THE OCTONIONS

by

DAVOUD GHATEI

A thesis submitted to
The University of Birmingham
for the degree of
Master of Philosophy

School of Mathematics
The University of Birmingham
OCTOBER 2010

Abstract

In this project we describe the non-associative finite-dimensional composition algebra called the Octonions and denoted $\mathbb{O}$. We begin by introducing the structure and then go on to describe its finite multiplicative substructures. We then introduce the number theory associated to it before studying its symmetry structure. The project ends with an application of the octonions to physics.

Acknowledgements

I would like to thank first and foremost my supervisor Robert Curtis for his continued support and patience throughout this project and for sharing his vast knowledge of mathematics. I would also like to thank Chris, Sergey, Rob Wilson, Kay and Ralf for taking the time to discuss any problems that came up. A special ‘thank you’ is owed to Janette whose tireless efforts keep us all going.

I would also like to thank Simon and Dr. R. Lawther for providing corrections to the thesis.

Contents

Chapter 1

Introduction and Hurwitz' Theorem

There are precisely four real finite-dimensional composition algebras $\mathbb{R}$, $\mathbb{C}$, $\mathbb{H}$ and $\mathbb{O}$. The real numbers $\mathbb{R}$ and the complex numbers $\mathbb{C}$ are well-known and their properties and applications widely-studied. The reals form a ordered field and the complex numbers are algebraically complete. The quaternions $\mathbb{H}$, which were discovered by Sir William Rowan Hamilton in 1843, fail to be commutative. The last of them, the octonions $\mathbb{O}$, discovered independently by Graves and Cayley, are even more 'exotic' as not only are they non-commutative but they also fail to be associative.

In this chapter we will introduce the octonions and investigate some of their basic properties. The chapter ends with Hurwitz' theorem which states that the four division algebras we introduce are the only finite-dimensional ones. We do this by introducing a process known as the Cayley-Dixon doubling process which generalises the construction of the complex numbers from the reals.

1.1 The Complex Numbers

We begin with the real numbers. These form a field and hence they are both associative and commutative. Also, every element λ of $\mathbb{R}$ can be assigned a length $|\lambda| = \sqrt{\lambda^2}$ which satisfies the multiplicative property that if $\lambda, \mu \in \mathbb{R}$, then

$$|\lambda\mu| = |\lambda||\mu|.$$

Also every element λ has an inverse $\lambda^{-1} = \frac{1}{\lambda}$.

A complex number is of the form $z = \lambda + \mu i$, where λ, μ are both real and $i^2 = -1$. We define the conjugate of z to be

$$\overline{z} = \lambda - \mu i.$$

It is easy to see that $\overline{z_1 z_2} = \overline{z_2}\,\overline{z_1}$. Every non-trivial complex number z has a norm

$$N(z) = z\overline{z} = \overline{z}z = \lambda^2 + \mu^2.$$

The function N is a positive-definite quadratic form. From the above definition we get that

$$z^{-1} = \frac{\overline{z}}{N(z)}.$$

Now, we have

$$N(z_1 z_2) = (z_1 z_2)(\overline{z_1 z_2}) = z_1 z_2 \overline{z_2}\,\overline{z_1} = z_1 \overline{z_1} z_2 \overline{z_2} = N(z_1)N(z_2).$$

This is equivalent to the 2-squares identity

$$(\lambda_1^2+\mu_1^2)(\lambda_2^2+\mu_2^2)=(\lambda_1\lambda_2-\mu_1\mu_2)^2+(\lambda_1\mu_2+\mu_1\lambda_2)^2.$$

1.2 The Quaternions

A typical quaternion $q \in \mathbb{H}$ is normally written in the form

$$q=\alpha+\beta i+\gamma j+\delta k$$

with $\alpha,\beta,\gamma,\delta \in \mathbb{R}$. We have the mulitiplication rules

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

and

$$ijk=-1.$$

These immediately imply

$$ij=k \quad jk=i \quad ki=j \quad ji=-k \quad ik=-j \quad kj=-i.$$

Note that these show that the quaternions are not commutative. However, a simple check of the elements i,j,k shows they are associative.

Define the conjugate of a quaternion q to be $\overline{q}=\alpha-\beta i-\gamma j-\delta k$. Direct computation shows that $\overline{q_1q_2}=\overline{q_2}\,\overline{q_1}$. The norm of a quaternion is defined as

$$N(q)=q\overline{q}=\overline{q}q=\alpha^2+\beta^2+\gamma^2+\delta^2.$$

N is a positive-definite quadratic form. From the definition of the norm it follows that

$$q^{-1} = \frac{\overline{q}}{N(q)}.$$

As norms are real numbers, they commute with every quaternion. Using this fact and the associativity of $\mathbb{H}$, yields

$$N(q_1q_2) = (q_1q_2)(\overline{q_1q_2}) = (q_1q_2)(\overline{q_2}\,\overline{q_1}) = q_1(q_2\overline{q_2})\overline{q_1} = q_1N(q_2)\overline{q_1}$$

$$= q_1\overline{q_1}N(q_2) = N(q_1)N(q_2).$$

When written out in full, this is the 4-squares identity

$$(\alpha_1^2 + \beta_1^2 + \gamma_1^2 + \delta_1^2)(\alpha_2^2 + \beta_2^2 + \gamma_2^2 + \delta_2^2)$$

$$= (\alpha_1\alpha_2 + \beta_1\beta_2 + \gamma_1\gamma_2 + \delta_1\delta_2)^2 + (\alpha_1\beta_2 + \beta_1\alpha_2 + \gamma_1\delta_2 - \delta_1\gamma_2)^2$$

$$+(\alpha_1\gamma_2 - \beta_1\delta_2 + \gamma_1\alpha_2 + \delta_1\beta_2)^2 + (\alpha_1\delta_2 + \beta_1\gamma_2 - \gamma_1\beta_2 + \delta_1\alpha_2)^2.$$

We can consider

$$q = (\alpha + \beta i) + (\gamma + \delta i)j$$

and so $\mathbb{H} = \mathbb{C} + \mathbb{C}j$ which is analogous to the construction of the complex numbers from the reals above. The quaternions are therefore a 4-dimensional real vector space with basis $\{1, i, j, k\}$ or a 2-dimensional complex vector space with basis $\{1, j\}$. Then a typical quaternion is just a pair of complex numbers $a = (x, y)$. Addition is again componentwise and multiplication is given by

$$a_1a_2 = (x_1, y_1)(x_2, y_2) = (x_1x_2 - \overline{y_2}y_1, y_2x_1 + y_1\overline{x_2}).$$

We can define the conjugate of a quaternion as

$$\overline{a} = (\overline{x}, -y).$$

We now define the real and imaginary parts of a quaternion a to be $Re(a) = \frac{1}{2}(a+\overline{a})$ and $Im(a) = \frac{1}{2}(a-\overline{a})$, respectively. This definition differs from that in the complex case as we do not take a real number to be the imaginary part but an expression in i, j, k.

1.3 The Octonions

We now move to our final protagonist and the main theme of this project, the 8-dimensional non-associative algebra of the octonions.

An octonion a is normally written in the form

$$a = \lambda_\infty + \sum_{k=0}^{6} \lambda_k i_k$$

with $\lambda_k \in \mathbb{R}$ for $k \in \{\infty, 0, 1, 2, 3, 4, 5, 6\}$. Addition is again componentwise and multiplication is given by the following rules,

$$i_k^2 = -1$$

$$i_k i_{k+1} i_{k+3} = -1$$

with the subscripts read modulo 7. The second of these identities should be taken to mean the same as for the quaternions. This shows there are seven natural **associative triples** namely, $\{i_0, i_1, i_3\}$, $\{i_1, i_2, i_4\}$, $\{i_2, i_3, i_5\}$, $\{i_3, i_4, i_6\}$, $\{i_4, i_5, i_0\}$, $\{i_5, i_6, i_1\}$ and $\{i_6, i_0, i_2\}$. Each of these behaves as i, j, k in $\mathbb{H}$. This is represented in Figure 1.1, where following the arrows yields a positive product for example $i_0 i_1 = i_3$,

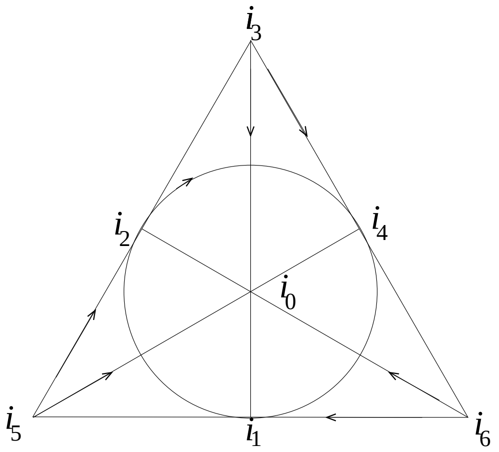

Figure 1.1: Multiplication in $\mathbb{O}$

$i_1 i_3 = i_0$, $i_3 i_0 = i_1$ and going against the arrows yields a negative product. The full multiplication table can then be obtained from these relations.

1	i_0	i_1	i_2	i_3	i_4	i_5	i_6
i_0	-1	i_3	i_6	$-i_1$	i_5	$-i_4$	$-i_2$
i_1	$-i_3$	-1	i_4	i_0	$-i_2$	i_6	$-i_5$
i_2	$-i_6$	$-i_4$	-1	i_5	i_1	$-i_3$	i_0
i_3	i_1	$-i_0$	$-i_5$	-1	i_6	i_2	$-i_4$
i_4	$-i_5$	i_2	$-i_1$	$-i_6$	-1	i_0	i_3
i_5	i_4	$-i_6$	i_3	$-i_2$	$-i_0$	-1	i_1
i_6	i_2	i_5	$-i_0$	i_4	$-i_3$	$-i_1$	-1

From this table it is immediately clear that the multiplication of the seven basis vectors i_k is anti-commutative $i_m i_n = -i_n i_m$ for $n \neq m$. However, 1 commutes with everything. It is also easy to see that multiplication is not associative as

$$i_5(i_4 i_6) = i_5 i_3 = -i_2 \neq i_2 = -i_0 i_6 = (i_5 i_4) i_6.$$

If $a = \lambda_\infty + \lambda_0 i_0 + \lambda_1 i_1 + \lambda_2 i_2 + \lambda_3 i_3 + \lambda_4 i_4 + \lambda_5 i_5 + \lambda_6 i_6$ is a typical octonion, then we let the conjugate of a be

$$\overline{a} = \lambda_\infty - \lambda_0 i_0 - \lambda_1 i_1 - \lambda_2 i_2 - \lambda_3 i_3 - \lambda_4 i_4 - \lambda_5 i_5 - \lambda_6 i_6$$

Direct computation again yields

$$\overline{a_1 a_2} = \overline{a_2}\,\overline{a_1}.$$

The norm is defined to be

$$N(a) = a\overline{a} = \overline{a}a = \lambda_\infty^2 + \lambda_0^2 + \lambda_1^2 + \lambda_2^2 + \lambda_3^2 + \lambda_4^2 + \lambda_5^2 + \lambda_6^2.$$

This a positive-definite quadratic form on $\mathbb{O}$. From the above definition we get

$$a^{-1} = \frac{\overline{a}}{N(a)}.$$

From our definition of the inverse of a, we get $\overline{a} = a^{-1}N(a)$ and so

$$N(a_1 a_2) = (a_1 a_2)(\overline{a_1 a_2}) = (a_1 a_2)(\overline{a_2}\,\overline{a_1}) = (a_1 a_2)(a_2^{-1}N(a_2)a_1^{-1}N(a_1)).$$

Again the norms are real numbers and commute with each other. This yields

$$N(a_1 a_2) = N(a_1)N(a_2)(a_1 a_2)(a_2^{-1}a_1^{-1}).$$

It will be shown later that any subalgebra of $\mathbb{O}$ generated by two linearly independent elements is associative. This implies that the two terms on the right-hand side of the above expression cancel and we are left with

$$N(a_1a_2) = N(a_1)N(a_2).$$

Writing this out in full gives the remarkable 8-squares identity;

$$(\lambda_\infty^2+\lambda_0^2+\lambda_1^2+\lambda_2^2+\lambda_3^2+\lambda_4^2+\lambda_5^2+\lambda_6^2)(\mu_\infty^2+\mu_0^2+\mu_1^2+\mu_2^2+\mu_3^2+\mu_4^2+\mu_5^2+\mu_6^2)$$

$$\begin{aligned}
&= (\lambda_\infty\mu_\infty - \lambda_0\mu_0 - \lambda_1\mu_1 - \lambda_2\mu_2 - \lambda_3\mu_3 - \lambda_4\mu_4 - \lambda_5\mu_5 - \lambda_6\mu_6)^2 \\
&+(\lambda_\infty\mu_0 + \lambda_0\mu_\infty + \lambda_1\mu_3 + \lambda_2\mu_6 - \lambda_3\mu_1 + \lambda_4\mu_5 - \lambda_5\mu_4 - \lambda_6\mu_2)^2 \\
&+(\lambda_\infty\mu_1 - \lambda_0\mu_3 + \lambda_1\mu_\infty + \lambda_2\mu_4 + \lambda_3\mu_0 - \lambda_4\mu_2 + \lambda_5\mu_6 - \lambda_6\mu_5)^2 \\
&+(\lambda_\infty\mu_2 - \lambda_0\mu_6 - \lambda_1\mu_4 + \lambda_2\mu_\infty + \lambda_3\mu_5 + \lambda_4\mu_1 - \lambda_5\mu_3 + \lambda_6\mu_0)^2 \\
&+(\lambda_\infty\mu_3 + \lambda_0\mu_1 - \lambda_1\mu_0 - \lambda_2\mu_5 + \lambda_3\mu_\infty + \lambda_4\mu_6 + \lambda_5\mu_2 - \lambda_6\mu_4)^2 \\
&+(\lambda_\infty\mu_4 - \lambda_0\mu_5 + \lambda_1\mu_2 - \lambda_2\mu_1 - \lambda_3\mu_6 + \lambda_4\mu_\infty + \lambda_5\mu_0 + \lambda_6\mu_3)^2 \\
&+(\lambda_\infty\mu_5 - \lambda_0\mu_4 - \lambda_1\mu_6 + \lambda_2\mu_3 - \lambda_3\mu_2 + \lambda_4\mu_0 + \lambda_5\mu_\infty + \lambda_6\mu_1)^2 \\
&+(\lambda_\infty\mu_6 + \lambda_0\mu_2 + \lambda_1\mu_5 - \lambda_2\mu_0 + \lambda_3\mu_4 - \lambda_4\mu_3 - \lambda_5\mu_1 + \lambda_6\mu_\infty)^2.
\end{aligned}$$

Continuing as before, we can define an octonion as

$$a = (\lambda_\infty + \lambda_0 i_0 + \lambda_1 i_1 + \lambda_3 i_3) + (\lambda_2 + \lambda_4 i_1 - \lambda_5 i_3 + \lambda_6 i_0)i_2$$

and so $\mathbb{O} = \mathbb{H}+\mathbb{H}i_2$. The octonions can be considered as an 8-dimensional real vector space with basis $\{1, i_0, i_1, i_2, i_3, i_4, i_5, i_6\}$, a 4-dimensional complex vector space with basis $\{1, i_1, i_2, i_4\}$ (with complex numbers of the form $\lambda + \mu i_0$) and a 2-dimensional quaternion 'vector space' with basis $\{1, i_2\}$ (strictly speaking a vector space is defined over a field and $\mathbb{O}$ here is a module over $\mathbb{H}$). So an octonion can be considered as a pair (x, y) with $x, y \in \mathbb{H}$. Addition is again componentwise and multiplication is given by

$$a_1 a_2 = (x_1, y_1)(x_2, y_2) = (x_1 x_2 - \overline{y_2} y_1, y_2 x_1 + y_1 \overline{x_2}).$$

Once more, we have that $Re(a) = \frac{1}{2}(a + \overline{a})$ and $Im(a) = \frac{1}{2}(a - \overline{a})$.

We end this section showing how the algebras are nested inside each other and in fact the octonions contain copies of the other three. The proof comes from [7]

Theorem 1.1

We have the following

1. *Any single element of* $\mathbb{O} \setminus \mathbb{R}$ *generates a copy of* $\mathbb{C}$ *as an* $\mathbb{R}$*-algebra;*

2. *Any two linearly independent elements of* $\mathbb{O} \setminus \mathbb{R}$ *generate a copy of* $\mathbb{H}$ *as an* $\mathbb{R}$*-algebra;*

3. *Any three linearly independent elements of* $\mathbb{O} \setminus \mathbb{R}$ *generate the whole of* $\mathbb{O}$ *as an* $\mathbb{R}$*-algebra.*

Proof. We first note that given any octonion a if we choose $\widehat{i}$ to be the unit vector in the $Im(a)$ direction then we can write a uniquely as

$$a = re^{\widehat{i}\theta}$$

where $r = \sqrt{N(a)}$ and θ is the angle between the real axis and the the vector a in the plane with basis $\{1, \widehat{i}\}$ (indeed the same is true of quaternions and complex numbers).

