1$. Since each of $N(u)$ and $N(y)$ are positive integers, we must have $N(y) = N(u) = 1$.
Conversely, suppose that $N(u) = 1$. By definition of norm, $u\bar{u} = 1$. Since $\bar{u} \in \mathbb{H}_\mathbb{Z}$, u is a unit. ■

Theorem 20. There are 24 units in $\mathbb{H}_\mathbb{Z}$, namely the eight Lipschitz units $\pm 1, \pm i, \pm j, \pm k$, and the 16 others $\pm\frac{1}{2} \pm \frac{1}{2}i \pm \frac{1}{2}j \pm \frac{1}{2}k$.

Proof. If $a+bi+cj+dk$ is a Lipschitz unit, we must have at least one of $|a|$, $|b|$, $|c|$, $|d| \geq 1$. Also, by Theorem 12 we have $a^2+b^2+c^2+d^2 = 1$. If we have any two of $|a|$, $|b|$, $|c|$, $|d| \geq 1$, then $a^2 + b^2 + c^2 + d^2 > 1$. Therefore we must have exactly one coordinate equal to ± 1 and the rest 0. This gives us the eight Lipschitz units $\pm 1, \pm i, \pm j, \pm k$,.
For a non-Lipschitz unit, we must have $|a|$, $|b|$, $|c|$, $|d| \geq \frac{1}{2}$. If any one of these is $> \frac{1}{2}$ then $a^2 + b^2 + c^2 + d^2 > \frac{9}{4}$, which contradicts the definition of a unit. Therefore we must have $|a| = |b| = |c| = |d| = \frac{1}{2}$. This gives us 16 other units of the form $\pm\frac{1}{2} \pm \frac{1}{2}i \pm \frac{1}{2}j \pm \frac{1}{2}k$. . ■

We first state and prove the division algorithm for Lipschitz integers and then for Hurwitz integers with an explanation of why Hurwitz's definition of integral quaternions is preferable.

Theorem 21. The division algorithm for Lipschitz integers states that if Z and z are two Lipschitz integers, then there are Lipschitz integers Q and R such that $N(R) \leq N(z)$ and $Z = Qz + R$.

Proof. Let $Zz^{-1} = x+yi+zj+wk$. Define $Q = X+Yi+Zj+Wk$ to be the closest Lipschitz integer to $x + yi + zj + wk$ and $R = Z - Qz$. We will thus have $|X - x| \leq 1/2, |Y - y| \leq 1/2, |Z - z| \leq 1/2, |W - w| \leq 1/2$. It remains to show that $N(R) \leq N(z)$. Observe that $N(Rz^{-1}) = N(Zz^{-1}-Q) = (x-X)^2+(y-Y)^2+(z-Z)^2+(w-W)^2 \leq \frac{1}{4}+\frac{1}{4}+\frac{1}{4}+\frac{1}{4} = 1$. Therefore $N(R) \leq N(z)$.

■

The inequality in $N(R) \leq N(z)$ is not strict for the Lipschitz integers, unlike in the case of Gaussian integers and rational integers. If we have $|X - x| = \frac{1}{2}, |Y - y| = \frac{1}{2}, |Z - z| = \frac{1}{2}, |W-w| = \frac{1}{2}$, then $N(Rz^{-1}) = N(Zz^{-1}-Q) = (x-X)^2+(y-Y)^2+(z-Z)^2+(w-W)^2 = \frac{1}{4}+\frac{1}{4}+\frac{1}{4}+\frac{1}{4} = 1$. In other words, $N(R) = N(z)$. In fact, we have $N(R) = N(z)$ exactly when $|X - x| = \frac{1}{2}, |Y - y| = \frac{1}{2}, |Z - z| = \frac{1}{2}$ and $|W - w| = \frac{1}{2}$.
No such difficulty arises for the Hurwitz integers. This is because $N(R) = N(z)$ implies that each of x, y, z, w lies in $\mathbb{Z} + \frac{1}{2}$, i.e., $Zz^{-1} = x + yi + zj + wk$ is a Hurwitz integer, and we have $Z = qz + 0$ with $N(0) < N(z)$.
We state the division algorithm for Hurwitz integers separately:

Theorem 22. The division algorithm for Hurwitz integers states that if Z and z are two Hurwitz integers, then there are Hurwitz integers Q and R such that $N(R) < N(z)$ and $Z = Qz + R$.

We now turn our attention to the prime factorization of Hurwitz integers. Two cases arise, one where the integer is imprimitive and the other of primitive integers. We say a Hurwitz integer is **imprimitive** if it is divisible by a natural number greater than 1. The following theorem deals with the primitive case.

Theorem 23. To any factorization of the norm q of a primitive Hurwitz integer Q into a product $p_0p_1p_2\cdots p_k$ of rational primes, there is a factorization

$$Q = P_0P_1\cdots P_k$$

of Q into a product of Hurwitz primes with $N(P_0) = p_0, ..., N(P_k) = p_k$. We say that "the factorization of $P_0P_1\cdots P_k$ of Q is modelled on the factorization $p_0p_1p_2\cdots p_k$ of $N(Q)$." Also, if $Q = P_0P_1\cdots P_k$ is any factorization modelled on $p_0p_1p_2\cdots p_k$, then the others have the form

$$Q = P_0U_1 \cdot U_1^{-1}P_1U_2 \cdot ... \cdot U_k^{-1}P_k$$

i.e. "the factorization on a given model is unique up to unit migration."

