An introduction to algebras and space time block coding

Angus Pointer

May 24, 2021

MATH4001

Mathematics Dissertation

Supervisor: Susanne Pumplün

School of Mathematical Sciences

University of Nottingham

I have read and understood the School and University guidelines on plagiarism. I confirm that this work is my own, apart from the acknowledged references.

Abstract

In this paper we introduce algebras over fields F of $\mathrm{char}(F) \neq 2$. We explore composition algebras via the classifications given in Hurwitz' theorem and the Cayley-Dickson doubling. We then consider central simple algebras and their relationship with matrix algebras over division algebras, given by Wedderburn's theorem. In the final chapter we introduce space time block coding, an application of algebras to digital data transmission.

Contents

Chapter 1

Introduction

An algebra A over a field F is a mathematical structure determined by assigning an F-bilinear product to an F-vector space. In this paper, we will only consider fields of $\mathrm{char}(F) \neq 2$. We begin by defining the general notion of an algebra and describe classifications given by properties of their corresponding product. We end our first chapter with an introduction to field extensions and some relevant results.

With key ideas in place, we move on to describe the class of composition algebras. We do so by equipping our algebra with a multiplicative quadratic form n. The chapter consists of an exploration of said algebras (most notably quaternion algebras, octonion algebras, matrix algebras and Zorn's vector-matrices) followed by a full classification via Hurwitz' theorem. It ends with a description of the Cayley-Dickson doubling process, which generates a sequence of 2^m-dimensional F-algebras from some initial field F and natural numbers m.

We then move on to another class of algebras: central simple algebras. We give a short exploration of said algebras and related machinery, followed by a statement of Wedderburn's theorem. We conclude with a description of the ten-

sor product of algebras and apply this to prove that the dimension of a central simple algebra is square.

Our final chapter provides an explanation of space time block coding, a technique used in digital data transmission. We formally apply the ideas we have covered up to here to construct codes from division algebras. We give a worked example of said construction using a general quaternion algebra and its left regular representation.

To conclude our paper, we give a few short paragraphs describing related content that strayed from the narrative. For each topic, we give some recommendations for texts that nicely cover the structures involved.

Chapter 2

General algebras

2.1 Basic definition

Definition 2.1.1 (F-algebra)**.** Let F be a field. An algebra A over F is an F-vector space equipped with an F-bilinear product $* : A \times A \to A$, which means

$$(ax + by) * z = ax * z + by * z$$
$$x * (by + cz) = bx * y + cx * z$$

for all $x, y, z \in A$ and scalars $a, b, c \in F$. When the use of $*$ is clear from the context, we can denote it via juxtaposition, $x * y = xy$.

This is the most general definition for an algebra. In this this chapter, we will define some specific properties that we will require our algebras to satisfy, which will leave us with algebraic structures that are easier to work with.

Example 2.1.2. F^3 together with the cross product $\times$ is an F-algebra. Let $\mathbf{i}, \mathbf{j}, \mathbf{k}$ be basis vectors for F^3, then

$\times$	$\mathbf{i}$	$\mathbf{j}$	$\mathbf{k}$
$\mathbf{i}$	$\mathbf{0}$	$\mathbf{k}$	$-\mathbf{j}$
$\mathbf{j}$	$-\mathbf{k}$	$\mathbf{0}$	$\mathbf{i}$
$\mathbf{k}$	$\mathbf{j}$	$-\mathbf{i}$	$\mathbf{0}$

It is clear from the table that $\times$ is anti-commutative, which means $\forall \mathbf{a}, \mathbf{b} \in F^3$, $\mathbf{a} \times \mathbf{b} = -\mathbf{b} \times \mathbf{a}$. We can express $\times$ explicitly by writing $\mathbf{a} = a_1\mathbf{i} + a_2\mathbf{j} + a_3\mathbf{k}$ and $\mathbf{b} = b_1\mathbf{i} + b_2\mathbf{j} + b_3\mathbf{k}$ where $a_i, b_i \in F$. Then

$$
\begin{aligned}
\mathbf{a} \times \mathbf{b} &= (a_1\mathbf{i} + a_2\mathbf{j} + a_3\mathbf{k}) \times (b_1\mathbf{i} + b_2\mathbf{j} + b_3\mathbf{k}) \\
&= \quad a_1b_1(\mathbf{i} \times \mathbf{i}) + a_1b_2(\mathbf{i} \times \mathbf{j}) + a_1b_3(\mathbf{i} \times \mathbf{k}) \\
&\quad + a_2b_1(\mathbf{j} \times \mathbf{i}) + a_2b_2(\mathbf{j} \times \mathbf{j}) + a_2b_3(\mathbf{j} \times \mathbf{k}) \\
&\quad + a_3b_1(\mathbf{k} \times \mathbf{i}) + a_3b_2(\mathbf{k} \times \mathbf{j}) + a_3b_3(\mathbf{k} \times \mathbf{k}) \\
&= a_1b_2\mathbf{k} + a_1b_3(-\mathbf{j}) + a_2b_1(-\mathbf{k}) + a_2b_3\mathbf{i} + a_3b_1\mathbf{j} + a_3b_2(-\mathbf{i}) \\
&= (a_2b_3 - a_3b_2)\mathbf{i} + (a_3b_1 - a_1b_3)\mathbf{j} + (a_1b_2 - a_2b_1)\mathbf{k}
\end{aligned}
$$

where we used $\mathbf{a} \times \mathbf{a} = -\mathbf{a} \times \mathbf{a} = 0$, which follows from anti-commutativity.

Now we can show that $\times$ is F-bilinear. For $\mathbf{a}, \mathbf{b}, \mathbf{c} \in F^3$ and $\alpha, \beta, \gamma \in F$,

$$\begin{aligned}
(\alpha\mathbf{a} + \beta\mathbf{b}) \times \gamma\mathbf{c} &= (\alpha(a_1\mathbf{i} + a_2\mathbf{j} + a_3\mathbf{k}) + \beta(b_1\mathbf{i} + b_2\mathbf{j} + b_3\mathbf{k})) \times \gamma(c_1\mathbf{i} + c_2\mathbf{j} + c_3\mathbf{k}) \\
&= \alpha\gamma(a_1(c_1\mathbf{i} \times \mathbf{i} + c_2\mathbf{i} \times \mathbf{j} + c_3\mathbf{i} \times \mathbf{k}) \\
&\quad + a_2(c_1\mathbf{j} \times \mathbf{i} + c_2\mathbf{j} \times \mathbf{j} + c_3\mathbf{j} \times \mathbf{k}) \\
&\quad + a_3(c_1\mathbf{k} \times \mathbf{i} + c_2\mathbf{k} \times \mathbf{j} + c_3\mathbf{k} \times \mathbf{k})) \\
&\quad + \beta\gamma(b_1(c_1\mathbf{i} \times \mathbf{i} + c_2\mathbf{i} \times \mathbf{j} + c_3\mathbf{i} \times \mathbf{k}) \\
&\quad + b_2(c_1\mathbf{j} \times \mathbf{i} + c_2\mathbf{j} \times \mathbf{j} + c_3\mathbf{j} \times \mathbf{k}) \\
&\quad + b_3(c_1\mathbf{k} \times \mathbf{i} + c_2\mathbf{k} \times \mathbf{j} + c_3\mathbf{k} \times \mathbf{k})) \\
&= \alpha\gamma(a_1(c_2\mathbf{k} - c_3\mathbf{j}) + a_2(-c_1\mathbf{k} + c_3\mathbf{i}) + a_3(c_1\mathbf{j} - c_2\mathbf{i})) \\
&\quad + \beta\gamma(b_1(c_2\mathbf{k} - c_3\mathbf{j}) + b_2(-c_1\mathbf{k} + c_3\mathbf{i}) + b_3(c_1\mathbf{j} - c_2\mathbf{i})) \\
&= \alpha\gamma((a_2c_3 - a_3c_2)\mathbf{i} + (a_3c_1 - a_1c_3)\mathbf{j} + (a_1c_2 - a_2c_1)\mathbf{k}) \\
&\quad + \beta\gamma((b_2c_3 - b_3c_2)\mathbf{i} + (b_3c_1 - b_1c_3)\mathbf{j} + (b_1c_2 - b_2c_1)\mathbf{k}) \\
&= \alpha\gamma(\mathbf{a} \times \mathbf{c}) + \beta\gamma(\mathbf{b} \times \mathbf{c})
\end{aligned}$$

Here we have shown linearity in the first argument. The process for the second argument, showing $\alpha\mathbf{a} \times (\beta\mathbf{b} + \gamma\mathbf{c}) = \alpha\beta(\mathbf{a} \times \mathbf{b}) + \alpha\gamma(\mathbf{a} + \mathbf{c})$, is much of the same. A useful simplifying property of this algebra is that its elements satisfy the Jacobi identity

$$\mathbf{a} \times (\mathbf{b} \times \mathbf{c}) + \mathbf{b} \times (\mathbf{c} \times \mathbf{a}) + \mathbf{c} \times (\mathbf{a} \times \mathbf{b}) = 0 \qquad \forall \mathbf{a}, \mathbf{b}, \mathbf{c} \in F^3.$$

Euclidean space $\mathbb{R}^3$ is a familiar case from linear algebra, with $F = \mathbb{R}$.

Definition 2.1.3 (Unital algebra)**.** An algebra is unital if it has a multiplicative identity, or "unit", $1_A \in A$ such that $1_A * x = x * 1_A, \forall x \in A$.

We can show that this element is unique: let 1_a and 1_b be units in A, then

$$1_a * 1_b = 1_b = 1_b * 1_a = 1_a.$$

Remark. Euclidean space in (2.1.2) is a non-unital algebra.

Definition 2.1.4 (Dimension)**.** The dimension of an F-algebra A, $dim_F(A)$, is the dimension of A as an F-vector space. If $dim_F(A)$ is finite, A is called finite-dimensional.

In this paper we will only discuss finite-dimensional algebras.

Definition 2.1.5 (Division algebra)**.** A finite dimensional, unital F-algebra is a division algebra if it has no (non-trivial) zero divisors. That means

$$xy = 0 \Rightarrow x = 0 \text{ or } y = 0, \forall x, y \in A.$$

We will cover division algebras in more detail with some specific examples in the next chapter.

Definition 2.1.6 (Associator)**.** For $x, y, z \in A$, the associator is

$$[x, y, z] = (xy)z - x(yz).$$

Definition 2.1.7 (Nucleus)**.** The nucleus of A is

$$\mathcal{N}(A) = \{x \in A \mid [x, A, A] = [A, x, A] = [A, A, x] = 0\}.$$

Definition 2.1.8 (Associative algebra)**.** An F-algebra A is called associative if $[x, y, z] = 0 \ \ \forall x, y, z \in A$.

Remark. Note that A is an associative algebra if it is exactly equal to its nucleus, $A = \mathcal{N}(A)$. For any F-algebra A, the nucleus $\mathcal{N}(A)$ is an associative F-subalgebra (see [5] page 7).

Definition 2.1.9 (Inverse)**.** For a unital associative algebra A, the inverse of a non-zero element $x \in A$ is an element $x^{-1} \in A$ such that $x * x^{-1} = x^{-1} * x = 1_A$.

Lemma 2.1.10. For a unital associative algebra A, each inverse is unique.

Proof. Let x_a^{-1} and x_b^{-1} be inverses for $x \in A^\times$, such that $x_a^{-1} * x = x * x_a^{-1} = 1_A$ and $x_b^{-1} * x = x * x_b^{-1} = 1_A$. Then $x_a^{-1} * x = 1_A \Rightarrow x_a^{-1} * x * x_b^{-1} = x_b^{-1} \Rightarrow x_a^{-1} = x_b^{-1}$. □

Remark. The set of invertible elements in an associative algebra A is denoted $A^\times$. For an associative division algebra, this is the set of non-zero elements.

Definition 2.1.11 (Involution)**.** An involution on an algebra A is a map $\sigma : A \to A$ such that

$$\sigma(x + y) = \sigma(x) + \sigma(y),$$
$$\sigma(xy) = \sigma(y)\sigma(x),$$
$$\sigma^2 = id,$$

for all $x, y \in A$, where $id : A \to A : x \mapsto x, \forall x \in A$ is the identity map.

Definition 2.1.12 (Commutator)**.** For elements $x, y \in A$ of an F-algebra A, the commutator is

$$[x, y] = xy - yx.$$

Definition 2.1.13 (Centre)**.** The centre of an F-algebra A is

$$\mathcal{Z}(A) = \{x \in A \mid [x, y] = 0 \text{ and } x \in \mathcal{N}(A), \ \forall y \in A\}.$$

Definition 2.1.14 (Commutative algebra)**.** An F-algebra A is called commutative if $[x, y] = 0 \ \ \forall x, y \in A$.

Remark. For any F-algebra A, the centre $\mathcal{Z}(A)$ is a commutative F-subalgebra (see [5] page 5). If A is associative, then it is also commutative iff it is exactly equal to its center, $A = \mathcal{Z}(A)$.

