COMPOSITION ALGEBRAS, THE SQUARES IDENTITY, AND A PROBLEM OF HURWITZ

By

JOANNE LYNN EARY

Bachelor of Science
Oklahoma City University
Oklahoma City, Oklahoma
1993

Master of Science
Oklahoma State University
Stillwater, Oklahoma
1997

Submitted to the Faculty of the
Graduate College of the
Oklahoma State University
in partial fulfillment of
the requirements for
the degree of
DOCTOR OF EDUCATION
May, 2001

COMPOSITION ALGEBRAS, THE SQUARES
IDENTITY, AND A PROBLEM OF HURWITZ

Thesis Approval:

James W Cogdell
Thesis Advisor

Alan Adolphson

Denis Bertholf

Martin Burlingame

Benny Evans

Alfred Carlozzi
Dean of the Graduate College

PREFACE

The Squares Identity is a equation of the form $(a_1^2 + \ldots + a_n^2)(b_1^2 + \ldots + b_n^2) = c_1^2 + \ldots + c_n^2$ where $c_1 \ldots c_n$ are bilinear functions of $a_1 \ldots a_n$ and $b_1 \ldots b_n$. An old number theory problem asked for what values of n does this identity exist. Solutions can easily be found for the case $n = 2$, 4 or 8 by using the fact that $|u \cdot v| = |u| \cdot |v|$ in the complex numbers, the quaternions and the Cayley numbers. In 1898 Hurwitz showed that in fact solutions exists only in the case $n = 1$, 2, 4 or 8 while trying to determine what quadratic forms permit composition. We say a quadratic form N permits composition if for all x and y in the algebra $N(x)N(y) = N(xy)$. Since quadratic forms were always positive definite for Hurwitz, the Squares Identity problem was equivalent to his problem. More than fifty years later Jacobson reformulated Hurwitz's problem in terms of *composition algebras*, nonassociative algebras that arise from quadratic forms which permit composition. He solved a generalized version of Hurwitz's problem by determining all composition algebras. While the first half of this paper focuses on the history of the Squares Identity and Hurwitz's solution, the second half presents the solution to Hurwitz's problem reformulated in terms of composition algebras.

I wish to express my gratitude to my thesis advisor Dr. Jim Cogdell for his patience, wisdom, and encouragement. I also wish to thank Dr. Alan Adolphson for his assistance with the research.

TABLE OF CONTENTS

LIST OF TABLES

CHAPTER 1

INTRODUCTION

An old number theory problem asks for what value of n does there exist an identity of the form $(a_1^2 + \cdots + a_n^2)(b_1^2 + \cdots + b_n^2) = c_1^2 + \cdots + c_n^2$ where $c_1, \ldots, c_n$ are bilinear functions in $a_1, \ldots, a_n$ and $b_1, \ldots, b_n$. This identity became know as the Squares Identity, and William R. Hamilton recognized this identity in the complex numbers as the "law of the moduli", the rule that for all complex numbers u and v we have $|u| \cdot |v| = |u \cdot v|$. After spending ten years looking for an algebra of dimension three that possessed this property, he discovered the quaternions in 1843, the real algebra of dimension four whose elements satisfy the law of the moduli. Many other mathematicians began searching for algebras of higher dimensions with the law of the moduli property. Only two months after Hamilton's discovery, John T. Graves, who corresponded with Hamilton, constructed an eight dimensional algebra with this property. This algebra became known as the Cayley numbers after Arthur Cayley independently discovered the same algebra the following year.

In 1898 while studying the composition of quadratic forms, Adolf Hurwitz showed that solutions to the Squares Identity existed only in cases where $n = 1$, 2, 4 or 8. We say a quadratic form N permits composition if for all x and y in the algebra we have $N(x)N(y) = N(xy)$. Since quadratic forms were always positive definite for Hurwitz, every quadratic form could be written as a sum of squares. Then determining which quadratic forms permitted composition was equivalent to finding a solution to the Squares Identity. In 1919 Leonard Dickson published a paper connecting Hurwitz's Theorem to the norm forms of three real algebras: the complex numbers, the quaternions and the Cayley numbers. He noted that Hurwtiz's Theorem implies that these are the only real algebras whose elements satisfy the law of the moduli.

In Dickson's 1919 work he gave a useful construction for the Cayley numbers in terms of the quaternions. In a manner similar to constructing the complex numbers with ordered pairs of real numbers, Dickson constructed the Cayley numbers using the quaternions. He noted that every Cayley number can be written as a pair of quaternions (q_1, q_2), and multiplication for two Cayley numbers can be defined by $(q_1, q_2)(q_3, q_4) = (q_1q_3 - \overline{q_4}q_3, q_4q_1 + q_2\overline{q_3})$ where $\overline{q}$ represents the conjugate of q. This process of "doubling" the quaternions to obtain the Cayley numbers became known as the Cayley-Dickson process. In 1941 A. A. Albert generalized the Cayley-Dickson process to arbitrary fields.

Some years after Albert's work was published, Nathan Jacobson turned to Hurwitz's problem of determining what quadratic forms permit composition. He reformulated this problem in terms of composition algebras, nonassociative algebras that arise from quadratic forms which permit composition. In a 1958 paper Jacobson solves a generalized version of Hurwitz's problem by determining all composition algebras.

The first half of this paper is devoted to a more detailed description of the history of the Squares Identity problem, the development of the quaternions and the Cayley numbers and their connection to the problem. A detailed account of Dickson's construction of the Cayley numbers is also found in this first portion as well as Dickson's version of Hurwitz's proof of Hurwitz's Theorem.

The second half of the paper focuses on the generalization of Hurwitz's Theorem in terms of composition algebras. The first section 3.1 discusses the algebraic structure of composition algebras. An *involution* is an antiautomorphism of period two, and we will see that all composition algebras have an involution. Also, although not all composition algebras are associative, we will see that they are all *alternative*, that is, for all x and y we have $x^2y = x(xy)$ and $yx^2 = (yx)x$. We will also show that any algebra that is alternative with an involution must be a composition algebra.

In the second section, 3.2, we construct a composition algebra using the Cayley-Dickson doubling process. An important result from this section is that if $\mathcal{C}$ is the Cayley-Dickson double of the algebra $\mathcal{B}$, then $\mathcal{C}$ is alternative if and only if $\mathcal{B}$ is associative. This implies that the Cayley-Dickson double of an algebra is a composition algebra if and only if the algebra being doubled is associative.

The next section 3.3 begins with examples of composition algebras. If the characteristic of the field F is not two, one can begin the doubling process with F to construct a quadratic algebra. Doubling a quadratic algebra yields a quaternion algebra, and doubling the quaternions yields a Cayley algebra. If the characteristic of F is two, we cannot begin the iterative process with the field F but we can begin with a quadratic algebra. Since the Cayley-Dickson double of an algebra is a composition algebra only if the algebra being doubled is associative, we can use this iterative construction to prove the main result of this paper: generalized version of Hurwitz's Theorem. This theorem states that the only composition algebras are a field, a quadratic algebra, a quaternion algebra, or a Cayley algebra.

Sections 3.4 and 3.5 give a further classification of composition algebras over a field not of characteristic 2 by analyzing split and division algebras. A composition algebra that does not contain zero divisors is a division algebra and one that does is considered *split*. We will see that a composition algebra is a division algebra if and only if the norm form is nonzero for every nonzero element. We say two norm forms are equivalent if there exists an injective linear mapping $f : \mathcal{C} \to \mathcal{C}'$ such that $N'(f) = N$. One important result in this section tells us when two composition algebras are the same; two composition algebras are isomorphic as algebras if and only if their corresponding norm forms are equivalent. We use this fact to prove that any two split composition algebras of the same dimension are isomorphic. We then show that the unique split algebras over a field F are $F \oplus F$, the 2×2 matrices over F, and Zorn's vector matrices. For the case of division algebras, we show that two Cayley-Dickson doubles of the same composition algebra are isomorphic if and only if the doubling parameters differ by a norm. The paper ends with a discussion of how one may use cohomological techniques to completely determine when two division composition algebras are isomorphic by comparing doubling parameters.

CHAPTER 2

A PROBLEM OF HURWITZ

2.1 The Squares Identity

The Squares Theorem solves the following problem: for what values of n does there exist an identity

$$(a_1^2 + \ldots + a_n^2)(b_1^2 + \ldots + b_n^2) = c_1^2 + \ldots + c_n^2 \tag{2.1}$$

where $c_1 \ldots c_n$ are bilinear functions of $a_1, \ldots, a_n$, and $b_1, \ldots, b_n$.

The simplest form of the Squares Identity is the familiar formula

$$(a_1^2 + a_2^2)(b_1^2 + b_2^2) = (a_1b_1 - a_2b_2)^2 + (a_1b_2 + a_2b_1)^2 \tag{2.2}$$

for all real numbers a, b, c, and d, known as the Two Squares Identity. The Greek mathematician Diophantus knew of this formula and proved it using right triangles. In 1856, Brioschi proved the identity by applying determinants to the matrix equation

$$\begin{pmatrix} a_1 & a_2 \\ -a_2 & a_1 \end{pmatrix} \cdot \begin{pmatrix} b_1 & b_2 \\ -b_2 & b_1 \end{pmatrix} = \begin{pmatrix} a_1b_1 - a_2b_2 & a_1b_2 + a_2b_1 \\ -a_1b_2 - a_2b_1 & a_1b_1 - a_2b_2 \end{pmatrix}. \tag{2.3}$$

Another way to verify formula (2.2) is to note that since the modulus of a product of complex numbers is the product of the modulus of each of the factors, equation (2.2) is simply the identity

$$|uv|^2 = |u|^2|v|^2$$

for complex numbers $u = a_1 + a_2 i$ and $v = b_1 + b_2 i$.

Formula (2.1) for the case $n = 4$ is the Four Squares Identity which states that for all real numbers a_1, a_2, a_3, a_4, b_1, b_2, b_3, b_4 we have

$$(a_1^2 + a_2^2 + a_3^2 + a_4^2)(b_1^2 + b_2^2 + b_3^2 + b_4^2) = c_1^2 + c_2^2 + c_3^2 + c_4^2$$

where

$$\begin{aligned} c_1 &= a_1b_1 - a_2b_2 - a_3b_3 - a_4b_4 \\ c_2 &= a_1b_2 + a_2b_1 + a_3b_4 - a_4b_3 \\ c_3 &= a_1b_3 + a_3b_1 + a_4b_2 - a_2b_4 \\ c_4 &= a_1b_4 + a_4b_1 + a_2b_3 - a_3b_2. \end{aligned} \tag{2.4}$$

Euler related this formula to Goldbach in a letter dated May 4, 1748. He discovered this identity while investigating Bachet's Theorem, which states every natural number is the sum of four or fewer squares of natural numbers. In 1770 Lagrange provided the first proof of Bachet's Theorem. He first showed that any prime p is the sum of four squares and then applied Euler's four squares identity, since the identity showed that the product of two numbers representable as sums of four squares was again representable as sums of four squares. Another proof of the four squares identity was given by Hamilton after his discovery of the Quaternions in 1843.

An interesting interpretation of the four squares identity can be found in the posthumous works of Gauss. In an unpublished manuscript found after his death he remarks that the equation (2.4) can be rewritten in a simpler form using complex numbers:

$$(|u|^2+|v|^2)(|w|^2+|z|^2)=|uw-v\overline{z}|^2+|uz+v\overline{w}|^2$$

where $u=a_1+a_2i$, $v=a_3+a_4i$, $w=b_1+b_2i$, and $z=b_3+b_4i$. This equation can be obtained by applying determinants to the matrix equation

$$\begin{pmatrix} u & v \\ -\overline{v} & \overline{u} \end{pmatrix}\cdot\begin{pmatrix} w & z \\ -\overline{z} & \overline{w} \end{pmatrix}=\begin{pmatrix} uw-v\overline{z} & u\overline{z}+v\overline{w} \\ -\overline{uz}-\overline{v}w & \overline{uw}-\overline{v}z \end{pmatrix}.$$

In this form it resembles Brioschi's matrix interpretation (2.3) of the two squares identity, and it foreshadows a more modern way of interpreting the squares identity.

Degen proved a formula for sums of eight squares in 1818:

$$\begin{aligned}(a_1^2+a_2^2+a_3^2+a_4^2+a_5^2+a_6^2+a_7^2+a_8^2)&(b_1^2+b_2^2+b_3^2+b_4^2+b_5^2+b_6^2+b_7^2+b_8^2)\\ &=c_1^2+c_2^2+c_3^2+c_4^2+c_5^2+c_6^2+c_7^2+c_8^2\end{aligned}$$

where

$$\begin{aligned}
c_1 &= a_1b_1-a_2b_2-a_3b_3-a_4b_4-a_5b_5-a_6b_6-a_7b_7-a_8b_8\\
c_2 &= a_1b_2+a_2b_1+a_3b_4-a_4b_3+a_5b_6-a_6b_5-a_7b_8+a_8b_7\\
c_3 &= a_1b_3-a_2b_4+a_3b_1+a_4b_2+a_5b_7+a_6b_8-a_7b_5-a_8b_6\\
c_4 &= a_1b_4+a_2b_3-a_3b_2+a_4b_1+a_5b_8-a_6b_7+a_7b_6-a_8b_5\\
c_5 &= a_1b_5-a_2b_6-a_3b_7-a_4b_8+a_5b_1+a_6b_2+a_7b_3+a_8b_4\\
c_6 &= a_1b_6+a_2b_5-a_3b_8+a_4b_7-a_5b_2+a_6b_1-a_7b_4+a_8b_3\\
c_7 &= a_1b_7+a_2b_8+a_3b_5-a_4b_6-a_5b_3+a_6b_4+a_7b_1-a_8b_2\\
c_8 &= a_1b_8-a_2b_7+a_3b_6+a_4b_5-a_5b_4-a_6b_3+a_7b_2+a_8b_1. \qquad (2.5)
\end{aligned}$$

At the time Degen thought the formula could be extended to 2^n squares. For the case of 16 squares, he even gave the 16 bilinear functions but left most the signs undetermined. Graves and Cayley also established the eight squares identity in 1844 and 1845 with the independent discovery of the Cayley numbers. This began a flurry of research as mathematicians tried to extend the formula to 2^n squares. In 1847, J.R. Young, who corresponded with Hamilton, also established the eight squares identity independent of Graves and Cayley. He too initially thought his formula could be extended to 16 squares but quickly discovered that it could not and went on to prove that a 16 squares identity did not exist.

The problem for what n was an identity of form (2.1) possible was not completely solved until 1898, when Adolph Hurwitz showed that in fact the Squares Identity exists only for $n = 1, 2, 4, 8$. His proof will be presented in a later section, but first we will trace the developments that led to the solution. Specifically, we will cover the discovery of the Quaternions and the Cayley numbers and how those number systems relate the Squares Theorem, which is a simple number theory statement, to Hurwitz's problem, which is a statement about the composition of quadratic forms.

2.2 Hamilton's Quaternions

William Rowan Hamilton was aware of modulus identity (2.4) for complex numbers and called it the "law of the moduli", officially to mean that the Euclidean length of a vector product is equal to the product of their individual lengths. Although Gauss was the first to represent complex numbers as points in the plane, Hamilton was the first to formally define a complex number $a + bi$ as an ordered pair of real numbers

(a, b). In the early 1830's while developing his "Theory of couples", he wanted to extend this theory to higher dimensions, and posed this problem: Can real triplets (a_1, a_2, a_3) and (b_1, b_2, b_3) be multiplied in a way analogous to the complex numbers? In particular, can they be multiplied so that the law of moduli is satisfied? This is exactly the Squares Theorem for the case $n = 3$. Fortunately, Hamilton was not aware that Legendre had already proved that an identity of this form was impossible in his "Théorie des nombres" in 1830. Legendre remarked that while 3 and 21 can be expressed as the sums of three squares of rational numbers,

$$3 = 1^2 + 1^2 + 1^2$$

$$21 = 4^2 + 2^2 + 1^2,$$

their product $3 \times 21 = 63$ cannot. By a theorem of Fermat, no integer of the form $8k + 7$ is the sum of three rational squares and $63 = 8(7) + 7$.

In his first attempts, Hamilton writes his triple (a_1, a_2, a_3) with one real and two complex parts: $a_1 + a_2 i + a_3 j$ where $i^2 = j^2 = -1$. Then calculating in the ordinary way using commutative laws we have

$$(a_1 + a_2 i + a_3 j)^2 = (a_1^2 - a_2^2 - a_3^2) + (2a_1 a_2)i + (2a_1 a_3)j + (2a_2 a_3)ij. \tag{2.6}$$

Hamilton was not satisfied by this calculation because the product of two triplets should again be another triplet, but instead we have the extra ij term. In calculating the modulus of $a_1 + a_2 i + a_3 j$ we see that

$$(a_1^2 - a_2^2 - a_3^2)^2 = (a_1^2 - a_2^2 - a_3^3)^2 + (2a_1 a_2)^2 + (2a_1 a_3)^2$$

which is the Euclidean length of the right hand side of equation (2.6) providing the ij

term is zero. But even though the law of modulus holds if $ij = 0$, Hamilton finds this unnatural. Next he notices that if commutativity is not assumed, the $(2a_2a_3)ij$ term on the right side of equation (2.6) would be $a_2a_3(ij + ji)$ and this term would vanish if he set $ij = -ji$. In October of 1843 Hamilton writes to John Graves: "Behold me therefore tempted for a moment to fancy that $ij = 0$. But this seemed odd and uncomfortable, and I perceived that the same suppression of the term which was *de trop* might be attained by assuming what seemed to me less harsh, namely, that $ji = -ij$." ([13], 107) Using this new definition he now decides to "Try boldly then the general product of two triplets, and seek whether the law of moduli is satisfied." He computed

$$(a_1 + a_2i + a_3j)(b_1 + b_2i + b_3j)$$
$$= (a_1b_1 - a_2b_2 - a_3b_3) + (a_1b_2 + a_1b_1)i + (a_1b_3 + a_3b_1)j + (a_2b_3 - a_3b_2)ij.$$

In calculating the modulus we see that

$$(a_1^2 - a_2^2 - a_3^2)(b_1^2 - b_2^2 - b_3^2)$$
$$= (a_1b_1 - a_2b_2 - a_3b_3)^2 + (a_1b_2 + a_1b_1)^2 + (a_1b_3 + a_3b_1)^2 + (a_2b_3 - a_3b_2)^2.$$

So modulus of the product was preserved, but the product of two triplets still had four terms.

Hamilton's breakthrough came in October of 1843 on his way to a meeting of the Royal Irish Academy. He was walking along the Royal Canal talking with his wife but thinking of the triplets. In a letter to his son he describes the moment of insight: "An electric circuit seemed to close, and a spark flashed forth..." ([12], xv)

Hamilton writes more in a letter to Graves: "And here there dawned on me the notion that we must admit, in some sense, a fourth dimension of space for the purpose of calculating triplets...or transferring the paradox to algebra, we must admit a third distinct imaginary symbol k, not to be confounded with either i and j, but equal to the product of the first as multiplier, the second as multiplicand, and therefore I was led to introduce *quaternions* such as $a + bi + cj + dk$, or (a, b, c, d)." ([13], 108).

In order test his discovery by computing products and moduli, he needed to compute rules for multiplying i, j, and k. He reasons that $k^2 = -1$ since

$$k^2 = (ij)(ij) = i(ji)i = i(-ij)j = -i^2j^2 = -1.$$

He also calculates

$$ik = i(ij) = i^2j = -j, \;\; kj = (ij)j = ij^2 = -i$$

and in a similar fashion he finds that

$$ki = j \text{ and } jk = i.$$

In the letter to his son concerning his discovery mentioned earlier, Hamilton writes: "I pulled out on the spot a pocket-book, which still exists, and made an entry there and then. Nor could I resist the impulse - unphilosophical as it may have been - to cut with a knife on a stone of Brougham Bridge, as we passed it, the fundamental formula with the symbols i, j, k:

$$i^2 = j^2 = k^2 = ijk = -1, \, ij = -ji = k$$

which contains the solution of the Problem, but of course, as an inscription has long since moldered away." ([12], xv-xvi) On the way to the council meeting Hamilton checked that the law of the modulus held, writing out a sketch of the proof in his notebook.

Next we wish to obtain the four squares identity from the quaternions. However, first we need the product rule for multiplying two quaternions. We will use this to verify that indeed the quaternions satisfy the law of the moduli.

The rules for multiplying i, j, and k are generally referred to as the Hamilton relations. These nine rules are laid out in the following table. Using Hamilton's

	i	j	k
i	-1	k	$-j$
j	$-k$	-1	i
k	j	$-i$	-1

Table 2.1: Quaternion Multiplication

relations, we can find the product of two arbitrary quaternions:

$$(a_1 + a_2 i + a_3 j + a_4 k)(b_1 + b_2 i + b_3 j + b_4 k)$$
$$= (a_1 b_1 - a_2 b_2 - a_3 b_3 - a_4 b_4) + (a_1 b_2 + a_2 b_1 + a_3 b_4 - a_4 b_3) i$$
$$+ (a_1 b_3 + a_3 b_1 + a_4 b_2 - a_2 b_4) j + (a_1 b_4 + a_4 b_1 + a_2 b_3 - a_3 b_2) k \qquad (2.7)$$

The law of moduli can be verified by direct computation, but L. E. Dickson gave a less messy approach in his 1918 paper "Quaternions and their generalization and the history of the eight squares theorem" [8]. Dickson defines the quaternions as an algebra over the real or complex numbers with basis elements 1, i, j, k that satisfy Hamilton's relations given in Table 2.1. He notes that associativity follows from checking triples of basis elements such as $(ij)k = -1 = i(jk)$, etc. and goes on to define the *conjugate* $\overline{q} = a_1 - a_2 i - a_3 j - a_4 k$ to the quaternion $q = a_1 + a_2 i + a_3 j + a_4 k$. He also defines the *norm* $N(q)$ to be $N(q) = q \cdot \overline{q}$, which can be easily calculated to show $N(q) = a_1^2 + a_2^2 + a_3^2 + a_4^2$. Note that this is just the square of the Euclidean length of a real quaternion. Dickson also notes that the real quaternions are a division algebra; if q is a nonzero quaternion, then $N(q) \neq 0$, so $q^{-1} = \frac{\overline{q}}{N(q)}$ and every nonzero quaternion is invertible.

