WHAT IS... G_2?

MARTIN H. WEISSMAN

MARCH 17, 2009

Octonions

Let k be a field, with $char(k) \neq 2$. 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 $N\colon A \to k$, such that the associated bilinear form is nondegenerate and:

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

Resulting structures on a Hurwitz algebra A include a trace,

$$Tr(a) = N(a+1) - N(a) - N(1),$$

and involution $\bar{a} = Tr(a) - a$. Hurwitz algebras are quadratic; every element a satisfies the polynomial

$$a^2 - Tr(a) + N(a) = 0.$$

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

[1] This was first proven over $\mathbb{R}$ by Adolph Hurwitz, in *Über die Composition der quadratischen Formen von beliebig vielen Variablen*, found in Math. Werke I. For a general field, a proof can be found in Irving Kaplansky, *Infinite-dimensional quadratic forms admitting composition*, Proc. Amer. Math. Soc. 4, (1953).

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., $(xy)x = x(yx)$).

Figure 1: A. Hurwitz (1859-1919), conducting, while his daughter plays violin with A. Einstein. Taken from David Rowe's Intelligencer article *Felix Klein, Adolph Hurwitz, and the "Jewish Question" in German academia* (original source, Polya's *Photo Album*).

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. [2] 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.

[2] A nice historical overview of the quaternions and octonions can be found in the first few pages of Baez's article *The Octonions*, in Bull. A.M.S. Vol. 39, 2001.

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":

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

Max Zorn, 1906–1993, a student of Artin, most famous probably for "Zorn's Lemma", but also active in algebra and analysis. His work on "octonions" can be found in *Theorie der Alternativen Ringe*, Abh. Math. Sem. Hamburgishcen Univ., vol. 8 (1930).

with composition given by the following formula:[3]

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

[3] Here, we use the standard dot product, cross product, and scalar multiplication.

Automorphisms and Embeddings

Let us fix a base field k ($char(k) \neq 2$), and a complete chain[4] of Hurwitz algebras $k \subset K \subset B \subset C$. One may consider the groups of k-linear automorphisms that preserve the algebra structure[5]; this yields groups:

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

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

Suppose, for example, that $B = M_2(k)$ is the "split quaternion algebra"[6]. If $g \in GL_2(k)$, then define the **inner automorphism** $Int[g]$ by:

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

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

$$\overline{Int}\colon PGL_2(k) = GL_2(k)/k^\times \hookrightarrow Aut(B/k).$$

Conversely, if $\alpha \in Aut(B/k)$, then α is determined by the resulting linear automorphism $\alpha_\circ$ of the trace-zero subspace $B_\circ \subset B$. Moreover, $\alpha_\circ$ preserves the norm quadratic form N on $B_\circ$, so that $Aut(B/k)$ embeds into $O(B_\circ, N)$. In fact, a bit more work[7] shows that:

$$PGL_2(k) \cong Aut(B/k) \cong SO(B_\circ, N).$$

AUTOMORPHISMS OF CAYLEY ALGEBRAS are more complicated than automorphisms of quaternion algebras. An automorphism α of (for example, the split) Cayley algebra C restricts to a linear, norm-preserving, automorphism $\alpha_\circ$ of the seven-dimensional trace-zero subspace $C_\circ$. Furthermore, α is determined from $\alpha_\circ$. This provides an embedding $Aut(C/k) \hookrightarrow O(C_\circ, N)$.

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

$$G_{2,C} = Aut(C/k).$$

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

$$\mathbb{R} \subset \mathbb{R} \times \mathbb{R} \subset M_2(\mathbb{R}) \subset \mathbb{O}_{spl}.$$

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

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

[7] To show that the image of $Aut(B/k)$ in $O(B_\circ, N)$ is contained in $SO(B_\circ, N)$, one must check that no automorphism of B acts as a reflection of $B_\circ$. A reflection would preserve two orthogonal vectors x, y in $B_\circ$, and send a third vector z to its negative. But, a basis of $B_\circ$ as a k-vector space is given by $x, y, (xy - \bar{y}\bar{x})$, so that the action of an algebra automorphism α on $B_\circ$ is uniquely determined by its action on x and y. In particular, if α fixes x and y, then α fixes z. This demonstrates that $Aut(B/k)$ injectively maps to $SO(B_\circ, N)$. 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[8]. 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.

