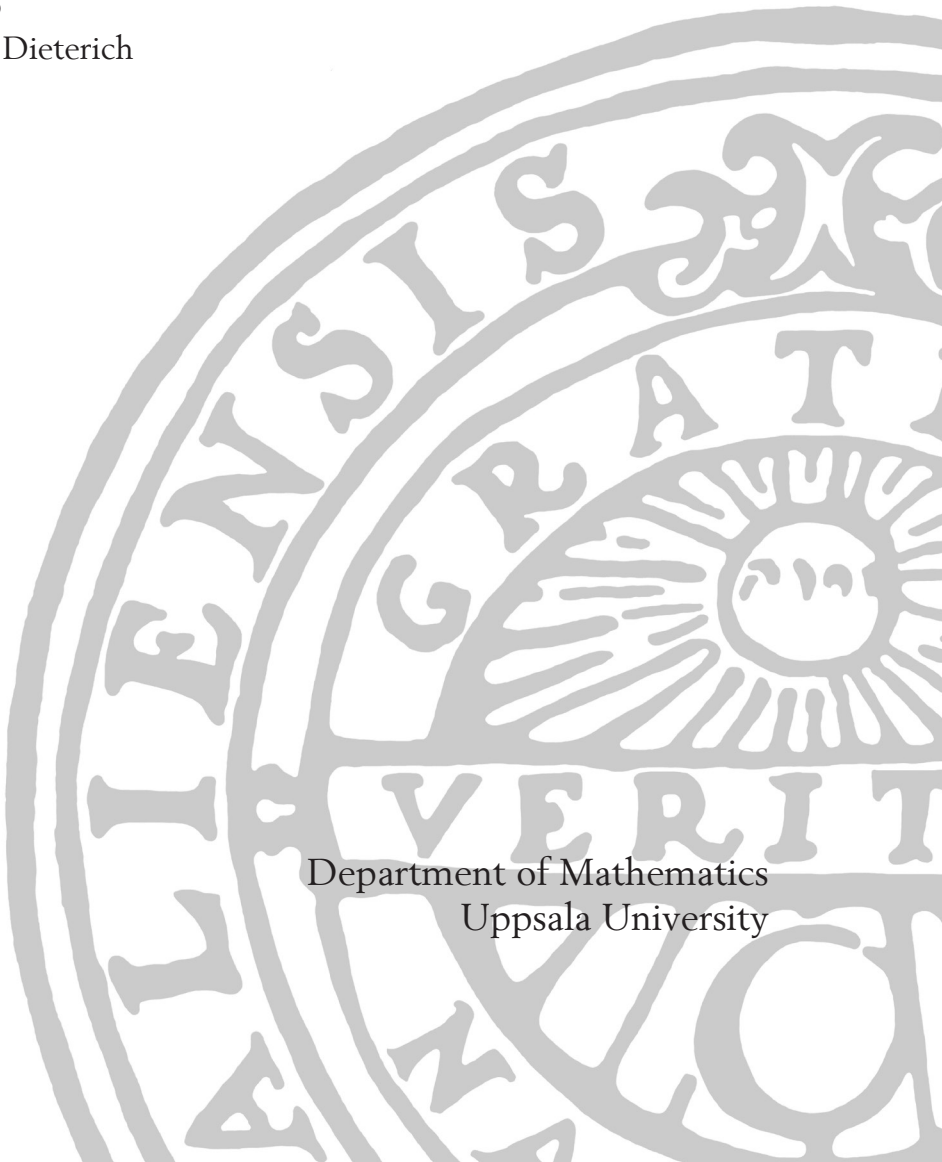
UPPSALA
UNIVERSITET

U.U.D.M. Project Report 2015:8

On a theorem by Cayley

Elin Persson Westin

Examensarbete i matematik, 15 hp
Handledare och examinator: Ernst Dieterich
Juni 2015



Department of Mathematics
Uppsala University

On a theorem by Cayley

Elin Persson Westin

June 2015

Abstract

In the year 1855 Arthur Cayley proved an interesting theorem about orthogonal mappings on the quaternion algebra. He proved that each orthogonal mapping $f : \mathbb{H} \to \mathbb{H}$ can be written in the simple form $f(x) = axb$ or $f(x) = a\overline{x}b$, where $a, b \in \mathbb{S}^3$. The quaternion algebra is a Hurwitz algebra of dimension 4 and in this paper we show that Cayley's Theorem in fact holds in much greater generality, namely for all Hurwitz division algebras H of dimension at most 4 over a field F of characteristic not 2 such that each element in the image of Q has a square root in F, where Q is the quadratic form of H.

1 Cayley's Theorem for Quaternions

1.1 Properties of the Quaternions

In this paper we will begin by studying Sir William Rowan Hamilton's quaternion algebra.[1, 2] It is a real vector space of dimension four and is denoted $\mathbb{H}$. In $\mathbb{R}^4$ we choose the standard basis

$$e := (1, 0, 0, 0) \quad i := (0, 1, 0, 0) \quad j := (0, 0, 1, 0) \quad k := (0, 0, 0, 1).$$

We let e be the identity element and define the multiplication of the other base-elements by

	i	j	k
i	$-e$	k	$-j$
j	$-k$	$-e$	i
k	j	$-i$	$-e$

It should be noted that $\mathbb{H}$ is not commutative. Using the distributive law the product of two arbitrary elements in $\mathbb{H}$ looks as follows:

$$\begin{aligned}&(ae+bi+cj+dk)(a'e+b'i+c'j+d'k)\\&=(aa'-bb'-cc'-dd')e+(ab'+ba'+cd'-dc')i\\&+(ac'-bd'+ca'+db')j+(ad'+bc'-cb'+da')k\end{aligned}$$

We can also define a function κ similar to the complex conjugate. Let $\kappa : \mathbb{H} \to \mathbb{H}$ be defined as $x = ae + bi + cj + dk \mapsto ae - bi - cj - dk = \overline{x}$.

It is sometimes more convenient to view the quaternions as complex matrices. We will therefore define the matrix algebra $\mathcal{H} := \left\{ \begin{pmatrix} w & -z \\ \overline{z} & \overline{w} \end{pmatrix} : w, z \in \mathbb{C} \right\}$ and it is possible to construct an isomorphism $F : \mathbb{H} \tilde{\to} \mathcal{H}$. It is easy to verify that $\mathcal{H}$ is a $\mathbb{R}$-subspace of Mat(2,$\mathbb{C}$) with dimension four. Since Mat(2,$\mathbb{C}$) is associative so is $\mathcal{H}$.

Definition 1. *Let V be a vector space of finite dimension over a field F. We say that a map $B : V \times V \to F$ is a* bilinear form *if for any $y \in V$*

$$y_R(x) \mapsto B(x, y)$$

and for any $x \in V$

$$x_L(y) \mapsto B(x, y)$$

are linear functions on V. Furthermore, we say that $B(x, y)$ is symmetric *if $B(x, y) = B(y, x)$ for all $x, y \in V$ and* positive definite *if $B(x, x) \geq 0$ holds for all $x \in V$ and $B(x, x) = 0$ implies $x = 0$.*

In this section we will work with finite-dimensional vector spaces over $\mathbb{R}$ together with a positive definite bilinear form σ on V and will be denoted by (V, σ). σ is called the *scalar product*. These vector spaces are called *Euclidean vector spaces*. We denote by $\langle \cdot, \cdot \rangle$ the *canonical scalar product* defined by

$$\langle x, x' \rangle = aa' + bb' + cc' + dd' \in \mathbb{R} \tag{1.1}$$

where $x = ae + bi + cj + dk$ and $x' = a'e + b'i + c'j + d'k$. The *norm*, or length, of an element $x \in V$ is defined by $|x| = \sqrt{\sigma(x, x)}$. We let $\mathbb{S}^3$ denote the set $\{x \in \mathbb{H} : |x| = 1\}$.

Definition 2. *A vector v is* orthogonal *to u if $\sigma(v, u) = 0$.*

Definition 3. *A linear transformation $f : V \to V$ is called an* orthogonal mapping *if $\sigma(f(v), f(w)) = \sigma(v, w)$ $\forall v, w \in V$. The set of all orthogonal mappings on V is denoted $O(V)$.*

We can also, equivalently, define a mapping to be orthogonal if $|f(x)| = |x|$ for all $x \in V$.

All linear mappings have an associated determinant. Let $e_1, ..., e_n$ be a basis of V, then f can be defined by which elements e_i are mapped to. Let $T = [f(e_1), ..., f(e_n)]$, then the determinant of f is simply $\det(T)$. If f is orthogonal, then $\det(f) = \pm 1$.

Definition 4. *One defines*

$$O^+(V) := \{f \in O(V) : \det(f) = 1\}$$
$$O^-(V) := \{f \in O(V) : \det(f) = -1\}$$

The set $O(V)$ forms a group under composition and is therefore called the *orthogonal group of V*. The set $O^+(V)$ is a normal subgroup of $O(V)$.

A special kind of functions, called reflections, are important in the proof of Cayley's Theorem.

