FOLIA 345

Annales Universitatis Paedagogicae Cracoviensis

Studia ad Didacticam Mathematicae Pertinentia 13(2021)

ISSN 2080-9751
DOI 10.24917/20809751.13.4

Aleksandra Gałecka

A proof of the Hurwitz's theorem on composition algebras*

Abstract. We present a proof of the Hurwitz Theorem about construction and properties of real numbers, complex numbers, quaternions and octonions. In the proof we use the Dickson double for Cayley-Dickson algebras.

1. Introduction

The famous Hurwitz Theorem about real finite-dimensional composition algebras witnessed many proofs in the last decades, for example in (Ebbinghaus, H.D., Hermes, Hirzebruch, Koecher, Mainzer, Neukirch, J., Prestel, Remmert, 1990) and in (Adamaszek, 2006). In this article, we present a proof that is based on the so-called Dickson Double, i.e., a procedure of doubling the dimension of a given algebra. Unfortunately, in this process certain algebraic properties of the original algebra are lost.

In the article, we present an approach devoted to composition algebras. One can follow a different path; Frobenius limits to division algebras and therefore octonions are not included in his result (Sierpiński, 1966).

The article is organized as follows. We start with basic definitions and descriptions of quaternions and octonions which will be constructed later using the Dickson double. Next, we prove the Hurwitz Theorem and we obtain as conclusion that every finite-dimensional composition algebra has dimension $1, 2, 4$ or 8. Hopf, using methods of topology, proved that the dimension of a division algebra over the real numbers is a power of 2. We clarify that this power of two must be either $1, 2, 4$ or 8 (Hopf, 1940). The original proof of the Hopf Theorem uses a major result from algebraic topology that is known under the name of Bott periodicity and proven by Kervaire and Milnor (Bott, Milnor, 1958).

---

*2020 Mathematics Subject Classification: Primary: *17A75*; Secondary: *11R52, 15A63, 17A35*

Keywords and phrases: *Hurwitz theorem, hypercomplex number, Dickson double, composition algebra, division algebra*

The proof we are about to present is mostly a collection of well-known results with a little twist from the author. Instead of relying on the results from various branches of mathematics, we use just classical algebraic tools and hence the proof itself is elementary and self-contained. We establish the missing components in the existing results and improve several existing results, such as Lemmas 3.12 – 3.14. This approach simplifies the understanding of the theorem and the structure of composition algebras, which is often complicated by the use of different tools from other fields.

This work is based on the Author's bachelor's thesis.

Main Theorem 1 (Hurwitz) *(Smith, D.A., Conway, J.H., 2003) The only real finite-dimensional composition algebras are* $\mathbb{R}$, $\mathbb{C}$, $\mathbb{H}$ *and* $\mathbb{O}$.

2. Preliminaries

Let us start by introducing fundamental definitions used in this article.

2.1. Algebras

Definition 2.1 *An algebra* $(A, +, \cdot, \mathbb{R}, \cdot)$ *with identity* $\mathbb{1}$ *is called a* division algebra *if every nonzero element in this algebra is invertible, i.e, for every* $x \in A \setminus \{0\}$ *there exists* $x' \in A \setminus \{0\}$ *such that* $xx' = x'x = \mathbb{1}$.

Definition 2.2 *Consider a linear operator* $A \ni x \mapsto x^* \in A$ *having the following properties:*

(i) $(xy)^* = y^*x^*$ *for all* $x, y \in A$,

(ii) $x^{**} := (x^*)^* = x$ *for all* $x \in A$.

A pair $(A, *)$ *is called* *-algebra.

Definition 2.3 The Cayley-Dickson algebra $(A,^*)$ *is defined as* $*$*-algebra* $(A \times A,^*)$ *with the operations:*

$$\begin{aligned} (a,b)+(c,d) &= (a+c, b+d) && \text{for } (a,b),(c,d) \in A \times A, \\ \alpha \cdot (a,b) &= (\alpha a, \alpha b) && \text{for } \alpha \in \mathbb{R},\ (a,b) \in A \times A, \\ (a,b)\cdot(c,d) &= (ac - db^*, cb + a^*d) && \text{for } (a,b),(c,d) \in A \times A, \end{aligned}$$

where the conjugate $^* : A \times A \to A \times A$ *is defined by the formula:*

$$(a,b)^* = (a^*, -b) \qquad \text{for } (a,b) \in A \times A.$$

Cayley-Dickson algebras are defined in an iterative way, starting from the field of real numbers (with trivial conjugation). In the first step we obtain the field of complex numbers which is a two dimensional Cayley-Dickson algebra over the field of real numbers. Note that the algebra of real numbers has dimension $1 = 2^0$. In general, a Cayley–Dickson algebra of dimension 2^n is constructed using the Cayley–Dickson construction from an algebra of dimension 2^{n-1}.

Definition 2.4 *Let* $(A, +, \cdot, \mathbb{R}, \cdot)$ *be an algebra with identity.*

- *A nondegenerate quadratic form* $[\cdot] : A \to \mathbb{R}$ *is called a* quadratic norm.
- *We say that* A *with a quadratic norm* $[\cdot] : A \to \mathbb{R}$ *is a* composition algebra *if* $[x \cdot y] = [x] \cdot [y]$ *for all* $x, y \in A$.

For the purpose of this article we consider finite- dimensional composition algebras. This assumption holds for all results in the article.

Definition 2.5 *Let* H *be a non-empty subset of vector space* V *with inner product* $[\cdot, \cdot]$. *A linear subspace*

$$A^{\perp} = \{v \in V : [v, u] = 0 \text{ for all } u \in A\}$$

is called the orthogonal complement *of the set* H.