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

First, let us consider $\alpha \in Aut(C/K)$; such an automorphism α 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:

$$K^\perp = \{\omega \in C \colon Tr(\omega \bar{z}) = 0 \text{ for all } z \in K\}.$$

The alternative property[9] of C implies that $K^\perp$ is a (left) K-module: in particular,

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

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

Now, every element of C can be expressed uniquely as a sum $z + \omega$ (or ordered pair (z, ω)), where $z \in K$ and $\omega \in K^\perp$. There is a unique Hermitian form[10] $\Phi \colon K^\perp \times K^\perp \to K$, such that:

$$proj_K \left((z, \omega) \cdot (z', \omega') \right) = (zz' - \Phi(\omega, \omega')).$$

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

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:

$$K^\perp = \{ \begin{pmatrix} 0 & \vec{v} \\ \vec{w} & 0 \end{pmatrix} \colon \vec{v}, \vec{w} \in k^3 \}.$$

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 $\vec{z} = (z_1, z_2, z_3) \in K^3$ and $\vec{w} = (w_1, w_2, w_3) \in K^3$, then the Hermitian form is given by:

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

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:

$$g \begin{pmatrix} a & \vec{v} \\ \vec{w} & d \end{pmatrix} = \begin{pmatrix} a & g\vec{v} \\ {}^t g^{-1} \vec{w} & d \end{pmatrix}.$$

This yields the **long root** embedding

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

Quaternion subalgebras

One may also consider the automorphisms $Aut(C/B)$ fixing every element of the quaternion algebra B. Since $K \subset B$, we find that $Aut(C/B) \subset Aut(C/K)$. 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 $\alpha \in Aut(C/B)$, then it is a theorem that there exists a unique element $u_\alpha \in B$ such that $N(u_\alpha) = 1$ and

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

This provides an isomorphism:

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

When $B = M_2(k)$, $SB^{\times} = SL_2(k)$, providing the **highest root** embedding $e_{high} \colon SL_2(k) \hookrightarrow G_{2,C}$. Of course, since $Aut(C/B) \subset Aut(C/K)$, the image of e_{high} is contained in the image of e_{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 $e_{short} \colon SL_2(k) \hookrightarrow G_{2,C}$. Observe that the images of e_{high} and e_{short} commute[11], and their intersection consists of $\{\pm 1\} \subset SB^{\times}$. This provides the embedding:[12]

$$e_{high} \times e_{short} \colon SB^{\times} \times_{\pm 1} SB^{\times} \hookrightarrow G_{2,C}.$$

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

$$\tau \begin{pmatrix} a & \vec{v} \\ \vec{w} & d \end{pmatrix} = \begin{pmatrix} a & \tau\vec{v} \\ \tau\vec{w} & d \end{pmatrix}.$$

We find an embedding $w \colon A_3 \hookrightarrow G_{2,C}$ in this way.

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

$$\iota_i \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} a & be_i \\ ce_i & d \end{pmatrix},$$

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

$$e_{short,i} \colon SL_2(k) \hookrightarrow G_{2,C}.$$

In fact, $G_{2,C}$ is generated by the images:

$$e_{short,i}(SL_2(k)), e_{long}(SL_3(k)).$$

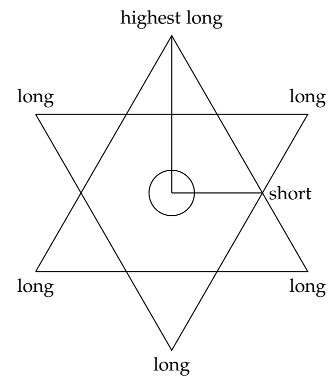

Figure 2: The long roots for G_2. The other six intersection points are short roots.

[11] This reflects the orthogonality of the short root and highest long root in the diagram above

[12] This embedding is very important for the split real Lie group G_2, where B is Hamilton's quaternion algebra and C is the split octonion algebra (such embeddings exist!). There, one finds an embedding $SU_2 \times_{\pm 1} SU_2$ as the maximal compact subgroup of the split Lie group G_2. From this, one finds that the split G_2 is not simply-connected as a topological group; rather, it has a two-fold covering which is simply-connected. This leads to great confusion!