Definition 5. *A* reflection *is a function $s_a : V \to V$, $a \in V \setminus \{0\}$, defined in the following way:*

$$s_a(x) = x - 2\frac{\sigma(a,x)}{\sigma(a,a)}a$$

There is a similar definition of reflections in $V = \mathbb{H}$ where $a \in \mathbb{S}^3$:

$$s_a(x) = x - 2\langle a, x\rangle a$$

One immediately sees that the two definitions coincide for $a \in \mathbb{S}^3$ since $\langle a, a\rangle = 1$. Moreover, every reflection s_a with $a \in \mathbb{H}$ is equal to s_b where $b = \dfrac{a}{|a|} \in \mathbb{S}^3$:

$$\begin{aligned} s_a(x) &= x - 2\frac{\langle a, x\rangle}{\langle a, a\rangle}a \\ &= x - 2\frac{\langle a, x\rangle}{|a|^2}a \\ &= x - 2\langle \frac{a}{|a|}, x\rangle \frac{a}{|a|} \\ &= x - 2\langle b, x\rangle b \\ &= s_b(x) \end{aligned}$$

Definition 6. *An* algebra *is a vector space A equipped with a bilinear product from $A \times A$ to A, $(x, y) \mapsto xy$.*

The next definition will be important in the generalization to Hurwitz algebras.

Definition 7. *We say that an algebra $A \neq 0$ is a* division algebra *if $\forall a, b \in A, a \neq 0$ the equations $ax = b$ and $ya = b$ have unique solutions.*

For an algebra of finite dimension we have the following theorem that helps us determine whether or not an algebra is a division algebra:

Theorem 1. *If A is a finite-dimensional algebra the following is equivalent:*

1. *A is a division algebra,*
2. *A does not have zero divisors.*

Proof. $1 \Rightarrow 2$ is obvious since if $a \neq 0$ the equations $ax = 0$ and $ya = 0$ have the *unique* solutions $x = 0$ and $y = 0$. Now assume that A does not have zero divisors. Since A is finite dimensional, $x \mapsto ax$ and $y \mapsto ya$ being bijective is equivalent to $x \mapsto ax$ and $y \mapsto ya$ being injective. But since A does not have zero-divisors the kernel of both maps must be $\{0\}$ and the theorem is thus proven. [5, Lemma 2.6] □

Now we want to show that $\mathcal{H}$, and therefore also $\mathbb{H}$, is a division algebra. Assume $A, B \in \mathcal{H}$ and $AB = 0$. Then $\det(AB) = \det(A) \cdot \det(B) = 0$, which implies that $\det(A) = 0$ or $\det(B) = 0$. But since $\det \begin{pmatrix} w & -z \\ \overline{z} & \overline{w} \end{pmatrix} = |w|^2 + |z|^2$, $\det \begin{pmatrix} w & -z \\ \overline{z} & \overline{w} \end{pmatrix} = 0$ if and only if both $w = 0$ and $z = 0$ and we can conclude that $A = 0$ or $B = 0$. By the theorem stated above $\mathcal{H}$ is a division algebra.

1.2 The Generation Theorem

In this section we examine some properties of reflections and begin by interpreting reflections geometrically. Throughout this section V is a real vector space and σ is a positive definite bilinear form. [2]

Assume we have an Euclidean vector space V and let U be any subspace of V. We define the *orthogonal complement* $U^\perp$ to be the set of vectors in V orthogonal to all vectors in U:

$$U^\perp := \{x \in V : \sigma(x, u) = 0 \ \forall u \in U\}$$

Every $x \in V$ can then be written

$$x = u + v$$

where $u \in U$ and $v \in U^\perp$ are uniquely determined. The mapping

$$proj_U : V \to U, \quad proj_U(x) = u$$

is then well-defined. We notice that

$$\begin{aligned} proj_U(u) &= u \quad \forall u \in U \\ proj_U(v) &= 0 \quad \forall v \in U^\perp \end{aligned}$$

If we let $U = \mathbb{R}a$ we can interpret s_a geometrically. Then the projection of x into U will be $proj_U(x) = \dfrac{\sigma(a,x)}{\sigma(a,a)}a$.

Assume $x = u + v$ where $u \in \mathbb{R}a$ and $v \in (\mathbb{R}a)^\perp$.

$$\begin{aligned} s_a(x) &= s_a(u+v) \\ &= s_a(u) + s_a(v) \\ &= (u - 2\frac{\sigma(a,u)}{\sigma(a,a)}a) + (v - 2\frac{\sigma(a,v)}{\sigma(a,a)}a) \\ &= (u - 2proj_U(u)) + (v - 2proj_U(v)) \\ &= (u - 2u) + (v) \\ &= -u + v \end{aligned}$$

Theorem 2. *For $u, v \in V$ such that $u \neq v$ and $|u| = |v|$, there is $a \in V \backslash \{0\}$ such that $s_a(u) = v, s_a(v) = u$.*

Proof. Choose $a = u - v$ and compute $s_a(u)$. To make the calculations easier we first verify that $2\sigma(a,u) = \sigma(a,a)$:

$$\begin{aligned} 2\sigma(a,u) &= 2\sigma(u-v,u) \\ &= \sigma(u-v,u) + \sigma(u-v,u) \\ &= \sigma(u-v,u) + \sigma(u,u) - \sigma(v,u) \\ &\overset{|u|=|v|}{=} \sigma(u-v,u) + \sigma(v,v) - \sigma(v,u) \\ &= \sigma(u-v,u) + \sigma(v,v-u) \\ &= \sigma(u-v,u) - \sigma(u-v,v) \\ &= \sigma(u-v,u-v) \\ &= \sigma(a,a) \end{aligned}$$

In the equations above we have only used the fact that $|u| = |v|$ and that σ

is a symmetric bilinear function. Next we use the equality we just proved.

$$\begin{aligned} s_a(u) &= u - 2\frac{\sigma(a,u)}{\sigma(a,a)}a \\ &= u - (u - v) \\ &= v \end{aligned}$$

Since $s_a \circ s_a = Id$ the proof is complete. □

This theorem can also be proved geometrically. Let $a = u - v$ and $b = u + v$, then a and b will be orthogonal to each other. We can then express u, v in the following way:

$$\begin{aligned} u &= \frac{1}{2}a + \frac{1}{2}b \\ v &= -\frac{1}{2}a + \frac{1}{2}b \\ \implies &\begin{cases} s_a(u) & = -\frac{1}{2}a + \frac{1}{2}b = v \\ s_a(v) & = \frac{1}{2}a + \frac{1}{2}b = u \end{cases} \end{aligned}$$

Theorem 3 (Generation Theorem of $O(V,\sigma)$ through reflections)**.** *Every $f \in O(V,\sigma)$ is a product of at most $n = dim(V)$ reflections.*

Proof. First we define the empty product of reflections to be the identity map Id. We can therefore hereafter assume that $f \neq Id$.

The theorem will be proven by induction on $n = dim(V)$. If $n = 1$ we can, without loss of generality, assume that $V = \mathbb{R}$ and $\sigma(x,y) = xy$. It then follows that $s_a = -x \quad \forall x, a \in V$. For all vector spaces with $dim(V) = 1$ we have $O(V) = \pm Id$ and hence the theorem hold for $dim(V) = 1$.

Assume that $dim(V) = n$ and that the theorem holds for vector spaces with dimension $< n$. Since $f \neq Id$ there is $q \in V$ with $f(q) \neq q$, but $|f(q)| = |q|$ since $f \in O(V)$. Theorem 2 states that there exists $a \in V$ such that $s_a(f(q)) = q$.

Let $U := (\mathbb{R}q)^{\perp}$, since $s_a \circ f(q) = q$ the function will map U to itself. We can then define the induced function $g : U \to U$ where $g := s_a \circ f|_U$. U is made into a Euclidean vector space by the restriction σ_U of σ on $U \times U$ and we obtain $g \in O(U, \sigma_U)$. By the induction assumption g is a product of at most $n - 1$ reflections $s_b : U \to U, b \in U$. Thus there is $b_1, ...b_r \in U$, $r < n$, with $g = s_{b_1} \circ ... \circ s_{b_r}$. It follows that

$$(s_a \circ f)(x) = (s_{b_1} \circ ... \circ s_{b_r})(x) \quad \forall x \in U \tag{1.2}$$

Since $b_i \in U = \mathbb{R}q^{\perp}\ \forall i$, for $x \in \mathbb{R}q$ we have $\sigma(b_i, x) = 0$ and get the following result:

$$s_{b_i}(x) = x - 2\frac{\sigma(b_i, x)}{\sigma(b_i, b_i)}b_i = x$$
$$\Rightarrow s_{b_1} \circ ... \circ s_{b_r}(x) = x \tag{1.3}$$

We previously showed that $s_a \circ f(q) = q$ which implies that $s_a \circ f(x) = x$ for all $x \in \mathbb{R}q$. From Equation 1.3 we get the following equality:

$$(s_a \circ f)(x) = (s_{b_1} \circ ... \circ s_{b_r})(x) \quad \forall x \in \mathbb{R}q \tag{1.4}$$

Since $V = U \perp \mathbb{R}q$ and f is linear, together with Equations 1.2 and 1.4 we get:

$$(s_a \circ f)(x) = (s_{b_1} \circ ... \circ s_{b_r})(x) \quad \forall x \in V$$

Since $s_a \circ s_a = Id$ we finally get the desired result

$$f(x) = (s_a \circ s_{b_1} \circ ... \circ s_{b_r})(x) \quad \forall x \in V$$

□

1.3 Proof of Cayley's Theorem

In *H.-D. Ebbinghaus et al.*[1] we find Cayley's theorem. The goal of this section is to prove that the set of orthogonal mappings on $\mathbb{H}$, $O(\mathbb{H})$, is equal to $\{f : \mathbb{H} \to \mathbb{H} : f(x) = axb,\ a, b \in \mathbb{S}^3\} \cup \{f : \mathbb{H} \to \mathbb{H} : f(x) = a\overline{x}b,\ a, b \in \mathbb{S}^3\}$.

