SJÄLVSTÄNDIGA ARBETEN I MATEMATIK

MATEMATISKA INSTITUTIONEN, STOCKHOLMS UNIVERSITET

Geometric interpretation of non-associative composition algebras

av

Fredrik Cumlin

2020 - No K13

MATEMATISKA INSTITUTIONEN, STOCKHOLMS UNIVERSITET, 106 91 STOCKHOLM

Geometric interpretation of non-associative composition algebras

Fredrik Cumlin

Självständigt arbete i matematik 15 högskolepoäng, grundnivå

Handledare: Wushi Goldring

2020

Abstract

This paper aims to discuss the connection between non-associative composition algebra and geometry. It will first recall the notion of an algebra, and investigate the properties of an algebra together with a composition norm. The composition norm will induce a law on the algebra, which is stated as the composition law. This law is then used to derive the multiplication and conjugation laws, where the last is also known as convolution. These laws are then used to prove Hurwitz's celebrated theorem concerning the different finite composition algebras.

More properties of composition algebras will be covered, in order to look at the structure of the quaternions $\mathbb{H}$ and octonions $\mathbb{O}$. The famous Fano plane will be the finishing touch of the relationship between the standard orthogonal vectors which construct the octonions.

Lastly, the notion of invertible maps in relation to invertible loops will be covered, to later show the connection between $8-$dimensional rotations and multiplication of unit octonions.

Contents

1 Algebra **4**
1.1 The multiplication laws 6
1.2 The conjugation laws 7
1.3 Dickson double 8
1.4 Hurwitz's theorem 11

2 Properties of composition algebras **14**
2.1 The left-, right- and bi-multiplication maps 16
2.2 Basic properties of quaternions and octonions 16

3 Geometric interpretation of the Octonions $\mathbb{O}$ **18**
3.1 Isotopy and inverse loops 19
3.2 Isotopies and SO_8 22
3.3 Triality 24

1 Algebra

We start with the definition of an algebra and a composition algebra.

Definition 1.1. An algebra, A, is a vector space over a field K, equipped with a bilinear map $m : A \times A \to A$ called *multiplication*, and a non-zero element, $1 \in A$, that satisfy $m(a, 1) = m(1, a) = a$. The multiplication also satisfies the left and right distributive law for all elements in A.

Remark 1.1. From now on we assume that the field K of an algebra A, does not have characteristic 2. This implies $2 \neq 0$ in K, which is important in coming definitions.

Remark 1.2. Some texts usually mean associative algebra when defining an algebra. This text will use the more exotic definition of an algebra, that does not require multiplication to be associative.

Remark 1.3. We will abbreviate $m(a, b) = ab$, where a, b are elements in A.

Example 1.1. The following are examples of algebras over the field of real numbers $\mathbb{R}$.

1. The real numbers $\mathbb{R}$ with multiplication as binary operation.
2. Matrices with entries in $\mathbb{R}$, of dimensions $n \times n$ with matrix multiplication as binary operation.
3. The complex numbers $\mathbb{C}$ with multiplication as binary operation.

Definition 1.2. Let Z be an algebra over a field K. A subalgebra, A, of Z is a K-vectorsubspace $A \subseteq Z$, which is closed under multiplication and $1 \in A$.

We continue with the components needed in order to define a composition algebra. We start with the composition norm.

Definition 1.3. Let A be and algebra over a field K. A **composition norm**, N, is a map $N : A \to K$, that satisfies the following conditions for all $a, b \in A$ and $k \in K$

1. $N(ka) = k^2 N(a)$,
2. $N(a + b) - N(a) - N(b)$ is a bilinear map $A \times A \to K$,
3. $N|_{A^\times} : A^\times \to K^\times$ is a group homomorphism.

Remark 1.4. The third condition of the composition norm implies that $N(ab) = N(a)N(b)$.

Definition 1.4. Let A be an algebra over a field K. We define the **bracket of a and b**, where $a, b \in A$, to be given by

$$[a, b] := \frac{1}{2}(N(a + b) - N(a) - N(b)).$$

Remark 1.5. Note that $[a, a] = N(a)$, since $[a, a] = \frac{1}{2}(N(a+a) - N(a) - N(a)) = \frac{1}{2}(4N(a) - 2N(a)) = N(a)$ by the quadratic property of the norm. Thus, $[a, a]$ will be abbreviated as $[a]$. Both $[a]$ and $N(a)$ will be used, and the reader should be comfortable that they are equivalent.

Remark 1.6 (Properties of the bracket operation). Let A be an algebra over the field K. Then the following are properties of the bracket operation.

1. The bracket is symmetric, i.e. $[a, b] = [b, a]$ for all $a, b \in A$.
2. We have that $[a, a] = 1/2(N(a + a) - N(a) - N(a)) = N(a)$ because of the quadratic property.
3. For all $a \neq 0$ in A, $[a, a] \neq 0$ since $N|_{A^\times}$ is a homomorphism.
4. $N(0) = 0$ since $N(0) = 0N(1) = 0$ where 1 is the unit in A.
5. Combining 3 and 4 shows that $[a, a] = 0$ if and only if $a = 0$.
6. For $1 \in A$, we have $N(1) = N(1)N(1)$, which implies $N(1) = 1$ since $N(1) \neq 0$.

Definition 1.5. Let A be an algebra over a field K. The conjugation of an element $a \in A$, denoted $\overline{a}$, is given by

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

where 1 is the unit in A.

We are now ready for the definition of a composition algebra.

Definition 1.6. An algebra A over a field K is said to be a composition algebra, if there exists some composition norm on A.

Remark 1.7. A composition algebra is also a division algebra.

The geometric interpretation of the norm, when considering an algebra over the field of real numbers $\mathbb{R}$, is that each element in an algebra, A, has a length associated with it. The length is determined by the norm N. In a composition algebra, for any elements a and $b \in A$, the length of the product of ab should be the same as evaluating the length of each element a, b individually and multiplying them together.

From a different perspective, the distributive law in the definition of an algebra, says that the binary operator is repeated addition (this argument is basically taking place in $\mathbb{Q}$). To see this, we have $ab = a(1 + r_1) = a1 + ar_1 = a1 + a(1 + r_2) = a1 + a1 + ar_2$ and so on, where $r_1 = b - 1$ and $r_2 = r_1 - 1$. Thus, measuring the length of ab can be pronounced in the following way: Measure a the number of times a unit fits in b, then add them all up. But if we assume that the lenght of a unit is 1, this is the same as measuring a, then adding them up the number of times a unit fits in b. But its the same thing. Thus, intuitively, we are interested in the equation $N(ab) = N(a)N(b)$.

We are interested in the number of composition algebras. To investigate this, we need to understand the fundamental properties of compositions algebras.