2.2. Quaternions

Consider the standard four-dimensional vector space $\mathbb{H} := \mathbb{R}^4$ over the field of real numbers. Let us denote $\mathbb{1} := (1, 0, 0, 0), i := (0, 1, 0, 0), j := (0, 0, 1, 0), k := (0, 0, 0, 1)$. We define multiplication in $\mathbb{H}$ as follows: for two elements $x_0\mathbb{1} + x_1 i + x_2 j + x_3 k, y_0\mathbb{1} + y_1 i + y_2 j + y_3 k \in \mathbb{H}$ we put

$$\begin{aligned}(x_0\mathbb{1} &+ x_1 i + x_2 j + x_3 k) \cdot (y_0\mathbb{1} + y_1 i + y_2 j + y_3 k) \\ &:= (x_0y_0 - x_1y_1 - x_2y_2 - x_2y_3)\mathbb{1} + (x_0y_1 + x_1y_0 + x_2y_3 - x_3y_2)i + \\ &\quad (x_0y_2 - x_1y_3 + x_2y_0 + x_3y_1)j + (x_0y_3 + x_1y_2 - x_2y_1 + x_3y_0)k.\end{aligned}$$

Then $\mathbb{H}$ is a non-commutative division algebra of dimension four, called the *quaternions.*

Note that we can also define $\mathbb{H}$ as the standard two-dimensional vector space $\mathbb{C}^2$ over $\mathbb{C}$.That is, each element $x_0\mathbb{1} + x_1 i + x_2 j + x_3 k$ is identified with a pair of complex numbers $(x_0 + x_1 i, x_2 + x_3 i)$ with the following multiplication (Sierpiński, 1966)

$$(x_0, x_1) \cdot (x_2, x_3) = (ac - bd^*, ad + bc^*) \qquad \text{for } (x_0, b), (c, d) \in \mathbb{C} \times \mathbb{C},$$

where z^* denotes the complex conjugate of a complex number z. This is a second way of defining multiplication in $\mathbb{H}$ after Definition 2.3.

2.3. Octonions

We can construct the octonions $\mathbb{O}$ in three different ways (Baez, J.C., 2002):

- as an eight-dimensional algebra with identity $\mathbb{1}$ over the field of real numbers, which elements are of the form

  $$x_0\mathbb{1} + x_1e_1 + x_2e_2 + x_3e_3 + x_4e_4 + x_5e_5 + x_6e_6 + x_7e_7,$$

  where $e_m \neq e_n$ for $m \neq n$ and $e_m^2 = -\mathbb{1}$ for all $m, n \in \{1, \ldots, 7\}$,

- as quadruples of complex numbers,
- as pairs of quaternions.

Addition in $\mathbb{O}$ is understood as adding vectors in eight-dimensional vector space with the basis $\{\mathbb{1}, e_1, \ldots, e_7\}$, but multiplication is based on the rule described on the graph presented in Figure 1.

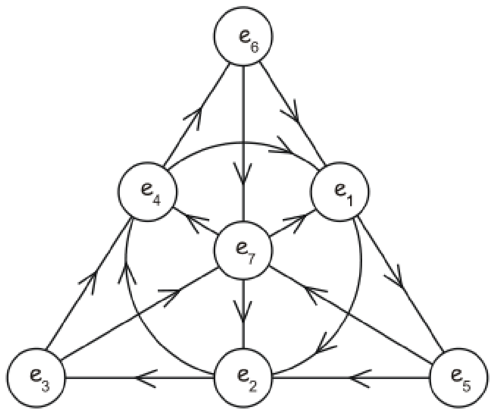

Figure 1: Multiplication rule for the basis in octonions (this picture was captured from (Baez, J.C., 2002)).

The product of two adjacent elements on a segment (or a circle) is given as the third element on that segment (or circle) if the product is taken in the direction of the arrow (e.g. $e_3 \cdot e_4 = e_6$), or as minus the third element on that segment (or circle) if the product is taken in the opposite direction (e.g $e_6 \cdot e_4 = -e_3$). On the other hand, when calculating the product of non-adjacent elements on the same segment, we get the third element on this segment with the "-" sign for arrow direction (e.g. $e_3 \cdot e_6 = -e_4$) or with the "+" sign (e.g. $e_6 \cdot e_3 = e_4$) otherwise.

Corollary 2.6 *According to the above rules, it turns out that the operation of multiplication in the set $\mathbb{O}$ is not associative, because for example we have $(e_3 \cdot e_4) \cdot e_5 = e_6 \cdot e_5 = -e_1$ and $e_3 \cdot (e_4 \cdot e_5) = e_3 \cdot e_7 = e_1$.*

3. A proof of the Main Theorem

Before we prove the Main Theorem, which is the Hurwitz Theorem, we have to present some auxiliary results. This part is based on (Smith, D.A., Conway, J.H., 2003) and (Schafer, R.D., 1966).

3.1. Properties of quadratic norms and inner products

Let us show some properties which follow from the existence of a norm in a composition algebra.

Let $(X, [\cdot])$ be a composition algebra. In this algebra we can consider the inner product $[\cdot,\cdot] : X \to \mathbb{R}$ defined as follows

$$[x, y] = \frac{1}{2}\big([x + y] - [x] - [y]\big) \qquad \text{for } x, y \in X.$$

LEMMA 3.1 *(Smith, D.A., Conway, J.H., 2003) Let $(X, [\cdot])$ be a composition algebra and take $x, y \in X$. If $[x, t] = [y, t]$ for all $t \in X$, then $x = y$.*

Proof. Let us assume that $[x, t] = [y, t]$ for every $t \in X$. Then

$$[x - y, t] = [x, t] - [y, t] = 0 \qquad \text{for } t \in X.$$

In particular, for $t = x - y$ we get $[x - y] = [x - y, x - y] = 0$. Since, the norm $[\cdot]$ is nondegenerate, so $x - y = 0$, and thus $x = y$.