To begin with we show that $x \mapsto axb$ and $x \mapsto a\overline{x}b$ are orthogonal mappings. This follows directly from the fact that $|xy| = |x| \cdot |y|$ and that $a, b \in \mathbb{S}^3$:

$$|axb| = |a| \cdot |x| \cdot |b| = 1 \cdot |x| \cdot 1 = |x|$$
$$|a\overline{x}b| = |a| \cdot |\overline{x}| \cdot |b| = 1 \cdot |\overline{x}| \cdot 1 = |\overline{x}|$$

To show that every $f \in O(\mathbb{H})$ can be written axb or $a\overline{x}b$ with $a, b \in \mathbb{S}^3$ we look at reflections in $\mathbb{H}$, s_a,$a \in \mathbb{S}^3$, which we define in the following way:

$$s_a : \mathbb{H} \to \mathbb{H}, \quad x \mapsto x - 2\langle a, x\rangle a$$

The next lemma will help us find a very simple formula for reflections.

Lemma 1 (Triple product identity)**.** *For every $x, y \in \mathbb{H}$ the following equality holds:*

$$y\overline{x}y = 2\langle x, y\rangle y - \langle y, y\rangle x$$

Proof. One can easily verify that

$$x\overline{x} = \overline{x}x = \langle x, x\rangle e \quad \forall x \in \mathbb{H}.$$

If we replace x with $x + y$ we get the following result:

$$(x+y)(\overline{x+y}) = \langle x+y, x+y\rangle e \tag{1.5}$$

$$\begin{aligned}(x+y)(\overline{x+y}) &= x\overline{x} + x\overline{y} + y\overline{x} + y\overline{y} \\ &= \langle x, x\rangle e + \langle y, y\rangle e + (x\overline{y} + y\overline{x}) \end{aligned} \tag{1.6}$$

By combining Equations 1.5 and 1.6 we arrive at the following equality.

$$\begin{aligned}\langle x+y, x+y\rangle e &= \langle x, x\rangle e + \langle y, y\rangle e + (x\overline{y} + y\overline{x}) \\ &\Leftrightarrow \\ x\overline{y} + y\overline{x} &= (\langle x+y, x+y\rangle - \langle x, x\rangle - \langle y, y\rangle)e \\ &= (\langle x+y, x\rangle - \langle x, x\rangle + \langle x+y, y\rangle - \langle y, y\rangle)e \\ &= (\langle y, x\rangle + \langle x, y\rangle)e \\ &= 2\langle x, y\rangle e \end{aligned}$$

If we multiply both sides with y from the right we end up with the desired equality.

$$\begin{aligned}(x\overline{y} + y\overline{x})y &= 2\langle x, y\rangle y \\ &\Leftrightarrow \\ y\overline{x}y &= 2\langle x, y\rangle y - x\overline{y}y \\ &= 2\langle x, y\rangle y - \langle y, y\rangle x \end{aligned} \tag{1.7}$$

□

Using the Triple product identity we can now rewrite the formula for $s_a,\ a \in \mathbb{S}^3$.

$$\begin{aligned}-a(\overline{x})a &= -(2\langle x, a\rangle a - \langle a, a\rangle x) \\ &= -2\langle a, x\rangle a + x \\ &= s_a(x) \\ &\Leftrightarrow \\ s_a(x) &= -a\overline{x}a \end{aligned} \tag{1.8}$$

Next we define a new mapping $p_a : \mathbb{H} \to \mathbb{H}$ by $x \mapsto axa,\ a \in \mathbb{S}^3$. From 1.8 it follows that

$$s_a \circ s_b = s_a(-b\overline{x}b) = (-a)\overline{(-b\overline{x}b)}(a) = a\overline{b}x\overline{b}a \tag{1.9}$$

$$p_a \circ p_{\overline{b}} = p_a(\overline{b}x\overline{b}) = a\overline{b}x\overline{b}a \tag{1.10}$$

From this the following identity can be derived:

$$s_a \circ s_b = p_a \circ p_{\overline{b}} \quad \forall a, b \in \mathbb{S}^3 \tag{1.11}$$

Using Equations 1.8 and 1.11 along with the Generation Theorem for $O(V, \sigma)$ we can now formulate the Generation Theorem for $O(\mathbb{H})$.

Theorem 4 (Generation Theorem for $O(\mathbb{H})$)**.** *Every $f \in O^+(\mathbb{H})$ is a product of at most four mappings $p_a,\ a \in \mathbb{S}^3$. Furthermore, $O(\mathbb{H})$ is generated by the mappings $x \mapsto axa,\ a \in \mathbb{S}^3$ and $x \mapsto \overline{x}$.*

From the theorem just stated we can deduce the main theorem of this section.

Theorem 5 (Cayley's Theorem)**.** *For every orthogonal mapping $f : \mathbb{H} \to \mathbb{H}$ there exist two quaternions $a, b \in \mathbb{S}^3$ satisfying one of the following:*

(a) $f(x) = axb$ *if* $f \in O^+(\mathbb{H})$

(b) $f(x) = a\overline{x}b$ *if* $f \in O^-(\mathbb{H})$

Proof. (a) From the Generation Theorem for $O(\mathbb{H})$ we get that for all $f \in O^+(\mathbb{H})$ there exists $a_1, a_2, a_3, a_4 \in \mathbb{S}^3$ such that

$$\begin{gathered} f = p_{a_1} \circ p_{a_2} \circ p_{a_3} \circ p_{a_4} \\ \Leftrightarrow \\ f(x) = a_1a_2a_3a_4 \cdot x \cdot a_4a_3a_2a_1 \end{gathered}$$

If we put $a := a_1a_2a_3a_4$ and $b := a_4a_3a_2a_1$ then $a, b \in \mathbb{S}^3$ and $f(x) = axb$.

(b) If $f \in O^-(\mathbb{H})$ then $f \circ \kappa \in O^+(\mathbb{H})$ where κ is the conjugation map $x \mapsto \overline{x}$. From a) it follows that $f(\overline{x}) = f \circ \kappa(x) = axb$ where $a, b \in \mathbb{S}^3$. This is equivalent to $f(x) = a\overline{x}b,\ a, b \in \mathbb{S}^3$ and the theorem is now proven.

□

2 Generalisation of Cayley's Theorem to Hurwitz algebras

In the next part of this paper we are going to try and prove Cayley's Theorem for a more general kind of algebras: Hurwitz algebras. The Quaternion algebra is a Hurwitz algebra of dimension four and we prove that all necessary properties that we used in the previous section to prove Cayley's Theorem also holds for a large number of Hurwitz algebras. [3, 4]

2.1 Bilinear and Quadratic Forms

In this section, if not otherwise stated, V is a finite dimensional vector space over an arbitrary field F. Let $B(x, y)$ denote a symmetric bilinear form. We define a *quadratic form* $Q(x)$ as follows.

Definition 8. *A map from a vector space V into its base field F is called a* quadratic form *if:*

1. $Q(ax) = a^2 Q(x) \quad \forall a \in F, x \in V$
2. $B(x, y) = Q(x + y) - Q(x) - Q(y)$ *is a bilinear form.*

It follows immediately that this bilinear form must be symmetric. We say that B is *associated* with Q. Since $B(x, x) = 2Q(x)$, if $char(F) \neq 2$ then Q is determined by B. If $char(F) = 2$ then $B(x, x) = 0$ for all $x \in V$ which is the definition of an *alternate* bilinear form.

A symmetric bilinear form $B(x, y)$ is *non-degenerate* if $B(a, x) = 0$, $\forall x \in V$, implies that $a = 0$. A quadratic form $Q(x)$ is said to be *strictly non-degenerate* if the corresponding bilinear form is non-degenerate, and it is said to be *non-degenerate* if $Q(a) = 0 = B(a, x)$ $\forall x \in V \Rightarrow a = 0$. With these definitions it is clear that a quadratic form is non-degenerate if it is strictly non-degenerate, and if $char(F) \neq 2$ the converse is also true.

Definition 9. *A quadratic form $Q(x)$ is called* isotropic *if $Q(a) = 0$ for some $a \in A \setminus \{0\}$ and* anisotropic *if $Q(a) \neq 0$ for all $a \in A \setminus \{0\}$.*

We can now define reflections in a general finite dimensional vector space V with a quadratic form $Q(x)$ and the associated bilinear form $B(x, y)$. If $a \in V$ and $Q(a) \neq 0$ then the reflection $s_a : V \to V$ is defined by

$$s_a(x) := x - \frac{B(a, x)}{Q(a)} a.$$

For vectors spaces over certain fields the set of all reflections is equal to the set $\{s_a : a \in \mathbb{S}(V)\}$, where $\mathbb{S}(V) = \{x \in V : Q(x) = 1\}$. This means that for every $b \in V$ with $Q(b) \neq 0$ there exists $a \in \mathbb{S}(V)$ such that $s_b(x) = s_a(x)$ for all $x \in V$. But for this to hold we have to be able to define the square root for every element in the image of Q. This is equivalent to $X^2 - a \in F[X]$ having a root for each $a \in im(Q) \subseteq F$. We denote the two roots $\pm\sqrt{a}$. One can show that $a = \frac{b}{\sqrt{Q(b)}}$. This will later be of great importance to the main result of this section.