To show the quaternions satisfy the law of the moduli, Dickson first shows that the conjugate of a product of quaternions is equal to the product of their conjugates in reverse order. That is, for quaternions q_1 and q_2, we have $\overline{(q_1 q_2)} = \overline{q_2}\,\overline{q_1}$. Then we have $N(q_1 q_2) = (q_1 q_2)\overline{(q_1 q_2)} = (q_1 q_2)(\overline{q_2}\,\overline{q_1})$ by the definition of the norm and the previous equation. By associativity, the norm of $q_1 q_2$ can be written $q_1(q_2 \overline{q_2})\overline{q_1}$. But now $N(q_2) = q_2 \overline{q_2}$ is a real number, so $N(q_2)$ commutes with quaternion q_1 and we have $N(q_1 q_2) = N(q_1)N(q_2)$. This equation and the formula for the product of two quaternions (2.7) yields exactly the four squares identity (2.6) for $q_1 = a_1 + a_2 i + a_3 j + a_4 k$ and $q_2 = b_1 + b_2 i + b_3 j + b_4 k$.

Also, although Hamilton usually gets credit for the discovery of the quaternions, one should note that Gauss already knew of the rules for multiplying quaternions. Although it was not published at the time, in 1819 he included the formula for multiplying quaternions in a short note on "Mutations of space".

2.3 Cayley Numbers

In December of 1843, only two months after Hamilton notified Graves of his discovery of the quaternions by letter, Graves himself constructed an algebra with eight basis elements that satisfied the law of the moduli. Graves called his algebra the *octads*, and immediately notified Hamilton of his discovery. In July of 1844, Hamilton made an important observation regarding Grave's octads: "In general, in my system of quaternions it is indifferent where we place the points, in any successive multiplication: $A \cdot BC = AB \cdot C = ABC$, if A, B, C be quaternions; but not so generally with your octaves." ([11], 650) This appears to be the first clear statement of the associative law, and the realization that not all algebras may have this property.

Today Graves' octads are more commonly referred to as the *octonions*, *octaves*, or the *Cayley numbers*. Cayley's name became associated with this algebra because the following year Cayley too discovered the eight-dimensional algebra and published his results in 1845, five years before Graves' work was published. Unfortunately for Graves, in January of 1844 he had accepted an offer of Hamilton to make his discovery public after notifying Hamilton of his discovery through correspondence. Hamilton had become almost completely absorbed in his research on the quaternions and did not announce Graves discovery right away.

In a postscript to a paper on elliptic functions [5], Cayley writes: "It is possible to form an analogous theory [to Hamilton's quaternions] with seven imaginary roots of -1". He adds, "with $\nu = 2^n - 1$ roots when ν is a prime number," leaving open the possibility for higher dimension algebras of dimension 2^n. In the postscript he goes on to define multiplication rules between the basis elements $\{1, i_1, i_2, i_3, i_4, i_5, i_5, i_6, i_7\}$ in the following way. He instructs the reader to group together the basis elements according to the types

$$123,\ 145,\ 624,\ 653,\ 725,\ 734,\ 176$$

where each type corresponds to a system of equations. For example, type 123 corresponds to the system

$$\begin{array}{lll} i_1 i_2 = i_3 & i_2 i_3 = i_1 & i_3 i_1 = i_2 \\ i_2 i_1 = -i_3 & i_3 i_2 = -i_1 & i_1 i_3 = -i_2. \end{array}$$

Cayley also writes out the general expression for the product of two elements and mentions that the modulus of the product is the product of the moduli of the factors. Clearly the Cayley numbers are not commutative, just as the quaternions are not commutative, but two years after Cayley introduced the Cayley numbers he published a short note [6] explaining that the algebra fails to be associative as well. He notes that while

$$(i_3 i_4) \cdot i_5 = i_7 \cdot i_5 = -i_2,$$

we have

$$i_3 \cdot (i_4 i_5) = i_3 \cdot i_1 = i_2.$$

Cayley's rules for multiplying the basis element are summarized in the following table. Note that the multiplication table for the quaternion basis elements is contained in the upper left corner with $i_1 = i$, $i_2 = j$, and $i_3 = k$. It is easy to verify from the table that the algebra is neither commutative nor associative. A formula for

	i_1	i_2	i_3	i_4	i_5	i_6	i_7
i_1	-1	i_3	$-i_2$	i_5	$-i_4$	$-i_7$	i_6
i_2	$-i_3$	-1	i_1	i_6	i_7	$-i_4$	$-i_5$
i_3	i_2	$-i_1$	-1	i_7	$-i_6$	i_5	$-i_4$
i_4	$-i_5$	$-i_6$	$-i_7$	-1	i_1	i_2	i_3
i_5	i_4	$-i_7$	i_6	$-i_1$	-1	$-i_3$	i_2
i_6	i_7	i_4	$-i_5$	$-i_2$	i_3	-1	$-i_1$
i_7	$-i_6$	i_5	i_4	$-i_3$	$-i_2$	i_1	-1

Table 2.2: Cayley Number Multiplication

the product of an arbitrary product of two Cayley numbers can be computed using the table, but is obviously going to be a very complicated formula. For this reason, verifying that the law of the moduli is satisfied by the Cayley numbers directly would be very tedious. However, as in the case of the Quaternions, Dickson [8] discovered a clever and less tedious way to verify this by writing the Cayley numbers in a less complex way. Dickson noticed, as can be seen in the table above, that the four Cayley units 1, i_1, i_2, i_3 satisfied the same relations as the four quaternion units 1, i, j, and k. Further, if we let $e = i_4$, he realized that the remaining Cayley units were related to the quaternion units by $ie = i_5$, $je = i_6$, and $ke = i_7$. Then every Cayley number can be written using two quaternions in the less complicated form $q_1 + q_2e$. Dickson claims that one can verify that the multiplication of two Cayley numbers using the relations in Table 2.2 is equivalent to multiplying two Cayley numbers written using quaternions with the following formula:

$$(q_1 + q_2e)(q_3 + q_4e) = (q_1q_3 - \overline{q_4}q_2) + (q_4q_1 + q_2\overline{q_3})e \tag{2.8}$$

where $\overline{q_3}$, $\overline{q_4}$ are conjugate to q_3, q_4 as defined in Section 2.2. In Section 2.1 we will examine Dickson's definition of the Cayley numbers more closely, but for now we will take Dickson's word that the definitions are equivalent. He defines the norm $N(q_1 + q_2e) = q_1\overline{q_1} + q_2\overline{q_2}$, which is the square of the Euclidean length of the Cayley number $q_1 + q_2e$ (and therefore the sum of eight squares of real numbers). Recall that conjugation preserves addition and reverses multiplication; we now begin to calculate the norm of the product of two Cayley numbers using (2.8):

$$\begin{aligned}
&N((q_1q_3 - \overline{q_4}q_3) + (q_4q_1 + q_2\overline{q_3})e) \\
&\quad = (q_1q_3 - \overline{q_4}q_3)\overline{(q_1q_3 - \overline{q_4}q_3)} + (q_4q_1 + q_2\overline{q_3})\overline{(q_4q_1 + q_2\overline{q_3})} \\
&\quad = (q_1q_3 - \overline{q_4}q_3)(\overline{q_3}\,\overline{q_1} - \overline{q_3}q_4) + (q_4q_1 + q_2\overline{q_3})(\overline{q_1}\,\overline{q_4} + q_3\overline{q_2}) \\
&\quad = (q_4q_1q_3\overline{q_2} + q_2\overline{q_3}\,\overline{q_1}\,\overline{q_4}) - (q_1q_3\overline{q_2}q_4 + \overline{q_4}q_2\overline{q_3}\,\overline{q_1}) \\
&\qquad\qquad + (q_1q_3\overline{q_3}\,\overline{q_1} + \overline{q_4}q_2\overline{q_2}q_4 + q_2\overline{q_3}q_3\overline{q_2}).
\end{aligned} \tag{2.9}$$

The last equality follows from simply multiplying out directly and grouping terms. Let a represent the first grouping in the last equality, b the second, and c the third. Rewriting equation (2.9) using a, b, and c we have

$$N((q_1q_3 - \overline{q_4}q_3) + (q_4q_1 + q_2\overline{q_3})e) = a - b + c.$$

We apply a trick to show that $a - b = 0$. Since $\overline{(q_4q_1q_3\overline{q_2})} = q_2\overline{q_3}\,\overline{q_1}\,\overline{q_4}$, we have the conjugate of the first term of a the same as the second term, and so a is a real number and commutes with the quaternions. Recall that $q\overline{q}$ is real and also commutes. Using these facts we see that

$$a = a(\overline{q_4}q_4)\,(\overline{q_4}q_4)^{-1} = (\overline{q_4}aq_4)(\overline{q_4}q_4)^{-1}$$
$$=(\overline{q_4}q_4q_1q_3\overline{q_2}q_4 + \overline{q_4}q_2\overline{q_3}q_1\overline{q_4}q_4)(\overline{q_4}q_4)^{-1}$$
$$= (q_1q_3\overline{q_2}q_4 + \overline{q_4}q_2\overline{q_3}q_1) = b$$

so $a - b = 0$. Again using the fact that $q\overline{q}$ is real we can factor c:

$$q_1q_3\overline{q_3}\,\overline{q_1} + \overline{q_4}q_2\overline{q_2}q_4 + q_2\overline{q_3}q_3\overline{q_2} = q_1\overline{q_1}q_3\overline{q_3} + q_1\overline{q_1}q_4\overline{q_4} + q_2\overline{q_2}q_4\overline{q_4} + q_2\overline{q_2}q_3\overline{q_3}$$
$$= (q_1\overline{q_1} + q_2\overline{q_2})(q_3\overline{q_3} + q_4\overline{q_4})$$
$$= N(q_1 + q_2e)N(q_3 + q_4e).$$

Then the product of the norms of two Cayley numbers is equal to the norm of the product, or equivalently, the law of the moduli is satisfied by the Cayley numbers. With this fact established, the eight squares identity (2.5) can be obtained by computing the modulus of the product and the product of the moduli of the Cayley numbers

$$a_1 + a_2i_1 + a_3i_2 + a_4i_3 + a_5i_4 + a_6i_5 + a_7i_6 + a_8i_7$$

and

$$b_1 + b_2i_1 + b_3i_2 + b_4i_3 + b_5i_4 + b_6i_5 + b_7i_6 + b_8i_7.$$

2.4 Hurwitz's Theorem

As already mentioned, Adolph Hurwitz solved the problem of for what n the squares identity of the form (3.2) exists by proving n must be 1, 2, 4 or 8. The solution is the subject of his 1898 paper "On the composition of quadratic forms". The concept of the composition of binary quadratic forms was introduced by Gauss in his 1801 work *Disquisitiones arithmeticae.* To Gauss, a binary quadratic form is a polynomial of the form $f(x_1, x_2) = ax_1^2 + 2bx_1x_2 + cx_2^2$ where a, b and c are integers. In his work, Gauss was investigating the problem of representing integers by binary quadratic forms. In Article 235, he introduces the idea of the composition of two quadratic form as he explains that given three binary quadratic forms $f(x_1, x_2) = ax_1^2 + 2bx_1x_2 + cx_2^2$, $g(y_1, y_2) = a'y_1^2 + 2b'y_1y_2 + c'y_2^2$, and $h(z_1, z_2) = Az_1^2 + 2Bz_1z_2 + Cz_2^2$, h is composed of f and g if the equation

$$Az_1^2 + 2Bz_1z_2 + Cz_2^2 = (ax_1^2 + 2bx_1x_2 + cx_2^2)(a'y_1^2 + 2b'y_1y_2 + c'y_2^2) \qquad (2.10)$$

holds for all x_1, x_2, and all y_1, y_2 where z_1 and z_2 are bilinear forms in x_1, x_2 and y_1, y_2 with integer coefficients. If we allow the coefficients to be any real numbers and assume the forms are positive definite, then with a suitable change of variables, equation (2.10) is transformed into the two squares identity $c_1^2+c_2^2 = (a_1^2+a_2^2)(b_1^2+b_2^2)$ which is solved by $c_1 = a_1b_1 - a_2b_2$ and $c_2 = a_1b_2 + a_2b_1$ (2.2).

Many mathematicians began trying to extend Gauss' idea of the composition of quadratic forms to forms in n variables over the 19th century. Hurwitz was among them, forming new questions concerning the theory of quadratic forms in n variables. For Hurwitz, who was working over the real numbers, quadratic forms were always positive definite so every quadratic form can be written as a sum of squares. He begins his paper with the following: "In the domain of quadratic forms in n variables, a theory of composition exists, if for any three quadratic forms ϕ, ψ, χ of nonvanishing determinant the equation

$$\phi(x_1, x_2, \ldots, x_n)\psi(y_1, y_2, \ldots, y_n) = \chi(z_1, z_2, \ldots, z_n) \tag{2.11}$$

can be satisfied by replacing the variables $z_1, z_2, \ldots, z_n$ by suitably chosen bilinear functions of the variables $x_1, x_2, \ldots, x_n$ and $y_1, y_2, \ldots, y_n$. As a quadratic form can be expressed as a sum of squares by a suitable linear transformation of the variables, one can consider, without loss of generality, in place of the equation above the following equation:

$$(x_1^2 + x_2^2 + \cdots + x_n^2)(y_1^2 + y_2^2 + \cdots + y_n^2) = z_1^2 + z_2^2 + \cdots + z_n^2.$$

In view of this the question as to whether a composition theory exists for quadratic forms with n variables is essentially equivalent to this other question, as to whether the equation can be satisfied by suitable chosen bilinear functions $z_1, \ldots, z_n$ of the $2n$ independent variables $x_1, \ldots, x_n, y_1, \ldots, y_n$." ([9], 268)

In this manner Hurwitz linked the relatively new idea of the theory of composition with the rather old squares identity problem. In his paper he solves the squares problem with the following theorem. In a later section we will give a more modern and elegant proof of this theorem. Here we will outline Dickson's version [8] of Hurwitz's proof. The proof is highly computational and a rather complicated argument involving matrices. This should provide a nice contrast to the modern proof to be given later.

Theorem 2.4.1 (Hurwitz Theorem) *Let $n \geq 1$ be an integer and $z_1, \ldots, z_n$ be real bilinear forms in real variables $x_1, \ldots, x_n, y_1, \ldots, y_n$ such that*

$$(x_1^2 + x_2^2 + \cdots + x_n^2)(y_1^2 + y_2^2 + \cdots + y_n^2) = z_1^2 + z_2^2 + \cdots + z_n^2. \tag{2.12}$$

Then $n = 1, 2, 4$ or 8.

Proof. The first step is to rewrite equation (2.12) using matrices. Let $\chi(z_1, \ldots, z_n)$ be a quadratic form given by $z_1^2 + \cdots + z_n^2$ so that in matrix form $\chi(z_1, \ldots, z_n) = zIz^t$ where z is the row matrix $(z_1, \cdots, z_n)$, z^t represents the transpose of z, and I is the n by n identity matrix. Let A represent the matrix

$$A = \begin{pmatrix} a_{11} & a_{12} & \ldots & a_{1n} \\ a_{21} & a_{22} & \ldots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \ldots & a_{nn} \end{pmatrix}$$

and A^t represent its transpose, where each a_{ij} is a linear function of $x_1, \ldots, x_n$. Now if we replace each z_i by the linear function $a_{i1}y_1 + \cdots + a_{in}y_n$ then

$$z = (z_1, \ldots, z_n) = (\sum_{j=1}^{n} a_{1j}y_j, \cdots, \sum_{j=1}^{n} a_{nj}y_j) = (y_1, \cdots, y_n)A^t$$

and since $zIz^t = (y_1, \cdots, y_n)A^t \cdot I \cdot A(y_1, \cdots, y_n)^t$ we obtain a new quadratic form in $y_1, \cdots, y_n$ with matrix expression A^tA. Note that the quadratic form in $y_1, \cdots, y_n$ on the left side of equation (2.12) has associated matrix $(x_1^2 + \ldots + x_n^2)I$. Then there exists an identity of form (2.12) only if the matrix representations of the resulting quadratic forms are equal, that is,

$$A^tA = (x_1^2 + \ldots + x_n^2)I. \tag{2.13}$$

We have rewritten equation (2.12) using matrices, and now we will further expand our matrix equation and prove some relations that will be needed later in the proof and also we will show that n must be even. We have assumed that each entry in the matrix A is a linear function of $x_1, \ldots, x_n$, so we can find matrices $A_1, \ldots, A_n$ such that $A = x_1A_1 + \ldots + x_nA_n$. In multiplying out A^tA, one sees that the coefficient of x_n^2 is $A_n^tA_n$, and equation (2.13) implies $A_n^tA_n = I$. Let $B_i = A_n^tA_i$ for $i = 1, \ldots, n-1$. Left multiplication by A_n gives $A_nB_i = A_i$ since $A_n^tA_n = I$, and the transpose of this matrix equation gives $B_i^tA_n^t = A_i^t$. Using these new relations we compute A^tA:

$$\begin{aligned}
(\sum_{i=1}^{n} x_iA_i^t)(\sum_{i=1}^{n} x_iA_i) &= (\sum_{i=1}^{n-1} x_iB_i^tA_n^t + x_nA_n^t)(\sum_{i=1}^{n-1} x_iA_nB_i + A_nx_n) \\
&= (\sum_{i=1}^{n-1} x_iB_i^t + x_n)A_n^tA_n(\sum_{i=1}^{n-1} x_iB_i + x_n) \\
&= (\sum_{i=1}^{n-1} x_iB_i^t + x_n)(\sum_{i=1}^{n-1} x_iB_i + x_n) \qquad (2.14)
\end{aligned}$$

with the last equality following from the fact that $A_n^tA_n = I$. Multiplying out and regrouping terms in expression (2.14) and recalling equation (2.13) yields the equality

$$(x_1^2 + \ldots + x_n^2)I = \sum_{1 \leq i < j \leq n-1} x_ix_j(B_i^tB_j + B_j^tB_i) + \sum_{i=1}^{n-1} x_ix_n(B_i^t + B_i) + \sum_{i=1}^{n} x_i^2B_i^tB_i.$$

Equating coefficients on both sides gives the equations $B_i^tB_j + B_j^tB_i = 0$, $B_i^t + B_i = 0$, and $B_i^tB_i = I$. The second of these equations gives $B_i^t = -B_i$, that is, each B_i for $i = 1, \ldots, n-1$ is skew symmetric. Using this fact we can replace B_i^t in the first and third equation with $-B_i$ to obtain

$$B_i^2 = -I \qquad \text{and} \qquad B_iB_j = -B_jB_i. \qquad (2.15)$$

These relations will be needed in the next stage of the proof. There is another important fact we can obtain from the fact that B_i is skew symmetric. We know that the determinant of the transpose of a matrix is the same as the determinant of the original matrix, and so $B_i^t = -B_i$ implies $\det(B_i^t) = (-1)^n\det(B_i)$. Then either

$\det(B_i) = 0$ or n must be even. But $B_i^t B_i = I$ tells us that B_i is nonzero, so we have shown that there cannot exists an identity of form (2.12) if n is odd.

Consider the 2^{n-1} matrices

$$I, \ B_{i_1}, \ B_{i_1}B_{i_2}, \ B_{i_1}B_{i_2}B_{i_3}, \ \ldots, \ B_1 B_2 \cdots B_{n-1} \tag{2.16}$$

where $i_1 < n, i_1 < i_2 < n, \ldots$. The next stage of the proof involves showing that at least half of these matrices are linearly independent. We will do this by finding all the irreducible linear relations which hold between these matrices. By irreducible we mean a relation $R = 0$ where R cannot be written $R = R_1 + R_2$ with both $R_1 = 0$ and $R_2 = 0$.

There are two important points to make before preceding with the argument. The first concerns a property of the matrices (2.16). We already know that the transpose of a product of matrices is the product of the transpose of each matrix in the reverse order. We apply this familiar fact and the fact that each B_i is skew symmetric along with the relations (2.15) to calculate the transpose of a product of the matrices in (2.16):

$$\begin{aligned}
(B_{i_1}B_{i_2}\ldots B_{i_r})^t &= B_{i_r}^t B_{i_{r-1}}^t \ldots B_{i_1}^t \\
&= (-1)^r B_{i_r} B_{i_{r-1}} \ldots B_{i_1} \\
&= (-1)^r(-1)^{r-1} B_{i_1} B_{i_r} B_{i_{r-1}} \ldots B_{i_2} \\
&= (-1)^r(-1)^{r-1}(-1)^{r-2} B_{i_1} B_{i_2} B_{i_r} B_{i_{r-1}} \ldots B_{i_3} \\
&= (-1)^{(r)+(r-1)+(r-2)+\ldots+(1)} B_{i_1} B_{i_2} \ldots B_{i_r} \\
&= (-1)^{\frac{r(r+1)}{2}} B_{i_1} B_{i_2} \ldots B_{i_r}.
\end{aligned} \tag{2.17}$$

Then the product of r of these matrices (2.16) is symmetric if $\frac{r(r+1)}{2}$ is even, that is, when $r \equiv 0, 3 \pmod 4$), and skew symmetric if $\frac{r(r+1)}{2}$ is odd, which happens when $r \equiv 1, 2 \pmod 4$.

The second point to make before preceding is that any irreducible linear relation holding between the matrices (2.16) must involve either all symmetric matrices or all skew symmetric matrices. If we had such an irreducible linear relation $R = 0$ involving both types and grouped the symmetric matrices in the sum R_1 and the skew symmetric matrices in the sum R_2, then we could write the relation $R = 0$ in the form $R_1 = R_2$. But then $R_1^t = R_2^t$, and since $R_1^t = R_1$ and $R_2^t = -R_2$, we must have $R_1 = R_2 = 0$. This contradicts that assumption that R was irreducible.