LEMMA 3.2 *(Smith, D.A., Conway, J.H., 2003) Let $(X, [\cdot])$ be a composition algebra. Then*

(i) $[xy] = [x][y]$ *for all* $x, y \in X$,

(ii) $[xy, xz] = [x][y, z]$ *and* $[xz, yz] = [x, y][z]$ *for all* $x, y, z, \in X$,

(iii) $[xy, uz] = 2[x, u][y, z] - [xz, uy]$ *for all* $x, y, z, u \in X$.

Proof. The property (i) is a consequence of Definition 2.4. Take any $x, y, z, \in X$. Then using the property (i) we get

$$\begin{aligned}[xy, xz] &= \frac{[xy + xz] - [xy] - [xz]}{2} = \frac{[x(y + z)] - [x][y] - [x][z]}{2} \\ &= \frac{[x][y + z] - [x][y] - [x][z]}{2} = \frac{[x]\big([y + z] - [y] - [z]\big)}{2} \\ &= [x]\frac{[y + z] - [y] - [z]}{2} = [x][y, z].\end{aligned}$$

Similarly we show that

$$[xz, yz] = [x, y][z]$$

This shows the property (ii).

Now, by substituting $x + u$ for x in the property (ii), we obtain

$$[(x + u)y, (x + u)z] = [xy + uy, xz + uz] = [xy, xz] + [xy, uz] + [uy, xz] + [uy, uz].$$

Thus

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

Now we prove more properties of composition algebras connected with the inner product and the conjugation.

Definition 3.3 *Let $(X,[\cdot])$ be a composition algebra and $x \in X$. A* conjugate $\overline{x}$ *of x is the element of X defined as follows*

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

Lemma 3.4 *(Smith, D.A., Conway, J.H., 2003) Let $(X,[\cdot])$ be a composition algebra. Then*

(i) $[xy,z] = [y,\overline{x}z]$ *and* $[xy,z] = [x,z\overline{y}]$ *for* $x,y,z \in X$,

(ii) $\overline{\overline{x}} = x$ *for* $x \in X$,

(iii) $\overline{xy} = \overline{y}\,\overline{x}$ *for* $x,y \in X$.

Proof. Substituting $\mathbb{1}$ for u in Lemma 3.2 (iii), we get

$$\begin{aligned} [xy,z] &= [xy,\mathbb{1}z] = 2[x,\mathbb{1}][y,z] - [xz,\mathbb{1}y] = [y,2[x,\mathbb{1}]z] - [xz,y] \\ &= [y,2[x,\mathbb{1}](\mathbb{1}z)] - [y,xz] = [y,(2[x,\mathbb{1}]\mathbb{1})z - xz] \\ &= [y,(2[x,\mathbb{1}]\mathbb{1} - x)z] = [y,\overline{x}z]. \end{aligned}$$

Similarly we show that

$$[xy,z] = [x,z\overline{y}].$$

Let us substitute $\mathbb{1}$ for y and t for z in the property (i). As a consequence, we have

$$[x,t] = [x\mathbb{1},t] = [\mathbb{1},\overline{x}t] = [\overline{x}t,\mathbb{1}] = [t,\overline{\overline{x}}\mathbb{1}] = [\overline{\overline{x}}\mathbb{1},t] = [\overline{\overline{x}},t].$$

Thus $x = \overline{\overline{x}}$. By (ii) for arbitrary t we have

$$[\overline{y}\,\overline{x},t] = [\overline{x},\overline{\overline{y}}t] = [\overline{x},yt] = [\overline{x}\,\overline{t},y] = [\overline{t},\overline{\overline{x}}y] = [\overline{t},xy] = [\overline{t},\mathbb{1}(xy)] = [\overline{t}\,\overline{xy},\mathbb{1}] = [\overline{xy},t],$$

so by Lemma 3.1 we have $\overline{y}\,\overline{x} = \overline{xy}$.

Corollary 3.5 *(Springer, T.A., Veldkamp, F.D., 2000) Every composition algebra is a division algebra.*

Proof. Let $(X,[\cdot])$ be a composition algebra. We will prove that for any $x \in X \setminus \{0\}$, the element $\widehat{x} := \frac{1}{[x]}\overline{x}$ is the inverse of x.

Take any $x \in X$. Using Lemma 3.4 (i) we obtain

$$\begin{aligned} [\overline{x}x,t] &= [x,xt] = [x\mathbb{1},xt] = [x][\mathbb{1},t] = [[x]\mathbb{1},t], \\ [x\overline{x},t] &= [x,tx] = [\mathbb{1}x,tx] = [x][\mathbb{1},t] = [[x]\mathbb{1},t]. \end{aligned}$$

By Lemma 3.1 we get $x\overline{x} = [x]\mathbb{1} = \overline{x}x$, which means that

$$x\left(\frac{1}{[x]}\overline{x}\right) = \mathbb{1} = \left(\frac{1}{[x]}\overline{x}\right)x.$$

Thus $x^{-1} = \widehat{x} = \frac{1}{[x]}\overline{x}$.

3.2. Cayley-Dickson algebras

In this section we prove the Hurwitz Theorem. We start with the construction of the Cayley-Dickson subalgebra.