We define two elements $x, y \in V$ to be *orthogonal* if $B(x, y) = 0$ and the *orthogonal complement* $U^\perp := \{x \in V : B(u, x) = 0 \ \forall u \in U\}$. Note that if $char(F) \neq 2$ then

$$s_u(u) = u - \frac{B(u,u)}{Q(u)}u = u - 2u = -u$$

and if $v \in Fu^\perp$ then

$$s_u(v) = v - \frac{B(u,v)}{Q(u)}u = v.$$

If B is non-degenerate then $V = Fa \oplus (Fa)^\perp$ for all $a \in V$ and we can write every element x in V as $x = u + v$ where $u \in Fa$ and $v \in Fa^\perp$ are uniquely determined. This let us describe reflections in a very simple form. If $char(F) \neq 2$ then

$$\begin{aligned} s_a(x) &= s_a(u + v) \\ &= s_a(u) + s_a(v) \\ &= (u - \frac{B(u,a)}{Q(a)}a) + (v - \frac{B(v,a)}{Q(a)}a) \\ &= (u - 2u) + (v - 0) \\ &= -u + v \end{aligned}$$

If $char(F) = 2$ then $B(u, u) = 0$ and $s_u(u) = u$. Furthermore, we cannot write every element $x \in V$ as a sum of $u \in Fa$ and $v \in (Fa)^\perp$ and the result presented above does not hold if $char(F) = 2$.

Let $a \in V$ be fixed. Then choose a basis $\underline{b} = (b_1, ..., b_n)$ such that $b_1 \in Fa$ and $b_i \in (Fa)^\perp$ for $i = 2, ..., n$. Then the matrix of the map s_a will look as follows:

$$(s_a)_{\underline{b}} = \begin{pmatrix} -1 & & & \\ & 1 & & \\ & & \ddots & \\ & & & 1 \end{pmatrix}$$

The determinant of this matrix is clearly -1 and every reflection s_a has therefore determinant -1.

A linear mapping $f : V \to V$ is called *orthogonal* if $Q(f(x)) = Q(x)$ for every $x \in V$, or equivalently, if $B(f(x), f(y)) = B(x, y)$ for all $x, y \in V$. We define the *orthogonal group* of V relative to Q, $O(V, Q)$ or $O(V)$, as the set of all orthogonal mappings. The orthogonal group is a subgroup of the group of all bijective linear transformations.

We would now like to show that all reflections $s_a, Q(a) \neq 0$, are orthogonal. Note that from the definition of a quadratic form we have that $Q(x + y) = Q(x) + Q(y) + B(x, y)$ and $Q(-x) = Q(x)$.

$$\begin{aligned} Q(s_a(x)) &= Q(x - \frac{B(a,x)}{Q(a)}a) \\ &= Q(x) + Q(\frac{B(a,x)}{Q(a)}a) - B(x, \frac{B(a,x)}{Q(a)}a) \\ &= Q(x) + \frac{B(a,x)^2}{Q(a)^2}Q(a) - \frac{B(a,x)}{Q(a)}B(x,a) \\ &= Q(x) \end{aligned}$$

2.2 Hurwitz Algebras

Definition 10. *An algebra A over a field F is called a* Hurwitz algebra *if there exists a quadratic form $Q : A \to F$ such that*

1. *Q is multiplicative, i.e. $Q(xy) = Q(x)Q(y)$*
2. *The quadratic form Q is strictly non-degenerate*
3. *There is an unity 1 in $A \setminus \{0\}$.*

Definition 11. *An involution is an endomorphism f of a vector space A such that $f(f(a)) = a$ and $f(ab) = f(b)f(a)$ for all $a, b \in A$.*

We can now define the map $\kappa : A \to A$, where $\kappa = -s_1$, with properties similar to the complex conjugate. Since Q is multiplicative we have $Q(x)Q(1) = Q(x)$ which implies that $Q(1) = 1$. From the definition of reflections we then get

$$\kappa(x) = B(x, 1)1 - x.$$

We write $\kappa(x) = \overline{x}$ and $B(x, 1) = T(x)$. Since s_a is an orthogonal mapping and $Q(x) = Q(-x)$ we can conclude that $Q(\overline{x}) = Q(x)$.

Lemma 2. *Let A be a Hurwitz algebra. Then every element $x \in A$ satisfies the following equation:*

$$x^2 - T(x)x + Q(x) = 0 \tag{2.1}$$

Proof. From the property $Q(xy) = Q(x)Q(y)$ we get that $Q(x)Q(y+w) = Q(xy+xw)$. By subtracting $Q(xy)$ and $Q(xw)$ from both sides we get

$$Q(x)B(y,w) = B(xy,xw). \tag{2.2}$$

If we now replace x by $x+z$ and do the same procedure again we get

$$B(x,z)B(y,w) = B(xy,zw) + B(xw,zy) \tag{2.3}$$

Next put $z = 1$ and $y = xu$ in the equation above and use Equation 2.2 to get

$$\begin{aligned} B(x,1)B(xu,w) &= B(x \cdot xu, w) + B(xw, xu) \\ &= B(x \cdot xu, w) + Q(x)B(u,w) \end{aligned}$$

We can now rewrite this as

$$B(x \cdot xu + Q(x)u - T(x)xu, w) = 0$$

Since w was arbitrary and B is non-degenerate this means that

$$x \cdot xu + Q(x)u - T(x)xu = 0.$$

If we now put $u = 1$ we finally get

$$x^2 - T(x)x + Q(x) = 0.$$

□

Lemma 3. *For every finite dimensional vector space over a field F of characteristic not 2, where Q is a non-degenerate quadratic form, the following properties hold:*

$$\overline{x}x = Q(x)1 = x\overline{x} \tag{2.4}$$

$$\overline{x}(xy) = (\overline{x}x)y = Q(x)y \tag{2.5}$$

$$(yx)\overline{x} = y(x\overline{x}) = Q(x)y \tag{2.6}$$

$$\overline{xy} = \overline{y} \cdot \overline{x} \tag{2.7}$$

$$B(yz,x) = B(z,\overline{y}x) \tag{2.8}$$

$$B(xy,z) = B(x,z\overline{y}) \tag{2.9}$$

We also have the following interesting property of bilinear forms.

Lemma 4. *For every bilinear form that corresponds to a non-degenerate quadratic form we have the following equalities:*

$$B(x,y)1 = \overline{x}y + \overline{y}x$$
$$B(x,y)z = \overline{x}(yz) + \overline{y}(xz)$$

Proof.

$$\begin{aligned} B(x,y)z &= Q(x+y)z - Q(x)z - Q(y)z \\ &= \overline{(x+y)}(x+y)z - (\overline{x}x)z - (\overline{y}y)z \\ &= \overline{(x+y)}(xz+yz) - (\overline{x}x)z - (\overline{y}y)z \\ &= \overline{x}(xz) + \overline{x}(yz) + \overline{y}(yz) + \overline{y}(xz) - (\overline{x}x)z - (\overline{y}y) \\ &= \overline{x}(yz) + \overline{y}(xz) \end{aligned}$$

Put $z = 1$ and we obtain $B(x,y)1 = \overline{x}y + \overline{y}x$. □

Definition 12. *The associator* $[x,y,z]$ *of* $x,y,z \in A$ *is defined by*

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

Definition 13. *An algebra* A *is called alternative if*

$$[x,x,y] = 0 = [y,x,x] \tag{2.10}$$

holds for all $x,y \in A$.

Assume A is a Hurwitz algebra. By the way κ is defined we get that $x + \overline{x} = T(x)1$. We can also easily see that κ is an involution of the algebra A. From the previous lemma we got that $\overline{x}(xy) = (\overline{x}x)y$ and $(yx)\overline{x} = y(x\overline{x})$ which is equivalent to the associator relations

$$[\overline{x},x,y] = 0 = [y,x,\overline{x}].$$

If we combine this with the fact that $[1,x,y] = 0 = [y,x,1]$ and $x = T(x) - \overline{x}$ we get

$$[x,x,y] = 0 = [y,x,x].$$

This proves the following lemma.

Lemma 5. *Every Hurwitz algebra is alternative.*

Lemma 6. *For every alternative algebra we have*

$$(xy)x = x(yx) \tag{2.11}$$

To abbreviate we simply write xyx instead of $(xy)x = x(yx)$.

Proof. We know that $[x, x, y] = 0 = [y, x, x]$ holds and that the associator function is linear in each variable. If we exchange x for $x + z$ we get that $[x, z, y] + [z, x, y] = 0 = [y, x, z] + [y, z, x]$. This implies that $[x, y, x] = -[y, x, x] = 0$ and hence $(xy)x = x(yx)$ holds. □

Theorem 6. *All Hurwitz algebras are alternative and an involution* $\kappa : x \to \overline{x}$ *can be defined such that* $x\overline{x} = Q(x)1$.