Choose $a \in \mathbb{O}$ then we can assume without loss of generality that $N(a) = 1$. Hence $a = e^{\widehat{i}\theta}$ where $\widehat{i}$ is as above and $\widehat{i}^2 = -1$. We get that $e^{\widehat{i}\theta}, e^{2\widehat{i}\theta} \in \mathbb{R}(e^{\widehat{i}\theta})$ which implies that $\cos 2\theta e^{\widehat{i}\theta} - \cos\theta e^{2\widehat{i}\theta} \in \mathbb{R}(e^{\widehat{i}\theta})$. This tells us that $\widehat{i} \in \mathbb{R}(e^{\widehat{i}\theta})$ so we get the inclusions

$$\mathbb{R}(e^{\widehat{i}\theta}) \subseteq \mathbb{R}(\,\widehat{i}\,) \subseteq \mathbb{R}(e^{\widehat{i}\theta}),$$

from which we conclude that

$$\mathbb{R}(a) = \mathbb{R}(\,\widehat{i}\,) = \mathbb{R}(e^{\widehat{i}\theta}).$$

Now choose a second element b such that $N(b) = 1$ and $\widehat{j}(\neq \widehat{i})$ is the unit vector in the $Im(b)$ direction, then $b = e^{\widehat{j}\phi}$ as before. Then as above we get

$$\mathbb{R}(a, b) = \mathbb{R}(\,\widehat{i}\,, \widehat{j}\,).$$

If the inner-product $\langle \widehat{i}, \widehat{j} \rangle = \lambda$ for some non-zero λ, we get $\langle \widehat{i}, \widehat{j} - \lambda\widehat{i} \rangle = 0$. It follows that

$$\mathbb{R}(\widehat{i}, \widehat{j}) = \mathbb{R}(\widehat{i}, \widehat{j} - \lambda\widehat{i}).$$

However, $Re(\widehat{\widehat{i}\widehat{j}}) = -\langle \widehat{i}, \widehat{j} \rangle = 0$ and $\widehat{\widehat{i}\widehat{j}}$ is purely imaginary. Moreover,

$$N(\widehat{\widehat{i}\widehat{j}}) = N(\widehat{i})N(\widehat{j}) = 1 = \langle \widehat{\widehat{i}\widehat{j}}, \widehat{\widehat{i}\widehat{j}} \rangle = -(\widehat{\widehat{i}\widehat{j}})^2$$

similarly $\widehat{\widehat{i}\widehat{j}} = -\widehat{\widehat{j}\widehat{i}}$. Since $N(\widehat{i}) = N(\widehat{j}) = 1$, multiplication by $\widehat{i}$ or $\widehat{j}$ is an orthogonal map and should therefore preserve inner-products. So, $\langle \widehat{\widehat{i}\widehat{j}}, \widehat{i} \rangle = \langle \widehat{j}, 1 \rangle = 0$ and so $\langle \widehat{i}, \widehat{j} \rangle = 0$. We conclude that the vectors $\{\widehat{i}, \widehat{j}, \widehat{\widehat{i}\widehat{j}}\}$ form a mutually orthogonal basis which behaves exactly like the basis $\{i, j, k\}$ of $\mathbb{H}$.

Lastly, adjoin an element c of unit norm and with $c = e^{\widehat{k}\psi}$ as before with $\widehat{k} \notin \mathbb{R}(\widehat{i}, \widehat{j})$ and $\widehat{k}^2 = -1$. If $\widehat{k}$ is not perpendicular to the space $\mathbb{R}(\widehat{i}, \widehat{j})$ then if the inner-products of $\widehat{k}$ with $\widehat{i}, \widehat{j}$ and $\widehat{\widehat{i}\widehat{j}}$ are λ_1, λ_2 and λ_3, respectively, then we get $\widehat{c} = \widehat{k} - \lambda_1\widehat{i} -$

$\lambda_2\widehat{j} - \lambda_3\widehat{\widehat{i}\widehat{j}}$ is perpendicular to $\mathbb{R}(\widehat{i},\widehat{j})$ and we could take a normalised vector of $\widehat{c}$ as $\widehat{k}$. Hence we may assume $\widehat{k}$ is perpendicular to $\mathbb{R}(\widehat{i},\widehat{j})$. The set $\{1, \widehat{i}, \widehat{j}, \widehat{\widehat{i}\widehat{j}}, \widehat{k}, \widehat{\widehat{i}\widehat{k}}, \widehat{\widehat{j}\widehat{k}}, \widehat{(\widehat{i}\widehat{j})}\widehat{k}\}$ contains eight mutually orthogonal vectors. To check this note

$$\langle \widehat{(\widehat{i}\widehat{j})}\widehat{k}, \widehat{j}\rangle = 0 \Leftrightarrow \langle -\widehat{\widehat{i}\widehat{j}}, \widehat{\widehat{j}\widehat{k}}\rangle = 0 \Leftrightarrow \langle -\widehat{\widehat{i}\widehat{j}}, -\widehat{\widehat{k}\widehat{j}}\rangle = 0 \Leftrightarrow \langle \widehat{i}, \widehat{k}\rangle = 0.$$

The other relations are similarly checked. The set in fact forms a basis for the algebra $\mathbb{O}$ under the correspondence $\widehat{i} = i_0, \widehat{j} = i_1, \widehat{\widehat{i}\widehat{j}} = i_3, \widehat{k} = i_2, \widehat{\widehat{i}\widehat{k}} = i_6, \widehat{\widehat{j}\widehat{k}} = i_4, \widehat{(\widehat{i}\widehat{j})}\widehat{k} = -i_5$. □

1.4 Hurwitz' Theorem

In [13] we learn that in 1898 Hurwitz was interested in finding for what values of n there exist equations of the form

$$\left(\sum_{n=1}^{n} a_i^2\right)\left(\sum_{n=1}^{n} b_i^2\right) = \sum_{n=1}^{n} c_i^2$$

with $c_i = \sum_{j,k=1}^{n} \lambda_{ijk} a_j b_k, \lambda_{ijk} \in \mathbb{C}$. For $n = 1, 2, 4$ and 8 such equations were known. For the case $n = 1$, this is the simple relation $a_1^2 b_1^2 = (a_1 b_1)^2$. The case $n = 2$ was discovered by Diophantus [14] and is equivalent to the multiplicative property of the modulus of complex numbers. The identity for $n = 4$ is said to be due to Euler [14] and follows again from the multiplicative properties of Hamilton's quaternions. Degen in 1822 [14] is said to have found an identity for the case $n = 8$.

Hurwitz' theorem states that these are the only values of n for which such an identity exists. The solution to this problem tells us which algebras can admit a multiplicative norm such as in the complex numbers.

We begin with a few definitions.

Definition 1.2

*An **algebra** is a vector space A defined over a field $\mathbb{K}$ together with a bilinear map $A \times A \to A$, called multiplication, together with a unique $1 \in A$, called one, such that for all $\lambda \in \mathbb{K}$ and $a, b, c \in A$*

1. $1 \cdot a = a \cdot 1 = a$*, for all* $a \in A$;
2. $\lambda(a \cdot b) = (\lambda a) \cdot b = a \cdot (\lambda b)$;
3. $a \cdot (b + c) = a \cdot b + a \cdot c$ *and* $(a + b) \cdot c = a \cdot c + b \cdot c$.

If the bilinear map is associative $a \cdot (b \cdot c) = (a \cdot b) \cdot c$, then A will be called an **associative algebra** and we can omit any bracketing. Also, since no ambiguity will occur, we write ab for $a \cdot b$. A vector space is really an abelian group with a field of scalars and an algebra satisfies the ring axioms with a field of scalars.

Definition 1.3

*A **division algebra** is an algebra A such that for every nonzero $a \in A$, there exists $a^{-1} \in A$ with $aa^{-1} = a^{-1}a = 1$.*

Since every nonzero element of $\mathbb{R}, \mathbb{C}, \mathbb{H}$ and $\mathbb{O}$ is invertible, they are clearly division algebras over $\mathbb{R}$ of dimension one, two, four and eight respectively. It should be noted here that although the quaternions and octonions can be considered as complex vector spaces, they are not algebras over the complex numbers. In an algebra A over a field $\mathbb{K}$ we must have that $(\lambda a)(\mu b) = \lambda\mu(ab)$ for $a, b \in A$ and $\lambda, \mu \in \mathbb{K}$. However, if we take $A = \mathbb{H}$, $\mathbb{K} = \mathbb{C}$,$a = j, b = j$ and $\mu = i$, then

$$j(ij) = jk = i$$

but

$$i(j^2) = -i.$$

From [12] we get the following result.

Theorem 1.4

If $\mathbb{K}$ is algebraically closed, then the only finite dimensional division algebra over $\mathbb{K}$ is $\mathbb{K}$.

Proof. Let A be a finite dimensional division algebra over the algebraically closed field $\mathbb{K}$ and choose $a \in A$. The minimal polynomial p of a is linear as $\mathbb{K}$ is algebraically closed and p is irreducible. We therefore have that $\mathbb{K}(a) = \mathbb{K}$ so $a \in \mathbb{K}$. Since this holds for all $a \in A$, we get $A = \mathbb{K}$. □

Definition 1.5

A ***normed vector space*** *is a vector space V over a field $\mathbb{K}$ with a positive-definite quadratic form $N : V \to \mathbb{K}$.*

Definition 1.6

A ***composition algebra*** *is a division algebra A which is also a normed vector space such that for all $a, b \in A$*

$$N(ab) = N(a)N(b).$$

Each of our algebras under consideration is a composition algebra which is due to the 1,2,4 and 8-squares identities.

We can define a symmetric bilinear form $\langle\ ,\ \rangle : A \times A \to \mathbb{K}$ on our composition algebra A using the identity

$$\langle a, b\rangle = \frac{1}{2}(N(a+b) - N(a) - N(b)).$$

Example 1.7

Let $a, b \in \mathbb{H}$. Then if $a = x_\infty + x_1 i + x_2 j + x_3 k$ and $b = y_\infty + y_1 i + y_2 j + y_3 k$, we get

$$\langle a, b\rangle = \frac{1}{2}(N(a+b) - N(a) - N(b))$$

$$= \frac{1}{2}((x_\infty + y_\infty)^2 + (x_1 + y_1)^2 + (x_2 + y_2)^2 + (x_3 + y_3)^2 - (x_\infty^2 + x_1^2 + x_2^2 + x_3^2) - (y_\infty^2 + y_1^2 + y_2^2 + y_3^2))$$

$$= x_\infty y_\infty + x_1 y_1 + x_2 y_2 + x_3 y_3.$$

So our inner-product thus defined is equivalent to the standard dot product in $\mathbb{R}^n$. The definition is identical in $\mathbb{C}$ and $\mathbb{O}$.

We will explore some of the properties of these algebras so from now on we assume A is a finite dimensional composition algebra over $\mathbb{R}$ and $a, b, c, d \in A$. The following results can be found in [1] and [5].

Lemma 1.8 (The Scaling Law)

$$\langle ab, ac \rangle = N(a)\langle b, c \rangle.$$

Proof. We have $N(ab) = N(a)N(b)$ so replacing b by $b + c$, yields

$$N(a(b + c)) = N(a)N(b + c)$$

$$N(ab + ac) = N(a)N(b + c)$$

$$2\langle ab, ac \rangle + N(ab) + N(ac) = N(a)(2\langle b, c \rangle + N(b) + N(c))$$

and we can cancel to get the result. □

Similarly, we have that $\langle ab, cb \rangle = \langle a, c \rangle N(b)$.

Lemma 1.9 (The Exchange Law)

$$\langle ab, dc \rangle + \langle ac, db \rangle = 2\langle a, d \rangle \langle b, c \rangle.$$

Proof. In the scaling law replace a with $a + d$ then we have

$$\langle (a + d)b, (a + d)c \rangle = N(a + d)\langle b, c \rangle$$

and

$$\langle ab, ac\rangle + \langle ab, dc\rangle + \langle db, ac\rangle + \langle db, dc\rangle$$

$$= (N(a) + 2\langle a, d\rangle + N(d))\langle b, c\rangle$$

which gives

$$\langle ab, dc\rangle + \langle db, ac\rangle = 2\langle a, d\rangle\langle b, c\rangle.$$

□

We now introduce a map $* : A \longrightarrow A$ given by

$$a^* = 2\langle a, 1\rangle - a,$$

which is the negative of the reflection in the hyperplane orthogonal to 1 and is called the conjugate of a in A. Hence, we denote the mapping by $a^* = \overline{a}$. It is worth noting that 1 here represents the vector whose real part equals 1 and with imaginary part 0.

We now examine a few properties of this mapping.

Lemma 1.10 (The Braid Law)

$$\langle ab, c\rangle = \langle b, \overline{a}c\rangle.$$

Proof. Take $d = 1$ in the exchange law, then

$$\langle ab, c\rangle = 2\langle a, 1\rangle\langle b, c\rangle - \langle b, ac\rangle$$

$$= \langle ab, c\rangle + \langle ac, b\rangle - \langle b, ac\rangle$$

$$= \langle b, (2\langle a, 1\rangle - a)c\rangle = \langle b, \overline{a}c\rangle.$$

□

Lemma 1.11 (Biconjugation)

$$\overline{\overline{a}} = a.$$

Proof. Let $b = 1$ in the braid law and

$$\langle a, c\rangle = \langle a.1, c\rangle = \langle 1, \overline{a}c\rangle = \langle \overline{\overline{a}}1, c\rangle = \langle \overline{\overline{a}}, c\rangle$$

which holds for all c and hence $a = \overline{\overline{a}}$. □

Lemma 1.12 (Product Conjugation)

$$\overline{ab} = \overline{b}\overline{a}.$$

Proof. By repeatedly applying biconjugation and the braid law we get

$$\langle \overline{ab}, c\rangle = \langle \overline{c}\overline{ab}, 1\rangle = \langle \overline{c}, ab\rangle = \langle \overline{a}\,\overline{c}, b\rangle = \langle \overline{a}, bc\rangle = \langle \overline{b}\overline{a}, c\rangle,$$

which again holds for all c. □

Lemma 1.13

For all $a, b \in A$, we have,

$$\overline{a}(ab) = N(a)b$$

and

$$(ab)\overline{b} = N(b)a.$$

Proof. Let c be an arbitrary element of A and consider

$$\langle \overline{a}(ab), c\rangle = \langle (2\langle a, 1\rangle - a)(ab), c\rangle = 2\langle a, 1\rangle\langle ab, c\rangle - \langle a(ab), c\rangle$$

$$= \langle a(ab), c\rangle + \langle ab, ac\rangle - \langle a(ab), c\rangle = \langle ab, ac\rangle = N(a)\langle b, c\rangle = \langle N(a)b, c\rangle.$$

Again, as this holds for all c in A and we have non-degeneracy, the result follows. The second statement is similar. □

Lemma 1.14 (The Moufang Identities)

If A is a composition algebra with conjugation, then for all $a, b, c \in A$ we have,

1. $(ab)(ca) = a((bc)a)$;
2. $a(b(ac)) = (a(ba))c$;
3. $b(a(ca)) = ((ba)c)a$.

It is known that any one of the above identities implies the other two.

Proof. Take $d \in A$ then

$$\langle (ab)(ca), d\rangle = \langle ca, (\overline{ab})d\rangle = \langle ca, (\overline{b}\overline{a})d\rangle = 2\langle c, \overline{b}\overline{a}\rangle\langle a, d\rangle - \langle cd, (\overline{b}\overline{a})a\rangle$$

$$= 2\langle bc, \overline{a}\rangle\langle a, d\rangle - N(a)\langle cd, \overline{b}\rangle$$

and

$$\langle a((bc)a), d\rangle = \langle (bc)a, \overline{a}d\rangle = 2\langle bc, \overline{a}\rangle\langle a, d\rangle - \langle (bc)d, \overline{a}a\rangle = 2\langle bc, \overline{a}\rangle\langle a, d\rangle - N(a)\langle bc, \overline{d}\rangle$$

$$= 2\langle bc, \overline{a}\rangle\langle a, d\rangle - N(a)\langle cd, \overline{b}\rangle.$$

□

Now taking $b = 1$ or $c = 1$ in the Moufang identities, we get the following

1. $(ab)a = a(ba)$

2. $a(ac) = a^2c$

3. $ba^2 = (ba)a$.

The above are known as the **alternative laws**.

Definition 1.15

*If an algebra satisfies the alternative laws, we call it **alternative**.*

Hence we have shown that

Theorem 1.16

If A is a composition algebra, then A is alternative.

In an alternative algebra any 2-generated subalgebra is clearly associative. This result is known as Artin's Theorem.

Theorem 1.17

Let A be an algebra equipped with conjugation, i.e. a linear map $* : A \longrightarrow A$ such that $a^{**} = a$ and $(ab)^* = b^*a^*$. Then A is a composition algebra if, and only if, A is alternative and $a.a^* = N(a)$ where N is a positive-definite quadratic form.