LEMMA 3.6 *Let X be an algebra with a quadratic norm $[\cdot]$. Assume that H is a finite-dimensional proper subalgebra of X. Then there exists a unit vector $i \in H^{\perp}$, i.e., a vector $i \in X$ such that $[i] = 1$ and $[a, i] = 0$ for all $a \in H$.*

Proof. Since H is a finite-dimensional proper linear subspace of X, there exists a non-zero vector $j \in H^{\perp}$. Using the fact that a quadratic norm in a composition algebra is positive-definite, we get $[j] > 0$. Let us define $i := \frac{1}{\sqrt{[j]}} \cdot j$. Then

$$[i] = \left[\frac{1}{\sqrt{[j]}} \cdot j\right] = \frac{1}{[j]} \cdot [j] = 1.$$

For all $a \in H$ we have

$$[a, i] = \left[a, \frac{1}{\sqrt{[j]}} \cdot j\right] = \frac{1}{\sqrt{[j]}}[a, j] = 0,$$

thus $i \in H^{\perp}$.

The following lemmas present a relation between the quadratic norm and the inner product in the composition algebra $H + iH$.

LEMMA 3.7 *(Smith, D.A., Conway, J.H., 2003) Let $(H, [\cdot]_H)$ be a proper subalgebra of a composition algebra $(X, [\cdot])$. Let $i \in H^{\perp}$ be such that $[i] = 1$. Then:*

(i) $[a + ib, c + id] = [a, c] + [b, d]$ *for* $a, b, c, d \in H$,

(ii) $[a + ib] = [a] + [b]$ *for* $a, b \in H$,

(iii) $\overline{a + ib} = \overline{a} - ib$ *for* $a, b \in H$,

(iv) $(a + ib)(c + id) = (ac - d\overline{b}) + i(cb + \overline{a}d)$ *for* $a, b, c, d \in H$.

Proof. Let us show property (i). Notice that

$$\begin{aligned}
[a + ib, c + id] &= [a, c] + [a, id] + [ib, c] + [ib, id] \\
&= [a, c] + [a\overline{d}, i] + [i, c\overline{b}] + [ib, id] \\
&= [a, c] + 0 + 0 + [i][b, d] = [a, c] + [b, d]
\end{aligned}$$

and as an immediate consequence of the above we also have property (ii):

$$[a + ib] = [a + ib, a + ib] = [a, a] + [b, b] = [a] + [b].$$

Next we have

$$\overline{ib} = 2[ib, \mathbb{1}] - ib = 2[i, \mathbb{1}\overline{b}] - ib = -ib,$$

so $\overline{a+ib} = \overline{a} + \overline{ib} = \overline{a} - ib$. Moreover, we have

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

To prove property (iv), let us start from the obvious equality

$$(a+ib)(c+id) = ac + a(id) + (ib)c + (ib)(id).$$

Then note that the following equalities hold for each $t \in X$:

$$\begin{aligned}[] [a(id),t] &= [id,\overline{a}t] = 2[i,\overline{a}][d,t] - [it,\overline{a}d] = 0 - [it,\overline{a}d] = -[t,\overline{i}(\overline{a}d)] \\ &= -[t,(-i)(\overline{a}d)] = [t,i(\overline{a}d)] = [i(\overline{a}d),t], \end{aligned}$$

$$\begin{aligned}[] [(ib)c,t] &= [ib,t\overline{c}] = [\overline{b}i,t\overline{c}] = 2[\overline{b},t][i,\overline{c}] - [\overline{b}\overline{c},ti] = 0 - [\overline{b}\overline{c},ti] = -[(\overline{b}\overline{c})\overline{i},t] \\ &= -[(\overline{b}\overline{c})(-i),t] = [(\overline{cb})i,t] = [i(cb),t], \end{aligned}$$

$$\begin{aligned}[] [(ib)(id),t] &= [ib,t(\overline{id})] = [ib,t(-(id))] = -[ib,t(id)] \\ &= -2[i,t][b,di] + [i(id),tb] = -2[i,t][bd,i)] + [id,\overline{i}(tb)] \\ &= 0 + [id,(-i)(tb)] = -[id,i(tb)] = -[i][d,tb] \\ &= -[d\overline{b},t] = [-d\overline{b},t]. \end{aligned}$$

These equalities and Lemma 3.1 imply that

$$\begin{aligned} (a+ib)(c+id) &= ac + a(id) + (ib)c + (ib)(id) = ac + i(\overline{a}d) + i(cb) - d\overline{b} \\ &= (ac - d\overline{b}) + i(\overline{a}d + cb). \end{aligned}$$

If H is a Cayley-Dickson algebra then the structure $H + iH$ with operations described in Lemma 3.7 is called the *Dickson Double*. Note that the operations described in Lemma 3.7 directly correspond to the operations on $(A \times A, ^*)$ described in Definition 2.3.

Corollary 3.8 *(Smith, D.A., Conway, J.H., 2003) If a composition algebra $(X, [\cdot])$ contains a proper subalgebra H and $i \in H^\perp$ is such that $[i] = 1$, then this algebra also contains the Dickson double subalgebra $H + iH$ of H.*

Proof. Let $a + ib, c + id \in H + iH$, where $a, b, c, d \in H$. Then

$$(a+ib) + (c+id) = (a+c) + i(b+d) \in H + iH,$$
$$\alpha(a+ib) = \alpha a + \alpha(ib) = \alpha a + i(\alpha b) \in H + iH,$$
$$(a+ib)\cdot(c+id) = ac - d\overline{b} + i(cb + \overline{a}d) \in H + iH.$$

Moreover, $0 + i0 \in H + iH$ is the zero element and $1 + i0 \in H + iH$ is the identity in $H + iH$. Thus $H + iH$ is a subalgebra of X.

Lemma 3.9 *(Schafer, R.D., 1966) Assume that* H *is a proper subalgebra of dimension* n *of a composition algebra* $(X, [\cdot])$, $i \in H^\perp$ *and* $[i] = 1$. *Then* $\dim(H + iH) = 2n$.

Proof. Let $h_1, \dots, h_n$ be a basis of H. We will prove that $h_1, \dots, h_n, ih_1, \dots, ih_n$ form a basis of $H + iH$.

