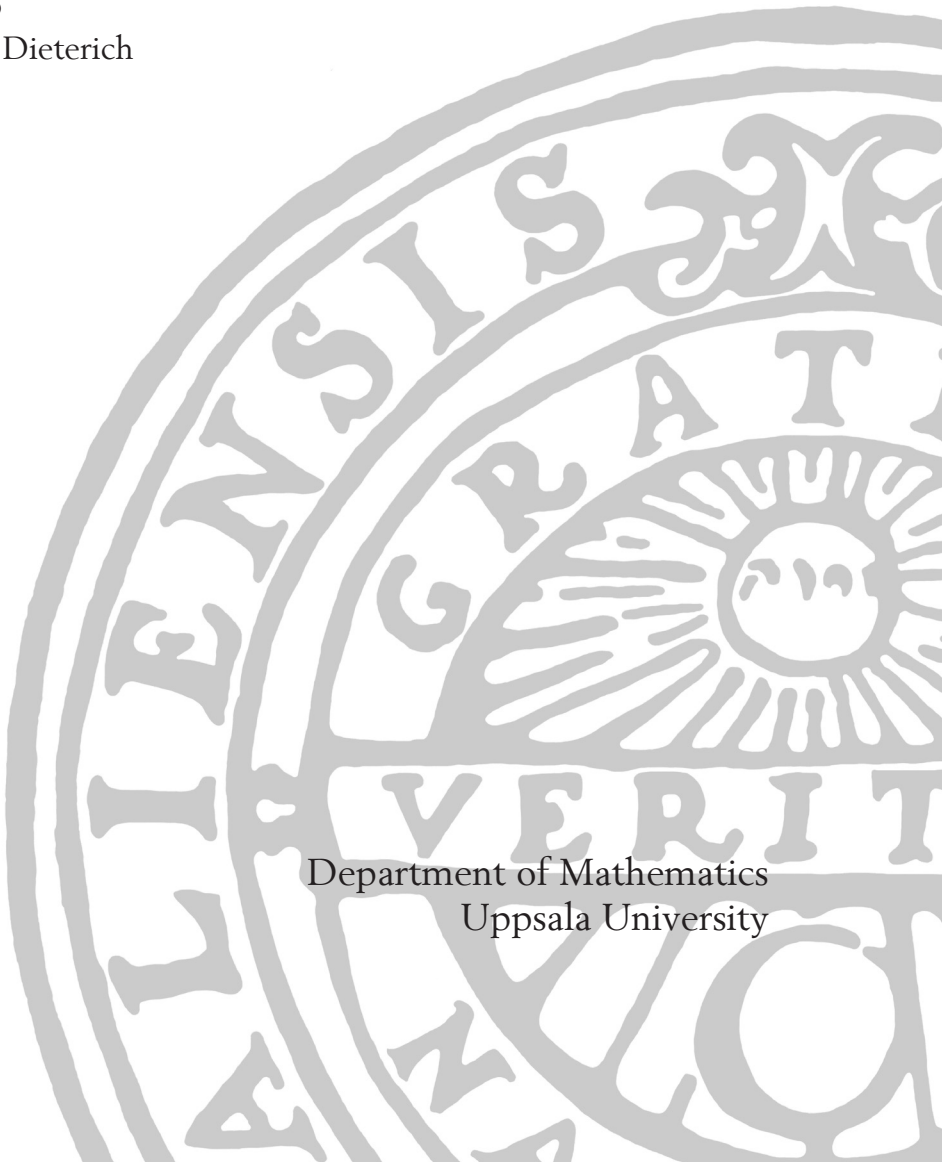
UPPSALA
UNIVERSITET

U.U.D.M. Project Report 2013:11

The (1, 2, 4, 8)-Theorem for Composition Algebras

Rasmus Précenth

Examensarbete i matematik, 15 hp
Handledare och examinator: Ernst Dieterich
Juni 2013



Department of Mathematics
Uppsala University

The $(1, 2, 4, 8)$-Theorem for Composition Algebras

Rasmus Précenth

June 2, 2013

Contents

1 Introduction **3**
1.1 Hurwitz Problem 3
1.2 The (1,2,4,8)-Theorem for Real Division Algebras 3

2 Preliminaries **4**
2.1 Quadratic Forms and Bilinear Forms 4
2.2 Algebras 8

3 Composition Algebras **9**
3.1 Definition and Basic Properties 9
3.2 Purely Imaginary Elements and Conjugation 12
3.3 Associativity Properties 15
3.4 Doubling 19

4 The (1, 2, 4, 8)-Theorem **23**
4.1 Proving Hurwitz Theorem 25

Appendices **28**

Appendix A Hurwitz Problem **28**

1 Introduction

1.1 Hurwitz Problem

The topic of quadratic forms comes up in various parts of algebra. The so-called *Hurwitz Problem*, named after the german mathematician Adolf Hurwitz, asks for what values of n the following identity holds

$$\left(\sum_{i=1}^{n} x_i^2\right)\left(\sum_{i=1}^{n} y_i^2\right) = \sum_{i=1}^{n} z_i^2 \tag{1.1}$$

where all $x_i, y_i \in \mathbb{R}$ and each z_i is a linear combination of $\{x_i y_j \mid 1 < i, j \leq n\}$. The values of n where this is true is for $n = 1, 2, 4, 8$. This statement is called Hurwitz Theorem. This thesis will show that these are in fact the only valid values of n no matter which field we're considering. A theorem proved using the framework of composition algebras by Nathan Jacobson for fields with characteristic not two (Jacobson 1958 [3]). Tonny Albert Springer completed this theorem by proving it for characteristic two as well (Springer 1963 [4]).

The identities for 1 and 2 are relatively simple and are

$$x_1^2 y_1^2 = (x_1 y_1)^2 \tag{1.2}$$

and

$$(x_1^2 + x_2^2)(y_1^2 + y_2^2) = (x_1 y_1 - x_2 y_2)^2 + (x_1 y_2 + x_2 y_1)^2. \tag{1.3}$$

The ones for 4 and 8 are highly non-trivial. They are included in in Appendix A.

1.2 The (1,2,4,8)-Theorem for Real Division Algebras

A division algebra is a non-zero algebra[1] A in which the linear operators L_a and R_a are invertible for each $a \in A \setminus \{0\}$. If the base field is $\mathbb{R}$ then the algebra is called real. Well-known examples of real division algebras are;

- The algebra of real numbers $\mathbb{R}$
- The algebra of complex numbers $\mathbb{C}$
- The algebra of quaternions $\mathbb{H}$
- The algebra of octinions $\mathbb{O}$

These have dimensions 1,2,4 and 8 respectively.

In 1877 the german mathematician Ferdinand Georg Frobenius proved the following theorem for finite-dimensional real division algebras (Frobenius 1878 [2]).

Theorem 1.1 (Theorem of Frobenius)**.** *There are, up to isomorphism, only three associative finite-dimensional real division algebras. They are* $\mathbb{R}$*,* $\mathbb{C}$ *and* $\mathbb{H}$ *with* $\mathbb{H}$ *being the only non-commutative algebra among them.*

[1] See section 2.2 for the definition of an algebra.

Max Zorn, most famous for his lemma considering partial orders, later proved a theorem analogous to the theorem of Frobenius (Zorn 1931 [6]). In 1931 he proved the following.

Theorem 1.2. *There are, up to isomorphism, only four* alternative[2] *finite-dimensional real division algebras. They are* $\mathbb{R}$, $\mathbb{C}$, $\mathbb{H}$ *and* $\mathbb{O}$ *with* $\mathbb{O}$ *being the only non-associative algebra among them.*

This thesis will show that there is a similar theorem for composition algebras, where there is no restriction on the field.

2 Preliminaries

2.1 Quadratic Forms and Bilinear Forms

Definition Given a field k of any characteristic and a vector space V over said field. A *quadratic form* on V is a map $N : V \to k$ satisfying

$$N(\lambda x) = \lambda^2 N(x) \quad \forall \lambda \in k, x \in V \tag{2.1}$$

and that the associated map $\langle\ ,\ \rangle_N : V \times V \to k$ given by

$$\langle x, y \rangle_N = N(x + y) - N(x) - N(y) \tag{2.2}$$

is bilinear. It follows easily that $N(0) = 0$ and that $\langle\ ,\ \rangle_N$ is symmetric. The rest of this thesis will only consider symmetric bilinear forms for this reason. That means that if nothing else is specified we assume that bilinear forms are symmetric. For readability the subscript N will be omitted when it's clear from the context what quadratic form the bilinear form refers to.

Example If $V = \mathbb{R}^{n\times 1}$ then all quadratic forms on V are described by symmetric matrices via the equation

$$N(x) = x^T A x. \tag{2.3}$$

Moreover, A is uniquely determined by N.

Proof. Given a symmetric matrix $A \in \mathbb{R}^{n\times n}$ define the map $N : V \to k$ as in (2.3). The first property holds because

$$N(\lambda x) = (\lambda x)^T A(\lambda x) = \lambda^2 x^T A x = \lambda^2 N(x)$$

and the second since

$$\begin{aligned} \langle x, y \rangle &= N(x + y) - N(x) - N(y) \\ &= (x + y)^T A(x + y) - x^T A x - y^T A y \\ &= x^T A x + x^T A y + y^T A x + y^T A y - x^T A x - y^T A y \\ &= x^T A y + y^T A x \\ &= x^T (2A) y. \end{aligned}$$

[2]See section 2.2 for the definition of alternative.