Definition 2.1.15 (Homomorphism)**.** For F-algebras A and B, an (algebra) homomorphism $\mu : A \to B$ is a map that satisfies, $\forall x, y \in A, \alpha \in F$,

$$\mu(x + y) = \mu(x) + \mu(y),$$
$$\mu(\alpha x) = \alpha\mu(x),$$
$$\mu(xy) = \mu(x)\mu(y).$$

Remark. The first two requirements mean μ is an F-linear map. The last implies it is a ring-homomorphism.

A bijective homomorphism is an isomorphism. A homomorphism $\mu : A \to A$ is an endomorphism. We denote the ring of endomorphisms on A by $\mathrm{End}_F(A)$. An endomorphism that is also an isomorphism is called an automorphism. We denote the group of automorphisms on A by $\mathrm{Aut}(A)$. If an isomorphism $\mu : A \to B$ exists, we say A and B are isomorphic, written $A \cong B$.

Example 2.1.16. For fixed non-square $a \in F^\times$, a quadratic field extension $A = F(\sqrt{a})$ is a 2-dimensional F-vector space with basis $\{1, \sqrt{a}\}$. A is a 2-dimensional F-algebra with the product defined by this table:

$\cdot$	1	$\sqrt{a}$
1	1	$\sqrt{a}$
$\sqrt{a}$	$\sqrt{a}$	a

Since $\cdot$ is commutative, every automorphism on A is an involution. There

are only two F-linear automorphisms on A. These are id and the canonical involution, $^* : \sqrt{a} \mapsto -\sqrt{a}$.

Example 2.1.17. The complex numbers $\mathbb{C}$ are a 2-dimensional $\mathbb{R}$-algebra, defined as

$$\mathbb{C} = \{z = x + iy \mid x, y \in \mathbb{R}, \ \ i^2 = -1\}.$$

The basis elements $\{1, i\}$ multiply as

$\cdot$	1	i
1	1	i
i	i	-1

Comparing this with (2.1.16), it is clear that the complex numbers are a real field extension, $\mathbb{C} \cong \mathbb{R}(\sqrt{-1})$. Taking the canonical involution in $\mathbb{C}$, * described in (2.1.16) is the same as taking the complex conjugate,

$$z = x + iy \quad \Rightarrow \quad z^* = x - iy.$$

Since it is a field extension, $\mathbb{C}$ is associative, commutative and unital. The complex numbers are also a division algebra, as $z_1 z_2 = 0$ iff $z_1 = 0$ or $z_2 = 0$.

2.2 Base field extensions

Definition 2.2.1 (Field extension)**.** Let K be a field and $F \subseteq K$ a subfield. We say K is an extension field of F and denote the pairing (K, F) as K/F.

Definition 2.2.2 (Degree of extension)**.** The extension field K is an F-vector space. Then the degree of the extension is $[K : F] = \dim_F(K)$. The field extension K/F is finite if $[K : F]$ is finite.

Theorem 2.2.3. Let $F \subseteq K \subseteq L$ be fields, with $[L : K], [K : F]$ finite. Then

$$[L : F] = [L : K][K : F]$$

Proof. See [1], Theorem 4.7. □

Definition 2.2.4 (Generating set)**.** Let $S \subseteq K$ be a subset and let K/F be a field extension. Let $E_i \subseteq K$ be a subfield with $F \subseteq E_i$, $S \subseteq E_i$, then

$$F(S) = \bigcap_i E_i$$

is the smallest subfield of K containing F and S, or the field "generated" by S over F. Then, we call S a generating set of $F(S)$ over F.

Definition 2.2.5 (Simple extension)**.** Let a generating set of $F(S)$ over F consist of a single element, $S = \{s\}$. Then we call $F(s)/F$ a simple extension, and s a primitive element of the extension.

Example 2.2.6. $\mathbb{C}/\mathbb{R} = \mathbb{R}(i)/\mathbb{R}$ is a simple extension, with primitive element $i = \sqrt{-1}$. $\mathbb{C}$ has $\mathbb{R}$-basis $\{1, i\}$, so $[\mathbb{C} : \mathbb{R}] = 2$.

Definition 2.2.7 (Polynomial ring)**.** $F[x]$ is the ring of polynomials taking coefficients in F.

Definition 2.2.8 (Algebraic extension)**.** Let K/F be a field extension. Then K/F is algebraic if every element of K is a root of some non-zero polynomial with coefficients in F.

Definition 2.2.9 (Algebraically closed field)**.** A field F is algebraically closed if every non-constant polynomial in $F[x]$ has a root in F.

Theorem 2.2.10. For every field F, there exists an algebraic extension that is algebraically closed and unique up to isomorphism. We call this the algebraic closure of F, denoted $\bar{F}$.

Proof. The essence of this proof lies in Zorn's lemma [2]. Consider the set of algebraic extensions K of F. The union of a chain of algebraic extensions of F is, itself, an algebraic extension of F. By Zorn's lemma, there exists some maximal element $K = \bar{F}$. Then $\bar{F}$ must be algebraically closed, else there would exist some irreducible polynomial in $\bar{F}[x]$ with a root in a larger field (which can't exist as $\bar{F}$ is maximal). For a detailed proof, see [3]. □

Corollary 2.2.11. Let $\bar{F}$ be the algebraic closure of a field F. The only finite-dimensional associative division $\bar{F}$-algebra is $\bar{F}$ itself.

Proof. All finite field extensions are algebraic. We will later consider Wedderburn's little theorem (4.1.3), which says that every division algebra is a field. Then, a division $\bar{F}$-algebra is a field, and we have a finite field extension $D/\bar{F}$. However, $\bar{F}$ is maximal, so we have $D \cong \bar{F}$. For details, see [4] pg2. □

Chapter 3

Composition algebras

In this chapter we will introduce a class of not necessarily associative algebras which are distinguished from the others by the existence of a certain well behaved quadratic form. An algebra that exhibits such a form is called a composition algebra, all of which have been classified by Hurwitz. We will also introduce some of the tools required to understand and construct these algebras, most notably the Cayley-Dickson construction.

3.1 The norm

Definition 3.1.1 (Quadratic form)**.** For a finite-dimensional F-vector space A, a quadratic form is a map $n : A \to F$ satisfying:

$$\begin{aligned} &n(ax) = a^2 n(x), \quad \forall a \in F, x \in A \\ &b(x,y) \stackrel{\text{def}}{=} n(x+y) - n(x) - n(y) \quad \text{is } F\text{-bilinear,} \end{aligned}$$

where $b : A \times A \to F : (x, y) \mapsto n(x+y) - n(x) - n(y)$ is known as the associated bilinear form.

Definition 3.1.2 (Non-degenerate form)**.** For a finite-dimensional F-vector space A, a quadratic form $n : A \to F$ is non-degenerate iff

$$b(x, y) = 0, \forall y \in A \Rightarrow x = 0.$$

Definition 3.1.3 (Quadratic algebra)**.** For a unital F-algebra A, let $n : A \to F$ be a quadratic form. We say A is a quadratic algebra if, for all $x \in A$,

$$x^2 - b(1_A, x)x + n(x)1_A = 0.$$

Definition 3.1.4 (Alternative algebra)**.** A not necessarily associative F-algebra A is an alternative algebra if for all $x, y \in A$,

$$[x, x, y] = 0, \quad \text{i.e. } (xx)y = x(xy),$$
$$[x, y, x] = 0, \quad \text{i.e. } (xy)x = x(yx),$$
$$[x, y, y] = 0, \quad \text{i.e. } (xy)y = x(yy).$$

Lemma 3.1.5. Any two of the above conditions implies the third.

Proof. See [5] (Lemma 1.9). □

Definition 3.1.6 (Composition algebra)**.** A finite dimensional, unital F-algebra A is a composition algebra if there exists a multiplicative, non-degenerate quadratic form $n : A \to F$ such that

$$n(xy) = n(x)n(y) \quad \forall x, y \in A.$$

It can be shown that this form is uniquely determined up to isomorphism. We refer to this n as the norm of A.

Theorem 3.1.7. A quadratic alternative F-algebra A is a composition algebra iff its norm is non-degenerate. [7] (4.6).

Definition 3.1.8 (Canonical involution)**.** For a composition algebra A with quadratic form n, the canonical involution is defined as $x^* = b(1_A, x)1_A - x$.

Theorem 3.1.9. For a composition algebra A with norm form n and canonical involution *, we have $n(x) = xx^* = x^*x$.

Proof. Left multiply (3.1.8) by x to give $xx^* = xb(1_A, x) - x^2$. From (3.1.3), $n(x) = b(1_A, x)x - x^2$. Since $b(1_A, x) \in F$, it commutes with x, so $xx^* = b(1_A, x)x - x^2 = n(x)$. Right multiply (3.1.8) to obtain $x^*x = n(x)$. □

Corollary 3.1.10. When A is a composition algebra, the inverse of each element $x \in A$ with $n(x) \neq 0$ is given by $x^{-1} = \frac{x^*}{n(x)}$, and is unique.

Proof. $xx^{-1} = \frac{xx^*}{n(x)} = \frac{n(x)}{n(x)} = 1$. We can do the same for $x^{-1}x$ since $n(x) = x^*x = xx^*$. For any algebra over a field, multiplication is distributive. Then consider some other inverse y such that $yx = xy = 1$. We have $xx^{-1} - xy = 1 - 1 = 0 \Rightarrow x(x^{-1} - y) = 0 \Rightarrow x^{-1} = y$. □

An obvious question then arises; what about elements x where $n(x) = 0$?

Definition 3.1.11 (Isotropic form)**.** For a quadratic form n on an F-vector space A, a non-zero element $x \in A$ is isotropic if $n(x) = 0$. If such an element exists (i.e. $y \in A^\times$ such that $n(y) = 0$) then the form n is isotropic. Otherwise, it is anisotropic.

Definition 3.1.12 (Split algebra)**.** If the norm n of a composition algebra A is isotropic, we say that A is a split algebra.

Theorem 3.1.13. If the norm n of a composition algebra A is anisotropic, A is a division algebra.

Proof. n is anisotropic iff $n(a) = 0 \iff a = 0$. Let[1] $a = xy$, then $n(xy) = 0 \iff xy = 0$. The norm form is multiplicative, i.e. $n(xy) = n(x)n(y)$, so

[1]For any $a \in A$ we can always write $a = xy$ where $x, y \in A$ because A is unital, so $a = 1_A a = a1_A$.

$n(xy) = 0 \iff n(x)n(y) = 0$. F is a field and $n : A \to F$ so $n(x)n(y) = 0 \iff n(x) = 0$ or $n(y) = 0$. But, n is anisotropic so this must mean $x = 0$ or $y = 0$. So, $n(xy) = 0 \iff xy = 0 \iff x = 0$ or $y = 0$. □

Corollary 3.1.14. Every composition algebra A is either a split algebra or a division algebra.

Example 3.1.15. The complex numbers $\mathbb{C}$ described in (2.1.17) are a composition algebra. We stated that they are a division algebra, which we can now verify. The canonical involution as $^* : x + iy \mapsto x - iy$ for $x, y \in \mathbb{R}$. Then the norm is

$$\begin{aligned} n(z) &= zz^* \\ &= (x + iy)(x - iy) \\ &= x^2 - ixy + iyx - i^2y^2 \\ &= x^2 + y^2. \end{aligned}$$

This never vanishes for $(x, y) \neq (0, 0)$, so $n(z)$ is anisotropic and $\mathbb{C}$ is a division algebra.

Example 3.1.16. We can define another 2-dimensional composition algebra by taking the $\mathbb{R}$-basis $\{1, i\}$ with $i^2 = 1$, and the product given by:

$\cdot$	1	i
1	1	i
i	i	1

We can write the norm explicitly as follows:

$$\begin{aligned} n(z) &= zz^* \\ &= (x+iy)(x-iy) \\ &= x^2 - ixy + iyx - i^2y^2 \\ &= x^2 - y^2. \end{aligned}$$

$n(z) = 0$ when $x = \pm y$, so the norm is isotropic and we have a split algebra. To learn a little more about this algebra, it is helpful to consider a change of basis. Let $e = (1+i)/2$, $e^* = (1-i)/2$. These form a basis $\{e, e^*\}$, since we can write

$$z = x + iy = (x-y)e + (x+y)e^*.$$

The elements e and e^* are mutually orthogonal

$$ee^* = (1/4)(1+i)(1-i) = (1/4)(1+i-i-i^2) = 0,$$

and idempotent

$$\begin{aligned} ee &= (1/4)(1+i)(1+i) = (1/4)(1+i+i+i^2) = (1/2)(1+i) = e \\ e^*e^* &= (1/4)(1-i)(1-i) = (1/4)(1-i-i+i^2) = (1/2)(1-i) = e^*. \end{aligned}$$

Letting $a = x - y$ and $b = x + y$ with $a, b \in \mathbb{R}$, we can define some more appropriate notation,

$$z = ae + be^* \stackrel{\text{def}}{=} (a, b).$$

With this notation, the canonical involution swaps a and b:

$$\begin{aligned}(a,b)^* &= (ae + be^*)^* \\ &= ae^* + be \\ &= (b,a),\end{aligned}$$

and multiplication is given for $z_1 = (a_1, b_1)$ and $z_2 = (a_2, b_2)$ by

$$\begin{aligned}(a_1,b_1)(a_2,b_2) &= (a_1e + b_1e^*)(a_2e + b_2e^*) \\ &= a_1a_2e^2 + a_1b_2ee^* + b_1a_2e^*e + b_1b_2(e^*)^2 \\ &= a_1a_2e + b_1b_2e^* \\ &= (a_1a_2, b_1b_2).\end{aligned}$$

Having written multiplication explicitly for arbitrary elements, it is clear that this algebra obeys pairwise addition and multiplication - it is ring isomorphic to $\mathbb{R} \oplus \mathbb{R}$.