Note that if $a + ib \in H + iH$, where $a, b \in H$, then $a = \sum_{k=1}^n \alpha_k h_k$ and $b = \sum_{k=1}^n \beta_k h_k$ for some $\alpha_1, \dots, \alpha_n, \beta_1, \dots, \beta_n \in \mathbb{R}$. Then

$$a+ib = \sum_{k=1}^n \alpha_k h_k + i\left(\sum_{k=1}^n \beta_k h_k\right) = \sum_{k=1}^n \alpha_k h_k + \sum_{k=1}^n i(\beta_k h_k) = \sum_{k=1}^n \alpha_k h_k + \sum_{k=1}^n \beta_k (ih_k),$$

which means that $h_1, \dots, h_n, ih_1, \dots, ih_n$ generates an algebra $H + iH$.

Consider $\alpha_1, \dots, \alpha_n, \beta_1, \dots, \beta_n \in \mathbb{R}$ such that $\sum_{k=1}^n \alpha_k h_k + \sum_{k=1}^n \beta_k (ih_k) = 0$. In particular, it means that

$$\left[\sum_{k=1}^n \alpha_k h_k + \sum_{k=1}^n \beta_k (ih_k)\right] = 0.$$

Then

$$0 = \left[\sum_{k=1}^n \alpha_k h_k + \sum_{k=1}^n \beta (ih_k)\right] = \left[\sum_{k=1}^n \alpha_k h_k + i\left(\sum_{k=1}^n \beta_k h_k\right)\right] = \left[\sum_{k=1}^n \alpha_k h_k\right] + \left[\sum_{k=1}^n \beta_k h_k\right].$$

Since the norm $[\cdot]$ is positive-definite, we get

$$\left[\sum_{k=1}^n \alpha_k h_k\right] = 0 \quad \text{and} \quad \left[\sum_{k=1}^n \beta_k h_k\right] = 0.$$

Since the norm is nondegenerate, we also have

$$\sum_{k=1}^n \alpha_k h_k = 0 \quad \text{and} \quad \sum_{k=1}^n \beta_k h_k = 0.$$

Since $h_1, \dots, h_n$ are linearly independent, we obtain $\alpha_k = 0$ and $\beta_k = 0$ for $k \in \{1, \dots, n\}$. This means that $h_1, \dots, h_n, ih_1, \dots, ih_n$ are linearly independent in $H + iH$.

Finally we obtain $\dim(H + iH) = 2n$.

Theorem 3.10 *(Hopf, 1940) Let* $(X, [\cdot])$ *be a finite-dimensional composition algebra over* $\mathbb{R}$. *Then* $\dim X = 2^m$ *for some* $m \in \{0\} \cup \mathbb{N}$.

Proof. If $X = \mathbb{R}$ then $\dim X = 1 = 2^0$. Let us assume that $\dim X \geq 2$ and suppose that $\dim X \neq 2^m$ for any $m \in \mathbb{N}$. Take $k \in \mathbb{N}$ such that $2^k < \dim X < 2^{k+1}$. We know that X contains the subalgebra $\mathbb{R}\mathbb{1}$ and, according to Corollary 3.8, it contains every double Dickson subalgebra of $\mathbb{R}\mathbb{1}$ up to the k-th one. It implies that X contains a subalgebra H of dimension 2^k. Thus X contains also the subalgebra $H + iH$ of dimension $2^{k+1} > \dim X$, which is a contradiction.

Using Lemma 3.7 we can show the construction of extension of a composition algebra. Such a construction uses the Dickson double.

Theorem 3.11 *Let $(H, [\cdot]_H)$ be a finite-dimensional composition algebra. In the set $H + iH$ (where $i \notin H$) we define the following operations*

$$\begin{aligned}
&(a+ib)+(c+id) = a+c+i(b+d) && \text{for } a+ib, c+id \in H+iH,\\
&\alpha(a+ib) = \alpha a + i(\alpha b) && \text{for } \alpha \in \mathbb{R}, a+ib \in H+iH,\\
&(a+ib)(c+id) = (ac - d\overline{b}) + i(cb + \overline{a}d) && \text{for } a+ib, c+id \in H+iH,\\
&\overline{a+ib} = \overline{a} - ib && \text{for } a+ib \in H+iH.
\end{aligned}$$

The mapping $[\cdot,\cdot]_{H+iH} : (H+iH)\times(H+iH) \to \mathbb{R}$,

$$[a+ib, c+id]_{H+iH} = [a,c]_H + [b,d]_H \qquad \text{for } a+ib, c+id \in H+iH,$$

is a well-defined inner product in $H + iH$ and $[\cdot]_{H+iH} : H + iH \to \mathbb{R}$,

$$[a+ib]_{H+iH} = [a+ib, a+ib]_{H+iH} = [a]_H + [b]_H \qquad \text{for } a+ib \in H+iH,$$

is a non-trivial quadratic norm on $H+iH$. In particular, the pair $(H+iH, [\cdot]_{H+iH})$ is a $2n$-dimensional algebra with a quadratic norm.

In the next part, we will prove that the procedure of doubling composition algebras retains the appropriate properties only for three consecutive iterations, but at every stage it loses some algebraic properties. We will prove three equivalences in Lemmas 3.12, 3.13, 3.14. One can find similar results in (Smith, D.A., Conway, J.H., 2003), where they are presented as implications only.