Proof. Note that the ideal $p_0H + QH$ must be principal. Hence, we have that

$$p_0H + QH = P_0H$$

for some P_0. Therefore $[P_0]$ must divide $[p_0] = p_0^2$, forcing it to be one of $1, p_0, p_0^2$. We now rule out the cases $[P_0] = 1$ and $[P_0] = p_0^2$. The general element $p_0a + Qb$ has norm $[p_0a] + 2[p_0a, Qb] + [Qb] = p_0^2[a] + 2p_0[a, Qb] + [Q][b]$ which is divisible by p_0 since $[Q]$ is divisible by p_0. This eliminates the case $[P_0] = 1$. If $[P_0]$ is p_0^2, then since P_0 divides p_0 we must have $P_0 = p_0U$ for some unit U. This shows that p_0 divides Q, since P_0 divides Q. However, we assumed that Q is a primitive Hurwitz integer, and thus we arrive at a contradiction. Therefore, we must have that $[P_0] = p_0$. Hence, P_0 is a Hurwitz prime dividing Q.
This gives us $Q = P_0Q_1$ where $[Q_1] = p_1p_2\cdots p_k$, and P_0 is unique upto right multiplication by a unit. We can now repeat the argument ot write $Q = P_1P_2...P_kQ'$ where Q' is a unit. The argument also shows that the factorization is unique up to unit migration.

■

Example 8. We give an example of the prime factorization of a primitive Hurwitz quaternion of norm 90. Up to unit migration, such a quaternion will have 12 factorizations into prime quaternions. These are exactly the ones that are modelled on the following 12 factorizations of 90 into rational primes:

2.3.3.5	2.3.5.3	2.5.3.3	5.2.3.3	5.3.2.3	5.3.3.2
3.3.5.2	3.5.2.3	3.3.2.5	3.2.5.3	3.5.3.2	3.2.3.5

The total number of factorizations will be $24^3 \cdot 12 = 165888$ since there are 24 units in the Hurwitz integers and 3 places for these units to migrate across.

Octonions

Definition 18. The **octonions** are formal expressions

$$x_\infty + x_0 i_0 + x_1 i_1 + x_2 i_2 + x_3 i_3 + x_4 i_4 + x_5 i_5 + x_6 i_6$$

with each x_t being a real number. These formal expressions constitute the $\mathbb{R}$-algebra generated by the units $i_0, i_1, i_2, i_3, i_4, i_5, i_6, i_\infty$. The units satisfy

$$i_n^2 = -1$$

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

The octonions can be thought of 8-tuples of real numbers. We represent the unit octonions as $i_0, i_1, i_2, i_3, i_4, i_5, i_6, i_\infty$ with i_∞ being the real element which we take to be 1. Any octonion x can be expressed as a linear combination of the unit elements as $x = x_\infty i_\infty + x_0 i_0 + x_1 i_1 + x_2 i_2 + x_3 i_3 + x_4 i_4 + x_5 i_5 + x_6 i_6$.
One can also define the octonions using the Cayley-Dickson construction in the following manner: Within the Cayley Dickson construction, quaternions are defined as pairs of complex numbers. Similarly, one defines octonions as pairs of quaternions with the multiplication defined by

$$(a, b)(c, d) = (ac - \overline{d} b, da + b\overline{c})$$

This definition is equivalent to the previous one. The unit octonions in this definition are the pairs

$$(1, 0)\ (i, 0)\ (j, 0)\ (k, 0)\ (0, 1)\ (0, i)\ (0, j)\ (0, k)$$

A useful mnemonic for remembering the multiplication of the octonions is given by the Fano plane. Each of the seven lines in the figure is oriented and generates a subalgebra which is isomorphic to the quaternions. Each basis element of the imaginary octonions is a point in the figure.

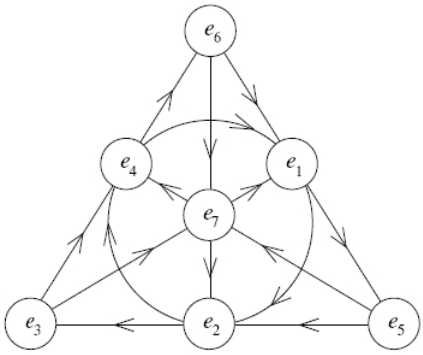

Figure 3.1: The Fano plane as a mnemonic.

Example 9. The octononions are not asssociative. For instance

$$i_0.i_2i_1 = -i_5$$

$$i_0i_2.i_1 = i_5$$

Composition algebras

One can prove the two-square identity

$$(x_1y_1 - x_2y_2)^2 + (x_1y_2 + x_2y_1)^2 = (x_1^2 + x_2^2)(y_1^2 + y_2^2)$$

using the fact that the norm of a product of two complex numbers is the product of the norms. In this section we look into general algebraic structures with this property. We begin with the necessary definitions.

Definition 19. An $\mathbb{R}-$**algebra** is a vector space V over the real numbers with a binary operation $\cdot : V \times V \to V$ satisfying the following properties:

- Right distributivity: $(x + y) \cdot z = (x \cdot z) + (y \cdot z)$
- Left distributivity: $x \cdot (y + z) = (x \cdot y) + (x \cdot z)$
- Compatibility with scalars: $(ax) \cdot (by) = (ab)(x \cdot y)$

Here x, y and z denote elements of the vector space while a, b are elements of the field $\mathbb{R}$. A binary operation that satisfies the above three axioms is said to be **bilinear**. One need not worry about having separate axioms for right and left distributivity when the binary operation is commutative. However this is not always the case. Indeed, the quaternions are an example of a noncommutative algebra.

Example 10. The set of $n \times n$ real matrices form an algebra with the usual matrix multiplication.

Definition 20. A **bilinear form** on a vector space V is a bilinear map from $V \times V \to F$ where F is the underlying field.