1.1 The multiplication laws

For a more concise writing, let $[a] = [a, a] = N(a)$ for $a \in A$. We begin by looking at the consequences of the homomorphism property of the composition norm. We will call a consequence of this the composition law.

$$\textbf{The composition law: } [ab] = [a][b] \tag{1.1.1}$$

Theorem 1.1. *Let A be a composition algebra over a field K and $a, b \in A$. If $[a, t] = [b, t]$ for all $t \in A$, then $a = b$.*

Proof. If $[a, t] = [b, t]$ then $[a - b, t] = 0$ due to the bilinear property of the bracket. Since it is true for all $t \in A$, we can take $t = a-b$. Thus, $[a-b, a-b] = 0$, hence $N(a-b) = 0$. From the properties of the bracket operation, $N(a-b) = 0$ is true if and only if $a - b = 0$ and the theorem follows. □

$$\textbf{Bracket identity: } [a + b] = [a] + [b] + 2[a, b] \tag{1.1.2}$$

Proof. By the definition of the bracket, $2[a, b] = [a + b] - [a] - [b]$. Hence, $[a + b] = [a] + [b] + 2[a, b]$. □

$$\textbf{The scaling laws: } [ab, ac] = [a][b, c] \ (\textit{and } [ac, bc] = [a, b][c]) \tag{1.1.3}$$

Proof. Using the definition of the bracket operator and the composition law (1.2.6) , we have

$$\begin{aligned}
[ab, ac] &= \frac{1}{2}([ab + ac] - [ab] - [ac]) \\
&= \frac{1}{2}[a]([b + c] - [b] - [c]) \\
&= [a][b, c].
\end{aligned}$$

The second scaling law follows by similar argument on $[ac, bc]$. □

$$\textbf{Composition law bracket: } [ab, dc] + [db, ac] = 2[a, d][b, c] \tag{1.1.4}$$

Proof. Using the bilinear property of the bracket on the left-hand side, and later the scaling law (1.1.3), we have

$$\begin{aligned}[ab, dc] + [db, ac] &= [ab + db, dc] - [db, dc] + [ab + db, ac] - [ab, ac] \\ &= [ab + db, ac + dc] - [d][b, c] - [a][b, c] \\ &= [(a + d)b, (a + d)c] - [d][b, c] - [a][b, c] \\ &= [a + d][b, c] - [d][b, c] - [a][b, c] \\ &= ([a + d] - [a] - [d])[b, c] \\ &= 2[a, d][b, c],\end{aligned}$$

where we used the definition of the bracket in the last equality. The composition law bracket follows. □

$$\textbf{The exchange law:}\ [ab, dc] = 2[a, d][b, c] - [ac, bd] \tag{1.1.5}$$

Proof. Expanding $[(a + d)b, (a + d)c]$ with the bilinear property of the bracket, then using the scaling law (1.1.3) and composition law bracket (1.1.4), gives

$$\begin{aligned}[(a + d)b, (a + d)c] &= [ab, ac] + [ab, dc] + [db, ac] + [db, dc] \\ &= [a][b, c] + [d][b, c] + 2[a, d][b, c] \\ &= ([a] + 2[a, d] + [d])[b, c].\end{aligned}$$

The right distributive law and the scaling law, after cancellation, gives the desired equality. □

1.2 The conjugation laws

We will now investigate the laws including conjugation.

$$\textbf{The braid laws:}\ [ab, c] = [b, \overline{a}c]\ (\textit{and}\ [ab, c] = [a, c\overline{b}]) \tag{1.2.6}$$

Proof. Letting $d = 1$ in (1.1.5)

$$\begin{aligned}[ab, c] &= 2[a, 1][b, c] - [ac, b] \\ &= [b, 2[a, 1]c] - [ac, b] \\ &= [b, (2[a, 1] - a)c] \\ &= [b, \overline{a}c]\end{aligned}$$

and the first braid law follows. The second braid law is shown similarly, by letting $c = 1$ in (1.1.5). ☐

$$\textbf{Biconjugation: } \overline{\overline{a}} = a. \tag{1.2.7}$$

Proof. Letting $b = 1$ and $c = t$ in (1.2.6), this gives

$$\begin{aligned} [a, t] &= [a1, t] \\ &= [1, \overline{a}t] \\ &= [\overline{\overline{a}}1, t] \\ &= [\overline{\overline{a}}, t]. \end{aligned}$$

From Theorem 1.1, this is true for all $t \in A$. Hence, the equality is proven. ☐

$$\textbf{Product conjugation: } \overline{ab} = \overline{b}\overline{a}. \tag{1.2.8}$$

Proof. Let t be an arbitrary element in A. Repeated use of (1.2.6) and (1.2.7) gives

$$\begin{aligned} [\overline{b}\overline{a}, t] &= [\overline{a}, bt] \\ &= [\overline{a}\overline{t}, b] \\ &= [\overline{t}, ab] \\ &= [\overline{t}\overline{ab}, 1] \\ &= [\overline{ab}, t]. \end{aligned}$$

The result follows from Theorem 1.1, since t was arbitrarily chosen. ☐

1.3 Dickson double

We are interested in the composition algebras of finite dimension. The idea to approach this problem, is to construct these from a smallest algebra, and show that a finite dimensional composition algebra has to be constructed from its smallest subalgebra. We begin with defining what we mean with constructing an algebra from another, the so called Dickson double.

Definition 1.7. Let A be a composition algebra over a field K. Then the **external product algebra**, $A \times A$, is defined to consist of elements (a, b) where $a, b \in A$, i.e. ordered pairs of elements in A. The unit is given by $(1, 0)$ where 1 is the unit in A, and multiplication is given by $(a, b)(c, d) = (ac - d\overline{b}, cb + \overline{a}d)$.

Definition 1.8 (**External Dickson double**)**.** Let A be an algebra over a field K. We define the external Dickson double of A, denoted $D_e(A)$, to be given by the external product algebra,

$$D_e(A) := A \times A.$$

Definition 1.9. Let A be a composition algebra over a field K and let $\iota \in A$. We say that ι is a unit vector in A, if $[\iota] = 1$ where 1 is the unit in K.

Definition 1.10 (**Internal Dickson double**)**.** Let Z be a compositional algebra over a field K, and let A be a proper subalgebra of Z. Let ι be a unit vector in Z, that satisfies $[\iota, a] = 0$ for all $a \in A$. We define the internal Dickson double of A as

$$D_i(A) := (D_i(A), \iota) := A + \iota A.$$

Remark 1.8. Recall from the properties of the bracket operation, that the choice of ι implies that $\iota \in Z \backslash A$. The definition also assumes that such ι exists. We will later prove that if A is a proper subalgebra of Z, this has to be the case.

Remark 1.9. The elements in $A + \iota A$ will be represented as $a + \iota b$ where $a, b \in A$. The construction of ι will be clarified in Corollary 1.6.1.

It is clear that $D_i(A)$ in Definition 1.10 is a sub-vectorspace of Z, and it will be shown now that it is a subring of Z, hence a subalgebra.

Lemma 1.2. *Let A be a subalgebra of a composition algebra Z over a field K, and let $D_i(A)$ be an internal Dickson double. Then for all $a, b, c, d \in A$, we have $[a + \iota b, c + \iota d] = [a, c] + [b, d]$.*

Proof. We have $[a + \iota b, c + \iota d] = [a, c] + [a, \iota d] + [\iota b, c] + [\iota b, \iota d]$. From the braids law (1.2.6), $[a, \iota d] = [a\overline{d}, \iota] = 0$ and $[\iota b, c] = [\iota, c\overline{b}] = 0$. From the scaling law (1.1.3), we have $[\iota b, \iota d] = [\iota][b, d] = [b, d]$. Thus, the Lemma follows. □

Lemma 1.3. *Let A be a subalgebra of a composition algebra Z over a field K, and let $D_i(A)$ be an internal Dickson double. Then for all $a, b \in A$, $\overline{a + \iota b} = \overline{a} - \iota b$. Also, $\iota b = -\overline{\iota b} = -\overline{b}\overline{\iota} = \overline{b}\iota$.*

Proof. From the definition of conjugation and braid laws 1.2.6,

$$\begin{aligned}\overline{\iota b} &= 2[\iota b, 1] - \iota b \\ &= 2[\iota, 1\overline{b}] - \iota b \\ &= -\iota b\end{aligned}$$

Thus, $\overline{a + \iota b} = \overline{a} - \iota b$ since the bracket is bilinear. To see that $\iota b = \overline{b}\iota$, note that $\overline{a + \iota b} = \overline{a} - \iota b$, and $\overline{a + \overline{b}\iota} = \overline{a} - \iota b$, which follows from product conjugation. If the conjugates of two elements are equal, the elements have to be equal, which follows from biconjugation (1.2.7).