The last equality holds since A is symmetric.

$$x^T Ay = (x^T Ay)^T = y^T A^T (x^T)^T = y^T Ax$$

This shows that $\langle\ ,\ \rangle$ is bilinear which proves that N is a quadratic form.

The converse is shown using the fact that all symmetric bilinear forms $\langle\ ,\ \rangle : \mathbb{R}^{n\times 1} \times \mathbb{R}^{n\times 1} \to \mathbb{R}$ are given by a symmetric matrix A in the following way

$$\langle x, y\rangle = x^T Ay.$$

The quadratic form is recovered from the bilinear form via the formula $N(x) = \frac{1}{2}\langle x, x\rangle$ since

$$\langle x, x\rangle = N(2x) - 2N(x) = 2N(x) \tag{2.4}$$

and hence $N(x) = \frac{1}{2}x^T Ax = x^T Bx$ where $B = \frac{1}{2}A$ is symmetric.

Finally assume that for some quadratic form N on V we have

$$N(x) = x^T Ax = x^T Bx$$

for $A \neq B$. It follows that $0 = x^T Ax - x^T Bx = x^T(A - B)x$ which implies that $A - B = 0$ and hence $A = B$. □

The equation in (2.4) is true for all quadratic forms on all vector spaces and gives a way to recover the quadratic form from the associated bilinear form provided that char $k \neq 2$.

Proposition 2.1. *If* char $k \neq 2$ *all quadratic forms* N *on* V *can be recovered from the bilinear form* $\langle\ ,\ \rangle_N$ *via the formula*

$$N(x) = \frac{1}{2}\langle x, x\rangle_N. \tag{2.5}$$

However, if char $k = 2$ *we have* $\langle x, x\rangle_N = 0$ *for all* $x \in V$.

Proof.

$$\langle x, x\rangle_N = N(2x) - 2N(x) = 4N(x) - 2N(x) = 2N(x) \tag{2.6}$$

If char $k \neq 2$ we get $N(x) = \frac{1}{2}\langle x, x\rangle_N$ and if char $k = 2$ we have $\langle x, x\rangle_N = 2N(x) = 0$. □

We now move on to properties of symmetric bilinear forms.

Definition Two vectors $x, y \in V$ are said to be *orthogonal* with respect to a bilinear form $\langle\ ,\ \rangle$ on V if $\langle x, y\rangle = 0$. We denote this with $x \perp y$ (or $y \perp x$ since $\langle x, y\rangle = \langle y, x\rangle$). Two subsets $U_1, U_2 \subseteq V$ are said to be orthogonal if all their vectors are orthogonal, i.e

$$U_1 \perp U_2 \Leftrightarrow x \perp y \quad \forall x \in U_1, y \in U_2.$$

The notation $x \perp U$ is short for $\{x\} \perp U$. The *orthogonal complement* $U^\perp$ of a subset $U \subseteq V$ is the set consisting of all vectors orthogonal to all vectors in U, i.e

$$U^\perp = \{x \in V \mid x \perp U\}$$

or equivalently, the largest subset $U^\perp$ of V satisfying $U^\perp \perp U$.

Proposition 2.2. *Given a bilinear form $\langle\ ,\ \rangle : V \times V \to k$ and a subset $U \subseteq V$, then $U^\perp$ is a subspace of V and $U \subseteq (U^\perp)^\perp$.*

Proof. (SS1) $\langle 0, x\rangle = \langle 0 + 0, x\rangle = \langle 0, x\rangle + \langle 0, x\rangle$. This shows that $\langle 0, x\rangle = 0$ for all $x \in U$ so 0 must belong to $U^\perp$.

(SS2) Assume that x and y lie in $U^\perp$. Then $\langle x, u\rangle = \langle y, u\rangle = 0$ for all $u \in U$. It follows that $\langle x + y, u\rangle = \langle x, u\rangle + \langle y, u\rangle = 0 + 0 = 0$ for all $u \in U$. Hence $x + y \in U^\perp$.

(SS3) Assume that $x \in U^\perp$. Then, since $\langle x, u\rangle = 0$ for all $u \in U$, we have $\langle \lambda x, u\rangle = \lambda\langle x, u\rangle = \lambda 0 = 0$ for all $u \in U$ and this shows the final subspace axiom, namely $\lambda x \in U^\perp$.

This proves that $U^\perp$ is a subspace of V. Now assume that $x \in U$, then $x \perp U^\perp$ by definition. But that is also the definition of an element in $(U^\perp)^\perp$, hence $x \in (U^\perp)^\perp$. □

The converse $(U^\perp)^\perp \subseteq U$ is not true for all bilinear forms and subspaces U. For a subspace to behave that way we need a property on both the subspace and the form to make sure it behaves nicely.

Definition A bilinear form $\langle\ ,\ \rangle$ is called *non-degenerate* if the only vector in V orthogonal to all other vectors is 0, i.e $V^\perp = \{0\}$ or equivalently

$$\langle x, y\rangle = 0, \quad \forall y \in V \Longrightarrow x = 0. \tag{2.7}$$

A quadratic form N on V is said to be non-degenerate if its associated bilinear form $\langle\ ,\ \rangle_N$ is non-degenerate.

If the restriction of $\langle\ ,\ \rangle$ to a subspace U of V is non-degenerate we call that subspace *non-singular*. The notations $\langle\ ,\ \rangle|_{U\times U}$ and $\perp_U$ will denote the restricted form and the restricted orthogonality relation, respectively.

Proposition 2.3. *If the form $\langle\ ,\ \rangle$ is non-degenerate and $\langle a, y\rangle = \langle b, y\rangle$ for all $y \in V$ then $a = b$.*

Proof. Using (2.7) we get

$$\begin{array}{lll} & \langle a, y\rangle = \langle b, y\rangle & \forall y \in V \\ \Longleftrightarrow & \langle a - b, y\rangle = 0 & \forall y \in V \\ \Longrightarrow & a - b = 0 & \\ \Longleftrightarrow & a = b & \end{array}$$

□

The last proposition will be very useful later when proving identities in composition algebras. By proving that $\langle x, z\rangle = \langle y, z\rangle$ holds for all z one can show that $x = y$.

One thing useful for proving things for bilinear forms is the following equivalence.

Proposition 2.4. *If $\langle\ ,\ \rangle$ is a bilinear form on a vectorspace V and U is a subspace of V, then the following are equivalent.*

(i) U is non-singular.

(ii) $U \cap U^\perp = \{0\}$.

Proof. $(i) \Rightarrow (ii)$ If U is non-singular, then $\langle\ ,\ \rangle|_{U\times U}$ is non-degenerate. Which is the same as $U^{\perp_U} = \{0\}$. On the other hand $U^{\perp_U} = \{x \in U \mid x \perp U\} = U \cap U^\perp$. So $U \cap U^\perp = \{0\}$.

$(ii) \Rightarrow (i)$ Assume $U \cap U^\perp = \{0\}$. Let $x \in U$ and assume

$$\langle x, y\rangle = 0, \quad \forall y \in U.$$

If we can show $x = 0$, then we are done. The above property is the same as $x \perp U$, so $x \in U^\perp$. That means that $x \in U \cap U^\perp = \{0\}$ so x must be 0. □

Lemma 2.5. *Let V be a finite-dimensional vector space and $\langle\ ,\ \rangle$ a non-degenerate bilinear form on V. Then the linear map $\lambda : V \to V^*$, $v \mapsto \lambda_v = \langle v, \cdot\rangle$ is an isomorphism.*

Proof. Let V be a vector space over k and $\dim V = n$ for some $n \in \mathbb{N}$. Also let $\langle\ ,\ \rangle : V \times V \to k$ be a non-degenerate bilinear form.

Now let $\lambda : V \to V^*$, $v \mapsto \lambda_v = \langle v, \cdot\rangle$. We see that λ is linear since, $\lambda_{v+w} = \langle v + w, \cdot\rangle = \langle v, \cdot\rangle + \langle w, \cdot\rangle = \lambda_v + \lambda_w$ and $\lambda_{cv} = \langle cv, \cdot\rangle = c\langle v, \cdot\rangle = c\lambda_v$ for all $v, w \in V$ and $c \in k$. Now look at the kernel of λ,

$$\begin{aligned}
\ker\lambda &= \{v \in V \mid \lambda_v = 0\} \\
&= \{v \in V \mid \lambda_v(w) = 0,\ \forall w \in V\} \\
&= \{v \in V \mid \langle v, w\rangle = 0,\ \forall w \in V\} \\
&= \{0\}.
\end{aligned}$$

So λ is injective. It is also surjective since $\dim V^* = \dim V$ holds when V is finite-dimensional. Hence λ is an isomorphism. □

Theorem 2.6. *If V is a vector space over k, $\langle\ ,\ \rangle$ a bilinear form on V and $U \subseteq V$ a finite-dimensional non-singular subspace, then*

$$V = U \oplus U^\perp.$$

If moreover $\langle\ ,\ \rangle$ is non-degenerate, then $U^\perp$ is non-singular.

Proof. Assume that $U \subseteq V$ is non-singular and that $\dim U < \infty$. Then $U \cap U^\perp = \{0\}$ from Proposition 2.4 which makes the sum $U \oplus U^\perp$ direct. It remains to show that $U + U^\perp = V$. Let $w \in V$. Since U is finite dimensional and the restriction $\langle\ ,\ \rangle|_{U\times U}$ is non-degenerate then $\mu : U \to U^*$, $v \mapsto \mu_v = \langle v, \cdot\rangle|_{U\times U}$ is an isomorphism by Lemma 2.5. Let $\lambda : V \to V^*, v \mapsto \lambda_v = \langle v, \cdot\rangle$. The form $\lambda_w|_U$ belongs to U^* so there must be a vector $u \in U$ such that $\mu_u = \lambda_w|_U$ which is the same as

$$\langle u, v\rangle = \langle w, v\rangle, \quad \forall v \in U.$$

Subtracting by $\langle w, v\rangle$ yields

$$\langle u - w, v\rangle = 0, \quad \forall v \in U.$$

Let $u' = u - w$ then $u' = u - w \perp U$ so $u' \in U^\perp$ and

$$w = u + u'$$

which concludes the proof of the first statement.