Definition 21. A **degenerate bilinear form** $f(x, y)$ on a finite dimensional vector space V is a bilinear form such that it has a non-trivial kernel, i.e., there exists a non-zero x in V such that

$$f(x, y) = 0 \text{ for all } y \in V.$$

Definition 22. A bilinear form f is called **symmetric** if it satisfies

$$f(v, w) = f(w, v) \text{ for all } v, w \in V.$$

Example 11. The standard dot product on $\mathbb{R}^n$ is an example of a symmetric bilinear form.

Definition 23. A **nondegenerate bilinear form** on a finite dimensional vector space is a bilinear form that is not degenerate. In other words,

$$f(x, y) = 0 \text{ for all } y \in V \text{ implies that } x = 0.$$

Definition 24. A **quadratic form** is a map from V to the underlying field F satisfying

- $f(kv) = k^2 v$ for all $v \in V$ and $k \in F$.
- $b_f(u, v) = f(u + v) - f(u) - f(v)$ is a symmetric bilinear form.

Theorem 24. If f is a symmetric bilinear form on V, then $f(v) = b_f(v, v)$ is a quadratic form in V. Furthermore, $b_f(u, v) = 2(u, v)$ for all $u, v \in V$.

Definition 25. A **composition algebra** over a field K is a not necessarily associative algebra together with a non degenerate quadratic form N that satisfies

$$N(xy) = N(x)N(y) \text{ for all } x \text{ and } y \text{ in } A.$$

Throughout this section and the next, we adopt the convention that $[x]$ denotes the norm of x and $[x, y]$ denotes the inner product of x and y. Here, the inner product $[x, y]$ is the symmetric bilinear form $\frac{b_f(u,v)}{2}$ associated with the quadratic from $[\cdot]$. Hence, we have that

$$[x, y] = \frac{[x + y] - [x] - [y]}{2}.$$

We also assume that our algebra is **unital**, that is, there exists an identity element satisfying

$$x \cdot 1 = 1 \cdot x = x.$$

Properties of composition algebras

We now explore the properties of composition algebras.

Theorem 25. If $[x,t] = [y,t]$ for all t then $x = y$.

Proof. Since $[x,t] = [y,t]$, we have that $[x-y,t] = 0$ for all t. Since the norm $[\cdot]$ is a non-degenerate quadratic form, we must have that $x - y = 0$ which gives $x = y$. ■

5.1 Multiplication laws

We state the composition law and deduce its consequences. In the proofs of the theorems that follow, we make considerable use of Theorem 25 and the relation between the inner product and the norm.

Theorem 26. The Composition Law:

$$[xy] = [x][y] \tag{M1}$$

Theorem 27. The Scaling Laws:

$$[xy, xz] = [x][y,z] \tag{M2.1}$$

Proof. Replacing y by $y + z$ in (M1) gives

$$[x(y+z)] = [x][y+z].$$

$$\begin{aligned}
& [x(y+z)] = [xy + xz] \\
\implies \quad & [x][y+z] = [xy] + [xz] + 2[xy, xz] \\
\implies \quad & [x]([y] + [z] + 2[y,z]) = [xy] + [xz] + 2[xy, xz] \\
\implies \quad & [x][y] + [x][z] + 2[x][y,z] = [xy] + [xz] + 2[xy, xz] \\
\implies \quad & [xy] + [xz] + 2[x][y,z] = [xy] + [xz] + 2[xy, xz] \\
\implies \quad & [x][y,z] = [xy, xz]
\end{aligned}$$

■

$$[xz, yz] = [x,y][z] \tag{M2.2}$$

Proof. Replace x by $x + z$ in M1. This gives

$$[(x+z)y] = [x+z][y]$$

$$\begin{aligned}
& [(x+z)y] = [xy+zy] \\
\implies \quad & [x+z][y] = [xy]+[zy]+2[xy,zy] \\
\implies \quad & ([x]+[z]+2[x,z])[y] = [xy]+[zy]+2[xy,zy] \\
\implies \quad & [x][y]+[z][y]+2[x][y,z] = [xy]+[zy]+2[xy,zy] \\
\implies \quad & [xy]+[zy]+2[x][y,z] = [xy]+[zy]+2[xy,zy] \\
\implies \quad & [x,z][y] = [xy,zy]
\end{aligned}$$

■

Theorem 28. The Exchange Law:

$$[xy,uz] = 2[x,u][y,z] - [xz,uy] \tag{M3}$$

Proof. Replacing x by $x + u$ in M2.1 gives

$$[(x+u)y,(x+u)z] = [x+u][y,z]$$

The left hand side is

$$\begin{aligned}
[xy+uy,xz+uz] &= [xy,xz]+[xy,uz]+[uy,xz]+[uy,uz] \\
&= [x][y,z]+[xy,uz]+[uy,xz]+[u][y,z]
\end{aligned}$$

The right hand side is

$$\begin{aligned}
[x+u][y,z] &= ([x]+[u]+2[x,u])([y,z]) \\
&= [x][y,z]+[u][y,z]+2[x,u][y,z]
\end{aligned}$$

Equating the two sides gives

$$2[x,u][y,z] = [xy,uz]+[uy,xz], \text{ as desired.}$$

■

5.1.1 Conjugation Laws

Definition 26. The **conjugate** of x is defined as

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

Theorem 29. Braid Laws:

$$[xy,z] = [y,\bar{x}z] \tag{C1}$$

Proof. Put $u = 1$ in M3. We get

$$\begin{aligned}[xy, z] &= 2[x, 1][y, z] - [y, xz] \\ &= [y, 2[x, 1]z] - [y, xz] \\ &= [y, (2[x, 1] - x)z] \\ &= [y, \overline{x}z]\end{aligned}$$

■

$$[xy, z] = [x, z\bar{y}]$$

Proof. Put $z = 1$ in M3. We get

$$\begin{aligned}[xy, u] &= 2[x, u][y, 1] - [x, uy] \\ &= [x, u(2[y, 1] - y)] \\ &= [x, u\overline{y}]\end{aligned}$$