□

Lemma 1.4. *Let A be a subalgebra of a composition algebra Z over a field K, and let $D_i(A)$ be an internal Dickson double. Then for all $a, b, c, d \in A$, $(a + \iota b)(c + \iota d) = (ac - d\overline{b}) + \iota(cb + \overline{a}d)$. In other words, $D_i(A)$ is closed under multiplication.*

Proof. From the distributive law, we have $(a+\iota b)(c+\iota d) = ac+a.\iota d+\iota b.c+\iota b.\iota d$. Now, starting with the exchange law (1.1.5), and using the braids law (1.2.6) repeatedly, for any element t in the algebra $D_i(A)$ we have

$$\begin{aligned}
[a.\iota d, t] &= [\iota d, \overline{a}t] \\
&= 2[\iota, \overline{a}][t, d] - [\iota t, \overline{a}d] \\
&= 0 - [\iota t, \overline{a}d] \\
&= [t, \iota.\overline{a}d] \\
&= [\iota.\overline{a}d, t],
\end{aligned}$$

in which the equality $a.\iota d = \iota.\overline{a}d$ follows from Theorem 1.1 . Remember from Lemma 1.3, $\iota b = \overline{b}\iota$. Using this, and the exchange law, we also have

$$\begin{aligned}
[\iota b.c, t] &= [\iota b, t\overline{c}] \\
&= [\overline{b}\iota, t\overline{c}] \\
&= 0 - [\overline{b}\overline{c}, t\iota] \\
&= [\overline{b}\overline{c}.\iota, t] \\
&= [\iota.cb, t],
\end{aligned}$$

and thus $\iota b.c = \iota.cb$. Lastly, we have

$$\begin{aligned}
[\iota b.\iota d, t] &= -[\iota b, t.\iota d] \\
&= 0 + [\iota.\iota d, tb] \\
&= -[\iota.\iota d, tb] \\
&= -[\iota][d, tb] \\
&= [-d\overline{b}, t],
\end{aligned}$$

and it follows that $\iota b.\iota d = -d\overline{b}$. In total, $(a+\iota b)(c+\iota d) = ac+a.\iota d+\iota b.c+\iota b.\iota d = ac + \iota.\overline{a}d + \iota.cb - d\overline{b} = (ac - d\overline{b}) + \iota(cb + \overline{a}d)$ because addition is commutative in a vector space. Thus, $D_i(A)$ is closed under multiplication. $\square$

Remark 1.10. Note that this is also consistent with an abstract Dickson double, $D_e(A) = A \times A$, of an algebra A over K, defined to consist of ordered pairs of elements in A. In other words, multiplication in $D_e(A)$ is defined via $(a,b)(c,d) = (ac - d\bar{b}, cb + \bar{a}d)$ for a, b, c, d in A.

Theorem 1.5. *Given an algebra Z and a proper subalgebra A of Z over K, and assume that there exists a ι in Z with properties mentioned in Definition 1.10. Then the internal Dickson double $D_i(A) = A + \iota A$ is a subalgebra of Z.*

Proof. Since $D(A)$ is a vector space, and thus a subspace of Z, it is clear that it is closed under addition and scalar multiplication (not to be confused by multiplication in an algebra). Lemma 1.4 shows that $D_i(A)$ is closed under multiplication, and therefore $D_i(A)$ is a subalgebra of Z. □

Theorem 1.6. *Let Z be an algebra over a field K, and let A be a proper subalgebra of Z. Assume that there exists a ι in Z with the properties mentioned in Definition 1.10. Then the external Dickson double of A is isomorphic to the internal Dickson double of A.*

Proof. It is sufficient to prove that the internal sum of the definition of the internal Dickson double is a direct sum. Hence, we need to prove that the intersection of A and ιA is trivial and equal to $\{0\}$. Let a be an element in the intersection of A and ιA. Then for $a = \iota b$, we have $[a] = [a, a] = [a, \iota b] = 0$ by the braid law (1.2.6). Hence, $a = 0$ and thus the intersection is trivial. This shows that $D_e(A)$ is isomorphic to $D_i(A)$. □

Corollary 1.6.1. *Let Z be an algebra over a field K, let A be a proper subalgebra of Z and assume there exist two different unit vectors ι, ι' in Z such that $(D_i(A), \iota)$ and $(D_i(A), \iota')$ exist. Then $(D_i(A), \iota)$ is isomorphic to $(D_i(A), \iota')$.*

Proof. From Theorem 1.6, $D_e(A)$ is isomorphic to $(D_i(A), \iota)$ and $(D_i(A), \iota')$, hence $(D_i(A), \iota)$ is isomorphic to $(D_i(A), \iota')$. □

Remark 1.11. From now on, both the internal or external Dickson double will be called the **Dickson double**, and abbreviated $D(A)$. Elements in $D(A)$ will be represented by $a + \iota b$, where $a, b \in A$ and ι is a fixed orthogonal vector to A.

1.4 Hurwitz's theorem

We now come to the main idea of our construction of the composition algebras; there exist only four (of finite dimension) over the field of real numbers $\mathbb{R}$. Thus, in this subsection we restrict our scope by studying algebras over the field of real numbers.

Theorem 1.7 (Hurwitz)**.** *The only composition algebras with finite dimension over the field of real numbers $\mathbb{R}$, are the real numbers $\mathbb{R}$, the complex numbers $\mathbb{C}$, the quaternions $\mathbb{H}$, and the octonions $\mathbb{O}$, up to isomorphism.*

Remark 1.12. We will later give a construction of the quaternions and the octonions.

We will prove this theorem with a sequence of lemmas. First, a definition.

Definition 1.11. Let A be a composition algebra, n a natural number and Alg be the category of algebras. We define the map $D^n : \mathsf{Alg} \to \mathsf{Alg}$ by

$$D^n(A) = \begin{cases} A & \text{if } n = 0 \\ D(D^{n-1}(A)) & \text{otherwise.} \end{cases}$$

Lemma 1.8. *Let A be a composition algebra over the field of real numbers $\mathbb{R}$. Then there exist an $n \in \mathbb{N}$ such that $D^n(\mathbb{R}) \simeq A$. In other words, A can be constructed from repeated use of Dickson double on $\mathbb{R}$, up to isomorphism.*