We now proceed in showing that at least half of the matrices in (2.16) are linearly independent. Let $R = 0$ be an irreducible relation holding between these matrices. We would like the leading term in our relation to be I and this can be achieved in the following manner. Suppose for example that our leading term is $cB_{i_1}B_{i_2}$. Then we can multiply the leading term by $(\frac{-1}{c})B_{i_1}B_{i_2}$. Applying relations (2.15) we see

$$\begin{aligned}(cB_{i_1}B_{i_2})(-\frac{1}{c}B_{i_1}B_{i_2}) &= (-1)(B_{i_1}B_{i_2})(B_{i_1}B_{i_2}) \\ &= (-1)^2 B_{i_1}^2 B_{i_2}^2 \\ &= (-1)^2(-I)(-I) \\ &= I.\end{aligned}$$

So we obtain another irreducible relation that can be written in the form

$$I = \sum_{i_1<i_2<i_3} c_{i_1 i_2 i_3} B_{i_1}B_{i_2}B_{i_3} + \sum_{i_1<i_2<i_3<i_4} d_{i_1 i_2 i_3 i_4} B_{i_1}B_{i_2}B_{i_3}B_{i_4} + \cdots. \tag{2.18}$$

We noted earlier that an irreducible linear relation cannot contain both symmetric and skew symmetric matrices. Then since the identity matrix I is symmetric, all terms in this sum must be symmetric. In particular, the number of terms r in each product must satisfy $r \equiv 0, 3 \pmod 4$ by the statement following equations in (2.17).

We now show that all coefficients in relation (2.18) must be zero unless $r = n-1$. Consider first the coefficient $c_{i_1 i_2 i_3}$. Multiply relation (2.18) by B_i to obtain the new linear relation

$$B_i = \sum_{i_1<i_2<i_3} c_{i_1 i_2 i_3} B_{i_1} B_{i_2} B_{i_3} B_i + \sum_{i_1<i_2<i_3<i_4} d_{i_1 i_2 i_3 i_4} B_{i_1} B_{i_2} B_{i_3} B_{i_4} B_i + \cdots$$

Since each B_i is skew symmetric, now every term in this sum must be skew symmetric. Provided that $n-1 > 3$, we can always choose $i \neq i_1 i_2 i_3$ so the first term in the sum $B_{i_1} B_{i_2} B_{i_3} B_i$ is the product of four distinct matrices. Since we know the product of four of these matrices is symmetric, $c_{i_1 i_2 i_3}$ must be zero as long as $n-1 \neq 3$. This same argument can be applied to any term in the sum where $r \equiv 3 \pmod 4$. As long as $n-1 \not\equiv 3 \pmod 4$ and $r > n-1$, we can choose $i \neq i_1, \ldots, i_r$ such that $\prod_{j=1}^{r} B_{i_j} B_i$ is the product of $r+1 \equiv 0 \pmod 4$ distinct matrices which must be symmetric and therefore its coefficient must be zero. Now consider the terms in relation (2.18) such that $r \equiv 0 \pmod 4$. We first look at $r = 4$, and show that $d_{i_1 i_2 i_3 i_4}$ must be zero. Multiply relation (2.18) by B_i as in the preceding argument but take $i = i_4$. Then again we have a relation where each term must be skew symmetric and we have the term $d_{i_1 i_2 i_3 i_4} B_{i_1} B_{i_2} B_{i_3} B_{i_4} B_i = d_{i_1 i_2 i_3 i_4} B_{i_1} B_{i_2} B_{i_3}(-I)$ which must be symmetric since the product of 3 of these matrices must be symmetric. So the coefficient $d_{i_1 i_2 i_3 i_4}$ must be zero. As before, this argument works for any $r \equiv 0 \pmod 4$. Thus we have shown that if an irreducible linear relation exists between the matrices (2.16), it must be of the form

$$I = kB_1B_2 \dots B_{n-1}.$$

Further, we know that $kB_1B_2 \dots B_{n-1}$ must be symmetric and so $n - 1 \equiv 0, 3 \pmod 4$, but we showed earlier that n must be even so $n \equiv 0 \pmod 4$. Also, from computations in equation (2.17) and relations (2.15) we know that

$$(kB_1B_2 \dots B_{n-1})^2 = (-1)^{\frac{r(r+1)}{2}} I = I$$

so we can conclude that $k^2 = 1$ or $k = \pm 1$.

Next we summarize what we have shown thus far: We know that if we are to have an identity of form (2.12), n must be even. If $n \equiv 2 \pmod 4$, the 2^{n-1} matrices (2.16) are linearly independent. If $n \equiv 0 \pmod 4$ and the matrices (2.16) are not independent, the only basic irreducible linear relation between them is the relation $I = \pm B_1B_2 \dots B_{n-1}$. Any other irreducible linear relations are obtained from this relation by multiplying by the various B_i.

We started this stage of the proof wanting to show that at least half of the matrices (2.16) were linearly independent. As stated in the previous paragraph we have shown that all 2^{n-1} are linearly independent if $n \equiv 2 \pmod 4$. For $n \equiv 0 \pmod 4$, any linear relation between the matrices (2.16) is derived from the relation $I = \pm B_1B_2 \dots B_{n-1}$ by multiplication by one of the matrices (2.16), but multiplying this relation by any B_i (or product of B_i's) eliminates the B_i (or product of B_i's) from the right side of the equality. Then if relations exists between the matrices, they express a product of B_i's in terms of the remaining B_i's. So the matrices (2.16) which are products of at most $(n-2)/2$ B_i's must be linearly independent. This describes half of the matrices in (2.16). Since there are 2^{n-1} total, this is 2^{n-2} of them.

We know n must be even, but it remains to be shown that $n \leq 8$ and $n \neq 6$. Observe that any set of n^2+1 $n \times n$ matrices must be linearly dependent, since a space of $n \times n$ matrices can be spanned by at most n^2 elements. Then in our set of matrices (2.16) where we know at least 2^{n-2} of them are linearly independent, we must have $2^{n-2} \leq n^2$. This condition fails for $n \geq 10$; it fails for $n = 10$ by inspection and if we assume if fails for N, we can show if fails for $N+1$. For if $2^{N-2} > N^2$, we have $2^{(N+1)+1} = 2 \cdot 2^{N-2} > 2 \cdot N^2$ and for any $N > 2$, $2 \cdot N^2 > (N+1)^2$. Now since the condition fails for $n \geq 10$, we have shown that $n \leq 8$.

We still must exclude $n = 6$. Since $6 \equiv 2 \pmod 4$, if there exists a solution to (2.4) the 2^5 matrices (2.16) are linearly independent. Recall that a product of 1, 2, or 5 B_i's is skew symmetric. Then of the matrices (2.16), 5+10+1=16 of them are skew symmetric. But a space of $n \times n$ skew symmetric matrices has dimension at most $n(n-1)/2 = 15$. Then the matrices cannot be linearly independent and there exists no solution to (2.12).

First we showed that if there exists an identity of form (2.12), n must be even. Then we showed that n must be less than 10, and finally we excluded $n = 6$. So n must be 1, 2, 4, or 8, and we have already shown the problem has a solution in these cases. □

CHAPTER 3

COMPOSITION ALGEBRAS

3.1 Structure

In Chapter 2 we showed the connection between the quadratic forms permitting composition as in Hurwitz's Theorem and the norm forms of three different *nonassociative* algebras: the complex numbers, the quaternions, and the Cayley numbers. Here we are using the term nonassociative algebra to mean a vector space over a field with a bilinear multiplication that is not necessarily associative. Hurwitz's Theorem implies that there is no larger nonassociative algebra over the real numbers than the Cayley numbers that satisfies the property that the product of norms is equal to the norm of a product. In this chapter we will generalize Hurwitz's Theorem by considering quadratic forms defined on a vector space over an arbitrary field and their corresponding *composition algebras*, that is, nonassociatve algebras that arise from quadratic forms which permit composition. With this idea the question of determining what quadratic forms permit composition becomes a question of determining composition algebras. Hurwitz's problem as presented in the previous chapter is a statement about the possible dimensions of these algebras. A more general version of Hurwitz's problem, which is the aim of this chapter, is not just to determine the dimensions of these algebras, but to classify all such algebras. In this first section we will prove some basics facts about composition algebras and their structure.

We begin with a vector space $\mathcal{C}$ over a field F. Assume $\mathcal{C}$ is equipped with a nondegenerate quadratic form N. By quadratic form we mean precisely a mapping from $\mathcal{C}$ into F such that for all α in F, x in $\mathcal{C}$ we have

$$N(\alpha x) = \alpha^2 N(x)$$

and

$$q(x,y) = N(x+y) - N(x) - N(y)$$

is a symmetric bilinear form. The quadratic form N is nondegenerate when $N(x) = 0$ and $q(x,y) = 0$ for all y in $\mathcal{C}$ implies $x = 0$. In a more general sense, Hurwitz's problem was to determine all quadratic forms which permit composition in the sense that it is possible to define a bilinear composition xy in $\mathcal{C}$ such that

$$N(x)N(y) = N(xy)$$

for all x, y in $\mathcal{C}$. The vector space $\mathcal{C}$ together with the given addition, scalar multiplication and the product defined by the bilinear composition xy defines a nonassociative algebra.

Definition 3.1.1 *A* composition algebra *is a finite dimensional nonassociative algebra $\mathcal{C}$ with a nondegenerate quadratic form N on $\mathcal{C}$ such that for all x, y in $\mathcal{C}$ we have*

$$N(x)N(y) = N(xy).$$

With the following lemma we will see that we may always assume that a composition algebra has an identity. This was first shown by Kaplansky [19] by the argument given here.

Lemma 3.1.2 *If it is possible to define a bilinear product xy on a vector space C that makes it into a composition algebra, then the product can be modified to make C into a composition algebra with an identity.*

Proof. Since we assumed the quadratic form N is nondegenerate, we can find a in C such that $N(a) \neq 0$. Put $u = N(a)^{-1}a^2$ so that $N(u) = N(N(a)^{-1})a^2) = (N(a)^{-1})^2 N(a)^2 = 1$ and we have

$$N(xu) = N(x) = N(ux) \tag{3.1}$$

for all x. Let R_u denote right multiplication by u and L_u denote left multiplication by u. The previous statement implies R_u and L_u are injective: if $x \neq 0$ then $N(x)$ nondegenerate implies we can find y such that $q(x, y) \neq 0$, and by (3.1) $q(ux, uy) = q(x, y)$ so that $q(ux, uy)$ is also nonzero and then $ux \neq 0$. Since C is finite dimensional both mappings also are surjective. So we know these maps are linear, bijective, and $N(R_u(x)) = N(L_u(x)) = N(x)$ by (3.1). An injective linear transformation from a bilinear space to itself that satisfies (3.1) is an *isometry*, and it is well known that the set of all isometries from a bilinear space V to itself forms a group with respect to composition which is called the orthogonal group of V. ([17], 344) Then by the preceding analysis, the maps R_u and L_u both are isometries and therefore elements of the orthogonal group of C. This fact tells us that R_u^{-1} and L_u^{-1} are also elements of the orthogonal group of C so that $N(R_u^{-1}(x)) = N(L_u^{-1}(x)) = N(x)$. Now we define a new bilinear multiplication $\cdot$ on C by

$$x \cdot y = R_u^{-1}(x) L_u^{-1}(y).$$

This multiplication defines a composition algebra structure on C since

$$N(x \cdot y) = N(R_u^{-1}(x)L_u^{-1}(y)) = N(R_u^{-1}(x))N(L_u^{-1}(y)) = N(x)N(y)$$

with the last equality following from the fact that R_u^{-1} and L_u^{-1} are isometries. Finally we claim that u^2 an identity element relative to the $\cdot$ multiplication. This follows from the calculations

$$u^2 \cdot x = R_u^{-1}(u^2)L_u^{-1}(x) = R_u^{-1}(R_u(u))L_u^{-1}(x) = uL_u^{-1}(x) = L_u(L_u^{-1}(x)) = x$$

and

$$x \cdot u^2 = R_u^{-1}(x)L_u^{-1}(u^2) = R_u^{-1}(x)L_u^{-1}(L_u(u)) = R_u^{-1}(x)uR_u(R_u^{-1}(x)) = x.$$

Then we may always assume that a composition algebra contains an identity. Indeed, we have shown that if a composition algebra does not to have an identity to begin with, we can redefine the multiplication to obtain a composition algebra that does without changing the quadratic form. With this change, we then have a copy of F contained in C as $F \cdot 1$. □

Before proceeding to analyze the structure of composition algebras, we first derive some relations that we will need later in this section. First note that since N permits composition, we have $N(x) = N(x)N(1)$ so that $N(1) = 1$. Additional relations are given in the following lemma.

Lemma 3.1.3 *Let C be a composition algebra. Then the following relations hold for all x, y, z, w in C:*

$$q(xy, zy) = q(x, z)N(y) \tag{3.2}$$

$$q(xy, xw) = N(x)q(y, w) \tag{3.3}$$

$$q(xw, zy) + q(xy, zw) = q(x, z)q(y, w). \tag{3.4}$$

Proof. To show relation (3.2) we compute directly

$$\begin{aligned} q(xy, zy) &= N(xy + zy) - N(xy) - N(zy) \\ &= [N(x + z)N(y) - (N(x) + N(z))N(y)] \\ &= [N(x + z) - N(x) - N(z)]N(y) \\ &= q(x, z)N(y). \end{aligned}$$

Similarly relation (3.3) holds. For relation (3.4), replace y with $y+w$ in relation (3.2). This gives the statement

$$q(xy + xw, zy + zw) = q(x, z)N(y + w). \tag{3.5}$$

Using bilinearity we can expand the left side of this equation into

$$q(xy + xw, zy + zw) = q(xy, zy) + q(xy, zw) + q(xw, zy) + q(xw, zw). \tag{3.6}$$

We have $q(y, w) = N(y+w) - N(y) - N(w)$ so the right side of equation (3.5) becomes

$$\begin{aligned} q(x, z)N(y + w) &= q(x, z)[q(y, w) + N(y) + N(w)] \\ &= q(x, z)q(y, w) + q(xy, zy) + q(xw, zw) \qquad (3.7) \end{aligned}$$

with the last equality following from relation (3.2). Combining equations (3.6) and (3.7) gives relation (3.4). □

We now proceed with our investigation of the structure of composition algebras. Because we do not wish to restrict our results on the structure of composition algebras, we have not made any requirement on the characteristic of the field F. However, we will need to treat one special case separately that can only happen in the event that the characteristic of F is 2. We have the following result in the special case that the bilinear form is identically zero.

Proposition 3.1.4 *Suppose $q(x, y) = 0$ for every x, y in the composition algebra $\mathcal{C}$. Then $\mathcal{C}$ is a purely inseparable extension field of F, with $N(x) = x^2$ for all x in $\mathcal{C}$.*

Proof. We show first that the map $\phi : \mathcal{C} \to F : x \mapsto N(x)$ is an injective ring homomorphism. Since $0 = q(x, y) = N(x + y) - N(x) - N(y)$ for all x, y in $\mathcal{C}$, ϕ is an additive homomorphism. We have $N(xy) = N(x)N(y)$ since $\mathcal{C}$ is a composition algebra so ϕ also preserves multiplication. Now if $x \in \ker\phi$, $N(x) = 0$. But we have assumed $q(x, y) = 0$ for all x and y so the nondegeneracy of N implies x must be zero. Then ϕ is an injective ring homomorphism. To complete the proof that $\mathcal{C}$ is a field, we need only show that every element has an inverse. We know that $N(x^2) = N(x)^2$ since N preserves composition. Also, $N(\alpha) = \alpha^2$ for all $\alpha \in F$ and so $N(x) \in F$ implies $N(N(x)) = N(x)^2$. Then $N(x^2 - N(x)) = N(x^2) - N(N(x)) = 0$, and ϕ injective implies $N(x) = x^2$ for all x in $\mathcal{C}$. So for all $x \in \mathcal{C}$, $x^{-1} = xN(x)^{-1}$ and $\mathcal{C}$ must be a field. Also, since x^2 is in F for every x in $\mathcal{C}$, $\mathcal{C}$ is purely inseparable over F. $\square$

Note that if the characteristic of F is not 2, the nondegeneracy of the quadratic form is equivalent to the nondegeneracy of the bilinear form since $N(x) = 2q(x, x)$. For the remainder of this paper, we will assume that the bilinear form is not identically zero. This assumption will allow us to assume that the bilinear form in a composition algebra is nondegenerate even if the characteristic of F is 2.

Lemma 3.1.5 *If the bilinear form $q(x, y)$ is not identically 0 in the composition algebra C, then the nondegeneracy of N is equivalent to the nondegeneracy of the bilinear form. In other words, if $q(x, y) = 0$ for every y in C, then $x = 0$.*

Proof. Suppose there exists a nonzero y such that $q(y, w) = 0$ for all $w \in C$. Since N is nondegenerate, $N(y) \neq 0$. Now set $x = 1$ in (3.2) so we have $0 = q(y, zy) = q(1, z)N(y)$. Then $q(1, z) = 0$ for all z in C. Setting $x = w = 1$ in (3.4) yields $q(1, zy) + q(y, z) = q(1, z)q(y, 1)$. But $q(1, z) = 0$ for all z so $q(y, z) = 0$ for all y, z in C. This contradicts the assumption that the bilinear form is not identically zero. Hence if $q(y, w) = 0$ for all w, then $y = 0$. $\square$

We now proceed with the structure of composition algebras in the case that the bilinear form not identically zero. We wish to show that the composition algebra C has an *involution*, that is, a linear map $^{-} : C \to C$ such that $\overline{(x+y)} = \overline{x} + \overline{y}$, $\overline{xy} = \overline{y}\,\overline{x}$, and $\overline{\overline{x}} = x$ for all x, y in C. In particular, we want an involution that satisfies the properties

$$x + \overline{x} \in F \cdot 1 \quad \text{and} \quad x\overline{x} \in F \cdot 1 \tag{3.8}$$

for all x in C. We will refer to $x + \overline{x} = T(x)$ as the *trace* and $x\overline{x} = N(x)$ as the *norm*. We will see that the norm is the quadratic form associated with the composition algebra. Note that since we require the involution to be linear, the trace will be linear and also the norm and trace will satisfy the equation $x^2 - T(x)x + N(x) \cdot 1 = 0$. Define a map $x \mapsto \overline{x}$ by $\overline{x} = q(1, x) \cdot 1 - x$. We have the following properties:

Lemma 3.1.6 *For all x, y in the composition algebra C with the map $^{-} : x \mapsto \overline{x}$ as defined above, we have the relations*

$$\overline{xy} = \overline{y}\,\overline{x} \tag{3.9}$$

$$\overline{x}x = N(x) \cdot 1 = x\overline{x} \tag{3.10}$$

$$\overline{x}(xy) = (\overline{x}x)y = N(x)y \tag{3.11}$$

$$(yx)\overline{x} = y(x\overline{x}) = yN(x) \tag{3.12}$$

Proof. We will need the following relations to prove the lemma:

$$q(xy, z) = q(x, z\overline{y}) = q(y, \overline{x}z). \tag{3.13}$$

We prove the first equality by direct computation:

$$\begin{aligned} q(x, z\overline{y}) &= q(x, zq(1, y) - zy) \\ &= q(x, zq(1, y)) - q(x, zy) \\ &= q(x, z)q(1, y) - q(x, zy) \\ &= [q(xy, z) + q(x, zy)] - q(x, zy) \\ &= q(xy, z) \end{aligned}$$

with the fourth equality following from (3.4). A similar computation shows $q(y, \overline{x}z) = q(xy, z)$, thus relation (3.13) holds. To prove relation (3.9), we first apply (3.13) repeatedly to obtain

$$\begin{aligned} q(\overline{xy}, z) &= q(\overline{xy} \cdot 1, z) = q(1, (xy)z) \\ &= q(\overline{z}, xy) \end{aligned}$$

$$= q(\overline{z}\,\overline{y}, x)$$

$$= q(\overline{y}, zx)$$

$$= q(\overline{y}\,\overline{x}, z).$$

From this we see that $q(\overline{xy} - \overline{y}\,\overline{x}, z) = 0$ for all z, but since the bilinear form is nondegenerate we have $\overline{xy} - \overline{y}\,\overline{x} = 0$ and we have shown relation (3.9). Next we let $y = 1$ in equation (3.3) and apply (3.13):

$$N(x)q(1, w) = q(x, xw) = q(\overline{x}x, w).$$

Since $N(x) \in F$, $N(x)q(1, w) = q(N(x) \cdot 1, w)$ so we have $q(N(x) \cdot 1, w) = q(\overline{x}x, w)$ for all w. Again using the nondegeneracy of the bilinear form, we obtain $N(x) = \overline{x}x$. Similarly we can show $N(x) = x\overline{x}$ by replacing x with 1 in (3.2) and applying (3.13), thus (3.10) has been shown. To prove (3.11), compare the relations

$$q(xw, xy) = q(w, \overline{x}(xy))$$

from (3.13) and

$$q(xw, xy) = N(x)q(w, y) = q(w, N(x)y)$$

which follows from (3.3) of Lemma 3.1.3. This implies $q(w, \overline{x}(xy)) = q(w, N(x)y)$ and so (3.11) follows from nondegeneracy of the bilinear form. One can prove (3.12) in a similar fashion. □

Clearly the map $^- : x \mapsto \overline{x}$ preserves addition. Relation (3.9) in the lemma shows $\overline{xy} = \overline{y}\,\overline{x}$, and we also have

$$\overline{\overline{x}} = q(1, \overline{x}) - \overline{x}$$

$$= q(1, q(1,x) - x) - (q(1,x) - x)$$

$$= q(1, q(1,x)) - q(1,x) - (q(1,x) - x)$$

$$= q(1,1)q(1,x) - 2q(1,x) + x = x$$

so our map is an involution. We wanted our involution to satisfy the properties in (3.8). Relation (3.10) in the previous lemma shows $N(x) \cdot 1 = x\overline{x} \in F \cdot 1$, and $T(x) \cdot 1 = x + \overline{x} = q(1,x) \cdot 1 \in F \cdot 1$ so properties in (3.8) are satisfied.

