Octonions, Quaternions, and Involutions

Nathaniel Schwartz
Joint work with John Hutchens

Washington College
nschwartz2@washcoll.edu

November 7th, 2015
Contents

1 Bilinear forms / Quadratic forms
2 Algebras
3 Composition algebras
4 Doubling
5 Automorphisms
6 Results
7 Interesting Things
8 Current & Future work
Bilinear & Quadratic Forms

Let $V$ be a finite dimensional vector space over a field $k$. Then a **bilinear form** is a mapping

$$\langle \ , \ \rangle : V \times V \rightarrow k$$

that is linear in both coordinates. We say that $\langle \ , \ \rangle$ is **nondegenerate** if

$$V^\perp = \{ x \in V \mid \langle x, y \rangle = 0 \ \forall \ y \in V \} = 0.$$
Bilinear & Quadratic Forms

Let $V$ be a finite dimensional vector space over a field $k$. Then a **bilinear form** is a mapping

$$\langle \ , \ \rangle : V \times V \to k$$

that is linear in both coordinates. We say that $\langle \ , \ \rangle$ is **nondegenerate** if

$$V^\perp = \{ x \in V \mid \langle x, y \rangle = 0 \ \forall \ y \in V \} = 0.$$ 

A **quadratic form** is a mapping

$$q : V \to k$$

such that $q(\lambda x) = \lambda^2 q(x)$ for all $x \in V$, $\lambda \in k$. This uniquely determines a bilinear form

$$\langle x, y \rangle = q(x + y) - q(x) - q(y).$$
Quadratic Forms

Notice that

\[ \langle x, x \rangle = q(x + x) - q(x) - q(x) \]
\[ = q(2x) - 2q(x) \]
\[ = 4q(x) - 2q(x) \]
\[ = 2q(x) \]

When the characteristic is not 2, the associated symmetric bilinear form defines the quadratic form. If \( k \) has characteristic 2, then \( \langle x, x \rangle = 0 \) for all \( x \in V \). Thus \( \langle , \rangle \) is alternate and symmetric, and the quadratic form cannot be recovered from the bilinear form.
Quadratic Forms

Notice that

$$\langle x, x \rangle = q(x + x) - q(x) - q(x)$$
$$= q(2x) - 2 q(x)$$
$$= 4 q(x) - 2 q(x)$$
$$= 2 q(x)$$

When the characteristic is not 2, the associated symmetric bilinear form defines the quadratic form. If $k$ has characteristic 2, then $\langle x, x \rangle = 0$ for all $x \in V$. Thus $\langle , \rangle$ is alternate and symmetric, and the quadratic form cannot be recovered from the bilinear form.

A vector $x$ is called **isotropic** if $q(x) = 0$, and **anisotropic** otherwise.
Algebras

An algebra $A$ over a field $k$ is a vector space equipped with a multiplication which is not necessarily associative:

$$x(yz) \neq (xy)z$$

or commutative:

$$xy \neq yx.$$
Algebras

An algebra $A$ over a field $k$ is a vector space equipped with a multiplication which is not necessarily associative:

$$x(yz) \neq (xy)z$$

or commutative:

$$xy \neq yx.$$  

Examples:
- The complex numbers over (Complex multiplication).
- Euclidean 3-space (Cross product).
- Lie algebras (Lie bracket).
- Jordan Algebras (Jordan multiplication).

Jordan algebras are commutative.
Composition Algebras

A composition algebra $C$ is an algebra over a field together with a quadratic form which admits composition:

$$q(xy) = q(x) q(y).$$

Composition algebras may or may not be associative.
Composition Algebras

A composition algebra $C$ is an algebra over a field together with a quadratic form which admits composition:

$$q(xy) = q(x)q(y).$$

Composition algebras may or may not be associative.

A subalgebra $D$ of a composition algebra $C$ is a linear subspace which is nonsingular, closed under multiplication, and contains the identity element $e$. (A subspace is nonsingular if the restriction of $\langle , \rangle$ is nondegenerate.)
Composition Algebras

A composition algebra $C$ is an algebra over a field together with a quadratic form which admits composition:

$$q(xy) = q(x)q(y).$$

Composition algebras may or may not be associative.

A subalgebra $D$ of a composition algebra $C$ is a linear subspace which is nonsingular, closed under multiplication, and contains the identity element $e$. (A subspace is nonsingular if the restriction of $\langle \ , \ \rangle$ is nondegenerate.)

Notice that, so far, there has been no restriction made on the dimension of a composition algebra.
Doubling

Let $C$ be a composition algebra, and let $D$ be a finite-dimensional subalgebra. Then $D$ is a nonsingular subspace, so $C = D \oplus D^\perp$, and $D^\perp$ is also nonsingular.

**Lemma**

*If $D$ is a finite-dimensional proper subalgebra of $C$, then there exists $a \in D^\perp$ so that $q(a) \neq 0$, then $D_1 = D \oplus Da$ is a composition subalgebra.*

Note: the quadratic form, product and conjugation on $D_1$ require attention.
Doubling

Let $C$ be a composition algebra, and let $D$ be a finite-dimensional subalgebra. Then $D$ is a nonsingular subspace, so $C = D \oplus D^\perp$, and $D^\perp$ is also nonsingular.