Proof. If $A = \mathbb{R}$, then we are done by letting $n = 0$. Otherwise, assume there exist enough orthogonal unit elements in A such that for k, $D^k(\mathbb{R})$ exists. If $D^k(\mathbb{R}) = A$, we are done. Otherwise, according to Theorem 1.5, $D^k(\mathbb{R})$ is a subalgebra of A, and hence a proper subalgebra. Note that $D^k(\mathbb{R})$ is a vector space, thus there exist orthogonal vectors that spans $D^k(\mathbb{R})$. By Gram-Schmidt, we can expand this set and construct a set of orthogonal vectors that expands A, and thus we can continue with Dickson doubling. This shows that whenever $D^k(\mathbb{R})$ is of lower dimension that A, then we can continue to perform Dickson doubling. Thus, the iterative process will end when $D^n(\mathbb{R})$ is of same dimension as A, and thus consists of all orthogonal unit vectors that construct A. Hence, $D^n(\mathbb{R}) = A$. $\square$

Lemma 1.9. *Let Z be an algebra over the field of real numbers $\mathbb{R}$. Then the smallest nontrivial subalgebra A of Z, is the real numbers $\mathbb{R}$.*

Proof. Let A be the smallest subalgebra of Z. Then $1 \in A$ and for all $r \in \mathbb{R}$, $r1 \in A$. Hence, $\mathbb{R} \subseteq A$. Since $\mathbb{R}$ is an algebra, it has to be the smallest subalgebra. $\square$

To give the reader a better understanding of Lemma 1.8 and 1.9. If Z is an algebra over the field of real numbers $\mathbb{R}$, and A is a proper subalgebra of Z, then $D(A)$ is also a subalgebra of Z by Theorem 1.5. We can repeat this process until it does not exist a unit vector in Z in order to construct a Dickson double. When does this happen? It happens when $D(Y) = Z$ for some subalgebra Y. Since Z is finite dimensional, this means that Z can be constructed by an iterative process of Dickson doubles from the smallest subalgebra, which is according to Lemma 1.9 the real numbers $\mathbb{R}$. Thus, all the composition algebras of finite order over $\mathbb{R}$ can be constructed by repeated use of the Dickson double from $\mathbb{R}$.

Lemma 1.10. *Let Y be a composition algebra. Then $Z = D(Y)$ is a composition algebra if and only if Y is associative.*

Proof. Let $\iota = (0,1) \in Z$, then for all $a, b, c, d \in Y$, we have from Lemma 1.4 and the composition law, $[a + \iota b][c + \iota d] = [(ac - d\bar{b}) + \iota(cb + \bar{a}d)]$. The bilinear property can be used to expand the above equality, hence

$$[a][c] + [a][d] + [b][c] + [b][d] = [ac] - 2[ac, d\bar{b}] + [d\bar{b}] + [cb] + 2[cb, \bar{a}d] + [\bar{a}d]$$

. After cancellation of terms, we have $[ac, d\overline{b}] = [cb, \overline{a}d]$, using the braid law and biconjugation, we have $[ac.b, d] = [a.cb, d]$. Since d is arbitrary, Theorem 1.1 shows Y is associative. Thus, if Z is a composition algebra, then Y is associative.

If Y is associative, then the last equality holds and hence Z is a composition algebra. This shows the equivalence. $\square$

Lemma 1.11. *Let X be a composition algebra. Then $Y = D(X)$ is a associative composition algebra if and only if X is and associative, commutative composition algebra.*

Proof. Let $\iota \in Y$. By Lemma 1.10, X is associative. Let $a, b, c, d, e, f \in X$, we have

$$\begin{aligned}
(a + \iota b)(c + \iota d).(e + \iota f) &= ((ac - d\overline{b}) + \iota(cb + \overline{a}d))(e + \iota f) \\
&= (ac - d\overline{b})e - f(\overline{b}\overline{c} + \overline{d}a) \\
&\qquad + \iota(e(cb - f\overline{d}) + (\overline{c}\overline{a} - b\overline{d})f) \\
&= (ac.e - d\overline{b}.e - f.\overline{b}\overline{c} - f.\overline{d}a) \\
&\qquad + \iota(e.cb + e.\overline{a}d + \overline{c}\overline{a}.f - b\overline{d}.f)
\end{aligned}$$

and

$$\begin{aligned}
(a + \iota b).(c + \iota d)(e + \iota f) &= (a + \iota b)(ce - f\overline{d}) + \iota(ed + \overline{c}f) \\
&= a(ce - f\overline{d}) - (ed + \overline{c}f)\overline{b} \\
&\qquad + \iota((ce - f\overline{d})b + \overline{a}(ed + \overline{c}f)) \\
&= (a.ce - ed.\overline{b} - \overline{c}f.\overline{b} - a.f\overline{d}) \\
&\qquad + \iota(ce.b + \overline{a}.ed + \overline{a}.\overline{c}f - f\overline{d}.b).
\end{aligned}$$

If X is commutative, both expressions are equal, hence Y is associative. If Y is associative, then X has to be commutative. This shows the equivalence. $\square$

Lemma 1.12. *Let W be a composition algebra. Then $X = D(W)$ is an associative, commutative composition algebra if and only if W is an associative, commutative composition algebra with trivial conjugation ($\overline{a} = a$ for $a \in W$).*

Proof. By the Lemmas 1.10 and 1.11, that W is an associative commutative composition algebra is equivalent with X being an associative composition algebra. We need to show that trivial conjugation is equivalent with the commutative law for the Dickson double.

If X is commutative, we have from Lemma 1.3 $\iota e = \overline{e}\iota$ for all $e \in W$ and $\iota \in X$. Hence, $e = \overline{e}$.

If W has trivial conjugation, for all $a, b, c, d \in W$, we have

$$(a + \iota b)(c + \iota d) = (ac - d\bar{b}) + \iota(cb + \bar{a}d)$$

and

$$(c + \iota d)(a + \iota b) = (ca - b\bar{d}) + \iota(ad + \bar{c}b),$$

and thus, X is also commutative because W is commutative with trivial conjugation. □

Proof of Hurwitz's Theorem. The smallest composition algebra over the field of real numbers, is according to Lemma 1.9 the real numbers $\mathbb{R}$. The real numbers are commutative, associative and have trivial conjugation. According to Lemma 1.12, the complex numbers $\mathbb{C}$ is an associative, commutative composition algebra but they to not posess trivial conjugation. Thus, the quaternions $\mathbb{H}$ is a associative composition algebra from Lemma 1.11. That they are not commutative will be shown later in this paper. Lastly, the octonions $\mathbb{O}$ is a composition algebra from Lemma 1.10. That they are not associative will again be shows later in this paper. Since they are not associative, there exist no other composition algebra according to Lemma 1.10. □

2 Properties of composition algebras

We will now deduce some more properties of the composition algebras, before looking deeper into the octonions, $\mathbb{O}$.

Definition 2.1. Let A be a composition algebra over the real numbers $\mathbb{R}$, and let a be an element in A such that that $N(a) \neq 0$. We define the inverse of a to be

$$a^{-1} := \bar{a}/N(a).$$

Remark 2.1. If $N(a) \neq 0$ for $a \in A$, we say a is invertible in A. That this is indeed an inverse is given by the next Theorem.

Theorem 2.1. *Let A be a composition algebra over $\mathbb{R}$. For all invertible $a \in A$, then*

$$a^{-1}.ab = b = ba.a^{-1}$$

is satisfied for all $b \in A$.

Proof. Let t be an arbitrary element in A, and simplifying the following expression,

$$\begin{aligned}[\bar{a}.ab, t] &= [ab, at] \\ &= [a][b, t] \\ &= [[a]b, t],\end{aligned}$$

which follows from the braid laws and scaling laws. According to Theorem 1.1, $\overline{a}.ab = [a]b$. Thus, $a^{-1}.ab = b$. The other equality, $b = ba.a^{-1}$, is shown analogously. □

We will now investigate the alternate laws.