3.2 Hurwitz' theorem

In (3.1.15) and (3.1.16), we described two distinct 2-dimensional composition algebras. Hurwitz [8] fully classified all composition algebras over fields of $\mathrm{char} \neq 2$.

Theorem 3.2.1. Let A be a composition algebra. Then $\dim(A) \in \{1, 2, 4, 8\}$.

We will explore what these algebras are before giving the full theorem.

Definition 3.2.2 (Binion algebra)**.** Let $A = (a)_F$ be a 2-dimensional F-vector space with fixed $a \in F^\times$ and F-basis $\{1_F, i\}$ such that $i^2 = a$. Then A is an

associative, commutative F-algebra called a binion algebra.

Both of the algebras in the previous two examples are binion $\mathbb{R}$-algebras.

Theorem 3.2.3. If $a \in F^\times$ is a square, $(a)_F$ is a split algebra. Otherwise, $(a)_F$ is a division algebra and $(a)_F \cong F(\sqrt{a})$.

Proof. The norm for a general element $z = (x + iy) \in (a)_F$ is given by

$$\begin{aligned} n(z) &= zz^* \\ &= (x+iy)(x-iy) = x^2 - xiy + xiy - i^2y^2 \\ &= x^2 - ay^2. \end{aligned}$$

$(a)_F$ is a split algebra when $n(z) = x^2 - ay^2 = 0$ has nonzero solutions $(x, y) \in F \times F$. There are two distinct cases:

$a = \alpha^2$ for some $\alpha \in F$, then $x = \pm\alpha y$ is a set of solutions, and $(a)_F$ is a split algebra.

$a \neq \alpha^2$ for all $\alpha \in F$, then $x^2 = ay^2$ has only $(0, 0)$ as a solution, and $(a)_F$ is a division algebra. □

Corollary 3.2.4. If A is a 2-dimensional composition algebra over a field F, then A is either a quadratic field extension of F (a division algebra), or $A \cong F \oplus F$ (a split algebra).

Definition 3.2.5 (Quaternion algebra)**.** Let $A = (a, b)_F$ be a 4-dimensional F-vector space with fixed $a, b \in F^\times$ and F-basis $\{1_F, i, j, k\}$. Define a unital associative algebra on A with unit element 1_F via

$$i^2 = a, \quad j^2 = b, \quad ij = k = -ji.$$

Then A is a non-commutative F-algebra called a quaternion algebra.

To develop an intuition for quaternion algebras, we will first consider some examples for $F = \mathbb{R}$.

Example 3.2.6. [9] Hamilton's quaternions $\mathbb{H}$ are defined by the relations $i^2 = j^2 = k^2 = ijk = -1$. Using the notation in (3.2.5), $\mathbb{H} = (-1, -1)_{\mathbb{R}}$. We can write a general element as $p = q + ri + sj + tk$ with $q, r, s, t \in \mathbb{R}$, and the product is given by the following table:

$\cdot$	1	i	j	k
1	1	i	j	k
i	i	-1	k	$-j$
j	j	$-k$	-1	i
k	k	j	$-i$	-1

From the table it is clear that the elements i, j, k anti-commute, meaning $ij = -ji, ik = -ki, jk = -kj$. The canonical involution is given by $p^* = q - ri - sj - tk$, and the norm is

$$\begin{aligned} n(p) &= pp^* \\ &= (q + ri + sj + tk)(q - ri - sj - tk) \\ &= (q^2 - qri - qsj - qtk) + (qri - (ri)^2 - rsij - rtik) \\ &\quad + (qsj - rsji - (sj)^2 - stjk) + (qtk - rtki - stkj - (tk)^2) \\ &= (q^2 + r^2 + s^2 + t^2). \end{aligned}$$

This never vanishes for non-zero $a, b, c, d \in \mathbb{R}$, so n is anisotropic and $\mathbb{H}$ is a division algebra.

Example 3.2.7. Let us now consider $A = (1, 1)_{\mathbb{R}}$. The product is given by the following table:

$\cdot$	1	i	j	k
1	1	i	j	k
i	i	1	k	j
j	j	$-k$	1	$-i$
k	k	$-j$	i	-1

Again, the elements i, j, k anti-commute. The canonical involution is $p^* = q - ri - sj - tk$, and the norm is

$$\begin{aligned} n(p) &= pp^* \\ &= (q^2 - r^2 - s^2 + t^2). \end{aligned}$$

This vanishes for (q, r, s, t) satisfying $q^2 + t^2 = r^2 + s^2$. There are many such elements in $\mathbb{R}^4$, one example being $(1, 1, 0, 0)$ which corresponds to $p = 1 - ir$. So, n is isotropic and $(1, 1)_{\mathbb{R}}$ is a split algebra.

Lemma 3.2.8. For $a, b \in F^\times$, $(a, b)_F \cong (b, a)_F$.

Proof. Define a map $\phi : (a, b)_F \to (b, a)_F$ by $\phi(1) = 1, \phi(i) = j, \phi(j) = i, \phi(k) = k$. ϕ is an isomorphism since

$$\begin{aligned} \phi(i + j) &= j + i = \phi(i) + \phi(j), \\ \phi(ij) &= \phi(k) = k = ji = \phi(i)\phi(j). \end{aligned}$$

□

Corollary 3.2.9. For squares $c, d \in F^\times$ and $a, b \in F^\times$, $(ac, bd)_F \cong (a, b)_F$.

Example 3.2.10. In light of (3.2.8), it is instructive to consider the algebra $(1, -1)_{\mathbb{R}} \cong (-1, 1)_{\mathbb{R}}$. The product is given by the following table:

$\cdot$	1	i	j	k
1	1	i	j	k
i	i	1	k	j
j	j	$-k$	-1	i
k	k	$-j$	$-i$	1

We can compare this with the table in (3.2.7) and see that by swapping the rows and columns labelled j and k, these are the same table. So, taking the map $\phi(1) = 1, \phi(i) = i, \phi(j) = k, \phi(k) = j$, we have

$$\phi(j+k) = k + j = \phi(j) + \phi(k),$$
$$\phi(jk) = \phi(i) = i = kj = \phi(j)\phi(k).$$

Thus, ϕ is an isomorphism and $(1,-1)_{\mathbb{R}} \cong (-1,1)_{\mathbb{R}} \cong (1,1)_{\mathbb{R}}$.

Lemma 3.2.11. The set of n by n matrices taking entries in a field F, denoted $M_n(F)$, is an F-algebra with matrix multiplication as the product.

Proof. $M_n(F)$ is an n^2-dimensional F-vector space with basis elements:

$$\begin{pmatrix} 1 & 0 & \dots & 0 \\ 0 & 0 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 & \dots & 0 \\ 0 & 0 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & 0 \end{pmatrix}, \text{etc.}$$

F-bilinearity of matrix multiplication is a standard linear algebra result. □

Corollary 3.2.12. $M_2(F)$ is a composition algebra with $n(\mathbf{X}) = \det \mathbf{X}, \forall \mathbf{X} \in M_2(F)$.

Proof. It is a standard result from linear algebra that $\det \mathbf{XY} = \det \mathbf{X} \det \mathbf{Y}$ for

matrices $\mathbf{X}$ and $\mathbf{Y}$. For $\mathbf{X} \in M_2(F)$ and $a \in F$, we also have:

$$\det a\mathbf{X} = \begin{vmatrix} ax_{00} & ax_{01} \\ ax_{10} & ax_{11} \end{vmatrix} = a^2(x_{00}x_{11} - x_{10}x_{01}) = a^2 \det X$$

Now we will prove F-bilinearity of $b(\mathbf{X}, \mathbf{Y}) = \det(\mathbf{X} + \mathbf{Y}) - \det \mathbf{X} - \det \mathbf{Y}$. For $\mathbf{X} \in M_2(F)$, we can write

$$\begin{aligned} \det \mathbf{X} &= \begin{vmatrix} x_{00} & x_{01} \\ x_{10} & x_{11} \end{vmatrix} = x_{00}x_{11} - x_{10}x_{01} \\ &= \begin{pmatrix} x_{00} & x_{11} & x_{01} & x_{10} \end{pmatrix} \begin{pmatrix} 0 & \frac{1}{2} & 0 & 0 \\ \frac{1}{2} & 0 & 0 & 0 \\ 0 & 0 & 0 & -\frac{1}{2} \\ 0 & 0 & -\frac{1}{2} & 0 \end{pmatrix} \begin{pmatrix} x_{00} \\ x_{11} \\ x_{01} \\ x_{10} \end{pmatrix} \\ &\stackrel{\text{def}}{=} \mathbf{x}^\mathsf{T}\mathbf{D}\mathbf{x}. \end{aligned}$$

With this notation, and the fact that $(\mathbf{x} + \mathbf{y})^\mathsf{T} = (\mathbf{x}^\mathsf{T} + \mathbf{y}^\mathsf{T})$, we can write

$$\begin{aligned} b(\mathbf{X}, \mathbf{Y}) &= \det(\mathbf{X} + \mathbf{Y}) - \det \mathbf{X} - \det \mathbf{Y} \\ &= (\mathbf{x}^\mathsf{T} + \mathbf{y}^\mathsf{T})\mathbf{D}(\mathbf{x} + \mathbf{y}) - \mathbf{x}^\mathsf{T}\mathbf{D}\mathbf{x} - \mathbf{y}^\mathsf{T}\mathbf{D}\mathbf{y} \\ &= \mathbf{x}^\mathsf{T}\mathbf{D}\mathbf{x} + \mathbf{x}^\mathsf{T}\mathbf{D}\mathbf{y} + \mathbf{y}^\mathsf{T}\mathbf{D}\mathbf{x} + \mathbf{y}^\mathsf{T}\mathbf{D}\mathbf{y} - \mathbf{x}^\mathsf{T}\mathbf{D}\mathbf{x} - \mathbf{y}^\mathsf{T}\mathbf{D}\mathbf{y} \\ &= \mathbf{x}^\mathsf{T}\mathbf{D}\mathbf{y} + \mathbf{y}^\mathsf{T}\mathbf{D}\mathbf{x}. \\ &= 2\mathbf{x}^\mathsf{T}\mathbf{D}\mathbf{y} \end{aligned}$$

Then we have

$$\begin{aligned} b(\alpha\mathbf{A}+\beta\mathbf{B},\gamma\mathbf{C}) &= 2(\alpha\mathbf{a}^{\mathsf{T}}+\beta\mathbf{b}^{\mathsf{T}})\mathbf{D}(\gamma\mathbf{c}) \\ &= 2\alpha\gamma\mathbf{a}^{\mathsf{T}}\mathbf{D}\mathbf{c}+2\beta\gamma\mathbf{b}^{\mathsf{T}}\mathbf{D}\mathbf{c} \\ &= \alpha\gamma b(\mathbf{A},\mathbf{C})+\beta\gamma b(\mathbf{B},\mathbf{C}). \end{aligned}$$

Thus, the form b associated with $n(\mathbf{X}) = \det\mathbf{X}$ is F-linear in the first argument. It is also symmetric, meaning $b(\mathbf{X},\mathbf{Y}) = b(\mathbf{Y},\mathbf{X})$, so we have F-bilinearity and $\det\mathbf{X}$ is a multiplicative quadratic form. Non-degeneracy is obvious. □

Corollary 3.2.13. $M_2(F)$ is a split algebra.

Proof. Let $a \in F^\times$ and $\mathbf{X} = \begin{pmatrix} a & a \\ a & a \end{pmatrix}$. Then $n(\mathbf{X}) = a^2 - a^2 = 0$, so n is an isotropic form. By (3.1.12), this makes $M_2(F)$ a split algebra. Alternatively, the $\mathbf{X} \in M_2(F)$ given above is a non-trivial zero divisor, meaning $M_2(F)$ cannot be a division algebra. By (3.2.12), we know it is a composition algebra, so from (3.1.14) it must be a split algebra. □

Theorem 3.2.14. $(a,b)_F \cong M_2(F)$ if $a,b \in F^\times$ and at least one of a,b is a square.

