# Real Composition Algebras

by

Steven Clanton

A Thesis Submitted to the Faculty of

The Wilkes Honors College

in Partial Fulfillment of the Requirements for the Degree of

Bachelor of Arts in Liberal Arts and Sciences

with a Concentration in Mathematics

Wilkes Honors College of

Florida Atlantic University

Jupiter, FL

May 2009

# Real Composition Algebras

by

Steven Clanton

This thesis was prepared under the direction of the candidates thesis advisor, Dr. Ryan Karr, and has been approved by the members of his supervisory committee. It was submitted to the faculty of The Honors College and was accepted in partial fulfillment of the requirements for the degree of Bachelor of Arts in Liberal Arts and Sciences.

SUPERVISORY COMMITTEE:

_____
Dr. Ryan Karr

_____
Dr. Eugene Belogay

_____
Dean, Wilkes Honors College

_____
Date

## Abstract


| | |
|---|---|
| Author: | Steve Clanton |
| Title: | Real Composition Algebras |
| Institution: | Wilkes Honors College of Florida Atlantic University |
| Thesis Advisor: | Dr. Ryan Karr |
| Degree: | Bachelor of Arts in Liberal Arts and Sciences |
| Concentration: | Mathematics |
| Year: | 2009 |

According to Koecher and Remmert [Ebb91, p. 267], Gauss introduced the "composition of quadratic forms" to study the representability of natural numbers in binary (rank 2) quadratic forms. In particular, Gauss proved that any positive definite binary quadratic form can be linearly transformed into the two-squares formula $w_1^2 + w_2^2 = (u_1^2 + u_2^2)(v_1^2 + v_2^2)$. This shows not only the existence of an algebra for every form but also an isomorphism to the complex numbers for each. Hurwitz generalized the "theory of composition" to arbitrary dimensions and showed that exactly four such systems exist: the real numbers, the complex numbers, the quaternions, and octonions [CS03, p. 72].

We present a proof of Hurwitz's theorem, as given in [CS03, p. 67–72]. Along the way, we build algebras over the real numbers and define bilinear forms and quadratic forms. The proof itself uses properties of these forms, along with Dickson's doubling procedure.

# Contents

# Chapter 1

# Elements of Real Algebras

## 1.1 Structures of Real Numbers

Whenever we talk about algebraic structures, we are dealing with three kinds of objects: sets, operations, and properties. The sets for real algebras are real numbers and the real coordinate spaces.

**Definition 1.1.** An **operation** $*$ on a nonempty set $X$ is a function

$$*\,(x_1, x_2, \ldots, x_n) \mapsto x_0$$

from $X^n$ to $X$, where $X^n$ denotes the cartesian product

$$\overbrace{X \times X \times \cdots \times X}^{\text{n times}} = \{(x_1, x_2, \ldots x_n) : x_1, x_2, \ldots x_n \in X\}\,.$$

If the operation is defined for every element of the cartesian product, the set $X$ is **closed under the $n$-ary operation**. An operation that is not closed on $X$ is a **partial $n$-ary operation**.

**Definition 1.1.a.** A **unary operation** on $X$ is an operation $* : X \to X$.

**Definition 1.1.b.** A **binary operation** on $X$ is an operation $* : X \times X \to X$. We generally use the familiar infix notation $a * b$ for $*\,(a,\ b)$.

*Example* 1.1. Inversion is an example of a unary operation. The additive inverse is denoted by the prefix notation $- : x \mapsto -x$, while the multiplicative inverse is denoted by a postfix operator $^{-1} : x \mapsto x^{-1}$.

*Example* 1.2. Since the sine and cosine functions are defined for all real numbers, they are unary operations on $\mathbb{R}$. The natural logarithm is a partial operation on $\mathbb{R}$, since it is not defined for non-positive values.

*Example* 1.3. [MB99, p. 12] The sum $(m, n) \mapsto m + n$ of integers and product $(x, y) \mapsto xy$ of real numbers give the operations

$$+ : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}, \quad \cdot : \mathbb{R} \times \mathbb{R} \to \mathbb{R}$$

The sum of integers is a binary operation $+$ on the set $\mathbb{Z}$. Following tradition, we will denote the product $x \cdot y$ of $x$ and $y$ simply by $xy$.

*Example* 1.4. While the real numbers are closed under multiplication, division by zero is undefined. Thus, division is a partial operation on $\mathbb{R}$. However, division is a binary operation on $\mathbb{R} \setminus \{0\}$ .

## 1.2 The Groups of $\mathbb{R}$

**Definition 1.2.** [Haz01] The set $X$ equipped with a single binary operation $*$ is called a **magma under *** and is denoted as $(X, *)$.

*Remark.* A magma is not required to have any structure. The only property it must have is closure, as required by the definition of binary operator. While it is not required to have structure, it usually does.

*Example* 1.5. In Example 1.3, we have the magmas $(\mathbb{Z}, +)$ and $(\mathbb{R}, \cdot)$.

We now list some properties associated to a magma $(X, *)$.

**Associativity:** A magma is **associative** if $a * (b * c) = (a * b) * c$ for all $a, b, c \in X$. On the set of real numbers, addition is associative, but subtraction is not associative since $5 - (3 - 2) \neq (5 - 3) - 2$.

**Commutativity:** A magma is **commutative** if $a * b = b * a$ for all $a, b \in X$. For example, addition is commutative, while subtraction is not.

**Identity:** A magma is **unital** if it has an **identity element** $e \in X$ such that $a * e = a = e * a$ for all $a \in X$. The identity element of an additive magma $(X, +)$ is usually written as 0, and the identity element of a multiplicative magma $(X, \cdot)$ is usually written as 1. The magma formed by multiplication on the set of integers is unital, while the multiplicative magma on the even integers is not.

**Invertibility:** If there is an element $d \in X$ such that $a * d = d * a = e$ for every element $a \in X$, a magma is **invertible**.

**Definition 1.3.** A **group** is a magma that is associative, unital, and invertible. An **abelian group** is a group that is also commutative.

*Example* 1.6. We have given multiplication and addition as examples of binary operations. When we list the properties in the usual notation, we can quickly verify that $(\mathbb{R}, +)$ and $(\mathbb{R} \setminus \{0\}, \cdot)$ are abelian groups. Note that $(\mathbb{R}, \cdot)$ is not invertible (and hence not a group).

## 1.3 The Field of Real Numbers

Several operations are defined for the real numbers. In particular, the real numbers are both an additive abelian group and a multiplicative abelian group. The two groups satisfy the distributive law, and hence form a field.

| Property | $(\mathbb{R}, +)$ | $(\mathbb{R} \setminus \{0\}, \cdot)$ |
|---|---|---|
| Associative | $(a+b)+c = a+(b+c)$ | $(ab)\,c = a\,(bc)$ |
| Unital | $a+0 = a = 0+a$ | $a1 = a = 1a$ |
| Invertible | $a+(-a) = 0 = -a+a$ | $(1/a)\,a = 1 = a\,(1/a) \quad a \neq 0$ |
| Commutative | $a+b = b+a$ | $ab = ba$ |

Table 1.1: Properties of an abelian group for $+$ and $\cdot$

**Definition 1.4.** An operation $\cdot$ is **distributive** over an operation $+$ if it satisfies both left-distributive and right-distributive identities:

$$a\,(b+c) = ab + ac \qquad \text{(Left distributive)}$$

$$(a+b)\,c = ac + bc \qquad \text{(Right distributive)}$$

If it satisfies only one of the identities it is called left or right distributive, respectively.