Definition 2.2. Let A be an algebra over $\mathbb{R}$. We say that A is alternative, if for all elements a, b in A, they satisfy the so called *alternate laws* [1],

1. $a.ab = a^2 b$
2. $ba.a = ba^2$.

Theorem 2.2. *Let a, b be elements in a composition algebra A. Then $a.ab = a^2 b$ and $ba.a = ba^2$.*

Proof. We begin by looking at $\overline{a}.ab = \overline{a}a.b$ which follows from Theorem 2.1. Using the defintion of conjugation, we have $\overline{a} = 2[a, 1] - a$, hence,

$$\begin{aligned}(2[a, 1] - a).ab &= (2[a, 1] - a)a.b \\ &= (2[a, 1]a - a^2)b.\end{aligned}$$

This simplifies to $a.ab = a^2 b$. Similarly we have $ba.a = ba^2$. □

Corollary 2.2.1. *A composition algebra is an alternative algebra.*

We will prove the so called third alternate law $ab.a = a.ba$ with a help from the Moufang law.

Theorem 2.3 (Moufang law)**.** *Let A be a composition algebra. Then for all $a, b, c \in A$, we have $ab.ca = a(bc).a = a.(bc)a$.*

Proof. For any $t \in A$, we have

$$\begin{aligned}[ab.ca, t] &= [ab, t.\overline{ac}] \\ &= 2[a, t][b, \overline{ac}] - [a.\overline{ac}, bt] \\ &= 2[a, t][bc, \overline{a}] - [\overline{ac}, \overline{a}.bt] \\ &= 2[bc, \overline{a}][a, t] - [a][\overline{cb}, t] \\ &= 2[a, \overline{bc}][a, t] - [a][\overline{bc}, t].\end{aligned}$$

Hence, $ab.ca$ is a function of bc and a only. This allows us to replace b and c by any elements with the same product. Let $b = bc$ and $c = 1$, this gives $ab.ca = a(bc).1a = a(bc).a$. Similarly, we get $ab.ca = a.(bc)a$. □

Theorem 2.4. *Let A be a composition algebra. Then for all $a, b \in A$, $ab.a = a.ba$.*

Proof. This is simply a consequence of the Moufang law. Let $c = 1$, we have $a(b1).a = ab.a = a.(b1)a = a.ba$. □

2.1 The left-, right- and bi-multiplication maps

The fact that the Octonions $\mathbb{O}$ are non-associative makes it interesting to investigate the maps so called left-multiplication, right-multiplication and bi-multiplication,

$$L_a : b \to ab, \quad R_a : b \to ba, \quad B_a : b \to aba.$$

Remark 2.2. In the following text, the notation b^{R_a} will be used, and is defined as $b^{R_a} := R_a(b) = ba$, as Conway does in the book *On quaternions and Octonions* [2]. Moreover, $b^{R_a L_a} := (b^{R_a})^{L_a}$.

The defintion of Bi-multilication in a composition algebra is well-defined, because $b^{L_a R_a} = ab.a = a.ba = b^{R_a L_a}$ by Theorem 2.4. This also shows that $B_a = L_a R_a = R_a L_a$.

Definition 2.3. Let A be a composition algebra and let $a, t \in A$. The reflection of t relative to a, is a map given by

$$\text{ref}(a) : t \to \frac{2[a,t]}{[a]} a - t.$$

Theorem 2.5. *Let A be a composition algebra and ι be an unit element in A. Then $B_\iota = \text{ref}(1)\text{ref}(\iota)$.*

Proof. Let $a, b, c \in A$. In the proof of the Moufang law, we deduced that $ab.ca = 2[a, \overline{bc}]a - [a]\overline{bc}$. Using the defintion of reflection, we have $ab.ca = [a](\overline{bc})^{\text{ref}(a)}$. Moreover, note that $\overline{bc} = 2[bc, 1] - bc = \frac{2[bc,1]1}{[1]} - bc = (bc)^{\text{ref}(1)}$, hence, $[a](\overline{bc})^{\text{ref}(a)} = [a](bc)^{\text{ref}(1)\text{ref}(a)}$. By letting $a = \iota$ be a unit element in A, thus $[a] = 1$, we deduce that $B_\iota = \text{ref}(1)\text{ref}(\iota)$. □

We can now continue investigating the octonions.

2.2 Basic properties of quaternions and octonions

We will now construct the quaternions and octonions based of the maps given in the previous section and the Dickson double.

We start with the quaternions. Let i be the fixed orthogonal unit of the Dickson double of $\mathbb{R}$, in other words we have $\mathbb{C} = D(\mathbb{R}) = a + ib$ where $a, b \in \mathbb{R}$. Let j be the element of the extension of $\mathbb{C}$. Because $B_i = \text{ref}(1)\text{ref}(i)$, we have that $j^{B_i} = iji = j$ since $\text{ref}(1)\text{ref}(i)$ fixes j. The fourth orthonormal element in $\mathbb{H}$ is given by $k := ij$. That this is orthonormal follows from the braid law. We thus have $ij = k$ which implies $ki = j$. We also have $jk = i$. Also, $i^2 = -1$, since $i^{-1} = -i$ by the definition of inverse. Similarly, $j^2 = -1$ and we have $k^2 = ijij = j^2 = -1$. We can conclude our results with the relations

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

and figure 1.

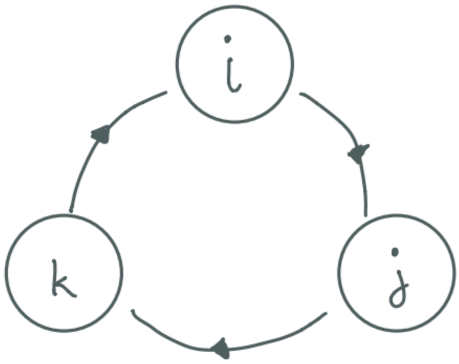

Figure 1: The figure displays the relation between multiplication of two elements from i, j, k. Taking two elements and multiplying them going clockwise, gives the next element by clockwise again. Multiplying two elements by following the arrow counterclockwise, gives the element by going counterclockwise again, but negative. For example, $ij = k$ and $ji = -k$.

For the octonions, we rename the units in the quaternions via

$$i_1 := i, \quad i_2 := j, \quad i_4 := k.$$

Let i_0 be the unit element using in construction of the Octonions, i.e. $\mathbb{O} = D(\mathbb{H}) = \mathbb{H} + i_0\mathbb{H}$. The other orthogonal units of $\mathbb{O}$ are given by $i_0 i_n := i_{3n}$, where the subscript n is taken module 7. [2] This results in

$$i_0 i_1 = i_3, \quad i_0 i_2 = i_6, \quad i_0 i_4 = i_5.$$

That these are orthonormal to i_0, i_1, i_2 and i_4 follows once again from the braid law. Recall that the quaternions $\mathbb{H}$ satisfy $i_0 a.b = i_0.ba$ for all $a, b \in \mathbb{H}$, thus

$$i_6 i_1 = i_0 i_2.i_1 = i_0.i_1 i_2 = i_0 i_4 = i_5,$$

$$i_5 i_2 = i_0 i_4.i_2 = i_0.i_2 i_4 = i_3,$$

and

$$i_3 i_4 = i_0 i_1.i_4 = i_0.i_4 i_1 = i_0 i_2 = i_6.$$

We can conclude our results with the relations

$$i_n^2 = -1, \quad n \in \mathbb{Z}/7\mathbb{Z}$$

and figure 2.