Proof. We have already shown one direction. So let A be an alternative algebra with conjugation $*$ and $a.a^* = N(a)$ as above. Then as a, a^*, b, b^* all belong to the associative subalgebra generated by a and b, we get

$$N(ab) = (ab)(ab)^* = (ab)(b^*a^*) = a((bb^*)a^*) = aa^*N(b) = N(a)N(b)$$

and A is a composition algebra. □

We now introduce the Cayley-Dixon construction which is used to get the complex numbers from the reals. Given an algebra A which has a conjugation $*$, define a new algebra C, called the **Cayley-Dixon double** of A, which is made of pairs (a_1, a_2) with $a_1, a_2 \in A$. We think of C as taking another copy of A and attaching an square root of -1, i say, which is orthogonal to all of A. It should be noted that we can take either

$$C = A + Ai$$

or

$$C = A + iA.$$

In the first case the multiplication would be given by

$$(a_1, a_2)(b_1, b_2) = (a_1b_1 - b_2^*a_2, b_2a_1 + a_2b_1^*),$$

however in the second case we have multiplication given by

$$(a_1, a_2)(b_1, b_2) = (a_1b_1 - b_2a_2^*, a_1^*b_2 + b_1a_2).$$

We will choose to use the first case as it is consistent with our earlier definitions of $\mathbb{H}$ and $\mathbb{O}$ although both are equally valid. The conjugate of an element of C is given by,

$$(a_1, a_2)^* = (a_1^*, -a_2).$$

Lemma 1.18

The Cayley-Dixon double of A, C say, is an algebra with a conjugation $*$ such that $c^{**} = c$ and $(c_1c_2)^* = c_2^*c_1^*$ for all a, b in C.

Proof. It is immediate that $c^{**} = c$ for all $c \in C$. For the second part let $a_i, b_i \in A$

$i = 1, 2$ and $c_1 = (a_1, a_2)$ and $c_2 = (b_1, b_2)$ be in C. Then

$$(c_1c_2)^* = (a_1b_1 - b_2^*a_2, b_2a_1 + a_2b_1^*)^* = ((a_1b_1 - b_2^*a_2)^*, -(b_2a_1 + a_2b_1^*))$$

$$= (b_1^*a_1^* - a_2^*b_2, -b_2a_1 - a_2b_1^*),$$

whilst

$$c_2^*c_1^* = (b_1^*, -b_2)(a_1^*, -a_2) = (b_1^*a_1^* - a_2^*b_2, -a_2b_1^* - b_2a_1).$$

□

Lemma 1.19

If A is a composition algebra such that for all non-zero $a \in A$ we have $a + a^* \in \mathbb{R}$ and $aa^* = a^*a > 0$, then every non-zero element of C has these properties.

Proof. Let $a, b \in A$ with $0 \neq (a, b) \in C$ then

$$(a, b) + (a, b)^* = (a, b) + (a^*, -b) = (a + a^*, 0) \in \mathbb{R}$$

and

$$(a, b)(a, b)^* = (a, b)(a^*, -b) = (aa^* + bb^*, 0) > 0.$$

□

Definition 1.20

An algebra A will be called ***real*** *if $a^* = a$, for all $a \in A$.*

Lemma 1.21

If A is an algebra with a conjugation, then C is never real.

Proof. Let A be an algebra with a conjugation and C its Cayley-Dixon double. Let $(a,b) \in C$ with $0 \neq b$ in A. Then we have $(a,b)^* = (a^*, -b) = (a, -b)$. So $(a,b)^* = (a,b)$ if, and only if, $b = -b$ which in turn implies $b = 0$. □

Lemma 1.22

A is real and commutative if, and only if, C is commutative and associative.

Proof. Suppose A is real and commutative and let $(a,b),(c,d)$ be in C. As A is real we have

$$(a,b)(c,d) = (ac - d^*b, da + bc^*) = (ac - db, da + bc).$$

Also

$$(c,d)(a,b) = (ca - b^*d, ad + cb^*) = (ca - bd, ad + cb).$$

These are clearly equal since A is commutative. Associativity follows similarly. Now suppose C is commutative and associative, then we have that

$$(a,b)(c,d) = (ac - d^*b, da + bc^*) = (ca - b^*d, ad + cb^*) = (c,d)(a,b);$$

$$((a,b)(c,d))(e,f) = ((ac)e - (d^*b)e - f^*(da) - f^*(bc^*), f(ac) - f(d^*b) + (da)e^* + (bc^*)e^*)$$

which is equal to

$$(a,b)((c,d)(e,f)) = (a(ce) - a(f^*d) - (c^*f^*)b - (ed^*)b, (fc)a + (de^*)a + b(e^*c^*) - b(d^*f)).$$

We see that these hold if A is both real and commutative. □

Lemma 1.23

A is commutative if, and only if, C is associative.

Proof. The proof of this is almost identical to the proof of Lemma 1.22. □

Lemma 1.24

A is associative if, and only if, C is alternative.

Proof. This is again similar to the proof of Lemma 1.22 □

So we have seen that starting with an associative and commutative composition algebra A with trivial conjugation one can apply the Cayley-Dixon doubling process at most three times to obtain new composition algebras. Before proving that the composition algebras we introduced at the beginning of this chapter are the only real division algebras, we need a result of Frobenius from [12]

Theorem 1.25 (Frobenius' Theorem)

The only finite-dimensional real associative division algebras are $\mathbb{R}$, $\mathbb{C}$ and $\mathbb{H}$.

Proof. Let A be a finite-dimensional real division algebra and let A' be the subset $\{u \in A \,|\, u^2 \in \mathbb{R}, u^2 \leqslant 0\}$. We want to show that A' is in fact a subspace. To this end choose $u \in A'$ and $\lambda \in \mathbb{R}$, then we have $\lambda u \in A'$ and A' is closed under scalar multiplication. Next choose two linearly independent $u, v \in A'$, we wish to show that $u + v$ is also in A'. Observe that it is impossible to have an expression of the form

$$u = av + b$$

for $a, b \in \mathbb{R}$ because if we let $u^2 = c \leqslant 0$ and $v^2 = d \leqslant 0$, then we have

$$c = (av + b)^2 = a^2 d + 2avb + b^2.$$

Since v does not lie in $\mathbb{R}$ but c and d do, we get that $avb = 0$ and so $ab = 0$ which implies that either $a = 0$ or $b = 0$. If $a = 0$ we get that $u = b \in \mathbb{R}$ contradicting the fact that $u^2 \leqslant 0$. Assuming $b = 0$ yields $u = av$, which contradicts our assumption. Hence the elements $1, u, v$ are linearly independent.

We now consider the vectors $u + v$ and $u - v$. They are both roots of quadratic equations and so we can write

$$(u + v)^2 = p(u + v) + q \qquad (u - v)^2 = r(u - v) + s.$$

We also have that

$$(u \pm v)^2 = u^2 \pm (uv + vu) + v^2.$$

Substituting the values $u^2 = c$ and $v^2 = d$, we get

$$c + d + (uv + vu) = p(u + v) + q \qquad c + d - (uv + vu) = r(u - v) + s.$$

Adding these expressions

$$(p + r)u + (p - r)v + (q + s - 2c - 2d) = 0.$$

We have seen that $1, u, v$ are linearly independent, which means that all the coefficients must be zero and we can conclude that $p = r = 0$. So $(u+v)^2 = q \in \mathbb{R}$ and as $u + v \notin \mathbb{R}$ we must have $q < 0$. Therefore $u + v \in A'$ and A' is a subspace of A. We have already seen that any element of A is of the form $a + y$ for $a \in \mathbb{R}$ and $y \in A'$ and so

$$A = \mathbb{R} \oplus A'.$$

Choose $u \in A'$ and let

$$Q(u) = -u^2$$

with $Q(u) \in \mathbb{R}$ and $Q(u) \geqslant 0$. We have that $Q(u) = 0 \Leftrightarrow u = 0$. If $a \in \mathbb{R}$, then

$Q(au) = a^2Q(u)$ and we can define

$$2B(u,v) = Q(u+v) - Q(u) - Q(v) = -(u+v)^2 + u^2 + v^2 = -(uv+vu).$$

So $B(u,v)$ is a symmetric bilinear form on A and $Q(u)$ is the positive-definite quadratic form associated to it.

Now we look at the possibilities for A. If $A = \mathbb{R}$, then we get the first division algebra we considered. Suppose then that $\mathbb{R} \subsetneq A$, then we get $A' \neq 0$ and can choose $i \in A$ with $Q(i) = 1$. From this it follows that $i^2 = -1$ and $\mathbb{R}(i) = \mathbb{C}$. Suppose further that $\mathbb{C} \subsetneq A$ then $\mathbb{R}i \subsetneq A'$ and we can choose a j which is perpendicular to $\mathbb{R}i$ and such that $Q(j) = 1$. It follows that $j^2 = -1$ and $\frac{1}{2}(ij + ji) = -B(i,j) = 0$ so $ij = -ji$. Let $k = ij$ then $k^2 = -1$, and $ik + ki = 0 = kj + jk$ so $k \in A'$. Moreover, k is perpendicular to both i and j. We get that $1, i, j, k$ are linearly independent so we have

$$A = \supseteq R + \mathbb{R}i + \mathbb{R}j + \mathbb{R}k = \mathbb{H}$$

Suppose finally that $A \neq \mathbb{H}$, then there exists an $l \in A'$ with $Q(l) = 1$ which is perpendicular to i, j and k. We then have

$$li = -il \quad lj = -jl \quad lk = -kl \quad k = ij$$

from which it follows that

$$l(ij) = (li)j = -(il)j = -i(lj) = i(jl) = (ij)l$$

and so

$$lk = kl$$

which contradicts the fact that

$$lk = -kl$$

and we are done. □

We are now in position to state and prove Hurwitz' Theorem.

Theorem 1.26 (Hurwitz 1898)

The only finite-dimensional real composition algebras are $\mathbb{R}$, $\mathbb{C}$, $\mathbb{H}$ *and* $\mathbb{O}$.

Proof. Every finite-dimensional composition algebra is a (not necessarily associative) division algebra and since by Frobenius' theorem the only associative division algebras over $\mathbb{R}$ are $\mathbb{R}, \mathbb{C}$ and $\mathbb{H}$ by our previous lemmas we can obtain the octonions $\mathbb{O}$ by doubling $\mathbb{H}$. The octonions are non-associative and so their Cayley-Dixon double is not a composition algebra. □

So we have met the four real composition algebras and seen that they are the only four. In this project we will examine the substructures of them and their number theory as well as see how they are being used to describe rotations in higher dimensions by physicists.

Chapter 2

The Finite Multiplicative Substructures of the Division Algebras

In the real, complex and quaternion cases the multiplication is associative and so the set of invertible elements form a group. So in these cases we look for the finite subgroups. The Octonions are not associative but they do satisfy the Moufang identities and so the invertible elements of $\mathbb{O}$ form a Moufang Loop and we seek the finite subloops.

2.1 Finite Subgroups of the Complex Numbers

The finite subgroups of $\mathbb{R}$ are contained in the set of elements $\{x \in \mathbb{R} \mid x^n = 1, \text{ some } n \in \mathbb{N}\}$. It is obvious that the only elements with this property are ± 1. Thus the finite subgroups of $\mathbb{R}$ are $\{1\}$ and $\{\pm 1\}$.

Any complex number $z = \lambda + \mu i$ defines a unique point (λ, μ) in $\mathbb{R}^2$ and any point in $\mathbb{R}^2$ defines a unique complex number z. The complex number $z = \lambda + \mu i$

can be written in the form

$$re^{i\theta}$$

where $r = \sqrt{N(z)}$ and $\tan\theta = \frac{\mu}{\lambda}$. The set $\{z \in \mathbb{C} \mid N(z) = \lambda^2 + \mu^2 = 1\}$ defines a unit circle in $\mathbb{R}^2$ which is denoted S^1. Let z_1 lie on the unit circle, then $z = e^{i\theta}$ for some $0 \leqslant \theta < 2\pi$. If $z_2 = re^{i\alpha}$ is any other complex number, then

$$z_1 z_2 = e^{i\theta}(re^{i\alpha}) = re^{i(\theta+\alpha)}.$$

So we see that multiplication by z_1 rotates z_2 through an angle of θ. This rotation is in the anti-clockwise direction as $i^2 = -1$. We have the identity $re^{i\theta} = r(\cos\theta + i\sin\theta)$ and since any element of a finite subgroup of $\mathbb{C}$ must have $r = 1$ we get a map

$$\phi(e^{i\theta}) = \begin{bmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{bmatrix}.$$

This is clearly an isomorphism into $SO(2)$ the rotation group in 2-dimensions. Then by [11] the finite subgroups of $SO(2)$ are just the cyclic groups of finite order.

2.2 Finite Subgroups of the Quaternions

Just as the unit complex numbers give a complete description of rotations in 2-dimensions, so the unit quaternions can be used to describe rotations in 3-dimensions. The set of isometries that preserve orientations in 3-dimensions is denoted $SO(3)$. In this section we aim to associate the subset of pure quaternions, those with no real part, with $\mathbb{R}^3$ and show that the unit quaternions act on this subset via rotations and that every rotation of $\mathbb{R}^3$ can be realised in this way.

As in the complex case the quaternions are in bijection with the space $\mathbb{R}^4$. Let $\mathbb{H}_p = \{a \in \mathbb{H} \mid Re(a) = 0\}$ be called the set of pure quaternions, which is in obvious bijection with the set $\mathbb{R}^3$. We will call $\mathbb{H}_1 = \{a \in \mathbb{H} \mid N(a) = 1\}$ the set of unit quaternions. If we equip $\mathbb{R}^3$ with the standard Euclidean metric then we get a bijection between $\mathbb{H}_1 \cap \mathbb{H}_p$ and the unit sphere S^2. The group $SO(3)$ is the set of rotations of S^2 and so we will show that the set $\mathbb{H}_1$ forms a group under multiplication and that it acts on the space $\mathbb{H}_p$ as rotations and we aim to find a surjective homomorphism between $\mathbb{H}_1$ and $SO(3)$ with kernel $\{\pm 1\}$.

For q in $\mathbb{H}_1$ define C_q to be the linear map from $\mathbb{H}$ to $\mathbb{H}$ given by

$$C_q(x) = qx\overline{q}$$

for all x in $\mathbb{H}$. It should be noted here that

$$N(C_q(x)) = qx\overline{q}\,\overline{qx\overline{q}} = qx\overline{q}q\overline{x}\,\overline{q} = N(q)qx\overline{x}\,\overline{q} = N(q)^2N(x) = N(x)$$

as $N(q) = 1$. So C_q is an isometry. If x is such that $Im(x) = 0$, then x commutes with all of $\mathbb{H}$ and so C_q will fix x. So we want to know the effect of C_q on the space $\mathbb{H}_p$

To show a quaternion x is a member of $\mathbb{H}_p$ we need only check that $\overline{x} = -x$. We have that

$$\overline{C_q(x)} = \overline{qx\overline{q}} = q\overline{x}\,\overline{q} = C_q(\overline{x})$$

for all x in $\mathbb{H}$. If x is in $\mathbb{H}_p$, then

$$\overline{C_q(x)} = C_q(\overline{x}) = C_q(-x) = -C_q(x)$$

and $C_q(x)$ is in $\mathbb{H}_p$ as C_q is linear.

We have seen in Chapter 1 that any quaternion q can be written in the form $q = r(\cos\theta + \widehat{\imath}\sin\theta)$ where $\widehat{\imath}$ is of unit length in the $q - Re(q)$ direction and $r = \sqrt{N(q)}$.

We want to show that if q is as above with $r = 1$, then C_q is a rotation about the axis $\widehat{\imath}$ through 2θ. Choose an orthonormal basis $\{\widehat{\imath}, \widehat{\jmath}, \widehat{k}\}$ for $\mathbb{H}_p$ and define an orientation on it by letting $\widehat{\imath}\,\widehat{\jmath} = \widehat{k}$ (the only choices here are $\pm\widehat{k}$ since the product must be a unit vector perpendicular to both $\widehat{\imath}$ and $\widehat{\jmath}$; Either choice is fine and corresponds to a choice of the direction of rotation). We have

$$\begin{aligned} C_q(\widehat{\imath}\,) &= (\cos\theta + \widehat{\imath}\sin\theta)\widehat{\imath}(\cos\theta - \widehat{\imath}\sin\theta) \\ &= (\widehat{\imath}\cos\theta - \sin\theta)(\cos\theta - \widehat{\imath}\sin\theta) \\ &= \widehat{\imath}\cos^2\theta + \widehat{\imath}\sin^2\theta \\ &= \widehat{\imath}, \end{aligned}$$

$$\begin{aligned} C_q(\widehat{\jmath}\,) &= (\cos\theta + \widehat{\imath}\sin\theta)\widehat{\jmath}(\cos\theta - \widehat{\imath}\sin\theta) \\ &= (\widehat{\jmath}\cos\theta + \widehat{k}\sin\theta)(\cos\theta - \widehat{\imath}\sin\theta) \\ &= \widehat{\jmath}\cos 2\theta + \widehat{k}\sin 2\theta, \end{aligned}$$

$$\begin{aligned} C_q(\widehat{k}\,) &= (\cos\theta + \widehat{\imath}\sin\theta)\widehat{k}(\cos\theta - \widehat{\imath}\sin\theta) \\ &= (\widehat{k}\cos\theta - \widehat{\jmath}\sin\theta)(\cos\theta - \widehat{\imath}\sin\theta) \\ &= \widehat{k}\cos 2\theta - \widehat{\jmath}\sin 2\theta, \end{aligned}$$

and it is clear that C_q rotates about the axis $\widehat{\imath}$ through an angle of 2θ.