■

Theorem 30. Biconjugation:

$$\bar{\bar{x}} = x. \tag{C2}$$

Proof. We use Theorem 25.

$$[x, t] = [1.x, t] = [1, \overline{x}t] = [\overline{x}t, 1] = [t, \bar{\bar{x}}.1] = [\bar{\bar{x}}.1, t] = [\bar{\bar{x}}, t]$$

■

Theorem 31. Product conjugation:

$$\overline{xy} = \bar{y}\bar{x}. \tag{C3}$$

Proof. Theorem 25 is used along with (C2).

$$[\bar{y}\bar{x}, t] = [\overline{x}, yt] = [\overline{x}\bar{t}, y] = [\bar{t}, xy] = [\bar{t}.\overline{xy}, 1] = [\overline{xy}, t]$$

■

5.2 The Doubling Laws

Definition 27. Suppose H is an n-dimensional subalgebra of an algebra A conatining 1, and i is a unit vector orthogonal to H. The **Dickson double** of H is the algebra $H + iH$.

The inner product, conjugation and multiplication on the double of H are given by the following theorems.

Theorem 32. Inner-Product Doubling:

$$[a+ib, c+id] = [a,c] + [b,d] \tag{D1}$$

Proof. Since

$$[a, id] = [a\overline{d}, i] = 0 \qquad [ib, c] = [i, c\overline{b}] = 0 \qquad [ib, id] = [i][b,d] = [b,d],$$

we have $[a+ib, c+id] = [a,c] + [a,id] + [ib,c] + [ib,id] = [a,c] + [b,d]$. ■

Theorem 33. Conjugation Doubling:

$$\overline{a+ib} = \overline{a} - ib. \tag{D2}$$

Proof. By definition of conjugate,

$$\begin{aligned}\overline{a+ib} &= 2[a+ib, 1] - (a+ib) \\ &= 2[a,1] + 2[ib,1] - a - ib \\ &= 2[a,1] - a - ib \\ &= \overline{a} - ib.\end{aligned}$$

■

Corollary 1. $ib = \overline{b}i$.

Theorem 34. Composition Doubling:

$$(a+ib)(c+id) = (ac - d\overline{b}) + i(cb + \overline{a}d). \tag{D3}$$

Proof. Theorem 25 is used again. We have the following equalities using previous properties.

$$[a.id, t] = [id, \overline{a}t] = 0 - [it, \overline{a}d] = [t, i\overline{a}d] = [i\overline{a}d, t] \tag{5.1}$$

$$[ib.c, t] = [ib, t\overline{c}] = [\overline{b}i, t\overline{c}] = 0 - [\overline{b}\overline{c}, ti] = [\overline{b}\overline{c}.i, t] = [i.cb, t] \tag{5.2}$$

$$[ib.id, t] = [ib, t.\overline{id}] = -[ib, t.\overline{d}i] = [ib, t.id] \overset{\text{M3}}{=} 0 + [i.id, tb] = -[id, i.tb] = -[i][d, tb] = [-d\overline{b}, t] \tag{5.3}$$

Now we use the above to rewrite

$$[(a+ib)(c+id), t] = [ac, t] + [a.id, t] + [ib.c, t] + [ib.id, t] = [(ac - d\overline{b}) + i(cb + \overline{a}d), t].$$

■

5.2.1 Hurwitz's theorem

The previous subsection and the theorems within constitute a proof of the following theorem.

Theorem 35. If a composition algebra Z contains a proper subalgebra Y, it also contains its double $Y + iY$.

Lemma 36. $Z = Y + i_Z Y$ is a composition algebra if and only if Y is an associative composition algebra.

Proof. Suppose $Z = Y + i_Z Y$ is a composition algebra. Then for all $a, b, c, d \in Y$, we have

$$[a + ib][c + id] = [(ac - d\bar{b}) + i(cb + \bar{a}d)].$$
$$[a][c] + [a][d] + [b][c] + [b][d] = [ac] - 2[ac, d\bar{b}] + [cb] + 2[cb, \bar{a}d] + [ad].$$

Cancelling some terms gives us

$$[ac, d\bar{b}] = [cb, \bar{a}d]$$

By the braid law,

$$[ac.b, d] = [a.cb, d].$$

Since the above holds for all d in Y, we have that Y is an associative composition algebra. The same proof followed in the reverse direction proves the converse. ■

Lemma 37. $Y = X + i_Y X$ is an associative composition algebra if and only if X is a commutative associative composition algebra.

Proof. Suppose Y is an associative composition algebra. Then X must also be an associative composition algebra, by the previous theorem. Since in (5.2) we have shown that $i_0.bc = i_0 c.b$, we can use associativity to obtain $bc = cb$ for all b, c in X. Hence X is commutative.

For the converse, observe that on expanding out the expressions $(a+ib).(c+id)(e+if)$ and $(a + ib)(c + id).(e + if)$ we obtain two expressions that are equal precisely when we use the commutativity and associativity of X.

■

Lemma 38. $X = W + i_X W$ is an associative commutative composition algebra if and only if W is an associative commutative composition algebra with trivial conjugation.

Proof. Suppose X is an associative commutative algebra. Since we have $ei = i\bar{e}$ by Corollary 1, we use the commutativity of X to get $e = \bar{e}$ for all $e \in W$. Hence W has trivial conjugation.

Conversely, we need to show that X is commutative. Note that

$$(a + ib)(c + id) = (ac - d\bar{b}) + i(cb + \bar{a}d)$$
$$(c + id)(a + ib) = (ca - b\bar{d}) + i(ad + \bar{c}d)$$

are equal exactly when we use the fact that conjugation in W is trivial along with commutativity. ■

We now have all tools to prove the following theorem.