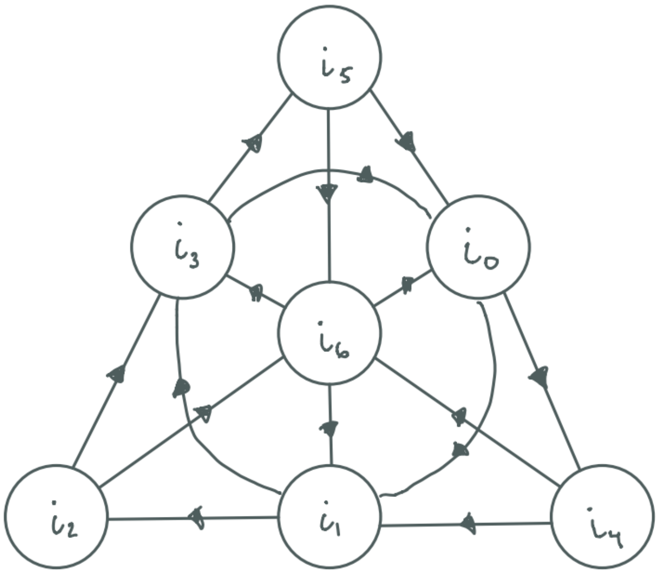

Figure 2: This is the Fano plane [3]. It contains 7 nodes and 7 edges. Each pair of nodes lies on a unique line. Multiplication between to elements i_n where $n \in \mathbb{Z}/7\mathbb{Z}$, is given by the uniqueness of the line. If we want to multiply $i_m i_n$, we look at the line of i_m and i_n. We start in the node i_m, and if we go one edge in the positive direction to i_n, the answer is the last node on the line and positive. If we go in the negative direction of one edge, the answer is the last node on the line but negative. If we go two edges in the positive direction it is negative, otherwise positive. For example, $i_2 i_0 = -i_6$ and $i_6 i_0 = i_2$.

3 Geometric interpretation of the Octonions $\mathbb{O}$

We will now investigate the geometric properties of the octonions $\mathbb{O}$.

Definition 3.1. The special orthogonal group $SO_n(F)$, is the group of orthogonal matrices with entries in a field F, of size $n \times n$ such that $det(A) = 1$ when $A \in SO_n(F)$.

Remark 3.1. When $n = 2$, $SO_n(\mathbb{R})$ is the group consisting of rotations in the two dimensional euclidean plane.

Remark 3.2. Note that if A is an element of SO_n, then $[Aa] = [a]$ where a is an element in a composition algebra. To see this, note that $[Aa, Ab] = [A^T Aa, b] = [a, b]$, why $[Aa] = [Aa, Aa] = [a, a] = [a]$. Hence, elements in A preserve length in a composition algebra. Thus, every element in SO_n can be viewed as a rotation, which itself can be viewed as an even number of reflections. This result will be used when looking at the connection between geometry and the Octonions $\mathbb{O}$.

It turns out that the special orthogonal group of dimension 8 over the field of real numbers $\mathbb{R}$, $SO_8(\mathbb{R})$, can be represented by multiplication of unit elements in $\mathbb{O}$. Before we look at the connection, we need to establish a notion of isotopy and inverse loops.

3.1 Isotopy and inverse loops

Definition 3.2 (Inverse loop)**.** An inverse loop L is a set of elements, together with a binary operation, that satisfy the following conditions for all $x, y \in L$.

1. There exist a unit $1 \in L$, such that $1x = x1 = x$.
2. There exist an element $x^{\dashv} \in L$ such that $x^{\dashv}(xy) = y = (yx)x^{\dashv}$.
3. $(x^{\dashv})^{\dashv} = x$. [2]

Remark 3.3. To make the reader more comfortable with the notion of an inverse loop, note that informally we can say an inverse loop is a group that is not *necessarily* associative.

Remark 3.4. Note that the existence of a left and right inverse of an element x in an inverse loop, together with a unit 1, is enough to prove that these are equal. To see this, let $x^{\dashv}$ be its left inverse and $y^{\dashv}$ be its right inverse. This gives $x^{\dashv} = x^{\dashv}1 = x^{\dashv}.xy^{\dashv} = y^{\dashv}$.

We can know define an isotopy.

Definition 3.3 (Isotopy)**.** An isotopy Σ of an inverse loop, is a tuple of three invertible maps $\Sigma = (\alpha, \beta|\gamma)$, such that if $xy = z$ for $x, y, z \in L$, then $x^{\alpha}y^{\beta} = z^{\gamma}$. [2]

Remark 3.5. The set of all isotopies of an inverse loop forms a group under function composition, i.e. $(\alpha, \beta|\gamma) \circ (\alpha', \beta'|\gamma') = (\alpha \circ \alpha', \beta \circ \beta'|\gamma \circ \gamma')$ for two isotopies $(\alpha, \beta|\gamma)$ and $(\alpha', \beta'|\gamma')$.

Remark 3.6. For an isotopy, we will use the notation $(\alpha, \beta|\gamma)$ to represent the **dublex form**. There is an analogous definition of an isotopy, that of the **triplex form**. For if $(\alpha, \beta|\gamma)$ is an isotopy, we have that $x^{\alpha}y^{\beta} = z^{\gamma}$ which implies $x^{\alpha}y^{\beta}z^{\gamma\dashv} = 1$. The last notation is called the triplex form, and the notation $(\alpha, \beta, \gamma \dashv)$ will be used to represent an isotopy satisfying $x^{\alpha}y^{\beta}z^{\gamma\dashv} = 1$. Hence, $\{\alpha, \beta, \gamma\}$ will be written as $(\alpha, \beta|\gamma)$ or (α, β, γ), which represents the isotopy in the dublex form and triplex form respectively.

Remark 3.7. The expression $xyz = 1$ is well defined. To see this, note that the Moufang law can be written as $x.yz = xyx.x^{\dashv}z$. Now, if $x.yz = 1$, then $z^{\dashv} = xyx.x^{\dashv}$ which implies $z^{\dashv} = xy$, hence $xy.z = 1$.

The notion of an isotopy makes the relation $xy = z$ interesting. Because if $xy = z$, then figure 3 shows six ways equivalent ways the relation can be written, based of the definition of an inverse loop.

$$
\begin{tikzcd}
 & xy = z \arrow[dl, dash] \arrow[dr, dash] & \\
y = x^{\dashv} z \arrow[d, dash] & & x = z y^{\dashv} \arrow[d, dash] \\
y z^{\dashv} = x^{\dashv} \arrow[dr, dash] & & z^{\dashv} x = y^{\dashv} \arrow[dl, dash] \\
 & z^{\dashv} = y^{\dashv} x^{\dashv} &
\end{tikzcd}
$$

Figure 3: This is the hexad of the relation $xy = z$. It shows the different ways the equation $xy = z$ can be written.

Definition 3.4 (Monotopy)**.** Given an isotopy $(\alpha, \beta|\gamma)$, any of these three maps is called a monotopy.