**Definition 1.5.** A **field** $(F, \cdot, +)$ is a set $F$ with two binary operations, addition and multiplication, such that

- the additive magma $(F, +)$ and the multiplicative magma $(F\backslash\{0\}, \cdot)$ are abelian groups;
- multiplication is distributive over addition.

There are also ways to combine sets and operations. Scalar multiplication is an important example.

**Definition 1.6.** A group $G$ **acts on a set** $X$ when there is a function $(g, x) \mapsto gx$ from $G \times X$ to $X$ that satisfies

$$1_G x = x \quad \text{and} \quad g_2\,(g_1 x) = (g_2 g_1)\,x.$$

**Definition 1.7.** A **scalar multiplication** is an action of the multiplicative group of a field $F$ on an additive abelian group $G$ where each action is left distributive over addition in $G$ and right distributive over addition in $F$. That is,

$$\lambda\left(u+v\right)=\lambda u+\lambda v$$

$$\left(\kappa+\lambda\right)u=\kappa u+\lambda u$$

for all $\lambda$ and $\kappa$ in $F$ and for all $u$ and $v$ in $G$.

*Remark.* Since an action on $X$ defines a function $X \to X$, each action is a unary operation.

*Example* 1.7. The multiplicative group of any field acts on its own additive group and on itself.

## 1.4 Vectors in Real Coordinate Space

We have reviewed the properties of the field $\mathbb{R}$ on which our algebras will be built. The other important set is that of $n$-tuples of real numbers, or points in $\mathbb{R}^n$. We will consider three operations on points. The first two, vector addition and scalar multiplication, define the real coordinate space. They are defined concretely, by an explicit function. The remaining operation is multiplication in the algebra.

**Definition 1.8.** A **real vector space** $V$ is an additive abelian group $V$ with a scalar multiplication from $\mathbb{R}$.

*Example* 1.8. A field is a trivial vector space. If we define the elements of the field to be both scalars and vectors, the axioms for a vector space hold. Note that the sum $+ : \mathbb{R}^2 \to \mathbb{R}, (x, y) \mapsto x + y$ and product $\cdot : \mathbb{R}^2 \to \mathbb{R}, (x, y) \mapsto xy$ in the field $\mathbb{R}$ are binary operations, while the scalar product is a set of unary operations $c : \mathbb{R} \to \mathbb{R}, y \mapsto cy$. We still have a set of vectors and a set of scalars, but the two sets are equal.

**Definition 1.9.** The $n$**-space** $\mathbb{R}^n$ is the set of ordered $n$-tuples

$$\mathbb{R}^n = \{(x_1, x_2, \ldots, x_n) : x_i \in \mathbb{R}\}$$

with pointwise addition

$$x + y = (x_1 + y_1, x_2 + y_2, \ldots, x_n + y_n)$$

and scalar multiplication

$$\lambda x = (\lambda x_1, \lambda x_2, \ldots, \lambda x_n)$$

for $\lambda \in \mathbb{R}$ and $x, y \in \mathbb{R}^n$.

**Definition 1.10.** The **standard basis vectors**, also called **basis elements**, for the $n$-space $\mathbb{R}^n$ are denoted

$$\begin{aligned} e_1 &= (1, 0, \ldots, 0), \\ e_2 &= (0, 1, \ldots, 0), \\ &\vdots \\ e_n &= (0, 0, \ldots, 1). \end{aligned}$$

The basis elements allow us to use the notation

$$(x_1, x_2, \ldots, x_n) = x_1 (1, 0, \ldots, 0) + x_2 (0, 1, \ldots, 0) + \cdots + x_n (0, 0, \ldots, 1) = \sum_{i=1}^{n} x_i e_i$$

and to restate vector addition and scalar multiplication as

$$x + y = \sum_{i=1}^{n} x_i e_i + \sum_{i=1}^{n} y_i e_i = \sum_{i=1}^{n} (x_i + y_i) e_i$$

$$\lambda x = \lambda \sum_{i=1}^{n} x_i e_i = \sum_{i=1}^{n} \lambda x_i e_i = \sum_{i=1}^{n} (\lambda x_i) e_i,$$

where $x$, $y$, and $e_i$ are vectors and $x_i$, $y_i$, and $\lambda$ are scalars.

## 1.5 Real Algebras

At this point, we have defined our two main sets, the scalars $\mathbb{R}$ and real coordinate space $\mathbb{R}^n$. We know that $\mathbb{R}$ satisfies the axioms for a field, and we know that $\mathbb{R}^n$ is a vector space. The remaining operation, multiplication in the algebra, is defined by its properties, and our main objective is to find the algebras that satisfy these properties.

**Definition 1.11.** A **real algebra** $A$ is a vector space $A$ with an additional binary operation on $A$, usually called multiplication, where multiplication is distributive over addition and

$$\lambda (ab) = (\lambda a) b = a (\lambda b) \tag{1.1}$$

holds for all scalars $\lambda$ in $\mathbb{R}$ and all vectors $a$ and $b$ in $A$.

*Remark.* An algebra over a field is made of two structures: a vector space and a multiplicative magma. Distributivity and Property (1.1) are called the **conditions for bilinearity**.

*Example* 1.9 (Algebra of Real Numbers)*.* As previously noted, the real numbers form a vector space. The bilinearity of its product is obvious since the scalars and vectors are elements from the same field.

The complex numbers are one of the real composition algebras. Accordingly, it appears in multiple examples.

*Example* 1.10 (Algebra of Complex Numbers). We have seen that $\mathbb{R}^2$ is a vector space. Multiplication of complex numbers is defined by

$$(a, b) (c, d) = (ac - bd, ad + bc) .$$

First we must show that the multiplication so defined is closed, not partial. Since the real numbers are closed under multiplication and addition, complex multiplication

is a binary operation. To show bilinearity, we verify the distributive laws, and we expand each of the three products in (1.1) to compare:

$$\begin{aligned}(a+a_1, b+b_1)(c,d) &= ((a+a_1)c - (b+b_1)d, (a+a_1)d + (b+b_1)c) \\ &= (ac + a_1c - bd - b_1d, ad + a_1d + bc + b_1c) \\ &= (ac - bd, ad + bc) + (a_1c - b_1d, a_1d + b_1c) \\ &= (a,b)(c,d) + (a_1,b_1)(c,d).\end{aligned}$$

$$\begin{aligned}(a,b)(c+c', d+d') &= (a(c+c') - b(d+d'), a(d+d') + b(c+c')) \\ &= (ac + ac' - bd - bd', ad + ad' + bc + bc') \\ &= (ac - bd, ad + bc) + (ac' - bd', ad' + bc') \\ &= (a,b)(c,d) + (a,b)(c',d').\end{aligned}$$

$$\begin{aligned}\lambda((a,b)(c,d)) &= \lambda(ac - bd, ad + bc) = (\lambda ac - \lambda bd, \lambda ad + \lambda bc), \\ (\lambda(a,b))(c,d) &= (\lambda a, \lambda b)(c,d) = (\lambda ac - \lambda bd, \lambda ad + \lambda bc), \\ (a,b)(\lambda(c,d)) &= (a,b)(\lambda c, \lambda d) = (a\lambda c - b\lambda d, a\lambda d + b\lambda c) \\ &= (\lambda ac - \lambda bd, \lambda ad + \lambda bc).\end{aligned}$$

We see that the verification is fairly tedious. However, an algebra can be defined in another way. First, we will prove the general distributive law. Then we will use it to show that multiplication in an algebra is specified completely by the products of its basis elements.