Proof. Consider the following basis (given in [10] (3.1.3)) for $M_2(K)$, where $K = F(\sqrt{a})$ (Note: When a is a square in F, we have $F(\sqrt{a}) = F$) and $a,b \in F^\times$:

$$\mathbf{1} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad \mathbf{I} = \begin{pmatrix} \sqrt{a} & 0 \\ 0 & -\sqrt{a} \end{pmatrix}, \quad \mathbf{J} = \begin{pmatrix} 0 & b \\ 1 & 0 \end{pmatrix}, \quad \mathbf{K} = \begin{pmatrix} 0 & b\sqrt{a} \\ -\sqrt{a} & 0 \end{pmatrix}$$

We have the following relations:

$$\mathbf{I}^2 = \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} = a\mathbf{1}, \qquad \mathbf{J}^2 = \begin{pmatrix} b & 0 \\ 0 & b \end{pmatrix} = b\mathbf{1},$$
$$\mathbf{IJ} = \begin{pmatrix} \sqrt{a} & 0 \\ 0 & -\sqrt{a} \end{pmatrix} \begin{pmatrix} 0 & b \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & b\sqrt{a} \\ -\sqrt{a} & 0 \end{pmatrix} = \mathbf{K},$$
$$\mathbf{JI} = \begin{pmatrix} 0 & -b\sqrt{a} \\ \sqrt{a} & 0 \end{pmatrix} = -\mathbf{K}$$

These are exactly the relations for the quaternion algebra $(a, b)_F$, so we have an algebra homomorphism $\phi : M_2(K) \to (a, b)_F$ with

$$\phi(\mathbf{1}) = 1, \phi(\mathbf{I}) = i, \phi(\mathbf{J}) = j, \phi(\mathbf{K}) = k.$$

This is bijective if a is a square in F, in which case, we have an isomorphism $M_2(F) \cong (a, b)_F$. From (3.2.8), the same is true if b is a square in F. □

Theorem 3.2.15 (Frobenius [12])**.** Up to isomorphism, there are only two real quaternion algebras. These are $\mathbb{H} \cong (-1, -1)_{\mathbb{R}}$ and $M_2(\mathbb{R}) \cong (1, 1)_{\mathbb{R}}$.

Proof. In $\mathbb{R}$, the squares are exactly the positive numbers $\mathbb{R}^+$. With this and (3.2.14), we have $(a, b)_{\mathbb{R}} \cong M_2(\mathbb{R})$ when either of $a, b \in \mathbb{R}^+$. Every negative number in $\mathbb{R}$ can be written as $c(-1)$ with $c \in \mathbb{R}^+$. With this and (3.2.9), we know $(c(-1), d(-1))_{\mathbb{R}} \cong (-1, -1)_{\mathbb{R}} = \mathbb{H}$ for $c, d \in \mathbb{R}^+$. □

For 2-dimensional composition algebras, we were able to classify exactly when $(a)_F$ is a split algebra, and when it is a division algebra. We can do the same for 4-dimensional composition algebras.

Definition 3.2.16. For $a \in F^\times$, the norm subgroup is

$$N_a = \{b = x^2 - ay^2 \quad | \quad b \neq 0, \quad x, y \in F\}.$$

Lemma 3.2.17. N_a is a group.

Proof. We only need to prove closure:

$$\begin{aligned}(x_1^2 - ay_1^2)(x_2^2 - ay_2^2) &= (x_1^2x_2^2 - ay_1^2x_2^2 - ay_2^2x_1^2 + a^2y_1^2y_2^2) \\ &= (x_1^2x_2^2 + a^2y_1^2y_2^2 + 2ax_1x_2y_1y_2) - (2ax_1x_2y_1y_2 + a(x_1^2y_2^2 + x_2^2y_1^2)) \\ &= (x_1x_2 + ay_1y_2)^2 - a(x_1y_2 + x_2y_1)^2 \in N_a.\end{aligned}$$

□

Theorem 3.2.18. For $a, b \in F^\times$, $\quad (a, b)_F \cong M_2(F) \iff b \in N_a$.

Proof. $\Leftarrow$

Let $b = x^2 - ay^2$ where $a, b \in F^\times$, $x, y \in F$. That is, $b \in N_a$. Then $(a, b)_F$ is given by

$$i^2 = a, \quad j^2 = (x^2 - ay^2), \quad ij = k = -ji.$$

Now, consider the map $\phi : (a, b)_F \to (a, b^2)_F$:

$$\phi(1) = 1, \quad \phi(i) = i, \quad \phi(j) = xj + yk, \quad \phi(k) = i(xj + yk)$$

Then we have:

$$\begin{aligned}
\phi(i)^2 &= i^2 = a \\
\phi(j)^2 &= (xj + yk)^2 = (x^2j^2 + y^2k^2 + xyjk + xykj) \\
&= x^2j^2 - y^2(ij)(ji) + xyjk - xyjk \\
&= x^2(x^2 - ay^2) - ay^2(x^2 - ay^2) \\
&= (x^2 - ay^2)^2 = b^2 \\
\phi(i)\phi(j) &= i(xj + yk) = xij + yik = -(xj)i - (yk)i = -\phi(j)\phi(i)
\end{aligned}$$

So, this is an isomorphism and we have $(a, b)_F \cong (a, b^2)_F$, which gives $(a, b)_F \cong M_2(F)$ by (3.2.14).

$\Rightarrow$

First consider the case where $a = c^2$ for some $c \in F^\times$. Then we can write every $k \in N_a$ as:

$$\begin{aligned}
k &= x^2 - ay^2 = x^2 - c^2y^2 \\
&= (x + cy)(x - cy)
\end{aligned}$$

Then letting $x' = x - cy$ and $y' = x + cy$, we have $N_a = \{x'y' : x', y' \in F^\times\}$. We can set $y' = 1$ to give $N_a \cong F^\times$ as groups. Then $b \in F^\times \Rightarrow b \in N_a$ when a is square.

Now consider the case where a is not square, but $(a, b)_F \cong M_2(F)$. We know $M_2(F)$ is split, so $(a, b)_F$ must be split. This means that there exists some non-zero $p = q + ri + sj + tk \in (a, b)_F$ such that

$$\begin{aligned} n(p) = q^2 - ar^2 - bs^2 + abt^2 = 0 \\ \Rightarrow (q^2 - ar^2) = b(s^2 - at^2) \\ \Rightarrow b = \frac{(q^2 - ar^2)}{(s^2 - at^2)}. \end{aligned}$$

We have assumed a is not square, so we can safely assume both $(s^2 - at^2)$ and $(q^2 - ar^2)$ are non-zero, meaning $b \in N_a$ and is well-defined.

□

Now we will move on to composition algebras with $\dim_F A = 8$.

Definition 3.2.19 (Octonion algebra)**.** Let $A = (a, b, c)_F$ be an 8-dimensional F-vector space with fixed $a, b, c \in F^\times$ and F-basis $\{1_F, i, j, k, l, il, jl, kl\}$ such that

$$\begin{aligned} &i^2 = a, \quad j^2 = b, \quad ij = k = -ji, \quad l^2 = c, \\ &il = -li, \quad jl = -lj, \quad kl = -lk. \end{aligned}$$

Defining 1_F to be the unit element, A is a unital, non-associative, non-commutative F-algebra called an octonion algebra.

We will cover octonion algebras in a little more detail in the next section, but for now let us consider some examples for $F = \mathbb{R}$.

Example 3.2.20. $A = (-1, -1, -1)_{\mathbb{R}}$ is a real octonion algebra known as the Cayley numbers. For a general element x and conjugate x^*,

$$\begin{aligned} x &= a_0 + a_1 i + a_2 j + a_3 k + a_4 l + a_5 il + a_6 jl + a_7 kl, \\ x^* &= a_0 - a_1 i - a_2 j - a_3 k - a_4 l - a_5 il - a_6 jl - a_7 kl, \end{aligned}$$

the norm is given by

$$n(x) = xx^* = a_0^2 + a_1^2 + a_2^2 + a_3^2 + a_4^2 + a_5^2 + a_6^2 + a_7^2.$$

This vanishes only when $x = 0$ (i.e. $a_i = 0, \forall i$), so $(-1,-1,-1)_{\mathbb{R}}$ is a division algebra.

Definition 3.2.21 (Zorn's vector-matrices [14])**.** Zorn's vector-matrix algebra $A = \mathrm{Zorn}(F)$ consists of "vector-matrices" $\mathbf{M}$ given by

$$\mathbf{M} = \begin{pmatrix} a & \mathbf{x} \\ \mathbf{y} & b \end{pmatrix},$$

where $a, b \in F$ and $\mathbf{x}, \mathbf{y} \in F^3$. Multiplication is defined in terms of the dot product $\cdot : F^3 \times F^3 \to F$ and the cross product $\times : F^3 \times F^3 \to F^3$ by

$$\begin{aligned} \mathbf{M}\mathbf{M}' &= \begin{pmatrix} a & \mathbf{x} \\ \mathbf{y} & b \end{pmatrix} \begin{pmatrix} a' & \mathbf{x}' \\ \mathbf{y}' & b' \end{pmatrix} \\ &\stackrel{\text{def}}{=} \begin{pmatrix} aa' + \mathbf{x} \cdot \mathbf{y}' & a\mathbf{x}' + b'\mathbf{x} + \mathbf{y} \times \mathbf{y}' \\ a'\mathbf{y} + b\mathbf{y}' - \mathbf{x} \times \mathbf{x}' & bb' + \mathbf{x}' \cdot \mathbf{y} \end{pmatrix}. \end{aligned}$$

We showed in (2.1.2) that $\times$ is $\mathbb{R}$-bilinear. This also holds for any field F with $\mathrm{char}(F) \neq 2$. Since scalar multiplication and $\cdot$ are also F-bilinear, so too must be the product defined above.

Lemma 3.2.22. Zorn's vector-matrix algebra is a unital algebra.

Proof.

$$\mathbf{1}_A = \begin{pmatrix} 1 & \mathbf{0} \\ \mathbf{0} & 1 \end{pmatrix}$$

is the unit element since $\mathbf{1}_A\mathbf{M} = \mathbf{M}\mathbf{1}_A = \mathbf{M}$:

$$\begin{pmatrix} 1 & \mathbf{0} \\ \mathbf{0} & 1 \end{pmatrix} \begin{pmatrix} a & \mathbf{x} \\ \mathbf{y} & b \end{pmatrix} = \begin{pmatrix} a + \mathbf{0}\cdot\mathbf{y} & \mathbf{x} + b\mathbf{0} + \mathbf{0}\times\mathbf{y} \\ a\mathbf{0} + \mathbf{y} - \mathbf{0}\times\mathbf{x} & b + \mathbf{x}\cdot\mathbf{0} \end{pmatrix} = \begin{pmatrix} a & \mathbf{x} \\ \mathbf{y} & b \end{pmatrix}$$
$$\begin{pmatrix} a & \mathbf{x} \\ \mathbf{y} & b \end{pmatrix} \begin{pmatrix} 1 & \mathbf{0} \\ \mathbf{0} & 1 \end{pmatrix} = \begin{pmatrix} a + \mathbf{x}\cdot\mathbf{0} & a\mathbf{0} + \mathbf{x} + \mathbf{y}\times\mathbf{0} \\ \mathbf{y} + b\mathbf{0} - \mathbf{x}\times\mathbf{0} & b + \mathbf{0}\cdot\mathbf{y} \end{pmatrix} = \begin{pmatrix} a & \mathbf{x} \\ \mathbf{y} & b \end{pmatrix}.$$

□

In the next proof, we will use three important identities from linear algebra in F^3:

$$\mathbf{x}\cdot(\mathbf{y}\times\mathbf{z}) = \mathbf{y}\cdot(\mathbf{z}\times\mathbf{x}) = \mathbf{z}\cdot(\mathbf{x}\times\mathbf{y})$$
$$\mathbf{x}\times\mathbf{x} = \mathbf{0} \quad \forall\mathbf{x}\in F^3$$
$$(\mathbf{a}\times\mathbf{b})\cdot(\mathbf{c}\times\mathbf{d}) = (\mathbf{a}\cdot\mathbf{c})(\mathbf{b}\cdot\mathbf{d}) - (\mathbf{b}\cdot\mathbf{d})(\mathbf{a}\cdot\mathbf{d})$$

The first two facts imply that if a vector appears twice in the scalar triple product, it vanishes. The final fact is the Binet-Cauchy identity.