2.3 The Cayley-Dickson process

We will now explain the Cayley-Dickson process which can be used to construct Hurwitz algebras. This is then used to formulate a theorem called The Generalized Hurwitz Theorem which lists all kinds of possible Hurwitz algebras.

Let A be an algebra that has a unity 1 and with a strictly non-degenerate quadratic form $Q(x)$. Assume that there is an involution κ such that $\overline{x}x = Q(x)1$. Pick any non-zero c from the base field F. We will now construct a new algebra (A, c) from A, κ and c that satisfies the same conditions as A but with dimension $2 \cdot \dim(A)$. This construction is called the *Cayley-Dickson process* and (A, c) is called a *c-double* of A.

Let $(A, c) = A \times A$ where addition and multiplication of elements in (A, c) are defined in the following way:

$$(u, v) + (x, y) = (u + x, v + y)$$
$$(u, v)(x, y) = (ux + c\overline{y}v, yu + v\overline{x})$$

This binary product is a bilinear function, which can be easily checked. We now have an algebra on (A, c) with unity $1 = (1, 0)$. Since $(u, 0)(x, 0) = (ux, 0)$ we have a monomorphism $u \to (u, 0)$ of A into (A, c). We can therefore identify A with the subalgebra A' of (A, c) that consists of all elements $(u, 0), u \in A$. If we put $v = (0, 1)$ we find that $v^2 = c(1, 0)$ and can view (A, c) as a direct sum of A and vA. This means that every element x in (A, c) can be written $a_1 + va_2$, where a_1, a_2 are uniquely defined.

Let $\tilde{Q}((x, y)) = Q(x) - cQ(y)$. $\tilde{Q}$ is a quadratic form since:

– For $a \in F$ and all $x \in (A, c)$, $\tilde{Q}(ax) = a^2\tilde{Q}(x)$.

– $\tilde{B}(x,y) = \tilde{Q}(x+y) - \tilde{Q}(x) - \tilde{Q}(y)$ is a symmetric bilinear form,

such that $\tilde{B}(x,y) = B(a_1,a_3) - cB(a_2,a_4)$ and $x = a_1 + va_2, y = a_3 + va_4 \in (A,c)$. We define an involution on (A,c) by extending the involution κ on A:

$$\kappa : (x,y) \to \overline{(x,y)} = (\overline{x}, -y)$$

If we write $(x,y) = x + vy$ we have $\overline{x+vy} = \overline{x} - vy$. From the definition of (A,c) and the multiplication on it we get

$$\begin{aligned}\overline{(x,y)}(x,y) &= (\overline{x},-y)(x,y)\\ &= (\overline{x}x - cy\overline{y}, xy - xy)\\ &= ((Q(x) - cQ(y))1_A, 0)\\ &= (Q(x) - cQ(y))1_{(A,c)}\end{aligned}$$

This means that the property $x\overline{x} = \tilde{Q}(x)1$ is preserved.

We assumed that Q was a strictly non-degenerate quadratic form and would now like to show that so is $\tilde{Q}$. If $x = a_1 + va_2$ and $y = a_3 + va_4$, then $\tilde{B}(x,y) = B(a_1,a_3) - cB(a_2,a_4)$. Assume that $\tilde{B}(x,y) = 0$ for all $y = a_3 + va_4 \in (A,c)$. If $a_4 = 0$ then $B(a_1,a_3) = 0$ and by the non-degeneracy of B this implies that $a_1 = 0$. Now if $a_3 = 0$ then $B(a_2,a_4) = 0$ and again this implies that $a_2 = 0$. Hence $x = a_1 + va_2 = 0$ and $\tilde{B}$ is therefore non-degenerate. By definition $\tilde{Q}$ is then strictly non-degenerate.

Next we have a lemma about the connection of commutativity, associativity and alternativity between (A,c) and A.

Lemma 7. *1. (A,c) is commutative and associative if and only if A is commutative, associative and κ is the identity function.*

2. (A,c) is associative if and only if A is commutative and associative.

3. (A,c) is alternative if and only if A is associative.

Proof. Let $x = (x_1,x_2), y = (y_1,y_2), z = (z_1,z_2)$ for $x_i, y_i, z_i \in A$. Let $[x,y] = xy - yx$ be the *commutator* and $[x,y,z] = (xy)z - x(yz)$ the *associator*, then

$$[x,y] = ([x_1,y_1] + c(y_2\overline{x_2} - x_2\overline{y_2}), (\overline{x_1} - x_1)y_2 + (y_1 - \overline{y_1})x_2) \tag{2.12}$$

$$\begin{aligned}[x,y,z] =& ([x_1,y_1,z_1] + c((y_2\overline{x_2})z_1 - (z_1y_2)\overline{x_2} +\\ & z_2(\overline{y_2}x_1) - x_1(z_2\overline{y_2}) + z_2(\overline{x_2y_1}) - (\overline{y_1}z_2)\overline{x_2});\\ & (\overline{y_1x_1})z_2 - \overline{x_1}(\overline{y_1}z_2) + z_1(\overline{x_1}y_2) - \overline{x_1}(z_1y_2) +\\ & z_1(y_1x_2) - (y_1z_1)x_2 + c((x_2\overline{y_2})z_2 - (z_2\overline{y_2})x_2)\end{aligned} \tag{2.13}$$

We will use these expressions to prove the lemma. We begin with proving Part 1 and 2 at the same time. First of all, since A is a subalgebra of (A, c), if (A, c) is both commutative and associative then so is of course the subalgebra A. If (A, c) is commutative then $[x, y] = 0$ for all $x, y \in (A, c)$. If we put $x_1 = 0 = y_1, x_2 = 1$ then we must have $y_2 = \overline{y_2}$ which means that κ is the identity function, this proves the "only if" direction in Part 1. If we instead assume that (A, c) is associative and put $x_2 = y_1 = z_1 = 0, y_2 = 1$ then 2.13 implies that $z_2 x_1 - x_1 z_2 = 0$, or equivalently, that A is commutative. Now one direction of Part 2 is proven. If we now assume that A is commutative and associative and κ is the identity function then from Equation 2.12 we get that $[x, y] = 0$ which means that (A, c) is commutative. If we only assume that A is commutative and associative we can still prove from Equation 2.13 that $[x, y, z] = 0$ and hence (A, c) is associative. We have now proven both directions of Part 1 and 2.

Now assume that A is associative. We want to show that (A, c) is alternative. Since we know by assumption that $x + \overline{x} = T(x)$, we can instead prove that $[\overline{x}, x, y] = 0$ for all $x, y \in (A, c)$ since this is then equivalent to $[x, x, y] = 0 = [y, x, x]$. Assume that A is alternative. By using the properties $\overline{x}(xy) = (\overline{x}x)y = Q(x)y = (yx)\overline{x} = y(x\overline{x})$ from Lemma 4 together with Equation 2.13 we get that

$$[\overline{x}, x, y] = (c[\overline{x_1}, y_2, \overline{x_2}], [x_1, y_1, x_2]) \tag{2.14}$$

If A also is associative, then $[\overline{x}, x, y] = 0$ and (A, c) is alternative. If (A, c) is alternative, then $[\overline{x}, x, y] = 0$ and this implies that A is associative. Part 3, and therefore the whole lemma, is now proven. □

Now follows a list of examples of Hurwitz algebras obtained from the Cayley-Dickson process.

1. The first case is $A = F$ where F is a field of characteristic not 2 and $Q(x) = x^2$. The restriction of the characteristic is important since if $char(F) = 2$ then there does not exist Hurwitz algebras of dimension 1 due to the fact that $B(x, y) = (x + y)^2 - x^2 - y^2 = 0$ for all $x, y \in F$ and Q is therefore not strictly non-degenerate.

2. The second case is $A = K(\mu) := F + Fv_1$, where F is an arbitrary field, $v_1^2 = v_1 + \mu$ and $4\mu + 1 \neq 0$. The involution of an element is defined as $\overline{\alpha + \beta v_1} = (\alpha + \beta) - \beta v_1$ and we have the quadratic form $Q(x) = x\overline{x}$. We have now two separate cases, if $x^2 - x - \mu$ is irreducible in $F[X]$, then $K(\mu)$ is a separable field extension of F, and if not then $K(\mu) = F \oplus F$. Once again, we can divide this example into two cases.

First assume that the characteristic of F is not 2, then we can define $v := v_1 - \frac{1}{2}$ which will satisfy $v^2 = \alpha := \frac{1}{4}(4\mu + 1) \neq 0$. We then have $K(\mu) = (F, \alpha)$. We can also see that (F, α) is always of this type if F is a field of characteristic not 2. If the characteristic of the field F is equal to 2 then $4\mu + 1 \neq 0$ holds for all μ.

We call these algebras *quadratic algebras* and they are commutative and associative, but as one can easily see from the definition the involution κ is not the identity mapping.

3. Next we have $A = Q(\mu, \beta) := (K(\mu), \beta)$, where $\beta \neq 0$. A is called a *(generalized) quaternion algebra* and since it is a β-double of a quadratic algebra it is associative but not commutative.