**General Distributive Law.** Let $a_1, \ldots, a_m$ and $b_1, \ldots, b_n$ be elements from some algebraic structure where the operation denoted by juxtaposition is distributive over the operation denoted by $+$. Then,

$$\left(\sum_{i=1}^{m} a_i\right)\left(\sum_{j=1}^{n} b_j\right) = \sum_{i=1}^{m}\sum_{j=1}^{n}(a_i b_j) \qquad \text{(General Distributive Property)}$$

*Proof.* Since addition is closed, there is some element $b$ that is the sum

$$b = \sum_{j=1}^{n} b_j.$$

We use induction on $m$ and $n$ with right and left distributivity, respectively, to show that

$$\left(\sum_{i=1}^{m} a_i\right) b = \sum_{i=1}^{m}(a_i b) \quad \text{and} \quad a_i \sum_{j=1}^{n} b_j = \sum_{j=1}^{n} a_i b_j.$$

always hold. Now, we combine these identities to show

$$\left(\sum_{i=1}^{m} a_i\right)\left(\sum_{j=1}^{n} b_j\right) = \left(\sum_{i=1}^{m} a_i\right) b = \sum_{i=1}^{m}(a_i b) = \sum_{i=1}^{m}\left(a_i \sum_{j=1}^{n} b_j\right) = \sum_{i=1}^{m}\sum_{j=1}^{n}(a_i b_j).$$

□

Now we apply the general distributive law to the product of vectors:

$$\begin{aligned} xy &= \left(\sum_{i=1}^{n} x_i e_i\right)\left(\sum_{j=1}^{n} y_j e_j\right) && \text{(by def. of basis)} \\ &= \sum_{i=1}^{n}\sum_{j=1}^{n}\left((x_i e_i)(y_j e_j)\right) && \text{(by general distributivity)} \\ &= \sum_{i=1}^{n}\sum_{j=1}^{n}\left((x_i y_j)(e_i e_j)\right). && \text{(by bilinearity)} \end{aligned}$$

*Example* 1.11 (The Complex Numbers). We start with $\mathbb{R}^2$ and write $e_1 = 1$ and $e_2 = i$, where $i^2 = -1$ as usual. We have $2^2$ products of the two basis vectors:

$$1^2 = 1, \quad i^2 = -1, \quad 1i = i, \quad i1 = i.$$

We examine the equation

$$xy = \sum_{i}^{n}\sum_{j}^{n}\left((x_i y_j)(e_i e_j)\right)$$

to determine the coefficients for basis vectors in the product. For example, since 1 is the product of two basis elements $1 = 1^2 = e_1 e_1$ and $1 = -i^2 = -e_2 e_2$, the coefficient of 1 will be the sum of $x_1 y_1$ and $-x_2 y_2$. Likewise, the coefficients of $i$ in the product will be the sum of $x_1 x_2$ and $x_2 x_1$, since $i = e_1 e_2$ and $i = e_2 e_1$. Thus, we recover the usual complex multiplication as defined by

$$(x_1 + x_2 i)(y_1 + y_2 i) = (x_1 y_1 - x_2 y_2) + (x_1 y_2 + x_2 y_1) i$$

*Example* 1.12 (The Quaternions). Here, we start with $\mathbb{R}^4$. As is traditional, we call the basis elements for the quaternions 1, $i$, $j$, and $k$. They satisfy Hamilton's equations

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

From this, we can verify

$$\begin{aligned} 1 = 1^2 = -i^2 = -j^2 = -k^2. \\ i = 1i = i1 = jk = -kj \\ j = 1j = j1 = ki = -ik \\ k = 1k = k1 = ij = -ji. \end{aligned}$$

Finding the corresponding basis element coefficients, we have

$$\begin{aligned} (x_1 + x_2 i + x_3 j + x_4 k)(y_1 + y_2 i + y_3 j + y_4 k) = {} & (x_1 y_1 - x_2 y_2 - x_3 y_3 - x_4 y_4) \\ & + (x_1 y_2 + x_2 y_1 + x_4 y_3 - x_4 x_3) i \\ & + (x_1 y_3 + x_3 y_3 + x_4 y_2 - x_1 x_4) j \\ & + (x_1 y_4 + x_4 y_1 + x_1 y_2 - x_2 y_1) k. \end{aligned}$$

# Chapter 2

# Composition Algebras

In this chapter, all vector spaces and algebras will be real. Also, we will work in $\mathbb{R}^n$ for some fixed but arbitrary $n$. We have the basis vectors $e_1, \ldots, e_n$. When we use ordinary variables, such as $x$ and $y$ to represent vectors or elements of an algebra, it is understood that they have coordinates in $\mathbb{R}^n$:

$$x = (x_1, \ldots, x_n) \text{ and } y = (y_1, \ldots, y_n).$$

## 2.1 Bilinear and Quadratic forms

**Definition 2.1.** Let $V$ and $W$ be real vector spaces. A function $f : V \times V \to W$ is **bilinear** if

$$f(\lambda v + \mu v', w) = \lambda f(v, w) + \mu f(v', w) \qquad \text{(Left linearity)}$$

and

$$f(v, \lambda w + \mu w') = \lambda f(v, w) + \mu f(v, w') \qquad \text{(Right linearity)}$$

both hold for all $v$ and $w$ in $V$ and all $\lambda$ and $\mu$ in $\mathbb{R}$.

We called the axioms for an algebra the condition for bilinearity. We now verify the appropriateness of the term.

**Proposition 2.1.** *Suppose $V$ is a real vector space with a binary multiplication. If the multiplication is bilinear, then $V$ is an algebra.*

*Proof.* Bilinearity of multiplication gives us

$$a(\lambda b + \mu b') = a(\lambda b) + a(\mu b') = \lambda(ab) + \mu(a'b)$$
$$= (\lambda a + \mu a')b = (\lambda a)b + (\mu a')b = \lambda(ab) + \mu(a'b).$$

The distributive laws are a special case with $\lambda = \mu = 1$:

$$a(b + b') = a(1b + 1b') = 1(ab) + 1(ab') = ab + ab'$$
$$(a + a')b = (1a + 1a')b = 1(ab) + 1(a'b) = ab + a'b.$$

Bilinearity also implies that (1.1) holds:

| | | |
|---|---|---|
| $(\lambda v)w = ((\lambda + 0)v)w$ | $v(\lambda w) = v((\lambda + 0)w)$ | Additive Identity in $\mathbb{R}$ |
| $= (\lambda v + 0v)w$ | $= v(\lambda w + 0w)$ | Scalar law for $V$ |
| $= \lambda(vw) + 0(vw)$ | $= \lambda(vw) + 0(vw)$ | Bilinearity |
| $= (\lambda + 0)(vw)$ | $= (\lambda + 0)(vw)$ | Scalar Law for $V$ |
| $= \lambda(vw).$ | $= \lambda(vw).$ | Additive Identity for $\mathbb{R}$ |

□

**Definition 2.2.** Let $x$ and $y$ be vectors. A **bilinear form** $B$ is a polynomial of the form

$$B(x, y) = \sum_{i=1}^{n}\sum_{j=1}^{n} x_i a_{ij} y_j.$$

We can express the bilinear form using matrix notation:

$$\sum_{i=1}^{n}\sum_{j=1}^{n} x_i a_{i,j} y_j = \sum_{i=1}^{n} x_i \sum_{j=1}^{n} a_{i,j} y_j = \sum_{i=1}^{n} x_i \left(Ay^T\right) = xAy^T.$$

Thus $B(x, y) = xAy^T$ for some matrix $A$.