We now want to show that any rotation of $\mathbb{R}^3$ can be realised as the conjugate of a pure quaternion by a unital one. Any rotation in 3-dimensions is defined by its axis of rotation, $\widehat{\imath}$ say, and its angle of rotation θ. By our previous work and choosing $q = \cos\frac{\theta}{2} + \widehat{\imath}\sin\frac{\theta}{2}$, we get the rotation we desire.

We have seen that there is a mapping φ from $\mathbb{H}_1$ to $SO(3)$ given by

$$q \mapsto C_q.$$

Since

$$(C_p \circ C_q)(x) = C_p(qx\overline{q}) = pqx\overline{q}\,\overline{p} = pqx\overline{pq} = C_{pq}(x)$$

for all x in $\mathbb{H}_p$, the map φ is a homomorphism. As any rotation can be described in this manner, φ is surjective and we want to find $ker(\varphi)$. As C_q is linear, it is not difficult to see that q and $-q$ define the same rotation and so $ker(\varphi)$ contains $\{\pm 1\}$. If q is in $\mathbb{H}_p \smallsetminus \{\pm 1\}$, then C_q is nontrivial and so we have that $ker(\varphi) = \{\pm\}$. To summarise

$$\mathbb{H}_1^\times / \{\pm 1\} \cong SO(3).$$

The finite subgroups of $SO(3)$ are discussed in detail in [11] and are

1. the cyclic groups C_n of finite order;

2. the dihedral groups D_{2n};

3. the tetrahedral group T, isomorphic to A_4;

4. the octahedral group O, isomorphic to S_4;

5. the icosahedral group I, isomorphic to A_5.

So the finite subgroups of $\mathbb{H}^\times$ are those in the above list along with their double covers which we will denote $2C_n$, $2D_{2n}$, $2T$, $2O$, and $2I$, respectively.

We note in passing that there is an isomorphism between the groups $\mathbb{H}_1$ and $SU(2)$, the group of 2×2 unitary matrices of determinant 1, given by

$$\psi : a_\infty + a_1 i + a_2 j + a_3 k \mapsto \begin{bmatrix} a_\infty + a_1 i & a_2 + a_3 i \\ -a_2 + a_3 i & a_\infty - a_1 i \end{bmatrix}.$$

It can easily be checked that ψ is an isomorphism and that $det(\psi(a)) = N(a)$. Hence by using the quaternions we immediately see that

$$SU(2)/\{\pm 1\} \cong SO(3).$$

2.3 Curtis' Construction of the Finite Subloops of the Octonions

The octonions are non-associative and hence $\mathbb{O}^\times$ does not form a group. However, we have seen that they satisfy weaker conditions namely the Moufang identities with three octonions and the alternative laws for two of them. The octonions form a Moufang Loop, named after Ruth Moufang, and in this case we seek a complete list of the finite subloops. We follow Curtis' construction which was first discovered in 1970 but went unpublished for over thirty years. A similar construction was given by Chein in 1978 but his was less general. The construction now carries his name. In this section we closely follow the exposition given in [8].

We have already seen the Moufang identities in Chapter 1 and know that our division algebras satisfy them. Here we give a definition of a structure that satisfies these properties and then show that the non-associative substructures of the octonions are of this type.

Definition 2.1

A Moufang loop is a closed multiplicative structure M with an identity 1_M where for all $x \in M$ the maps $L_x : a \mapsto xa$ and $R_x : a \mapsto ax$ are both bijections, for all $a \in M$, and the multiplication in M satisfies:

1. $(ab)(ca) = a((bc)a)$,

2. $a(b(ac)) = (a(ba))c$,

3. $b(a(ca)) = ((ba)c)a$,

for all $a, b, c \in M$.

It is known that any of the identities implies the other two.

Theorem 2.2

Let G be a group which contains an element a which lies in $Z(G)$ such that $a^2 = 1$; so a is an involution or the identity. Introduce a new symbol x and define $\widehat{G} = G \cup xG$, where we identify x with $x1_G$. Then if we define multiplication in $\widehat{G}$ by:

1. $(xg)h = x(hg)$;

2. $g(xh) = x(g^{-1}h)$;

3. $(xg)(xh) = ahg^{-1}$;

for all g, h in G, then $(\widehat{G}, .)$ is a Moufang loop.

This is Curtis' construction which was submitted for the Rayleigh prize in 1970. Chein's is similar but he requires that $a = 1$. In this way his result yields fewer loops than Curtis'.

Proof. For all g in G, the maps R_g and L_g are obviously bijections as G is a group. Note that $R_{xh}(hg^{-1}) = x(gh^{-1}h) = xg$ and $R_{xh}(xag^{-1}h) = ahh^{-1}ga^{-1} = g$ as $a \in Z(G)$. So R_{xh} is surjective and injectivity is obvious.

We now need to verify that $a(ba) = (ab)a$. Clearly, if a, b both lie in G, we are done. So we need only check the three other cases. We have,

$$(g.xh)g = (x.g^{-1}h)g = x(gg^{-1}h) = xh = x(g^{-1}gh) = g(xgh) = g(xh.g);$$

$$(xg.h)xg = (xhg)xg = ag(hg)^{-1} = ah^{-1} = a(h^{-1}g)g^{-1} = xg(xh^{-1}g) = xg(h.xg);$$

$$(xg.xh)xg = (ahg^{-1})xg = x(gh^{-1}ag) = x(agh^{-1}g) = xg(agh^{-1}) = xg(xh.xg).$$

Hence aba is well-defined for all a and b in $\widehat{G}$. It is now only left to check that the Moufang identities hold. Let g, h and k be elements in G. As G is a group, the case $g(h(gk)) = (g(hg))k$ is trivial and we need only consider the other seven when one or more of the elements lies in xG. Now,

$$ghg.xk = x(g^{-1}h^{-1}g^{-1}k) = g(h(g(xk)));$$

$$(g.xh.g)k = xh.k = xkh = x(g^{-1}gkh) = g(xgkh) = g(xh(gk));$$

$$(g.xh.g)xk = xh.xk = akh^{-1} = g(ag^{-1}kh^{-1}) = g(xh(xg^{-1}k)) = g(xh(g.xk));$$

$$(xg.h.xg)k = ah^{-1}k = ah^{-1}kgg^{-1} = xg.xh^{-1}kg = xg(h.xkg) = xg(h(xg.k));$$

$$(xg.h.xg)xk = ah^{-1}.xk = xahk = xg(hakg^{-1}) = xg(h(xg.xk));$$

$$(xg.xh.xg)k = xagh^{-1}g.k = xakgh^{-1}g = xg.akgh^{-1} = xg(xh.xkg) = xg(xh(xg.k));$$

and finally,

$$(xg.xh.xg)xk = xagh^{-1}g.xk = kg^{-1}hg^{-1}$$

$$= xg.xakg^{-1}h = xg(xh.akg^{-1}) = xg(xh(xg.xk)).$$

Hence the identities hold for all elements in $\widehat{G}$ and it is therefore a Moufang loop.□

Theorem 2.3

Let G be a group and let $a \in Z(G)$ such that $a^2 = 1$. Adjoin an element x to G and define $\langle G, x\rangle_M$ be the Moufang loop generated by G and x in which the multiplication of G holds and we have the relation

$$xgx = ag^{-1}$$

for all $g \in G$. Then G has index 2 in $\langle G, x\rangle_M$ and the multiplication is the same as that in $\widehat{G}$ above.

Proof. The relation gives us that $x^2 = a$, and hence $x^{-1} = ax$ and $xg = g^{-1}x$. So for all g, h in G

1. $(xg)h = xg(xah^{-1}x) = ((xgx)ah^{-1})x = (ag^{-1}ah^{-1})x = (g^{-1}h^{-1})x = xhg$;
2. $g(xh) = (xag^{-1}x)xh = x(ag^{-1}(x^2h)) = xg^{-1}h$;
3. $(xg)(xh) = xg(h^{-1}x) = x(gh^{-1})x = ahg^{-1}$.

□

Theorem 2.4

The Moufang loop $\widehat{G}$ is associative, and hence a group, if, and only if, G is abelian.

Proof. Suppose that $\widehat{G}$ is associative, then we have $x(gh) = (xg)h = x(hg)$, for all $g, h \in G$ and so G is commutative.

On the other hand if G is commutative then the map that sends each element to its inverse is an isomorphism as $(xy)^{-1} = y^{-1}x^{-1} = x^{-1}y^{-1}$. Choosing $a \in G$ with

$a^2 = 1$, we adjoin an element x such that $x^2 = a$ and $x^{-1}gx = g^{-1}$, for all g in G. Now,

$$g.xh = xx^{-1}gxh = xg^{-1}h$$

$$xg.h = xgh = xhg$$

and

$$xg.xh = ax^{-1}gxh = ag^{-1}h = ahg^{-1}.$$

This group $\langle G, x\rangle$ is actually the semi-direct product of G with $\langle x\rangle \cong C_4$ with $g^x = g^{-1}$ factored by the subgroup $\langle ax^2\rangle$. □

In his essay [7] Curtis proves that up to isomorphism the finite multiplicative subloops of $\mathbb{O}$ are precisely the Moufang loops $\widehat{G}$ when G is a finite non-abelian subgroup of $\mathbb{H}$ which contains the element $a = -1$. These are listed in the previous section. There is one exception, the infinite subloop of the Integral Octonions, which will be the subject of the next chapter.

We now give an example.

Let $Q_8 = \{\pm 1, \pm i, \pm j, \pm k\}$ be the quaternion group of order eight under the usual multiplication. If we then adjoin an element x such that $x^2 = -1$, then we get a group with elements

$$\pm 1, \pm i, \pm j, \pm k, \pm x, \pm xi, \pm xj, \pm xk$$

which is equivalent to the set

$$\pm 1, \pm i_0, \pm i_1, \pm i_3, \pm i_2, \mp i_6, \mp i_4, \pm i_5,$$

respectively. So the loop $\widehat{Q}_8$ is the subloop of basis elements of $\mathbb{O}$.

We have seen the finite substructures of our division algebras. However, as was mentioned in this chapter, there is one more but it is infinite. This Moufang loop is called the Integral Octonions and in some sense is the analogue of the Gaussian integers in $\mathbb{C}$. Our next chapter is devoted to the number theory aspect of the division algebras and we introduce and study the integral elements of both $\mathbb{H}$ and $\mathbb{O}$.

Chapter 3

Arithmetics of the Division Algebras

Since the Division Algebras carry the extra structure of a ring it makes sense to seek a 'Number Theory' inside of them. In the real case the subring is the normal rational integers and in the complex case we get the ring $\mathbb{Z}[i]$ which is the set of Gaussian Integers. In this chapter we describe the equivalent structures in both the quaternions and octonions and explain the theory of prime factorisation in each.

3.1 The Hurwitz Integers

In direct analogy to the Gaussian numbers, Lipschitz in 1886 defined the integral quaternions to be the set $L = \{a+bi+cj+dk \mid a, b, c, d \in \mathbb{Z}\}$. We will call quaternions of this form **Lipschitz** and note that if q is Lipschtiz, then it can be written in the form $q = x + yj$ where x, y are Gaussian numbers. However, the Lipschitz integers do not behave well under division. For example, let $a, b \in L$ and set

$$a/b = q_1 + q_2 i + q_3 j + q_4 k,$$

with the $q_k \in \mathbb{Q}$, then take p_k to be the nearest integer to q_k so we obtain a Lipschitz integer

$$p = p_1 + p_2 i + p_3 j + p_4 k.$$

Setting $r = a/b - p$, we get

$$a = bp + r.$$

Now it is a requirement for the division algorithm that $N(r) < N(b)$ and so we calculate

$$N(r/b) = N(a/b - p) = (q_1 - p_1)^2 + (q_2 - p_2)^2 + (q_3 - p_3)^2 + (q_4 - p_4)^2$$

$$\leqslant \left(\frac{1}{2}\right)^2 + \left(\frac{1}{2}\right)^2 + \left(\frac{1}{2}\right)^2 + \left(\frac{1}{2}\right)^2 = 1.$$

So the inequality is not strict. In fact we have equality precisely when every coefficient lies in $\mathbb{Z} + \frac{1}{2}$. To overcome this problem Hurwitz in 1896 suggested defining the integral quaternions to be quaternions $q = a + bi + cj + dk$ with a, b, c, d either all in $\mathbb{Z}$ or all in $\mathbb{Z} + \frac{1}{2}$. Quaternions of this type will be called **Hurwitz** and we will denote the set of all Hurwitz integers by H.

We now wish to study the primes and units of the Hurwitz integers in order to develop the theory of prime factorisations. We follow the work in [5] As usual, a prime Hurwitz integer P will be one whose norm $N(P)$ is a rational prime p. Since the only factorisations of p are $p \times 1$ and $1 \times p$, the only factorisations of P must be of the form

$$P = U \times P'$$

or

$$P = P' \times U$$

where $N(P') = p$ and $N(U) = 1$. Hence, the unit Hurwitz quaternions are defined to be the Hurwitz quaternions of norm 1.

Theorem 3.1

There are twenty-four Hurwitz units which are ± 1, $\pm i$, $\pm j$, $\pm k$ *and* $\pm\frac{1}{2}\pm\frac{1}{2}i\pm\frac{1}{2}j\pm\frac{1}{2}k$.

Proof. Obvious. □

The Hurwitz units in fact form a copy of the binary tetrahedral group $2T$ which we met in the last chapter. Now that we know the Hurwitz units, we can determine the factorisations of the Hurwitz primes. If P is a Hurwitz prime, then it can only have factorisations of the form

$$P = (PU^{-1})U$$

or

$$P = U(U^{-1}P)$$

where U is a Hurwitz unit. Note also that as U is a unit, U^{-1} is also a unit.

How a Hurwitz integer factorises depends on whether it is divisible by some natural number $n > 1$. We therefore make the following definition.

Definition 3.2

A Hurwitz integer q is called ***primitive*** *if it is not divisible by a natural number $n > 1$. If q is not primitive, we will call it* ***imprimitive****.*

Theorem 3.3 (Primitive Unique Factorisation Theorem)

Given any primitive Hurwitz integer Q whose norm $N(Q) = q$ where q has a prime factorisation $q = p_1 p_2 ... p_n$, then there is a factorisation of Q into Hurwitz primes

$$Q = P_1 P_2 ... P_n$$

where $N(P_k) = p_k$.

We will call the factorisation $Q = P_1P_2...P_n$ ***modelled on*** *the factorisation $p_1p_2...p_n$ of q. Moreover, if $Q = P_1P_2...P_n$ is a factorisation of Q modelled on $q = p_1p_2...p_n$, then the other factorisations modelled on it will be of the form*

$$Q = P_1U_1.U_1^{-1}P_2U_2.U_2^{-1}P_3U_3...U_{n-1}^{-1}P_n$$

where the U_k are Hurwitz units. We call the factorisations unique ***upto unit-migration***

Proof. Since we have the division by small remainder property and a multiplicative norm, the set H is a Euclidean domain and so every ideal is principal. So the ideal

$$p_1H + QH$$

is principal and so there is a $P_0 \in H$ such that

$$p_1H + QH = P_0H$$

We must have that $N(P_0)$ divides $N(p_1)$ and so $N(P_0)$ is either $1, p_1$ or p_1^2 as p_1 is prime. If $P_0 = 1$, then $p_1H + QH$ would be the whole of H. This is impossible as then every element of H would be of the form $p_1h_1 + Qh_2$ and so would have norm

$$N(p_1h_1 + Qh_2) = 2\langle p_1h_1, Qh_2\rangle + N(p_1h_1) + N(Qh_2)$$

$$= 2p_1\langle h_1, qh_2\rangle + p_1^2N(h_1) + p_1p_2...p_nN(h_2)$$

which is clearly divisible by p_1. Next if $N(P_1)$ is equal to p_1^2, then P_1 would divide p_1 and so $p_1 = P_1U$, where U is a unit. But then $p_1U^{-1} = P_1$ so p_1 divides Q but

Q is primitive. Hence $N(P_1)$ must be equal to p_1 and so we have $Q = P_1 Q_1$ with $N(Q_1) = p_2 ... p_n$. By repeatedly applying the above argument, we get $Q_k = P_{k+1} Q_{k+1}$ with $N(Q_{k+1}) = p_{k+1} ... p_n$. We end up with $Q = P_1 P_2 ... P_n Q_{n+1}$ where Q_{n+1} is a unit. □

Example 3.4

Consider a Hurwitz integer Q of norm 315. This has prime factoristion $3^2.7.5$ *so there are twelve different ways of ordering this*

3.3.5.7 3.3.7.5 3.5.3.7 3.7.3.5 3.5.7.3 3.7.5.3

5.3.3.7 7.3.3.5 5.3.7.3 7.3.5.3 5.7.3.3 7.5.3.3

There are twenty-four units in H and so we have $24^3.12 = 165,888$ *possible prime factorisations of Q.*

Let p be a prime, then a quadratic residue of p is an integer a such that $a \equiv b^2(p)$, for $b \not\equiv 0(p)$. Any other integer not congruent to a square (or zero) modulo p is called a quadratic non-residue. If we fix a non-residue n and multiply it by all the quadratic residues, we obtain all the non-residues. Let n be the smallest non-residue, then $n = a + 1$ for some quadratic residue a. Since a is a residue, we can write it as $a \equiv b^2(p)$ for some $b \not\equiv 0(p)$ and we get $n \equiv b^2 + 1^2(p)$. As all other non-residues can be obtained by multiplying n by the residues, we have shown that every non-residue n_0 can be written in the form $n_0 \equiv c^2 + d^2(p)$. Furthermore, -1 is either a residue or the sum of two residues and so $0 \equiv -1 + 1^2(p)$ is the sum of either two or three residues. In other words $0 \equiv a^2 + b^2 + c^2(p)$ for some a, b, c not all zero. We are now ready to prove our next theorem.