Theorem 3.2.23. Zorn's vector-matrix algebra A is a composition algebra with norm

$$n(\mathbf{M}) = \det\begin{pmatrix} a & \mathbf{x} \\ \mathbf{y} & b \end{pmatrix} \stackrel{\text{def}}{=} ab - \mathbf{x}\cdot\mathbf{y}, \qquad \forall\mathbf{M}\in A.$$

Proof. We can show that n is a multiplicative, non-degenerate quadratic form.

$$\begin{aligned}
\det \mathbf{M}\mathbf{M}' &= (aa' + \mathbf{x}\cdot\mathbf{y}')(bb' + \mathbf{x}'\cdot\mathbf{y}) - (a\mathbf{x}' + b'\mathbf{x} + \mathbf{y}\times\mathbf{y}')\cdot(a'\mathbf{y} + b\mathbf{y}' - \mathbf{x}\times\mathbf{x}') \\
&= (aba'b' + aa'\mathbf{x}'\cdot\mathbf{y} + bb'\mathbf{x}\cdot\mathbf{y}') + (\mathbf{x}\cdot\mathbf{y}')(\mathbf{x}'\cdot\mathbf{y}) \\
&\quad - (aa'\mathbf{x}'\cdot\mathbf{y} + ab\mathbf{x}'\cdot\mathbf{y}' + b'b\mathbf{x}\cdot\mathbf{y}' + b'a'\mathbf{x}\cdot\mathbf{y}) \\
&\quad - a'\mathbf{y}\cdot(\mathbf{y}\times\mathbf{y}') - b\mathbf{y}'\cdot(\mathbf{y}\times\mathbf{y}') \\
&\quad + a\mathbf{x}'\cdot(\mathbf{x}\times\mathbf{x}') + b'\mathbf{x}\cdot(\mathbf{x}\times\mathbf{x}') \\
&\quad + (\mathbf{y}\times\mathbf{y}')\cdot(\mathbf{x}\times\mathbf{x}'). \\
&= aba'b' + (\mathbf{x}\cdot\mathbf{y}')(\mathbf{x}'\cdot\mathbf{y}) - (ab\mathbf{x}'\cdot\mathbf{y}' + b'a'\mathbf{x}\cdot\mathbf{y}) + (\mathbf{y}\times\mathbf{y}')\cdot(\mathbf{x}\times\mathbf{x}') \\
&= (ab - \mathbf{x}\cdot\mathbf{y})(a'b' - \mathbf{x}'\cdot\mathbf{y}'),
\end{aligned}$$

where we used the Binet-Cauchy identity in the final step. We will now write the determinant as we did in the proof for (3.2.12), with a small abuse of notation:

$$\begin{aligned}
\det \mathbf{M} &= \begin{vmatrix} a & \mathbf{x} \\ \mathbf{y} & b \end{vmatrix} = ab - \mathbf{x}\cdot\mathbf{y} \\
&= \begin{pmatrix} a & b & \mathbf{x} & \mathbf{y} \end{pmatrix} \begin{pmatrix} 0 & \frac{1}{2} & 0 & 0 \\ \frac{1}{2} & 0 & 0 & 0 \\ 0 & 0 & 0 & -\frac{1}{2} \\ 0 & 0 & -\frac{1}{2} & 0 \end{pmatrix} \begin{pmatrix} a \\ b \\ \mathbf{x} \\ \mathbf{y} \end{pmatrix} \\
&\overset{\text{def}}{=} \mathbf{a}^{\mathsf{T}}\mathbf{D}\mathbf{a}.
\end{aligned}$$

The remainder of the proof is identical to that of (3.2.12), so this is a non-degenerate, quadratic form and A is a composition algebra. □

Corollary 3.2.24. Zorn's vector-matrix algebra is an octonion algebra.

Proof. Consider a real octonion algebra $A = (a, b, c)_F$, and some element $x \in A$. We can write this element in the following form:

$$x = (a_0 + \mathbf{x}) + l(b_0 + \mathbf{y}) \qquad \mathbf{x} = a_1 i + a_2 j + a_3 k, \quad \mathbf{y} = b_1 i + b_2 j + b_3 k,$$

where $a_i, b_i \in F$. Then consider the map $\phi : (a, b, c)_F \to \mathrm{Zorn}(F)$ given by

$$\phi(x) = \begin{pmatrix} a_0 + b_0 & \mathbf{x} + \mathbf{y} \\ -\mathbf{x} + \mathbf{y} & a_0 - b_0 \end{pmatrix}.$$

Computing the norm in $\mathrm{Zorn}(F)$ yields

$$\begin{aligned}
\det \phi(x) &= (a_0 + b_0)(a_0 - b_0) - (\mathbf{x} + \mathbf{y}) \cdot (-\mathbf{x} + \mathbf{y}) \\
&= a_0^2 - b_0^2 - \begin{pmatrix} (a_1 + b_1) \\ (a_2 + b_2) \\ (a_3 + b_3) \end{pmatrix} \cdot \begin{pmatrix} (b_1 - a_1) \\ (b_2 - a_2) \\ (b_3 - a_3) \end{pmatrix} \\
&= a_0^2 - b_0^2 - (b_1 + a_1)(b_1 - a_1) \\
&\quad - (b_2 + a_2)(b_2 - a_2) - (b_3 + a_3)(b_3 - a_3) \\
&= a_0^2 - b_0^2 - b_1^2 + a_1^2 - b_2^2 + a_2^2 - b_3^2 + a_3^2 \\
&= a_0^2 + a_1^2 + a_2^2 + a_3^2 - b_0^2 - b_1^2 - b_2^2 - b_3^3.
\end{aligned}$$

This is exactly the norm form for $(-1, -1, 1)_F$, the split-octonion algebra. Since isomorphic composition algebras have the same norm form up to isotopy, we must have $(-1, -1, 1)_F \cong \mathrm{Zorn}(F)$. □

Corollary 3.2.25. $\mathrm{Zorn}(F)$ is a split algebra.

Proof. From (3.2.24), $x = 1_F + l$ is an isotropic vector for $n(x) = \det \phi(x)$. Thus, n is isotropic and $\mathrm{Zorn}(F)$ is split. □

We will now give the full statement of Hurwitz' theorem:

Theorem 3.2.26 (Hurwitz [8])**.** Let A be a unital composition algebra over F. Then $\dim_F(A) \in \{1, 2, 4, 8\}$ and we have:

(i) When $\dim_F(A) = 1$ we have $A = F$

(ii) When $\dim_F(A) = 2$ we have $A = (a)_F \cong F \oplus F$ iff $a \in F^\times$ is square. Otherwise, we have $(a)_F \cong F(\sqrt{a})$, a division algebra.

(iii) When $\dim_F(A) = 4$ we have $A = (a, b)_F \cong M_2(F)$ iff $b \in N_a$. Otherwise, $(a, b)_F$ is a division algebra.

(iv) When $\dim_F(A) = 8$ we have either $A = (a, b, c)_F \cong \mathrm{Zorn}(F)$, or $(a, b, c)_F$ is a division algebra.

Proof. (i) is obvious. We showed (ii) in (3.2.1) and (3.1.16). (iii) follows from (3.2.18) and (3.1.14). We have not shown (iv), and we did not state the conditions on a, b, c by which $(a, b, c)_F$ is a split algebra or a division algebra. However, we did gain a little insight from (3.2.20) and our exploration of Zorn's algebra. The full proof is beyond the scope of this paper, see [8, 15, 16, 17, 18]. □

3.3 Cayley-Dickson doubling

Having explored some composition algebras, we will now describe a method of constructing them from some starting field F.

Take the 2-dimensional F-vector space $F \oplus F$, and some fixed $a \in F^\times$. Define an involution denoted by * and a product denoted by juxtaposition for $x_0, x_1, y_0, y_1 \in F$ as follows:

$$(x_0, y_0)^* = (x_0, -y_0),$$
$$(x_0, y_0)(x_1, y_1) = (x_0x_1 + ay_1y_0, y_1x_0 + y_0x_1).$$

This is a 2-dimensional F-algebra, denoted $\mathrm{Cay}(F, a)$.

Lemma 3.3.1. $\mathrm{Cay}(F, a)$ is a composition algebra, specifically $\mathrm{Cay}(F, a) \cong (a)_F$.

Proof. Taking * to be the canonical involution, the norm is given for $(x, y) \in \mathrm{Cay}(F, a)$ by:

$$\begin{aligned} n(x,y) &= (x, y)(x, -y) \\ &= (x^2 - ay^2, -yx + yx) \\ &= (x^2 - ay^2, 0). \end{aligned}$$

Writing this in terms of the F-basis $\{(1, 0), (0, 1)\}$, we have $n(x, y) = x^2 - ay^2$. This is the norm for the binion algebra $(a)_F$, which is unique up to isomorphism, so we must have $\mathrm{Cay}(F, a) \cong (a)_F$. Explicitly, the isomorphism is given by $\phi(1, 0) = 1, \phi(0, 1) = i$. □

Now take the 4-dimensional F-vector space $(a)_F \oplus (a)_F$, and some fixed $b \in F^\times$. Define an involution and product for $x_0, x_1, y_0, y_1 \in (a)_F$ as follows:

$$\begin{aligned} (x_0, y_0)^* &= (x_0^*, -y_0) \\ (x_0, y_0)(x_1, y_1) &= (x_0x_1 + by_1^*y_0, y_1x_0 + y_0x_1^*). \end{aligned}$$

This is a 4-dimensional F-algebra, denoted $\mathrm{Cay}((a)_F, b)$. Taking * to be the canonical involution gives the norm for $(x, y) \in \mathrm{Cay}((a)_F, b)$, $n(x, y) = (x, y)(x, y)^* = (x, y)(x^*, -y)$.

Remark. In general, for $\mathrm{Cay}(A, \alpha)$, we take * inside the brackets to denote the canonical involution for A, and outside of the brackets to denote the canonical involution for $\mathrm{Cay}(A, \alpha)$.

Lemma 3.3.2. $\mathrm{Cay}((a)_F, b) \cong (a, b)_F$.

Proof. We once again take * to be the canonical involution (noting the previous remark). Then taking $x = (p, q), y = (r, s) \in (a)_F$, we have

$$\begin{aligned} n(x, y) &= (x, y)(x^*, -y) \\ &= (xx^* - by^*y, -yx + yx) \\ &= (xx^* - by^*y, 0) \\ &= ((p, q)(p, -q) - b(r, -s)(r, s), 0) \\ &= (p^2 - aq^2 - b(r^2 - as^2), 0) \\ &= (p^2 - aq^2 - br^2 + abs^2, 0). \end{aligned}$$

Now, we write $\mathrm{Cay}((a)_F, b) = (F \oplus F) \oplus i(F \oplus F)$ as an F-vector space, giving a basis $\{(1, 0), (i, 0), (0, 1), (0, i)\}$. Then the norm is $n(x, y) = p^2 - aq^2 - br^2 + abs^2$. This is the norm for the quaternion algebra $(a, b)_F$, which is unique up to isomorphism, so we must have $\mathrm{Cay}((a)_F, b) \cong (a, b)_F$. Explicitly, the isomorphism is given by $\phi(1, 0) = 1, \phi(i, 0) = i, \phi(0, 1) = j, \phi(0, i) = k$. □

Now take the 8-dimensional F-vector space $(a, b)_F \oplus (a, b)_F$, and some fixed $c \in F^\times$. Define an involution and product for $x_0, x_1, y_0, y_1 \in (a, b)_F$ as follows:

$$\begin{aligned} (x_0, y_0)^* &= (x_0^*, -y_0) \\ (x_0, y_0)(x_1, y_1) &= (x_0x_1 + cy_1^*y_0, y_1x_0 + y_0x_1^*). \end{aligned}$$

This is an 8-dimensional F-algebra, denoted $\mathrm{Cay}((a, b)_F, c)$. Inside the brackets, * now refers to the canonical involution on $(a, b)_F$, following the general rule laid out in the previous remark. Then outside of the brackets, * refers to the canonical involution on $\mathrm{Cay}((a, b)_F, c)$. We can then define the norm for $(x, y) \in \mathrm{Cay}((a, b)_F, c)$ as $n(x, y) = (x, y)(x, y)^* = (x, y)(x^*, -y)$.

Lemma 3.3.3. $\mathrm{Cay}((a, b)_F, c) \cong (a, b, c)_F$.

Proof. It can be shown that the norm of $\mathrm{Cay}((a,b)_F, c)$ is identical to that of $(a,b,c)_F$, writing $\mathrm{Cay}((a,b)_F, b) = ((F \oplus F) \oplus i(F \oplus F)) \oplus l(F \oplus F) \oplus i(F \oplus F))$ as an F-vector space. This follows the same process as (3.3.1) and (3.3.2), so we will simply state the isomorphism $\phi : \mathrm{Cay}((a,b)_F, c) \to (a,b,c)_F$.

$$\phi(1,0) = 1, \qquad \phi(i,0) = i, \qquad \phi(0,1) = j, \qquad \phi(0,i) = k,$$
$$\phi(l,0) = l, \qquad \phi(li,0) = li, \qquad \phi(0,l) = lj, \qquad \phi(0,li) = lk.$$

□

For both $\mathrm{Cay}((a)_F, b)$ and $\mathrm{Cay}((a,b)_F, c)$, we defined the involution and product in the exact same way. We can continue this process ad infinitum, constructing 2^n-dimensional F-algebras for $n \in \mathbb{N}$. However, we know that composition algebras exist only for dimensions $\{1, 2, 4, 8\}$. Therefore all algebras obtained through this construction that have a higher dimension, whilst still having a quadratic form, are not composition algebras (i.e. the form is not multiplicative). To finish this chapter, we will present the symmetries of each composition algebra, and display how each successive application of the Cayley-Dickson doubling loses a property of the doubled algebra.

Definition 3.3.4 ($\Re(x)$ and $\Im(x)$)**.** Let A be a composition algebra over F with canonical involution * and F-basis $\{e_0, e_1, e_2, ...\}$, where $e_0 \in F$. For $x = x_0e_0 + x_1e_1 + ...$ with $x_0, x_1, ... \in F$, we define the real and imaginary parts of x as

$$\Re(x) = 1/2(x + x^*) = x_0e_0,$$
$$\Im(x) = 1/2(x - x^*) = x_1e_1 + x_2e_2 + ...,$$

respectively.

Lemma 3.3.5. Every octonion algebra is alternative.