Now assume that $\langle\ ,\ \rangle$ is non-degenerate, that $U^\perp$ is singular and that $x \in U^\perp \cap (U^\perp)^\perp$. If we can prove that $x = 0$ then we are done. Let $y \in V$. Then we can write $y = u + u'$ where $u \in U$ and $u' \in U^\perp$ since $V = U \oplus U^\perp$ by the first statement of this theorem. By our assumption $x \in U^\perp$ and $x \in (U^\perp)^\perp$ so $\langle x, u\rangle = 0$ and $\langle x, u'\rangle = 0$ respectively. Adding these we get $\langle x, u\rangle + \langle x, u'\rangle = \langle x, u + u'\rangle = 0$. This means that we have $\langle x, y\rangle = 0$ for all $y \in V$ which implies that $x = 0$ since $\langle\ ,\ \rangle$ is non-degenerate. □

Corollary 2.7. *If $\langle\ ,\ \rangle : V \times V \to k$ is a bilinear form on a vector space V and $U \subseteq V$ a finite-dimensional non-singular subspace, then*

$$\dim V = \dim U + \dim U^\perp \tag{2.8}$$

Proof. Follows from Theorem 2.6. □

Corollary 2.8. *If $\langle\ ,\ \rangle : V \times V \to k$ is a non-degenerate bilinear form and U a finite-dimensional non-singular subspace of V, then*

$$(U^\perp)^\perp = U \tag{2.9}$$

Proof. We already know from Proposition 2.2 that $U \subseteq (U^\perp)^\perp$ so we only need to prove the inclusion $(U^\perp)^\perp \subseteq U$. Let $x \in (U^\perp)^\perp$. From Theorem 2.6 we know that $V = U \oplus U^\perp$ so we can write $x = u + u'$ where $u \in U$ and $u' \in U^\perp$. But $u \in (U^\perp)^\perp$ since $u \in U$ which means that $x - u \in (U^\perp)^\perp$. On the other hand $x - u = u' \in U^\perp$ so $x - u \in U^\perp \cap (U^\perp)^\perp$ and hence $x - u = 0$. Moving the u to the other side gives $x = u$ so $x \in U$. □

2.2 Algebras

Definition An algebra A over a field k is a vector space over k together with a bilinear multiplication $A \times A \to A$, $(x, y) \mapsto xy$. It follows that the maps $L_a : A \to k, x \mapsto ax$ and $R_a : A \to k, x \mapsto xa$ are linear for all $a \in A$.

Reminder A multiplication $A \times A \to A$, $(x, y) \mapsto xy$ is bilinear if the following axioms are satisfied.

1. $x(y + z) = xy + xz$ for all $x, y, z \in A$.
2. $(x + y)z = xz + yz$ for all $x, y, z \in A$.
3. $\lambda(xy) = (\lambda x)y = x(\lambda y)$ for all $x, y \in A$ and $\lambda \in k$.

They are called *right additivity*, *left additivity* and *homogenity*, respectively.

Definition The dimension of an algebra A is the dimension of its underlying vector space.

Here follows a list of some various types of algebras

Division Algebra A non-zero algebra in which the maps L_a and R_a are bijective for all $a \neq 0$. Division by non-zero elements is possible in division algebras, hence its name. A commutative and associative division algebra with unity forms a field together with vector addition and multiplication.

Quadratic Algebra An algebra with unity e in which the square of an element x is contained in the span of e and x, i.e

$$x^2 = \alpha e + \beta x \qquad \text{for some } \alpha, \beta \in k \tag{2.10}$$

Alternative Algebra An algebra A is called *alternative* if for all $x, y \in A$

$$\begin{aligned} x(xy) &= (xx)y \\ x(yy) &= (xy)y \\ x(yx) &= (xy)x. \end{aligned}$$

In other words, the subalgebra generated by x and y is associative.

3 Composition Algebras

In this section we will speak of an algebraic objects known as composition algebras. These were introduced by Nathan Jacobson as a means to prove Hurwitz Theorem for any field of characteristic not two.

The way this is presented in follows closely to that in [5].

3.1 Definition and Basic Properties

Definition A *composition algebra* C over a field k is a pair (C, N) where C is a non-zero algebra with identity e and $N : C \to k$ a non-degenerate quadratic form that satisfies

$$N(xy) = N(x)N(y) \quad \forall x, y \in C. \tag{3.1}$$

The equation (3.1) is what relates the composition algebras to the quadratic forms.

Composition algebras are sometimes called normed algebras. The quadratic form N is called the *norm* and the associated bilinear form $\langle\ ,\ \rangle_N$ is called the *inner product*. Note that it is not neccesarily an inner product in the usual sense, it doesn't have to be positive definite.

Definition A *composition subalgebra* D of a composition algebra C is a non-singular subspace D of C that is closed under multiplication and contains the identity e.

Examples The set of real numbers $\mathbb{R}$ and the set of complex numbers $\mathbb{C}$ are real composition algebras with the quadratic forms $N_{\mathbb{R}}(x) = x^2$ and $N_{\mathbb{C}}(x + iy) = x^2 + y^2$ respectively.

A slightly more advanced example is the algebra $\mathbb{Z}_2 \oplus \mathbb{Z}_2$ over $\mathbb{Z}_2$ with multiplication $(x_1, y_1)(x_2, y_2) = (x_1x_2, y_1y_2)$, quadratic form $N((x, y)) = xy$ and identity $e = (1, 1)$.

Proposition 3.1. *Let C be any composition algebra. Then the identity e satisfies*

$$N(e) = 1. \tag{3.2}$$

Proof.

$$N(e) = N(ee) = N(e)N(e) \Longrightarrow N(e) = 1 \text{ or } N(e) = 0$$

Assume that $N(e) = 0$ then $N(x) = N(x)N(e) = 0$ for all $x \in C$ so

$$\langle e, x \rangle = 0 \qquad \forall x \in C$$

which, since $\langle\ ,\ \rangle$ is non-degenerate, implies that $e = 0$. But a composition algebra is by definition non-zero so we have a contradiction. Hence $N(e) = 1$. □

Definition An element x of C is said to have an inverse if there is some $y \in C$ such that $xy = yx = e$.

Remark Nothing is yet said about the uniqueness of inverses. Until the uniqueness is proven we have to include the possibility of mulitple inverses.

Proposition 3.2. *If x is an element of a composition algebra and x has an inverse x^{-1} then*

$$N(x^{-1}) = N(x)^{-1}.$$

In particular, $N(x)$ and $N(x^{-1})$ are both non-zero.

Proof. Assume x is an invertible element in a composition algebra C. Then the following holds

$$1 = N(e) = N(xx^{-1}) = N(x)N(x^{-1}).$$

Hence, $N(x^{-1}) = N(x)^{-1}$. □

We will see later that the condition $N(x) \neq 0$ is in fact sufficient for x to have an inverse and that the inverse is, in fact, unique.

We now continue with some more technical identities that will prove very useful.

Proposition 3.3. *In every composition algebra C the following identities hold for all $x, x_1, x_2, y, y_1, y_2 \in C$*

$$\langle x_1 y, x_2 y \rangle = \langle x_1, x_2 \rangle N(y) \tag{3.3}$$

$$\langle xy_1, xy_2 \rangle = N(x)\langle y_1, y_2 \rangle \tag{3.4}$$

$$\langle x_1 y_1, x_2 y_2 \rangle + \langle x_1 y_2, x_2 y_1 \rangle = \langle x_1, x_2 \rangle \langle y_1, y_2 \rangle. \tag{3.5}$$

Proof. Regarding (3.3) we have for all $x_1, x_2, y \in C$

$$\begin{aligned}
\langle x_1 y, x_2 y \rangle &= N(x_1 y + x_2 y) - N(x_1 y) - N(x_2 y) \\
&= N((x_1 + x_2)y) - N(x_1 y) - N(x_2 y) \\
&= N(x_1 + x_2)N(y) - N(x_1)N(y) - N(x_2)N(y) \\
&= (N(x_1 + x_2) - N(x_1) - N(x_2))N(y) \\
&= \langle x_1, x_2 \rangle N(y).
\end{aligned}$$

The identity (3.4) is proved in the same way as (3.3). The last one is proved by using (3.3). On one hand we have

$$\begin{aligned}\langle x_1(y_1+y_2), x_2(y_1+y_2)\rangle &= \langle x_1y_1 + x_1y_2, x_2y_1 + x_2y_2\rangle \\ &= \langle x_1y_1, x_2y_1 + x_2y_2\rangle + \langle x_1y_2, x_2y_1 + x_2y_2\rangle \\ &= \langle x_1y_1, x_2y_1\rangle + \langle x_1y_1, x_2y_2\rangle + \langle x_1y_2, x_2y_1\rangle + \\ &\quad \langle x_1y_2, x_2y_2\rangle \\ &= \langle x_1y_1, x_2y_2\rangle + \langle x_1y_2, x_2y_1\rangle + \langle x_1, x_2\rangle N(y_1) + \\ &\quad \langle x_1, x_2\rangle N(y_2)\end{aligned}$$

and on the other we have

$$\begin{aligned}\langle x_1, x_2\rangle N(y_1+y_2) &= \langle x_1, x_2\rangle(\langle y_1, y_2\rangle + N(y_1) + N(y_2)) \\ &= \langle x_1, x_2\rangle\langle y_1, y_2\rangle + \langle x_1, x_2\rangle(N(y_1) + N(y_2)).\end{aligned}$$