Lemma 3.12 *Let $(Y, [\cdot]_Y)$ be a composition algebra and let $Z = Y + i_Z Y$ be the Dickson double of Y, where $i_Z \in Z$, $[i_Z]_Z = 1$ and $i_Z \in Y^\perp$. Then Z is a composition algebra if and only if Y is an associative composition algebra.*

Proof. Assume that Z is a composition algebra, that is

$$[a + i_Z b]_Z [c + i_Z d]_Z = [(ac - d\overline{b}) + i_Z(cb + \overline{a}d)]_Z \qquad \text{for all } a,b,c,d \in Y.$$

Using Lemma 3.7 we get

$$\begin{aligned}
([a]_Y + [b]_Y)([c]_Y + [d]_Y) &= [ac - d\overline{b}]_Y + [cb + \overline{a}d]_Y\\
&= [ac - d\overline{b}, ac - d\overline{b}]_Y + [cb + \overline{a}d, cb + \overline{a}d]_Y\\
&= [ac, ac]_Y - [ac, d\overline{b}]_Y - [d\overline{b}, ac]_Y + [d\overline{b}, d\overline{b}]_Y\\
&\quad + [cb, cb]_Y + [cb, \overline{a}d]_Y + [\overline{a}d, cb]_Y + [\overline{a}d, \overline{a}d]_Y\\
&= [ac]_Y - 2[ac, d\overline{b}]_Y + [d\overline{b}]_Y + [cb]_Y + 2[cb, \overline{a}d]_Y + [\overline{a}d]_Y,
\end{aligned}$$

that is

$$[ac]_Y + [ad]_Y + [bc]_Y + [bd]_Y = [ac]_Y - 2[ac, d\overline{b}]_Y + [d\overline{b}]_Y + [cb]_Y + 2[cb, \overline{a}d]_Y + [\overline{a}d]_Y$$

for all $a, b, c, d \in Y$. Hence $[cb, \overline{a}d]_Y = [ac, d\overline{b}]_Y$. By Lemma 3.4 (i) it is equivalent to

$$[a(cb), d]_Y = [(ac)b, d]_Y \qquad \text{for all } a, b, c, d \in Y. \tag{1}$$

Thus, using Lemma 3.1, we get $a(cb) = (ac)b$ for every $a, b, c \in Y$, which means that Y is an associative composition algebra.

Now let us suppose that Y is an associative composition algebra. From Theorem 3.11 we know that $(Z, [\cdot]_Z)$ is an algebra with quadratic norm. Let $a, b, c, d \in Y$, then

$$\begin{aligned} [(a+ib)(c+id)]_Z &= [(ac - d\overline{b}) + i_Z(cb + \overline{a}d)]_Z = [ac - d\overline{b}]_Y + [cb + \overline{a}d)]_Y \\ &= [ac - d\overline{b}, ac - d\overline{b}]_Y + [cb + \overline{a}d, cb + \overline{a}d]_Y \\ &= [ac, ac]_Y - [ac, d\overline{b}]_Y - [d\overline{b}, ac]_Y + [d\overline{b}, d\overline{b}]_Y \\ &\quad + [cb, cb]_Y + [cb, \overline{a}d]_Y + [\overline{a}d, cb]_Y + [\overline{a}d, \overline{a}d]_Y \\ &= [ac]_Y - 2[ac, d\overline{b}]_Y + [d\overline{b}]_Y + [cb]_Y + 2[cb, \overline{a}d]_Y + [\overline{a}d]_Y. \end{aligned}$$

The associativity in Y implies the equality (1). By Lemma 3.4 (i) we have $[ac, d\overline{b}]_Y = [cb, \overline{a}d]_Y$. This implies

$$\begin{aligned} [(a+ib)(c+id)]_Z &= [ac]_Y + [d\overline{b}]_Y + [cb]_Y + [\overline{a}d]_Y \\ &= [a]_Y[c]_Y + [d]_Y[\overline{b}]_Y + [c]_Y[b]_Y + [\overline{a}]_Y[d]_Y \\ &= [a]_Y[c]_Y + [d]_Y[b]_Y + [c]_Y[b]_Y + [a]_Y[d]_Y \\ &= ([a]_Y + [b]_Y)([c]_Y + [d]_Y) = [a+ib]_Z[c+id]_Z. \end{aligned}$$

Thus $(Z, [\cdot]_Z)$ is a composition algebra.

LEMMA 3.13 *Let $(X, [\cdot]_X)$ be a composition algebra and let $Y = X + i_Y X$ be the Dickson double of X, where $i_Y \in Y$, $[i_Y]_Y = 1$ and $i_Y \in X^{\perp}$. Then $(Y, [\cdot]_Y)$ is an associative composition algebra if and only if X is an associative and commutative composition algebra.*

Proof. If $Y = X + i_Y X$ is an associative composition algebra, then its subalgebra X is also associative. Let $a, b, c, d, e, f \in X$. Note that

$$\begin{aligned} \big((a+i_Yb)(c+i_Yd)\big)(e+i_Yf) &= \big((ac - d\overline{b}) + i_Y(cb + \overline{a}d)\big)(e + i_Yf) \\ &= (ac - d\overline{b})e - f(\overline{b}\overline{c} + \overline{d}a) + i_Y\big(e(cb + \overline{a}d) + (\overline{c}\,\overline{a} - b\overline{d})f\big) \\ &= (ac)e - (d\overline{b})e - f(\overline{b}\overline{c}) - f(\overline{d}a) + i_Y\big(e(cb) + e(\overline{a}d) + (\overline{c}\,\overline{a})f - (b\overline{d})f\big) \end{aligned} \tag{2}$$

and

$$\begin{aligned} (a+i_Yb)\big((c+i_Yd)(e+i_Yf)\big) &= (a+i_Yb)\big((ce - f\overline{d}) + i_Y(ed + \overline{c}f)\big) \\ &= a(ce - f\overline{d}) - (ed + \overline{c}f)\overline{b} + i_Y\big((ce - f\overline{d})b + \overline{a}(ed + \overline{c}f)\big) \\ &= a(ce) - a(f\overline{d}) - (ed)\overline{b} - (\overline{c}f)\overline{b} + i_Y\big((ce)b - (f\overline{d})b + \overline{a}(ed) + \overline{a}(\overline{c}f)\big). \end{aligned} \tag{3}$$