**Lemma**

If $D$ is a finite-dimensional proper subalgebra of $C$, then there exists $a \in D^\perp$ so that $q(a) \neq 0$, then $D_1 = D \oplus Da$ is a composition subalgebra.

Note: the quadratic form, product and conjugation on $D_1$ require attention.

Also notice that $Da$ and $D$ have the same dimension, so that $D_1$ has twice the dimension of $D$. In other words, we’ve just doubled $D$. 

Lemma

If $C$ is a composition algebra and $D$ is a finite-dimensional proper subalgebra, then $D$ is associative. Moreover, a subalgebra $D \oplus Da$ is associative if and only if $D$ is both associative and commutative.
Doubling

Lemma

If \( C \) is a composition algebra and \( D \) is a finite-dimensional proper subalgebra, then \( D \) is associative. Moreover, a subalgebra \( D \oplus Da \) is associative if and only if \( D \) is both associative and commutative.

Lemma

Let \( D \) be a composition algebra, and let \( \lambda \in k^* \), and let \( C = D \oplus D \).

1. If \( D \) is associative, then \( C \) is a composition algebra.
2. \( C \) is associative if and only if \( D \) is commutative and associative.
Differences in Low Dimension

Lemma
Let $C$ be a composition algebra of $k$. If $\text{char}(k) \neq 2$, then $D = ke$ is a composition algebra of dimension 1. A 2-dimensional algebra is obtained by doubling.

If $\text{char}(k) = 2$, then $ke$ is singular, since $\langle e, e \rangle = 0$. (There are no 1-dimensional composition algebras in this case).

In case $\text{char}(k) = 2$, take some $\langle a, e \rangle \neq 0$. Then a 2-dimensional composition algebra is $ke \oplus ka$. In either case, we get a 2-dimensional composition algebra.
Differences in Low Dimension

Lemma

Let $C$ be a composition algebra of $k$. If $	ext{char}(k) \neq 2$, then $D = ke$ is a composition algebra of dimension 1. A 2-dimensional algebra is obtained by doubling.

If $	ext{char}(k) = 2$, then $ke$ is singular, since $\langle e, e \rangle = 0$. (There are no 1-dimensional composition algebras in this case).
Differences in Low Dimension

Lemma

Let $C$ be a composition algebra of $k$. If $\text{char}(k) \neq 2$, then $D = ke$ is a composition algebra of dimension 1. A 2-dimensional algebra is obtained by doubling.

If $\text{char}(k) = 2$, then $ke$ is singular, since $\langle e, e \rangle = 0$. (There are no 1-dimensional composition algebras in this case).

In case $\text{char}(k) = 2$, take some $\langle a, e \rangle \neq 0$. Then a 2-dimensional composition algebra is $ke \oplus ka$. 
Differences in Low Dimension

Lemma

Let $C$ be a composition algebra of $k$. If $\text{char}(k) \neq 2$, then $D = ke$ is a composition algebra of dimension 1. A 2-dimensional algebra is obtained by doubling.

If $\text{char}(k) = 2$, then $ke$ is singular, since $\langle e, e \rangle = 0$. (There are no 1-dimensional composition algebras in this case).

In case $\text{char}(k) = 2$, take some $\langle a, e \rangle \neq 0$. Then a 2-dimensional composition algebra is $ke \oplus ka$.

In either case, we get a 2-dimensional composition algebra.
Structure Theorem

Theorem

*Every composition algebra is obtained by repeated doubling, starting from $ke$ if $\text{char}(k) \neq 2$ or from the 2-dimensional algebra if $\text{char}(k) = 2$. In this way, we obtain algebras of dimensions 1 (if $\text{char}(k) \neq 0$), 2, 4, and 8. So we have a sequence*

$$D_1 \subset D_2 \subset D_3.$$
Structure Theorem

**Theorem**

*Every composition algebra is obtained by repeated doubling, starting from $k e$ if $\text{char}(k) \neq 2$ or from the 2-dimensional algebra if $\text{char}(k) = 2$. In this way, we obtain algebras of dimensions 1 (if $\text{char}(k) \neq 0$), 2, 4, and 8. So we have a sequence

$$D_1 \subset D_2 \subset D_3.$$*

Using the lemmas, and since $D_1$ is commutative and associative, we have that $D_2$ is associative. However, $D_2$ is not commutative.
Structure Theorem

Theorem

Every composition algebra is obtained by repeated doubling, starting from $k e$ if $\text{char}(k) \neq 2$ or from the 2-dimensional algebra if $\text{char}(k) = 2$. In this way, we obtain algebras of dimensions 1 (if $\text{char}(k) \neq 0$), 2, 4, and 8. So we have a sequence

$$D_1 \subset D_2 \subset D_3.$$ 

Using the lemmas, and since $D_1$ is commutative and associative, we have that $D_2$ is associative. However, $D_2$ is not commutative. (This fact is not completely obvious).
Structure Theorem

Theorem

Every composition algebra is obtained by repeated doubling, starting from $k e$ if $\text{char}(k) \neq 2$ or from the 2-dimensional algebra if $\text{char}(k) = 2$. In this way, we obtain algebras of dimensions 1 (if $\text{char}(k) \neq 0$), 2, 4, and 8. So we have a sequence

$$D_1 \subset D_2 \subset D_3.$$  

Using the lemmas, and since $D_1$ is commutative and associative, we have that $D_2$ is associative. However, $D_2$ is not commutative. (This fact is not completely obvious).