By (3.3), the starting terms of both chains coincide. Subtracting $\langle x_1, x_2\rangle(N(y_1)+N(y_2))$ from the end terms we obtain (3.5). □

Corollary 3.4. *Let C be a composition algebra and let $x, y \in C$ with $\langle x, y\rangle = 0$. Then for all $x_1, y_1 \in C$,*

$$\langle x_1x, y_1y\rangle = -\langle x_1y, y_1x\rangle. \tag{3.6}$$

Proof. Follows directly from (3.5). □

Proposition 3.5. *Let C be a composition algebra and x an element in C. Then the following identity holds*

$$x^2 - \langle x, e\rangle x + N(x)e = 0. \tag{3.7}$$

Proof. Let $x \in C$. Then create the inner product of the left hand side of (3.7) with an arbitrary y.

$$\begin{aligned}\langle x^2 - \langle x, e\rangle x + N(x)e, y\rangle &= \langle x^2, y\rangle - \langle x, e\rangle\langle x, y\rangle + N(x)\langle e, y\rangle \\ &= \langle x^2, y\rangle - \langle x, e\rangle\langle x, y\rangle + \langle xe, xy\rangle \\ &= 0\end{aligned}$$

The equalities are valid since $N(x)\langle e, y\rangle = \langle xe, xy\rangle$ by (3.4) and $\langle x^2, y\rangle + \langle xe, xy\rangle = \langle x, e\rangle\langle x, y\rangle$ by (3.5). Using Proposition 2.3 we obtain (3.7). □

Corollary 3.6. *If (C, M) and (C, N) are composition algebras, then $M = N$.*

Proof. For every $x \in C$ we have by (3.7)

$$\begin{aligned}x^2 &= \langle x, e\rangle_M x - M(x)e \\ x^2 &= \langle x, e\rangle_N x - N(x)e.\end{aligned}$$

So

$$\langle x, e\rangle_M x - M(x)e = \langle x, e\rangle_N x - N(x)e. \tag{3.8}$$

Now we have two cases, e and x are either linearly independent or linearly dependent.

First case If e and x are linearly independent then $-M(x) = -N(x)$ by (3.8) so $M(x) = N(x)$.

Second case If e and x are linearly dependent then $x = \lambda e$ for some scalar λ. Thus we obtain

$$M(x) = \lambda^2 M(e) = \lambda^2 = \lambda^2 N(e) = N(x).$$

Both cases lead to $M(x) = N(x)$ which concludes the proof. □

The identity (3.7) can be interpreted (weaker) as follows.

Corollary 3.7. *Every composition algebra is a quadratic algebra.*

Proof. Let C be a composition algebra. Then for all $x \in C$, $x^2 = \langle x, e\rangle x - N(x)e$ by (3.7). So $x^2 \in \text{span}\{e, x\}$. □

This gives us some geometric understanding of the multiplication in a composition algebra.

3.2 Purely Imaginary Elements and Conjugation

We will now generalize the notion of imaginary complex numbers that shows up in many parts of mathematics.

Definition The set of all purely imaginary elements of a composition algebra C over k is the set

$$\text{Im } C = \{x \in C \mid x^2 \in ke,\ x \notin ke \setminus \{0\}\}. \tag{3.9}$$

Proposition 3.8. *Let C be a composition algebra over a field k with* char $k \neq 2$. *Then* Im C *is a non-singular subspace of C,* Im $C = (ke)^\perp$ *and*

$$C = \text{Im } C \oplus ke.$$

Proof. To prove Proposition 3.8 it is enough to show that ke is a non-singular subspace and that Im $C = (ke)^\perp$. The rest will follow from Theorem 2.6 since $\dim ke = 1$.

Assume that ke is singular. Then $x \in (ke)^\perp \cap ke$ for some non-zero $x \in C$. So $x = \lambda e, \lambda \neq 0$ and $\langle x, e\rangle = 0$. But this is a contradiction since $0 = \langle \lambda e, e\rangle = \lambda\langle e, e\rangle = \lambda(N(2e) - 2N(e)) = 2\lambda$ when char $k \neq 2$. Hence ke is non-singular.

To show Im $C = (ke)^\perp$ we first show Im $C \subseteq (ke)^\perp$. Let $x \in$ Im $(C) \setminus \{0\}$ then e and x are linearly independent and $x^2 = \lambda e$ for some λ. The identity (3.7) on the other hand gives us $x^2 = \langle x, e\rangle x - N(x)e$. Combining these two we get $N(x) = -\lambda$ and $\langle x, e\rangle = 0$. So $x \in (ke)^\perp$. Now assume that $x \in (ke)^\perp$. Then $\langle x, e\rangle = 0$ and from (3.7) we have, once again, $x^2 = \langle x, e\rangle x - N(x)e = -N(x)e$. Also, since $x \perp ke$, we have $x \notin ke \setminus \{0\}$ because ke is non-singular. Hence $x \in$ Im C. That concludes the proof that Im $C = (ke)^\perp$.

By Theorem 2.6, Im C is a non-singular subspace of C and $C =$ Im $C \oplus ke$, a direct sum decomposition. □

The above proposition has a generalization called Frobenius Lemma ([1, p. 227]) that states that all real quadratic algebras A can be written as $A = \mathbb{R}e \oplus \text{Im } A$. That proof can easily be extended to all quadratic algebras over a field with characteristic not equal to two.

Hopefully, Proposition 3.8 gives the reader some more understanding of what Im C looks like. For example, Im $\mathbb{R} = \{0\}$, $\mathbb{R} = \mathbb{R} \oplus \{0\}$ and Im $\mathbb{C} = \mathbb{R}i$, $\mathbb{C} = \mathbb{R}i \oplus \mathbb{R}$. In $\mathbb{Z}_2 \oplus \mathbb{Z}_2$, however, we have Im $(\mathbb{Z}_2 \oplus \mathbb{Z}_2) = \{0\}$ and $\mathbb{Z}_2 e = \{0, (1,1)\}$. It follows that $\mathbb{Z}_2 \oplus \mathbb{Z}_2 \neq \text{Im } (\mathbb{Z}_2 \oplus \mathbb{Z}_2) \oplus \mathbb{Z}_2 e$.

Definition Let C be a composition k-algebra. The conjugation map $^- : C \to C$, $x \mapsto \bar{x}$ is defined by

$$\bar{x} = \langle x, e \rangle e - x. \tag{3.10}$$

This can also be seen as $-s(x)$ where $s(x)$ is the reflection of x in $(ke)^\perp$ (or Im C if char $k \neq 2$). For $C = \mathbb{C}$ the definition coincides with the normal understanding of conjugates. In $\mathbb{R}$ we have $\bar{x} = x$ and in $\mathbb{C}$ we have $\overline{x + iy} = x - iy$. Computing the conjugate for each element in $\mathbb{Z}_2 \oplus \mathbb{Z}_2$ one gets $\bar{0} = 0$, $\bar{e} = e$, $\overline{(0,1)} = (1,0)$ and $\overline{(1,0)} = (0,1)$.

Many of the usual properties of conjugates hold with the above definition of conjugation for every composition algebra.

Proposition 3.9. *Let C be a composition algebra. Then conjugation is a linear map and $\bar{\bar{x}} = x$.*

Proof. The proof that conjugation is linear follows from the definition since $\langle\ ,\ \rangle$ is a bilinear form;

$$\overline{x + y} = \langle x + y, e \rangle e - (x + y) = \langle x, e \rangle e - x + \langle y, e \rangle e - y = \bar{x} + \bar{y},$$

and similarily for multiplication with scalars. The last part follows from the computation

$$\begin{aligned} \bar{\bar{x}} &= \langle \bar{x}, e \rangle e - \bar{x} \\ &= \langle \langle x, e \rangle e - x, e \rangle e - \langle x, e \rangle e + x \\ &= \langle x, e \rangle \langle e, e \rangle e - \langle x, e \rangle e - \langle x, e \rangle e + x \\ &= 2\langle x, e \rangle e - 2\langle x, e \rangle e + x \\ &= x. \end{aligned}$$

since $\langle e, e \rangle = 2N(e) = 2$ by Proposition 2.1 and 3.1. □

This is a good start. But one might ask what other properties hold. For example, in $\mathbb{C}$ (with the ordinary conjugate) we have $x\bar{x} = |x|^2$, $\overline{xy} = \bar{x}\bar{y}$ and $|x| = |\bar{x}|$. It turns out that these also hold in general composition algebras, with slight modifications.

Proposition 3.10. *In every composition algebra C the following holds for all $x, y \in C$.*

(i) $x\bar{x} = \bar{x}x = N(x)e$

(ii) $\overline{xy} = \bar{y}\bar{x}$

(iii) $N(\bar{x}) = N(x)$

(iv) $\langle \bar{x}, \bar{y} \rangle = \langle x, y \rangle$

Proof. (i) Follows from (3.7) in the following way

$$\begin{aligned} N(x)e &= \langle x, e\rangle x - x^2 \\ &= (\langle x, e\rangle e - x)x \\ &= \bar{x}x. \end{aligned}$$

The other way round, $N(x)e = x\bar{x}$ is done in the same way. Remember that $\lambda x = (\lambda x)e = x(\lambda e)$ for all scalars λ.