*Example* 2.1. Consider the complex number $z = (z_1, z_2)$ and suppose $z = xy$ for some complex numbers $x$ and $y$. We obtain two examples of bilinear forms:

$$f(x,y) = z_1 = x_1y_1 - x_2y_2 \quad \text{and} \quad g(x,y) = z_2 = x_1y_2 + x_2y_1.$$

**Proposition 2.2.** *If $x$ and $y$ are elements of an algebra, there are bilinear forms $B_1, \ldots, B_n$ such that*

$$xy = \left( \sum_{k=1}^{n} B_k(x,y) \right) e_k. \tag{2.1}$$

*Proof.* Let $x$ and $y$ be arbitrary elements of the algebra. Since multiplication is closed, the product of two basis elements will be in the space spanned by the basis elements. Thus there are real coefficients such that

$$x = \sum_{i=1}^{n} x_i e_i, \quad y = \sum_{j=1}^{n} y_j e_j, \quad \text{and} \quad e_i e_j = \sum_{k=1}^{n} a_{i,j}^{(k)} e_k.$$

Using these representations, the product is

$$\begin{aligned} \left( \sum_{i=1}^{n} x_i e_i \right) \left( \sum_{j=1}^{n} y_j e_j \right) &= \sum_{i,j=1}^{n} \left( (x_i e_i)(y_j e_j) \right) = \sum_{i,j=1}^{n} \left( (x_i y_j)(e_i e_j) \right) \\ &= \sum_{i,j=1}^{n} \left( (x_i y_j) \sum_{k=1}^{n} a_{i,j}^{(k)} e_k \right) = \sum_{i,j,k=1}^{n} x_i y_j a_{i,j}^{(k)} e_k. \end{aligned}$$

To get the coordinate of some particular basis element, just fix $k$:

$$\sum_{i,j=1}^{n} x_i y_j a_{i,j}^{(k)} e_k = \left( \sum_{i,j=1}^{n} x_i y_j a_{i,j}^{(k)} \right) e_k = \left( x A_k y^T \right) e_k = B_k(x,y)\, e_k.$$

□

*Example* 2.2. The cross product in $\mathbb{R}^3$ is an example of a bilinear multiplication. For the cross product $w = u \times v$, we have three bilinear forms:

$$\begin{aligned} w_1(u_1, u_2, u_3; v_1, v_2, v_3) &= u_2v_3 - u_3v_2, \\ w_2(u_1, u_2, u_3; v_1, v_2, v_3) &= u_3v_1 - u_1v_3, \\ w_3(u_1, u_2, u_3; v_1, v_2, v_3) &= u_1v_2 - u_2v_1. \end{aligned}$$

The corresponding matrices can be constructed using coefficients:

$$A_1 = \begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & -1 & 0 \end{bmatrix}, A_2 = \begin{bmatrix} 0 & 0 & -1 \\ 0 & 0 & 0 \\ 1 & 0 & 0 \end{bmatrix}, A_3 = \begin{bmatrix} 0 & 1 & 0 \\ -1 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix}.$$

We could have also determined these matrices by using the products of the basis vectors:

$$e_1^2 = e_2^2 = e_3^2 = 0$$

$$e_1 e_2 = e_3 = -e_2 e_1$$

$$e_2 e_3 = e_1 = -e_3 e_2$$

$$e_3 e_1 = e_2 = -e_1 e_3.$$

**Definition 2.3.** [MB99, p. 341] A bilinear form $B$ is **symmetric** if $B(u, v) = B(v, u)$. If, for some nonzero $u$, we have $B(u, v) = 0$ for all $v$, then the form is called **degenerate**; otherwise it is **nondegenerate**.

**Definition 2.4.** [CS03, MB99] A function $q : V \to W$ is called a **quadratic form** if and only if scalars behave quadratically, that is

$$q(\lambda v) = \lambda^2 q(v),$$

and the function $B$ defined by

$$2B(u, v) = q(u + v) - q(u) - q(v)$$

is a symmetric bilinear form.

We call the form $B$ the bilinear form **associated** to $q$. Conversely, if we are given a bilinear form $B$ we can construct a unique quadratic form $q$ such that $B$ is associated to $q$:

**Proposition 2.3.** *Given a symmetric bilinear form $B : V \times V \to W$, there is exactly one quadratic form $q : V \to W$ such that*

$$2B(u, v) = q(u + v) - q(u) - q(v), \tag{2.2}$$

*and it is the function $q : v \mapsto B(v, v)$.*

*Proof.* The bilinear form for $q$ is symmetric by hypothesis. Since $B$ is bilinear, we have

$$q(\lambda v) = B(\lambda v, \lambda v) = \lambda^2 B(v, v) = \lambda^2 q(v).$$

Next, we have

$$\begin{aligned} q(u + v) - q(u) - q(v) &= B(u + v, u + v) - B(u, u) - B(v, v) \\ &= B(u, u + v) + B(v, u + v) - B(u, u) - B(v, v) \\ &= B(u, v) + B(v, u). \end{aligned}$$

However, since B is symmetric we have

$$q(u + v) - q(u) - q(v) = B(u, v) + B(v, u) = 2B(u, v).$$

□

## 2.2 Composition and Quadratic Forms

In this section we will eventually define what is known as a "composition algebra." The real numbers, the complex numbers, and the quaternions are composition algebras, as we shall soon see. The majority of books on quaternions focus on their geometric interpretation, in particular, their connection to rotations in $\mathbb{R}^3$. The multiplication of complex numbers and quaternions may suggest that the idea of a composition algebra originally arose from "composing" rotations in $n$-space, but that is not the case. Composition algebras arose from "composing" quadratic forms.