4. The last example is the *Cayley-Dickson algebra*, also called the *octonion algebra*, $C(\mu, \beta, \gamma) := K(Q(\mu, \beta), \gamma)$ with $\gamma \neq 0$. This algebra is alternative but not associative nor commutative, which means that a c-double of this algebra would not be a alternative and hence not a Hurwitz algebra.

Before we get to the main theorem of this section we need one more lemma.

Lemma 8. *Let A be a Hurwitz algebra and $B \subset A$ a subalgebra such that $1_a \in B$. It then follows that $B^\perp B + B B^\perp \subseteq B^\perp$ and the following equalities hold for all $a, b \in B$ and $v \in B^\perp$:*

$$\begin{aligned} \overline{v} &= -v \\ av &= v\overline{a} \\ a(vb) &= v(\overline{a}b) \\ (vb)a &= v(ab) \\ (va)(vb) &= -Q(v)b\overline{a} \end{aligned}$$

Proof. Since $1, a \in B$ and $v \in B^\perp$ it follows that $B(v, 1) = 0 = B(a, v)$ and we have $v + \overline{v} = 0$ and $a\overline{v} + v\overline{a} = 0$. By using the identity $B(x, z)B(y, w) = B(xy, zw) + B(xw, zy)$, which can be derived from the property $Q(xy) = Q(x)Q(y)$, we get

$$B(a, vb) = B(a1, vb) = -B(ab, v) + B(a, v)B(1, b) = 0$$

and analogously

$$B(a, bv) = 0.$$

But this means, since $a, b \in B$ and $v \in B^\perp$ were arbitrary, that $B^\perp B + BB^\perp \subseteq B^\perp$. By putting $x = a, y = v, z = b$ in Lemma 4 we obtain

$$a(\overline{v}b) = -v(\overline{a}b).$$

By conjugating both sides and using the equalities just shown we obtain

$$(vb)a = v(ab)$$

Finally, we want to show that $(va)(vb) = -Q(v)b\overline{a}$ and will do so by using previous equalities of the lemma along with Lemma 3 and 4.

$$\begin{aligned}
(va)(vb) &= -\overline{v}(\overline{va} \cdot b) + B(va, \overline{v})b \\
&= v(\overline{a}\overline{v} \cdot b) - B(va, v)b \\
&= -v(\overline{a}v \cdot b) - Q(v)B(a, 1)b \\
&= v(va \cdot b) - Q(v)B(a, 1)b \\
&= v(\overline{v} \cdot ba) - Q(v)B(a, 1)b \\
&= Q(v)(ba - B(a, 1)b) = -Q(v)b\overline{a}
\end{aligned}$$

□

Theorem 7 (Generalized Hurwitz Theorem)**.** *If A is a Hurwitz algebra, then A is isomorphic to one of the four types of algebras mentioned in the example above.*

Proof. In this proof, when we say "subalgebra", we mean a subalgebra containing the identity element 1. It should also be noted that since $a + \overline{a} \in F$, every subalgebra B satisfies $\overline{B} \subseteq B$.

Let B be a subalgebra of the Hurwitz algebra A which is finite-dimensional and such that the restriction of the bilinear form $B(x, y)$ to B is still non-degenerate. Since the restriction of $B(x, y)$ to B is non-degenerate so it is for $B^\perp$. It also follows that $A = B + B^\perp$.

We now assume that $B \neq A$. This implies that there exists $v \in B^\perp$ such that $Q(v) = -c \neq 0$. Since $B(x, y)$ is non-degenerate on B and $B(va, vb) = Q(v)B(a, b) = -cB(a, b)$ it follows that the mapping $x \mapsto vx$ from B into vB is one-to-one. Furthermore, it follows that $B(x, y)$ is non-degenerate on vB and that B and vB has the same dimension. We can then construct a new subspace $B_1 = B + vB$ where, again, the restriction of $B(x, y)$ to B_1 is non-degenerate.

From the previous lemma we can see that $B_1 = B + vB$ is the subalgebra (B, c) obtained from the Cayley-Dickson process. First we shall verify that

the multiplication of two elements agrees with the definition of multiplication in the Cayley-Dickson process.

$$\begin{aligned}(a_1 + vb_1)(a_2 + vb_2) &= a_1a_2 + a_1(vb_2) + (vb_1)a_2 + (vb_1)(vb_2) \\ &= a_1a_2 - Q(v)b_2\overline{b_1} + v(\overline{a_1}b_2) + v(a_2b_1) \\ &= a_1a_2 + cb_2\overline{b_1} + v(\overline{a_1}b_2 + a_2b_1)\end{aligned}$$

From the fact that $\overline{v} = -v$ it follows that $\overline{a + vb} = \overline{a} - \overline{b}v = \overline{a} - vb$, which means that the involution induced on B_1 agrees with the involution of the c-double of B. From this we can conclude that $B_1 = (B, c)$. Now we have a subalgebra B_1 that satisfies the same conditions as B and we can therefore repeat the same process with B_1.

If we return to the algebra A we can consider two separate cases depending on the characteristic of the base field F. We will begin with the case where $char(F) \neq 2$. If this is the case then F is a subalgebra of A and the restriction of $B(x, y)$ to F is non-degenerate. This means that we can set $B = F$. If $A = F$ then we have case 1, else, by what we just have shown, there is a subalgebra B_1 of A that is a quadratic algebra. Again, if $A = B_1$ we are done and if not, then there is a subalgebra B_2 of type 3, a generalized quaternion algebra, contained in A. At last, if $A \neq B_2$ there is a subalgebra B_3 that is a octonion algebra. But this subalgebra must be equal to A, else A would contain a c-double of a octonion algebra, but such subalgebra is not alternative which would contradict the fact that A is a Hurwitz algebra.

Now we consider the case where the characteristic of F is 2. In this case we must have $A \neq F$, because otherwise the assumption that A is a Hurwitz algebra is contradicted. We can now find $a \in A \setminus F$ such that $T(a) \neq 0$. Assume that there were no such element and that $T(x) = B(1, x) = 0$ for all $x \in A \setminus F$. For $\alpha \in F$ we have $T(\alpha) = 2\alpha = 0$ and thus $B(1, x) = 0$ for all $x \in A$ which contradicts the non-degeneracy of the bilinear form $B(x, y)$. Now, pick $a \in A \setminus F$ such that $T(a) \neq 0$ and put $s = \dfrac{a}{T(a)}$. Then $T(s) = 1$ and $s^2 = s + \mu$, where $\mu = -Q(s) \in F$. We can now construct a subalgebra $B = F + Fs$ that is non-degenerate with respect to $B(x, y)$ and where $\overline{\alpha + \beta s} = \alpha + \beta - \beta s$. This means that the subalgebra B is a quadratic algebra. As we have previously shown this means that A is one of the three latter algebras mentioned in the example. □

2.4 Split Hurwitz algebras and Hurwitz division algebras

In this section we define what a split Hurwitz algebra is and what consequences the property will have. We will also present some theorems to give a better picture of the number of split Hurwitz algebras compared to Hurwitz division algebras. We begin with the following lemma.

Lemma 9. *Let A be a Hurwitz algebra. Then the following conditions are equivalent:*

(a) Q is isotropic, i.e. there exists $x \in A \setminus \{0\}$ such that $Q(x) = 0$.

(b) There are zero-divisors in A.

(c) A contains an idempotent $e \neq 0, 1$.

Proof. We will first prove that (a) and (b) are equivalent. If $x \neq 0$ and $Q(x) = x\overline{x} = 0$, it is obvious that x is a zero-divisor. Now assume that there are zero-divisors in A: let $x, y \in A \setminus \{0\}$ and $xy = 0$. Then $Q(x)Q(y) = Q(xy) = 0$, but since $Q(x), Q(y) \in F$ and F is a field that means that $Q(x) = 0$ or $Q(y) = 0$. This means that (a) and (b) are equivalent. Now assume that there is an idempotent $e \neq 0, 1$. Then $e^2 = e$ and $e(e-1) = 0$, hence e is a zero-divisor. Suppose that properties (a) and (b) are satisfied. Then there must exist an element $x \in A \setminus \{0\}$ such that $Q(x) = 0$ and $T(x) = \alpha \neq 0$. If not, then $Q(x) = 0$ implies that $T(x) = 0$, and since property (a) is satisfied there must exist $a \in A \setminus \{0\}$ such that $Q(a) = 0 = T(a)$. For every $x \in A$ we have $Q(ax) = Q(a)Q(x) = 0$ and thus also $T(ax) = 0$. From Equation 2.3 we obtain $B(a, x) = T(a)T(x) - T(ax) = 0$ and by the non-degeneracy of B we get that $a = 0$ which is a contradiction. Let $x \in A \setminus \{0\}$ be such that $Q(x) = 0$ and $T(x) = \alpha \neq 0$, then $\alpha^{-1}x$ will be idempotent. This proves that (c) is equivalent to (a) and (b). □

Definition 14. *A Hurwitz algebra is called* split *if one of the conditions in Lemma 9 is satisfied.*

It should we noted that an Hurwitz algebra is split if and only if it is not a division algebra.

Next we have a theorem that shows that the case with split Hurwitz algebras is not the general case.