In addition to having an involution, composition algebras have another important property, but we need the following definition.

Definition 3.1.7 *An algebra A satisfying the left alternative law*

$$x^2 y = x(xy) \quad \text{for all } x, y \in A \tag{3.14}$$

and the right alternative law

$$yx^2 = (yx)x \quad \text{for all } x, y \in A \tag{3.15}$$

is an alternative *algebra.*

For x in the composition algebra C we have $x + \overline{x} = T(x) \cdot 1 \in F$. We compute

$$\overline{x}(xy) = (T(x) \cdot 1 - x)(xy) = T(x)xy - x(xy)$$

and

$$(\overline{x}x)y = (T(x) \cdot 1x - x^2)y = T(x)xy - x^2 y.$$

Relation (3.11) $\overline{x}(xy) = (\overline{x}x)y$ allows us to combine the two previous expressions and prove that C satisfies the left alternative law. With a similar computation one may use (3.12) $(yx)\overline{x} = y(x\overline{x})$ to show that C also satisfies the right alternative law. We have proved the following:

Proposition 3.1.8 *If C is a composition algebra, then C is alternative with involution $^- : x \mapsto \overline{x}$ such that $x\overline{x} = N(x) \cdot 1$ where $N(x)$ is the given quadratic form and $x + \overline{x} = T(x) \cdot 1$ with $T(x) \in F$.*

This proposition is only half of our main result on the structure of composition algebras. We will see that the converse of this statement is also true, that is, if we begin with an alternative algebra A with the conditions described in the proposition then A must be a composition algebra. However, to prove this, we will need some basic results on alternative algebras.

We denote the *associator* $(xy)z - x(yz)$ by (x, y, z). An algebra is associative if the associator is always 0. An algebra A is alternative if

$$(x, x, y) = (y, x, x) = 0$$

for all x, y in A. This is just the left and right alternative laws (3.14) and (3.15) written using the associator. The associators in alternative algebras have an important property:

Proposition 3.1.9 *Associators in alternative algebras are* alternating *in the sense that an associator does not change under an even permutation of its argument and changes sign under an odd permutation of its argument. In other words, for all x, y, z in the alternative algebra A we have*

$$(x, y, z) = -(y, x, z) = -(z, y, x) = (y, z, x) = -(x, z, y) = (z, x, y).$$

Proof. To prove this claim, it is sufficient to show $(x,y,z) = -(y,x,z) = (y,z,x)$. The first equality follows from the computation

$$\begin{aligned}(x,y,z)+(y,x,z) &= (x,x,z)+(x,y,z)+(y,y,z)+(y,x,z)\\ &= x^2z - x(xz) + (xy)z - x(yz) + y^2z - y(yz) + (yx)z - y(xz)\\ &= (x+y)^2z - (x+y)(xz+yz) = (x+y,x+y,z) = 0.\end{aligned}$$

The equality $(y,z,x)+(y,x,z) = 0$ can be shown using a similar computation, and we have shown that the associator is alternating in alternative algebras. We will use this fact to prove some basic identities for alternative algebras. □

Lemma 3.1.10 *In an alternative algebra A, we have the* flexible law

$$(xy)x = x(yx) \tag{3.16}$$

and the Moufang identities

$$(aya)x = a[y(ax)] \tag{3.17}$$

$$x(aya) = [(xa)y]a \tag{3.18}$$

$$(ax)(ya) = a(xy)a \tag{3.19}$$

for all x, y, and a in A.

Proof. The flexible law follows immediately from the fact that the associator is alternating: $(x,y,x) = -(y,x,x)$ which must be 0 since A is alternative. We can now write xyx to mean $(xy)x$ or $x(yx)$. To prove the first Moufang identity (3.17), we again use the fact that the associator is alternating to compute:

$$(axa)y = (ax,a,y) + (ax)(ay)$$

$$= (ax, a, y) + (a, x, ay) + a[x(ay)]$$

$$= -[(a, ax, y) + (a, ay, x)] + a[x(ay)]$$

$$= -[(a^2x)y - a[(ax)y] + (a^2y)x - a[(ay)x]] + a[x(ay)]$$

$$= -[(a^2, x, y) + (a^2, y, x) + a^2(xy) - a[(ax)y] + a^2(yx) - a[(ay)x]] + a[x(ay)]$$

$$= -[(a^2, x, y) - (a^2, x, y) + a(a, x, y) + a(a, y, x)] + a[x(ay)]$$

$$= -a[(a, x, y) - (a, x, y)] + a[x(ay)] = a[x(ay)].$$

The second Moufang identity (3.18) can be shown using a similar calculation. Note that identity (3.17) can be written in an equivalent form using associators

$$(a, ya, x) = (aya)x - a[(ya)x] = a[y(ax)] - a[(ya)x] = -a(y, a, x) = a(x, y, a).$$

We will use this form of the first Moufang identity to prove (3.19):

$$\begin{aligned}(ax)(ya) &= (a, x, ya) + a[x(ya)] \\ &= (a, x, ya) + a[x(ya)] - a(xy)a + a(xy)a \\ &= (a, x, ya) - a(x, y, a) + a(xy)a = a(xy)a.\end{aligned}$$

Thus we have shown that alternative algebras are flexible and satisfy the Moufang identities. □

Now we proceed with our proof of the converse of Proposition 3.1.8. Assume we have an alternative algebra A with identity and involution $^{-} : x \mapsto \overline{x}$ such that $\overline{x}x = N(x) \cdot 1$ and $x + \overline{x} = T(x) \cdot 1$ with both $N(x)$ and $T(x)$ in F. From the definition of $N(x)$ we see that $N(\alpha x) = \alpha^2 N(x)$. Also,

$$N(x + y) - N(x) - N(y) = (x + y)(\overline{x + y}) - x\overline{x} - y\overline{y} = x\overline{y} + y\overline{x} \qquad (3.20)$$

so $q(x, y)$ is a symmetric bilinear form and $N(x)$ is a quadratic form. We must show that $N(x)$ permits composition. Since $\overline{y} = T(y) \cdot 1 - y$ and A is alternative, we have

$$
\begin{aligned}
x(y\overline{y}) &= x[y(T(y) \cdot 1 - y)] \\
&= xyT(y) - xy^2 \\
&= xyT(y) - (xy)y \\
&= (xy)(T(y) \cdot 1 - y) = (xy)\overline{y}.
\end{aligned}
\tag{3.21}
$$

We now compute:

$$
\begin{aligned}
N(xy) &= (xy)(\overline{xy}) = (xy)(\overline{y}\,\overline{x}) \\
&= (xy)(\overline{y}(T(x) \cdot 1 - x)) \\
&= (xy)\overline{y}T(x) - (xy)(\overline{y}x) \\
&= x(y\overline{y})T(x) - x(y\overline{y})x \\
&= xN(y)T(x) - xN(y)x \\
&= x(T(x) - x)N(y) = x\overline{x}N(y) = N(x)N(y).
\end{aligned}
$$

The fourth equality follows from (3.21) and the Moufang identity (3.19). We formally state what we have shown:

Proposition 3.1.11 *If C is an alternative algebra with identity and involution $^- :$ $x \mapsto \overline{x}$ such that $\overline{x}x = N(x) \cdot 1$ and $x + \overline{x} = T(x) \cdot 1$ with both $N(x)$ and $T(x)$ in F, then C is a composition algebra.*

3.2 The Cayley-Dickson Doubling Process

Three examples of composition algebras that the reader is already familiar with are the complex numbers, Hamilton's quaternions, and the Cayley numbers; the fact that the norm form permits composition has already been shown. In this section we give a method for constructing composition algebras. This construction process can be thought of as a generalization of two familiar constructions, the first being the Hamilton's construction of the complex numbers as ordered pairs of real numbers and the second being Dickson's construction of the Cayley numbers in terms of the quaternions which was presented in Section 2.3.

As was first shown formally by Hamilton, the complex numbers can be thought of as ordered pairs of real numbers $u = (a, b) \in \mathbf{R} \times \mathbf{R}$. Recall that addition is naturally defined component-wise, and the product of two complex numbers (a_1, b_1) and (a_2, b_2) is defined by

$$(a_1, b_1)(a_2, b_2) = (a_1a_2 - b_1b_2, a_1b_2 + a_2b_1). \tag{3.22}$$

It is easily verified that this definition is equivalent to the usual definition of the product of $(a_1 + b_1i)(a_2 + b_2i)$. Compare this construction to Dickson's construction of the Cayley numbers given in Section 2.3. Dickson showed that every Cayley number could be written as $p + qe$ where $e^2 = -1$ and p, q are quaternions. We could just as easily write $p + qe$ as an ordered pair (p, q) and Dickson's definition of multiplication would be

$$(p_1, q_1)(p_2, q_2) = (p_1p_2 - \overline{q_2}q_1, q_2p_1 + q_1\overline{p_2}).$$

This is similar to (3.22) but with conjugates thrown in. It was Albert [1] who realized that Dickson's idea of taking a composition algebra and "doubling" it to obtain another composition algebra could be generalized to arbitrary fields. We now begin to describe this process, generally referred to as the Cayley-Dickson doubling process.

Suppose we have a nonassociative algebra $\mathcal{B}$ with identity and involution $^- : a \mapsto \overline{a}$ satisfying

$$x + \overline{x} = T(x) \in F \quad \text{and} \quad x\overline{x} = N(x) \in F \tag{3.23}$$

where $N(x)$ is a nondegenerate quadratic form. We will construct a new algebra $\mathcal{C}$ of twice the dimension of $\mathcal{B}$ having the same properties as $\mathcal{B}$ and having $\mathcal{B}$ as a subalgebra. Let $\mathcal{C}$ be the vector space of all ordered pairs (a, b) of elements of $\mathcal{B}$. Scalar multiplication and addition is defined component-wise, the usual direct sum vector space structure. Multiplication will be defined by

$$(a_1, b_1)(a_2, b_2) = (a_1a_2 + \mu\overline{b_2}b_1, b_2a_1 + b_1\overline{a_2}) \tag{3.24}$$

where μ is a nonzero element of F. This definition of multiplication makes it clear that $(1, 0)$ is an identity in $\mathcal{C}$. Also, since $(a_1, 0)(a_2, 0) = (a_1a_2, 0)$ we can identify $\mathcal{B}$ with the subalgebra $\mathcal{B}' = \{(a, 0)|a \in \mathcal{B}\}$ of $\mathcal{C}$. We define the map

$$^- : \mathcal{C} \to \mathcal{C} : (a, b) \mapsto \overline{(a, b)} = (\overline{a}, -b). \tag{3.25}$$

This map is F-linear and preserves addition since $a \mapsto \overline{a}$ is an involution in $\mathcal{B}$. We also have

$$\overline{\overline{(a, b)}} = \overline{(\overline{a}, -b)} = (\overline{\overline{a}}, -(-b)) = (a, b)$$

and

$$\overline{(a_2, b_2)}\,\overline{(a_1, b_1)} = (\overline{a_2}, -b_2)(\overline{a_1}, -b_1)$$
$$= (\overline{a_2}\,\overline{a_1} + \mu\overline{\overline{b_1}}b_2, -b_1\overline{a_2} - b_2 a_1)$$
$$= (\overline{a_1 a_2} + \mu\overline{\overline{b_2}b_1}, -b_2 a_1 - b_1\overline{a_2})$$
$$= \overline{(a_1, b_1)(a_2, b_2)}$$

so that (3.25) is an involution in $\mathcal{C}$. We compute

$$(a, b) + \overline{(a, b)} = (T(a), 0) = T(a)(1, 0) \in F \cdot 1_{\mathcal{C}} \tag{3.26}$$

and

$$(a, b)\overline{(a, b)} = (a, b)(\overline{a}, -b) = (N(a) - \mu N(b), -\overline{a}b + \overline{a}b)$$
$$= [N(a) - \mu N(b)](1, 0) \in F \cdot 1_{\mathcal{C}}. \tag{3.27}$$

The map $N((a, b)) = N(a) - \mu N(b)$ is a quadratic form because

$$N((\alpha a, \alpha b)) = N(\alpha a) - \mu N(\alpha b) = \alpha^2[N(a) - \mu N(b)] = \alpha^2 N((a, b))$$

and the associated bilinear form

$$q((a_1, b_1), (a_2, b_2)) = N((a_1 + a_2, b_1 + b_2)) - N((a_1, b_1)) - N((a_2, b_2))$$
$$= N(a_1 + a_2) - \mu N(b_1 + b_2) - N(a_1) + \mu N(b_1) - N(a_2) + \mu N(b_2)$$
$$= q(a_1, a_2) - \mu q(b_1, b_2)$$

is nondegenerate. To see why the bilinear form is nondegenerate, suppose for all (a_2, b_2) we have $q((a_1, b_1), (a_2, b_2)) = 0$. Then $q(a_1, a_2) = \mu q(b_1, b_2)$ for any choice of a_2, b_2 in $\mathcal{B}$ so we will assume $b_2 = 0$. We have $q(a_1, a_2) = 0$ for all a_2, so a_1 must be zero since the bilinear form is nondegenerate on $\mathcal{B}$. If we assume $a_2 = 0$, we see that $b_1 = 0$ by a similar argument. Therefore $q((a_1, b_1), (a_2, b_2)) = 0$ for all (a_2, b_2) implies $(a_1, b_1) = 0$ and so the bilinear form is nondegenerate on $\mathcal{C}$.

Thus we have constructed an algebra $\mathcal{C}$ with involution having the same properties as the algebra $\mathcal{B}$. We will call algebras constructed by applying the Cayley-Dickson doubling process *Cayley-Dickson algebras.* Next we prove that we have the following relationship between the algebraic properties of $\mathcal{B}$ and $\mathcal{C}$:

Proposition 3.2.1 *Suppose $\mathcal{C}$ is the Cayley-Dickson algebra constructed by doubling $\mathcal{B}$. Then*

1. *$\mathcal{C}$ is associative if and only if $\mathcal{B}$ is commutative and associative and*

2. *$\mathcal{C}$ is alternative if and only if $\mathcal{B}$ is associative.*

Proof. Before proving the proposition, we will write the associators $(x, y, z) = (xy)z - x(yz)$ of $\mathcal{C}$ in terms of the commutators and associators of $\mathcal{B}$. Here we use the notation $[x, y]$ for the commutator $xy - yx$. We calculate directly:

$$
\begin{aligned}
&\big((a_1, b_1), (a_2, b_2), (a_3, b_3)\big) \\
&\quad = \Big((a_2b_2)a_1 - a_2(b_2a_1) + \mu(\overline{b_3}(b_1a_2) - a_2(\overline{b_3}b_1) + \overline{b_3}(b_2\overline{a_1}) - (\overline{a_1}\,\overline{b_3})b_2 \\
&\qquad + (\overline{b_1}b_2)a_3 - (a_3\overline{b_1})b_2)\ ,\ b_3(a_2a_1) - (b_3a_1)a_2 + (b_1a_2)\overline{a_3} \\
&\qquad - (b_1\overline{a_3})a_2 + (b_2\overline{a_1})\overline{a_3} - b_2(\overline{a_3}\,\overline{a_1}) + \mu(b_3(\overline{b_1}b_2) - b_2(\overline{b_1}b_3))\Big) \\
&\quad = \Big((a_2, b_2, a_1) - \mu([\overline{b_3}b_1, a_2] - (\overline{b_3}, b_1, a_2) + [\overline{b_3}b_2, \overline{a_1}] - (\overline{b_3}, b_2, \overline{a_1}) - (\overline{a_1}, \overline{b_3}, b_2) \\
&\qquad + [\overline{b_1}b_2, a_3] - (a_3, \overline{b_1}, b_2)\ ,\ b_3[a_2, a_1] - (b_3, a_1, a_2) + b_1[a_2, \overline{a_3}] - (b_1, a_2, \overline{a_3}) \\
&\qquad + b_2[\overline{a_1}, \overline{a_3}] + (b_2, \overline{a_1}, \overline{a_3}) - \mu([b_2\overline{b_1}, b_3] + b_3[\overline{b_1}, b_2] + (b_2, \overline{b_1}, b_3))\Big).
\end{aligned}
\tag{3.28}
$$

Assume $\mathcal{C}$ is associative. Recall that all the associators in $\mathcal{C}$ must be zero so that the left side of (3.28) immediately reduces to 0. Also, since $\mathcal{B}$ is a subalgebra of $\mathcal{C}$, $\mathcal{B}$ must also be associative. Let b_1,b_2 be elements of $\mathcal{B}$. Setting $a_1 = a_2 = a_3 = 0$ and $b_3 = 1$ in (3.28), we find that $[b_1, b_2] = 0$ so that $\mathcal{B}$ is commutative. Conversely, when $\mathcal{B}$ is associative and commutative, all its associators and commutators must be zero so the right side of (3.28) immediately reduces to zero and we have $\big((a_1, b_1), (a_2, b_2), (a_3, b_3)\big) = 0$. Hence $\mathcal{C}$ is associative. This completes the proof of (1). To prove (2), we first assume that $\mathcal{C}$ is alternative. Then $\mathcal{B}$ must also be alternative since it is a subalgebra. From this we know that in $\mathcal{B}$, the associators must be alternating from Proposition 3.1.9 and we also have the flexible property $(x, y, x) = 0$ from Lemma 3.1.10. We will also make use of the following useful fact: in $\mathcal{B}$ we have $0 = (x, x, y) = (x, T(x) - \overline{x}, y) = (x, \overline{x}, y)$. Using these facts and the fact that $(x, y, z) + (x, y, \overline{z}) = 0$ and $[x, y] + [x, \overline{y}] = 0$ we compute from (3.28) with $a_1 = a_2$, $b_1 = b_2$, and $a_3 = 0$:

$$\begin{aligned}
\big((a_1, b_1), (a_1, b_1), (0, b_3)\big) &= \big((a_1, b_1, a_1) + \mu([\overline{b_3}b_1, a_1] - (\overline{b_3}, b_1, a_1) + [\overline{b_3}b_1, \overline{a_1}] \\
&\qquad -2(\overline{b_3}, b_1, \overline{a_1})\ ,\ b_3[a_1, a_1] - (b_3, a_1, a_1) \\
&\qquad +\mu((b_1, \overline{b_1}, b_3) - [b_1\overline{b_1}, b_3] - b_3[\overline{b_1}, b_1])\big) \\
&= \big((\overline{b_3}, b_2, a_1), 0\big).
\end{aligned}$$

Since $\mathcal{C}$ is alternative, this gives $(\overline{b_3}, b_2, a_1) = 0$, or equivalently for any a_1, b_1, b_3 in $\mathcal{B}$ $(a_1, b_1, b_3) = 0$ so that $\mathcal{B}$ must be associative. To prove the converse we note that $\mathcal{B}$ associative implies all associators in $\mathcal{B}$ are zero. Then given any (a_1, b_1), (a_3, b_3) in $\mathcal{C}$, from (3.28) with $a_2 = a_1$ and $b_2 = b_1$ we have

$$\begin{aligned}\big((a_1,b_1),(a_1,b_1),(a_3,b_3)\big) &= \big(\mu([\overline{b_3}b_1,a_1]+[\overline{b_3}b_1,\overline{a_1}]+[\overline{b_1}b_1,a_3])\ ,\ b_3[a_1,a_1] \\ &\qquad +b_1[a_1,\overline{a_3}]+b_1[\overline{a_1},\overline{a_3}]-\mu([b_1\overline{b_1},b_3]+b_3[\overline{b_1},b_1])\big) \\ &= \big(0,0\big)\end{aligned}$$

so that $\mathcal{C}$ must be alternative. $\square$

This proposition gives us an important result. Recall from Proposition 3.1.8 and 3.1.11 that $\mathcal{C}$ is a composition algebra if and only if $\mathcal{C}$ is alternative. Then by Proposition 3.2.1 $\mathcal{C}$ is a composition algebra if and only if $\mathcal{B}$ is associative. We formally state the result.

Corollary 3.2.2 *The Cayley-Dickson algebra $\mathcal{C}$ constructed by doubling $\mathcal{B}$ is a composition algebra if and only if $\mathcal{B}$ is associative.*

Before showing some examples of algebras constructed in this manner, we make a brief comment. Just as a complex number can be written as an ordered pair of real numbers (a,b) or as $a+bi$, at times we will prefer to write the elements of $\mathcal{C}$ in a different form. We have the subalgebra $\mathcal{B}' = \{(a,0)|a, \in \mathcal{C}\}$ isomorphic with $\mathcal{B}$. Let $l = (0,1)$ so that $l^2 = \mu \cdot 1_{\mathcal{C}}$ and we have that $\mathcal{C}$ is the direct sum $\mathcal{B}' \oplus \mathcal{B}'l$. Written this way the elements x of $\mathcal{C}$ are of the form $x = a + bl$ with a, b in $\mathcal{B}$ and multiplication (3.24) is given by

$$(a_1+b_1l)(a_2+b_2l) = (a_1a_2+\mu\overline{b_2}b_1)+(b_2a_1+b_1\overline{a_2})l.$$

The involution defined in (3.25) becomes

$$x \mapsto \overline{x} : a+bl \mapsto \overline{a} - bl$$

and we also have the trace (3.26) and norm (3.27)

$$T(a+bl) = T(a) \qquad \text{and} \qquad N(a+bl) = N(a) - \mu N(b).$$

3.3 A Generalization of Hurwitz's Theorem

Examples of Composition Algebras

We wish to determine all composition algebras, so we begin this section with a description of the composition algebras constructed with the Cayley-Dickson doubling process. The process is a little smoother in the case where the characteristic of F is not 2, so we will examine this case first.