Koecher and Remmert explain that mathematicicans, such as Legendre and Gauss, introduced the "composition of binary quadratic forms" to study the representability of natural numbers by binary quadratic forms. For example, consider $x^2 + y^2$, the sum of two squares. Using complex numbers, we can see how the two sums $u_1^2 + u_2^2$ and $v_1^2 + v_2^2$ can be multiplied, or "composed," to obtain a new sum of two squares:

$$\begin{aligned}\left|\left(u_1 + iu_2\right)\left(v_1 + iv_2\right)\right|^2 &= \left|\left(u_1v_1 + u_1iv_2 + iu_2v_1 + iu_2iv_2\right)\right|^2 \\ &= \left|\left(u_1v_1 - u_2v_2\right) + i\left(u_1v_2 + u_2v_1\right)\right|^2 \\ &= \left(u_1v_1 - u_2v_2\right)^2 + \left(u_1v_2 + u_2v_1\right)^2.\end{aligned}$$

Noting that

$$\left|\left(u_1 + iu_2\right)\left(v_1 + iv_2\right)\right|^2 = \left|\left(u_1 + iu_2\right)\right|^2\left|\left(v_1 + iv_2\right)\right|^2 = \left(u_1^2 + u_2^2\right)\left(v_1^2 + v_2^2\right),$$

we find that the product of the two forms on the right is once again a sum of squares $w_1^2 + w_2^2$, where $w_1 = u_1v_1 - u_2v_2$ and $w_2 = u_1v_2 + u_2v_1$.

Later, the composition of quadratic forms was generalized to dimensions higher than two. A "theory of composition" is said to exist when there is a set of bilinear forms $B_k(x, y)$ such that

$$q_1\left(x\right)q_2\left(y\right) = q_3\left(z\right) \tag{2.3}$$

holds, where $q_i$ is the quadratic form associated to $B_i$. Koecher and Remmert [Ebb91, p. 268] quote Hurwitz: "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 (2.3), the following equation:

$$\left(x_1^2 + x_2^2 + \cdots + x_n^2\right)\left(y_1^2 + y_2^2 + \cdots + z_n^2\right) = \left(z_1^2 + z_2^2 + \cdots + z_n^2\right)\text{"} \tag{2.4}$$

In fact, the multiplication rule for the first known composition algebras "gave the first intimation of their existence in the theory of sums of squares" [Sti02, p. 395].

**Definition 2.5.** A **real composition algebra** is a unital (but not necessarily associative) real algebra $A$, along with a nondegenerate quadratic form $[\ ] : A \to \mathbb{R}$, called a **norm**, that satisfies

$$[xy] = [x]\,[y] \qquad \text{(composition law)}$$

The bilinear form associated to $[\ ]$ will be denoted $[u, v]$. This is also called an **inner product**.

Note that the norm of a real composition algebra is the square of the usual Euclidean norm.

*Example* 2.3 (Real and complex numbers). The set of real numbers $\mathbb{R}$ forms a composition algebra over itself, with the usual multiplication; the norm is given by $[x] = x^2$. The complex numbers form a composition algebra over $\mathbb{R}$; the norm is given by $[z] = z_1^2 + z_2^2$. The associated inner product is

$$\begin{aligned}[x, y] &= \frac{[x + y] - [x] - [y]}{2} \\ &= \frac{(x_1 + y_1)^2 + (x_2 + y_2)^2 - (x_1^2 + x_2^2) - (y_1^2 + y_2^2)}{2} \\ &= x_1 y_1 + x_2 y_2.\end{aligned}$$

Complex multiplication has bilinear forms corresponding to the matrices

$$A_1 = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}, A_2 = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}.$$

Recall that these bilinear forms are not the basis elements themselves, but are specified by the multiplication of basis elements:

$$\left.\begin{aligned} e_1 e_1 &= a^{(1)}_{1,1} e_1 + a^{(2)}_{1,1} e_2 = e_1 \\ e_1 e_2 &= a^{(1)}_{1,2} e_1 + a^{(2)}_{1,2} e_2 = e_2 \\ e_2 e_1 &= a^{(1)}_{2,1} e_1 + a^{(2)}_{2,1} e_2 = e_2 \end{aligned}\right\} e_1 = 1 \text{ is the identity element;}$$

$$\left.e_2 e_2 = a^{(1)}_{2,1} e_1 + a^{(2)}_{2,1} e_2 = -e_1\right\} e_2^2 = -1, \text{ as expected.}$$

## 2.3 Properties and Operations for Composition

In the next chapter, we will give a proof that there are four real composition algebras, as given in [CS03]. There are a few things we still need. Ultimately, we need to define a Dickson double. First, we need to define conjugation, since conjugation is used to define multiplication in a Dickson double algebra.

**Definition 2.6.** We define the **conjugate** $\bar{x}$ of $x$ by the formula

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

*Note.* This is equivalent to the familiar definition of conjugation in $\mathbb{C}$, since $[x, 1]$ is just the real part of $x$ and we expect the conjugate to be the real part of $x$ minus the imaginary part of $x$. Hence subtracting both the real and imaginary parts from twice the real part of $x$ gives us the usual conjugate.

We next list some laws for composing nondegenerate quadratic forms.

**Composition Law:** $[xy] = [x]\,[y]$.

*Note.* This is true by definition.

**Cancellation Law:** $[x, t] = [y, t]$ for all $t$ implies $x = y$.

*Proof.* The difference of the forms is zero for all $t$:

$$0 = [x, t] - [y, t] = [x - y, t] \qquad \text{(by bilinearity)}$$

By the definition of a nondegenerate bilinear form, we know $x - y = 0$, that is $x = y$. □

**Scaling Laws:** $[xy, xz] = [x]\,[y, z]$ and $[xz, yz] = [x, y]\,[z]$.

*Proof.* Verification for the left multiplication is the same as for the right, since the form and the product are both bilinear.

$$\begin{aligned}
2\,[xy, xz] &= [xy + xz] - [xy] - [xz] && \text{(by Def. 2.4)} \\
&= [x\,(y + z)] - [xy] - [xz] \\
&= [x]\,[(y + z)] - [x]\,[y] - [x]\,[z] && \text{(by composition)} \\
&= [x]\,(2\,[y, z] + [y] + [z]) - [x]\,[y] - [x]\,[z] && \text{(by Def. 2.4)} \\
&= 2\,[x]\,[y, z] + ([x]\,[y]\,[x]\,[z]) - ([x]\,[y]\,[x]\,[z]) \\
&= 2\,[x]\,[y, z]\,.
\end{aligned}$$

□

**The Exchange Law:** $[xy, uz] = 2\,[x, u]\,[y, z] - [xz, uy]$.

*Proof.*

$$\begin{aligned}
2\,[x, u]\,[y, z] &= ([x + u] - [x] - [u])\,[y, z] && \text{(by Def. 2.4)} \\
&= [x + u]\,[y, z] - [x]\,[y, z] - [u]\,[y, z] \\
&= [(x + u)\,y, (x + u)\,z] - [xy, xz] - [uy, uz] && \text{(by scaling)} \\
&= [xy + uy, xz + uz] - [xy, xz] - [uy, uz] \\
&= [xy, xz + uz] + [uy, xz + uz] - [xy, xz] - [uy, uz] \\
& && \text{(by bilinearity)} \\
&= [xy, xz] + [xy, uz] + [uy, xz] + [uy, uz] - [xy, xz] - [uy, uz] \\
&= [xy, uz] + [uy, xz]\,.
\end{aligned}$$

□

**Braid Laws:** $[xy, z] = [y, \bar{x}z]$ and $[xy, z] = [x, z\bar{y}]$.

*Proof.* To show the left identity, we use $u = 1$ in the exchange law then simplify:

$$\begin{aligned}
[xy, z] &= 2\,[x, 1]\,[y, z] - [xz, y] && \text{(by exchange)} \\
&= [y, 2\,[x, 1]\,z] - [xz, y] && \text{(by bilinearity)} \\
&= [y, 2\,[x, 1]\,z] - [y, xz] && \text{(symmetry)} \\
&= [y, (2\,[x, 1] - x)\,z] && \text{(by bilinearity)} \\
&= [y, \bar{x}z]\,. && \text{(by Def. 2.6)}
\end{aligned}$$

To show the left, we multiply by 1 on the right:

$$\begin{aligned}
[xy, z1] = 2\,[x, z]\,[y, 1] - [x, zy] = [x, 2\,[y, 1]\,z] - [x, yz] \\
= [x, (2\,[y, 1] - y)\,z] = [x, z\bar{y}]\,.
\end{aligned}$$

□

The next two proofs are taken directly from [CS03].