Proof. Let $(a,b),(c,d) \in \mathrm{Cay}((\alpha,\beta)_F,\gamma) \cong (\alpha,\beta,\gamma)_F$, with $a,b,c,d \in (\alpha,\beta)_F$. Then

$$\begin{aligned}((a,b)(a,b))(c,d) &= (aa+\gamma b^*b, ba+ba^*)(c,d)\\ &= ((aa+\gamma b^*b)c+\gamma d^*(ba+ba^*), d(aa+\gamma b^*b)+(ba+ba^*)c^*)\\ &= (aac+\gamma b^*bc+\gamma d^*ba+\gamma d^*ba^*, daa+\gamma db^*b+bac^*+ba^*c^*)\\ &= (aac+\gamma b^*bc+\gamma d^*b(a+a^*), daa+\gamma db^*b+b(a+a^*)c^*)\\ &= (aac+\gamma n(b)c+2\gamma\Re(a)d^*b, daa+2\Re(a)bc^*+\gamma n(b)d).\end{aligned}$$

We used the fact that $(\alpha,\beta)_F$ is an associative algebra in the penultimate equality, and the fact that $2\Re(a) = (a+a^*)$ is scalar in the last. Continuing,

$$\begin{aligned}(a,b)((a,b)(c,d)) &= (a,b)(ac+\gamma d^*b, da+bc^*)\\ &= (a(ac+\gamma d^*b)+\gamma(da+bc^*)^*b, (da+bc^*)a+b(ac+\gamma d^*b)^*)\\ &= (aac+\gamma ad^*b+\gamma a^*d^*b+\gamma cb^*b, daa+bc^*a+bc^*a^*+\gamma bb^*d)\\ &= (aac+\gamma(a+a^*)d^*b+\gamma cb^*b, daa+bc^*(a+a^*)+\gamma bb^*d)\\ &= (aac+2\gamma\Re(a)d^*b+\gamma n(b)c, daa+2\Re(a)bc^*+\gamma n(b)d).\end{aligned}$$

So, we have $((a,b)(a,b))(c,d) = (a,b)((a,b)(c,d))$. It can be shown similarly that $(a,b)((c,d)(c,d)) = ((a,b)(c,d))(c,d)$. Then the result follows from (3.1.5). □

Definition 3.3.6. Let $A = \mathrm{Cay}((a,b,c)_F,d) = (a,b,c,d)_F$ be the 16-dimensional F-algebra generated by applying the Cayley-Dickson doubling to the octonion algebra $(a,b,c)_F$. This is called a sedenion algebra.

Definition 3.3.7 (Power associativity)**.** An algebra A is power associative if $x^nx^m = x^{n+m}, \quad \forall x \in A, m,n \in \mathbb{N}$.

Now, take some arbitrary field F and recursively apply the Cayley-Dickson doubling with $a, b, c, d \in F^{\times}$. This generates the following sequence of unital algebras:

$$F \to (a)_F \to (a, b)_F \to (a, b, c)_F \to (a, b, c, d)_F \to \dots$$

We know that multiplication in a field F is commutative, associative and alternative (in fact, associativity implies alternativity). The same is true for $(a)_F$. However, when we double from $(a)_F \to (a, b)_F$, we lose commutativity. Then from $(a, b)_F \to (a, b, c)_F$ we lose associativity. Finally, from $(a, b, c)_F \to (a, b, c, d)_F$ we lose alternativity. We do, however, retain power associativity for all remaining algebras in the sequence. From (3.1.7), we know that composition algebras are alternative, which explains the restriction to dimensions $\{1, 2, 4, 8\}$.

Remark. If F is an ordered field, we lose said ordering with $F \to (a)_F$.

Chapter 4

Central simple algebras

4.1 Definitions

Definition 4.1.1 (Central algebra)**.** Let A be an associative F-algebra over its centre, $\mathcal{Z}(A) = F$. Then A is a central algebra.

Example 4.1.2. Consider the binion algebra $A = (a)_F$. We know that $F \subset \mathcal{Z}(A)$ from bilinearity of the product in A. However, we also know that $(a)_F$ is a commutative algebra, so $\mathcal{Z}(A) = (a)_F \neq F$. Thus, $(a)_F$ is not a central algebra.

Theorem 4.1.3 (Wedderburn's little theorem)**.** Let A be a finite division algebra. Then A is a field.

We will not give the proof here as it is beyond the scope of this paper; see [20] p.204, [22] p.22, [21] ch.3.

Example 4.1.4. Now consider the quaternion algebra $A = (a, b)_F$. From the Cayley-Dickson construction, it is clear that $(a)_F$ is a sub-algebra of A, so we might consider it as a candidate for $\mathcal{Z}(A)$. However, this would be a mistake, since we know $ij = -ji$ in A. It can be shown that 1_A is the only basis element

that commutes with all the other elements, meaning $\mathcal{Z}(A) = \text{span}_F\{1_A\} = F$. So, $(a, b)_F$ is a central algebra.

Definition 4.1.5 (Ideal)**.** Let A be an algebra and $I \subset A$. We say I is a left ideal if it is an additive subgroup of A, and it absorbs multiplication on the left (i.e. $\forall a \in A, x \in I$, we have $xa \in I$). Similarly, I is a right ideal if it instead absorbs multiplication on the right (i.e. $ax \in I$). If I is both a left and right ideal, we call it a two-sided ideal.

Remark. For any algebra A, we have two trivial ideals; $\{0\}$ and A itself.

Definition 4.1.6 (Simple algebra)**.** Let A be an F-algebra with no non-trivial two-sided ideals. Then A is a simple algebra.

Definition 4.1.7 (Central simple algebra)**.** Let A be an associative F-algebra that is both central and simple. Then it is a central simple algebra or CSA.

Lemma 4.1.8. $A = (a, b)_F$ is a central simple algebra.

Proof. We have already seen from (4.1.4) that $A = (a, b)_F$ is a central algebra. Let $I \subset A$ be an ideal. For arbitrary $x_0, x_1, x_2, x_3 \in F$ we have $x = x_0 + x_1 i + x_2 j + x_3 k \in A$ and similarly defined $y \in I$. Then there must exist $z \in I$ such that:

$$\begin{aligned} xy &= (x_0 + x_1 i + x_2 j + x_3 k)(y_0 + y_1 i + y_2 j + y_3 k) \\ &= (x_0 y_0 + a x_1 y_1 + b x_2 y_2 - ab x_3 y_3) + (x_0 y_1 + x_1 y_0 - b x_2 y_3 + b x_3 y_2) i \\ &\quad + (x_0 y_2 + x_2 y_0 + a x_1 y_3 - a x_3 y_1) j + (x_0 y_3 + x_3 y_0 + x_1 y_2 - x_2 y_1) k \\ &= z_0 + z_1 i + z_2 j + z_3 k = z. \end{aligned}$$

For this to be true, we require y and z to have the same form when comparing coefficients (i.e. $y_i = 0 \iff z_i = 0$). It is clear that this can only happen when all of z_i vanishes, or none of them do. Hence, $I = \{0\}$ or $I = A$. □

4.2 Wedderburn's theorem

Theorem 4.2.1 (Wedderburn's theorem)**.** Let A be an F-algebra. Then A is simple iff there is a division F-algebra D and some $n \geq 1$ such that $A \cong M_n(D)$. D and n are uniquely determined by A up to isomorphism.

Proof. See [23] for an in-depth proof that is beyond the scope of this paper. □

Corollary 4.2.2. Every division algebra is simple.

Proof. Let A be a division algebra. Then $A = M_1(A)$, so A must be simple. □

We will now take a brief detour to describe some new tools. We can then use these tools to prove some more properties of CSA's.

Definition 4.2.3 (Tensor product)**.** Let A be an m-dimensional F-vector space, and B be an n-dimensional F-vector space. Define an F-basis for each of A and B by $\{\mathbf{a}_1, ..., \mathbf{a}_m\}$ and $\{\mathbf{b}_1, ..., \mathbf{b}_n\}$, respectively. Then, we define the tensor product $\otimes : A \times B \to A \otimes_F B$ as

$$\mathbf{a}_i \otimes \mathbf{b}_j \stackrel{\text{def}}{=} \mathbf{a}_i \mathbf{b}_j^{\mathsf{T}}$$

where $i = 1, ..., m$ and $j = 1, ..., n$ and $A \otimes_F B = \text{span}_F(\mathbf{a}_i \otimes \mathbf{b}_j)$.

Definition 4.2.4 (Pure tensor)**.** A tensor $\mathbf{w} \in A \otimes_F B$ is called a pure tensor if it can be written in the form $\mathbf{u} \otimes \mathbf{v}$ for some $\mathbf{u} \in A$, $\mathbf{v} \in B$.

For elements $\mathbf{u}_1, \mathbf{u}_2 \in A$, $\mathbf{v}_1, \mathbf{v}_2 \in B$ and $k \in F$, the tensor product has the following properties:

$$\begin{aligned}
&\text{(i)} && (\mathbf{u}_1 \otimes \mathbf{v}_1)^{\mathsf{T}} && = && (\mathbf{v}_1 \otimes \mathbf{u}_1),\\
&\text{(ii)} && (\mathbf{u}_1 + \mathbf{u}_2) \otimes (\mathbf{v}_1) && = && \mathbf{u}_1 \otimes \mathbf{v}_1 + \mathbf{u}_2 \otimes \mathbf{v}_1,\\
&\text{(iii)} && \mathbf{u}_1 \otimes (\mathbf{v}_1 + \mathbf{v}_2) && = && \mathbf{u}_1 \otimes \mathbf{v}_1 + \mathbf{u}_1 \otimes \mathbf{v}_2,\\
&\text{(iv)} && k(\mathbf{u}_1 \otimes \mathbf{v}_1) && = && (k\mathbf{u}_1) \otimes (\mathbf{v}_1) = \mathbf{u}_1 \otimes (k\mathbf{v}_1).
\end{aligned}$$

Example 4.2.5. Given (4.2.4), we might wonder what an "impure" tensor looks like. Consider two pairs of linearly independent vectors $\mathbf{u}_1, \mathbf{u}_2 \in A$ and $\mathbf{v}_1, \mathbf{v}_2 \in B$. Then $\mathbf{u}_1 \otimes \mathbf{v}_1 + \mathbf{u}_2 \otimes \mathbf{v}_2 \in A \otimes_F B$ cannot be written as a pure tensor.

From now on, we will drop the bold vector notation and use a and b to refer to arbitrary elements in A and B respectively.

Lemma 4.2.6. Let A and B be unital F-algebras. Then $A \otimes_F B$ is also a unital F-algebra, with unit $1_A \otimes 1_B$.

Proof. Consider the map given by $(a_1 \otimes b_1)(a_2 \otimes b_2) = a_1a_2 \otimes b_1b_2$. This maps pure tensors to pure tensors, but we can extend it to all tensors by enforcing linearity:

$$\begin{aligned}
(a_1 \otimes b_1 + a_2 \otimes b_2)(a_3 \otimes b_3) &\overset{\text{def}}{=} (a_1 \otimes b_1)(a_3 \otimes b_3) + (a_2 \otimes b_2)(a_3 \otimes b_3)\\
&= a_1a_3 \otimes b_1b_3 + a_2a_3 \otimes b_2b_3
\end{aligned}$$

Rather than showing this is F-bilinear, we have defined it to be so! We then know that the unit element is $1_A \otimes 1_B$ as

$$(a \otimes b)(1_A \otimes 1_B) = a1_A \otimes b1_B = (a \otimes b) = 1_Aa \otimes 1_Bb = (1_A \otimes 1_B)(a \otimes b),$$

where we used the fact that 1_A commutes with all $a \in A$, and 1_B commutes with all $b \in B$. □

Remark. From the treatment of 1_A and 1_B in the previous proof, it should be clear that if A and B are both commutative, so is $A \otimes_F B$.

Lemma 4.2.7. $\dim_F (A \otimes_F B) = \dim_F (A) \dim_F (B)$.

Proof. We can write an element in A as a $(\dim_F A) \times 1$ matrix (i.e. a column vector), and an element in B as a $(\dim_F B) \times 1$ matrix. The transpose of an element in B will be a $1 \times (\dim_F B)$ matrix (i.e. a row vector). Then from linear algebra, we can write an element in $A \otimes_F B$ as $(\dim_F A) \times (\dim_F B)$ matrix. The F-vector space of $(\dim_F A) \times (\dim_F B)$ matrices, unsurprisingly, has dimension $\dim_F A \dim_F B$. □

Lemma 4.2.8. Let A be a finite F-algebra and let K/F be a finite field extension (2.2.1). Then A is a CSA over F iff $A \otimes_F K$ is a CSA over K.

Proof. Recall that the product in $A \oplus_F K$ I is given for pure tensors by $(a_1 \otimes k_1)(a_2 \otimes k_2) = a_1 a_2 \otimes k_1 k_2$ (i.e. multiplication occurs componentwise). Then if I is a non-trivial ideal of A, $I \otimes_F K$ must be a non-trivial ideal of $A \otimes_F K$. Similarly, if $A \otimes_F K$ is central (i.e. its centre is precisely the embedding of K into $A \otimes_F K$, $k \hookrightarrow 1_F \otimes k$), then A must be central (i.e. its centre is F, since F is a subfield of K). Thus, $A \otimes_F K$ is a CSA over $K \Rightarrow A$ is a CSA over F.

Proof of the converse is beyond the scope of this paper, but can be found in [25] Lemma 2.2.2. □

Corollary 4.2.9. If A is a finite-dimensional CSA over F, $\dim_F A$ is square.