(ii) We first observe that

$$xy = \langle y, e\rangle x + \langle x, e\rangle y - \langle x, y\rangle e - yx \tag{3.11}$$

since

$$\begin{aligned} xy &= (x+y)^2 - x^2 - y^2 - yx \\ &= \langle x+y, e\rangle(x+y) - N(x+y)e - \langle x, e\rangle x + \\ &\quad N(x)e - \langle y, e\rangle y + N(y)e - yx \\ &= \langle x, e\rangle y + \langle y, e\rangle x - (N(x+y) - N(x) - N(y))e - yx \\ &= \langle y, e\rangle x + \langle x, e\rangle y - \langle x, y\rangle e - yx \end{aligned}$$

by (3.7). By the definition of conjugates, (3.11) and (3.5) we have

$$\begin{aligned} \bar{y}\bar{x} &= (\langle y, e\rangle e - y)(\langle x, e\rangle e - x) \\ &= \langle x, e\rangle\langle y, e\rangle e - \langle x, e\rangle y - \langle y, e\rangle x + yx \\ &= \langle x, e\rangle\langle y, e\rangle e - \langle x, y\rangle e - xy \\ &= \langle xy, e\rangle e - xy \\ &= \overline{xy}. \end{aligned}$$

(iii) From the previous proposition and part (i);

$$N(\bar{x})e = \bar{\bar{x}}\bar{x} = x\bar{x} = N(x)e$$

so $N(\bar{x}) = N(x)$.

(iv) Using part (iii) and the linearity of conjugation

$$\begin{aligned} \langle \bar{x}, \bar{y} \rangle &= N(\bar{x} + \bar{y}) - N(\bar{x}) - N(\bar{y}) \\ &= N(\overline{x+y}) - N(\bar{x}) - N(\bar{y}) \\ &= N(x+y) - N(x) - N(y) \\ &= \langle x, y \rangle. \end{aligned}$$

□

We saw earlier in Proposition 3.2 that if x has an inverse x^{-1} then $N(x^{-1}) = N(x)^{-1}$. We will now show something stronger using the newly established properties of conjugation.

Proposition 3.11. *In every composition algebra C and for every $x \in C$ the following are equivalent*

(i) x has an inverse.

(ii) $N(x) \neq 0$.

In that case, $N(x)^{-1}\bar{x}$ is inverse to x.

Proof. $(i) \Rightarrow (ii)$ See Proposition 3.2.

$(ii) \Rightarrow (i)$ Assume $N(x) \neq 0$. Let $y = N(x)^{-1}\bar{x}$, then

$$xy = x(N(x)^{-1}\bar{x}) = N(x)^{-1}(x\bar{x}) = N(x)^{-1}N(x)e = e$$

The equality $yx = e$ is similar which concludes that $xy = yx = e$.

□

3.3 Associativity Properties

So far we have not established any facts about associativity in composition algebras. It turns out that they need not be associative but they satisfy some other, although weaker, properties. Unfortunately, these properties are not obvious and need some technical propositions first.

Proposition 3.12. *Let C be a composition algebra and let $x, y, z \in C$, then*

$$\langle xy, z\rangle = \langle y, \bar{x}z\rangle \tag{3.12}$$
$$\langle xy, z\rangle = \langle x, z\bar{y}\rangle \tag{3.13}$$
$$\langle xy, \bar{z}\rangle = \langle yz, \bar{x}\rangle \tag{3.14}$$

Proof.

$$\begin{aligned}
\langle y, \bar{x}z\rangle &= \langle y, (\langle x, e\rangle e - x)z\rangle \\
&= \langle y, \langle x, e\rangle z\rangle - \langle y, xz\rangle \\
&= \langle x, e\rangle\langle y, z\rangle - \langle y, xz\rangle \\
&= \langle xy, z\rangle + \langle xz, y\rangle - \langle y, xz\rangle \\
&= \langle xy, z\rangle
\end{aligned}$$

The only non-trivial step follows from (3.5);

$$\langle x, e\rangle\langle y, z\rangle = \langle xy, z\rangle + \langle xz, y\rangle$$

To prove (3.13) and (3.14) we use part (ii) and (iv) of Proposition 3.10 and (3.12).

$$\begin{aligned}
\langle xy, z\rangle &= \langle y, \bar{x}z\rangle \\
&= \langle \bar{y}, \bar{z}x\rangle \\
&= \langle z\bar{y}, x\rangle \\
&= \langle x, z\bar{y}\rangle
\end{aligned}$$

proves (3.13) and

$$\begin{aligned}\langle xy, \bar{z}\rangle &= \langle \bar{z}, xy\rangle \\ &= \langle z, \overline{xy}\rangle \\ &= \langle z, \bar{y}\bar{x}\rangle \\ &= \langle yz, \bar{x}\rangle\end{aligned}$$

proves (3.14) □

Remark Recall that the adjoint of a linear operator f on an inner product space V is the unique linear operator f^* on V such that $\langle f(x), y\rangle = \langle x, f^*(y)\rangle$ for all $x, y \in V$. Using that definition we can define the notion of adjoints in composition algebras, which gives us a nice way of interpreting (3.12) and (3.13);

$$\begin{aligned}L_x^* &= L_{\bar{x}} \\ R_y^* &= R_{\bar{y}}\end{aligned}$$

since $\langle L_x(y), z\rangle = \langle xy, z\rangle = \langle y, \bar{x}z\rangle = \langle y, L_{\bar{x}}(z)\rangle$ and similarily for R_y.

We can now prove a slight generalization to the identity $\bar{x}x = N(x)e$.

Proposition 3.13. *If C is a composition algebra and $x, y \in C$ then the following holds*

$$x(\bar{x}y) = N(x)y \tag{3.15}$$
$$(x\bar{y})y = N(y)x \tag{3.16}$$

Proof. Using Proposition 2.3 we can show that if $\langle x(\bar{x}y), z\rangle = \langle N(x)y, z\rangle$ for all $z \in C$ then (3.15) will hold. That is done using (3.12), (3.4) and part (iii) of Proposition 3.10 in the following way:

$$\begin{aligned}\langle x(\bar{x}y), z\rangle &= \langle \bar{x}y, \bar{x}z\rangle \\ &= N(\bar{x})\langle y, z\rangle \\ &= N(x)\langle y, z\rangle \\ &= \langle N(x)y, z\rangle.\end{aligned}$$

Now using part (ii) of Proposition 3.10 and conjugating both sides in (3.15) we get

$$\overline{x(\bar{x}y)} = (\overline{\bar{x}y})\bar{x} = (\bar{y}x)\bar{x}$$

and

$$\overline{N(x)y} = N(x)\bar{y}.$$

Combining the above expressions proves (3.16). □

We are now ready to state our first associativity related result.

Corollary 3.14. *For all x and y in a composition algebra C the following holds*

$$x(\bar{x}y) = (x\bar{x})y \tag{3.17}$$
$$x(\bar{y}y) = (x\bar{y})y \tag{3.18}$$

Proof. Follows immediately from (3.15), (3.16) and Proposition 3.10 (i). □

Corollary 3.15. *Let C be a composition algebra. Then every element $x \in C$ that satisfies $N(x) \neq 0$ has a unique inverse $N(x)^{-1}\bar{x}$.*

Proof. Let $x \in C$ and $N(x) \neq 0$. Then x has an inverse $y = N(x)^{-1}\bar{x}$ by Proposition 3.11. Assume that there is another element z such that $xz = zx = e$. Then

$$\begin{aligned} y &= y(xz) \\ &= N(x)^{-1}\bar{x}(xz) \\ &= N(x)^{-1}(\bar{x}x)z \\ &= N(x)^{-1}N(x)z \\ &= z \end{aligned}$$

by Corollary 3.14. □

Proposition 3.16. *In every composition algebra C the* Moufang *identities hold for all $x, y, a \in C$.*

$$(ax)(ya) = a((xy)a) \tag{3.19}$$
$$a(x(ay)) = (a(xa))y \tag{3.20}$$
$$x(a(ya)) = ((xa)y)a \tag{3.21}$$

Proof. Once again we use Proposition 2.3 to show an identity. The reader should at this point be familiar with the tools used so we won't write every identity and proposition used, which will increase readability. We will point out, however that (3.5) is used twice.

$$\begin{aligned} \langle (ax)(ya), z\rangle &= \langle ya, (\overline{a}\overline{x})z\rangle \\ &= \langle ya, (\bar{x}\bar{a})z\rangle \\ &= \langle y, \bar{x}\bar{a}\rangle\langle a, z\rangle - \langle yz, (\bar{x}\bar{a})a\rangle \\ &= \langle xy, \bar{a}\rangle\langle a, z\rangle - \langle yz, N(a)\bar{x}\rangle \\ &= \langle xy, \bar{a}\rangle\langle a, z\rangle - N(a)\langle yz, \bar{x}\rangle \\ &= \langle xy, \bar{a}\rangle\langle a, z\rangle - N(a)\langle xy, \bar{z}\rangle \\ &= \langle xy, \bar{a}\rangle\langle a, z\rangle - N(a)\langle (xy)z, e\rangle \\ &= \langle xy, \bar{a}\rangle\langle a, z\rangle - \langle (xy)z, \bar{a}a\rangle \\ &= \langle (xy)a, \bar{a}z\rangle \\ &= \langle a((xy)a), z\rangle \end{aligned}$$

This proves (3.19). To prove (3.20) we use a similar chain of equalities where

we use (3.19) once.