The condition of associativity in the algebra $Y = X + i_Y X$ implies

$$(ac)e - (d\overline{b})e - f(\overline{bc}) - f(\overline{d}a) + i_Y\big(e(cb) + e(\overline{a}d) + (\overline{ca})f - (b\overline{d})f\big)$$
$$= a(ce) - a(f\overline{d}) - (ed)\overline{b} - (\overline{c}f)\overline{b} + i_Y\big((ce)b - (f\overline{d})b + \overline{a}(ed) + \overline{a}(\overline{c}f)\big)$$

for all $a, b, c, d, e, f \in X$. In particular, for $a, c, f = 0$ and $b = \mathbb{1}$ we have $de = ed$ for all $d, e \in X$. It means that X is a commutative algebra.

Let $(X, [\cdot]_X)$ be an associative and commutative composition algebra. Then, by Lemma 3.12, the pair $Y = X + i_Y X$ with some $i_Y \in Y$ such that $[i_Y]_Y = 1$, the pair $(Y, [\cdot]_Y)$ is a composition algebra. We will prove that this algebra is associative. Let $a, b, c, d, e, f \in X$. Using (2) and (3) we get

$$\big((a + i_Y b)(c + i_Y d)\big)(e + i_Y f)$$
$$= (ac)e - (d\overline{b})e - f(\overline{bc}) - f(\overline{d}a) + i_Y\big(e(cb) + e(\overline{a}d) + (\overline{ca})f - (b\overline{d})f\big)$$

and

$$(a + i_Y b)\big((c + i_Y d)(e + i_Y f)\big)$$
$$= a(ce) - a(f\overline{d}) - (ed)\overline{b} - (\overline{c}f)\overline{b} + i_Y\big((ce)b - (f\overline{d})b + \overline{a}(ed) + \overline{a}(\overline{c}f)\big).$$

Now using associative and commutativity of algebra X we get

$$(ac)e = a(ce),\ (d\overline{b})e = (ed)\overline{b},\ f(\overline{bc}) = (\overline{c}f)\overline{b},\ f(\overline{d}a) = a(f\overline{d}),$$
$$e(cb) = e(cb),\ e(\overline{a}d) = \overline{a}(ed),\ (\overline{ca})f = \overline{a})(\overline{c}f),\ (b\overline{d})f = (f\overline{d})b,$$

that is

$$\big((a + i_Y b)(c + i_Y d)\big)(e + i_Y f) = (a + i_Y b)\big((c + i_Y d)(e + i_Y f)\big).$$

Hence $(Y, [\cdot]_Y)$ is an associative composition algebra.

Lemma 3.14 *Let $(W, [\cdot]_W)$ be a composition algebra and let $X = W + i_X W$ be its Dickson double, where $i_X \in X$ is such that $[i_X]_X = 1$ and $i_X \in W^\perp$. Then X is an associative and commutative composition algebra if only and if W is commutaive and associative composition algebra such that the operation of conjugate is trivial, i.e, $\overline{a} = a$ for every $a \in W$.*

Proof. The algebra W is associative and commutative as subalgebra of X. Let $a \in W$. We have $\overline{i}_X = -i_X$. By Lemma 3.4 (iii) and Lemma 3.7 (iii) we obtain

$$-(\overline{a}i_X) = \overline{a}(-i_X) = \overline{a}\overline{i}_X = \overline{i_X a} = -i_X a,$$

Thus, since W is commutative, we have $\overline{a}i_X = ai_X$ for $a \in W$. This implies $(\overline{a} - a)i_X = \overline{a}i_X - ai_X = 0$. Hence $0 = [(\overline{a} - a)i_X]_X = [\overline{a} - a]_X \cdot [i_X]_X = [\overline{a} - a]_W$. Simultaneously, the norm $[\cdot]_W$ is positive definite, thus $\overline{a} = a$ for all $a \in W$.

On the other hand, if $(W, [\cdot]_W)$ is a commutative and associative composition algebra with trivial conjugation and $X = W + i_X W$ is its Dickson double algebra, then for all $a, b, c, d \in W$ we have

$$(a+i_X b)(c+i_X d) = (ac-d\overline{b})+i_X(cb+\overline{a}d) = (ca-b\overline{d})+i_X(ad+\overline{c}b) = (c+i_X d)(a+i_X b),$$

what means that $(X, [\cdot]_X)$ is a commutative and associative composition algebra.

The following Lemma, according to our best knowledge, is well-known in algebra. However, we were unable to find any reliable source of that fact. We therefore leave it without citing any source.

LEMMA 3.15 *If* $(W, [\cdot]_W)$ *is a composition algebra with a trivial conjugation, then* $\dim W = 1$.

Proof. Let $(W, [\cdot]_W)$ be a composition algebra with trivial conjugation and suppose that $\dim W \geq 2$. Then $\mathbb{R}\mathbb{1}$ is a non-trivial subalgebra. By Lemma 3.6, there exists an identity vector $i_X \in (\mathbb{R}\mathbb{1})^\perp$ (that is $[i_X, \mathbb{1}] = 0$). On the other hand, $i_X = \bar{i}_X = 2[i_X, \mathbb{1}]\mathbb{1} - i_X = -i_X$, what implies that $i_X = 0$. This is a contradiction.

We are ready to prove the Hurwitz Theorem.