Theorem 3.5

Every rational prime p has at least one factorisation

$$p = P\overline{P}$$

where P is a Hurwitz integer.

Proof. For any x, we have $x^2 \equiv (p-x)^2(p)$ so we can assume that $0 \leqslant a, b, c \leqslant p/2$ as above. Hence we get $a^2 + b^2 + c^2 = mp$ for some $0 < m < p$. This defines a quaternion $Q = ai + bj + ck$ with $N(Q) = mp$. Then the ideal $pH + QH = PH$ as before and by a similar argument to the proof of the Primitive Unique Factorisation Theorem , we get $N(P) = P\overline{P} = p$. □

We have completed our analysis of the factorisations of primitive Hurwitz integers and we now look at the imprimitive case. Before we start our analysis, we will need to define the Catalan triangle and the associated polynomials. The Catalan numbers are obtained in almost the same way as Pascal's triangle but we do not read from the left.

$$\begin{array}{|lllllll}
1 \\
 & 1 \\
1 & & 1 \\
 & 2 & & 1 \\
2 & & 3 & & 1 \\
 & 5 & & 4 & & 1 \\
5 & & 9 & & 5 & & 1
\end{array}$$

We can now read off the Catalan polynomials. We have

$$
\begin{aligned}
C_0(x) = C_1(x) &= 1 \\
C_2(x) &= x + 1 \\
C_3(x) &= 2x + 1 \\
C_4(x) &= 2x^2 + 3x + 1 \\
C_5(x) &= 5x^2 + 4x + 1
\end{aligned}
$$

We now define the truncated Catalan polynomial $C_{n,m}(x)$ to be the terms in the Catalan polynomial $C_n(x)$ that have degree no greater than m. For example

$$C_{5,1} = 4x + 1.$$

Theorem 3.6

Suppose Q has norm $2^{n_0} p_1^{n_1} ... p_t^{n_t}$ and is divisble by the rational integer $2^{m_0} p_1^{m_1} ... p_t^{m_t}$ then up to unit migration, the number of factorisations of Q modelled on the factorisation of $N(Q)$ is

$$\prod_{k \geqslant 1} C_{n_k, m_k}(p_k)$$

evaluated at the odd primes $p_1, p_2, ..., p_t$.

We sketch the proof.

Proof. We will consider Hurwitz integers which factorise as

$$Q = P_1 P_2 ... P_n$$

where $N(P_k)$ is prime. Since Q may be imprimitive, suppose it is divisible by p^s but not p^{s+1} then

$$Q = p^s P.$$

Then P is a primitive Hurwitz integer and as such, by the Primitive Unique Factorisation Theorem, it can be factored up to unit migration as

$$P = R_1 R_2 ... R_{n-2s}.$$

For every prime p, it can be shown that there exist up to unit right multiplication $p+1$ Hurwitz integers of norm p. So we need to know if

$$P_1 = R_1$$

up to unit right multiplication. So there are $p$cases where it does and only one where it does not. If it does, then we get a Hurwitz integer of norm p^{n-1} which is divisible by p^s but not p^{s+1} and so inductively has $C_{n-1,s}(p)$ solutions. In the other p cases we get Hurwitz integers of norm p^{n-1} that are divisible by p^{s-1} but not p^s and so we get $C_{n-1,s-1}(p)$ solutions for each. Recursively we get

$$C_{n,s}(p) = C_{n-1,s}(p) + pC_{n-1,s-1}(p)$$

and this defines the Catalan numbers. □

3.2 The Integral Octonions

Dickson [9] first gave a definition of what it means for a set in an algebra to be a set of 'integral' elements. In this chapter we again follow closely the work in [5].

Definition 3.7 *A set of elements from an algebra is called an* ***order*** *if*

1. *Each element of the order is the solution to an equation with integer coefficients,*
2. *The set is closed under subtraction and multiplication and*
3. *1 is in the set.*

If, further, the order is maximal we call it an ***arithmetic****.*

So it is the aim of this section to define the arithmetics and hence the set of integral elements. Any octonion $a = a_\infty + a_0 i_0 + a_1 i_1 + a_2 i_2 + a_3 i_3 + a_4 i_4 + a_5 i_5 + a_6 i_6$ satisfies the equation

$$x^2 - 2a_\infty x - N(x) = 0$$

which Coxeter [6] calls the rank equation. In fact any quaternion or complex number would also satisfy the equation with a_∞ replaced by the real part. We are now ready to start building the Integral Octonions. We begin with the integer span of the basis elements which Conway [5] calls the Gravesian Integers and we label G. There are, however, other orders which contain G. Just as with the Hurwitz integers we will have cause to take the halves of certain coordinates of the octonions. To this end we define the set of elements in an integral octonion whose coordinates are halves of odd integers to be a **halving-set**. So for example the octonion

$$b = \frac{1}{2} + 3i_0 + 5i_1 + \frac{7}{2}i_2 + 9i_3 + \frac{9}{2}i_4 + 6i_5 + \frac{1}{2}i_6$$

is said to have halving-set $\infty, 2, 4, 6$. We shall call the arithmetic of the octonions the **integral octonions**.

Lemma 3.8

For an element in the integral octonions the double of every coordinate is an integer and the size of a halving-set is either $0, 4$ *or* 8.

Proof. In the first case we can multiply any integral octonion by i_k for any k and so make any coordinate the real part. Since the integral octonions must be closed and since $2Re(a)$ must be an integer in the rank equation, we are done. For the second part note that $N(a)$ must be an integer in the rank equation and so the number of 'halves' can be either $0, 4$ or 8. □

We will write i_{abcd} for the integral octonion whose halving set is $\frac{1}{2}(i_a + i_b + i_c + i_d$. In this way we can denote the different orders inside the octonions by their halving-sets. The Gravesian integers are those which are all integers and so the halving-set is $\emptyset$. If we then define the Kleinian integers to be the Gravesians along with those elements all of whose coordinates are halves of odd integers, then they have halving-sets $\emptyset$ and $\Omega = \infty, 0, 1, 2, 3, 4, 5, 6$.

Kirmse was the first to expand on this idea and took the halving-sets to be the associative triples of the quaternion subalgebras along with ∞, representing the real part, and their complements. These Conway has called the ∞-integers [5].

$\infty013$	2456
$\infty124$	3560
$\infty235$	4601
$\infty346$	5012
$\infty450$	6123
$\infty561$	0234
$\infty602$	1345
$\emptyset$	Ω

Unfortunately, the ∞-integers are not closed under multiplication as we have

$$i_{\infty026} i_{\infty013} = \frac{1}{2}(i_\infty + i_0 + i_2 + i_6)\frac{1}{2}(i_\infty + i_0 + i_1 + i_3) = \frac{1}{2}(i_0 + i_2 + i_3 + i_5) = i_{0235}$$

which is not in the list of ∞-integers. We learn in [6],([15],pg.130) that Kirmse claimed there were eight maximal orders in the octonions and then described the only one which does not work. Dickson then found three based on Kirmse's work before Coxeter, with the help of Bruck, then went on to construct all seven and show that they are maximal. The solution involves making a swap with ∞ and any n. Failure to make this swap has become known as **Kirmse's mistake.** We list all the sets below but note that only the n-integers for $n \in \{0, 1, 2, 3, 4, 5, 6\}$ are actually valid.

$\infty - integers$	
$\infty013$	2456
$\infty124$	3560
$\infty235$	4601
$\infty346$	5012
$\infty450$	6123
$\infty561$	0234
$\infty602$	1345
$\emptyset$	Ω

$0 - integers$	
$\infty013$	2456
0124	$\infty356$
0235	$\infty461$
0346	$\infty512$
$\infty450$	6123
0561	$\infty234$
$\infty602$	1345
$\emptyset$	Ω

$1 - integers$	
$\infty013$	2456
$\infty124$	3560
2351	$\infty460$
3461	$\infty502$
4501	$\infty623$
$\infty561$	0234
6021	$\infty345$
$\emptyset$	Ω

$2 - integers$	
0132	$\infty456$
$\infty124$	3560
$\infty235$	4601
3462	$\infty501$
4502	$\infty613$
5612	$\infty034$
$\infty602$	1345
$\emptyset$	Ω

$3 - integers$	
$\infty013$	2456
1243	$\infty560$
$\infty235$	4601
$\infty346$	5012
4503	$\infty612$
5613	$\infty024$
6023	$\infty145$
$\emptyset$	Ω

$4 - integers$	
0134	$\infty256$
$\infty124$	3560
2354	$\infty601$
$\infty346$	5012
$\infty450$	6123
5614	$\infty023$
6024	$\infty135$
$\emptyset$	Ω

$5 - integers$	
0135	$\infty246$
1245	$\infty360$
$\infty235$	4601
3465	$\infty012$
$\infty450$	6123
$\infty561$	0234
6025	$\infty134$
$\emptyset$	Ω

$6 - integers$	
0136	$\infty245$
1246	$\infty350$
2356	$\infty401$
$\infty346$	5012
4506	$\infty123$
$\infty561$	0234
$\infty602$	1345
$\emptyset$	Ω

One can also obtain the n-integers for $n \in \{0, 1, 2, 3, 4, 5, 6\}$ to obtain an equally valid set of integral elements. It is readily seen that each set is isomorphic to any other so we will only consider the 0-integers.

Theorem 3.9

The 0*-integers are multiplicatively closed.*

Proof. The halving-sets for the 0-integers are

$$\infty013 \quad 2456 \quad 0124 \quad \infty356 \quad 0235 \quad \infty461 \quad 0346 \quad \varnothing$$

$$\infty512 \quad \infty450 \quad 6123 \quad 0561 \quad \infty234 \quad \infty602 \quad 1345 \quad \Omega$$

which is spanned by $i_{\infty356}, i_{0235}, i_{0463}$ and i_{0156} over G. Since multiplying any two of these 0-integers leads to another, up to sign, we see that the set is closed. □

We have now identified eight of the orders inside $\mathbb{O}$. We have the seven n-integers as well as the Gravesian integers whose halving-set is $\emptyset$. If we take the intersection of any two n-integers, say the 1-integers and the 5-integers, we get the set

$$\begin{array}{cc} \infty561 & 4023 \\ \emptyset & \Omega \end{array}$$

which can be obtained from a copy of the Hurwitz integers inside $\mathbb{O}$ via the Cayley-Dixon doubling process. For this reason we call these the Double Hurwitz integers. There are seven such sets. Finally, the intersection of all the n-integers yields an order with halving-set Ω and $\emptyset$. These are the Kleinian integers since they are numbers of the form

$$a = \frac{1}{2}(1 + i_0 + i_1 + i_2 + i_3 + i_4 + i_5 + i_6).$$

These now account for all the orders in $\mathbb{O}$ and it is our aim to prove this result.

Definition 3.10

A halving-set will be called ***inner*** *if the corresponding octonions are ∞-integers, and* ***outer*** *otherwise.*

Lemma 3.11

The Gravesian integers and any octonion whose halving-set is an outer n-set generate all the n-integers.

Proof. Suppose, without loss of generality, that a is a 0-integer whose halving-set is one of the outer ones. We can subtract elements of the Gravesian integers to bring a into the form

$$\frac{1}{2}(i_a + i_b + i_c + i_d).$$

Then it can be seen ([5],pg.104) that multiplication by the sums of three Gravesian units (those of the form i_k) gives all outer 0-sets. Since any inner set is just the sum of two outer sets, we are done. □

Lemma 3.12

Along with the Gravesian integers

1. *any two octonions with complementary 4-element halving-sets generate each other and*
2. *two octonions with distinct non-complementary inner sets as halving-sets generate the n-integers, for some n.*

Proof. If we multiply $\frac{1}{2}(1+i_1+i_2+i_4)$ by i_0 on the left, we obtain $\frac{1}{2}(i_0+i_3+i_5+i_6)$. Since this can be done for any complementary set by a unit Gravesian integer, we are done. For the second note that by the first part we can assume that both sets contain ∞ so by looking at the tables above one can see that they are obtained from each other by increasing other subscripts by $1, 2$ or 4 (mod 7). Again, we can just assume it is one since there is the subscript doubling isomorphism (1 2 4)(3 6 5) which we will meet in the next chapter. Let the two halving sets be $\infty602$ and $\infty013$ then their product is $\frac{1}{2}(i_0 + i_2 + i_3 + i_5)$ as we saw before. But 0235 is an outer 0-set. Then by Lemma 3.11 we are done. □

Theorem 3.13

The sixteen orders of $\mathbb{O}$ we have described are the only ones containing the Gravesian integers.

Proof. Choose an order containing G then if it is not G or the Kleinian integers, it must contain one of the halving-sets and therefore the complementary one as it must be closed under addition with K. If these are the only halving-sets, we have a set of Double-Hurwitz integers. Suppose these are not all, then it must have either an outer n-set or two non-complementary inner ones. By our previous lemmas, it must contain all the n-integers for some n. Any larger order would contain two n-integer sets, n_1, n_2 say. Considering the subscript doubling again we see that we can suppose they differ by 2. So, without loss of generality, let them be the 0-integers and the 2-integers, however $i_{\infty235}$ is an 0-integer and i_{0235} is a 2-integer and their product is

$$i_{0235}i_{\infty235} = -\frac{3}{4} + \frac{1}{4}(i_0 - i_1 + i_2 + i_3 - i_4 + i_5 + i_6)$$

whose rank equation can be computed as $x^2 + \frac{3}{2}x + 1$ and so is not a member of an order. □

Corollary 3.14

The n-integers form an arithmetic for all n.

So we have a complete list of the orders and arithmetics in $\mathbb{O}$. As we did before we now want to study their properties and especially their prime factorisations. For this we will need some geometric considerations. We start by choosing one arithmetic in $\mathbb{O}$, the 0-integers.

Definition 3.15

*An n-dimensional **regular simplex** is the minimal convex set (or convex hull) containing $n+1$ points which are all equidistant from each other. The n-dimensional simplex lattice A_n is defined to be the structure generated over $\mathbb{Z}$ by the vectors along the edges of a regular simplex.*

A regular simplex can be thought of as generalising the triangle to higher dimensions. In 2-dimensions it is just the triangle and in 3 it is the tetrahedron. For A_n if we take the vertices of a regular simplex to be the $n+1$-dimensional points

$$v_i = (0, 0, ..., 1, ..., 0)$$

with 1 in the ith position, then the generators are

$$v_i - v_j = (0, 0, ..., 1, ..., -1, ..., 0).$$

Then A_n is simply the set of all points

$$(x_0, x_1, ..., x_n)$$

in $n+1$ dimensions whose coordinates are integers which sum to 0.

Definition 3.16

*A **regular orthoplex**, or convex polytope, has vertices which are the unit vectors on each axis of an orthonormal basis. They are therefore the vectors of type*

$$(\pm 1, 0, ..., 0)$$

with ± 1 *in an arbitrary position. The* n*-dimensional orthoplex lattice* D_n *is the lattice generated over* $\mathbb{Z}$ *by these vectors.*

Much like a regular simplex can be thought of as generalising the triangle into higher dimensions, a regular orthoplex is often thought to be the generalisation of the square to higher dimensions. In 2-dimensions it is just the square. In 3 it is the octahedron. For generators of D_n we simply take the vectors

$$v_i = (0, 0, ..., 1, ..., 0) \text{ and } \overline{v}_i = (0, 0, ..., -1, ..., 0).$$

So D_n is just the set of all vectors

$$(x_1, ..., x_n)$$

whose coordinates are integers which sum to an even number.

We are now in a position to define the E_8 root lattice which the Integral octonions form.

Definition 3.17 *The* E_8 *root lattice is the lattice generated by* S, O *where* S *is an* 8*-dimensional simplex and* O *is an adjacent orthoplex.*

We quote some facts about E_8 from ([5],109).