$$\begin{aligned}
\langle a(x(ay)), z\rangle &= \langle x(ay), \bar{a}z\rangle \\
&= \langle x, (\bar{a}z)(\overline{ay})\rangle \\
&= \langle \bar{x}, \overline{(\bar{a}z)(\overline{ay})}\rangle \\
&= \langle \bar{x}, (ay)(\bar{z}a)\rangle \\
&= \langle \bar{x}, a((y\bar{z})a)\rangle \\
&= \langle x, \overline{a((y\bar{z})a)}\rangle \\
&= \langle x, (\overline{(y\bar{z})a})\bar{a}\rangle \\
&= \langle x, (\bar{a}(z\bar{y}))\bar{a}\rangle \\
&= \langle xa, \bar{a}(z\bar{y})\rangle \\
&= \langle a(xa), z\bar{y}\rangle \\
&= \langle (a(xa))y, z\rangle
\end{aligned}$$

To prove the last equality we start with the second and conjugate it. The left hand side becomes

$$\overline{a(x(ay))} = (\overline{x(ay)})\bar{a} = ((\bar{y}\bar{a})\bar{x})\bar{a}$$

and the right hand side, with the help of (3.19) since $(ax)a = (ax)(ea) = a((xe)a) = a(xa)$,

$$\overline{(a(xa))y} = \bar{y}(\overline{a(xa)}) = \bar{y}((\bar{a}\bar{x})\bar{a}) = \bar{y}(\bar{a}(\bar{x}\bar{a})).$$

Substituting $\bar{y}$, $\bar{a}$ and $\bar{x}$ for x', a' and y' respectively (for readability) and combining the above equalities we get

$$x'(a'(y'a')) = ((x'a')y')a'$$

which proves (3.21). □

Proposition 3.17. *Let C be a composition algebra. Then C is alternative.*

Proof. To prove that C is alternative we have to prove the following equalities

$$\begin{aligned}
x(yx) &= (xy)x && (3.22)\\
(xx)y &= x(xy) && (3.23)\\
(xy)y &= x(yy). && (3.24)
\end{aligned}$$

The first follows from (3.19)

$$(xy)x = (xy)(ex) = x((ye)x) = x(yx).$$

The second follows if we start with (3.17) and expand both sides, starting with the left

$$\begin{aligned}
x(\bar{x}y) &= x((\langle x, e\rangle e - x)y) \\
&= x(\langle x, e\rangle y - xy) \\
&= \langle x, e\rangle xy - x(xy).
\end{aligned}$$

The right hand side is

$$\begin{aligned}(x\bar{x})y &= (x(\langle x,e\rangle e - x))y \\ &= (\langle x,e\rangle x - xx)y \\ &= \langle x,e\rangle xy - (xx)y.\end{aligned}$$

Combining the two chains proves (3.23).

Proving (3.24) is similar. □

Summarizing everything done so far we get the following theorem.

Theorem 3.18. *Let C be a composition algebra. Then C is a quadratic, alternative algebra that satisfies the Moufang identities.*

Even if this says something about the elements it still doesn't say anything about the structure of the algebra. We are still missing one vital part; a construction method called *doubling* that will prove very useful.

3.4 Doubling

Lemma 3.19. *Let C be a composition algebra. If $D \subsetneq C$ is a finite-dimensional proper non-singular subspace of C, then there is an element $a \in D^\perp \setminus \{0\}$ such that $N(a) \neq 0$.*

Proof. Assume that $N(x) = 0$ for all $x \in D^\perp$. Theorem 2.6 tells us that $C = D \oplus D^\perp$ where $D^\perp$ is non-singular. We also know that $D \neq C$ so $D^\perp \neq \{0\}$

Let a be any non-zero element in $D^\perp$. Then,

$$\langle a, x\rangle = N(a+x) - N(a) - N(x) = 0 - 0 - 0 = 0, \quad \forall x \in D^\perp$$

and since $D^\perp$ is non-singular, $a = 0$ which is a contradiction. □

If $D_1 \subsetneq C$ is a finite-dimensional proper composition subalgebra, then the lemma makes sure that we can create the following subalgebra of C

$$D_2 = D_1 \oplus D_1 a$$

where D_1 is a proper composition subalgebra of C and a is a non-zero element in $D^\perp$ such that $N(a) \neq 0$.

Proposition 3.20 (The doubling construction)**.** *If D_1 is a finite-dimensional proper composition subalgebra of a composition algebra C, $a \in D^\perp \setminus \{0\}$ and $N(a) \neq 0$ then the subspace*

$$D_2 = D_1 + D_1 a \tag{3.25}$$

of C is a composition subalgebra of C with $\dim D_2 = 2 \dim D_1$ and the sum being a direct sum decomposition of D_2. Multiplication in D_2 then is

$$(x + ya)(z + wa) = (xz - N(a)\overline{w}y) + (wx + y\bar{z})a. \tag{3.26}$$

Proof. There is quite a lot of information in this proposition but the proof essentially boils down to the following two parts.

(*i*) By showing $D_1 a \subseteq D_1^\perp$ we will show that the sum is direct.

(*ii*) By showing (3.26) we will show that D_2 is closed under multiplication and non-singular.

Proof of (i). We know that $a \in D_1^\perp$ so we need to show that $xa \perp D_1$ for all $x \in D_1$. Therefore, let $x \in D_1$ and look at the inner product $\langle xa, y\rangle$ where $y \in D_1$. Identity (3.12) gives us $\langle xa, y\rangle = \langle a, \bar{x}y\rangle$. Since D_1 is a composition algebra it must be closed under conjugation and multiplication so $\bar{x}y \in D_1$. So, since $a \perp \bar{x}y$ we must have $xa \perp y$. This concludes the proof that $D_1 a \subseteq D_1^\perp$. □

Since $\dim D_1 < \infty$ we can decompose C into $D_1 \oplus D_1^\perp$ which is a direct sum by Theorem 2.6. In particular, so is also $D_1 \oplus D_1 a$.

Proof of (ii). The left hand side of (3.26) is

$$(x + ya)(z + wa) = xz + x(wa) + (ya)z + (ya)(wa).$$

If we can prove the following equations we will have shown (3.26).

$$\begin{aligned} x(wa) &= (wx)a && (3.27)\\ (ya)z &= (y\bar{z})a && (3.28)\\ (ya)(wa) &= -N(a)\bar{w}y && (3.29) \end{aligned}$$

Note that $\bar{v} = -v$ for all $v \in C$ with $v \perp e$. In particular

$$\overline{va} = -va \tag{3.30}$$

for all $v \in D_1$. The following will prove (3.27);

$$\begin{aligned} \langle x(wa), v\rangle &= \langle wa, \bar{x}v\rangle \\ &= \langle \overline{wa}, \overline{\bar{x}v}\rangle \\ &= \langle -wa, \bar{v}x\rangle \\ &= -\langle wa, \bar{v}x\rangle \\ &= \langle wx, \bar{v}a\rangle \\ &= \langle wx, (\langle v, e\rangle e - v)a\rangle \\ &= \langle v, e\rangle\langle wx, a\rangle - \langle wx, va\rangle \\ &= \langle v, e\rangle 0 - \langle wx, va\rangle \\ &= -\langle (wx)\bar{a}, v\rangle \\ &= \langle (wx)a, v\rangle \end{aligned}$$

since it holds for arbitrary v. That $-\langle wa, \bar{v}x\rangle = \langle wx, \bar{v}a\rangle$ follows from (3.6).

Similarily we prove (3.28);

$$\begin{aligned} \langle (ya)u, z\rangle &= \langle ya, z\bar{u}\rangle \\ &= -\langle y\bar{u}, za\rangle \\ &= -\langle (y\bar{u})\bar{a}, z\rangle \\ &= \langle (y\bar{u})a, z\rangle. \end{aligned}$$

Here we once again used (3.6) to get $\langle ya, z\bar{u}\rangle = -\langle y\bar{u}, za\rangle$.

To prove the final equality we observe that from (3.30) we get

$$va = \overline{\overline{v}\overline{a}} = \overline{-va} = -\bar{a}\bar{v} = a\bar{v} \tag{3.31}$$

for all $v \in D_1$ so we have

$$\begin{aligned}(ya)(wa) &= (a\bar{y})(wa)\\ &= a((\bar{y}w)a)\\ &= a(a(\overline{\bar{y}w}))\\ &= a(a(\overline{w}y))\\ &= (aa)(\overline{w}y)\\ &= -(a\bar{a})(\overline{w}y)\\ &= -N(a)(\overline{w}y).\end{aligned}$$

This concludes the proof of (3.26) which shows that D_2 is closed under multiplication. The only thing left is to show that D_2 is non-singular. Looking at the norm N on D_2 we see that

$$N(x + ya) = \langle x, ya\rangle + N(x) + N(ya) = N(x) + N(y)N(a).$$

Looking at the inner product we similarily get for $x, y, v, w \in D_1$

$$\begin{aligned}\langle x + ya, v + wa\rangle &= \langle x, v\rangle + \langle x, wa\rangle + \langle ya, v\rangle + \langle ya, wa\rangle\\ &= \langle x, v\rangle + \langle ya, wa\rangle\\ &= \langle x, v\rangle + \langle y, w\rangle N(a)\end{aligned}$$

Let $x + ya \in D_2$ and assume that $\langle x + ya, v + wa\rangle = 0$ for all $v, w \in D_1$. Then $\langle x, v\rangle + \langle y, w\rangle N(a) = 0$ for all $v, w \in D_1$. In particular we have $w = 0$ which implies that $\langle x, v\rangle = 0$ for all $v \in D_1$. Since D_1 is non-singular we have $x = 0$. With a similar argument we also have $\langle y, w\rangle N(a) = 0$ for all $w \in D_1$ which (since $N(a) \neq 0$) implies that $y = 0$. Together these two cases gives us $x + ya = 0$ so D_2 is non-singular. □

To summarize the proof so far we know that $D_2 = D_1 \oplus D_1 a$ is a direct sum decomposition, that D_2 is a non-singular subspace of C and it is closed under multiplication. Hence D_2 is a composition subalgebra.