Theorem 39. (Hurwitz)
$\mathbb{R}$, $\mathbb{C}$, $\mathbb{H}$, $\mathbb{O}$ are the only composition algebras.

Proof. Suppose Z is an algebra. Since Z contains $\mathbb{R}$ as a subalgebra, it must be obtained by repeated doubling of $\mathbb{R}$ and must the double of some proper subalgebra, unless it is $\mathbb{R}$ itself. If Z is $\mathbb{R}$, we are done. If not, by Theorem 35, we have that Z must contain also the double of $\mathbb{R}$, which is $\mathbb{C}$. If now Z is $\mathbb{C}$, we are done. Otherwise, Z must contain the double of $\mathbb{C}$, which is the quaternions. If Z is $\mathbb{H}$, we are done. Otherwise Z contains the double of $\mathbb{H}$ which is the octonions. It seems as though one can repeat this process indefinitely. However we hit a roadblock at the very next step. If Z is not the octonions, then by Lemma 36, we have that the double of $\mathbb{O}$ is no longer a composition algebra. Hence we have shown that if Z is a composition algebra, it must be one of $\mathbb{R}, \mathbb{C}, \mathbb{H}, \mathbb{O}$. ■

5.3 Other properties of composition algebras

Definition 28. We define the **inverse** of x to be

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

Theorem 40. Inverse Laws:

$$\overline{x}.xy = y = yx.\overline{x}$$

Equivalently,

$$x^{-1}.xy = y = yx.x^{-1}$$

Proof. Theorem 25 and the braid law are used.

$$[\overline{x}.xy, t] = [xy, xt] = [x][y, t] = [[x]y, t].$$

$$[yx.\overline{x}, t] = [yx, tx] = [y, t][x] = [y[x], t].$$

■

Theorem 41. Alternative laws:

$$x.xy = x^2y$$

and

$$yx.x = yx^2$$

Proof. We use the definition of $\overline{x}$ in the inverse law (Theorem 40) to get

$$(2[x, 1] - x).xy = 2[x, 1]xy - x.xy = (2[x, 1] - 1)x.y = 2[x, 1]xy - x^2y.$$

Cancelling undesired terms gives us the result. ■

Theorem 42. Moufang laws:

$$xy.zx = x(yz)x = x.(yz)x$$

Proof. We have

$$\begin{aligned}
[xy.zx, t] = [xy, t.\bar{x}\bar{z}] &= 2[x, y][y, \bar{x}\bar{z}] - [x.\bar{x}\bar{z}, ty] \\
&= 2[x, t][yz, \bar{x}] - [\bar{x}\bar{z}, \bar{x}.ty] \\
&= 2[yz, \bar{x}][x, t] - [x][\bar{z}\bar{y}, t] \\
&= 2[x, \overline{yz}][x, t] - [x][\overline{yz}, t] \\
&= [2[x, \overline{yz}]x - [x]\overline{yz}, t].
\end{aligned}$$

Therefore, $xy.zx = 2[x, \overline{yz}]x - [x]\overline{yz}$ is a function of x and yz only. We can thus replace y and z with any two elements such that their product is still yz. If we replace y with yz and z with 1, we obtain

$$x(yz).x = xy.zx.$$

On replacing y with 1and z with yz we get

$$xy.zx = x.(yz)x$$

■

Theorem 43. Third alternative law

$$xy.x = x.yx$$

Proof. Replace z with 1 in the Moufang Law to get

$$xy.x = xy.1x = x.(1y)x = x.(y1)x = x.yx$$

■

5.4 The maps L_x, B_x and R_x

The left multiplication, right multiplication, bi-multiplication operators are defined as:

$$L_x : y \mapsto xy \qquad R_x : y \mapsto yx \qquad B_x : y \mapsto xyx$$

The third alternative law ensures that the bi-multiplication map is well defined. We introduce the notation

$$y^{L_x R_x} := R_x(L_x(y))$$

B_x is the product of R_x and L_x without regard to order since

$$y^{L_x R_x} = xy.x = x.yx = y^{R_x L_x}$$

The bi-multiplication map also has a geometric interpretation. Recall the expression for a reflection in the hyperplane perpendicular to a vector x:

$$\mathrm{ref}_x(t) = t - 2\frac{[x,t]}{[x]}x$$

Compare this to the expression obtained in the proof of the Moufang laws

$$xy.zx = 2[x,\overline{yz}]x - [x]\overline{yz}$$

Notice that $\mathrm{ref}_x\ (\overline{yz}) = \overline{yz} - 2\frac{[\overline{yz},x]}{[x]}x$. Also, $\mathrm{ref}_1(t) = t - 2\frac{[1,t]}{[1]}1 = -\bar{t}$. Therefore, we have that

$$B_x(yz) = xy.zx = [x](yz)^{\mathrm{ref}_1 \circ \mathrm{ref}_x}$$

Hence if we take z to be 1,we see that B_x is a scalar multiple of the composition of two reflections.