So $D_3$ is not associative, and thus no algebra properly contains $D_3$. So we are done.
Types of Compositions Algebras

A composition algebra $C$ is called **split** if $q$ is isotropic. If $q$ is anisotropic, then the composition algebra is called **division**. Split algebras over the same field are isomorphic.
Types of Compositions Algebras

A composition algebra $C$ is called **split** if $q$ is isotropic. If $q$ is anisotropic, then the composition algebra is called **division**. Split algebras over the same field are isomorphic.

In the split case, the four dimensional composition composition algebra is isomorphic to the $2 \times 2$ matrices over $k$ with the determinant as the quadratic form.
Types of Compositions Algebras

A composition algebra $C$ is called **split** if $q$ is isotropic. If $q$ is anisotropic, then the composition algebra is called **division**. Split algebras over the same field are isomorphic.

In the split case, the four dimensional composition algebra is isomorphic to the $2 \times 2$ matrices over $k$ with the determinant as the quadratic form.

The 4-dimensional composition algebras are called **quaternion** algebras, and the 8-dimensional algebras are called **octonion** algebras.
Types of Compositions Algebras

A composition algebra $C$ is called **split** if $q$ is isotropic. If $q$ is anisotropic, then the composition algebra is called **division**. Split algebras over the same field are isomorphic.

In the split case, the four dimensional composition algebra is isomorphic to the $2 \times 2$ matrices over $k$ with the determinant as the quadratic form.

The 4-dimensional composition algebras are called **quaternion** algebras, and the 8-dimensional algebras are called **octonion** algebras.

It is known that all quaternion and octonion algebras are split when taken over a perfect field $k$ of characteristic 2.
Automorphism Group

Let $C$ be an octonion algebra. The automorphisms of $C$ that fix a quaternion subalgebra $D$ form a group isomorphic to $G_2$. That is,

\[ \text{Aut}(C) \cong G_2. \]
Automorphism Group

Let $C$ be an octonion algebra. The automorphisms of $C$ that fix a quaternion subalgebra $D$ form a group isomorphic to $G_2$. That is,

$$\text{Aut}(C) \simeq G_2.$$ 

Springer & Veldkamp show that every automorphism $g \in \text{Aut}(C)$ has the form

$$g(x + yu) = cx c^{-1} + (pcyc^{-1})u,$$

where $w \in D^\perp$, $q(w) \neq 0$, $q(p) = 1$, and $q(c) \neq 0$. Here $x, y, c$ and $p \in D$ and $u \in D^\perp$. 
Automorphism Group

Let $C$ be an octonion algebra. The automorphisms of $C$ that fix a quaternion subalgebra $D$ form a group isomorphic to $G_2$. That is,

$$\text{Aut}(C) \simeq G_2.$$ 

Springer & Veldkamp show that every automorphism $g \in \text{Aut}(C)$ has the form

$$g(x + yu) = cx c^{-1} + (pcyc^{-1})u,$$

where $w \in D^\perp$, $q(w) \neq 0$, $q(p) = 1$, and $q(c) \neq 0$. Here $x, y, c$ and $p \in D$ and $u \in D^\perp$.

Also, every automorphism of $G_2$ is inner.
Some Preliminary Results

Theorem

Let $C$ be an octonion algebra. If $k$ is a perfect field of characteristic 2, there is one isomorphism class of inner $k$-involutions of $\text{Aut}(C)$. In this case, the fixed-point group of an inner $k$-involution is isomorphic to

$$\text{SL}_2(k) \times G_a(k)$$
Some Preliminary Results

Theorem

Let $C$ be an octonion algebra. If $k$ is a perfect field of characteristic 2, there is one isomorphism class of inner $k$-involutions of $\text{Aut}(C)$. In this case, the fixed-point group of an inner $k$-involution is isomorphic to

$$\text{SL}_2(k) \times \text{Ga}(k)$$

For the non-split case, when $k$ is not a perfect field of characteristic 2, we don’t know yet.
Some Preliminary Results

Theorem

Let $C$ be an octonion algebra. If $k$ is a perfect field of characteristic 2, there is one isomorphism class of inner $k$-involutions of $\text{Aut}(C)$. In this case, the fixed-point group of an inner $k$-involution is isomorphic to

$$\text{SL}_2(k) \times G_a(k)$$

For the non-split case, when $k$ is not a perfect field of characteristic 2, we don’t know yet.

Question: Are there always elements of order 2 in a division quaternion algebra?
Thank you!

Questions?