**Biconjugation:** $\bar{\bar{x}} = x$.

*Proof.* We use the braid law twice on the inner product with an arbitrary $t$:

$$[x, t] = [x1, t] = [1, \bar{x}t] = [\bar{\bar{x}}1, t] = [\bar{\bar{x}}, t]\,.$$

□

**Product Conjugation:** $\overline{xy} = \bar{y}\,\bar{x}$.

*Proof.* Repeatedly apply the braid laws to $\bar{y}\,\bar{x}$ and simplify with biconjugation:

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

□

## 2.4 The Dickson Double Algebra

In 1914, Dickson generalized the procedure for multiplying pairs of coordinates [Sti02, p. 394]. This procedure is called **doubling**. If we double the real numbers, as an example, we add a unit $i_1$ that squares to $-1$ and that is also orthogonal to the real—that is, $[i_1, x] = 0$ for every $x \in \mathbb{R}$. The algebra generated by this first doubling gives us $\mathbb{C}$. Next, we add another unit $i_2$ that squares to $-1$ and such that $[i_2, x] = 0$ for every $x \in \mathbb{C}$. This gives us the quaternions. Continuing, we add a unit $i_4$ that squares to $-1$ and is orthogonal to the set of quaternions. We use the notation $i_4$ since we are doubling a space of dimension 4. The double of the quaternions is called the **octonions**.

To multiply, we work backward with the **multiplication rule**

$$ab = (a_1, a_2) \times (b_1, b_2) = \left(a_1 b_1 - \bar{b}_2 a_2, b_2 a_1 + a_2 \bar{b}_1\right),$$

where $a$ and $b$ are in the double of the algebra containing $a_1, a_2, b_2$, and $b_2$.

We have just defined the octonions as the Dickson double of the quaternions. We can also describe the octonions by using the so-called Cayley matrices [Sti02, p. 392], as given by Cayley in 1858. The representation

$$a + bi + cj + dk = a \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} + b \begin{bmatrix} i & 0 \\ 0 & -i \end{bmatrix} + c \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix} + d \begin{bmatrix} 0 & i \\ i & 0 \end{bmatrix}$$

of a quaternion by Cayley matrices can be summed to yield

$$a + bi + cj + dk = \begin{bmatrix} a + bi & c + di \\ -c + di & a - bi \end{bmatrix} = \begin{bmatrix} a + bi & c + di \\ -\left(\overline{c + di}\right) & \overline{a + bi} \end{bmatrix}.$$

Now we can quickly verify that the matrices for $i$, $j$, and $k$ are roots of $x^2 = -1$ and that $ijk = -1$. We can also verify that setting $c = d = 0$ yields an isomorphism between 2-by-2 matrices and the complex numbers and that $b = c = d = 0$ yields an isomorphism to the reals. We now list the rest of the Cayley matrices:

$$1 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \qquad i_1 = \begin{bmatrix} i & 0 \\ 0 & -i \end{bmatrix} \qquad i_2 = \begin{bmatrix} j & 0 \\ 0 & -j \end{bmatrix} \qquad i_3 = \begin{bmatrix} k & 0 \\ 0 & -k \end{bmatrix}$$

$$i_4 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}\begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix} \quad i_5 = \begin{bmatrix} i & 0 \\ 0 & -i \end{bmatrix}\begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix} = \begin{bmatrix} 0 & i \\ i & 0 \end{bmatrix}$$

$$i_6 = \begin{bmatrix} j & 0 \\ 0 & -j \end{bmatrix}\begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix} = \begin{bmatrix} 0 & j \\ j & 0 \end{bmatrix} \quad i_7 = \begin{bmatrix} k & 0 \\ 0 & -k \end{bmatrix}\begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix} = \begin{bmatrix} 0 & k \\ k & 0 \end{bmatrix}$$

Finally, we give two more laws that are needed in the next chapter.

**Inner Product:** $[a + bi,\, c + di] = [a,\, c] + [b,\, d]$.

*Proof.* First we expand

$$\begin{aligned} [a + bi,\, c + di] &= [a,\, c + di] + [bi,\, c + di] && \text{(by bilinearity)} \\ &= [a,\, c] + [a,\, di] + [bi,\, c] + [bi,\, di] && \text{(by bilinearity)} \\ &= [a,\, c] + [a,\, di] + [bi,\, c] + [bi,\, di]\,[i]\,. && \text{(by composition)} \end{aligned}$$

Now we use the braid law to show $[a,\, di] = \left[\bar{d}a, i\right]$ and $[bi,\, c] = \left[i,\, \bar{b}c\right]$. Since $\bar{d}a$ and $\bar{b}c$ are in the space we double, $i$ is orthogonal and the inner products $[a,\, di] = [bi,\, c] = 0$.

□

**Double Conjugate:** $ib = -\overline{ib} = \bar{b}i$.

*Proof.*

$$\overline{ib} = 2\,[ib, 1] - ib = -ib \qquad \text{(by Def. 2.6)}$$

$$\bar{b}i = -\bar{b}\,\bar{i} = -\overline{ib} = ib.$$

□

# Chapter 3

# Enumerating the Real Composition Algebras

## 3.1 Real Composition Algebras

In the last chapter we defined the notion of a real composition algebra. Recall that we have already defined four real composition algebras up to this point: the real numbers, the complex numbers, the quaternions, and the octonions. There are several famous results about these algebras. In 1863, Weierstrass used the Fundamental Thereom of Algebra to prove that the real and complex numbers are the only two commutative and associative real composition algebras [Ebb91, p. 119-120]. There is also a proof by Hopf that does not use the Fundamental Theorem of Algebra. In fact, Hopf proves a lemma which implies the Fundamental Theorem of Algebra and the famous Gelfand-Mazur Theorem as "simple" corollaries [Ebb91, 230-235]. Frobenius proved that any associative real composition algebra is isomorphic to either the real numbers, the complex numbers, or the quaternions [Ebb91, p. 229]. In this chapter, we will give a proof of Hurwitz's theorem, which states that the only real composition algebras are the four algebras given above.