We begin by taking $\mathcal{B}$ to be the field F. Remember our only requirement for $\mathcal{B}$ was to be a nonassociative algebra with identity and involution such that $x\overline{x} = N(x)$ is a nondegenerate quadratic form. F trivially satisfies these requirements with $N(\alpha) = \alpha\overline{\alpha} = \alpha^2$. We double F to obtain our first example A_1 with basis $\{1, i_1\}$ where $i_1 = (0,1)$ and $A_1 = F \oplus F \cdot i_1$. Multiplication is completely described by

$$i_1^2 = \mu_1 1_{A_1}.$$

Let $x_1 = \alpha_0 + \alpha_1 i_1 \in A_1$. Then the involution is given by

$$\overline{x_1} = \overline{\alpha_0} - \alpha_1 i_1 = \alpha_0 - \alpha_1 i_1$$

so that

$$N(x_1) = N(\alpha_0) - \mu_1 N(\alpha_1) = {\alpha_0}^2 - \mu_1 {\alpha_1}^2$$

Note that this algebra is both commutative and associative. We will refer to this two dimensional algebra as a *quadratic* algebra. Since A_1 is a composition algebra, we can compute a composition law. If we take $x = \alpha_0 + \alpha_1 i_1$ and $y = \beta_0 + \beta_1 i_1$ then $xy = (\alpha_0\beta_0 + \mu_1\alpha_1\beta_1) + (\alpha_0\beta_1 + \alpha_1\beta_0)i_1$ so that $N(x)N(y) = N(xy)$ gives

$$(\alpha_0{}^2 - \mu_1\alpha_1{}^2)(\beta_0{}^2 - \mu_1\beta_1{}^2) = (\alpha_0\beta_1 + \mu_1\alpha_1\beta_0)^2 - \mu_1(\alpha_0\beta_1 + \alpha_1\beta_0)^2.$$

The Two Squares Identity discussed in Section 2.1 is a special case of this formula where the field F is the field of real numbers and $\mu_1 = -1$. According to van der Blij, the general version of the Two Squares Identity occurs in Indian mathematics for special values of μ_1 and was used by Euler in the theory of Pell's equation.

For the next example, we double A_1 to obtain $A_2 = A_1 \oplus A_1 i_2$ where $i_2 = (0, 1)$ and $i_2^2 = \mu_2 \in F$ is the parameter used in defining multiplication. A_2 has basis $\{1, i_1, i_2, i_3\}$ where $i_3 = i_1 i_2$. Using the definition (3.24) of multiplication one finds that $i_1 i_2 = -i_2 i_1$. A complete multiplication table for the basis elements can be computed from the relations

$$i_1^2 = \mu_1 1_{A_2}, \qquad i_2^2 = \mu_2 1_{A_2}, \qquad \text{and} \qquad i_1 i_2 = -i_2 i_1$$

and the fact that A_2 is associative. We will refer to these relations as Hamilton's relations. Four dimensional algebras whose basis elements satisfy these relations are the *generalized quaternions.* Note that Hamilton's quaternions are the special case where F is the field of real numbers and $\mu_1 = \mu_2 = -1$. Since A_1 is both commutative and associative, by Proposition 3.2.1 A_2 must be associative but cannot be commutative because $i_1 i_2 = -i_2 i_1$. Next we compute the involution and quadratic form for the generalized quaternion algebra A_2. Let $x_2 \in A_2$. We can write $x_2 = \alpha_0 + \alpha_1 i_1 + \alpha_2 i_2 + \alpha_3 i_3 = (\alpha_0 + \alpha_1 i_1) + (\alpha_2 + \alpha_3 i_1)i_2$, so the involution is

$$\overline{x_2} = \overline{\alpha_0 + \alpha_1 i_1} - (\alpha_2 + \alpha_3 i_1)i_2 = \alpha_0 - \alpha_1 i_1 - \alpha_2 i_2 - \alpha_3 i_3$$

and the norm map is given by

$$N(x_2) = N(\alpha_0 + \alpha_1 i_1) - \mu_2 N(\alpha_2 + \alpha_3 i_1) = {\alpha_0}^2 - \mu_1 {\alpha_1}^2 - \mu_2 {\alpha_2}^2 + \mu_2 \mu_1 {\alpha_3}^2.$$

Direct computation yields the formula for the product of two quaternions:

$$\begin{aligned}
&(\alpha_0 + \alpha_1 i_1 + \alpha_2 i_2 + \alpha_3 i_3)(\beta_0 + \beta_1 i_1 + \beta_2 i_2 + \beta_3 i_3 + \beta_4 i_4) \\
&\quad = (\alpha_0\beta_0 + \mu_1\alpha_1\beta_1 + \mu_2\alpha_2\beta_2 - \mu_1\mu_2\alpha_3\beta_3) + (\alpha_0\beta_1 + \alpha_1\beta_0 - \mu_2\alpha_2\beta_3 + \mu_2\alpha_3\beta_2)i_1 \\
&\qquad + (\alpha_0\beta_2 + \alpha_2\beta_1 - \mu_1\alpha_1\beta_3 - \mu_1\alpha_3\beta_1)i_2 + (\alpha_0\beta_3 + \alpha_3\beta_0 + \alpha_1\beta_2 - \alpha_2\beta_1)i_3.
\end{aligned}$$

Applying the fact that the norm permits composition to this formula and the formula for the norm, one can compute a law of composition as done for quadratic algebras:

$$\begin{aligned}
&({\alpha_0}^2 - \mu_1{\alpha_1}^2 - \mu_2{\alpha_2}^2 + \mu_2\mu_1{\alpha_3}^2)({\beta_0}^2 - \mu_1{\beta_1}^2 - \mu_2{\beta_2}^2 + \mu_2\mu_1{\beta_3}^2) \\
&\quad = (\alpha_0\beta_0 + \mu_1\alpha_1\beta_1 + \mu_2\alpha_2\beta_2 - \mu_1\mu_2\alpha_3\beta_3)^2 + \mu_1(\alpha_0\beta_1 + \alpha_1\beta_0 - \mu_2\alpha_2\beta_3 + \mu_2\alpha_3\beta_2)^2 \\
&\qquad + \mu_2(\alpha_0\beta_2 + \alpha_2\beta_1 - \mu_1\alpha_1\beta_3 - \mu_1\alpha_3\beta_1)^2 + \mu_2\mu_1(\alpha_0\beta_3 + \alpha_3\beta_0 + \alpha_1\beta_2 - \alpha_2\beta_1)^2.
\end{aligned}$$

In the special case where F is the field of real numbers, this composition law gives a generalization of the Four Squares Theorem that was known to Lagrange as early as 1770.

In our last example in the case the characteristic of F is not 2 we double A_2 to obtain $A_3 = A_2 \oplus A_2 i_4$ where $i_4^2 = \mu_3$. Since A_2 is not commutative, by Proposition 3.2.1 A_3 cannot be associative. But then Corollary 3.2.2 implies the double of A_3 cannot be a composition algebra. So A_3 is the last composition algebra we can obtain by the Cayley-Dickson doubling process. Now the basis of A_3 is $\{1, i_1, i_2, i_3, i_4, i_5, i_6, i_7\}$ where $i_3 = i_1 i_2$, $i_5 = i_1 i_4$,$i_6 = i_2 i_4$, and $i_7 = i_3 i_4$. These eight dimensional algebras are called the *Cayley algebras* since they are a generalization of the Cayley numbers

	i_1	i_2	i_3	i_4	i_5	i_6	i_7
i_1	$\mu_1 \cdot 1$	i_3	$\mu_1 i_2$	i_5	$\mu_1 i_4$	$-i_7$	$-\mu_1 i_6$
i_2	$-i_3$	$\mu_2 \cdot 1$	$-\mu_2 i_1$	i_6	i_7	$\mu_2 i_4$	$\mu_2 i_5$
i_3	$-\mu_1 i_2$	$\mu_2 i_1$	$-\mu_1\mu_2 \cdot 1$	i_7	$\mu_1 i_6$	$-\mu_2 i_5$	$-\mu_1\mu_2 i_4$
i_4	$-i_5$	$-i_6$	$-i_7$	$\mu_3 \cdot 1$	$-\mu_3 i_1$	$-\mu_3 i_2$	$\mu_3 i_3$
i_5	$-\mu_1 i_4$	$-i_7$	$-\mu_1 i_6$	$\mu_3 i_1$	$-\mu_1\mu_3 \cdot 1$	$\mu_3 i_3$	$\mu_2\mu_3 i_2$
i_6	i_7	$-\mu_2 i_4$	$\mu_2 i_5$	$\mu_3 i_2$	$-\mu_3 i_3$	$-\mu_2\mu_3 \cdot 1$	$-\mu_2\mu_3 i_1$
i_7	$-i_6$	i_5	i_4	$-i_3$	$-i_2$	i_1	$\mu_1\mu_2\mu_3 \cdot 1$

Table 3.1: Cayley Algebra Multiplication

over the field of real numbers with $\mu_1 = \mu_2 = \mu_3 = -1$. We pointed out in the previous example that i_1, i_2, and i_3 satisfy Hamilton's relations. Using the definition of multiplication one can also show that each set of triples $\{i_1, i_4, i_5\}$ and $\{i_2, i_4, i_6\}$ also satisfy the Hamilton relations:

$$i_1^2 = \mu_1 1_{A_3}, \quad i_2^2 = \mu_2 1_{A_3}, \quad \text{and} \quad i_2 i_1 = -i_3,$$

$$i_1^2 = \mu_1 1_{A_3}, \quad i_4^2 = \mu_3 1_{A_3}, \quad \text{and} \quad i_4 i_1 = -i_5,$$

$$i_2^2 = \mu_2 1_{A_3}, \quad i_4^2 = \mu_3 1_{A_3}, \quad \text{and} \quad i_4 i_2 = -i_6.$$

Using these relations and the fact that A_3 is alternative one can construct a multiplication table for the basis elements. Given $a_3 \in A_3$ we can write $a_3 = \alpha_0 + \alpha_1 i_1 + \alpha_2 i_2 + \alpha_3 i_3 + \alpha_4 i_4 + \alpha_5 i_5 + \alpha_6 i_6 + \alpha_7 i_7 = (\alpha_0 + \alpha_1 i_1 + \alpha_2 i_2 + \alpha_3 i_3) + (\alpha_4 + \alpha_5 i_1 + \alpha_6 i_2 + \alpha_7 i_3) i_4$. Then the involution on A_3 is given by

$$\begin{aligned} \overline{a_3} &= \overline{(\alpha_0 + \alpha_1 i_1 + \alpha_2 i_2 + \alpha_3 i_3)} - (\alpha_4 + \alpha_5 i_1 + \alpha_6 i_2 + \alpha_7 i_3) i_4 \\ &= \alpha_0 - \alpha_1 i_1 - \alpha_2 i_2 - \alpha_3 i_3 - \alpha_4 i_4 - \alpha_5 i_5 - \alpha_6 i_6 - \alpha_7 i_7. \end{aligned}$$

The norm is

$$N(a_3) = N(\alpha_0 + \alpha_1 i_1 + \alpha_2 i_2 + \alpha_3 i_3) - \mu_3 N(\alpha_4 + \alpha_5 i_1 + \alpha_6 i_2 + \alpha_7 i_3)$$
$$= {\alpha_0}^2 - \mu_1 {\alpha_1}^2 - \mu_2 {\alpha_2}^2 + \mu_2\mu_1 {\alpha_3}^2 - \mu_3 {\alpha_4}^2 + \mu_1\mu_3 {\alpha_5}^2 + \mu_2\mu_3 {\alpha_6}^2 - \mu_1\mu_2\mu_3 {\alpha_7}^2.$$

We could also compute the composition law for Cayley algebras using the formula for the norm and the formula for the product of two elements in the Cayley algebra but will not because of the length of the formulas. This composition law gives an extension of the Eight Squares Identity for real numbers that was discovered by Graves by trial and error only a month after his discovery of the Cayley numbers.

This iterative process can be generalized to include the case where the characteristic of F is 2; instead of beginning with the field F we begin with the two-dimensional algebra $F[\lambda]/(\lambda^2 - \lambda + \alpha)$ where $4\alpha \neq 1$, together with the quadratic form $N(a + bl) = a^2 + ab + b^2\alpha$ where $l = \lambda + (\lambda^2 - \lambda + \alpha)$. We will also refer to this algebra as a quadratic algebra, but this algebra is defined for a field F of any characteristic. The quadratic algebras defined earlier for Char$F \neq 2$ were a special case; these algebras are isomorphic via the map defined by $i_1 \mapsto l - \frac{1}{2} \cdot 1$. We will show that these general quadratic algebras for case Char$F = 2$ have an involution which satisfies properties (3.23). Define a map $^{-} : a + bl \mapsto \overline{a + bl}$ by $\overline{a + bl} = a + b(1 - l)$. Clearly $\overline{(a_1 + b_1 l) + (a_2 + b_2 l)} = \overline{(a_1 + b_1 l)} + \overline{(a_2 + b_2 l)}$. Also,

$$\overline{l^2} = \overline{l - \alpha} = 1 - l - \alpha = 1 - 2l + (l - a) = 1 - 2l + l^2 = (1 - l)^2 = \bar{l}^2$$

so that

$$\overline{(a_1 + b_1 l)(a_2 + b_2 l)} = a_1 a_2 + (a_1 b_2 + a_2 b_1)\bar{l} + b_1 b_2 \overline{l^2}$$

$$= a_1a_2 + (a_1b_2 + a_2b_1)\bar{l} + b_1b_2\bar{l}^2$$

$$= (a_1 + b_1\bar{l})(a_2 + b_2\bar{l})$$

$$= \overline{(a_1 + b_1 l)}\,\overline{(a_2 + b_2 l)}.$$

We have $\overline{\overline{a+bl}} = \overline{a + b(1-l)} = a + b(1-(1-l)) = a + bl$. Then $^- : a + bl \mapsto \overline{a+bl} = a + b(1-l)$ is an involution. Straightforward computations show that $x + \overline{x}$ and $x\overline{x}$ are in F: $(a + bl) + (a + b(1-l)) = 2a + b = b \in F$ and $(a + bl)(a + b(1-l)) = a^2 + ab + b^2 - b^2l^2 = a^2 + ab + b^2l - b^2(l - \alpha) = a^2 + ab + b^2\alpha \in F$. Also, since $F[\lambda]/(\lambda^2 - \lambda + \alpha)$ is isomorphic to either $F \oplus F$ or $F(l)$ depending on whether $\lambda^2 - \lambda + \alpha$ is reducible in $F[\lambda]$, it is associative. Then we can apply the Cayley-Dickson doubling process to $F[\lambda]/(\lambda^2 - \lambda + \alpha)$ to obtain a composition algebra of degree four, and again to obtain a composition algebra of degree eight. We will refer to the double of the quadratic algebra defined for a field of any characteristic as a generalized quaternion algebra, and the double of a generalized quaternion algebra defined for a field of any characteristic as a Cayley algebra.

Classification of Composition Algebras

We have shown that the algebras listed above are composition algebras. It turns out that in fact the field F and the algebras described above are the only composition algebras when the bilinear form is not identically zero. Before proceeding to show this, we pause to review a few definitions and a theorem on the orthogonal decomposition of bilinear spaces.

Recall the definition that if W is a subspace of V, the *orthogonal space* $W^\perp$ is the set of all vectors v in V such that $q(v, w) = 0$ for every w in W. Also recall that a vector v is *isotropic* if $q(v, v) = 0$ and that a space V is *isotropic* if V contains an isotropic vector. We say a subspace is *totally isotropic* if $q(w_1, w_2) = 0$ for all w_1, w_2 in W. Note then that a subspace W is nonisotropic if and only if $W \cap W^{\perp} = 0$. In other words, W does not contain any vectors that are perpendicular to all other vectors. We point out the following result on the orthogonal decomposition of bilinear spaces ([2], 117; [23], 7): If W is a nonisotropic subspace of a space V then we can write $V = W \oplus W^{\perp}$ where $W^{\perp}$ is also nonisotropic.

In our proof of the classification theorem for composition algebras we will use the following lemma repeatedly.

Lemma 3.3.1 *Let $\mathcal{C}$ be a composition algebra that contains a proper algebra B that is nonisotropic. Then $\mathcal{C}$ contains a larger subalgebra A obtained from B by applying the Cayley-Dickson doubling process that is also nonisotropic.*

Proof. With B nonempty and nonisotropic, by the remarks preceding the lemma we can decompose $\mathcal{C}$ as $B \oplus B^{\perp}$. Also, we can find l in $B^{\perp}$ such that $N(l) = \mu \neq 0$. We have $q(1, l) = l + \bar{l}$ but since l is orthogonal to 1, $q(1, l)$ must be zero so $\bar{l} = -l$. This gives $l^2 = -l\bar{l} = -N(l) \cdot 1 = -\mu \cdot 1$. We also have $q(x, l) = \bar{x}l + \bar{l}x$ for all $x \in \mathcal{C}$, but then if x is in B $q(x, l) = 0$ so that

$$\bar{x}l = -\bar{l}x = lx \tag{3.29}$$

for all $x \in B$. Consider the subspace $Bl = \{xl | x \in B\}$, and let $A = B + Bl$. Take x, y in B. Then $\bar{y}x$ is in B and since $\mathcal{C}$ is a composition algebra, we can apply (3.13) of Lemma 3.1.6 to compute $q(x, yl) = q(\bar{y}x, l)$ which must be 0 by (3.29). This shows that the subspace Bl is orthogonal to B so that $Bl \cap B$ is 0 and therefore A is the orthogonal direct sum of B and Bl. Again using relation (3.13) of Lemma 3.1.6, we have $q(xl, yl) = q((xl)\bar{l}, y)$ and since $\bar{l} = -l$ this is $q(x(-l^2), y) = \mu q(x, y)$ so that $q(xl, yl) = \mu q(x, y)$. Using this equality we see that if $xl = yl$, then $\mu q(x, y) = q(xl, yl) = q(xl, xl) = 2\mu N(x) = \mu q(x, x)$ and the nondegeneracy of the quadratic form gives $x = y$ so map $x \mapsto xl$ of B onto Bl is injective. So B and Bl are isomorphic vector spaces. Also from the equality $q(xl, yl) = \mu q(x, y)$ we see that since B is nonisotropic then Bl must be nonisotropic: B is nonisotropic means if $x = y$ then $q(x, y) \neq 0$, but then $q(xl, yl) \neq 0$ so that Bl must be nonisotropic also. Next we will need to compute the product of two elements of A and show the multiplication in $\mathcal{C}$ matches the multiplication given by the definition of the product in the Cayley Dickson double of B. Before proceeding with this, we derive a relation that we will need for this calculation. We have $x(\bar{x}y) = N(x)\bar{y}$ from Lemma 3.1.6; we replace x with $a + \bar{l}$ and y with b to obtain $a(l\bar{b}) - l(\bar{a}\,\bar{b}) = 2q(a, \bar{l})\bar{b}$. But $q(a, l) = 0$ for all $a \in B$, so $a(l\bar{b}) = l(\bar{a}\,\bar{b})$ for all a, $b \in B$. Since $xl = l\bar{x}$ (3.29), $a(l\bar{b}) = a(bl)$ and $l(\bar{a}\,\bar{b}) = (ba)l$ so we have the desired relation

$$a(bl) = (ba)l. \tag{3.30}$$

Now we compute the product of $a_1 + b_1 l$, $a_2 + b_2 l$ in A:

$$(a_1 + b_1 l)(a_2 + b_2 l) = a_1 a_2 + a_1(b_2 l) + (b_1 l)a_2 + (b_1 l)(b_2 l). \tag{3.31}$$

We have

$$a_1(b_2 l) = (b_2 a_1)l \tag{3.32}$$

directly from (3.30). From the same relation (3.30) we also have $\overline{a_2}(b_1 l) = (b_1 \overline{a_2})l$, and by applying the involution to this equality and then using (3.29), we obtain

$$(b_1 l)a_2 = (b_1 \overline{a_2})l. \tag{3.33}$$

We can use (3.29) and the Moufang identity to simplify the last term in (3.31):

$$(b_1 l)(b_2 l) = (l\overline{b_1})(b_2 l) = l(\overline{b_1} b_2)l = (\overline{\overline{b_1} b_2})l^2 = \mu(\overline{b_2} b_1). \tag{3.34}$$

Use (3.32), (3.33), and (3.34) in (3.31) to obtain

$$(a_1 + b_1 l)(a_2 + b_2 l) = a_1 a_2 + (b_1 \overline{a_2})l + (b_1 \overline{a_2})l + \mu(\overline{b_2} b_1).$$

So the multiplication in A matches the multiplication in the double of B. Also, $\overline{a + bl} = \overline{a} - l\overline{b} = \overline{a} - bl$ so the involution matches the involution defined in the construction of the double of B. We have shown that A is a subalgebra of C obtained by doubling B that satisfies the same conditions as B. □

We pause for a remark on the lemma. In the lemma we assumed that our composition algebra had a nonisotropic subalgebra, and from this we obtained the element l which was used in constructing the Cayley-Dickson subalgebra. The proof also shows that if you assume you have an element l with nonzero norm which is orthogonal to 1, and l has the property that $q(b, l) = 0$ for all b in some subalgebra B, then $B + Bl$ is a Cayley-Dickson subalgebra of the composition algebra C. We will have the opportunity to use this rewording of the lemma later.

Now we can prove our classification theorem for composition algebras.

Theorem 3.3.2 (Generalized Hurwitz Theorem) *Let C be a composition algebra over the field F. Then C is one of the following: $F \cdot 1$, a quadratic algebra, a* *generalized quaternion algebra, a Cayley algebra, or if the characteristic of F is 2, a purely inseparable field such that $N(x) = x^2$ for x in $\mathcal{C}$.*

Proof: We first address the case where the characteristic of F is not 2. Suppose we are given a composition algebra $\mathcal{C}$ equipped with a nondegenerate quadratic form N. The subalgebra $F \cdot 1$ is nonisotropic in $\mathcal{C}$, so if $\mathcal{C} \neq F$, by Proposition 3.3.1 $\mathcal{C}$ contains a nonisotropic subalgebra A_1, a quadratic algebra, obtained by doubling $F \cdot 1$. If $\mathcal{C} \neq A_1$, then we may apply the proposition again so that $\mathcal{C}$ contains a quaternion algebra A_2 obtained by doubling A_1. If A_2 is not all of $\mathcal{C}$, we can double A_2 to obtain a Cayley algebra A_3 that is contained in $\mathcal{C}$. If $\mathcal{C} \neq A_3$, $\mathcal{C}$ must contain the double of A_3. But as already discussed, Cayley algebras are not associative so their double cannot be alternative. So if $\mathcal{C}$ contains the double of A_3, the alternative algebra $\mathcal{C}$ contains a subalgebra that is not alternative. This contradiction means that $\mathcal{C}$ must be a Cayley algebra.