Proof. Consider $A \otimes_F \bar{F}$, where $\bar{F}$ is the algebraic closure of F and $[F : \bar{F}]$ is finite. From (4.2.8), $A \otimes_F \bar{F}$ is a CSA over $\bar{F}$. Then from (4.2.1), $A \otimes_F \bar{F} \cong M_n(D)$ for some $n \geq 1$ and division $\bar{F}$-algebra D. We must have $D = \bar{F}$ from (2.2.11). Then

$$\dim_{\bar{F}}(A \otimes_F \bar{F}) = \dim_{\bar{F}}(M_n(\bar{F})) = n^2.$$

We also know, from (2.2.3), that

$$\dim_{\bar{F}}(A \otimes_F \bar{F}) \dim_F(\bar{F}) = \dim_F(A \otimes_F \bar{F})$$

and from (4.2.7),

$$\dim_F(A \otimes_F \bar{F}) = \dim_F(A) \dim_F(\bar{F}).$$

Putting all of this together, we have

$$\dim_F(A) = \frac{\dim_F(A \otimes_F \bar{F})}{\dim_F(\bar{F})} = \frac{\dim_{\bar{F}}(A \otimes_F \bar{F}) \dim_F(\bar{F})}{\dim_F(\bar{F})} = \dim_{\bar{F}}(A \otimes_F \bar{F}) = n^2.$$

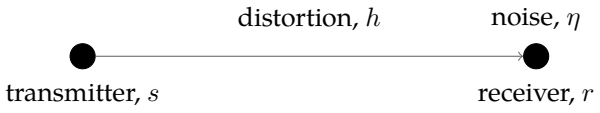
□

Chapter 5

Space time block coding

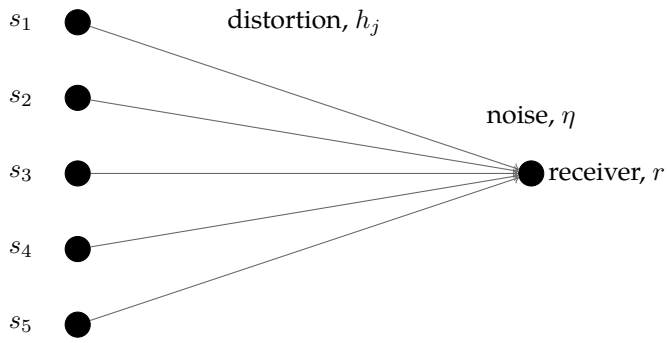
5.1 Introduction

This section will closely follow the treatment by Hendrickson in [26], as he introduces the topic in an intuitive fashion. Consider the following scenario: we have a single antenna and wish to transmit a signal to another antenna. We can model the *signal* as a complex number $s \in \mathbb{C}$. As the signal travels from the transmitter to the receiver, it is distorted, which we can model by multiplying s with another complex number $h \in \mathbb{C}$. We call h the *fade coefficient*. At the receiver there is some *noise*, which we can model by yet another complex number, $\eta \in \mathbb{C}$. Then, the *received signal* $r \in \mathbb{C}$ is $r = hs + \eta$. The aim of space time block coding is to maximise the probability that the receiver can obtain s from r.



A simple channel with a single transmitter and a single receiver.

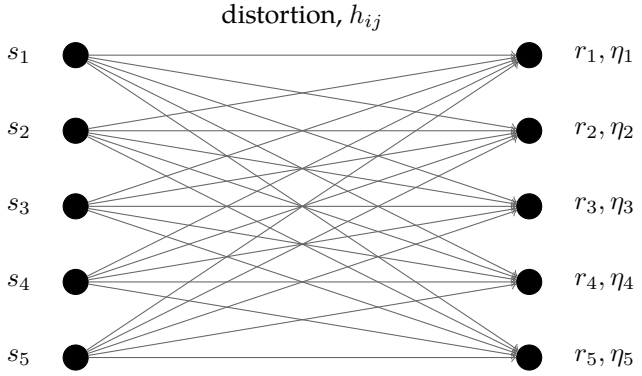
Of course, we likely want to send more data than a single complex number can contain, and we want it all to arrive at the same time. So, we can set up multiple transmit antennae (say, n_t of them), and transmit a signal from each. Model the signal sent from the j-th antenna by $s_j \in \mathbb{C}$, where $j \in \{1, ..., n_t\}$. Each antenna is distinct, so each signal s_i will take a different path to the receiver. Each path will have a distinct fade coefficient, h_j. Since there is still just one receiver, we model the noise by η. Assuming every signal arrives at the same time (as we hope it would), the received signal will be a linear combination $r = h_1 s_1 + \cdots + h_{n_t} s_{n_t} + \eta$.



A channel with $n_t = 5$.

Upon arrival, our transmitted signals may be difficult to understand due to distortion and noise. If each transmitter sends a copy of its signal to multiple reception antenna (say, n_r of them), it will be easier to decode our message. We can model the noise at the i-th receiver as η_i, where $i \in \{1, ..., n_r\}$. Each path from the j-th transmission antenna to the i-th reception antenna will have its own fade coefficient, $h_i j$. Then, the i-th reception antenna will receive $r_i = h_{i1} s_1 + \cdots + h_{in_t} s_{n_t} + \eta_i$. We can write this as a single matrix equation, $\mathbf{r} = \mathrm{Hs} + \boldsymbol{\eta}$:

$$\begin{pmatrix} r_1 \\ r_2 \\ \vdots \\ r_{n_r} \end{pmatrix} = \begin{pmatrix} h_{11} & h_{12} & \dots & h_{1n_t} \\ h_{21} & h_{22} & \dots & h_{2n_t} \\ \vdots & \vdots & \ddots & \vdots \\ h_{n_r1} & h_{n_r2} & \dots & h_{n_rn_t} \end{pmatrix} \begin{pmatrix} s_1 \\ s_2 \\ \vdots \\ s_{n_t} \end{pmatrix} + \begin{pmatrix} \eta_1 \\ \eta_2 \\ \vdots \\ \eta_{n_r} \end{pmatrix}.$$



A channel with $n_t = n_r = 5$.

By creating multiple paths to transmit our signals, we have made our channel *spatially diverse*. We can also make our channel *temporally diverse* by transmitting simultaneously from every antenna once per set interval of time. To model this, define a *block* to be the set of natural numbers $\tau \in \{1, ..., T\}$ where T is the duration of transmissions. For each time τ in the block, the j-th transmitter will send a signal $s_{j\tau} \in \mathbb{C}$, and the i-th receiver will receive a signal $r_{i\tau}$. We make the assumption that the channel is *quasi-static*, meaning the fade coefficients h_{ij} do not change over the duration T. Then we can transmit one full *code matrix*

per time T:

$$\mathbf{R} = \begin{pmatrix} r_{11} & r_{12} & \dots & r_{1T} \\ r_{21} & r_{22} & \dots & r_{2T} \\ \vdots & \vdots & \ddots & \vdots \\ r_{n_r1} & r_{n_r2} & \dots & r_{n_rT} \end{pmatrix} \qquad \mathbf{H} = \begin{pmatrix} h_{11} & h_{12} & \dots & h_{1n_t} \\ h_{21} & h_{22} & \dots & h_{2n_t} \\ \vdots & \vdots & \ddots & \vdots \\ h_{n_r1} & h_{n_r2} & \dots & h_{n_rn_t} \end{pmatrix}$$

$$\mathbf{S} = \begin{pmatrix} s_{11} & s_{12} & \dots & s_{1T} \\ s_{21} & s_{22} & \dots & s_{2T} \\ \vdots & \vdots & \ddots & \vdots \\ s_{n_t1} & s_{n_t2} & \dots & s_{n_tT} \end{pmatrix} \qquad \mathbf{W} = \begin{pmatrix} \eta_{11} & \eta_{12} & \dots & \eta_{1T} \\ \eta_{21} & \eta_{22} & \dots & \eta_{2T} \\ \vdots & \vdots & \ddots & \vdots \\ \eta_{n_r1} & \eta_{n_r2} & \dots & \eta_{n_rT} \end{pmatrix}$$

Concisely, $\mathbf{R} = \mathbf{HS} + \mathbf{W}$. It is convenient for us to set $T = n_t$, as this gives square code matrices $\mathbf{S} \in M_{n_t}(\mathbb{C})$.

5.2 Terminology

We will now formally define some of concepts we used in the introduction.

Definition 5.2.1 (Signal constellation)**.** Let S be the set of signals we can transmit. We call S the signal constellation.

Remark. We introduced space time block codes with $S = \mathbb{C}$, however, we can have any $S \subset D$ where D is a division ring.

Definition 5.2.2 (Codebook)**.** For n transmit antennae and n receive antennae, a space-time codebook is a subset $\mathcal{C} \subset M_n(S)$. An element $V \in \mathcal{C}$ is a space time block code.

Remark. Letting $n_t = n_r = n$ means that the codes received are of the same dimension as the codes transmitted.

Definition 5.2.3 (Symbol)**.** An element $s \in S$ in the constellation is referred to as a symbol.

Definition 5.2.4 (Block length)**.** The block length T is the number of successive transmissions required to send one full block code.

Definition 5.2.5 (Linear codebook)**.** A codebook $\mathcal{C}$ is linear if for any codes $V, W \in \mathcal{C}$, we have $(V + W), (V - W) \in \mathcal{C}$ (i.e. the codebook $\mathcal{C}$ is closed under addition).

To determine how good a code is, there are a number of performance criteria. We will define some of them here.

Definition 5.2.6 (Rank criterion [27])**.** The rank criterion for a codebook $\mathcal{C} \subset M_n(S)$ is given by:

$$\text{rank}(V - W) = n \quad \forall V, W \in \mathcal{C}, V \neq W$$

If $\mathcal{C}$ satisfies the rank criterion, we say it is fully-diverse.

Definition 5.2.7 (Determinant criterion [27])**.** The determinant criterion for a codebook $\mathcal{C}$ seeks to maximise the following:

$$\delta_{\min}(\mathcal{C}) = \min_{V \neq W \in \mathcal{C}} |\det(V - W)|^2$$

Definition 5.2.8 (Rate)**.** The rate of a code $C \in \mathcal{C}$ is the number of symbols it transmits per time slot.

Definition 5.2.9 (Orthogonal STBC)**.** Let C_i denote the i-th column of a code $C \in \mathcal{C}$. If the vectors C_i, C_j are orthogonal $\forall i, j$, C is an orthogonal STBC.

Example 5.2.10. The simplest example of a (complex) space time block code is

the Alamouti code. It consists of linear codes $C \in M_2(\mathbb{C})$ of the form

$$C = \begin{pmatrix} c_1 & c_2 \\ -c_2^* & c_1^* \end{pmatrix},$$

where $c_1, c_2 \in \mathbb{C}$ and c_1^*, c_2^* are their respective complex conjugates. This is an orthogonal STBC, as

$$\begin{aligned} \begin{pmatrix} c_1 \\ -c_2^* \end{pmatrix} \begin{pmatrix} c_2 \\ c_1^* \end{pmatrix}^{\mathsf{T}} &= \begin{pmatrix} c_1 \\ -c_2^* \end{pmatrix} \begin{pmatrix} c_2^* & c_1 \end{pmatrix} \\ &= c_1 c_2^* - c_1 c_2^* = 0. \end{aligned}$$

Further, the difference between any two matrices of the above form will have maximal rank, so these codes are fully diverse. A single block encodes two symbols c_1, c_2 which take two time-slots to transmit, so the Alamouti code has rate $R = 1$. We refer to this as full-rate. It happens that the Alamouti code is the only full-rate orthogonal STBC.

5.3 STBCs from quaternion algebras

To finish off this paper, we will construct some fully diverse STBCs from a general quaternion algebra. First we will define some tools that will give us a construction process for STBCs from any associative division algebra. Then we will specifically focus on $(a, b)_F$.

Theorem 5.3.1. Let $A \subset M_n(D)$ be a division subalgebra of some matrix D-algebra $M_n(D)$. Then any linear codebook $\mathcal{C} \subseteq A$ contains fully diverse codes.

Proof. Since A is a division algebra, every element is invertible. It is a standard linear algebra result that invertible square matrices have maximal rank. Then

we have $\mathrm{rank}(V - W)$ is maximal for any V, W in $\mathcal{C} \subseteq A$, yielding fully diverse codes. □

Definition 5.3.2 (Left regular representation)**.** Let A be an F-algebra. For fixed $k \in A$, define the left regular representation as

$$\lambda_k : A \to A : x \mapsto kx, \quad \forall x \in A.$$

Then for each $k \in A$, $\lambda_k \in \mathrm{End}_F(A)$ is an F-linear map.

Lemma 5.3.3. Let A be an associative division F-algebra and let λ_k be the left regular representation for each $k \in A$. Then $\Lambda : A \to \mathrm{End}_F(A) : k \mapsto \lambda_k$ is a ring homomorphism.