Theorem 8. *Any two split Hurwitz algebras over a field F that have the same dimension are isomorphic to each other.*

Corollary 1. *If F is an algebraically closed field, then there exist exactly four isomorphism classes of Hurwitz algebras over F if $char(F) \neq 2$ and there exist exactly three isomorphism classes if $char(F) = 2$.*

Proof. Since we know from the theorem above that all split Hurwitz algebras of the same dimension are isomorphic all we need to do is to prove that every Hurwitz algebra A with $\dim A > 1$ over F is split.

Pick any $a \in A \setminus F$ and let α be a root of the polynomial $X^2 - T(a)X + Q(a) \in F[X]$. Since F is algebraically closed such α does exist in F. We then have

$$a^2 - \alpha^2 = T(a)(a - \alpha)$$
$$\Leftrightarrow$$
$$(a - \alpha)(a + \alpha - T(a)) = 0$$

Since $a \notin F$ and $\alpha, T(a) \in F$ we have $a - \alpha \neq 0$ and $a + \alpha - T(a) \neq 0$. Hence there exists zero-divisors in A and A is therefore a split Hurwitz algebra. □

The final part of this section will be a theorem that proves the existence of Hurwitz division algebras in a number of cases. Before we can prove the theorem we need two lemmas. As a reminder, a *simple transcendental field extension* is a extension $F \subseteq E$ such that $E = F(\alpha)$ is generated by a single element and such that there exists an element a of E that is transcendental over F, meaning that $f(a) \neq 0$ for all polynomials $f \in F[X]$.

Lemma 10. *If $F_1 = F(\alpha)$ is a simple transcendental extension of the arbitrary field F, then the Hurwitz algebra $K(\alpha)$ over the field F_1, constructed from the Cayley-Dickson process, does not contain zero-divisors and is hence a Hurwitz division algebra.*

Proof. If we can prove that the polynomial $x^2 - x - \alpha$ is irreducible over $F_1 = F(\alpha)$ then from the Cayley-Dickson process we know that $K(\alpha)$ is a separable field extension and does therefore not contain zero-divisors. Suppose the opposite, that there is $a \in F_1$ such that $a^2 - a - \alpha = 0$. Since $F \subseteq F_1$ is a transcendental extension we can write $a = f \cdot g^{-1}$ with $f, g \in F[\alpha]$. From this we get that $(f \cdot g^{-1})^2 - f \cdot g^{-1} - \alpha = 0 \Leftrightarrow f^2 - fg = \alpha g^2$. Let $m = \deg f$ and $n = \deg g$, then $\max\{\deg f^2, \deg fg\} = \max\{2m, m+n\} = 2n+1 = \deg \alpha g^2$. But this this equality does not hold for any m, n and we have a contradiction. The lemma is therefore proven. □

Let A be an algebra over the field F and F_1 a extension of F. Now choose a F-base $(b_1, ..., b_n)$ of A. To define a bilinear form on A it is enough to define the product for each base element. Assume that the bilinear product

is defined by $B(b_i, b_j) = \sum_{k=1}^{n} \lambda_{ijk} b_k$ where $\lambda_{ikj} \in F$. Since $F \subseteq F_1$ we can define a new algebra over F_1 with the same base $(b_1, ..., b_n)$ since each $b_i \in F_1$ and use the same definition of the bilinear product. This algebra, which we will denote by $F_1 \otimes_F A$, is now a F_1-algebra.

Lemma 11. *Let F be a field and $F_1 = F(\alpha)$ a simple transcendental extension of the field. Furthermore, let A be a finite-dimensional algebra over F that has an involution κ such that for all $a \in A$ we have $a + \overline{a}, a\overline{a} \in F$ and also has an identity element 1. If A is a division algebra, then so is both A_{F_1} and the α-double $A_1 = (A_{F_1}, \alpha)$.*

Proof. We begin by proving that A_{F_1} has no zero-divisors and is therefore a division algebra. We assume that we can find $a = \sum_i t_i a_i \neq 0$ and $b = \sum_j s_j b_j \neq 0$ such that $t_i, s_j \in F(\alpha), a_i, b_j \in A$ and $ab = 0$. Now let f be the common denominator of t_i for all i, and likewise let g be the common denominator of all g_j's. Now multiplying a by f and b by g we obtain the following: $fa = \sum_i^n \alpha^i a'_i$, $gb = \sum_j^m \alpha^j b'_j$, where $a'_i, b'_j \in A$. Since $(fa)(gb) = 0$ we must have $a'_n b'_m = 0$ and since A is without zero-divisors either $a'_n = 0$ or $b'_m = 0$. But this implies that either $a = 0$ or $b = 0$ which is a contradiction. Hence A_{F_1} does not contain any zero-divisors.

Next we want to prove that $A_1 = (A_{F_1}, \alpha)$ does not contain any zero-divisors. Once again we assume that we can find non-zero $x = a + vb$ and $y = c + vd$ in (A_{F_1}, α) such that $xy = 0$. From the definition of the multiplication in (A_{F_1}, α) we have

$$ac + \alpha d\overline{b} = 0, \quad \overline{a}d + cb = 0 \tag{2.15}$$

As we just showed, there are no zero-divisors in A_{F_1} and therefore $a, b, c, d \in A_{F_1}$ are all non-zero. Like before there exist polynomials $f, g, h, t \in F[\alpha]$ such that

$$fa = \sum_{i=0}^{n} \alpha^i a_i, \quad gb = \sum_{i=0}^{m} \alpha^i b_i$$
$$hc = \sum_{i=0}^{k} \alpha^i c_i, \quad td = \sum_{i=0}^{l} \alpha^i d_i$$

where $a_i, b_i, c_i, d_i \in A$ and $a_n, b_m, c_k, d_l \neq 0$. From Equation 2.15 we get

$$gt(\sum_{i=0}^{n} \alpha^i a_i)(\sum_{i=0}^{k} \alpha^i c_i) + \alpha fh(\sum_{i=0}^{l} \alpha^i d_i)(\sum_{i=0}^{m} \alpha^i \overline{b_i}) = 0,$$

from this we can conclude that

$$\deg g + \deg t + n + k = \deg f + \deg h + l + m + 1 \tag{2.16}$$

and likewise we get

$$\deg g + \deg h + n + l = \deg f \deg t + k + m. \tag{2.17}$$

By subtracting 2.17 from 2.16 we get

$$2(\deg t - \deg h + k - l) = 1$$

which is clearly a contradiction since the left-hand side is an even number and 1 is of course *not* an even number. This means that (A_{F_1}, α) has no zero-divisors and is thus a division algebra. □

From Lemma 10 and 11 we get the final theorem of this section.

Theorem 9. *Let F be any field. Then for any $n = 2, 4, 8$ there exists an infinite extension F_1 of F and a Hurwitz division algebra of dimension n and with F_1 as its base field.*

2.5 Generation Theorem for anisotropic quadratic spaces

In this section we will assume that V is a finite-dimensional vector space over a field F of characteristic not 2 and with anisotropic quadratic form $Q(x)$. As we have seen in the previous section, if we have a Hurwitz algebra the general case is when the quadratic form is anisotropic and there exists only one isomorphism class for each dimension where this does not hold. We begin with a simple but important lemma and then proceed to prove the main theorem of this section.

Lemma 12. *For all $x, y \in V$ such that $x \neq y$ and $Q(x) = Q(y)$, there is $a \in V \setminus \{0\}$ such that $s_a(x) = y$ and $s_a(y) = x$.*

Proof. Choose $a = x - y$ and calculate $s_a(x)$. Since Q is anisotropic and $x \neq y$ we know that $Q(a) \neq 0$ and s_a is defined. To make the calculations easier we first need the following equality where we make use of the fact that $Q(x) = Q(y)$:

$$\begin{aligned} B(x - y, x) &= B(x, x) + B(-y, x) \\ &= Q(2x) - 2Q(x) + Q(-y + x) - Q(-y) - Q(x) \\ &= Q(x - y) + Q(x) - Q(y) \\ &= Q(x - y) \end{aligned}$$

We can then calculate $s_a(x)$.

$$\begin{aligned} s_a(x) &= x - \frac{B(a,x)}{Q(a)}a \\ &= x - \frac{B(x-y,x)}{Q(x-y)}(x-y) \\ &= x - (x-y) \\ &= y \end{aligned}$$

Since $s_a \circ s_a = Id$ the proof is now complete. □

Now we have all we need to prove the Generation Theorem. The proof will be similar to that of the Generation Theorem for Euclidean vector spaces. Note that the restrictions made on V will have the following consequences:

- Q is strictly non-degenerate.
- For every subspace $U \subset V$ the restriction $Q_U : U \to F$ will be anisotropic and strictly non-degenerate.
- For every subspace $U \subset V$ we have $V = U \oplus U^\perp$ and $(U^\perp)^\perp = U$.

It should be noted that if the characteristic of F is 2, then the restriction of the quadratic form Q to $U = (Fa)^\perp$, where $a \neq 0$, is not strictly non-degenerate. As we have shown previously $B(a,a) = 0$ and thus $a \in (Fa)^\perp$. But, by the definition of U, $B(a,x) = 0$ for all $x \in U$ but $a \neq 0$ and $Q|_U$ is not strictly non-degenerate.

Theorem 10 (Generation Theorem for anisotropic quadratic spaces)**.** *Let V be a finite-dimensional vector space over a field F of characteristic not 2, endowed with an anisotropic quadratic form Q. Then every orthogonal map $f \in O(V,Q)$ is a product of at most $n = \dim(V)$ reflections.*

Proof. We will define the empty product of reflections to be the identity mapping and we can therefore hereafter assume that $f \neq Id$.