We now assume the characteristic of F is 2. Recall from Proposition 3.1.4 that if $\mathcal{C}$ is a composition algebra such that the bilinear form is identically zero then $\mathcal{C}$ is a purely inseparable extension field of F. So suppose we are given a composition algebra $\mathcal{C}$ equipped with a nondegenerate quadratic form N and a bilinear form that is not identically zero. Since the bilinear form is not identically zero, by Lemma 3.1.5 the nondegeneracy of N is equivalent to the nondegeneracy of the bilinear form. The proof given for characteristic of F not 2 cannot work here because the subspace $F \cdot 1$ is isotropic in $\mathcal{C}$ when characteristic of F is 2, but we do wish to do something similar. Instead of starting the argument with the subspace $F \cdot 1$ and applying Lemma 3.3.1, we will begin the argument with a quadratic algebra, but we must show that $\mathcal{C}$ contains a quadratic subalgebra that is nonisotropic. Since the bilinear form is nondegenerate, there exists x in $\mathcal{C}$ such that $q(x, 1_{\mathcal{C}}) = \alpha$ where α is nonzero. Since $q(\alpha^{-1}x, 1_{\mathcal{C}}) = 1$, we might as well assume $q(x, 1_{\mathcal{C}}) = 1$. We claim $F + Fx$ is a subalgebra of $\mathcal{C}$: we have

$$(\alpha + \beta x)(\gamma + \delta x) = \alpha\gamma + (\alpha\delta + \beta\gamma)x + \beta\delta x^2$$

and since $q(x, 1_{\mathcal{C}}) = T(x) = 1$, $x + \overline{x} = 1$ so $x^2 = -x\overline{x} + x \in F + Fx$ and $(\alpha+\beta x)(\gamma + \delta x) \in F + Fx$. We will show that $F + Fx$ is nonisotropic by contradiction. Assume that $F + Fx$ is isotropic; then there exists α and β in F such that $q(\alpha + \beta x, x) = 0$ and $q(\alpha + \beta x, 1_{\mathcal{C}}) = 0$. Then

$$q(\alpha + \beta x, x) = \alpha q(1_{\mathcal{C}}, x) + \beta q(x, x) = \alpha q(1_{\mathcal{C}}, x) = 0$$

and

$$q(\alpha + \beta x, 1_{\mathcal{C}}) = \alpha q(1_{\mathcal{C}}, 1_{\mathcal{C}}) + \beta q(x, 1_{\mathcal{C}}) = \beta q(1_{\mathcal{C}}, x) = 0$$

so we see that α and β must be zero. This algebra is isomorphic to the general quadratic algebra defined at the end of section 3.3. Thus we have shown that $\mathcal{C}$ contains a nonisotropic quadratic subalgebra. The theorem follows by applying Lemma 3.3.1 as done in the case for characteristic of F not 2. $\square$

3.4 Split Algebras and Division Algebras

We can give a more detailed classification of composition algebras if we analyze them in terms of split algebras and division algebras. We will see that the split composition algebras are unique up to isomorphism for each degree. For division algebras, we will show a way to determine when two Cayley-Dickson doubles of the same composition algebra are isomorphic.

Recall that Hamilton's quaternions and the Cayley numbers presented in the first portion of this paper are division algebras. In fact, any composition algebra $\mathcal{C}$ over a field F is a division algebra if and only if the norm $N(x)$ is nonzero for all nonzero x in $\mathcal{C}$. Clearly $\mathcal{C}$ has zero divisors if there exists $x \neq 0$ such that $N(x) = 0$ since $N(x) = x\overline{x}$. Conversely, given any x in $\mathcal{C}$, if $N(x) \neq 0$ we can always take x^{-1} as $\overline{x}/N(x)$ so that every x is invertible. Composition algebras that contain zero divisors are called *split* composition algebras.

Proposition 3.4.1 *A composition algebra is a division algebra if and only if the norm form is nonisotropic.*

For any field F we can construct a composition algebra of degree 2, 4, or 8 that contains zero divisors. For characteristic of F not 2, we can just apply the Cayley-Dickson doubling process to F and take $\mu_i = 1$ at each step. The following proposition tells us when the double of a composition algebra is a division algebra and when it is split.

Proposition 3.4.2 *The Cayley-Dickson algebra $\mathcal{C} = B \oplus Bl$ where $l^2 = \mu$ is a division algebra if and only if B is a division algebra and $\mu \neq N(b)$ for some $b \in B$.*

Proof. Recall that the norm in the Cayley-Dickson double $B \oplus Bl$, with $l^2 = \mu \in F$, is $N(a + bl) = N(a) - \mu N(b)$. Note that if B is split, we can find a, b in B such that $N(a) = 0 = N(b)$ so that there exists $a + bl \in B \oplus Bl$ with zero norm. Then if B is split, the double of B must also be split for any choice of $\mu \in F$. Suppose now that

B is a division algebra. If $N(a+bl)=0$, $\mu = N(a)N(b)^{-1} = N(a)N(b^{-1}) = N(ab^{-1})$ so that μ is the norm of an element of B. Conversely, if $\mu = N(b)$ for some $b \in B$, then $N(b+l) = N(b) - \mu N(1) = 0$. So the Cayley-Dickson double of B is split if and only if μ is the norm of an element of B. □

In the previous section we showed that all composition algebras are either F, quadratic algebras, quaternions, or Cayley algebras. The main goal of this section is to further describe the classification of all composition algebras when the characteristic of F is not two 2 by analyzing the split and division algebras in each case. We will see that there are many division algebras, but there is a unique split composition algebra for each degree 2, 4, and 8. Although the results are still true in the case where characteristic of F is 2, the proofs are beyond the scope of this paper. Throughout this last section we will assume that the characteristic of F is not 2 and refer the reader to the work of Blij and Springer [4] for a discussion of the case where characteristic of F is 2.

In the proofs that follow, we will have the opportunity to use a certain decomposition for composition algebras in the special case the characteristic of F is not 2. Recall the discussion regarding the orthogonal decomposition of a bilinear space preceding Lemma 3.3.1. Here we consider the subspace $F \cdot 1$ of $\mathcal{C}$. For any nonzero $\alpha \in F$, $q(\alpha, 1) = \alpha q(1,1) = 2\alpha \neq 0$. So $(F \cdot 1) \cap (F \cdot 1)^{\perp} = 0$. Then we can write $\mathcal{C} = (F \cdot 1) \oplus \mathcal{C}_0$ where $\mathcal{C}_0 = (F \cdot 1)^{\perp}$, so any x in $\mathcal{C}$ can be written as $\alpha \cdot 1 + x_0$ where $\alpha \in F$ and $x_0 \in \mathcal{C}_0$. Note that from our definition $\overline{x} = q(1,x) \cdot 1 - x$ we have $\overline{x_0} = q(1, x_0) \cdot 1 - x_0 = -x_0$, so $\overline{\alpha \cdot 1 + x_0} = \alpha \cdot 1 - x_0$. Had we assumed that the characteristic of F was not 2 in the beginning, we could have defined our involution this way in the start.

Before proceeding to focus on split algebras and division algebras, we need a way to determine when two composition algebras are the same, precisely meaning that there is an isomorphism between the algebras that preserves both the algebra structure and the norm form. We say two norm forms N and N' are *equivalent* if there exists an injective linear mapping $f : \mathcal{C} \to \mathcal{C}'$ such that $N'(f(x)) = N(x)$ for all $x \in \mathcal{C}$. The proof will show that any algebra isomorphism between composition algebras must preserve the norm. Conversely, any injective linear mapping between two composition algebras that preserves the norm must also preserve the algebra multiplication.

Proposition 3.4.3 *Assume that the characteristic of F is not 2. Two composition algebras $\mathcal{C}$ and $\mathcal{C}'$ are isomorphic as algebras if and only if their corresponding norm forms N and N' are equivalent.*

Proof. Suppose we have an algebra isomorphism $\eta : \mathcal{C} \to \mathcal{C}'$. To show N and N' are equivalent, we must show that $N'(\eta(x)) = N(x)$ for all $x \in \mathcal{C}$. First we note that x is in the subspace $\mathcal{C}_0 = \{x \in \mathcal{C} | q(x, 1) = 0\}$ if and only if $x^2 \in F \cdot 1$ but $x \notin F \cdot 1$. To see this, take nonzero x in $\mathcal{C}$ and write $x = \alpha \cdot 1 + x_0$ where $\alpha \in F$ and $x_0 \in \mathcal{C}_0$. If $x \in \mathcal{C}_0$, then $\alpha = 0$ and $x = x_0 \neq 0$. So $x \notin F \cdot 1$. Since $\overline{x_0} = -x_0$, if $x \in \mathcal{C}_0$, we have

$$x^2 = x_0^2 = -x_0\overline{x_0} = -N(x_0) \cdot 1 \in F \cdot 1. \tag{3.35}$$

To show the converse of the statement, suppose $x \notin F \cdot 1$ and $x^2 \in F \cdot 1$. Then since

$$x^2 = (\alpha \cdot 1 + x_0)^2 = \alpha^2 \cdot 1 + 2\alpha x_0 + x_0^2 = (\alpha^2 - N(x_0)) \cdot 1 + 2\alpha x_0,$$

we must have $2\alpha x_0 = 0$. If $x_0 = 0$, we contradict our assumption that $x_0 \notin F \cdot 1$, so $\alpha = 0$ and $x = x_0 \in \mathcal{C}_0$. Thus we have shown that if $x \in \mathcal{C}$, then $x_0 \in \mathcal{C}_0$ if and only if $x \notin F \cdot 1$ and $x^2 \in F \cdot 1$. We use this fact to show that if $x_0 \in \mathcal{C}_0$, then $\eta(x_0) \in \mathcal{C}_0'$: if $x_0 = 0$ then statement is clear so assume $x_0 \neq 0$. Then we have $\eta(x_0) \notin \eta(F \cdot 1_{\mathcal{C}}) = F \cdot 1_{\mathcal{C}'}$ but $\eta(x_0^2) = \eta(x_0)^2 \in \eta(F \cdot 1_{\mathcal{C}}) = F \cdot 1_{\mathcal{C}'}$. It follows that $\eta(x_0) \in \mathcal{C}_0$. This fact tells us that since $\eta(x) = \alpha \cdot 1_{\mathcal{C}'} + \eta(x_0)$ we have $\overline{\eta(x)} = \alpha \cdot 1_{\mathcal{C}'} - \eta(x_0)$. Now we can prove that the norm forms N and N' are equivalent. We compute

$$\begin{aligned}
\eta(N'(\eta(x)) \cdot 1_{\mathcal{C}}) &= N'(\eta(x)) \cdot 1_{\mathcal{C}'} \\
&= \eta(x)\overline{\eta(x)} \\
&= (\alpha \cdot 1_{\mathcal{C}'} + \eta(x_0))(\alpha \cdot 1_{\mathcal{C}'} - \eta(x_0)) \\
&= \eta(x)\eta(\overline{x}) = \eta(x\overline{x}) = \eta(N(x) \cdot 1).
\end{aligned}$$

Since η is injective, $N'(\eta(x)) = N(x)$ for all $x \in \mathcal{C}$.

Next we prove the converse of the proposition; assume the norm forms N and N' are equivalent. Suppose we have a proper subalgebra B contained in $\mathcal{C}$ and a proper subalgebra B' contained in $\mathcal{C}'$ such that both subalgebras B and B' are nonisotropic. Now if there exists an isomorphism $\eta : B \to B'$, then N restricted to B and N' restricted to B' are equivalent. We assumed that N and N' are equivalent in the start; by Witt's theorem ([2], 121) the restrictions of N to $B^{\perp}$ and N' to $B'^{\perp}$ are equivalent. Then if we choose v in $B^{\perp}$ with $N(v) \neq 0$, we have a v' in $B'^{\perp}$ such that $N'(v') = N(v)$. The proof of Lemma 3.3.1 shows that we have an isomorphism from $B + Bv \to B' + B'v'$ given by $a + bv \mapsto \eta(a) + \eta(b)v'$. Hence we can begin with

$B = F \cdot 1$ and $B' = F \cdot 1'$ and apply the process repeatedly to obtain an isomorphism between $\mathcal{C}$ and $\mathcal{C}'$. $\square$

We now turn our attention to split composition algebras. First we will show that we have a special decomposition for split composition algebras. The proof given here is due to Jacobson [18], and the constructive nature of his proof will allow us to derive the unique split composition algebras for degree 4 and 8 after we have shown that there is only one for each degree.

Proposition 3.4.4 *Assume $\mathcal{C}$ is a composition algebra over a field F not of characteristic 2 that contains zero divisors. Then there exists idempotents e_1 and e_2 such that $e_1 + e_2 = 1$ and $e_1e_2 = 0 = e_2e_1$ and we have the splitting $\mathcal{C} = e_1\mathcal{C} \oplus e_2\mathcal{C}$ where the subspaces $e_1\mathcal{C}$ and $e_2\mathcal{C}$ are totally isotropic and exactly half the dimension of $\mathcal{C}$.*

Proof. Before we can define an e_1 and e_2, we must show there exists an $l \in \mathcal{C}_0$ such that $N(l) = -1$. Since $\mathcal{C}$ contains zero divisors there must exist a non-zero x in $\mathcal{C}$ such that $N(x) = 0$. We have the decomposition $\mathcal{C} = F \cdot 1 + \mathcal{C}_0$ so we can write $x = \alpha \cdot 1 + x_0$ for some $\alpha \in F$ and $x_0 \in \mathcal{C}_0$. Now since

$$N(x) = (\alpha \cdot 1 - x_0)(\alpha \cdot 1 + x_0) = \alpha^2 - x_0^2 = 0$$

we have $x_0^2 = \alpha^2$. So $N(x_0) = x_0\overline{x_0} = -x_0^2 = -\alpha^2$. As long as $\alpha \neq 0$, we can take $l = \alpha^{-1}x_0$ since clearly l would be in $\mathcal{C}_0$ and

$$N(l) = (\alpha^{-1})^2 N(x_0) = (\alpha^{-1})^2(-\alpha^2) = -1.$$

If $\alpha = 0$, then $N(x) = N(x_0) = 0$. We also have $q(x_0, x_0) = 2N(x_0) = 0$. Since $\mathcal{C}_0$ is not isotropic, there exists $y_0 \in \mathcal{C}_0$ such that $q(x_0, y_0) \neq 0$. Consider the element

$y_0 + \alpha x_0$ in $\mathcal{C}_0$. We calculate

$$\begin{aligned} N(y_0 + \alpha x_0) &= q(y_0 + \alpha x_0, y_0 + \alpha x_0) \\ &= q(y_0, y_0) + 2\alpha q(y_0, x_0) + \alpha^2 q(x_0, x_0) \\ &= q(y_0, y_0) + 2\alpha q(y_0, x_0). \end{aligned}$$

Then we can take $l = y_0 + \alpha x_0$ if we put $\alpha = \frac{-1-q(y_0,y_0)}{2q(y_0,x_0)}$. Thus we have shown that if $\mathcal{C}$ contains zero divisors we have an element $l \in \mathcal{C}_0$ with $N(l) = -1$.

We can now define e_1 and e_2: let $e_1 = \frac{1}{2}(1-l)$ and $e_2 = \frac{1}{2}(1+l)$ with the element l as described above. Since $-l^2 = l\bar{l} = N(l) = -1$, we have

$$N(e_1) = \frac{1}{4}N(1-l) = \frac{1}{4}(1-l)(1+l) = \frac{1}{4}(1-l^2) = \frac{1}{4}(1-1) = 0 \qquad (3.36)$$

and similarly $N(e_2) = 0$. Also

$$e_1^2 = \tfrac{1}{4}(1-l)^2 = \tfrac{1}{4}(1-2l-l^2) = \tfrac{1}{4}(1-2l-1) = \tfrac{1}{2}(1-l) = e_1.$$

Likewise $e_2^2 = e_2$ so that both e_1 and e_2 are idempotent. Also,

$$e_1e_2 = \frac{1}{4}(1-l)(1+l) = \frac{1}{4}(1-l^2) = \frac{1}{4}(1-1) = 0$$

and $e_2e_1 = 0$ by a similar computation. To show that subspace $e_1\mathcal{C}$ is totally isotropic, suppose e_1x and $e_1y \in e_1\mathcal{C}$. Since $N(e_1) = e_1\overline{e_1} = e_1e_2 = 0$, we have $N(e_1x) = N(e_1)N(x) = 0$ and $N(e_1y) = N(e_1)N(y) = 0$ and $N(e_1x+e_1y) = N(e_1)N(x+y) = 0$. Then $e_1\mathcal{C}$ must be totally isotropic since $q(e_1x, e_1y) = N(e_1x + e_1y) - N(e_1x) - N(e_1y) = 0$ for all x, y in $\mathcal{C}$. A similar argument shows that $e_2\mathcal{C}$ is also totally isotropic. Since the dimension of a totally isotropic subspace has maximal value half of the dimension of the entire space, ([2], 122), we have

$$\dim(e_1\mathcal{C}) \leq \frac{1}{2}\dim(\mathcal{C}) \quad \text{and} \quad \dim(e_2\mathcal{C}) \leq \frac{1}{2}\dim(\mathcal{C}). \tag{3.37}$$

Note that since $e_1 + e_2 = 1$, for any $x \in \mathcal{C}$

$$x = 1 \cdot x = (e_1 + e_2) \cdot x = e_1x + e_2x \in e_1\mathcal{C} + e_2\mathcal{C}$$

so $\mathcal{C} = e_1\mathcal{C} + e_1\mathcal{C}$. This tell us that

$$\dim(e_1\mathcal{C}) + \dim(e_2\mathcal{C}) \geq \dim(\mathcal{C}). \tag{3.38}$$

Comparing (3.37) and (3.38) we see that

$$\dim(e_1\mathcal{C}) = \dim(e_2\mathcal{C}) = \dim(\mathcal{C}).$$

Hence any composition algebra that contains zero divisors has the splitting $\mathcal{C} = e_1\mathcal{C} \oplus e_2\mathcal{C}$ with e_1 and e_2 as described in the theorem. □

The fact that $e_1\mathcal{C}$ and $e_2\mathcal{C}$ are totally isotropic and that each have dimensions that are exactly half of the dimension of $\mathcal{C}$ tells us that $\mathcal{C}$ is a *hyperbolic space*, which means that $\mathcal{C}$ is the orthogonal sum of *hyperbolic planes* ([2], 122; [23], 17). A hyperbolic plane is a two dimensional bilinear space which contains an isotropic vector. A useful fact concerning hyperbolic planes is that any two are *isometric*, which means that there exists a bijective linear map between spaces which preserves the norm map ([17], 343-346). With this information we are now ready to prove the main result for the split case: that any two split composition algebras of the same dimension are isomorphic.

Theorem 3.4.5 *Assume $\mathcal{C}$ and $\mathcal{C}'$ are split composition algebras over a fields not of characteristic 2. If $\mathcal{C}$ and $\mathcal{C}'$ have the same dimension, then $\mathcal{C}$ and $\mathcal{C}'$ are isomorphic.*

Proof. By the previous proposition and the discussion that followed, we know that $\mathcal{C}$ and $\mathcal{C}'$ are the orthogonal sum of hyperbolic planes; say $\mathcal{C}$ is the sum of H_i, and $\mathcal{C}'$ is the sum of H'_j. Since the algebras have the same dimension, they are the sum of the same number of hyperbolic planes. Since any two hyperbolic planes are isometric, there exists isometries $\eta_i : H_i \to H'_i$ for each i. Then the linear transformation η such that $\eta|_{H_i} = \eta_i$ is an isometry of $\mathcal{C}$ onto $\mathcal{C}'$. This tells us that $\mathcal{C}$ and $\mathcal{C}'$ have equivalent norm forms, and by Proposition 3.4.3, $\mathcal{C}$ and $\mathcal{C}'$ must be isomorphic. $\square$

We can now look at each split algebra in more detail. The split algebra of degree 2 is just a direct sum of two copies of the field F since $\dim(e_1\mathcal{C}) = \dim(e_2\mathcal{C}) = 1$ implies both $e_1\mathcal{C}$ and $e_2\mathcal{C}$ are isomorphic to F. In what follows, we will prove that the split algebra of degree 4 is isomorphic to $M_2(F)$, the set of all 2×2 matrices over F. We will also show that the split algebra of degree 8 is isomorphic to Zorn's *vector matrices.* Since we already know that any two split composition algebras of the same dimension are isomorphic, it would be enough to show that $M_2(F)$ and Zorn's vector matrices are split. However for the sake of completeness, we will give explicit isomorphisms.

Proposition 3.4.6 *If $\mathcal{C}$ is a four dimensional split composition algebra over a field F not of characteristic 2, then $\mathcal{C} \simeq M_2(F)$.*

Proof. By Theorem 3.4.5, we have the decomposition $\mathcal{C} = e_1\mathcal{C} \oplus e_2\mathcal{C}$ where $e_1\mathcal{C}$ and $e_2\mathcal{C}$ are two dimensional totally isotropic subspaces. We have

$$\begin{aligned} q(e_1, e_2) &= q(\frac{1}{2}(1-l), \frac{1}{2}(1+l)) \\ &= \frac{1}{4}q(1-l, 1+l) \end{aligned}$$

$$= \frac{1}{4}[N(2) - N(1-l) - N(1+l)]$$

$$= \frac{1}{4}N(2) = 1 \tag{3.39}$$

with the third equality following from (3.36). Now since the dimension of $(Fe_2)^\perp$ is 3, $e_1\mathcal{C} \cap (Fe_2)^\perp \neq 0$ so we can find a nonzero vector $z_1 \in e_1\mathcal{C} \cap (Fe_2)^\perp$. By a similar argument, we can find a nonzero $z_2 \in e_2\mathcal{C} \cap (Fe_1)^\perp$. If $z_1 \in Fe_1$, then $e_1 \in (Fe_2)^\perp$ and $q(e_1, e_2) = 0$. But this contradicts (3.39), so $z_1 \notin Fe_1$ and similarly $z_2 \notin Fe_2$. Thus $\{e_1, z_1\}$ is a basis for $e_1\mathcal{C}$, $\{e_2, z_2\}$ is a basis for $e_2\mathcal{C}$, and so $\{e_1, e_2, z_1, z_2\}$ is a basis for $\mathcal{C}$.