Theorem 3.1. *Given an inverse loop L. An invertible map $\gamma : L \to L$ is a monotopy of L if and only if there exist two elements $a, b \in L$ such that if $xy = z$ for $x, y, z \in L$, then $x^{\gamma} b.ay^{\gamma} = z^{\gamma}$.*

Proof. If γ is a monotopy, then there exist two maps α and β such that $x^{\alpha} y^{\beta} = z^{\gamma}$. If we let y be the unit, and $x = xy$, then $(xy)^{\alpha} 1^{\beta} = (xy)^{\gamma}$. Hence $(xy)^{\alpha} = (xy)^{\gamma} 1^{\beta \dashv} = (xy)^{\gamma} b$ where $\beta \dashv$ takes 1 to $b \in L$. Now, let x be the unit and let $y = xy$. Similarly, we have $(xy)^{\beta} = 1^{\alpha \dashv} (xy)^{\gamma} = a(xy)^{\gamma}$ where $\alpha \dashv$ takes 1 to $a \in L$. This shows that there exist elements a, b such that $(xy)^{\gamma} = x^{\gamma} b.ay^{\gamma}$.

If there exist two elements $a, b \in L$ such that $x^{\gamma} b.ay^{\gamma} = z^{\gamma}$, then $(\alpha, \beta|\gamma)$ is an isotopy with $\alpha = \gamma R_b$ and $\beta = \gamma L_a$ showing that γ is an monotopy of L. $\square$

We call a and b a pair of **companions** to the monotopy γ. What we see is that if γ is a monotopy, then the other monotopies that fulfil the triad $(\alpha, \beta|\gamma)$ are given by $\alpha = \gamma R_b$ and $\beta = \gamma L_a$, where R_b and L_a are the right- and left-multiplication maps defined in section 3.1. It turns out that even more is true.

Theorem 3.2 (The different monotopies)**.** *Let L be an inverse loop and let $a \in L$ be the image of 1 under some monotopy. Then the monotopy is either R_a or L_a. Even more, the only monotopies that exist in this inverse loop are given by $L_a, L_{a^{\dashv}}, R_a, R_{a^{\dashv}}, B_a$ and $B_{a^{\dashv}}$.*

To prove this, we need to establish the hexad of isotopies. If we apply the isotopy $(\alpha, \beta|\gamma)$ to the hexad in figure 3, we get the following hexad in figure 4.

$$\begin{tikzcd}[column sep=small]
 & x^{\alpha}y^{\beta} = z^{\gamma} \arrow[dl, no head] \arrow[dr, no head] & \\
x^{\dashv\alpha}z^{\beta} = y^{\gamma} \arrow[d, no head] & & z^{\alpha}y^{\dashv\beta} = x^{\gamma} \arrow[d, no head] \\
y^{\alpha}z^{\dashv\beta} = x^{\dashv\gamma} \arrow[dr, no head] & & z^{\dashv\alpha}x^{\beta} = y^{\dashv\gamma} \arrow[dl, no head] \\
 & y^{\dashv\alpha}x^{\dashv\beta} = z^{\dashv\gamma} &
\end{tikzcd}$$

Figure 4: This is the hexad of the relation $xy = z$. It shows the different ways the equation $xy = z$ can be written.

Undoing the hexad in figure 4, results in the following hexad in figure 5, showing the isotopies in the dublex from.

$$\begin{tikzcd}[column sep=small]
 & (\alpha, \beta|\gamma) \arrow[dl, no head] \arrow[dr, no head] & \\
(\dashv \alpha \dashv, \gamma|\beta) \arrow[d, no head] & & (\gamma, \dashv \beta \dashv |\alpha) \arrow[d, no head] \\
(\dashv \gamma \dashv, \alpha| \dashv \beta \dashv) \arrow[dr, no head] & & (\beta, \dashv \gamma \dashv | \dashv \alpha \dashv) \arrow[dl, no head] \\
 & (\dashv \beta \dashv, \dashv \alpha \dashv | \dashv \gamma \dashv) &
\end{tikzcd}$$

Figure 5: This is the hexad of isotopies. If $(\alpha, \beta|\gamma)$ is an isotopy, then the other elements in this hexad are also isotopies.

Proof of the different monotopies. If $(\alpha, \beta|\gamma)$ is an isotopy, then $(\alpha, \beta|\gamma)^{-1} = (\alpha^{-1}, \beta^{-1}|\gamma^{-1})$ and $(\dashv \alpha \dashv, \beta|\gamma)$ are also isotopies by the hexad of isotopies figure 5. Hence, $(\alpha, \beta|\gamma)^{-1} \cdot (\dashv \alpha \dashv, \beta|\gamma) := (\alpha^{-1} \dashv \alpha \dashv, \beta^{-1}\gamma)|\gamma^{-1}\beta)$ is also an isotopy. Recall that $\beta = \gamma L_a$, hence, $\gamma^{-1}\beta = L_a$ which also results in $\beta^{-1}\gamma = L_a^{-1}$. Now, $L_a^{-1} : x \to a^{\dashv}x$, and thus $L_a^{-1} = L_{a^{\dashv}}$. Therefore, the isotopy $(\alpha^{-1} \dashv \alpha \dashv, \beta^{-1}\gamma)|\gamma^{-1}\beta)$ can be rewritten as $(\alpha^{-1} \dashv \alpha \dashv, L_{a^{\dashv}}|L_a)$. We let this isotopy act on xa, which yields

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

Hence, $\alpha^{-1} \dashv \alpha \dashv$ takes an element x to $a(xa)$. Using the isotopy on arbitrary elements x, y in the inverse loop L, we have $a(xa).a^{\dashv}y = a(xy)$, and therefore $a(xa).a^{\dashv} = ax$ which implies that $a(xa) = (ax)a$. This relation allows us to use the bi-multiplication map B_a instead of $\alpha^{-1} \dashv \alpha \dashv$. This shows the equivalence between an arbitrary isotopy $(\alpha, \beta|\gamma)$ and $(B_a, L_{a^{\dashv}}|L_a)$.

To finish the proof, we need to show that the different ways the isotopy $(\alpha, \beta|\gamma)$ can be written as. In figure 3, we saw that the isotopy can be represented in six different ways. Each monotopy, say σ, occurred in the form σ or $\dashv \sigma \dashv$. Thus, we need to investigate the transformation of

1. $\dashv L_a \dashv$,
2. $\dashv R_a \dashv$,
3. and $\dashv B_a \dashv$.

Given an element x in the inverse loop L, $x^{\dashv L_a \dashv} = (ax^{\dashv})^{\dashv} = xa^{\dashv} = x^{R_{a^{\dashv}}}$. Similarly we show that $\dashv R_a \dashv = L_{a^{\dashv}}$ and $\dashv B_a \dashv = B_{a^{\dashv}}$. □

3.2 Isotopies and SO_8

In this section we will look at isotopies over the inverse loop $\mathbb{O}^{\times}$. From the previous section we saw the connection of an isotopy to the left-, right- and bi-multiplication maps, and that they had a connection to the octonions $\mathbb{O}$. Thus, this section will look deeper into the connection between $SO_8(\mathbb{R})$ and the octonions. We begin by showing that the octonions are *strongly* non-associative.