5.5 Coordinates for Quaternions and Octonions

In this section we recover the usual definition of algebras from the definition using Dickson doubles. We first deal with the quaternions. Let i be the unit vector that extends $\mathbb{R}$ to $\mathbb{C}$ and let j be the unit vector that extends $\mathbb{C}$ to $\mathbb{H}$. Note that these unit vectors i and j are orthogonal to 1 and also each other. We have that $\mathrm{ref}_1(j) = j$ and $\mathrm{ref}_i(j) = j$. Hence

$$iji = B_i(j) = [i]j^{\mathrm{ref}_1 \circ \mathrm{ref}_i} = j$$

We define $k = ij$. We thus have $ki = iji = j$ and $jk = jij = i$.Also, $k^2 = (iji)j = j^2 = i(jij) = i^2$. We now show $i^2 = -1$. Using the braid law, one can write

$$[i^2, t] = [i.i, t] = [i, -it] = -[i][1, t] = [-1, t].$$

We also have that

$$ji = \overline{ji} = \overline{ij} = \overline{k} = -k.$$

We have thus obtained the relations

$$\begin{aligned} i^2 = j^2 = k^2 = -1 \\ ij = k \qquad jk = i \qquad ki = j \\ ji = -k \qquad ik = -j \qquad kj = -i \end{aligned}$$

For the octonions, we shall find 7 units $i_0,\ i_1 \cdots i_6$ such that

$$\alpha : i_n \mapsto i_{n+1} \text{ and } \beta : i_n \mapsto i_{2n}$$

are symmetries of the multiplication.

. The units of the quaternion subalgebra are defined to be

$$i_1 = i \qquad i_2 = j \qquad i_4 = k.$$

We let i_0 be the unit vector which extends $\mathbb{H}$ to $\mathbb{O}$. Define $i_0 i_n = i_{3n}$. Thus we have

$$i_0 i_1 = i_3 \qquad i_0 i_2 = i_6 \qquad i_0 i_4 = i_5.$$

Recall that in the proof of Hurwitz's theorem we used the fact that $i_0.cb = i_0 b.c$. We use this to obtain

$$\begin{aligned} i_6 i_1 = i_0 i_2 . i_1 = i_0 . i_1 i_2 = i_0 i_4 = i_5 \\ i_5 i_2 = i_0 i_4 . i_2 = i_0 . i_2 i_4 = i_0 i_1 = i_3 \\ i_3 i_4 = i_0 i_1 . i_4 = i_0 . i_4 i_1 = i_0 i_2 = i_6. \end{aligned}$$

This shows that each of the 7 triplets i_x, i_y, i_z with subscripts

$$xyz = 124, 235, 346, 450, 561, 602, 013$$

behave like the quaternions. The general such system is

$$i_{n+1} . i_{n+2}, i_{n+4}$$

with n varying from 1 to 6. This also verifies the assertion that α and β are symmetries of the multiplication.

5.6 Diassociativity

Theorem 44. The algebra generated by any two octonions is associative.

Moufang Loops

6.1 Inverse loops

Definition 29. An inverse loop L is a set with a binary operation, a unary operation the inverse $\dashv$ and an identity 1 satisfying

$$x1 = 1x = x \tag{6.1}$$

$$(x^{\dashv})^{\dashv} = x \tag{6.2}$$

$$x^{\dashv} . xy = y = yx . x^{\dashv} \tag{6.3}$$

Theorem 45. The inverse of an element x is unique.

Proof. Suppose x has two inverses y and z. Then using (6.3) we get

$$y = y.1 = y.xz = yx.z = 1.z = z.$$

■

Theorem 46. In an inverse loop

$$(xy)^{\dashv} = y^{\dashv}x^{\dashv}.$$

Proof.

$$x^{\dashv} = x^{\dashv}.1 = x^{\dashv}.y^{\dashv}y = (x^{\dashv}y^{\dashv})y$$
$$(x^{\dashv}y^{\dashv})^{\dashv}x^{\dashv} = (x^{\dashv}y^{\dashv})^{\dashv}.(x^{\dashv}y^{\dashv})y = y$$
$$(x^{\dashv}y^{\dashv})^{\dashv} = yx$$

Taking inverse in the last eqaution above, we get $x^{\dashv}y^{\dashv} = (yx)^{\dashv}$.

■

The relation $xy = z$ can be written in 6 different ways. This is called a **hexad** of relations.

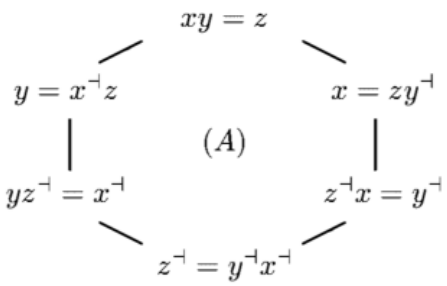

Figure 6.1: The duplex form of the hexad.

Lemma 47. $yz^{\dashv} = x^{\dashv} \Leftrightarrow z^{\dashv}x = y^{\dashv}$

Proof. For the forward direction, note $z^{\dashv}x = (1.z^{\dashv})x = (y^{\dashv}.yz^{\dashv})x = (y^{\dashv}.x^{\dashv})x = y^{\dashv}$ Conversely, $yz^{\dashv} = y(z^{\dashv}.1) = y(z^{\dashv}x.x^{\dashv}) = y(y^{\dashv}.x^{\dashv}) = x^{\dashv}$ ■

The above equivalence can be rewritten as $(yz^{\dashv})x = 1 \Leftrightarrow y(z^{\dashv}x) = 1$. We can then replace z with $z^{\dashv}$ and obtain $(xy)z = 1 \Leftrightarrow x(yz) = 1$. This makes the parentheses in $xyz = 1$ unneccessary. $xy = z$ is called the **duplex** form of the hexad while $xyz^{\dashv} = 1$ is called the **triplex** form of the hexad.

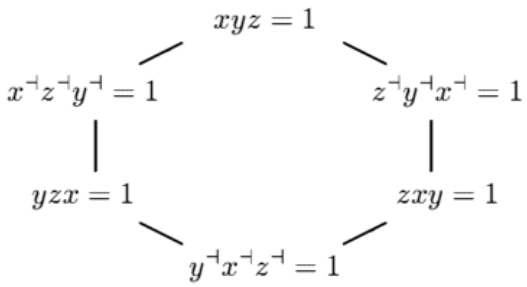

Figure 6.2: The triplex form of the hexad.