Consider the 2×2 matrix algebra $M_2(F)$ with basis $\{E_{11}, E_{12}, E_{21}, E_{22}\}$ where E_{ij} $(i, j = 1, 2)$ represents the matrix with a 1 in the ith row and jth column and zeros elsewhere. The multiplication table for the basis elements contains 16 relations:

$$E_{11}^2 = E_{11}, \;\; E_{22}^2 = E_{22}, \;\; E_{11}E_{22} = E_{22}E_{11} = 0; \tag{3.40}$$

$$E_{12}^2 = E_{21}^2 = 0; \tag{3.41}$$

$$E_{11}E_{12} = E_{12}, \;\; E_{22}E_{21} = E_{21}, \;\; E_{11}E_{21} = 0, \;\; E_{22}E_{12} = 0; \tag{3.42}$$

$$E_{12}E_{21} = E_{11}, \;\; E_{21}E_{12} = E_{22}; \tag{3.43}$$

$$E_{12}E_{11} = 0, \;\; E_{21}E_{22} = 0, \;\; E_{12}E_{22} = E_{12}, \;\; E_{21}E_{11} = E_{21}. \tag{3.44}$$

We wish to show the map from $\mathcal{C}$ into $M_2(F)$ given by

$$\alpha e_1 + \beta z_1 + \gamma z_2 + \delta e_2 \mapsto \alpha E_{11} + \beta E_{12} + \gamma E_{21} + \delta E_{22}$$

is an algebra isomorphism. To do so, we must verify that the basis elements of $\mathcal{C}$ satisfy the relations in the multiplication table for the basis elements of $M_2(F)$. Note that the relations in (3.40) are given in Proposition 3.4.4. Before showing the other relations, we must show that $q(z_i, e_j) = 0$ and $q(z_1, z_2) = -1$. Since $z_i \in e_i\mathcal{C}$ and $e_i\mathcal{C}$ is totally isotropic, we have $q(z_i, e_i) = 0$. By construction $q(z_i, e_j) = 0$ for $i \neq j$. Then if also $q(z_1, z_2) = 0$, z_i is orthogonal to everything in $\mathcal{C}$ which means z_i must be zero. This contradiction implies $q(z_1, z_2) \neq 0$. We may assume $(z_1, z_2) = -1$. Now, we have

$$q(1, z_i) = q(e_1 + e_2, z_i) = q(e_1, z_i) + q(e_2, z_i) = 0$$

which shows that $z_i \in \mathcal{C}_0$. By (3.35), $z_i^2 = N(z_i)$ and since z_i is contained in a totally isotropic subspace, $0 = q(z_i, z_i) = N(z_i)$ so that (3.41) is satisfied. For (3.42), note that since $e_i z_i = z_i$, we have

$$e_i z_j = e_i(e_j z_j) = (e_i e_j) z_j = 0$$

if $i \neq j$. Also, using the fact that $z_i \in \mathcal{C}_0$ and relation (3.20) we have

$$z_1 z_2 + z_2 z_1 = -(z_1 \overline{z_2} + z_2 \overline{z_1}) = -q(z_1, z_2) = 1$$

Next we multiply this equation on the left by e_1 and apply the fact that $e_1 z_1 = z_1$ and $e_1 z_2 = 0$:

$$\begin{aligned} e_1(z_1 z_2) + e_1(z_2 z_1) &= e_1 \\ (e_1 z_1) z_2 + (e_1 z_2) z_1 &= e_1 \\ z_1 z_2 &= e_1. \end{aligned}$$

Multiplying (3.45) by e_2 yields $z_2 z_1 = e_2$ which shows relations (3.43). Using these relations we also find that $z_1 e_1 = z_1(z_1 z_2) = (z_1)^2 z_2 = 0$ and $z_2 e_2 = z_2(z_2 z_1) =$

$(z_2)^2 z_1 = 0$. Therefore $z_1 e_2 = z_1(e_1 + e_2) = z_1$ and $z_2 e_1 = z_2$. These calculations show that the last relations (3.44) are satisfied. Therefore e_1, e_2, z_1, z_2 satisfy the same relations as the basis elements of $M_2(F)$ under the correspondence $e_1 \mapsto E_{11}$, $e_2 \mapsto E_{22}$, $z_1 \mapsto E_{12}$, $z_2 \mapsto E_{21}$ so the split composition algebra $\mathcal{C}$ of degree 4 is isomorphic to $M_2(F)$. □

We note that since $\overline{e_1} = e_2$, $\overline{e_2} = e_1$, $\overline{z_1} = -z_1$, $\overline{z_2} = -z_2$, the conjugation in the matrix algebra is given by

$$\begin{bmatrix} \alpha & \beta \\ \gamma & \delta \end{bmatrix} \mapsto \begin{bmatrix} \delta & -\beta \\ -\gamma & \alpha \end{bmatrix}.$$

The determinant is a quadratic form on $M_2(F)$; we can also calculate the norm using $N(x) \cdot 1 = x\overline{x}$.

$$\begin{bmatrix} \alpha & \beta \\ \gamma & \delta \end{bmatrix} \overline{\begin{bmatrix} \alpha & \beta \\ \gamma & \delta \end{bmatrix}} = (\alpha\delta - \beta\gamma) \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}.$$

Therefore

$$N\left(\begin{bmatrix} \alpha & \beta \\ \gamma & \delta \end{bmatrix}\right) = (\alpha\delta - \beta\gamma) = \det \begin{bmatrix} \alpha & \beta \\ \gamma & \delta \end{bmatrix}.$$

The fact that the split quaternions are isomorphic to the algebra of 2×2 matrices can be generalized to the split octonions. We introduce the Zorn's algebra of vector matrices, first introduced by Zorn in 1933 [27]. Begin with the set of matrices of the form

$$\begin{bmatrix} \alpha & a \\ b & \beta \end{bmatrix}$$

such that α, β scalars and a, b are vectors. We assume the vectors are elements of a three dimensional bilinear space where the vector product $a \times b$ is defined. Addition is defined in the usual way, and multiplication is given by

$$\begin{bmatrix} \alpha & a \\ b & \beta \end{bmatrix} \begin{bmatrix} \xi & x \\ y & \nu \end{bmatrix} = \begin{bmatrix} \alpha\xi - (a, y) & \alpha x + \nu a + b \times y \\ \xi b + \beta y + a \times x & \beta\nu - (b, x) \end{bmatrix}.$$

The norm map on this algebra is given by

$$N\left(\begin{bmatrix} \alpha & a \\ b & \beta \end{bmatrix}\right) = \alpha\beta - q(a, b).$$

We will show that the eight-dimensional split composition algebra is isomorphic to the vector matrix algebra. To do this, we will first decompose a Cayley algebra using a quaternion subalgebra, and then further decompose the Cayley algebra by breaking down the quaternion algebras as done in Proposition 3.4.4. This will give us a way to easily describe the multiplication in the Cayley algebra and make the connection with the multiplication in the vector matrices.

Assume we have a Cayley algebra $\mathcal{C}$. Choose $l \in \mathcal{C}_0$ with nonzero norm. We wish to write $\mathcal{C}$ as the Cayley-Dickson algebra $B \oplus Bl$ where B is a quaternion subalgebra such that B is orthogonal to l. We will use Lemma 3.3.1, as reworded in the remarks following its proof, repeatedly to construct $\mathcal{C}$. Using l to double F, we have the Cayley-Dickson subalgebra $F[l] = F + F \cdot l$. In the subspace $F[l]^{\perp} \subset \mathcal{C}_0$, choose i with nonzero norm. Then we know the subalgebra $B' = F[l] + F[l] \cdot i$ is a Cayley-Dickson subalgebra of $\mathcal{C}$, and because it is of dimension four we know that it is a quaternion algebra. Now choose $j \in B'^{\perp}$ with nonzero norm so we can write $\mathcal{C} = B' \oplus B'j$, where we have $B'j = B'^{\perp}$. Because of the construction, $\mathcal{C}$ has orthogonal basis $\{1, i, l, il, j, ij, lj, (il)j\}$. Then we see that $B = F \cdot 1 + F \cdot i + F \cdot j + F \cdot (ij)$ is a quaternion subalgebra orthogonal to l and $\mathcal{C} = B \oplus Bl$ where $Bl = B^{\perp}$. Further, let B_0

represent the set of elements of B orthogonal to 1. Then since $B_0 = F\cdot i + F\cdot j + F\cdot (ij)$ and the basis given above is an orthogonal, we have $F[l] = B_0 + B_0 l$.

We assume that $\mathcal{C}$ is split, so we may take $l^2 = 1$. From Proposition 3.4.4, we know that $\mathcal{C}$ contains four dimensional totally isotropic subspaces, and since $F[l]^\perp$ is six dimensional we can find a an element in $F[l]^\perp$ with zero norm. In the proof of Proposition 3.4.4 we showed that this implies that we can find i in $F[l]^\perp$ with $i^2 = 1$, but then this means that the quaternion subalgebra B must be split. Let $e_1 = \frac{1}{2}(1-l)$ and $e_2 = \frac{1}{2}(1+l)$ as in the proof of Proposition 3.4.4 so that e_1 and e_2 satisfy the properties given in the proposition and we have $B = e_1 B \oplus e_2 B$. Now since $\mathcal{C} = B \oplus Bl$ and $B = F\cdot 1 \oplus B_0$, we have $\mathcal{C} = F\cdot e_1 \oplus F\cdot e_2 \oplus B_0 e_1 \oplus B_0 e_2$. Recall that the basis for B_0 is $\{i, j, ij\}$ so that the basis for $\mathcal{C}$ is $\{e_1, ie_1, je_1, (ij)e_1, e_2, ie_2, je_2, (ij)e_2\}$. For simplicity let $e_2 = y_0$, $ie_1 = y_1$, $je_1 = y_2$, $(ij)e_1 = y_3$, $e_1 = x_0$, $ie_2 = x_1$, $je_2 = x_2$, and $(ij)e_2 = x_3$ so the basis for $\mathcal{C}$ is $\{y_0, y_1, y_2, y_3, x_0, x_1, x_2, x_3\}$. Note that this basis satisfies

$$q(x_i, y_j) = \delta_{ij} \text{ for } i, j = 1, 2, 3. \tag{3.45}$$

Indeed, if $k = i, j, ij$ then $k\bar{k} = k^2 = 1$ so

$$q(x_i, y_i) = q(ke_2, ke_1) = q(k\bar{k}e_2, e_1) = q(e_2, e_1) = 1.$$

If $b_1 \neq b_2$ we have

$$q(b_2 e_2, b_1 e_1) = q(e_2 \overline{e_1}, \overline{b_2} b_1) = q(e_2, 1)\overline{b_2} b_1 = 0$$

so that $q(x_i, y_j) = 0$ if $i \neq j$.

We wish to establish the basic relations between basis elements that completely describe the multiplication in $\mathcal{C}$. Recall that e_1 and e_2 are idempotent and $e_ie_j = 0$ for $i \neq j$ so we have

$$x_0^2 = x_0 \ , \ y_0^2 = y_0 \quad \text{and} \quad x_0y_0 = y_0x_0 = 0. \tag{3.46}$$

The next four relations will show us how to multiply x_0 with the x_i and y_i and how to multiply y_0 with the x_i and y_i. Also because the e_i are idempotent we have $(be_i)e_i = be_i$ for all b in B_0 or

$$xy_0 = x \text{ for all } x \in B_0e_2 \quad \text{and} \quad yx_0 = y \text{ for all } y \in B_0e_1. \tag{3.47}$$

We see that $e_j = 1 - e_i$ for $i \neq j$ which gives $(be_i)e_j = be_i - be_i^2 = 0$ for all b in B_0 or

$$xx_0 = 0 \text{ for all } x \in B_0e_2 \quad \text{and} \quad yy_0 = 0 \text{ for all } y \in B_0e_1. \tag{3.48}$$

Note that for all b in B we have $\bar{b}l = lb$, but also if $b \in B_0 \subset B$ then $\bar{b} = -b$ so that $-bl = lb$ for all $b \in B_0$. Using this and the fact that $l^2 = 1$ we have $e_i(be_i) = (1 \pm l)(b \pm bl) = b \pm bl \mp bl - l(lb) = 0$ for $b \in B_0$ so that $e_i(B_0e_i) = 0$ or

$$y_0x = 0 \text{ for all } x \in B_0e_2 \quad \text{and} \quad x_0y = 0 \text{ for all } y \in B_0e_1. \tag{3.49}$$

Then we also have $e_j(be_i) = (1 - e_i)(be_i) = be_i - e_i(be_i) = be_i$ for all b in B_0 or

$$x_0x = x \text{ for all } x \in B_0e_2 \quad \text{and} \quad y_0y = y \text{ for all } y \in B_0e_1. \tag{3.50}$$

Now we need to find relations that describe multiplication between the x_i and y_i for $i = 1, 2, 3$. Note that for b_1, b_2 in B_0 we have

$$4(b_1e_i)(b_2e_j) = (b_1 \pm b_1l)(b_2 \mp b_2l)$$

$$
\begin{aligned}
&= b_1b_2 \mp b_1(b_2l) \pm (b_1l)b_2 - (b_1l)(b_2l) \\
&= b_1b_2 \mp (b_2b_1)l \mp (b_1b_2)l + b_2b_1 \\
&= (b_1b_2 + b_2b_1)(1 \mp l) = -2q(b_1, b_2)e_j \in F \cdot e_j \qquad (3.51)
\end{aligned}
$$

for $i \neq j$ so that for $b_1, b_2 = i, j, ij$ we have

$$
(b_1e_i)(b_2e_j) = -2q(b_1, b_2)e_j = \begin{cases} -2 \cdot 2e_j = -e_j \text{ when } b_1 = b_2 \\ 0 \qquad\qquad\qquad \text{if } b_1 \neq b_2. \end{cases}
$$

Thus we have shown

$$
x_iy_j = -\delta_{ij}x_0 \quad \text{and} \quad y_ix_j = -\delta_{ij}y_0. \qquad (3.52)
$$

Next we notice for b_1 and b_2 in B_0 we have

$$
\begin{aligned}
4(b_1e_i)(b_2e_i) &= (b_1 \pm b_1l)(b_2 \pm b_2l) \\
&= b_1b_2 \pm b_1(b_2l) \pm (b_1l)b_2 + (b_1l)(b_2l) \\
&= b_1b_2 \pm (b_2b_1)l \mp (b_1b_2)l - (b_2b_1)l \\
&= (b_1b_2 - b_2b_1)(1 \mp l) = 2(b_1b_2 - b_2b_1)e_j \in B_0e_j
\end{aligned}
$$

where $i \neq j$. Then in particular we have $x_1x_2 = (ie_2)(je_2)$ is in B_0e_1. Recall that $\{y_1 = ie_1, y_2 = je_1, y_3 = (ij)e_1\}$ is a basis for B_0e_1, so there exists α, β, γ in F such that $x_1x_2 = \alpha y_1 + \beta y_2 + \gamma y_3$. To compute α, β, and γ we use the bilinear form. We know that $q(x_1, x_1x_2) = q(x_2, x_1x_2) = 0$ by (3.13), but also

$$
q(x_i, x_1x_2) = q(x_i, \alpha y_1 + \beta y_2 + \gamma y_3) = \alpha q(x_i, y_1) + \beta q(x_i, y_2) + \gamma q(x_i, y_3) = \begin{cases} \alpha \text{ if } i = 1 \\ \beta \text{ if } i = 2 \\ \gamma \text{ if } i = 3 \end{cases}
$$

so that $\alpha = \beta = 0$ and $\gamma = q(x_3, x_1x_2)$. Then $x_1x_2 = q(x_3, x_1x_2)$. Similar computations show that $x_ix_{i+1} = q(x_ix_{i+1}, x_{i+2})y_{i+2}$ and $y_iy_{i+1} = q(y_iy_{i+1}, y_{i+2})x_{i+2}$ where the indices are reduced modulo 3. It can be shown that $q(x_ix_{i+1}, x_{i+2})$ is an alternating function of x_1, x_2, x_3 so that $q(x_ix_{i+1}, x_{i+2}) = q(x_1x_2, x_3)$. But

$$\begin{aligned} q(x_1x_2, x_3) &= q((ie_2)(je_2), (ij)e_2) \\ &= q((ij)e_1, (ij)e_2) \\ &= q((\overline{ij})(ij), e_2\overline{e_1}) \\ &= q(-(ij)^2, {e_2}^2) = -q(1, e_2) = -1 \end{aligned}$$

where the second equality follows from (3.51) and the third from (3.13). Likewise $(y_iy_{i+1}, y_{i+2}) = -1$. Then if we replace x_3 with $-x_3$ and y_3 with $-y_3$ we have the relations

$$x_ix_{i+1} = y_{i+2} \text{ and } y_iy_{i+1} = x_{i+2} \tag{3.53}$$

for $i = 1, 2, 3$.

We can now define a map between our split Cayley algebra and Zorn's vector matrices. Let ϕ be the bijective map defined by

$$\phi(\alpha_0x_0 + \alpha_1x_1 + \alpha_2x_2 + \alpha_3x_3 + \beta_0y_0 + \beta_1y_1 + \beta_2y_2 + \beta_3y_3) = \begin{bmatrix} \alpha_0 & a \\ b & \beta_0 \end{bmatrix}$$

where $a = \alpha_1x_1 + \alpha_2x_2 + \alpha_3x_3$ and $b = \beta_1y_1 + \beta_2y_2 + \beta_3y_3$. Clearly this map is linear, and relations (3.46) through (3.53) imply that the map preserves the multiplication. Thus we have shown the following generalization of Proposition 3.4.6.

Proposition 3.4.7 *If C is an eight dimensional split composition algebra over a field not of characteristic 2, then C is isomorphic to Zorn's vector matrices.*

Note that since for any b in B_0 we have

$$\overline{be_i} = -e_j b = -\frac{1}{2}(b \pm lb) = -\frac{1}{2}(b \mp bl) = -be_i$$

so that $\overline{x_i} = -x_i$ and $\overline{y_i} = -y_i$ for $i = 1, 2, 3$. Then we have

$$\overline{a} = \overline{\alpha_1 x_1 + \alpha_2 x_2 + \alpha_3 x_3} = -a$$

and likewise

$$\overline{b} = \overline{\beta_1 y_1 + \beta_2 y_2 + \beta_3 y_3} = -b.$$

Also, $\overline{x_0} = y_0$ so that

$$\overline{\begin{bmatrix} \alpha_0 & a \\ b & \beta_0 \end{bmatrix}} = \begin{bmatrix} \beta_0 & -a \\ -b & \alpha_0 \end{bmatrix}.$$

Computing the norm in the vector matrix algebra under the isomorphism we find that

$$\begin{bmatrix} \alpha_0 & a \\ b & \beta_0 \end{bmatrix} \begin{bmatrix} \beta_0 & -a \\ -b & \alpha_0 \end{bmatrix} = \begin{bmatrix} \alpha_0\beta_0 - q(a,b) & 0 \\ 0 & \alpha_0\beta_0 - q(a,b) \end{bmatrix} = [\alpha_0\beta_0 - q(a,b)] \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

so

$$N\left(\begin{bmatrix} \alpha_0 & a \\ b & \beta_0 \end{bmatrix}\right) = \alpha_0\beta_0 - q(a,b)$$

which agrees with the norm defined when the vector matrices were introduced.

We have shown that there is only one split composition algebra for each possible degree and completely described the algebra for each case. We will now focus on division algebras. Unfortunately, we are not able to completely describe all possible division algebras as we did in the split case by classical means but we can determine in certain cases when the doubling process yields isomorphic algebras. We will see that two Cayley-Dickson doubles of the same composition algebra are isomorphic if and only if the doubling parameters differ by a norm.

Proposition 3.4.8 *Let $\mathcal{B}$ be an associative algebra over a field F not of characteristic 2. Then the Cayley-Dickson doubles $\mathcal{B}+\mathcal{B}u$ and $\mathcal{B}+\mathcal{B}v$ are isomorphic as composition algebras if and only if there exists b in $\mathcal{B}$ such that $u^2 = N(b)v^2$.*

Proof. Assume first that we have b in $\mathcal{B}$ such that $u^2 = N(b)v^2$; we claim the map from $\mathcal{B}+\mathcal{B}u$ onto $\mathcal{B}+\mathcal{B}v$ defined by $f : u \mapsto bv$ which fixes $\mathcal{B}$ is an algebra isomorphism. We need only to check the multiplication. Let x_1, x_2, y_1, y_2 be in $\mathcal{B}$. Using the definition of multiplication in a Cayley-Dickson algebra we have

$$\begin{aligned} f((x_1+y_1u)(x_2+y_2u)) &= f((x_1x_2+N(b)v^2\overline{y_2}y_1)+(y_2x_1+y_1\overline{x_2})u) \\ &= (x_1x_2+N(b)v^2\overline{y_2}y_1)+(y_2x_1+y_1\overline{x_2})(bv). \end{aligned}$$

We also have

$$\begin{aligned} f(x_1+y_1u)f(x_2+y_2u) &= [x_1+y_1(bv)][x_2+y_2(bv)] \\ &= [x_1+(by_1)v][x_2+(by_2)v] \\ &= [x_1x_2+v^2(\overline{by_2})(by_1)]+[(by_2)x_1+(by_1)\overline{x_2}]v \\ &= [x_1x_2+v^2(\overline{y_2}\,\overline{b})(by_1)]+[b(y_2x_1+y_1\overline{x_2})]v \\ &= [x_1x_2+N(b)v^2(\overline{y_2}y_1)]+[y_2x_1+y_1\overline{x_2}](bv) \end{aligned}$$

using the definition of multiplication in a double and the fact that $\mathcal{B}$ must be associative so we see that $\mathcal{B}+\mathcal{B}u$ and $\mathcal{B}+\mathcal{B}v$ are isomorphic as composition algebras.