1. Both A_8 and D_8 are contained in E_8.

2. For any point a in 8-dimensional space, there is a point b of the E_8 lattice such that $|a - b| \leqslant 1$.

It is remarkable that even though this 'small remainder' principle carries over to the Integral Octonions, the use of ideals to develop the theory of prime factorisations falls apart. In fact for any integral octonion a we can find another b such that $|a-b| \leqslant 1/2$. However, the result holds in E_8 and this is important as we shall see later. There is however something more remarkable! There is in the Integral Octonions a process equivalent to the Euclidean Algorithm in the rational integers. Conway ([5],pg.111) attributes the discovery to Rehm. We start by taking an octonion r_1 and a rational integer m_1 which divides $N(r_1)$. Then we have

$$N(r_1) = m_1 m_0$$

and we will obtain a series of $m_i \in \mathbb{Z}$ and r_i, g_i integral octonions using the following method;

$$\begin{array}{ccc} r_1 = g_1 m_1 + \overline{r_2} & N(r_1) = m_0 m_1 & \\ r_2 = g_2 m_2 + \overline{r_3} & N(r_2) = m_1 m_2 & m_1 > m_2 \\ \vdots & \vdots & \vdots \\ r_{n-1} = g_{n-1} m_{n-1} + \overline{r_{n-2}} & N(r_{n-1}) = m_{n-2} m_{n-1} & m_{n-2} > m_{n-1} \\ r_n = g_n m_n & N(r_n) = m_{n-1} m_n & m_{n-1} > m_n \end{array}$$

So, we begin with our original r_1, m_1 and then find two integral octonions g_1 and r_2 by the division algorithm for integral octonions and take the conjugate of the remainder r_2 and keep repeating the process. The following propositions show that it indeed works.

Proposition 3.18

m_i divides $N(r_{i+1})$, for all i.

Proof. As $N(\overline{r_{i+1}}) = N(r_i - g_i m_i) = N(r_i) + m_i^2 N(g_i) - 2m_i \langle r_i, g_i \rangle$ so m_i divides every term on the right-hand side and so divides the left-hand side from which we conclude that m_i divides $N(r_{i+1})$. □

This proof shows why we conjugate the remainder in each case.

Proposition 3.19

$m_{i+1} < m_i$, for all i.

Proof. This follows from the fact that $m_i m_{i+1} = N(r_i) \leqslant \frac{m_i^2}{2}$. □

Since the m_i are strictly decreasing and lie in $\mathbb{Z}$, this process must eventually terminate.

We now 'reverse' the process as with the standard Euclidean algorithm. Let μ_n be an element in O of norm m_n. We have that

$$r_n = g_n m_n = g_n(\mu_n \overline{\mu_n}) = (g_n \mu_n)\overline{\mu_n}.$$

There are no associativity issues here as every element lies in a 2-generated subalgebra. Setting $\mu_{n-1} = g_n \mu_n$, makes μ_{n-1} a left divisor of r_n such that $N(\mu_{n-1}) = m_{n-1}$. We also have that $\overline{\mu_{n-1}}$ is a right divisor of $\overline{r_n}$ and m_{n-1} and hence also of r_{n-1} because

$$\begin{aligned} r_{n-1} = g_{n-1}m_{n-1} + \overline{r_n} &= (g_{n-1}\mu_{n-1})\overline{\mu_{n-1}} + \mu_n\overline{\mu_{n-1}} \\ &= (g_{n-1}\mu_{n-1} + \mu_n)\overline{\mu_{n-1}}. \end{aligned}$$

If we let $\mu_{n-2} = g_{n-1}\mu_{n-1} + \mu_n$, then we obtain a left divisor of r_{n-1} whose norm is m_{n-2}. This process can be continued until there is a left divisor of r_1, μ_0, of norm m_0. We represent this as

$$\begin{array}{ccc} & & N(\mu_n) = m_n \\ r_n = \mu_{n-1}\overline{\mu_n} & \mu_{n-1} = g_n\mu_n & N(\mu_{n-1}) = m_{n-1} \\ r_{n-1} = \mu_{n-2}\overline{\mu_{n-1}} & \mu_{n-2} = g_{n-1}\mu_{n-1} + \mu_n & N(\mu_{n-2}) = m_{n-2} \\ \vdots & \vdots & \vdots \\ r_2 = \mu_1\overline{\mu_2} & \mu_1 = g_2\mu_2 + \mu_3 & N(\mu_1) = m_1 \\ r_1 = \mu_0\overline{\mu_1} & \mu_0 = g_1\mu_1 + \mu_2 & N(\mu_0) = m_0 \end{array}$$

If r is an integral octonion of norm mn we wish now to give a description of the sets of all possible left and right divisors of norm m and n. The number of them will turn out to be exactly the number of integral octonions of norm m and n.

Lemma 3.20

Let g be in O and factorise g in two ways so

$$g = ab = a'b'$$

where $N(a) = N(a') \neq 0$ and $N(b) = N(b') \neq 0$. Then if θ_a is the angle between a and a' and θ_b is the angle between b and b', we have

$$\theta_a = \theta_b.$$

Proof. We take the inner-product of g with ab' then by the Scaling Law we have

$$N(a)\langle b, b'\rangle = \langle ab, ab'\rangle = \langle g, ab'\rangle = \langle a'b', ab'\rangle = N(b')\langle a', a\rangle,$$

which implies that

$$\frac{\langle a', a\rangle}{N(a)} = \frac{\langle b, b'\rangle}{N(b')}$$

which is the same as

$$\cos\theta_a = \cos\theta_b.$$

□

Let $\{\mu_n\}, \{\mu_{n-1}\}, \{\mu_{n-2}\}, ..., \{\mu_0\}$ be the set of all μ_is that can occur in the reversing of our algorithm. Our work has shown that $\{\mu_n\}$ is the set of all integral octonions of norm m_n. It is similar to the set $\{\overline{\mu_n}\}$ as can be seen by letting $m_n = g$ in the above lemma. We indicate this by

$$\{\mu_n\} \sim_{m_n} \{\overline{\mu_n}\}.$$

So we obtain the similarities

$$\{\overline{\mu_n}\} \sim_{r_n} \{\mu_{n-1}\} \sim_{m_{n-1}} \{\overline{\mu_{n-1}}\} \sim_{r_{n-1}} ... \sim_{m_1} \{\overline{\mu_1}\} \sim_{r_1} \{\mu_0\}$$

Lemma 3.21

If r is an integral octonion such that $N(r) = mn$ with $m, n \in \mathbb{N}$ and $d = gcd(r, m, n)$, then the set of left divisors (μ_l) of r of norm m and the set of right divisors $(\overline{\mu_s})$ of r of norm n are geometrically similar to the set of all integral octonions (μ_t) of norm $d = m_t$

For a proof of this see ([5],pg.113).

The non-associativity of the octonions leads to a slight problem concerning prime factorisations modelled on a factorisation of the norm. We saw before that if a quaternion has norm 315, then there are twelve possible factorisations due to the lack of commutativity. In the integral octonions the problem is worse as for each factorisation we have

$$315 = ((3.3)5)7 = (3(3.5))7 = ...$$

But the theory of unit-migration also doesn't work as

$$au.u^{-1}b$$

is not necessarily equal to ab. If a change affects two adjacent factors it will be called **meta-migration** since it is similar to the unit-migration of the Hurwitz integers.

The number of factorisations $au.b'$ based on ab is equal to the number of units and the set of left divisors is similar to the set of units so we get the following

Theorem 3.22
The number of factorisations of a primitive integral octonion $Q = ((P_1P_2)(P_3...))P_k$ modelled on a given factorisation of the norm is 240^{k-1}. Also, if we fix all but two of the factors, then the sets of possible values for them is similar to the of the 240 units.

In the case where Q is not primitive we get a result similar to the one which holds for the Hurwitz integers.

Theorem 3.23
An integral octonion of norm $p_1^{n_1}p_2^{n_2}...p_k^{n_k}$ which is divisible by $p_1^{m_1}p_2^{m_2}...p_k^{m_k}$ has

$$240^{n-1}\prod_i C_{n_i,m_i}(p_i^3)$$

prime factorisations on a model with $n = n_1 + ... + n_k$.

Proof. The proof is very similar to the proof in the quaternion case. However, unit-migration does not work here so the 240 factors must be counted as they occur. We replace p with p^3 as there are $240(p^3+1)$ integral octonions of norm p ([5],pg.113).□

So we have developed the theory of arithmetics in both the quaternions and the octonions and developed a theory of prime factorisations. The integral octonions will be used in our next chapter when we need to work modulo 2 in order to obtain the group $G_2(2)$.

Chapter 4

Groups Associated with The Octonions

In this chapter we will look at some of the groups that the octonions yield. The automorphism group of the octonions turns out to be a 14-dimensional Lie group known as G_2. We give a sketch of its construction via a double cover of the special orthogonal group in 8-dimensions using some the properties of isotopies. We then move on to reading the octonions over the field $\mathbb{F}_q$ for $q = p^n$ where p is an odd prime and $n \geqslant 2$. We then examine the case where $q = 3$ and determine some generators for the group as well as showing the outer automorphism. For the case where the field has order 2 we will use the E_8 lattice to determine generators for the group.

4.1 The Automorphism Group of $\mathbb{O}$

We begin by working out the automorphism group of the octonions via the group $SO(8)$ which is the group of all orientation preserving isometries, rotations, in 8-dimensions. We will need a few results on isotopies, monotopies and their companions before we start.

Definition 4.1

An ***isotopy*** *of a loop is a triple of invertible maps* $(\alpha, \beta|\gamma)$ *such that if we have* $xy = z$, *then*

$$x^{\alpha}y^{\beta} = z^{\gamma}.$$

A single map in an isotopy is called a ***monotopy****.*

We can rewrite isotopies in the form (α, β, γ) and then we take the definition to mean

$$x^{\alpha}y^{\beta}z^{\gamma} = 1$$

when $xyz = 1$. After Conway [5] we call an isotopy of the first type a **duplex** and of the second type a **triplex**.

If we choose γ to be a monotopy, then there exists two maps α and β with $xy = z \Rightarrow x^{\alpha}y^{\beta} = z^{\gamma}$. This equation implies that

$$x^{\alpha}1^{\beta} = x^{\gamma} \Rightarrow x^{\alpha} = x^{\gamma}(1^{\beta})^{-1} = x^{\gamma}b$$

and

$$1^{\alpha}y^{\beta} = y^{\gamma} \Rightarrow y^{\beta} = (1^{\alpha})^{-1}y^{\gamma} = ay^{\gamma}$$

where a and b are the images of 1 under the respective maps.

So we get that if γ is a monotopy, then there exists elements a, b in our loop for which if $xy = z$ then

$$(xy)^{\gamma} = x^{\gamma}b.ay^{\gamma}.$$

Definition 4.2

The elements of the loop a, b *described above are called* ***companions*** *of the monotopy* γ.

Isotopies are in some way similar to automorphisms and indeed if a monotopy has companions $a = b = 1$, then it is an automorphism.

With this in place, we are now ready to begin our study of the automorphisms of the octonions. We begin by looking at how strongly the octonions fail to be associative.

Lemma 4.3

If $r \in \mathbb{O}$ is such that

$$x(ry) = (xr)y$$

for all x, y, then r is real.

Proof. For all k we have $(i_k i_{k-1})i_{k+1} = -i_k(i_{k-1}i_{k+1})$ by [6]. So taking $k = 1$ we get that if $(i_1 r)i_2 = i_1(ri_2)$, then the coefficient of i_0 in r must be zero. As we let k cycle through $0, ..., 6$, we get that the coefficient of i_k must be 0 for all k. Hence r is real. □

Theorem 4.4

If a, b are companions for the monotopy γ, any other pair of companions for γ will be of the form $ar, r^{-1}b$ for some real number r.

Proof. If we choose two other companions A, B, then we must have

$$x^\gamma a.by^\gamma = x^\gamma A.By^\gamma$$

for all x, y. Taking $x^\gamma = X$ and $y^\gamma = Y$, we get

$$Xa.bY = XA.BY$$

for all X, Y. Setting $A = ar$, $X = a^{-1}$ and $Y = 1$ we get that $b = rB$ or equivalently

$r^{-1}b = B$. Our identity now becomes

$$Xa.bY = X(ar).(r^{-1}b)Y$$

for all X, Y. If we let $Y = (r^{-1}b)^{-1} = b^{-1}r$ we get that $(Xa)r = X(ar)$ and if we let $X = (ar)^{-1} = r^{-1}a^{-1}$, we see $r^{-1}(bY) = (r^{-1}b)Y$. Now, we can put

$$Xa.bY = (Xa)r.r^{-1}(bY)$$

and then substituting x for Xa and ry for bY yields

$$x(ry) = (xr)y$$

and since this holds for all x, y, by our previous lemma r is real. □

Since the octonions are non-associative it makes sense to study the multiplications

$$L_x : a \mapsto xa \qquad R_x : a \mapsto ax \qquad B_x : a \mapsto xax.$$

Since the octonions are alternative $x(ax) = (xa)x$, the map B_x is well-defined and we have

$$a^{L_x R_x} = (xa)x = a^{B_x} = x(ax) = a^{R_x L_x}.$$

In our proof that the composition algebras satisfy the Moufang identities in Chapter 1, we had the identity (written here in a slightly different form),

$$(xy)(zx) = 2\langle x, \overline{yz}\rangle x - N(x)\overline{yz}.$$

Then as a reflection in x is given by

$$ref_x : a \mapsto a - \frac{2\langle x, a\rangle}{N(x)} x$$

we see that

$$(xy)(zx) = -N(x)(\overline{yz})^{ref_x} = N(x)(yz)^{ref_1 ref_x}.$$

We conclude that bimultiplication by x, B_x, is just a scalar multiple of $ref_1 ref_x$. This leads us to the following lemma;

Lemma 4.5

The operations $ref_1.ref_a$ and $ref_a.ref_1$ can be obtained from bimultiplication by unit octonions.

Proof. The reflections are unaffected by scaling and so we can take $N(a) = 1$. The expression $ref_1 ref_a$ is then as defined above and the second reflection is just the inverse of the first $B_{a^{-1}} = B_{\overline{a}}$. □

Theorem 4.6

If γ is an element of $SO(8)$, there exist α, β in $SO(8)$ such that $(\alpha, \beta|\gamma)$ is an isotopy (hence γ is a monotopy). Further, α, β are unique up to sign.

Proof. Since γ is an element of $SO(8)$, it is a rotation and as such can be generated by an even number of reflections [11]. So let

$$\gamma = ref_{a_1} ref_{b_1} ref_{a_2} ref_{b_2} ... ref_{a_{2k}} ref_{b_{2k}}.$$

We have that

$$ref_{a_n} ref_{b_n} = ref_{a_n} ref_1 ref_1 ref_{b_n}$$

is the product of two bimultiplications by the previous lemma. Hence, we can write γ as the product of $2n$ unit bimultiplications. Call these B_{m_i} for $i = 1, ..., 2k$. Then the isotopy $(\alpha, \beta|\gamma)$ can be written as

$$(L_{m_1}L_{m_2}..., R_{m_1}R_{m_2}...|B_{m_1}B_{m_2}...)$$

which is the isotopy we are looking for. As the m_i are unit octonions α and β are in $SO(8)$. They are also unique up to scalar multiplication but the only non-trivial scalar that keeps them in $SO(8)$ is -1. So we can conclude that $(\alpha, \beta|\gamma) = (-\alpha, -\beta|\gamma)$ and we are done. □

In what follows it will be more convenient to use the triplex form of an isotopy. The triplex (α, β, γ) therefore represents the isotopy of the form $(L_aL_b..., R_aR_b..., B_{\overline{a}}B_{\overline{b}}...)$.

Definition 4.7
*An isotopy (α, β, γ) will be called **orthogonal** if the three monotopies in it are elements of $SO(8)$.*

Our previous work has shown that the orthogonal isotopies form a double cover of $SO(8)$. This group is known as $Spin_8$ and it contains the automorphism group of the octonions. The relationship between the groups is seen through the map

$$(\pm\alpha, \pm\beta, \gamma) \mapsto \gamma.$$

The seven dimensional spin group $Spin_7$ is the preimage of $SO(7)$ in $Spin_8$ under this map. Hence the triples (α, β, γ) such that γ fixes the identity will form a copy of $Spin_7$. If, on the other hand, we had chosen the α or β which fix the identity, we would have other copies of $Spin_7$.

Theorem 4.8

The intersection of any two copies of the above $Spin_7$ groups is in fact the intersection of all three and, moreover, it is the group of automorphisms of the octonions.

Proof. If (α, β, γ) is an isotopy, we can apply it to the equation $1 \times 1 \times 1 = 1$ to get

$$1^{\alpha} \times 1^{\beta} \times 1^{\gamma} = 1.$$

This shows that if two of the monotopies fix 1, then they all do. Hence the intersection of any two copies of $Spin_7$ is the intersection of all three. If a, b are companions of γ, then

$$\alpha = \gamma R_a \text{ and } \beta = \gamma L_b$$

which implies that $a = b = 1$. So γ must be an isomorphism. □

This group is called G_2 and is a 14-dimensional Lie group. According to Baez [2] it was Elie Cartan in [3] in 1914 who first showed the isomorphism between $Aut(\mathbb{O})$ and G_2 however, here we just take it as a definition. Now that we have a description of the automorphism group over the real numbers, we look to find out about the group $G_2(q)$ over fields of finite characteristic. If our field has odd characteristic, then we can read the octonions in their usual basis. However, in fields of characteristic 2 we will have to study the automorphisms of the Integral Octonions and the E_8 root lattice which can be read modulo 2.