Proof. [Proof of Main Theorem] Let $(Z, [\cdot]_Z)$ be a finite-dimensional composition algebra. By Theorem 3.10, the dimension of Z is equal to 2^m for some $m \in \{0\} \cup \mathbb{N}$. From the proof of Theorem 3.10 we see that we can construct Z as an iteration of Dickson double of its non-trivial subalgebra $(\mathbb{R}\mathbb{1}, [\cdot]_\mathbb{R})$.

If $\dim Z = 1$, then $Z = \mathbb{R}$. Let us assume that $\dim Z > 1$. Using (3.8) and Lemma 3.9 we see that Z contains the two-dimensional Dickson doubled $\mathbb{R} + i\mathbb{R}$ of the algebra $\mathbb{R}$. By Theorem 3.11 and Lemma 3.14, the doubled $\mathbb{C} := \mathbb{R} + i\mathbb{R}$ is a commutative and associative composition algebra with non-trivial quadratic norm $[x + iy]_\mathbb{C} = [x]_\mathbb{R} + [y]_\mathbb{R} = x^2 + y^2$ for $x + iy \in \mathbb{C}$.

If $\dim Z = 2$, then $Z = \mathbb{C}$. Let us assume that $\dim Z > 2$. By Corollary 3.8 and Lemma 3.9 the algebra Z contains the four-dimensional Dickson double $\mathbb{C} + j\mathbb{C}$ of $\mathbb{C}$. Using Theorem 3.11 and Lemma 3.13, its Dickson double $\mathbb{H} := \mathbb{C} + j\mathbb{C}$ is an associative and composition algebra with the non-trivial quadratic norm $[x + jy]_\mathbb{H} := [x]_\mathbb{C} + [y]_\mathbb{C}$ for $x + jy \in \mathbb{H}$.

If $\dim Z = 4$, then $Z = \mathbb{H}$. Assume that $\dim Z > 4$. Using Corollary 3.8 and Lemma 3.9 we obtain that Z contains the eight-dimensional Dickson double $\mathbb{H} + \nu\mathbb{H}$ of $\mathbb{H}$. By Theorem 3.11 and Lemma 3.12 Dickson double $\mathbb{O} := \mathbb{H} + \nu\mathbb{H}$ is a composition algebra with the non-trivial quadratic norm $[x + \nu y]_\mathbb{O} := [x]_\mathbb{H} + [y]_\mathbb{H}$ for $x + \nu y \in \mathbb{O}$.

If $\dim Z = 8$, then $Z = \mathbb{O}$. Assume that $\dim Z > 8$. By Corollary 3.8, the algebra Z contains the doubled $\mathbb{O} + \mu\mathbb{O}$ of $\mathbb{O}$. Theorem 3.11 implies that $S := \mathbb{O} + \mu\mathbb{O}$ is an algebra with the quadratic norm $[x + \mu y]_\mathbb{S} = [x]_\mathbb{O} + [y]_\mathbb{O}$ for $x + \mu y \in \mathbb{S}$. Suppose that $(\mathbb{S}, [\cdot]_\mathbb{S})$ is a composition algebra. Then $(\mathbb{O}, [\cdot]_\mathbb{O})$ is an associative composition algebra by Lemma 3.12. Thus, by Corollary 2.6, we obtain a contradiction. It follows that the assumption $\dim Z > 8$ is impossible, what completes the proof of the theorem.

From the proof we obtain:

COROLLARY 3.16 *The only finite-dimensional composition algebras are:*

(i) $\mathbb{R}$ *which is ordered and one-dimensional commutative and associative composition algebra with the trivial conjugation,*

(ii) $\mathbb{C}$ *which is two-dimensional commutative and associative composition algebra with a non-trivial conjugation,*

(iii) *the non-commutative field* $\mathbb{H}$*, which is four-dimensional non-commutative and associative composition algebra with a non-trivial conjugation,*

(iv) *the non-commutative and non-associative field* $\mathbb{O}$*, which is eight-dimensional non-commutative and non-associative composition algebra with a non-trivial conjugation.*

Acknowledgments

This note is a part of the author's Bachelor's Thesis that is written under the supervision of Wojciech Jabłoński. I also would like to thank Beata Gryszka, Karol Gryszka and Piotr Pokora for their meaningful support and useful comments.

References

Adamaszek, M.: 2006, 1,2,4,8, *Matematyka-Społeczeństwo-Nauczanie* **37**, 24–27.

Baez, J.C.: 2002, The octonions, *Bull. Amer. Math. Soc.* **39**, 145–205.

Bott, R., Milnor, J.: 1958, On the parallelizability of the spheres, *Bull. Amer. Math. Soc.* **64**, 87–89.

Ebbinghaus, H.D., Hermes, H., Hirzebruch, F., Koecher, M., Mainzer, K., Neukirch, J., Prestel, A., Remmert, R.: 1990, *Numbers. With an introduction by K.Lamotke. Transl. from the 2nd German ed. by H. L. S. Orde. Edited by J. H. Ewing*, New York etc.: Springer-Verlag.

Hopf, H.: 1940, Ein topologischer Beitrag zur reellen Algebra, *Comment. Math. Helv.* **13**, 219–239.

Schafer, R.D.: 1966, *An introduction to nonassociative algebras*, Academic Press.

Sierpiński, W.: 1966, *Arytmetyka teoretyczna*, PWN.

Smith, D.A., Conway, J.H.: 2003, *On Quaternions and Octonions*, A K Peters Ltd.

Springer, T.A., Veldkamp, F.D.: 2000, *Octonions, Jordan Algebras and Exceptional Groups*, Springer-Verlag.

Aleksandra Gałecka
Department of Mathematics,
Pedagogical University of Kraków,
Podchorążych 2,
PL-30-084 Kraków, Poland.
e-mail: aleksandra.galecka@student.up.krakow.pl