6.2 Isotopy

Definition 30. An **isotopy** of a loop L is a triple of invertible maps that preserve the basic relation $xy = z$. We introduce two notations for an isotopy according to whether the relation is in duplex or triplex form. By $(\alpha, \beta|\gamma)$ we mean that $x^{\alpha}y^{\beta} = (xy)^{\gamma}$. By (α, β, γ) we mean $x^{\alpha}y^{\beta}z^{\gamma} = 1$.

Theorem 48. If $(\alpha, \beta|\gamma)$ is an isotopy in duplex form, then $(\alpha, \beta, \dashv \gamma \dashv)$ is it's representation in triplex form.

Proof. Suppose $xyz = 1$. Then $xy = z^{\dashv}$. Applying the isotopy $(\alpha, \beta|\gamma)$ to this relation, we obtain $x^{\alpha}y^{\beta} = z^{\dashv\gamma}$. Hence we have that $x^{\alpha}y^{\beta}z^{\dashv\gamma\dashv} = 1$. That is, $(\alpha, \beta, \dashv \gamma \dashv)$ is the same isotopy in triplex form. ■

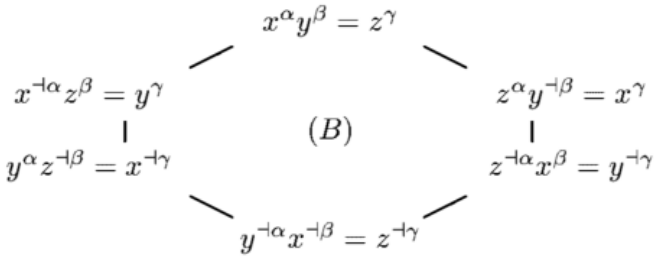

Figure 6.3: On applying $(\alpha, \beta|\gamma)$ to the basic hexad.

If we now rearrange the relations in the above hexad to obtain the $xy = z$ with variants of the original isotopy applied to it, we obtain

The above two figures represented as a hexad of isotopies in duplex form along with the same hexad in triplex form after replacing γ with $\dashv \gamma \dashv$ is shown in Figure 6 and 7.

6.3 Monotopies and companions

Definition 31. A **monotopy** is any of the three maps of an isotopy.

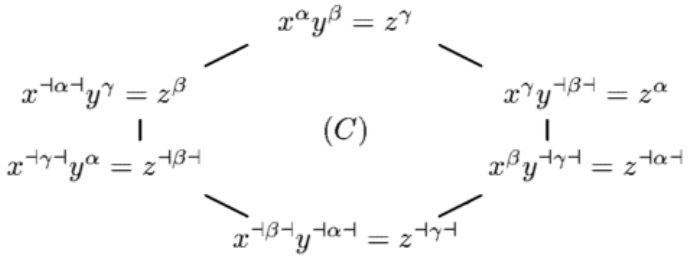

Figure 6.4: Variants of the isotopy $(\alpha, \beta|\gamma)$

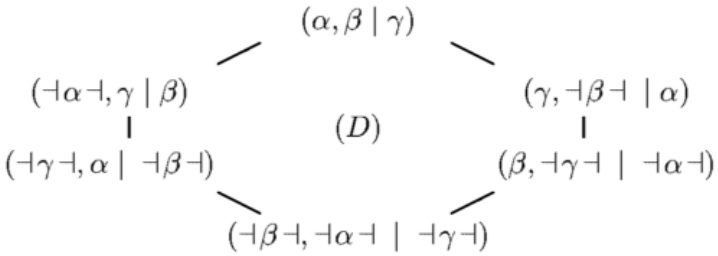

Figure 6.5: Hexad of isotopies in duplex form.

By definition, if γ is a monotopy then there exist maps α and β such that

$$xy = z \implies x^\alpha y^\beta = (xy)^\gamma.$$

In particular if we take x to be 1 and y to be z and then switch x and y we obtain

$$z^\alpha 1^\beta = z^\gamma, \text{ so } z^\alpha = z^\gamma 1^{\beta\dashv} = z^\gamma b$$

$$1^\alpha z^\beta = z^\gamma, \text{ so } z^\beta = 1^{\alpha\dashv} z^\gamma = a z^\gamma.$$

Theorem 49. γ is a monotopy if and only if there are loop elements b and a for which $(xy)^\gamma = x^\gamma b.ay^\gamma$.

Proof. The forward direction is a straightforward consequence of the calculation preceding this theorem. For the converse, consider the left and right multiplication operators

$$L_a : x \mapsto ax \qquad R_b : x \mapsto bx.$$

Since $(xy)^\gamma = x^\gamma b.ay^\gamma$ holds, we have that $(\gamma R_b,\ \gamma L_b|\ \gamma)$ is an isotopy and hence γ is a monotopy. Here the order of composition in function composition (for instance in γR_b) is to be taken to be opposite of the usual order. ■

If such loop elements a and b exist they are said to be a pair of **companions** to γ. An **automorphism** is just a monotopy that has $1, 1$ as a pair of companions.

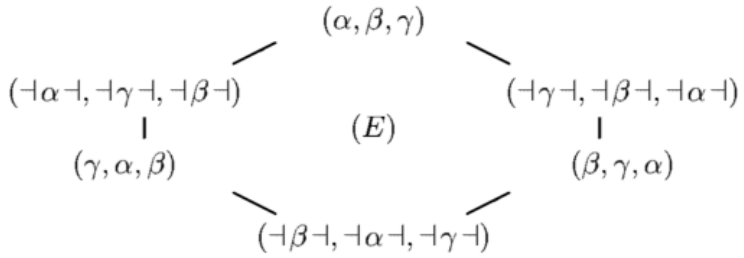

Figure 6.6: Hexad of isotopies in triplex form.