4.2 The Monomial Subgroup

Before we begin our study of the full automorphism group of the octonions in odd characteristic, we observe some symmetries of the multiplication table. These automorphism will form a group which will be called the monomial subgroup. We recall the table of the octonions given in Chapter 1.

1	i_0	i_1	i_2	i_3	i_4	i_5	i_6
i_0	-1	i_3	i_6	$-i_1$	i_5	$-i_4$	$-i_2$
i_1	$-i_3$	-1	i_4	i_0	$-i_2$	i_6	$-i_5$
i_2	$-i_6$	$-i_4$	-1	i_5	i_1	$-i_3$	i_0
i_3	i_1	$-i_0$	$-i_5$	-1	i_6	i_2	$-i_4$
i_4	$-i_5$	i_2	$-i_1$	$-i_6$	-1	i_0	i_3
i_5	i_4	$-i_6$	i_3	$-i_2$	$-i_0$	-1	i_1
i_6	i_2	i_5	$-i_0$	i_4	$-i_3$	$-i_1$	-1

There are some symmetries of this table, namely

$$i_k \mapsto i_{k+1}$$

and

$$i_k \mapsto i_{2k}.$$

The second of these is the natural extension of the automorphism

$$i \mapsto j \mapsto k \mapsto i$$

of the quaternions. There is another automorphim

$$(i_0, i_1, ..., i_6) \mapsto (i_0, i_2, i_1, i_6, -i_4, -i_5, i_3)$$

which is an extension of $i \leftrightarrow j, \quad k \mapsto -k$ with $i_1 = i, i_2 = j$ and $i_4 = k$.

If we work modulo signs, from Figure 1.1 the permutations

$$(0\ 1\ 2\ 3\ 4\ 5\ 6) \quad (1\ 2\ 4)(3\ 6\ 5) \quad (1\ 2)(3\ 6)$$

generate the full automorphism group of the plane, which is known to be $PSL_3(2)$. So there exists a homomorphism from the symmetry group onto $PSL_3(2)$. However, the signs of i_0, i_1 and i_2 can be altered and these will then determine the signs of all the elements. So, the homomorphim has a kernel 2^3 and the full symmetry group of the multiplication is $2^3PSL_3(2)$.

4.3 $G_2(q)$

In this section we will describe how the automorphism group of the octonions, when read over a field of odd characteristic, behaves and use this information to compute a formula for its order. We follow the work of [15].

We start this section by examining the group of automorphisms when we read $\mathbb{O}$ over a field $\mathbb{K}$ of size $q = p^n$ for p an odd prime. We will call this $\mathbb{O}(q)$. The automorphisms of $\mathbb{O}(q)$ must preserve 1 and so live inside $GO_7(q)$ as it acts on the orthogonal 7-space. However, since it must preserve the norm, which is multiplicative, we have that it is in fact an element of $SO_7(q)$. The multiplication in $\mathbb{O}(q)$ is completely determined by the vectors i_0, i_1 and i_2 since $i_0i_1 = i_3$ and $i_n = i_2i_m$ for $n \in \{4, 5, 6\}$ and $m \in \{0, 1, 3\}$ modulo signs. So if we know the image of these three vectors, then we know the whole multiplication table. This group is the natural analogue of G_2 over a finite field and we shall denote it $G_2(q)$.

We now wish to calculate the order of $G_2(q)$ for q a power of an odd prime. If i is any purely imaginary unit octonion of norm 1, then we get

$$i^2 = -i\bar{i} = -N(i) = -1.$$

If, further, we have that

$$i = \sum_{t=0}^{6} \lambda_t i_t \text{ and } j = \sum_{t=0}^{6} \mu_t i_t$$

are any two mutually orthogonal purely imaginary unit octonions, then when we multiply them every term $i_m i_n$ must anti-commute for $m \neq n$ and if $m = n$ then the terms $i_m i_m$ must sum to 0, for all m. Hence we get that

$$ij = -ji.$$

If we now set $k = ij$ and choose a new purely imaginary unit vector l orthogonal to i, j and k, then when we expand $(ij)l$ the terms $\lambda_a \mu_b \nu_c (i_a i_b) i_c$ for which it is true that $(i_a i_b) i_c = i_a (i_b i_c)$ correspond to the real parts of ij, jl, il or kl and all of these terms sum to 0. We conclude that

$$(ij)l = -i(jl).$$

The multiplicativity of the norm, $N(xy) = N(x)N(y)$, shows that multiplication by a unit octonion is an orthogonal map and so the set

$$\{1, i, j, l, k, il, jl, kl\}$$

is an orthonormal basis for $\mathbb{O}(q)$.

To compute the size of $G_2(q)$ we need only count the number of triples $\{i, j, l\}$ that behave as above. Since i can be any purely imaginary unit octonion, we get

$$|SO_7(q)|/|SO_6^{\varepsilon}(q)| = q^6 + \varepsilon q^3 = q^3(q^3 + \varepsilon)$$

where $\varepsilon = \pm 1$ satisfies $\varepsilon \equiv q \mod 4$. This corresponds to whether or not the bilinear form has a totally isotropic subspace of dimension 3. We now have that j can be any purely imaginary unit vector of the

$$q^5 - \varepsilon q^2 = q^2(q^3 - \varepsilon)$$

such vectors in the orthogonal 6-space of type ε. The last vector l can be any of the unit vectors in the remaining 4-space of plus type spanned by l, il, jl, kl. There are $q^3 - q$ of these and so the order of $G_2(q)$ is given by

$$|G_2(q)| = q^3(q^3 + \varepsilon)q^2(q^3 - \varepsilon)q(q^2 - 1) = q^6(q^6 - 1)(q^2 - 1).$$

This result puts us in a strong position to search for generating matrices for the groups $G_2(q)$. We do this in the case $q = 3$.

4.4 $G_2(3)$

In this section we aim to find generating matrices for the group $G_2(3)$ in terms of the work we have done before. The group has order $3^6(3^6 - 1)(3^2 - 1) = 4,245,696$. We have seen that the octonions have the automorphism

$$\alpha : i_t \mapsto i_{t+1}$$

and this gives us a 7×7-matrix

$$a = \begin{bmatrix} 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}.$$

We find another automorphism by fixing the quaternion subalgebra spanned by i_0, i_1 and i_3 and then sending i_2 to another unit octonion orthogonal to those three. We choose

$$e : i_2 \mapsto i_2 + i_4 + i_5 + i_6$$

remembering that we are working over $\mathbb{K} = \mathbb{F}_3$. We know that $i_4 = i_1 i_2$ and our automorphism β must preserve this so we get that

$$\beta(i_4) = \beta(i_1 i_2) = \beta(i_1)\beta(i_2) = i_1(i_2 + i_4 + i_5 + i_6) = (i_4 - i_2 + i_6 - i_5).$$

Similarly,

$$\beta(i_5) = \beta(i_2 i_3) = i_5 - i_6 - i_2 + i_4$$

and

$$\beta(i_6) = \beta(i_0 i_2) = i_6 + i_5 - i_4 - i_2.$$

Putting this into a matrix we get

$$b = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 2 & 0 & 1 & 2 & 1 & 0 \\ 0 & 2 & 0 & 1 & 1 & 2 & 0 \\ 0 & 2 & 0 & 2 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}.$$

In fact using Magma,

```
> am:=Matrix(GF(3),7,[0,1,0,0,0,0,0,

> 0,0,1,0,0,0,0,

> 0,0,0,1,0,0,0,

> 0,0,0,0,1,0,0,

> 0,0,0,0,0,1,0,

> 0,0,0,0,0,0,1,

> 1,0,0,0,0,0,0]);

> bm:=Matrix(GF(3),7,[1,0,0,0,0,0,0,

> 0,1,0,1,1,1,0,

> 0,0,1,0,0,0,0,

> 0,2,0,1,2,1,0,

> 0,2,0,1,1,2,0,

> 0,2,0,2,1,1,0,

> 0,0,0,0,0,0,1]);

> AB:=MatrixGroup<7,GF(3)|am,bm>;

> ‘hash’AB;
```

we can see that the two matrices A and B are enough to generate the whole of $G_2(3)$.

4.5 The Outer Automorphism of $G_2(3)$

The group $G_2(3)$ has an outer automorphism [15], which does not occur in other characteristics. In this section we construct this outer automorphism using an exterior square. Using this we can define a factor space which defines a linear map from the standard octonion basis to the factor space which is the automorphism we seek. We begin by constructing the exterior square, so for the basis vectors $\{i_n \,|\, n \in \mathbb{F}_7\}$ of the octonions define

$$i_n \wedge i_m = i_n \otimes i_m - i_m \otimes i_n = -i_m \wedge i_n.$$

Then the exterior square is the set with basis $\{i_n \wedge i_m \,|\, n < m\}$ which is a 21-dimensional subspace of the tensor product $\mathbb{O} \otimes \mathbb{O}$. Inside this space there is an 7-space spanned by

$$v_1 = i_1 \wedge i_3 + i_2 \wedge i_6 + i_4 \wedge i_5$$

and its images under the mapping $i_k \mapsto i_{k+1}$. We call this subspace W. Looking at the images of these vectors under our generators A and B of our group, we see that A leaves it invariant by construction. For the matrix B on the first element of the basis $i_1 \wedge i_3 + i_2 \wedge i_6 + i_4 \wedge i_5$, we see that $i_1 \wedge i_3$ is fixed and we get

$$B(v_1) = i_1 \wedge i_3 + 4(i_2 \wedge i_6 + i_4 \wedge i_5)$$

but since we are working modulo 3, the matrix B fixes this vector. Similar calculations for the other basis elements show that the whole space is invariant under $G_2(3)$. Working modulo W there is another invariant 7-space. This space exists in characteristic 3 since the exterior square of the $G_2(3)$-module has three composition factors of dimension 7. This can be seen in the Magma calculation

```
> print "Group G is G2(3) < GL(7,GF(3))";
Group G is G2(3) < GL(7,GF(3))
> V:=GModule(G);
> V;
GModule V of dimension 7 over GF(3)
> W:=ExteriorSquare(V);
> W;
GModule W of dimension 21 over GF(3)
> CompositionFactors(W);
GModule of dimension 7 over GF(3),
GModule of dimension 7 over GF(3),
GModule of dimension 7 over GF(3).
```

In other characteristics there is only the one 7-dimensional composition factor. Our new space V^* is spanned by the vectors

$$i_t^* = i_{t+1} \wedge i_{t+3} - i_{t+2} \wedge i_{t+6} + W.$$

The automorphism is induced by the map

$$* : i_t \mapsto i_t^*.$$

Proposition 4.9

The map

$$* : i_t \mapsto i_t^*$$

induces an outer automorphism of $G_2(3)$.

Proof. The map $*$ commutes with the permutations $(1\ 2\ 3\ 4\ 5\ 6\ 0)$ and $(1\ 2\ 4)(3\ 6\ 5)$ by construction. And it also commutes with the map that negates i_0, i_3, i_5 and i_6. Then the map

$$(i_0, ..., i_6) \mapsto (i_0, -i_1, i_4, -i_3, i_2, i_6, i_5)$$

takes

$$(i_0^*, ..., i_6^*) \mapsto (i_0^*, -i_1^*, i_4^*, -i_3^*, i_2^*, i_6^*, i_5^*)$$

so that it is an outer automorphism of the monomial subgroup $2^3PGL_3(2)$. However, this group is the automorphism group of the multiplication table and $G_2(3)$ is the automorphism group of the octonion multiplication so we can conclude that $*$ induces an outer automorphism of $G_2(3)$. This can be seen by sending $g \in G$ to $\widehat{g} \in G$ by setting

$$(\widehat{g}(v))^* = g(v^*).$$

We end this chapter with a look at the group $G_2(2)$. This cannot be done in the usual manner as $-1 = 1$. Instead we must consider a scaled copy of the E_8 root lattice and the integral octonions. In such a manner we can read these modulo 2 to obtain the results we need.

4.6 $G_2(2)$

To obtain the group $G_2(2)$ we will need to take the Integral octonions modulo 2. In his book Wilson [15] puts an octonion multiplication on to the E_8 lattice. We will

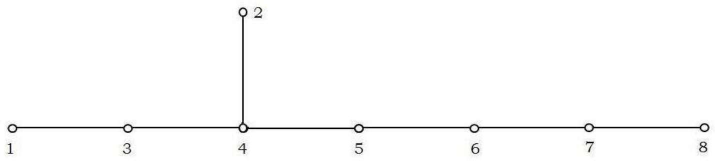

Figure 4.1: E8 Dynkin Diagram

use his construction to obtain generating matrices for the group $G_2(2)$ which can be thought of as the automorphism group of the Integral Octonions modulo 2. Wilson attaches the fundamental roots

where

$$\begin{array}{ll} e_1 = -i_5 & e_2 = \frac{1}{2}(-i_2 - i_4 + i_5 + i_6) \\ e_3 = -i_6 & e_4 = \frac{1}{2}(i_0 - i_3 - i_4 + i_6) \\ e_5 = -i_0 & e_6 = \frac{1}{2}(-1 + i_0 + i_1 + i_3) \\ e_7 = 1 = i_\infty & e_8 = \frac{1}{2}(i_0 + i_1 + i_2 + i_4) \end{array}$$

We reduce this lattice modulo 2. As such we define two vectors to be congruent mod 2 if their difference is twice a vector. Following that we wish to write our usual 8-dimensional basis $\{1, i_0, i_1, i_2, i_3, i_4, i_5, i_6\}$ in terms of these coordinates modulo 2. We see immediately that

$$\begin{array}{ll} i_5 = (1,0,0,0,0,0,0,0); & i_6 = (0,0,1,0,0,0,0,0); \\ 1 = i_\infty = (0,0,0,0,0,0,1,0); & i_0 = (0,0,0,0,1,0,0,0); \end{array}$$

We now need to calculate the remaining i_k for $k = 1, 2, 3, 4$ remembering that we are working modulo 2. For i_1 we get that

$$i_1 - (i_0 + i_5 + i_6) = -(i_0 - i_1 + i_5 + i_6) = 2(\frac{1}{2}(i_0 + i_1 + i_2 + i_4) + \frac{1}{2}(-i_2 - i_4 + i_5 + i_6))$$

So the difference is twice an integral octonion and so i_1 is congruent to $i_0 + i_5 + i_6$ modulo 2 in the lattice. So we get that the point i_1 is the vector $e_1 + e_3 + e_5$ given by

$$i_1 = (1, 0, 1, 0, 1, 0, 0, 0).$$

For i_2 we see that

$$i_2 - (1 + i_0 + i_6) = 2(\frac{1}{2}(-1 - i_0 + i_2 - i_6))$$

which is the double of

$$\frac{1}{2}(i_0 + i_1 + i_2 + i_4) + \frac{1}{2}(i_0 - i_3 - i_4 + i_6) + \frac{1}{2}(-1 + i_0 + i_1 + i_3)$$

modulo 2 and so i_2 has coordinates $e_7 + e_5 + e_3$ which is

$$i_2 = (0, 0, 1, 0, 1, 0, 1, 0).$$

Similar calculations yield

$$i_3 = (1, 0, 1, 0, 0, 0, 1, 0) \text{ and } i_4 = (1, 0, 0, 0, 1, 0, 1, 0).$$

So we have all our original basis vectors in terms of the E_8 lattice modulo 2. Again Wilson [15] gives us some automorphisms of the Integral Octonions. We quote them here.

$$\begin{aligned}
\alpha : & i_0 \mapsto i_6 \mapsto i_2 \mapsto i_0 \\
& i_1 \mapsto \frac{1}{2}(i_1 + i_3 - i_4 + i_5) \\
& i_3 \mapsto \frac{1}{2}(-i_1 + i_3 + i_4 + i_5) \\
& i_4 \mapsto \frac{1}{2}(i_1 - i_3 + i_4 + i_5) \\
& i_5 \mapsto \frac{1}{2}(-i_1 - i_3 - i_4 + i_5)
\end{aligned}$$

$$\beta : i_t \mapsto i_{t+1}$$

and

$$\gamma : (i_0, i_1, i_2, i_3, i_4, i_5, i_6) \mapsto (-i_0, -i_1, i_6, i_3, i_5, i_4, i_2).$$

