Octonions

Let $k$ be a field, with $\text{char}(k) \neq 2$. For example, $k$ may be $\mathbb{Q}$ or $\mathbb{R}$ or $\mathbb{C}$ (though the last case is not as interesting). A Hurwitz algebra over $k$ is a finite-dimensional, $k$-algebra $A$ with unit element, together with a quadratic form $N : A \to k$, such that the associated bilinear form is nondegenerate and:

$$N(xy) = N(x)N(y), \text{ for all } x, y \in A.$$ 

Every Hurwitz algebra over $k$ has dimension 1, 2, 4, or 8, as a $k$ vector space.

In what follows, we write $k, K, B, C$ for Hurwitz algebras of dimensions 1, 2, 4, 8 respectively; $K$ is called a quadratic étale $k$-algebra, $B$ is called a quaternion algebra over $k$, and $C$ is called a Cayley or octonion algebra over $k$.

Hurwitz algebras become more pathological as their dimension rises: quadratic étale algebras are commutative and associative. However, quaternion algebras are associative but never commutative. Cayley algebras are neither commutative nor associative. However, Cayley algebras are alternative, so that for any two elements $x, y \in C$, the algebra generated by $x$ and $y$ is associative (e.g., $(xy)x = x(yx)$).

There are exactly two complete chains of Hurwitz algebras over the real numbers $\mathbb{R}$. First is the sequence $\mathbb{R} \subset \mathbb{C} \subset \mathbb{H} \subset \mathbb{O}$, where, $\mathbb{C}$ denotes the complex numbers, $\mathbb{H}$ Hamilton’s quaternions, and $\mathbb{O}$ Graves’s octonions. The other complete chain of Hurwitz algebras over $\mathbb{R}$ is $\mathbb{R} \subset \mathbb{R} \times \mathbb{R} \subset M_2(\mathbb{R}) \subset \mathbb{O}_{spl}$, where $\mathbb{R} \times \mathbb{R}$ denotes the algebra of ordered pairs of real numbers (multiplication entry-wise), $M_2(\mathbb{R})$ denotes the two-by-two matrix algebra, and $\mathbb{O}_{spl}$ denotes the “split octonions”, which we discuss next.

For any field $k$ (or even a commutative ring!), Zorn’s algebra of split octonions over $k$ is defined to be the set of all two-by-two “matrices”: 

$$\omega = \{ \begin{pmatrix} a & \bar{v} \\ \bar{w} & d \end{pmatrix} : a, d \in k, \bar{v}, \bar{w} \in k^3 \},$$

with composition given by the following formula:

$$\begin{pmatrix} a & \bar{v} \\ \bar{w} & d \end{pmatrix} \cdot \begin{pmatrix} \alpha & \bar{\phi} \\ \bar{\psi} & \delta \end{pmatrix} = \begin{pmatrix} a\alpha + \bar{v} \cdot \bar{\phi} & a\bar{\phi} + d\bar{v} - \bar{w} \times \bar{\psi} \\ a\bar{\psi} + d\bar{v} + \bar{v} \times \bar{\phi} & d\delta + \bar{w} \cdot \bar{\phi} \end{pmatrix}.$$
Automorphisms and Embeddings

Let us fix a base field \( k \) (\( \text{char}(k) \neq 2 \)), and a complete chain of Hurwitz algebras \( k \subset K \subset B \subset C \). One may consider the groups of \( k \)-linear automorphisms that preserve the algebra structure; this yields groups:

\[
\text{Aut}(k/k), \text{Aut}(K/k), \text{Aut}(B/k), \text{Aut}(C/k).
\]

The group \( \text{Aut}(k/k) \) is trivial, and the automorphism \( \text{Aut}(K/k) = \{1, \sigma\} \), where \( \sigma(a) = \bar{a} \) for all \( a \in K \). The groups \( \text{Aut}(B/k) \) and \( \text{Aut}(C/k) \) are more complicated.

Suppose, for example, that \( B = M_2(k) \) is the “split quaternion algebra”. If \( g \in GL_2(k) \), then define the inner automorphism \( \text{Int}_g \) by:

\[
\text{Int}_g(b) = gbg^{-1}, \text{ for all } b \in B.
\]

Then, \( \text{Int} \) is a homomorphism from \( GL_2(k) \) to \( \text{Aut}(B/k) \). Furthermore, if \( z \in Z(GL_2(k)) \) is a scalar matrix, then \( \text{Int}[z] = 1 \). Conversely, if \( g \in GL_2(k) \), and \( \text{Int}[g] = 1 \), then \( g \) commutes with every \( b \in B \), and hence \( g \in Z(GL_2(k)) \). It follows that \( \text{Int} \) descends to a unique injective homomorphism:

\[
\text{Int}: \text{PGL}_2(k) = GL_2(k)/k^\times \hookrightarrow \text{Aut}(B/k).
\]

Conversely, if \( \alpha \in \text{Aut}(B/k) \), then \( \alpha \) is determined by the resulting linear automorphism \( \alpha_0 \) of the trace-zero subspace \( B_0 \subset B \). Moreover, \( \alpha_0 \) preserves the norm quadratic form \( N \) on \( B_0 \), so that \( \text{Aut}(B/k) \) embeds into \( O(B_0, N) \). In fact, a bit more work shows that:

\[
\text{PGL}_2(k) \cong \text{Aut}(B/k) \cong SO(B_0, N).
\]

**Automorphisms of Cayley algebras** are more complicated than automorphisms of quaternion algebras. An automorphism \( \alpha \) of (for example, the split) Cayley algebra \( C \) restricts to a linear, norm-preserving, automorphism \( \alpha_0 \) of the seven-dimensional trace-zero subspace \( C_0 \). Furthermore, \( \alpha \) is determined from \( \alpha_0 \).