## 3.2 Dimension of a Composition Algebra

The original counterexample to the existence of a composition algebra in $\mathbb{R}^3$ is due to Legendre. He used the decomposition $3 = 1^2 + 1^2 + 1^2$ and $21 = 4^2 + 2^2 + 1^2$, but we will use 3 and $5 = 0^2 + 1^2 + 2^2$ as given by Stillwell [Ebb91, Sti02]. In either case, the point is that there cannot be any bilinear functions $A(a_1, b_1, c_1; a_2, b_2, c_2)$, $B(a_1, b_1, c_1; a_2, b_2, c_2)$, and $C(a_1, b_1, c_1; a_2, b_2, c_2)$ with

$$A^2 + B^2 + C^2 = \left(a_1^2 + b_1^2 + c_1^2\right)\left(a_2^2 + b_2^2 + c_2^2\right),$$

since there are no three integers whose sum of squares equals

$$15 = 3 \cdot 5 = \left(1^2 + 1^2 + 1^2\right)\left(0^2 + 1^2 + 2^2\right)$$

This can be checked by trial-and-error.

Koecher and Remmert [Sti02, p. 190] gave a proof by contradiction by assuming the product of the bases elements $i$ and $j$ in $\mathbb{R}^3$ is in the space spanned by 1, $i$, and $j$. They assumed that the multiplication in $\mathbb{R}^3$ extends complex multiplication, where $i^2 = -1$, as usual. Their proof also assumes that the multiplication is associative, which implies $i(ij) = (ii)j = -j$. Suppose we can write $ij = a + bi + cj$ for real numbers $a$, $b$, and $c$. Now we can combine these facts to find the additive inverse of $j$:

$$-j = (ii)j = i(ij) = i(a + bi + cj) = ai - b + cij.$$

Substituting $a + bi + cj$ for $ij$ again, we find

$$-j = ai - b + cij = ai - b + c(a + bi + cj) = (ca - b) + (a - bc)i + c^2 j.$$

This gives us three conditions: the coefficient of 1 is $ca - b = 0$, the coefficient of $i$ is $a - bc = 0$, and the coefficient of $j$ is $c^2 = -1$. Of course, the last is our contradiction, since the square of a real number cannot equal $-1$.

Another result related to real composition algebras is that their dimension must be one or even.

**Theorem 1.** *Every real composition algebra $A$ of odd dimension necessarily has dimension 1.*

*Proof.* Let $a$ be an arbitrary element in $A$. Since the multiplication in $A$ is a bilinear operation, the function $x \mapsto ax$ is linear. Since a linear operator on a vector space with odd dimension has a characteristic equation with odd degree, we know there is a real soultion for the characteristic equation for $a$. Thus, there is a real eigenvalue $\lambda$ and nonzero eigenvector $v$ such that $av = \lambda v$. Since the norm $[\ ]$ on $A$ is nondegenerate and $v$ is nonzero, we can show $a = \lambda 1$:

$$0 = [av - \lambda v] = [(a - \lambda 1)\, v] = [a - \lambda 1][v]$$

Thus, we see that every element of the algebra is a *scalar* multiple of the multiplicative identity, namely 1. □

In fact, from Lemma 3.1 in the proof of Hurwitz's theorem that we give below, it follows that the dimension of a real composition algebra must be a power of two.

## 3.3 Hurwitz's Theorem

We now give a proof of Hurwitz's theorem. We state the theorem, prove some lemmas, then the main theorem. The plan is to show first that every composition algebra is the double of a smaller composition algebra. Then, we show that a composition algebra can only be doubled three times. This proof follows the proof in [CS03] very closely.

**Hurwitz's Theorem.** *The only real composition algebras are the real numbers, the complex numbers, the quaternions, and the octonions.*

We begin the proof by supposing $Z$ is a real composition algebra. Refer to Section 2.4 for comments related to the Dickson double.

**Lemma 3.1.** *Whenever $Z$ contains a proper subalgebra $Y$ with identity, it also contains the Dickson double of $Y$.*

*Proof.* Since $Y$ is a proper subalgebra, there is an orthogonal unit vector in $Z \setminus Y$, which we will call $i_Z$. Suppose $a_1, a_2, b_1, b_2$ are in $Y$. We expand the product to obtain

$$(a_1 + a_2 i_Z)(b_1 + b_2 i_Z) = a_1 b_1 + a_1.b_2 i_Z + a_2 i_Z.b_1 + a_2 i_Z.b_2 i_Z.$$

To show that the Dickson double $Y + Y i_Z$ is closed under multiplication and hence is a subalgebra of $Z$, we will simplify $a_1.b_2 i_Z$, $a_2 i_Z.b_1$, and $a_2 i_Z.b_2 i_Z$ in order to establish the so-called **composition doubling** law:

$$(a_1 + a_2 i_Z)(b_1 + b_2 i_Z) = (a_1 b_1 - \bar{b}_2 a_2) + (b_2 a_1 + a_2 \bar{b}_1) i_Z.$$

Let $t$ be an arbitrary element of $Z$. Then,

$$\begin{aligned}
[a_1.b_2 i_Z, t] &= [b_2 i_Z, \bar{a}_1 t] && \text{(by braid law)} \\
&= \left[i_Z \bar{b}_2, \bar{a}_1 t\right] && \text{(by conjugation doubling)} \\
&= 0 - \left[i_Z t, \bar{a}_1 \bar{b}_2\right] && \text{(by exchange law)} \\
&= \left[t, i_Z.\bar{a}_1 \bar{b}_2\right] && \text{(by braid law)} \\
&= [t, b_2 a_1.i_Z] && \text{(by scaling law)} \\
&= [b_2 a_1.i_Z, t]\,. && \text{(by braid law)}
\end{aligned}$$

$$\begin{aligned}
[a_2 i_Z.b_1, t] &= \left[a_2 i_Z, t \bar{b}_1\right] && \text{(by braid law)} \\
&= 0 - \left[a_2 \bar{b}_1, t i_Z\right] && \text{(by exchange law)} \\
&= \left[a_2 \bar{b}_1.i_Z, t\right]. && \text{(by braid law)}
\end{aligned}$$

$$
\begin{aligned}
[a_2 i_Z . b_2 i_Z, t] &= [b_2 i_Z, a_2 i_Z . t] && \text{(by braid law)} \\
&= 0 - [b_2 t, a_2 i_Z . i_Z] && \text{(by exchange law)} \\
&= [b_2 t . i_Z, a_2 i_Z] && \text{(by braid law)} \\
&= [b_2 t, a_2]\,[i_Z] && \text{(by scaling law)} \\
&= \left[t, \bar{b}_2 a_2\right] && \text{(by braid law)} \\
&= \left[\bar{b}_2 a_2, t\right]. && \text{(by Def. 2.4)}
\end{aligned}
$$

Since $t$ was arbitrary, the above computations are sufficient to establish the composition doubling law. It follows that $Y + Y i_Z$ is indeed a composition subalgebra of $Z$.

□

It follows that $Z$, being an algebra on a finite-dimensional vector space, must be equal to the (Dickson) double $Y + Y i_Z$ of some proper subalgebra $Y$ (unless $Z = \mathbb{R}$ itself).