We now conclude the proof by showing that $\dim D_2 = 2 \dim D_1$. Let $R_a : D_1 \to D_1 a$ be the map $x \mapsto xa$. It is a linear map since multiplication is bilinear. Moreover a has an inverse since $N(a) \neq 0$ so R_a has inverse $R_a^{-1} = R_{a^{-1}}$ which proves that R_a is bijective and hence an isomorphism. It then follows that $\dim D_1 a = \dim D_1$. From the direct sum we get $\dim D_2 = \dim D_1 + \dim D_1 a = 2 \dim D_1$ which completes the proof. □

Proposition 3.20 is a very powerful tool. It gives us a contructive method of creating new composition subalgebras from already existing ones. However, it does not say anything about the properties of the new ones except that they have double dimension.

Proposition 3.21. *Let C be a composition algebra and D a finite-dimensional proper composition subalgebra. Then D is associative.*

Proof. Let $a \in D^{\perp} \setminus \{0\}$ with $N(a) \neq 0$. The existence of such an a is guaranteed by Lemma 3.19. Using the equality $N((x+ya)(z+wa)) = N(x+ya)N(z+wa)$ for $x, y, z, w \in D$ we have

$$\begin{aligned} N((x+ya)(z+wa)) &= N((xz - N(a)\overline{w}y) + (wx + y\bar{z})a) \\ &= N(xz - N(a)\overline{w}y) + N(a)N(wx + y\bar{z}) \\ &= \langle xz, -N(a)\overline{w}y\rangle + N(xz) + N(-N(a)\overline{w}y) + \\ &\quad N(a)(\langle wx, y\bar{z}\rangle + N(wx) + N(y\bar{z})) \end{aligned}$$

and

$$\begin{aligned} N(x+ya)N(z+wa) &= (N(x) + N(y)N(a))(N(z) + N(w)N(a)) \\ &= N(x)N(z) + N(x)N(w)N(a) + \\ &\quad N(y)N(z)N(a) + N(y)N(w)N(a)N(a) \\ &= N(xz) + N(wx)N(a) + N(y\bar{z})N(a) + N(a)^2N(\overline{w}y) \end{aligned}$$

by Proposition 3.20. Combining the above we get

$$\langle wx, y\bar{z}\rangle = \langle xz, \overline{w}y\rangle.$$

Since we, from (3.13) and Proposition 3.10, have

$$\begin{aligned} \langle wx, y\bar{z}\rangle &= \langle y\bar{z}, wx\rangle \\ &= \langle (y\bar{z})\bar{x}, w\rangle \\ &= \langle x(z\bar{y}), \overline{w}\rangle \end{aligned}$$

and

$$\langle xz, \overline{w}y\rangle = \langle (xz)\bar{y}, \overline{w}\rangle$$

we then have

$$\langle x(z\bar{y}), \overline{w}\rangle = \langle (xz)\bar{y}, \overline{w}\rangle.$$

If we do a substitution for readability we see that

$$\langle x'(y'z'), w'\rangle = \langle (x'y')z', w'\rangle$$

holds for all $x', y', z', w' \in D$ so $x'(y'z') = (x'y')z'$ for all $x', y', z' \in D$ which shows that D is associative. □

Proposition 3.22. *Let C be a composition algebra and D_1 a finite-dimensional proper composition subalgebra. Also let $a \in D_1^{\perp}$ with $N(a) \neq 0$ and let $D_2 = D_1 \oplus D_1 a$. Then*

$$D_2 \text{ is associative} \iff D_1 \text{ is assosiative and commutative.}$$

Proof. D_2 is a composition subalgebra by Proposition 3.20 with multiplication as in (3.26).

"⇒" If D_2 is associative then so is every subalgebra of D_2. In particular, D_1 is associative. Let $x, y \in D_1$. Then $(xy)a = x(ya)$ and from (3.27) $x(ya) = (yx)a$. Combining these we get

$$xy = xyaa^{-1} = ((xy)a)a^{-1} = ((yx)a)a^{-1} = yxaa^{-1} = yx.$$

"⇐" Assume that D_1 is both commutative and associative. Then, for all $x_1, x_2, x_3, y_1, y_2, y_3 \in D_1$ we get[3]

$$\begin{aligned}(z_1z_2)z_3 &= (x_1x_2)x_3 - N(a)\big((\overline{y_2}y_1)x_3 + \overline{y_3}(y_2x_1) + \overline{y_3}(y_1\overline{x_1})\big) + \\ &\quad \big(y_3(x_1x_2) - N(a)y_3(\overline{y_2}y_1) + (y_2x_1)\overline{x_3} + (y_1\overline{x_2})\overline{x_3}\big)a \\ z_1(z_2z_3) &= x_1(x_2x_3) - N(a)\big(x_1(\overline{y_3}y_2) + (y_3x_2)y_1 + (y_2\overline{x_3})y_1\big) + \\ &\quad \big((y_3x_2)x_1 + (y_2\overline{x_3})x_1 + y_1(\overline{x_3}\overline{x_2}) - N(a)y_1(\overline{y_2}y_3)\big)a\end{aligned}$$

where $z_i = x_i + y_ia$, $i = 1, 2, 3$.

Since D_1 is associative and commutative we have that $x_1(x_2x_3) = (x_1x_2)x_3$ and that terms containing a in the above are equal. To show that $(z_1z_2)z_3 = z_1(z_2z_3)$ we are left with proving that

$$\begin{aligned}N(a)(\overline{y_2}y_1)x_3 &= N(a)x_1(\overline{y_3}y_2) \\ N(a)\overline{y_3}(y_2x_1) &= N(a)\overline{y_3}(y_1\overline{x_1}) \\ N(a)(y_3x_2)y_1 &= N(a)(y_2\overline{x_3})y_1.\end{aligned}$$

Using (3.28) we see that for $x, y, z \in D_1$

$$N(a)xyz = a\bar{a}xyz = \bar{a}z((ya)x) = \bar{a}z((y\bar{x})a) = N(a)\bar{x}yz$$

and similarily for y and z. So

$$N(a)xyz = N(a)\bar{x}yz = N(a)x\bar{y}z = N(a)xy\bar{z}$$

which proves the three equalities above since D_1 is both commutative and associative.

□

4 The (1, 2, 4, 8)-Theorem

With the doubling method to back us up we are now ready to take on the big theorem of this paper.

Theorem 4.1 (Theorem 3.18 revisited)**.** *Let C be a composition algebra over a field k. Then C is a quadratic, alternative algebra that satisfies the Moufang identities. Moreover, it must also satisfy one of the following;*

$\dim C$	k	commutative	associative	alternative
1	$\text{char}(k) \neq 2$	Yes	Yes	Yes
2	Any	Yes	Yes	Yes
4	Any	No	Yes	Yes
8	Any	No	No	Yes

Figure 1: Characteristics of composition algebras

[3]We omit most of the multiplications for readability since they are not the most important part.

Proof. Let C be a composition algebra. Then C is quadratic by Corollary 3.7, alternative by Proposition 3.17 and it satisifes the Moufang identities by Proposition 3.16.

1. Let's start with any composition algebra C. Then, if char $k \neq 2$, we can find a one-dimensional composition subalgebra $D_1 = ke$. It is non-singular since $\langle \lambda e, \mu e \rangle = \lambda\mu\langle e, e\rangle = 2\lambda\mu \neq 0$ if $\lambda, \mu \neq 0$. However if char $k = 2$ then $\langle \lambda e, \mu e\rangle = 0$ for all $\lambda, \mu \in k$ so ke is singular. Hence if char $k = 2$ then $\dim C > 1$.

2. If $\dim C > 1$ then, in the case of char $k \neq 2$, Lemma 3.19 and Proposition 3.20 gives us a two-dimensional subalgebra $D_2 = D_1 \oplus D_1 a$ for some element $a \in C$. Since D_1 is both associative and commutative D_2 must be associative by Proposition 3.22. A simple computation shows that it is also commutative. If char $k = 2$ we then use the following lemma.

   Lemma 4.2. *If C is a composition k-algebra with* char $k = 2$*, then there is $a \in C$ such that $\langle e, a\rangle \neq 0$. Also, $D = ke \oplus ka$ is a two-dimensional associative and commutative composition subalgebra.*

   Proof of Lemma 4.2. Assume that $\langle e, a\rangle = 0$ for all a, then $e = 0$ since $\langle\ ,\ \rangle$ is non-degenerate on C. So $\langle e, a\rangle \neq 0$ for some $a \in C$. Note that $a \notin ke$ (otherwise $\langle e, a\rangle = \langle e, \lambda e\rangle = 0$) so D must be two-dimensional. It is non-singular since if $\langle \lambda e + \mu a, x\rangle = 0$ for all $x \in D$ then in particular $\langle \lambda e + \mu a, e\rangle = 0$ and $\langle \lambda e + \mu a, a\rangle = 0$. These in turn give $\mu = 0$ and $\lambda = 0$ respectively since $\langle e, e\rangle = 0$ and $\langle a, a\rangle = 0$ so $\lambda e + \mu a = 0$. It is closed under multiplication as the following computation shows

   $$\begin{aligned} xy = (\alpha e + \beta a)(\gamma e + \delta a) &= \alpha\gamma e + (\alpha\delta + \beta\gamma)a + \beta\delta a^2 \\ &= \alpha\gamma e + (\alpha\delta + \beta\gamma)a + \beta\delta(\langle a, e\rangle a - N(a)e) \\ &= (\alpha\gamma - \beta\delta N(a))e + (\alpha\delta + \beta\gamma + \beta\delta\langle a, e\rangle)a. \end{aligned}$$

   That it is associative and commutative follows from two similar computations. □

   By this lemma we create, in the case char $k = 2$, $D_2 = ke \oplus ka'$ for some $a' \in C$ with $\langle e, a'\rangle \neq 0$. So now we have, no matter what the characteristic, a two-dimensional composition subalgebra $D_2 \subseteq C$.