This provides an embedding \( \text{Aut}(C/k) \hookrightarrow O(C_0, N) \).

The resulting group \( \text{Aut}(C/k) \) is not easy to describe, but has another name:

\[
G_{2,C} = \text{Aut}(C/k).
\]

The answer to the title of this lecture is: \( G_2 \) is the automorphism group of a Cayley (a.k.a. octonion algebra); which Cayley algebra and which base field should be made clear.

---

4 It would not be too harmful to consider the chain

\[
\mathbb{R} \subset \mathbb{R} \times \mathbb{R} \subset M_2(\mathbb{R}) \subset O_{gr}.
\]

5 Since every element \( a \) of a Hurwitz algebra satisfies a quadratic identity \( a^2 = \text{Tr}(a) + N(a) = 0 \), it can be seen that the algebra structure determines the quadratic form \( N \), the trace map \( \text{Tr} \), and hence the involution \( a = \text{Tr}(a) - a \).

6 The same methods work for nonsplit quaternion algebras as well; every automorphism of a quaternion algebra is inner, yielding an isomorphism from \( B^+/Z(B^+) \) to \( \text{Aut}(B/k) \). Indeed, every quaternion algebra splits over a Galois extension, and so descent applies to prove that \( \text{Int} \) is an isomorphism.

7 To show that the image of \( \text{Aut}(B/k) \) in \( O(B, N) \) is contained in \( SO(B, N) \), one must check that no automorphism of \( B \) acts as a reflection of \( B \). A reflection would preserve two orthogonal vectors \( x, y \in B \), and send a third vector \( z \) to its negative. But, a basis of \( B \) as a \( k \)-vector space is given by \( x, y, (xy - g) \), so that the action of an algebra automorphism \( a \) on \( B \), is uniquely determined by its action on \( x \) and \( y \). In particular, if \( a \) fixes \( x \) and \( y \), then \( a \) fixes \( z \). This demonstrates that \( \text{Aut}(B/k) \) injectively maps to \( SO(B, N) \). For surjectivity, a dimension argument suffices.
Subgroups of Automorphisms

Given a complete chain $k \subset K \subset B \subset C$ of Hurwitz algebras over $k$, we have considered groups:

$$Aut(k/k), \ Aut(K/k), \ Aut(B/k), \ Aut(C/k),$$

each arguably more interesting than the previous. The only group which is “really new” is $Aut(C/k)$. To “know” the group $Aut(C/k)$, it is most helpful to understand its subgroups. Two subgroups which arise most generally are $Aut(C/K)$ and $Aut(C/B)$: the algebra automorphisms of $C$, which fix every element of $K$ or of $B$, respectively.

First, let us consider $\alpha \in Aut(C/K)$; such an automorphism $\alpha$ preserves every element of the $k$-subspace $K$, and preserves the norm and trace, and hence stabilizes the subspace $K^\perp$ of elements orthogonal to $K$:

$$K^\perp = \{ \omega \in C : Tr(\omega \bar{z}) = 0 \text{ for all } z \in K \}.$$  The alternative property of $C$ implies that $K^\perp$ is a (left) $K$-module: in particular,

$$\omega \in K^\perp, \ z \in K \Rightarrow z \cdot \omega.$$

Now, every element of $C$ can be expressed uniquely as a sum $z + \omega$ (or ordered pair $(z, \omega)$), where $z \in K$ and $\omega \in K^\perp$. There is a unique Hermitian form $\Phi: K^\perp \times K^\perp \rightarrow K$, such that:

$$\text{proj}_K((z, \omega) \cdot (z', \omega')) = (zz' - \Phi(\omega, \omega')).$$

It follows that every automorphism $\alpha \in Aut(C/K)$ preserves this Hermitian form. More precisely, one arrives at an injective homomorphism $Aut(C/K) \hookrightarrow U(K^\perp, \Phi)$. The most precise possible result is that, in fact, $Aut(C/K)$ is isomorphic to the group $SU(K^\perp, \Phi)$.