Theorem 3.3. *If $a.rb = ar.b$ for all a, b in $\mathbb{O}$, then r is real.*

Proof. From section 3.2, we have $i_{n+1}i_n.i_{n+2} = -i_{n+1}.i_ni_{n+2}$ where the subscript n is run over modulo 7. Thus, if $a.rb = a.rb$, then the coefficient of i_n for all n must be 0. Hence, r is real. □

Theorem 3.4. *If $a, b \in \mathbb{O}$ is any pair of companions for the monotopy γ over the inverse loop $\mathbb{O}^{\times}$ (meaning if $xy = z$, then $z^{\gamma} = x^{\gamma}a.by^{\gamma}$), then any other pair has the form $ar, r^{-1}b$ where r is real.*

Proof. Let c, d be another pair of companions for γ, then

$$x^{\gamma}a.by^{\gamma} = x^{\gamma}c.dy^{\gamma} \qquad \text{for all}\, x, y.$$

Let $c = ar$ and choose $x^\gamma = a^{-1}$ and $y^\gamma = 1$. Thus, $b = rd$ and therefore $d = r^{-1}b$. This results in

$$x^\gamma a.by^\gamma = x^\gamma(ar).(r^{-1}b)y^\gamma \qquad \text{for all}\, x, y.$$

By choosing $y^\gamma = (r^{-1}b)^{-1} = b^{-1}r$ results in $x^\gamma a.r = x^\gamma.ar$. Similarly, choosing $x^\gamma = (ar)^{-1} = r^{-1}a^{-1}$ results in $r^{-1}.by^\gamma = r^{-1}b.y^\gamma$, showing the associative law of the companions and r. We therefore have

$$x^\gamma a.by^\gamma = (x^\gamma a)r.r^{-1}(by^\gamma) \qquad \text{for all}\, x, y.$$

Lastly, letting $x^\gamma a = p$ and $by^\gamma = rq$ results in

$$p.rq = pr.q \qquad \text{for all}\, p, q.$$

From Theorem 3.3, r has to be real. □

Before we look at the connection between elements in SO_8 and the octonions $\mathbb{O}$, we need this Lemma.

Lemma 3.5. *Let a be an octonion. The maps* $\mathrm{ref}(a)\mathrm{ref}(1)$ *and* $\mathrm{ref}(1)\mathrm{ref}(a)$ *are bimultiplications by unit octonions.*

Proof. We saw in Theorem 2.5 that if a is a unit, then the expression $\mathrm{ref}(1)\mathrm{ref}(a)$ can be represented by a bimultiplication. That this is also true for $\mathrm{ref}(a)\mathrm{ref}(1)$ follows from the fact that $t^{\mathrm{ref}(1)} = \bar{t}$, hence $ab.ca = [a](bc)^{\mathrm{ref}(a)\mathrm{ref}(1)}$. Furthermore, from the proof of the Moufang law, we had $\frac{ab.ca}{[a]} = (bc)^{\mathrm{ref}(1)\mathrm{ref}(a)}$. It is clear that the result is unaffected if we scale a to be a unit, since the norm is quadratic. Hence, the result follows. □

Theorem 3.6. *Let γ be an element in $SO_8(\mathbb{R})$. Then γ is a monotopy over $\mathbb{O}^\times$. Even more, there are precisely two isotopies that contains the monotopy γ. If one is given by $(\alpha, \beta|\gamma)$, then the other isotopy is given by $(-\alpha, -\beta|\gamma)$.*

Proof. Since γ is an element of SO_8, then it can be written as an even number of reflections, say $\mathrm{ref}(a_1)\mathrm{ref}(b_1)...\mathrm{ref}(a_n)\mathrm{ref}(b_n)$. The equality $\mathrm{ref}(a_1)\mathrm{ref}(b_1) = \mathrm{ref}(a_1)\mathrm{ref}(1)\mathrm{ref}(1)\mathrm{ref}(b_1)$ follows from the fact that $\mathrm{ref}(1)\mathrm{ref}(1)$ is the identity reflection. Furthermore, from Lemma 3.5, we know that $\mathrm{ref}(a_k)\mathrm{ref}(1)$ and $\mathrm{ref}(1)\mathrm{ref}(b_k)$ can be represented as bimultiplications by unit octonions, say $B_{c_{2k-1}}$ and $B_{c_{2k}}$. Then $(L_{c_1}...L_{c_{2n}}, R_{c_1}...R_{c_{2n}}|B_{c_1}...B_{c_{2n}})$ is an isotopy, showing that γ is a monotopy. That $\alpha = L_{c_1}...L_{c_{2n}}$ and $\beta = R_{c_1}...R_{c_{2n}}$ are elements in SO_8 is true since $c_1...c_{2n}$ are unit octionions.

From Theorem 3.3, α and β are unique up to scalar multiplication. Thus, the only scalar that keeps them in SO_8 is -1, showing that $(-\alpha, -\beta|\gamma)$ is the only other isotopy. □

Remark 3.8. For the rest of this paper, it is convenient to change to the triplex form of an isotopy, namely (α, β, γ). What we found in Theorem 3.6, is that if γ is an monotopy in SO_8, then it takes the form

$$(L_{c_1}L_{c_2}..., R_{c_1}R_{c_2}..., B_{\overline{c_1}}B_{\overline{c_2}}...).$$

We call the isotopy (α, β, γ) an **orthogonal** isotopy if the three monotopies α, β, γ are elements of SO_8. Theorem 3.6 shows that there exist a group homomorphism from the group of orthogonal isotopies to SO_8, namely the homomorphism taking $(\alpha, \beta, \gamma) \to \gamma$. Even more, the same Theorem shows that the group of orhogonal isotopies is a two-to-one cover of SO_8. We will call the group of orthogonal isotopies of the dublex form $\mathrm{Iso}_1(\mathbb{O})$, and the group of orthogonal isotopies of the triplex form $\mathrm{Iso}_2(\mathbb{O})$. In fact, $\mathrm{Iso}_1(\mathbb{O}) \simeq \mathrm{Iso}_2(\mathbb{O})$ which is discussed in remark 3.6.

3.3 Triality

Theorem 3.7. *The group* $\mathrm{Iso}_2(\mathbb{O})$ *has a triality automorphism, and is given by* $(\alpha, \beta, \gamma) \to (\beta, \gamma, \alpha)$.

Proof. If (α, β, γ) is an isotopy, then for all octonions x, y, z that satisfy $xyz = 1$, we have $x^\alpha y^\beta z^\gamma = 1$. Thus, we have $y^\beta z^\gamma = x^{\alpha^{-1}}$. Multiplying with the inverse again, but now on the right side, yields $y^\beta z^\gamma x^\alpha = 1$, showing that (β, γ, α) is an isotopy. Thus, the map is well-defined. □

We now come to the final theorem of this paper. That is that every element is SO_8 can be represented as left multiplication by unit octonions (or equally by right ones).

Theorem 3.8. *Every element in SO_8 can be represented as left multiplication by unit octonions (or by right multiplication by unit octonions).*

Proof. We showed earlier that every element can be represented as a bimultiplication of unit octonions. Applying Theorem 3.7, that of triality, shows that every element in SO_8 can be represented by either left- or right-multiplication of unit octonions. □

Acknowledgment

I would like to thank Wushi Goldring giving me material, giving me feedback and helping me overall with this topic.

References

[1] R. D. Shafer, *An Introduction To Nonassociative Algebras.* Stillwater, Oklahoma: Gutenberg, 1961, pp. 61-65.

[2] J. H. Conway and D. A. Smith, *On Quarternions and Octonions: Their Geometry, Arithmetic, and Symmetry.* Natick, Massachusetts: A K Peters, 2004, pp. 61-65.

[3] J. C. Baez, “The Octonions,” *Bull. Amer. Math. Soc.*, vol. 39, pp. 145–205, Dec. 2001.