**Lemma 3.2.** *If the algebra $Z$ is the double of a subalgebra $Y$, then the algebra $Z$ is a composition algebra only when $Y$ is an* associative *composition algebra.*

*Proof.* [CS03] Suppose $Z$ is a composition algebra. An algebra is a composition algebra when the composition law holds. Applied to an element of the double of $Y$, the law gives

$$
[a_1 + a_2 i_Z]\,[b_1 + b_2 i_Z] = \left[\left(a_1 b_1 - \bar{b}_2 a_2\right) + \left(b_2 a_1 + a_2 \bar{b}_1\right) i_Z\right].
$$

This allows us to expand:

$$
[a_1 + a_2 i_Z]\,[b_1 + b_2 i_Z] = [a_1]\,[b_1] + [a_1]\,[b_2] + [a_2]\,[b_1] + [a_2]\,[b_2]
$$

and

$$\left[\left(a_1b_1 - \bar{b}_2a_2\right) + \left(b_2a_1 + a_2\bar{b}_1\right) i_Z\right] = \left[a_1b_1 - \bar{b}_2a_2\right] + \left[b_2a_1 + a_2\bar{b}_1\right]$$
$$= [a_1b_1] + \left[\bar{b}_2a_2\right] + 2\left[a_1b_1, \bar{b}_2a_2\right] + [b_2a_1] + \left[a_2\bar{b}_1\right] - 2\left[b_2a_1, a_2\bar{b}_1\right].$$

The condition reduces to $\left[a_1b_1, \bar{b}_2a_2\right] = \left[b_2a_1, a_2\bar{b}_1\right]$, or equivalently $[b_2.a_1b_1, a_2] = [b_2a_1.b_1, a_2]$. Since this is true for all $a_1$, $a_2$, $b_1$, and $b_2$, the condition is equivalent to the associative law of multiplication for $Y$. □

**Lemma 3.3.** *Suppose $Y$ is the double of a subalgebra $X$. Then $Y$ is an* associative *composition algebra if and only if $X$ is an* associative and commutative *composition algebra.*

*Proof.* [CS03] Suppose $Y$ is associative. Since $X$ is a subalgebra of $Y$, then $X$ is associative. Since $(bc)i_Y = b(ci_Y) = (cb)i_Y$ for all $b, c$ in $X$, then$X$ must be commutative as well.

Conversely, suppose $X$ is associative and commutative. Now expand two multiplications in $Y$, as follows, and compare:

$$(a_1 + a_2i_X)(b_1 + b_2i_X).(c_1 + c_2i_X) = \left(\left(a_1b_1 - \bar{b}_2a_2\right) + \left(b_2a_1 + a_2\bar{b}_1\right) i_X\right)(c_1 + c_2i_X)$$
$$= \left(\left(a_1b_1 - \bar{b}_2a_2\right) c_1 - \bar{c}_2\left(b_2a_1 + a_2\bar{b}_1\right)\right) + \left(c_2\left(a_1b_1 - \bar{b}_2a_2\right) + \left(b_2a_1 + a_2\bar{b}_1\right)\bar{c}_1\right) i_X$$
$$= \left(a_1b_1.c_1 - \bar{b}_2a_2.c_1 - \bar{c}_2.b_2a_1 - \bar{c}_2.a_2\bar{b}_1\right) + \left(c_2.a_1b_1 - c_2.\bar{b}_2a_2 + b_2a_1.\bar{c}_1 + a_2\bar{b}_1.\bar{c}_1\right) i_X$$

and

$$(a_1 + a_2i_X).(b_1 + b_2i_X)(c_1 + c_2i_X) = (a_1 + a_2i_X)\left((b_1c_1 - \bar{c}_2b_2) + (c_2b_1 + b_2\bar{c}_1) i_X\right)$$
$$= \left(a_1\left(b_1c_1 - \bar{c}_2b_2\right) - \left(\bar{b}_1\bar{c}_2 + c_1\bar{b}_2\right)a_2\right) + \left(\left(c_2b_1 + b_2\bar{c}_1\right)a_1 + a_2\left(\bar{c}_1\bar{b}_1 - \bar{b}_2c_2\right)\right) i_X$$
$$= \left(a_1.b_1c_1 - a_1.\bar{c}_2b_2 - c_1\bar{b}_2a_2 - \bar{b}_1\bar{c}_2.a_2\right) + \left(c_2b_1.a_1 + b_2\bar{c}_1.a_1 + a_2.\bar{c}_1\bar{b}_1 - a_2.\bar{b}_2c_2\right) i_X.$$

The associativity and commutativity of $X$ show that these two products are equal. Thus $Y$ is associative. □

**Lemma 3.4.** *Suppose that $X$ is the double of a subalgebra $W$. Then $X$ is an* associative and commutative *composition algebra if and only if $W$ is an* associative and commutative *composition algebra* with trivial conjugation.

*Proof.* [CS03] Suppose $X$ is associative and commutative. We have $ti_X = i_X\bar{t}$ in $X$ for all $t$ in $W$. Since $X$ is commutative, we get $ti_X = \bar{t}i_X$, so conjugation must be trivial in $W$.

Conversely, suppose $W$ is associaitve, commutative, and has a trivial conjugation. By the lemma above, $X$ is associative. We have

$$(a_1 + a_2 i_W)(b_1 + b_2 i_W) = \left(a_1 b_1 - \bar{b}_2 a_2\right) + \left(a_1 b_2 + a_2 \bar{b}_1\right) i_W$$

and

$$(b_1 + b_2 i_W)(a_1 + a_2 i_W) = (b_1 a_1 - \bar{a}_2 b_2) + (a_2 b_1 + b_2 \bar{a}_1)\, i_W.$$

Using the properties of $W$, we see that $X$ is commutative. □

**Proof of Hurwitz's Theorem**

*Proof.* The real composition algebra $Z$ contains $\mathbb{R}$ as a subalgebra. If $\mathbb{R}$ is proper in $Z$, then $Z$ also contains its double. If this double itself is proper, then $Z$ contains the double of this double, and so on. Therefore, since $Z$ is finite-dimensional as a vector space, $Z$ must be obtained from $\mathbb{R}$ by a finite number of doublings. In particular, the dimension of $Z$ is a power of 2. However, starting from $\mathbb{R}$ we have only the following possibilities:

- $Z$ is $\mathbb{R}$ itself and is an associative, commutative real composition algebra with trivial conjugation,
- $Z$ is $\mathbb{C}$, the double of $\mathbb{R}$, and is an associative, commutative real composition algebra without trivial conjugation;

- $Z$ is $\mathbb{H}$, the double of $\mathbb{C}$, and is an associative, non-commutative real composition algebra;
- $Z$ is $\mathbb{O}$, the double of $\mathbb{H}$ and is a non-associative real composition algebra.

Since $\mathbb{O}$ is not associative, the double of $\mathbb{O}$ is not a composition algebra and hence the maximum number of doublings is three, showing that these are the only possibilities for $Z$. $\square$

# Bibliography

[CS03] John Horton Conway and Derek Alan Smith, *On quaternions and octonions: their geometry, arithmetic, and symmetry*, AK Peters, Natick, MA, 2003.

[Ebb91] John H. Ewing Ebbinghaus, Heinz-Dieter, *Numbers*, Graduate texts in mathematics, no. 123, Springer-Verlag, NewYork, 1991.

[Haz01] Michiel Hazewinkel, *Encyclopaedia of mathematics*, http://reference.kluweronline.com/?xmlid=1402006098, 2001.

[MB99] Saunders MacLane and Garrett Birkhoff, *Algebra*, third ed., AMS Chelsea Pub, Providence, RI, 1999.

[Sti02] John Stillwell, *Mathematics and its history*, second ed., Undergraduate texts in mathematics, Springer, New York, 2002.