A very good example of $Aut(C/K)$ is provided by Zorn’s split octonions, and the algebra $K = k \times k$ embedded as the diagonal matrices. Then we find that:

$$K^\perp = \left\{ \begin{pmatrix} 0 & \bar{v} \\
 v & 0 \end{pmatrix} : \bar{v}, \bar{v} \in k^3 \right\}.$$  

One can verify that $SU(K^\perp, \Phi)$ is isomorphic to $SL_3(k)$. Specifically, if $g \in SL_3(k)$, then the action of $g$ on $C$ is given by:

$$g \left( \begin{array}{cc} a & \bar{v} \\
 \bar{w} & d \end{array} \right) = \left( \begin{array}{cc} a \bar{g}^{-1} & \bar{g} \bar{v} \\
 g \bar{w} & d \end{array} \right).$$

This yields the long root embedding

$$e_{long}: SL_3(k) \hookrightarrow G_{2,C}.$$  

\[ ^8 \text{A good reference for automorphisms of Cayley algebras is Jacobson's Composition algebras and their automorphisms, Rend. Circ. Mat. Palermo 1958.} \]

\[ ^9 \text{The nontrivial fact is that if } z, w \in K, \text{ and } \omega \in C, \text{ then } z \cdot (w \cdot \omega) = (z \cdot w) \cdot \omega. \text{ But the alternative property implies that such a triple } z, w, \omega \text{ lie in an associative subalgebra of } C. \]

\[ ^{10} \text{For all } z, z' \in K, \text{ and } \omega, \omega' \in K^\perp, \Phi(\omega z, z' \omega') = zz' \Phi(\bar{\omega}, \omega'). \]

Here, we identify $K^\perp$ with $k^3 \times k^3$, with $k^3$, when $K = k \times k$. Note that “conjugation” in $K$ is given by $\bar{z} = (y, x)$ if $z = (x, y)$. If $z = (z_1, z_2, z_3) \in K^3$ and $\bar{w} = (w_1, w_2, \bar{w}_3) \in K^3$, then the Hermitian form is given by:

$$\Phi(\bar{z}, \bar{w}) = z_1 \bar{w}_1 + z_2 \bar{w}_2 + z_3 \bar{w}_3.$$
Quaternion subalgebras

One may also consider the automorphisms \( \text{Aut}(C/B) \) fixing every element of the quaternion algebra \( B \). Since \( K \subset B \), we find that \( \text{Aut}(C/B) \subset \text{Aut}(C/K) \). As in the case of quadratic subalgebras, we may consider the orthogonal complement \( B^\perp \) of \( B \) in \( C \). There exists an element \( \ell \in B^\perp \), such that every element of \( C \) has the form \( a + b\ell \), for some \( a, b \in B \). Moreover, if \( \alpha \in \text{Aut}(C/B) \), then it is a theorem that there exists a unique element \( u_\alpha \in B \) such that \( N(u_\alpha) = 1 \) and

\[
\alpha(a + b\ell) = a + (u_\alpha b)\ell, \quad \text{for all } a, b \in B.
\]

This provides an isomorphism:

\[
\text{Aut}(C/B) \cong SB^\times = \{ u \in B^\times : N(u) = 1 \}.
\]

When \( B = M_2(k), SB^\times = \text{SL}_2(k) \), providing the highest root embedding \( e_{\text{high}} : \text{SL}_2(k) \hookrightarrow G_{2,C} \). Of course, since \( \text{Aut}(C/B) \subset \text{Aut}(C/K) \), the image of \( e_{\text{high}} \) is contained in the image of \( e_{\text{long}} \).

Another embedding of \( SB^\times \) into \( G_{2,C} \) follows: if \( g \in SB^\times \), and \( a + b\ell \in C \), define:

\[
g(a + b\ell) = (gag^{-1}) + (bg^{-1})\ell.
\]

This defines the short root embedding \( e_{\text{short}} : \text{SL}_2(k) \hookrightarrow G_{2,C} \). Observe that the images of \( e_{\text{high}} \) and \( e_{\text{short}} \) commute\(^{11} \), and their intersection consists of \( \{ \pm 1 \} \subset SB^\times \). This provides the embedding:\(^{12} \)

\[
e_{\text{high}} \times e_{\text{long}} : SB^\times \times \pm_1 SB^\times \hookrightarrow G_{2,C}.
\]

Suppose \( C \) is Zorn’s split Cayley algebra. If \( \tau \) is a cyclic permutation of \( \{1, 2, 3\} \), then \( \tau \) naturally acts (by permuting basis elements) on \( k^3 \). This yields an automorphism:

\[
\tau \left( \begin{array}{ccc} a & \bar{v} \\ \bar{w} & d \end{array} \right) = \left( \begin{array}{ccc} a & \tau \bar{v} \\ \tau \bar{w} & d \end{array} \right).
\]

We find an embedding \( w : A_3 \hookrightarrow G_{2,C} \) in this way.

There are three ways of embedding \( M_2(k) \) into the split Cayley algebra \( C \), via:

\[
\ell_i \left( \begin{array}{cc} a & b \\ c & d \end{array} \right) = \left( \begin{array}{cc} a & be_i \\ ce_i & d \end{array} \right),
\]

where \( (e_1, e_2, e_3) \) is the standard basis of \( k^3 \). Altogether, we find three conjugate embeddings:

\[
e_{\text{short},i} : \text{SL}_2(k) \hookrightarrow G_{2,C}.
\]

In fact, \( G_{2,C} \) is generated by the images:

\[
e_{\text{short},i}(\text{SL}_2(k)), e_{\text{long}}(\text{SL}_3(k)).
\]