Theorem 50. The set of isotopies on an inverse loop L is a group under the operation defined as

$$(\alpha, \beta, \gamma) \cdot (\alpha', \beta', \gamma') = (\alpha\alpha', \beta\beta', \gamma\gamma')$$

Proof. Closure is clear since each map in the isotopy is a bijection and the second isotopy applied to $x^\alpha y^\beta = z^\gamma$ shows that $(\alpha\alpha', \beta\beta', \gamma\gamma')$ is an isotopy. Associativity follows from associativity of composition of functions. The identity is the isotopy $(\mathbb{1}, \mathbb{1}, \mathbb{1})$. The inverse is

$$(\alpha, \beta, \gamma)^{-1} = (\alpha^{-1}, \beta^{-1}, \gamma^{-1})$$

■

Lemma 51. $\dashv L_a \dashv = R_{a^\dashv}, \qquad \dashv R_a \dashv = L_{a^\dashv}, \quad \dashv B_a \dashv = B_{a^\dashv}.$

Proof. Observe that using Theorem 46 we have,

$$\begin{aligned}(\dashv L_a \dashv)(x) = (ax^\dashv)^\dashv = xa^\dashv = (R_{a^\dashv})(x)\\ (\dashv R_a \dashv)(x) = (x^\dashv a)^\dashv = a^\dashv x = L_{a^\dashv}\\ (\dashv B_a \dashv)(x) = (ax^\dashv a)^\dashv = a^\dashv x a^\dashv = B_{a^\dashv}\end{aligned}$$

■

Theorem 52. If a is the image of 1 under some monotopy, then $L_a, R_a, B_a, L_{a^\dashv}, B_{a^\dashv}, R_{a^\dashv}$ are monotopies. In particular, if there is any monotopy which takes 1 to a, then L_a and R_a are such monotopies.

Proof. Consider the product of two isotopies

$$(\dashv \alpha \dashv, \gamma|\beta) \cdot (\alpha, \beta|\gamma)^{-1} = (\dashv \alpha \dashv \alpha^{-1}, \gamma\beta^{-1}|\beta\gamma^{-1})$$

Since we have $\beta\gamma^{-1} = L_a$ (this is where we use the fact that 1 maps to a under some monotopy) and so $\gamma\beta^{-1} = L_{a^{-1}}$, the product can be rewritten as

$$(\dashv \alpha \dashv \alpha^{-1}, L_{a^\dashv}|L_a)$$

Applying this isotopy to $x.a = xa$ gives

$$a(xa) = x^{\alpha^{-1}\dashv\alpha\dashv}.a^\dashv a = x^{\alpha^{-1}\dashv\alpha\dashv}$$

We can thus identify the map $\alpha^{-1} \dashv \alpha \dashv$ with the map which takes x to $a(xa)$. Thus we have an isotopy which when applied to $xy = z$ gives $a(xa).a^{\dashv}y = a(xy)$ If we take y to be 1 we obtain

$$a(xa).a^{\dashv} = ax, \text{ so } a(xa) = (ax)a$$

. This shows that the bimultiplication map B_a is well defined and that our isotopy is $(B_a, L_{a^{\dashv}}|L_a)$. We obtain the hexad in Figure 6.7 for the isotopy $(L_a, R_a\,|B_a)$ if we use the following Lemma 51.

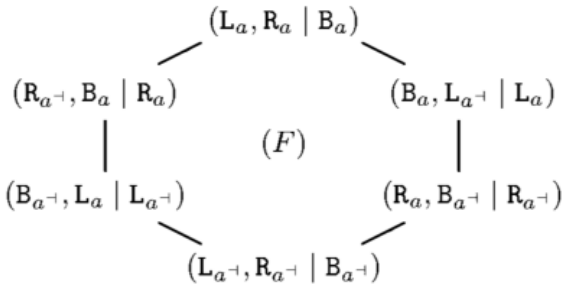

Figure 6.7: Hexad for isotopy $(L_a, R_a\,|B_a)$

■

Theorem 53. The monotopies are transitive if and only if the Moufang identity

$$zx.yz = z(xy)z$$

holds.

Proof. If the monotopies are transitive, there is only 1 orbit of the action of the set of monotopies on the loop. Hence for each element z in the loop, there is a monotopy α such that $\alpha(1) = z$. By Theorem 52, L_z is a monotopy and the Moufang identity follows from applying the monotopy $(L_a, R_a\,|B_a)$ to $xy = z$. Conversely, to show that the monotopies are transitive, we show there is only 1 orbit of the action of monotopies on the loop. That is, every element x of the loop is the image of a fixed y under some monotopy. The monotopy we seek is $L_{xy^{\dashv}}$. ■

Definition 32. A loop for which the Moufang identity holds is called a **Moufang** loop.

Example 12. Every group is an example of a Moufang loop.

Example 13. The nonzero octonions are an example of a nonassociative Moufang loop under octonion multiplication.

6.4 Different forms of the Moufang Laws

Theorem 54. We have the three Moufang Laws

$$z(xy)z = zx.yz \textbf{ Bi-Moufang Law}$$

$$z(xy) = zxz.z^{\dashv}y \textbf{ Left Moufang Law}$$

$$(xy)z = xz^{\dashv}.zyz \textbf{ Right Moufang Law}$$

Proof. Using the hexad in (F), we apply the isotopy $(L_z, R_z \,|B_z)$ to the relation $xy = z$ to obtain the Bi-Moufang Law $zx.yz = z(xy)z$. Applying the isotopy $(B_z, L_{z^{\dashv}} \,|L_z)$ to $xy = z$ we get $zxz.z^{\dashv}y = z(xy)$. Applying the isotopy $(R_{z^{\dashv}}, B_z \,|R_z)$ gives us the Right Moufang Law. ■