Conversely, assume that we have an algebra isomorphism $f : \mathcal{B} + \mathcal{B}u \to \mathcal{B} + \mathcal{B}v$ that fixes $\mathcal{B}$ and sends u to $b_1 + b_2 v$. We know for any x and y in $\mathcal{B}$

$$N(x + yu) = N(x) - u^2 N(y) \tag{3.54}$$

and

$$\begin{aligned} N((x + yb_1) + (b_2 y)v) &= N(x + yb_1) - v^2 N(b_2 y) \\ &= N(x) + N(y)N(b_1) + q(x, yb_1) - v^2 N(b_2)N(y). \end{aligned} \tag{3.55}$$

From Proposition 3.4.3 we know that any isomorphism between composition algebras must preserve the norm, so (3.54) and (3.55) must be equal for all x and y in $\mathcal{B}$. Setting these equations equal, choosing $y = 1$ and solving for $q(x, yb_1)$ gives

$$q(x, b_1) = v^2 N(b_2) - u^2 - N(b_1)$$

for all x in $\mathcal{B}$. But $v^2 N(b_2) - u^2 - N(b_1)$ is constant, so $q(x, b_1) = 0$ for all x and since the bilinear form is nondegenerate, b_1 must be zero. Then $v^2 N(b_2) - u^2 = 0$. □

In the case of the division quadratic algebra, this means two quadratic algebras $F(\sqrt{\mu}) \simeq F + Fu$ and $F(\sqrt{\nu}) \simeq F + Fv$, where $\mu = u^2$ and $\nu = v^2$, are isomorphic if and only if μ/ν is a square in F. So the multiplicative group of F modulo its squares parameterizes the quadratic algebras.

We can say a little about the division quaternion algebras and division Cayley algebras using the same reasoning. Let $\mu = u^2$ and $\nu = v^2$; we will use $\langle \mu, \nu \rangle$ to represent the quaternion algebra formed by doubling the quadratic algebra $F(\sqrt{\mu}) \simeq F + Fu$ using the parameter $\nu = v^2$. Then from the proposition we see that $\langle \mu, \nu_1 \rangle$ and $\langle \mu, \nu_2 \rangle$ are isomorphic if and only if ν_1/ν_2 is the norm of an element in $F(\sqrt{\mu}) \simeq$

$F+Fu$. Let $\langle \mu, \nu, \xi \rangle$ represent the Cayley algebra formed by doubling the quaternion algebra $\langle \mu, \nu \rangle$ using the parameter $\ell^2 = \xi$. Applying this to Cayley algebras tells us that $\langle \mu, \nu, \xi_1 \rangle$ is isomorphic to $\langle \mu, \nu, \xi_2 \rangle$ if and only if ξ_1/ξ_2 is a norm in the quaternion algebra $\langle \mu, \nu \rangle$.

This is about as much as one can say by classical means, although at this point it is natural to question when $\langle \mu_1, \nu_1 \rangle$ and $\langle \mu_2, \nu_2 \rangle$ are isomorphic as composition algebras, and when are $\langle \mu_1, \nu_1, \xi_1 \rangle$ and $\langle \mu_2, \nu_2, \xi_2 \rangle$ isomorphic as composition algebras. We will try to address these questions in the next section with more modern techniques.

3.5 Isomorphism Classes and Galois Cohomology

We wish to be able to determine when two division composition algebras are isomorphic by comparing doubling parameters. In this last section we outline an answer to this question by using cohomological techniques. First we will make the connection between equivalence classes of isomorphic algebras and cohomology using ideas from Serre's book *Galois Cohomology.* We will then use results from the book *Octonions, Jordan Algebras, and Exceptional Groups* by Springer and Veldkamp to relate isomorphism classes of composition algebras to the doubling parameters.

We begin with a little background material. Let A be a finite abelian group on which G acts continuously. Let $C^n(G, A)$ be the set of all continous maps of n variables in G to A. We define the *coboundary* $\delta : C^n(G, A) \to C^{n+1}(G, A)$ by the formula

$$\delta f(g_1, \ldots, g_{n+1}) = g_1 f(g_2, \ldots, g_{n+1})$$

$$+\sum_{i=1}^{n}(-1)^i f(g_1,\ldots,g_{i-1},g_ig_{i+1},\ldots,g_{n+1})$$
$$+(-1)^{n+1}f(g_1,\ldots,g_n).$$

This map is a homomorphism, and we let $Z^n(G,A)$ denote its kernal and $B^{n+1}(G,A)$ its image in $C^{n+1}(G,A)$. The group $Z^n(G,A)$ is the group of *n-cocycles* of G in A and $B^{n+1}(G,A)$ is the group of *n-coboundaries* of G in A. Then the nth *cohomology group of G with coefficients in A* is the factor group $H^n(G,A) = Z^n(G,A)/B^n(G,A)$. Two n-cocyles are *cohomologous* when they determine the same element in $H^n(G,A)$.

We also need the idea of the *cup product.* Suppose B is another finite abelian group on which G acts continously. For the tensor product $A \otimes B$ with A and B considered as $\mathbf{Z}$-modules, the action of G is defined by $\gamma(a\otimes b) = \gamma(a)\otimes\gamma(b)$. We have the cup product maps

$$H^i(G,A)\times H^j(G,B)\to H^{i+j}(G,A\otimes B) : (c,d)\mapsto c\cup d.$$

For the i-cocycle f and the j-cocycle g, let $[f]$ and $[g]$ represent their cohomology classes in $H^i(G,A)$ and $H^j(G,A)$. We have the cup product $[f]\cup[g] = [h]$ where h is the $(i+j)$-cocycle defined by

$$h(\sigma_1.\ldots.\sigma_i,\tau_1\ldots,\tau_j) = f(\sigma_1,\ldots,\sigma_i)\otimes\sigma_1\cdots\sigma_i(g(\tau_1,\ldots,\tau_j))$$

where $\sigma_1,\ldots,\sigma_i,\tau_1,\ldots,\tau_j$ are in G.

We are now ready to outline the connection between the equivalence classes of isomorphic algebras and cohomology. Here we will describe Serre's "general principle" ([24], 121), which will allow us to make the connection between the isomorphism classes of division algebras and cohomology. Begin with a field F, its algebraic closure

$\overline{F}$, and an object X over F. An object Y over F is a $\overline{F}/F$ form of X if $X \otimes_F \overline{F} \simeq Y \otimes_F \overline{F}$. The equivalence classes of F-isomorphic forms are denoted $E(\overline{F}/F, X)$. If $\overline{F}/F$ is Galois, there exists a bijective correspondence between $E(\overline{F}/F, X)$ and $H^1(\mathrm{Gal}(\overline{\mathrm{F}}/\mathrm{F}), \mathrm{Aut}_{\overline{\mathrm{F}}}(\mathrm{X}))$.

For us, we will take the object X to be a composition algebra over F of dimension n. Two composition algebras X and Y are $\overline{F}/F$ forms of each other if they become isomorphic when the base field is extended to $\overline{F}$, that is, if $X \otimes_F \overline{F} \simeq Y \otimes_F \overline{F}$. But since extending the base field to the closure of F results in a spilt algebra, all the composition algebras over F are isomorphic over $\overline{F}$. Then $E(\overline{F}/F, X)$ represents the F-isomorphism classes of composition algebras of dimension n over F.

Consider the case $n = 2$. We already know that the division composition algebras of dimension 2 over F are parameterized by the squares in F, but we will show that we can achieve the same result using the general principle described previously. Let X be a degree 2 composition algebra over F. Then we can write $X = F + F \cdot l$ where $l^2 = -\mu$ and $N(l) = \mu$. We have $X \otimes_F \overline{F} = \overline{F} + \overline{F} \cdot l$. Since $\overline{F} + \overline{F} \cdot l$ must be split, $\overline{F} + \overline{F} \cdot l \simeq \overline{F} \oplus \overline{F}$. Then the group $\mathrm{Aut}_{\overline{F}}(X)$ of $\overline{F}$ automorphisms of X is just the group of automorphisms of $\overline{F} \oplus \overline{F}$, which is $\{1, \alpha\} \simeq \mathbf{Z}/2\mathbf{Z}$ where $\alpha(a, b) = (b, a)$. So we have $H^1(\mathrm{Gal}(\overline{F}/F), \mathrm{Aut}_{\overline{F}}(X))$ is isomorphic to $H^1(\mathrm{Gal}(\overline{F}/F), \mathbf{Z}/2\mathbf{Z})$. Serre tells us ([24], 187) that $H^1(\mathrm{Gal}(\overline{F}/F), \mathbf{Z}/2\mathbf{Z}) = F^*/F^{*2}$ so the equivalence classes of composition algebras of dimension 2 over F is isomorphic to F^*/F^{*2}.

For the case $n = 4$, if X is a degree 4 composition algebra over F, we have $X \otimes_F \overline{F} \simeq M_2(\overline{F})$. Now we need the automorphism group of $M_2(\overline{F})$. Consider the general linear group, $\mathrm{GL}_2(\overline{F})$, which is the group of nonsingular 2×2 matrices in

$\overline{F}$, and the projective general linear group $\mathrm{PGL}_2(\overline{F})$, which is the quotient group of $\mathrm{GL}_2(\overline{F})$ modulo its center Z_2, the set of all scalar matrices. We know GL_2 acts on M_2 by conjugation and Z_2 acts trivially, so PGL_2 acts on M_2. In fact, by the Skolem-Noether Theorem, $\mathrm{PGL}_2 = Aut(M_2)$. So the equivalence classes of composition algebras of dimension 4 over F is isomorphic to $H^1(\mathrm{Gal}(\overline{F}/F), \mathrm{PGL}_2(\overline{F}))$. Let V_3 represent the 3 dimensional vector space of matrices of the form $\begin{bmatrix} a & b \\ c & -a \end{bmatrix}$. The determinant is a quadratic form on V_3. Now PGL_2 acts on V_3 by conjugation, and since $\det(g^{-1}xg) = \det(x)$, PGL_2 preserves this quadratic form. Through this action we have an isomorphism of PGL_2 onto the subgroup of the orthogonal group $O(V_3, \det)$ of matrices with determinant 1, which is the special orthogonal group $\mathrm{SO}(V_3, \det)$. So we have the equivalence classes of composition algebras of dimension 4 over F is isomorphic to $H^1(\mathrm{Gal}(\overline{F}/F), \mathrm{SO}(V_3, \det))$.

In Serre ([24], 141), we find the map

$$H^1(\mathrm{Gal}(\overline{F}/F), \mathrm{SO}(V_3, \det)) \to H^2(\mathrm{Gal}(\overline{F}/F), \mathbf{Z}/2\mathbf{Z}).$$

He claims that the image of this map consists of the elements of $H^2(\mathrm{Gal}(\overline{F}/F), \mathbf{Z}/2\mathbf{Z})$ which are cup-products of two elements of $H^1(\mathrm{Gal}(\overline{F}/F), \mathbf{Z}/2\mathbf{Z})$. Recall the relationship between $H^1(\mathrm{Gal}(\overline{F}/F), \mathbf{Z}/2\mathbf{Z})$ and the degree two composition algebras over F; this map gives us a connection between the sets equivalence classes of isomorphic quaternion algebras and two nonsquares in F^*.

In the case $n = 8$, for the octonion algebra X, we have $\mathrm{Aut}_{\overline{F}}(X)$ is isomorphic to the split exceptional group G_2 ([18], 15). Serre shows ([24], 190) that the map

$$H^1(\mathrm{Gal}(\overline{F}/F), G_2) \to H^3(\mathrm{Gal}(\overline{F}/F), \mathbf{Z}/2\mathbf{Z})$$

is a bijection, and that the image consists of cup-products of three elements from $H^1(\mathrm{Gal}(\overline{F}/F), \mathbf{Z}/2\mathbf{Z})$. This gives us a connection between classes of Cayley algebras over F and three nonsquares in F^*, presumably the three doubling parameters needed to construct a Cayley algebra from the field F.

We need to know if these nonsquares are the doubling parameters used to get from F to the composition algebra X. For the case $n = 4$, a lemma of Springer and Veldkamp shows this by connecting cup products of elements from $H^1(\mathrm{Gal}(\overline{F}/F), \mathbf{Z}/2\mathbf{Z})$ to *cyclic algebras*. For μ, ν in F^*, we define the cyclic algebra $A_\zeta(\mu, \nu)$ to be the associative algebra over F generated by the elements u and v such that

$$u^m = \mu, \quad v^m = \nu \quad , uvu^{-1} = \zeta v$$

where $\zeta \in F^*$ represents the mth root of unity. We are interested in the case $m = 2$. It is easy to see that the quaternion algebra with basis $\{1, u, v, uv\}$ where $u^2 = \mu$ and $v^2 = \nu$ is the cyclic algebra $A_{-1}(\mu, \nu)$.

Let $[\mu]$ and $[\nu]$ represent the cohomology classes in $H^1(\mathrm{Gal}(\overline{F}/F), \mathbf{Z}/2\mathbf{Z})$ for μ and ν in F. An equivalence relation can be defined on the class of central simple algebras over the field F making the set of equivalence classes into a group called the *Brauer Group*. According to Springer and Veldkamp ([25], 188), the equivalence class of $A_{-1}(\mu, \nu)$ in the Brauer group is the image of the cup product of $[\mu]$ and $[\nu]$ under the isomorphism $H^2(\mathrm{Gal}(\overline{F}/F), \mathbf{Z}/2\mathbf{Z} \otimes \mathbf{Z}/2\mathbf{Z})$ onto $H^2(\mathrm{Gal}(\overline{F}/F), \mathbf{Z}/2\mathbf{Z})$. This means that if we have two quaternion algebras $\langle \mu_1, \nu_1 \rangle$ and $\langle \mu_2, \nu_2 \rangle$, they are isomorphic as composition algebras if $[\mu_1] \cup [\nu_1]$ and $[\mu_2] \cup [\nu_2]$ represent the same element in $H^2(\mathrm{Gal}(\overline{F}/F), \mathbf{Z}/2\mathbf{Z})$. Also, if we begin with a cup product $[\mu] \cup [\nu]$, this determines an equivalence class $[X]$ in the Brauer group. Since X is only quaternion algebra in its equivalence class, it is determined by $[\mu] \cup [\nu]$ up to isomorphism. Then the isomorphism class of quaternion algebras $\langle \mu, \nu \rangle$ is completely specified by the cup product $[\mu] \cup [\nu]$ in $H^2(\mathrm{Gal}(\overline{F}/F), \mathbf{Z}/2\mathbf{Z})$.

There is a similar result for the case of the octonions. We obtain the Cayley algebra $X = \langle \mu, \nu, \xi \rangle$ by doubling the quaternion algebra $\langle \mu, \nu \rangle$, and we have just shown that the isomorphism class of this quaternion algebra is represented by the cup product $[\mu] \cup [\nu]$ in $H^2(\mathrm{Gal}(\overline{F}/F), \mathbf{Z}/2\mathbf{Z})$. For $[\xi]$ in $H^1(\mathrm{Gal}(\overline{F}/F), \mathbf{Z}/2\mathbf{Z})$, the cup product $[\mu] \cup [\nu] \cup [\xi]$ lies in $H^3(\mathrm{Gal}(\overline{F}/F), \mathbf{Z}/2\mathbf{Z})$. Springer and Veldkamp ([25], 190) prove that the algebra $X = \langle \mu, \nu, \xi \rangle$ determines the cup product $[\mu] \cup [\nu] \cup [\xi]$ and does not depend on the particular choice of μ, ν, and ξ used to construct X. Then as for the case of the quaternions, determining if two Cayley algebras $\langle \mu_1, \nu_1, \xi_1 \rangle$ and $\langle \mu_2, \nu_2, \xi_2 \rangle$ are isomorphic is equivalent to determining if the cup products $[\mu_1] \cup [\nu_1] \cup [\xi_1]$ and $[\mu_2] \cup [\nu_2] \cup [\xi_2]$ are cohomologous in $H^3(\mathrm{Gal}(\overline{F}/F), \mathbf{Z}/2\mathbf{Z})$. In fact, Springer and Veldkamp state that it has been shown ([25], 191) that this cup product completely determines the isomorphism class of X.

REFERENCES

[1] A. A. Albert. Quadratic forms permitting composition. *Ann. of Math.* **43** (1942), 161-177.

[2] E. Artin. *Geometric Algebra.* Interscience Publishers, Inc., New York, 1957.

[3] F. van der Blij. History of the octaves. *Simon Stevin* **34** (1961), 106-125.

[4] F. van der Blij, T. A. Springer. The arithmetics of octaves and of the group G_2. *Indag. Math.* **21** (1959), 406-418.

[5] A. Cayley. On Jacobi's elliptic functions, in reply to the Rev. B. Bronwin; and on quaternions. *Philosophical Magazine* **XXVI** (1845) 210-211. Also in *The Collected Works of Author Cayley,* Volume I. The University Press, Cambridge, 1889.

[6] ______. Note on a system of imaginaries. *Philosophical Magazine* **XXX** (1847) 257-258. Also in *The Collected Works of Author Cayley,* Volume I. The University Press, Cambridge, 1889.

[7] L. E. Dickson. *History of the Theory of Numbers, Vol. II: Diophantine analysis.* G. E. Stechert, New York, 1934.

[8] ______. On quaternions and their generalization and the history of the eight square theorem. *Ann. of Math.* **20** (1919), 155-171.

[9] H. D. Ebbinghaus, H. Hermes, F. Hirzebruch, M. Koecher, K. Mainzer, J. Neukirch, A. Prestel, R. Remmert. *Numbers.* Springer-Verlag, New York, 1991.

[10] E. Grosswald. *Representations of Integers as Sums of Squares.* Springer-Verlag, New York, 1985.

[11] W. R. Hamilton. Appendix 3: Four and Eight Squares Theorems. *Mathematical Papers of Sir William Rowan Hamilton,* Volume III: Algebra. Cambridge University Press, London-New York, 1967, 648-656.

[12] ______. Letter to Archibald. *Mathematical Papers of Sir William Rowan Hamilton,* Volume III: Algebra. Cambridge University Press, London-New York, 1967, xv-xvi.

[13] ______. Letter to Graves on Quaternions; or on a New System of Imaginaries in Algebra. *Philosophical Magazine* **XXV** (1844), 489-95. Also in *Mathematical Papers of Sir William Rowan Hamilton,* Volume III: Algebra. Cambridge University Press, London-New York, 1967, 106-110.

[14] ______. On a new species of imaginary quantities connected with the theory of quaternions. *Proc. Roy. Irish Acad.* **II** (1844), 424-434. Also in *Mathematical Papers of Sir William Rowan Hamilton*, Volume III: Algebra. Cambridge University Press, London-New York, 1967, 111-116.

[15] ______. Quaternions: Notebook Entry for 16 October 1843. *Proc. Roy. Irich Acac. L* (1945), 89-92. Also in *Mathematical Papers of Sir William Rowan Hamilton*, Volume III: Algebra. Cambridge University Press, London-New York, 1967, 103-105.

[16] T. L. Hankins. *Sir William Rowan Hamilton.* Johns Hopkins University Press, Baltimore, Md., 1980.

[17] N. Jacobson. *Basic Algebra I.* W. H. Freeman and Company, San Francisco, 1974.

[18] ______. Composition algebras and their automorphisms. *Rend. Circ. Mat. Palermo (2)* **7** (1958), 55-80.

[19] I. Kaplansky. Infinite-dimensional quadratic forms admitting composition. *Proc. Amer. Math. Soc.* **4** (1953), 956-960.

[20] S. H. Khalil, P. Yiu. The Cayley-Dickson algebras, a theorem of A. Hurwitz, and quaternions. *Bull. Soc. Sci. Lett. Łódź Sér. Rech. Déform.* **24** (1997), 117-169.

[21] R. D. Schafer. Forms permitting composition. *Advances in Math.* **4** (1970), 127-148.

[22] ______. *An Introduction to Nonassociative Algebras.* Dover Publications, Inc., New York, 1995.

[23] W. Scharlau. *Quadratic and Hermitian Forms.* Springer-Verlag, Berlin-New York, 1985.

[24] J-P. Serre. *Galois Cohomology.* Translated from the French by Patrick Ion and revised by the author. Springer-Verlag, Berlin, 1997.

[25] T. A. Springer,F. D. Veldkamp. *Octonions, Jordan Algebras and Exceptional Groups.* Springer, Berlin-New York, 2000.

[26] L. van der Waerden. *A History of Algebra.* Springer-Verlag, Berlin-New York, 1985.

[27] M. Zorn. Alternativkorper und quadratische Systeme. *Abh. Math. Sem. Hamb. Univ.* **9** (1933), 393-402.

γ

VITA

Joanne L. Eary

Candidate for the Degree of

Doctor of Education

Thesis: COMPOSITION ALGEBRAS, THE SQUARES IDENTITY, AND A PROBLEM OF HURWITZ

Major Field: Higher Education

Biographical:

Education: Bachelor of Science degree in Mathematics from Oklahoma City University in Oklahoma City, Oklahoma in May of 1993. Master of Science degree in Mathematics from Oklahoma State University in Stillwater, Oklahoma in May of 1997. Completed requirements for Doctor of Education with major in Higher Education at Oklahoma State University in May 2001.

Experience: Graduate Teaching Assistant at Oklahoma State 1993-2000, Graduate Research Assistant 1997-2000.

Professional Memberships: Mathematical Association of America, Association for Women in Mathematics