3. If we assume that $\dim C > 2$ then we can perform the doubling another time and get a four-dimensional subalgebra $D_3 = D_2 \oplus D_2 b$. It is also associative by Prop. 3.22 but not commutative as the following shows.

   Let $y = a$ or $y = a'$ depending on the characteristic. If $y = a$ then by the choice of a we have $\langle a, e\rangle = 0$, so $\bar{y} = -y \neq y$. If $y = a'$ then assume that $\bar{y} = y$. We then have $\bar{y} = \langle y, e\rangle e - y$ which in turn yields $2y = \langle y, e\rangle e$. So $\langle y, e\rangle e = 0 \Longrightarrow \langle y, e\rangle = 0$ which contradicts the choice of a'. In both cases we have $\bar{y} \neq y$. We will now show that $D_2 b$ is non-singular. Assume that for some $xb \in D_2 b$ we have $\langle xb, zb\rangle = 0$ for all $zb \in D_2 b$. Then $\langle xb, zb\rangle = \langle x, z\rangle N(b) = 0$ which implies that $\langle x, z\rangle = 0$ for all $z \in D_2$. Since D_2 is non-singular must have $x = 0$ so $xb = 0$ and $D_2 b$ is non-singular. Using the same method as in the proof of Lemma 3.19 we find

an element $x \in D_2 b$ such that $N(x) \neq 0$. We're now finally able to show that D_3 is not commutative. Since $x \in D_2 b$ we also have $x \in D_2^{\perp}$ so $\overline{xy} = -xy$ by (3.30). But $\overline{xy} = \bar{y}\bar{x} = -\bar{y}x$ since $x \perp e$. Combining the equalities and remembering that we have $\bar{y} \neq y$ we get

$$xy = \bar{y}x \neq yx.$$

4. If we assume that $\dim C > 4$ we can perform the doubling one final time to obtain an eight-dimensional subalgebra $D_4 = D_3 \oplus D_3 c$. It is not commutative since $D_3 \subset D_4$. It is *not* associative, by Proposition 3.22. Moreover, it is not a proper composition subalgebra of C by Proposition 3.21. So $C = D_4$ and the proof is complete.

□

4.1 Proving Hurwitz Theorem

With all the theory developed in the framework of composition algebras it is now trivial to prove Hurwitz Theorem for all fields with characteristic not equal to two[4].

Theorem 4.3 (Hurwitz Theorem)**.** *Let k be a field with* char $k \neq 2$*. The only values of $n \in \mathbb{N} \setminus \{0\}$ for which (1.1) holds are $n \in \{1, 2, 4, 8\}$ where $x_i, y_j \in k$ and $z_i = z_i(x, y)$ is bilinear.*

Proof. Assume that (1.1) holds for some bilinear map $z = z(x, y)$. Let $N(x) = \sum_{i=1}^{n} x_i^2$. Then N is clearly a non-degenerate quadratic form. Moreover, $N(x)N(y) = N(z(x, y))$ by (1.1). The only thing missing before (k^n, N) is a composition algebra is the existence of an identity element e.

Lemma 4.4. *Let $N : A \to k$ be a non-degenerate quadratic form and $A \times A \to A$, $(x, y) \mapsto xy$ a bilinear map such that*

$$N(xy) = N(x)N(y) \qquad \forall x, y \in A.$$

Then there is a map $* : A \times A \to A$, $(x, y) \mapsto x * y$ such that

$$N(x * y) = N(x)N(y) \qquad \forall x, y \in A$$

and there is an element $e \in A$ such that

$$e * x = x * e = x \qquad \forall x \in A.$$

Proof of Lemma 4.4. Let $v \in A$ such that $N(v) \neq 0$. It is guaranteed to exist since N is non-degenerate. Let $u = N(v)^{-1} v^2$. Then $N(u) = 1$ and $N(ux) = N(xu) = N(x)$ for all $x \in A$. We also have $\langle ux, uy \rangle = N(ux + uy) - N(ux) - N(uy) = N(x + y) - N(x) - N(y) = \langle x, y \rangle$ so

$$\langle L_u(x), L_u(y) \rangle = \langle x, y \rangle \tag{4.1}$$

[4]The case char $k = 2$ is uninteresting since $(\sum x_i)^2 = (\sum x_i^2)$ in that case.

and similarily for R_u. Let L_u^* be the adjoint[5] of L_u. Then for all $x, y \in A$

$$\langle x, y\rangle = \langle L_u(x), L_u(y)\rangle = \langle x, L_u^*(L_u(y))\rangle.$$

Which means that $y = L_u^*(L_u(y))$ for all $y \in A$. So $L_u^* = L_u^{-1}$. Note that $N(L_u^{-1}(x)) = N(uL_u^{-1}(x)) = N(x)$. Once again, a similar argument holds for R_u.

Now define the map $* : A \times A \to A$ as

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

Then $N(x * y) = N(R_u^{-1}(x))N(L_u^{-1}(y)) = N(x)N(y)$. We also have

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

which means that u^2 is an identity element relative to $*$. □

Lemma 4.4 gives us a way to construct a new bilinear map z' such that (k^n, N) is a composition algebra with the bilinear multiplication being z'. Theorem 4.1 then implies that n must be $1, 2, 4$ or 8 and we are done. □

[5]We'll leave it to the reader to prove that the adjoint is well-defined and unique on a finite-dimensional vector space together with a non-degenerate bilinear form.

References

[1] H.-D. Ebbinghaus. *Numbers*, chapter 8. Springer Verlag, 1991.

[2] F. G. Frobenius. Über lineare substitutionen und bilineare formen. *Journal für die reine und angewandte Mathematik*, 1878.

[3] N. Jacobson. Composition algebras and their automorphisms. *Rendiconti del Circolo Matematico di Palermo*, 1958.

[4] T. A. Springer. *Oktaven, Jordan-Algebren und Ausnahmegruppen.* Math. Institut der Universität Göttingen, 1963.

[5] T. A. Springer and F. D. Veldkamp. *Octonions, Jordan Algebras, and Exceptional Groups.* Springer Verlag, 2000.

[6] M. Zorn. Theorie der alternativen ringe. *Abhandlungen aus dem Mathematischen Seminar der Universität Hamburg*, 1931.

Appendix A Hurwitz Problem

The identity for $n = 4$ is

$$(x_1^2 + x_2^2 + x_3^2 + x_4^2)(y_1^2 + y_2^2 + y_3^2 + y_4^2) = z_1^2 + z_2^2 + z_3^2 + z_4^2 \tag{A.1}$$

where

$$\begin{aligned} z_1 &= x_1y_1 - x_2y_2 - x_3y_3 - x_4y_4 \\ z_2 &= x_1y_2 + x_2y_1 + x_3y_4 - x_4y_3 \\ z_3 &= x_1y_3 - x_2y_4 + x_3y_1 + x_4y_2 \\ z_4 &= x_1y_4 + x_2y_3 - x_3y_2 + x_4y_1. \end{aligned}$$

The identity for $n = 8$ is

$$(x_1^2 + \cdots + x_8^2)(y_1^2 + \cdots + y_8^2) = z_1^2 + \cdots + z_8^2 \tag{A.2}$$

where

$$\begin{aligned} z_1 &= x_1y_1 - x_2y_2 - x_3y_3 - x_4y_4 - x_5y_5 - x_6y_6 - x_7y_7 - x_8y_8 \\ z_2 &= x_1y_2 + x_2y_1 + x_3y_4 - x_4y_3 + x_5y_6 + x_6y_5 + x_7y_8 - x_8y_7 \\ z_3 &= x_1y_3 - x_2y_4 + x_3y_1 + x_4y_2 + x_5y_7 - x_6y_8 + x_7y_5 + x_8y_6 \\ z_4 &= x_1y_4 + x_2y_3 - x_3y_2 + x_4y_1 + x_5y_8 + x_6y_7 - x_7y_6 + x_8y_5 \\ z_5 &= x_1y_5 - x_2y_6 - x_3y_7 - x_4y_8 + x_5y_1 + x_6y_2 + x_7y_3 + x_8y_4 \\ z_6 &= x_1y_6 + x_1y_5 + x_3y_8 - x_4y_7 - x_5y_2 + x_6y_1 - x_7y_4 + x_8y_3 \\ z_7 &= x_1y_7 - x_2y_8 + x_3y_5 + x_4y_6 - x_5y_3 + x_6y_4 + x_7y_1 - x_8y_2 \\ z_8 &= x_1y_8 + x_2y_7 - x_3y_6 + x_4y_5 - x_5y_4 - x_6y_3 + x_7y_2 + x_8y_1. \end{aligned}$$