The theorem will we proven by induction of the dimension $n = \dim(V)$. If $\dim(V) = 1$, then $V = Fv$ for a chosen base vector v. If $f \in O(V,Q)$ then $f(v) = xv$ and we have $Q(v) = Q(f(v)) = x^2Q(v)$, which implies that $x^2 = 1 \Leftrightarrow x = \pm 1$ and thus $f = \pm Id$. Finally, $s_v = -Id$ and the theorem holds for $n = 1$.

Now assume that $f \in O(V,Q)$, $\dim(V) = n$ and that the theorem holds for all vector spaces of dimension less than n. We have assumed that $f \neq Id$ and hence $f(q) \neq q$ for some $q \in V$. Since f is an orthogonal mapping

$Q(f(x)) = Q(x)$ and we can use Lemma 12. It ensures us of the existence of $a \in V$ such that $s_a(f(q)) = q$.

Let $U = (Fq)^\perp$ and look at $s_a \circ f$ on U. Since f and s_a are both linear functions $s_a \circ f$ will map U to itself. We can thus define the induced function $g : U \to U$ where $g := s_a \circ f|_U$. Taking $Q|_U$ as the quadratic form we get a new vector space with an anisotropic quadratic form. The vector space U then satisfies the criterion of the theorem and by the induction hypothesis g is a product of at most $\dim(U) = n - 1$ reflections in U, which means that they are reflections $s_b : U \to U$, where $b \in U$. So $g = s_{b_1} \circ ... \circ s_{b_r}$ where $r < n$, or equivalently,

$$(s_a \circ f)(x) = (s_{b_1} \circ ... \circ s_{b_r})(x) \quad \forall x \in U \tag{2.18}$$

Since $b_i \in U = (Fq)^\perp$ we have $B(b_i, x) = 0$ for all $x \in Fq$ and it follows that $s_{b_i}(x) = x$ and hence also $(s_{b_1} \circ ... \circ s_{b_r})(x) = x$. We also know that $s_a \circ f(x) = x$ for all $x \in Fq$.

$$(s_a \circ f)(x) = x = (s_{b_1} \circ ... \circ s_{b_r})(x) \quad \forall x \in Fq \tag{2.19}$$

Since $V = U \oplus Fq$ and f is linear, Equations 2.18 and 2.19 implies that

$$(s_a \circ f)(x) = (s_{b_1} \circ ... \circ s_{b_r})(x) \quad \forall x \in A$$

We know that $s_a \circ s_a = Id$ and this finally gives us the desired result

$$f(x) = (s_a \circ s_{b_1} \circ ... \circ s_{b_r})(x) \quad \forall x \in Fq$$

□

We now know that every orthogonal mapping $f \in O(V)$ is a product of at most $\dim(V)$ reflections. As we showed earlier the determinant of a reflection is -1. Since $\det(ab) = \det(a)\det(b)$ it follows that for $f \in O(V)$ $f = s_{a_1} \circ ... \circ s_{a_r}$ and $\det(f) = (-1)^r$ where $r < \dim(V)$ and $s_{a_i} \neq Id$. We can thus define

$$O^+(V) := \{f : V \to V : f \in O(V), \det(f) = 1\}$$
$$O^-(V) := \{f : V \to V : f \in O(V), \det(f) = -1\}$$

2.6 Generalized Cayley's Theorem for Hurwitz algebras

In this section we look at Hurwitz division algebras over a field with characteristic not 2. We want to prove that the set of all orthogonal mappings on

a Hurwitz algebra H is equal to the set $\{f : H \to H : f(x) = axb,\ a, b \in \mathbb{S}(H)\} \cup \{f : H \to H : f(x) = a\overline{x}b,\ a, b \in \mathbb{S}(H)\}$.

Since the quadratic form Q is multiplicative it is easy to see that the mappings $a \mapsto axb$ and $x \mapsto a\overline{x}b$, where $a, b \in S(H)$ are orthogonal:

$$Q(axb) = Q(a)Q(x)Q(b) = 1 \cdot Q(x) \cdot 1 = Q(x)$$
$$Q(a\overline{x}b) = Q(a)Q(\overline{x})Q(b) = 1 \cdot Q(x) \cdot 1 = Q(x)$$

Lemma 13 (Triple product identity)**.** *For every $x, y \in H$ the following equality holds:*

$$y\overline{x}y = B(x, y)y - Q(y)x$$

Proof. From Lemma 4 we have $B(x, y)1 = x\overline{y} + y\overline{x}$. By multiplying both sides with y we get the following equality:

$$(\overline{x}y + \overline{y}x)y = B(x, y)y$$
$$\Leftrightarrow$$
$$(y\overline{x})y = B(x, y)y - (x\overline{y})y$$
$$\Leftrightarrow$$
$$y\overline{x}y = B(x, y)y - Q(y)x$$

Notice that in the last equality we used the fact that H is alternative. □

Once again reflections will be of special interest and we will see that the previous lemma will be very important for these functions. Let $a \in \mathbb{S}(H)$, then

$$\begin{aligned} a(-\overline{x})a &= B(-x, a)a + Q(a)x \\ &= -B(x, a) + x \\ &= s_a(x) \\ &\Leftrightarrow \\ s_a(x) &= -a\overline{x}a \end{aligned} \tag{2.20}$$

Next we define a new mapping $p_a : H \to H$ by $x \mapsto axa$ where $a \in \mathbb{S}(H)$. From 2.20 one can easily prove that $s_a \circ s_b = p_a \circ p_{\overline{b}}$ for every $a, b \in \mathbb{S}(H)$:

$$\begin{aligned} s_a \circ s_b(x) &= -a\overline{(-b\overline{x}b)}a \\ &= a(\overline{b}x\overline{b})a \\ &= p_a \circ p_{\overline{b}}(x) \end{aligned}$$

This fact together with the Generation Theorem for anisotropic quadratic spaces, gives us the Generation Theorem for Hurwitz division algebras. Remember that a Hurwitz algebra is a division algebra if and only if its quadratic form is anisotropic.

Theorem 11 (Generation Theorem for Hurwitz division algebras)**.** *Let H be a Hurwitz division algebra over a field F of characteristic not* 2 *such that each element in the image of Q has a square root in F, where Q is the quadratic form of H. Then every mapping $f \in O^+(H)$ is a product of at most* $\dim(H)$ *mappings $p_a,\ a \in \mathbb{S}(H)$. Furthermore, $O(H)$ is generated by the mappings $x \mapsto axa,\ a \in \mathbb{S}(H)$ and $x \mapsto \overline{x}$.*

For the next theorem, which is the main goal of this paper, we have to restrict ourself to Hurwitz algebras of dimension ≤ 4 since we need the associativity.

Theorem 12 (Generalization of a Cayley's Theorem)**.** *Let H be a Hurwitz division algebra of dimension at most* 4 *over a field F of characteristic not* 2 *such that each element in the image of Q has a square root in F, where Q is the quadratic form of H. Then for every orthogonal mapping $f : H \to H$ there exist two elements $a, b \in \mathbb{S}(H)$ such that:*

(a) $f(x) = axb$ *if* $f \in O^+(H)$

(b) $f(x) = a\overline{x}b$ *if* $f \in O^-(H)$

Proof. (a) Let $n = \dim(H)$. From the Generation Theorem for Hurwitz division algebras it follows that for every $f \in O^+(H)$ there exists $a_1, ..., a_n \in \mathbb{S}(H)$ such that

$$f = p_{a_1} \circ ... \circ p_{a_n}$$
$$\Leftrightarrow$$
$$f(x) = a_1(...(a_n x a_n)...)a_1$$

It is in this step that the alternative property is not enough and we need associativity. We have previously proven that H is associative if and only if $\dim(H) \leq 4$. This means that we can express the function f in the following way

$$f(x) = axb \tag{2.21}$$

where $a = a_1 \cdot ... \cdot a_n$ and $b = a_n \cdot ... \cdot a_1$. Part (a) is now proven.

(b) If $f \in O^-(H)$, then $f \circ \kappa \in O^+(H)$ and from (a) it follows that $f(\overline{x}) = f \circ \kappa(x) = axb$ for some $a, b \in \mathbb{S}(H)$. By replacing $\overline{x}$ by x we get that $f(x) = a\overline{x}b$ and we have our desired result.

□

References

[1] H.-D. Ebbinghaus et al., *Numbers*, Springer-Verlag, New York, 1991. Translated from German by J.H. Ewing.

[2] Max Koecher, *Lineare Algebra und analytische Geometrie*, Springer-Verlag, 1985.

[3] Nathan Jacobson, *Basic Algebra I*, W.H. Freeman and Company, second edition, 1985.

[4] K.A. Zhevlakov, A.M. Slin'ko, I.P. Shestakov, A.I. Shirshov, *Rings that are nearly associative*, volume 104 of *Pure and Applied Mathematics*. Academic Press Inc. [Harcourt Brace Jovanovich Publishers], New York, 1982. Translated from Russian by Harry F. Smith.

[5] Ernst Dieterich, *A general approach to finite dimensional division algebras*, Colloq. Math. 126 (2012), pp 73-86.