Using these automorphisms we want to find matrices that generate the group $G_2(2)$. Before we begin we give a list of some precalculated vectors which has come to bear the name **the dictionary**;

$$\begin{array}{ll}
0124 = (0,0,0,0,0,0,0,1) & \overline{\infty}36\overline{5} = (0,1,1,0,0,1,0,1) \\
02\overline{3}\,\overline{5} = (0,1,0,1,0,0,0,0) & \overline{\infty}1\overline{4}6 = (0,0,0,1,1,1,0,0) \\
0\overline{3}\,\overline{4}6 = (0,0,0,1,0,0,0,0) & \overline{\infty}12\overline{5} = (0,1,0,1,1,1,0,0) \\
045\infty = (0,1,0,1,1,1,0,1) & 12\overline{3}6 = (0,0,0,1,1,0,0,1) \\
0561 = (0,1,0,0,0,0,0,1) & \infty2\overline{3}4 = (0,0,0,0,0,1,0,1) \\
06\overline{\infty}2 = (1,0,1,1,0,1,0,1) & 1\overline{3}\,\overline{4}5 = (0,1,1,1,1,0,0,1) \\
0\overline{\infty}13 = (0,0,0,0,0,1,0,0) & \overline{2}\,\overline{4}56 = (0,1,0,0,0,0,0,0),
\end{array}$$

where here the four numbers $abcd$ represent the integral octonion $\frac{1}{2}(i_a + i_b + i_c + i_d)$ and the bars denote negation. We then use the dictionary to compute the images of the e_k We begin with the automorphism α. We have that

$$\alpha : e_1 = i_5 \mapsto \frac{1}{2}(-i_1 - i_3 - i_4 + i_5)$$

which we write as $1\overline{3}\,\overline{4}5$. Then using the dictionary we have

$$\begin{aligned} 1\overline{3}\,\overline{4}5 &= \overline{1}\,\overline{3}\,\overline{4}5 + i_1 \\ &= (0,1,1,1,1,0,0,1) = (1,0,1,0,1,0,0,0) \\ &= (1,1,0,1,0,0,0,1). \end{aligned}$$

Next we have

$$\alpha : e_2 = \overline{2}\,\overline{4}56 \mapsto \frac{1}{2}(-i_0 + i_2 + 1/2(-i_1 + i_3 - i_4 - i_5) + 1/2(-i_1 - i_3 - i_4 + i_5))$$

$$= \frac{1}{2}(-i_0 - i_1 - i_4 + i_2)$$

which is $\overline{0}\,\overline{1}\,\overline{4}2$. We have $\overline{0}\,\overline{1}\,\overline{4}2 = 0124 + i_0 + i_1 + i_4 = (0,0,1,0,1,0,1,1)$ Similarly,

$$\alpha : e_3 \mapsto (0,0,1,0,1,0,1,0)$$

$$\alpha : e_4 \mapsto (0,0,1,0,0,0,0,0,0)$$

$$\alpha : e_5 \mapsto (1,1,1,0,0,1,0,1)$$

$$\alpha : e_6 \mapsto (0,0,0,0,0,0,1,0)$$

$$\alpha : e_0 \mapsto (0,1,0,0,0,0,0,1).$$

This yields the matrix

$$A = \begin{bmatrix} 1 & 1 & 0 & 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}$$

Carrying out these calculations for β and γ gives us, respectively, the matrices B and C which are

$$B = \begin{bmatrix} 1 & 0 & 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}$$

$$C = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}.$$

Putting these matrices into Magma,

```
> am:=MatrixGroup<8,GF(2)|A>;

> ‘hash’am;

6

> bm:=MatrixGroup<8,GF(2)|B>;

> ‘hash’bm;

3

> cm:=MatrixGroup<8,GF(2)|C>;

> ‘hash’C;

2

> G22:=MatrixGroup<8,GF(2)|A,B,C>;

> ‘hash’G22;

12096
```

shows us that all three matrices together generate the group $G_2(2)$. However, the group is not perfect and $G_2(2)' \cong U_3(3)$ Using the Atlas [4] and Magma

```
> U33:=MatrixGroup<8,GF(2)|A,B>;

> ‘hash’U33;
```

```
6048
```

we see that the simple group $U_3(3) \cong G_2'(2)$ is generated by the matrices A and B.

So we have found generators for both $G_2(3)$ and $G_2(2)$ and described some of the symmetries of the octonions as well as the symmetries of one of the groups. The last chapter gives an example of how physicists are using the octonions to describe what is happening in higher dimensions.

Chapter 5
The Division Algebras and Higher Dimensional Spacetime

In this chapter we look at how the octonions are being used in physics to describe a 10-dimensional spacetime system and the rotations involved. The work presented here comes from [10].

In the theory of special relativity two observers moving at different speeds will have different measures of both space and time and could even see the events in different orders. Each observer will have his own frame of reference and a Lorentz transformation will map the observations in one frame to the other. If space is considered to be homogenous, the same everywhere, the Lorentz transformations are just linear transformations.

By the laws of relativity the speed of light is constant for all observers and a Lorentz transformation must take into account not only the Euclidean distance between two events but also the time interval. This is summed up as defining the spacetime distance s between two events to satisfy

$$s^2 = \Delta r^2 - c^2 \Delta t^2$$

with c the speed of light and Δr and Δt the differences in space and time, respectively. Special relativity is set in Minkowski spacetime which has four dimensions; the three usual space dimensions, up-down, left-right and forwards-backwards but it also has one timelike dimension. In this way Minkowski spacetime is a four dimensional manifold. The Lorentz transformations are those transformations which leave the origin fixed and so are considered as rotations of Minkowski space. The full set of symmetries of Minkowski spacetime, including the translations, is the Poincaré group.

A vector in Minkowski spacetime is given by

$$\overline{x} = \begin{pmatrix} t \\ x \\ y \\ z \end{pmatrix}$$

where x, y, z are the three spacelike coordinates and t is the timelike coordinate. The vector $\overline{x}$ can be written in matrix form as

$$X = \begin{bmatrix} t+z & x-iy \\ x+iy & t-z \end{bmatrix}.$$

This matrix is Hermitian in the sense that

$$X = X^{\dagger}$$

with $X^{\dagger}$ the conjugate-transpose of X. Any complex Hermitian 2×2 matrix has four real independent components as the diagonal entries must be real and the off diagonals must be conjugates of each other.

The squared length of a vector $\overline{x}$ in spacetime is defined as

$$|\overline{x}|^2 = x^2 + y^2 + z^2 - t^2$$

with the speed of light defined to be 1. Here we will only consider those transformations which preserve the relative orientation of the axes, the rotations, which is the Lorentz group $SO(3,1)$ where the one tells us about the minus sign in the squared length. The pair (3,1) is called the signature of the symmetric bilinear form. Now Lorentz transformations must preserve this squared length so how can we determine these in terms of X?

The given definition of X has the property that

$$-det(X) = |\overline{x}|^2$$

so we need to find those transformations which preserve determinants. Since

$$det(XY) = det(X)det(Y)$$

we could multiply X on either side by a matrix, Y say, of determinant 1. However, this raises two problems. The first is how to ensure that the product XY is still Hermitian and the bigger problem that over the quaternions and octonions the determinant does not retain its multiplicative property.

To solve the first problem instead of using multiplication, we can 'conjugate' X by a matrix M as

$$X \mapsto MXM^\dagger.$$

Using the fact that

$$(XY)^\dagger = Y^\dagger X^\dagger$$

we have that $MXM^\dagger$ is Hermitian if, and only if, X is. Hence our problem reduces to finding the complex matrices such that

$$det(MXM^\dagger) = det(M)det(X)det(M^\dagger) = det(X)$$

or equivalently

$$det(MM^\dagger) = det(M)det(M^\dagger) = 1.$$

We have the relation

$$det(M^\dagger) = \overline{det(M)}$$

and we reduce our problem to finding the complex matrices M that satisfy

$$|det(M)| = 1.$$

Over $\mathbb{C}$ we can just select those matrices of determinant 1 as M can be multiplied by a complex phase, $e^{i\theta}$, without affecting anything else. So we have that the set of all complex 2×2 matrices of determinant 1, which is known as $SL(2, \mathbb{C})$, maps surjectively onto the Lorentz group $SO(3, 1)$. The kernel of this mapping is $\{\pm 1\}$ and so we see that $SL(2, \mathbb{C})$ is in fact the double cover of $SO(3, 1)$.

We now examine the effect of a Lorentz transformation on our 4-dimensional Minkowski spacetime. The first things we look for are the spatial rotations, rotations in the xy, xz and yz planes. By taking the matrix

$$R_z = \begin{bmatrix} e^{-i\theta} & 0 \\ 0 & e^{i\theta} \end{bmatrix}$$

the mapping $X \mapsto R_z X R_z^\dagger$ becomes

$$\begin{aligned}(R_z X)R_z^\dagger &= \begin{bmatrix} e^{-i\theta}(t+z) & e^{-i\theta}(x-iy) \\ e^{i\theta}(x+iy) & e^{i\theta}(t-z) \end{bmatrix} \begin{bmatrix} e^{i\theta} & 0 \\ 0 & e^{-i\theta} \end{bmatrix} \\ &= \begin{bmatrix} t+z & e^{-i2\theta}(x-iy) \\ e^{i2\theta}(x+iy) & t-z \end{bmatrix}.\end{aligned}$$

So the transformation preserves the tz-plane and rotates the xy-plane through an angle 2θ in the positive direction. In the same way, the matrices

$$R_x = \begin{bmatrix} \cos\theta & -i\sin\theta \\ -i\sin\theta & \cos\theta \end{bmatrix} \qquad R_y = \begin{bmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{bmatrix}$$

correspond to rotations through 2θ in the yz and xz planes, respectively. Any spatial rotation can be generated by these.

A rotation of the time axis t is known as a boost. Geometrically a boost preserves area but is not necessarily Euclidean and is therefore a hyperbolic rotation. In the zt-plane boosts look like

$$B_z = \begin{bmatrix} e^{\phi} & 0 \\ 0 & e^{-\phi} \end{bmatrix}.$$

If we have $X' = B_z X B_z^\dagger$, then by multiplying out and comparing the coordinates we get

$$\begin{aligned} t' &= t\cosh 2\phi + z\sinh 2\phi \\ x' &= x \\ y' &= y \\ z' &= t\sinh 2\phi + z\cosh 2\phi \end{aligned}$$

which corresponds to a boost in the the zt-plane by 2ϕ. Boosts in the xt and yt planes are given by

$$B_x = \begin{bmatrix} \cosh\phi & \sinh\phi \\ \sinh\phi & \cosh\phi \end{bmatrix} \qquad B_y = \begin{bmatrix} \cosh\phi & -i\sinh\phi \\ i\sinh\phi & \cosh\phi \end{bmatrix}$$

respectively.

Since all rotations can be obatined by rotations in each plane, we have obtained a complete list of the matrices which generate all spatial rotations and boosts in 4-dimensional spacetime. We now proceed to see what happens over the other division algbras. If we replace $x + iy$ by an element a in a real division algebra A, we get

$$X = \begin{bmatrix} t+z & \overline{a} \\ a & t-z \end{bmatrix}$$

with $\overline{a}$ the conjugate of a. The element a has either one, two, four or eight components and so each corresponds to a spacetime vector $\overline{x}$ of dimension three, four, six or ten, respectively. The negative of the determinant still gives the Lorentzian norm

$$-det(X) = |\overline{x}|^2.$$

There are no problems with the determinant even in the Octonion case as here the components can be seen to lie in a complex subalgebra. We therefore still want transformations of the form

$$X \mapsto MXM^\dagger$$

that preserve determinants. It is here that we hit upon some problems. In the quaternion case the multiplicativity of the determinant is lost and it is not clear how to define the determinant for non-Hermitian matrices. This problem can be rectified by the identity

$$det(MXM^{\dagger}) = det(M^{\dagger}M)det(X).$$

So our problem reduces to that of finding quaternionic matrices M which satisfy

$$det(M^{\dagger}M) = 1.$$

In the octonion case things are even worse as due to the lack of associativity the map

$$X \mapsto MXM^{\dagger}$$

is not well-defined nor can we know if $MXM^{\dagger}$ is Hermitian. The solution is rather ad hoc as we select only those matrices for which the expression is well-defined! It is enough to take the coefficients as lying in a complex subalgebra of $\mathbb{O}$. In this case the mapping

$$X \mapsto MXM^{\dagger}$$

involves only two directions and is therefore quaternionic. So the identity

$$det(MXM^{\dagger}) = det(M^{\dagger}M)det(X)$$

holds.

We now wish to generalise the rotations we obtained earlier. The matrix R_y still gives a rotation in the plane defined by the real part of a and z. B_z and B_x still give boosts in the z and x directions. B_y also still gives a boost in the y direction and swapping i (which is equal to i_0 in the octonions) with j or k (or the other i_k

in the octonions) we get all the spatial directions. Similarly, R_x and R_z now rotate in the plane defined by the real part of a or z with i (or i_0) and making the correct replacements yields all the spatial rotations.

So for each division algebra we have all the boosts and spatial rotations except those involving two imaginary directions. However in $\mathbb{H}$ the jk-plane can be rotated for some element a by conjugating with $e^{i\theta}$. The same holds here. Conjugating X by

$$R_i = \begin{bmatrix} e^{i\theta} & 0 \\ 0 & e^{-i\theta} \end{bmatrix}$$

will leave the diagonal of X untouched because it is real and rotate a by 2θ in the jk-plane. Replacing i by j or k to get R_j and R_k, will rotate the other planes. Over the octonions things are a little harder. If we choose $a \in \mathbb{O}$ and write $a = z_\infty + z_1 i_0 + z_2 i_1 + z_3 i_3$ with each z_t lying in the complex subalgebra $\mathbb{R}(i_2)$, then conjugating by $e^{i_2\theta}$ yields

$$\begin{aligned} e^{i_2\theta} a e^{-i_2\theta} &= e^{i_2\theta} z_\infty e^{-i_2\theta} + e^{i_2\theta} z_1 i_0 e^{-i_2\theta} + e^{i_2\theta} z_2 i_1 e^{-i_2\theta} + e^{i_2\theta} z_3 i_3 e^{-i_2\theta} \\ &= z_\infty + z_1 e^{2i_2\theta} i_0 + z_2 e^{2i_2\theta} i_1 + z_3 e^{2i_2\theta} i_3 \end{aligned}$$

and this corresponds to a rotation of three planes at once. However we can solve this problem by the mapping

$$X \mapsto (i_0 \cos\theta + i_1 \sin\theta) i_0 X i_0 (i_0 \cos\theta + i_1 \sin\theta)$$

which is called a flip and is a rotation through 2θ in the $i_0 i_1$-plane.

We have found forms for the generators of the Lorentz transformations in three, four, six and ten dimensions. Moreover, we have also shown that the groups $SL(2,\mathbb{R})$, $SL(2,\mathbb{C})$, $SL(2,\mathbb{H})$ and $SL(2,\mathbb{O})$ map onto the groups $SO(2,1)$, $SO(3,1)$,

$SO(5,1)$ and $SO(9,1)$ respectively. In fact they are the double covers. We note finally that care should be taken as the determinant is not well-defined over $\mathbb{H}$ and so we require that $det(M^\dagger M) = 1$ for $SL(2,\mathbb{H})$. For the octonions we require that for $SL(2,\mathbb{O})$ the elements are those for which $X \mapsto MXM^\dagger$ is well-defined. As $\mathbb{O}$ is not associative, we cannot just define the group action in $SL(2,\mathbb{O})$ to be matrix multiplication and instead define it to be

$$(M_1 \circ M_2)X = M_1(M_2 X M_2^\dagger)M_1^\dagger$$

where $\circ$ represents the group operation.

The modern physical theory of supersymmetry requires spacetime to be 10 dimensional. The octonions, as we have seen, reduce the problem of working with 10×10-matrices to describe rotations in all planes to the case of 2×2-matrices. This is only one of the ways the octonions are being used in physics.

List of References

[1] V. Angeltveit. *http://math.uchicago.edu/ vigleik/lec1.pdf.*

[2] J.C. Baez. The octonions. *Bulletin-American Mathematical Society*, 39(2):145–206, 2002.

[3] É. Cartan. *Les groupes réels simples, finis et continus.* Gauthier-Villars, 1914.

[4] J.H. Conway. *Atlas of finite groups: maximal subgroups and ordinary characters for simple groups.* Oxford University Press, USA, 1985.

[5] J.H. Conway, D.A. Smith, and J.C. Baez. On Quaternions and Octonions: Their Geometry. In *Arithmetic, and Symmetry. AK Peters, Ltd.(2003). ISBN.* Citeseer, 2003.

[6] H.S.M. Coxeter. Integral Cayley numbers. *Duke Mathematical Journal*, 13(4):561–578, 1946.

[7] R.T. Curtis. *A Classification and Investigation of the Finite Subloops of the Cayley-Dickson Algebra. Essay submitted for the Smith and Rayleigh Prizes.* The University of Cambridge, 1970.

[8] R.T. Curtis. Construction of a family of Moufang loops. In *Mathematical Proceedings of the Cambridge Philosophical Society*, volume 142, pages 233–237. Cambridge Univ Press, 2007.

[9] L.E. Dickson and C. Sah. *Algebras and their arithmetics.* Dover New York, 1960.

[10] T. Dray and C.A. Manogue. *The Octonions.* Yet to appear., 2002.

[11] L.C. Grove and C.T. Benson. *Finite reflection groups.* Springer, 1985.

[12] IN Herstein. Topics in Algebra. *Co., Waltham, Mass.(l974).*

[13] N. Jacobson. *Basic Algebra. vol. 1.* Freeman, 1974.

[14] F. van der Blij. History of the octaves. *Simon Stevin*, 34:106–125, 1961.

[15] R. Wilson. *The Finite Simple Groups.* Springer Verlag, 2009.