A Group of Order 604800 That's Easy: Octonians, $G_2(q)$ and J_2

David A. Craven

21st February, 2007

In this talk we are going to construct the octonian algebra, both the split form and the compact form, and use it as a vehicle to define the simple groups $G_2(q)$, where q is a prime power. Using $G_2(2)' = \mathrm{PSU}_3(3)$, we construct a simple group J_2 as the automorphism group of a graph on 100 vertices. Finally, we see how the representation theory of the groups $G_2(4)$ and $G_2(2) = \mathrm{PSU}_3(3) : 2$ affects the representation theory of the group J_2, and in particular prove which simple modules for J_2 are non-algebraic, over a field of characteristic 2.

1 Quaternions

In this short section we recap how the quaternions are built up, and try to see how we can generalize this notion. Firstly, let i, j and k be elements, and let

$$\mathbb{H} = \{\alpha + \beta i + \gamma j + \delta k : \alpha, \beta, \gamma, \delta \in \mathbb{R}\},$$

with addition pointwise and multiplication defined on the basis elements by $i^2 = j^2 = k^2 = -1$, $ij = k$, $ki = j$ and $jk = i$, and the other products defined by anticommutativity. To get the multiplication on the whole of $\mathbb{H}$, extend this by linearity. This forms a 4-dimensional non-commutative $\mathbb{R}$-algebra. There is a bijective involution $\bar{\ }$ given by

$$\alpha + \beta i + \gamma j + \delta k \mapsto \alpha - \beta i - \gamma j - \delta k,$$

and a norm given by

$$N(q) = q\bar{q},$$

where $q \in \mathbb{H}$. Notice that $N(q) = \alpha^2 + \beta^2 + \gamma^2 + \delta^2$, where $q = \alpha + \beta i + \gamma j + \delta k$. As a vector space, it has basis $\{1, i, j, k\}$.

We can legitimately replace $\mathbb{R}$ with any field K, except possibly a field of characteristic 2, since $-1 = 1$, which is bad for the definition we have given above. We can thus create a K-algebra of quaternions, $\mathbb{H}_K$. Such an algebra has an automorphism group: since any automorphism fixes 1, it must fix the orthogonal complement, $\langle\{i,j,k\}\rangle$, and since $\{i,j,k\}$ is a collection of vectors of norm 1, $\mathrm{Aut}(\mathbb{H}_K)$ is a subgroup of $\mathrm{O}_3(K)$. In fact, one can check that

$$\mathrm{Aut}(\mathbb{H}_K) = \mathrm{SO}_3(K).$$

These ideas will be applied to the algebra of octonians.

2 Octonians

The octonians can be derived from the quaternions using the Fano plane.

The idea is to make every line into a copy of the quaternions, and every point into a complex number. Notice that every two points lie on a unique line, and so their product can be determined in their enveloping quaternion algebra.

More specifically, let i_j with $1 \leqslant j \leqslant 7$, together with 1, be the elements of a basis for an 8-dimensional real vector space. We will define a multiplication on them by assuming that $\{i_n, i_{n+1}, i_{n+3}\}$ (modulo 8) form a basis for the imaginary quaternions. [Note that i_n, i_{n+1}, i_{n+3} modulo 8, as n varies, gives seven collections of three basis elements, such that any two collections intersect in a unique basis element, and any two basis elements lie inside a unique collection.]

If one needs the basis multiplication written in a table, here it is.

	i_1	i_2	i_3	i_4	i_5	i_6	i_7
i_1	-1	i_4	i_7	$-i_2$	i_6	$-i_5$	$-i_3$
i_2	$-i_4$	-1	i_5	i_1	$-i_3$	i_7	$-i_6$
i_3	$-i_7$	$-i_5$	-1	i_6	i_2	$-i_4$	i_1
i_4	i_2	$-i_1$	$-i_6$	-1	i_7	i_3	$-i_5$
i_5	$-i_6$	i_3	$-i_2$	$-i_7$	-1	i_1	i_4
i_6	i_5	$-i_7$	i_4	$-i_3$	$-i_1$	-1	i_2
i_7	i_3	i_6	$-i_1$	i_5	$-i_4$	$-i_2$	-1

The multiplication is then extended by linearity to the whole vector space. This 8-dimensional vector space, together with this multiplication, becomes an 8-dimensional, non-commutative, non-associative, $\mathbb{R}$-algebra.

The group of units of this algebra, $\{\pm 1, \pm i_j\}$, do not form a group, although this is difficult to see just from the multiplication table. The reason is that this collection is non-associative. However, it does satisfy certain types of associativity laws, which we will come to soon. Before this, we will define a quasigroup and a loop.

A *quasigroup* is a set Q with a binary operation such that if $a, b \in Q$ then there exists unique elements x and y such that $ax = b$ and $ya = b$. Another way of thinking of this is that the multiplication table has as rows and columns permutations of the set Q. A *loop* is a quasigroup with an identity.

If we impose certain conditions about bracketing, we get a Moufang loop. A *Moufang loop* (Ruth Moufang 1905–1977) is a loop that satisfies any one of the three (equivalent) conditions

(i) $(xy)(zx) = (x(yz))x$;

(ii) $x(y(xz)) = ((xy)x)z$; and

(iii) $((xy)z)x = x(y(zx))$.

Again, we can exchange the ground field from $\mathbb{R}$ to any field of characteristic not equal to 2: to deal with the case when the field has characteristic 2, we will have to be sneaky. Before we do this, we will consider the automorphism group of $\mathbb{O}_K$, the algebra of octonians over the field K. (If $K = \mathrm{GF}(q)$, we will also write $\mathbb{O}_q$.