Proof. Let $k_1, k_2 \in A$ be arbitrary elements in A, and let $c_1, c_2 \in F$. Then

$$\begin{aligned}(\Lambda(k_2) \circ \Lambda(k_1))(x) &= \lambda_{k_2}(\lambda_{k_1}(x)) = \lambda_{k_2}(k_1 x) \\ &= k_2(k_1 x) = k_2 k_1 x \\ &= \lambda_{k_2 k_1}(x) = \Lambda(k_2 k_1)(x)\end{aligned}$$

and

$$\begin{aligned}(\Lambda(c_1 k_1 + c_2 k_2))(x) &= (\lambda_{(c_1 k_1 + c_2 k_2)})(x) \\ &= (c_1 k_1 + c_2 k_2)x = c_1 k_1 x + c_2 k_2 x \\ &= c_1 \lambda_{k_1}(x) + c_2 \lambda_{k_2}(x) \\ &= (c_1 \Lambda(k_1) + c_2 \Lambda(k_2))(x).\end{aligned}$$

Trivially we have $\Lambda(1_A)(x) = \lambda(1_A)(x)$, so Λ is a ring homomorphism. □

Remark. If we consider Λ as a map $A \to \mathrm{image}(\Lambda)$ instead of $A \to \mathrm{End}_F(A)$, we have a bijective homomorphism since A is a division algebra (meaning every

$k \in A$ has an inverse, which implies the same for $\lambda_k \in \text{image}(\Lambda))$. Then we have an isomorphism $A \cong \text{image}(\Lambda)$.

Corollary 5.3.4. For an associative division F-algebra A, there exists a codebook $\mathcal{C} \subseteq M_n(F)$ for some n such that $A \cong \mathcal{C} \subseteq M_n(F)$.

Proof. λ_k is an F-linear map, so we can represent it as a matrix in $M_n(F)$ for some n. For this, we can define some map $L : \text{End}_F(A) \to M_n(F)$. It is obvious that this map is a ring homomorphism. Now consider the following composition:

$$A \xrightarrow{\Lambda} \text{End}_F(A) \xrightarrow{L} M_n(F).$$

Then with appropriate restrictions on the range of Λ and domain of L, we have an isomorphism $A \overset{\Lambda}{\cong} \text{image}(\Lambda) \overset{L}{\cong} \mathcal{C}$, where we have let $\mathcal{C} = \text{image}(L)$. □

We now have the tools we need to provide a codebook constructed from a general quaternion algebra, $(a, b)_F$. We take some element $x \in (a, b)_F$ and define the left regular representation $\lambda_x : y \mapsto xy$. We can write these elements

explicitly as $x = x_0 + x_i i + x_j j + x_k k$ and $y = y_0 + y_i i + y_j j + y_k k$. Then

$$\begin{aligned}
\lambda_x(y) &= xy \\
&= (x_0 + x_i i + x_j j + x_k k)(y_0 + y_i i + y_j j + y_k k) \\
&= (x_0 y_0 + x_0 y_i i + x_0 y_j j + x_0 y_k k) \\
&\quad + (x_i y_0 i + x_i y_i i^2 + x_i y_j ij + x_i y_k ik) \\
&\quad + (x_j y_0 j + x_j y_i ji + x_j y_j j^2 + x_j y_k jk) \\
&\quad + (x_k y_0 k + x_k y_i ki + x_k y_j kj + x_k y_k k^2) \\
&= (x_0 y_0 + a x_i y_i + b x_j y_j - ab x_k y_k) \\
&\quad + (x_0 y_i + x_i y_0 + b x_k y_j - b x_j y_k) i \\
&\quad + (x_0 y_j + x_j y_0 + a x_i y_k - b x_k y_i) j \\
&\quad + (x_0 y_k + x_k y_0 + x_i y_j - x_j y_i) k \\
&= \begin{pmatrix} 1 \\ i \\ j \\ k \end{pmatrix}^{\mathsf{T}} \begin{pmatrix} x_0 & a x_i & b x_j & -ab x_k \\ x_i & x_0 & b x_k & -b x_j \\ x_j & -b x_k & x_0 & a x_i \\ x_k & -x_j & x_i & x_0 \end{pmatrix} \begin{pmatrix} y_0 \\ y_i \\ y_j \\ y_k \end{pmatrix}.
\end{aligned}$$

We have obtained a matrix equation featuring a matrix in $M_4(F)$. Now we can define the maps $\Lambda : A \to \mathrm{End}_F(A)$ and $L : \mathrm{End}_F(A) \to M_4(F)$ by

$$\Lambda(x) \stackrel{\text{def}}{=} \lambda_x, \quad L(\lambda_x) \stackrel{\text{def}}{=} \begin{pmatrix} x_0 & a x_i & b x_j & -ab x_k \\ x_i & x_0 & b x_k & -b x_j \\ x_j & -b x_k & x_0 & a x_i \\ x_k & -x_j & x_i & x_0 \end{pmatrix}.$$

We can then define our codebook $\mathcal{C} \subset M_4(F)$ as the subalgebra of matrices that take the form of $L(\lambda_x)$. These codes will be fully diverse as $(a,b)_F$ is a division algebra, giving the matrices in $\mathcal{C}$ full rank.

Remark. It was important that we made restrictions to the range of Λ and domain of L before declaring an isomorphism. Two isomorphic F-algebras must have the same dimension as F-vector spaces. We know that $\dim_F((a,b)_F) = 4$, but $\dim_F(M_4(F)) = 16$, meaning $(a,b)_F \ncong M_4(F)$. Instead we have $(a,b)_F \cong \mathcal{C} \subset M_4(F)$, where we restricted $\Lambda : A \to \mathrm{image}(\Lambda)$ and $L : \mathrm{image}(\Lambda) \to \mathcal{C}$.

The process we followed here will work for any associative division algebra, and there exist modified constructions [28] for non-associative division algebras. We could also find suitable matrix algebras from central simple algebras, using Wedderburn's theorem (4.2.1).

Chapter 6

Further reading

In an effort to keep this text mostly self-contained, and in the interests of brevity, we missed out on a lot of extremely interesting content. We began by defining algebras in general, and immediately moved on to defining convenient properties that made computations on said algebras simpler. In doing so, we restricted ourselves to a tiny subset of what is a gargantuan field. Here are some suggestions for accessible texts that will build upon, or take an entirely different direction from the content in this paper.

Lie algebras

The very first example we gave (2.1.2) is an example of a **Lie algebra**. A group that is also a smooth manifold is called a Lie group. The tangent space of a Lie group G at its identity is a Lie algebra $\mathfrak{g}$. The product in $\mathfrak{g}$ is called the Lie bracket. It is alternative, anti-commutative and satisfies the Jacobi identity.

Physically, a Lie algebra represents infinitesimal symmetries, and so they have applications in particle physics and quantum mechanics. Recommended texts include the archived Fall 2004 MIT lecture series [29] and Kirillov's *Introduction to Lie Groups and Lie Algebras* [30].

Clifford algebras

Let V be an F-vector space and $Q : V \to F$ a quadratic form. Take the tensor algebra [31] $T(V)$ and the two-sided ideal $I_Q \subset T(V)$ generated by $v \otimes v - Q(v)1$ for $v \in V$. Then the Clifford algebra $\mathrm{Cl}(V, Q)$ is the quotient $T(V)/I_Q$. Over the reals $\mathbb{R}$, any quadratic form can be classified by its signature (p, q). Then the corresponding Clifford algebra is $\mathrm{Cl}_{p,q}(\mathbb{R})$. Similarly for complex numbers $\mathbb{C}$, every non-degenerate quadratic form on an n dimensional $\mathbb{C}$-vector space is equivalent to the sum of the squares of the n components. The corresponding Clifford algebra is $\mathrm{Cl}_n(\mathbb{C})$. Each of $\mathrm{Cl}_{p,q}(\mathbb{R})$ and $\mathrm{Cl}_n(\mathbb{C})$ is isomorphic to A or $A \oplus A$ where A is a matrix ring taking entries in $\mathbb{R}, \mathbb{C}$, or $\mathbb{H}$. Baez's notes on Clifford algebras are a good read [32].

Brauer groups

Wedderburn's theorem (4.2.1) allows us to write any central simple algebra as a matrix algebra, $A \cong M_n(D)$. We can define the Brauer equivalence as $M_m(D) \sim M_n(D')$ for any integers m, n and division algebras D, D' over F. Then the Brauer group $\mathrm{Br}(F)$ is the set of Brauer equivalence classes of central simple algebras over F. More specifically, $\mathrm{Br}(F)$ is an abelian group of Morita equivalence classes ([35],[36]) of central simple algebras over F. Addition is given by the tensor product. Brauer groups can also be defined in terms of Galois cohomology [33], a meaty topic for brave mathematicians.

STBCs from cyclic algebras

In this paper we covered STBCs briefly, showing a generic construction from division algebras. There are more effective ways to construct codes with more desirable properties, most of which are beyond the scope of this paper. One such method is via the use of cyclic algebras. A cyclic algebra is a central simple algebra over a field F containing a strictly maximal subfield E such that E/F is a cyclic field extension. Recommended texts include [28] and [34].

References

[1] S. Moy *An introduction to the theory of field extensions*.
http://www.math.uchicago.edu/~may/VIGRE/VIGRE2009/REUPapers/Moy.pdf

[2] Wikipedia *Zorn's lemma - Wikipedia*.
https://en.wikipedia.org/wiki/Zorn%27s_lemma

[3] H. Fischer *Algebraic closure*.
http://www.cs.bsu.edu/~hfischer/math412/Closure.pdf

[4] K. Voelkel *Division Algebras*.
https://www.konradvoelkel.com/wp-content/uploads/voelkel-2015-01-27-basic-notions-division-algebras.pdf

[5] P. Clark *Non-associative algebras*.
http://alpha.math.uga.edu/~pete/nonassociativealgebra.pdf

[6] S. Pumplün *Involutions on Composition Algebras*.
http://agt2.cie.uma.es/~loos/jordan/archive/unitams/unitams.pdf

[7] K. McCrimmon *Nonassociative algebras with scalar involution*.

[8] A. Hurwitz *Über die Composition der quadratischen Formen von beliebig vielen Variabeln*.

[9] W. Hamilton *On Quaternions; or on a new System of Imaginaries in Algebra*, letter to J. Graves.

[10] K. Martin *Quaternion algebras and quadratic forms*. `http://www2.math.ou.edu/~kmartin/quaint/ch3.pdf`

[11] D. Hilbert *The theory of algebraic number fields*.

[12] F. Frobenius *Über lineare Substitutionen und bilineare Formen*.

[13] K. Conrad *Quaternion Algebras*. `https://kconrad.math.uconn.edu/blurbs/ringtheory/quaternionalg.pdf`

[14] M. Zorn *Alternativekörper und quadratische Systeme*.

[15] J. Radon *Lineare scharen orthogonaler matrizen*.

[16] B. Eckmann *Gruppentheoretischer Beweis des Satzes von Hurwitz–Radon über die Komposition quadratischer Formen*.

[17] H. Lee *Sur le théorème de Hurwitz-Radon pour la composition des formes quadratiques*.

[18] C. Chevalley *The algebraic theory of spinors and Clifford algebras*.

[19] J. Baez *The Octonions*. `https://math.ucr.edu/home/baez/octonions/octonions.html`

[20] T.Y. Lam *A First Course in Noncommutative Rings*.

[21] K. H. Parshall *The contributions of J. H. M. Wedderburn to the theory of algebras: 1900-10*.

[22] L. Dickson *On Finite Algebras*.

[23] G. McNinch *Semisimple algebras and Wedderburn's Theorem*.

[24] T. Bradley *The Tensor Product, Demystified*.
https://www.math3ma.com/blog/the-tensor-product-demystified

[25] P. Gille and T. Szamuely *Central Simple Algebras and Galois Cohomology*.
https://www.math.ens.fr/~benoist/refs/Gille-Szamuely.pdf

[26] A. Hendrickson *Space-Time Block Codes from Cyclic Division Algebras: An Introduction*.
https://people.math.wisc.edu/~boston/hendrickson.pdf

[27] V. Tarokh, N. Seshadri, A.R. Calderbank *Space-time codes for high data rate wireless communication: Performance criterion and code construction*.

[28] S. Pumplün, A. Steele, F. Oggier *MIDO Space-Time Codes from Associative and Nonassociative Cyclic Algebras*.
http://agt2.cie.uma.es/~loos/jordan/archive/itwdraft/itwdraft.pdf

[29] V. Kac *18.745, Fall 2004: Lie Algebras Notes*.
https://web.archive.org/web/20100420004313/http://math.mit.edu/~lesha/745lec/

[30] A. Kirillov *Introduction to Lie Groups and Lie Algebras*.
https://www.math.stonybrook.edu/~kirillov/mat552/liegroups.pdf

[31] Wikipedia *Tensor algebra - Wikipedia*
https://en.wikipedia.org/wiki/Tensor_algebra

[32] J. Baez *Clifford Algebras*
https://math.ucr.edu/home/baez/octonions/node6.html

[33] J.S. Milne *Arithmetic Duality Theorems*
https://www.jmilne.org/math/Books/ADTnot.pdf

[34] S. Pumplün, A. Steele *The nonassociative algebras used to build fast-decodable space-time block codes*.
`https://arxiv.org/pdf/1504.00182.pdf`

[35] K. Morita *Duality for modules and its applications to the theory of rings with minimum condition*.

[36] T.Y. Lam *Lectures on Modules and Rings*.

All web pages last accessed 24/05/2021.