3 The Automorphism Groups

The automorphism group of this non-associative algebra will be referred to as $G_2(K)$, where K is the field over which we are taking our octonians, or $G_2(q)$ when K has order q. It turns out that this is a finite simple group, and is in fact the group of Lie type corresponding to the Dynkin diagram of type G_2 (hence the name).

We will give a brief sketch of how to calculate the order of $G_2(q)$, when q is odd, from the natural 7-dimensional representation. Notice that i_1, i_2 and i_3 generate the entire algebra, so we simply need to determine the images of these elements. The triple (i_1, i_2, i_3) are a set of mutually orthogonal purely imaginary octonians of norm 1, and i_3 is orthogonal to $i_1 i_2$. The idea is to show that $G = G_2(q)$ is transitive on such triples. Then we count such triples.

In fact, we count the number of such triples (i, j, k) first. Let $\varepsilon = \pm 1$ so that $\varepsilon \equiv q \mod 4$. Then i is a vector of norm 1 in the 7-dimensional normed vector space, and so there are $|\operatorname{SO}_7(q)|/|\operatorname{SO}_6^{\varepsilon}(q)| = q^6 + \varepsilon q^3$ choices for i. Next, to choose j, we can pick any vector of norm 1 in the space $\mathrm{O}_6^{\varepsilon}(q)$, so we get $q^5 - \varepsilon q^2$. Lastly, we need to pick k, and it has to be orthogonal to i, j, and ij, so that k has to chosen from a $\mathrm{O}_4^{+}(q)$-space, and there are $q^3 - q$ such vectors.

Putting all of this together, we get

$$|G_2(q)| = q^6(q^6 - 1)(q^2 - 1).$$

It remains to show that G is transitive on all triples (i, j, k) where all elements are mutually orthogonal and ij is orthogonal to k. If i, j, k, and $ij = l$ are purely imaginary norm 1 octonians, then $i^2 = -1$, and so on with all of the others. Secondly, when one multiplies i by j, one gets a series of terms in $i_\alpha i_\beta$, and notice that the co-efficient of $i_\alpha i_\beta$ is the negative of that of $i_\beta i_\alpha$, unless $\alpha = \beta$, in which case the sum over all α is zero (as ij is purely imaginary). Hence $ij = -ji$.

In the expansion of $(ij)k$, the terms that are associative correspond to the real parts of ij, jk, ik or $(ij)k$, and each of these sets of terms individually adds up to 0, so that $(ij)k = -k(ij)$. Finally, $N(xy) = N(x)N(y)$, so that multiplication by a norm 1 octonian preserves norms and inner products. Thus

$$\{1, i, j, ij, k, ik, jk, (ij)k\}$$

is an orthonormal basis for $\mathbb{O}_q$. We can see that all multiplications of elements of $\mathbb{O}_q$ are determined by those of the basis, and so we are done.

4 A Change of Basis

At the moment we can only deal with the cases where the field has odd order. However, there are also groups of Lie type corresponding to G_2 over fields of even characteristic as well. To get an algebra over $\mathrm{GF}(2^n)$, we need to muck about with our basis, to get one that doesn't become commutative in characteristic 2.

If q is odd, then inside $\mathrm{GF}(q)$, there are solutions to the equation $a^2+b^2=-1$ and $b \neq 0$. We will define a basis using a and b.

$$\begin{aligned} 2x_1 &= ai_4 + i_6 + bi_7 & 2x_8 &= -ai_4 + i_6 - bi_7 \\ 2x_2 &= ai_2 + bi_3 + i_5 & 2x_7 &= -ai_2 - bi_3 + i_5 \\ 2x_3 &= -i_1 - bi_4 + ai_7 & 2x_6 &= -i_1 + bi_4 - ai_7 \\ 2x_4 &= 1 - ai_3 + bi_2 & 2x_5 &= 1 + ai_3 - bi_2 \end{aligned}$$

With respect to this basis, we have the multiplication as given below.

	x_1	x_2	x_3	x_4	x_5	x_6	x_7	x_8
x_1	0	0	0	0	x_1	$-x_2$	x_3	$-x_4$
x_2	0	0	x_1	x_2	0	0	$-x_5$	$-x_6$
x_3	0	$-x_1$	0	x_3	0	$-x_5$	0	x_7
x_4	x_1	0	0	x_4	0	x_6	x_7	0
x_5	0	x_2	x_3	0	x_5	0	0	x_8
x_6	x_2	0	$-x_4$	0	x_6	0	$-x_8$	0
x_7	$-x_3$	$-x_4$	0	0	x_7	x_8	0	0
x_8	$-x_5$	x_6	$-x_7$	x_8	0	0	0	0

Since $a^2+b^2=-1$ has no solutions in the real numbers, the algebra generated by the x_j is *not* isomorphic with the traditional, *compact form* of the octonians: this form is called the *split form.*

With this action we can now define an algebra in characteristic 2. The automorphism group, $G_2(2^n)$, is both simple, and has the same order as its odd counterparts, $q^6(q^6-1)(q^2-1)$.

5 The Group J_2

The group $\mathrm{PSU}_3(3)$ is a permutation group on 28 points, or is a matrix group of 3×3 unitary matrices, generated by

$$\begin{pmatrix} \omega & 0 & 0 \\ 0 & \omega^2 & 0 \\ 0 & 0 & \omega^5 \end{pmatrix} \text{ and } \begin{pmatrix} \omega^5 & -1 & 1 \\ -1 & -1 & 0 \\ 1 & 0 & 0 \end{pmatrix}.$$

It has a single conjugacy class of involutions, $\mathscr{I}$, totalling some 63 members. It also has a single conjugacy class of 36 maximal subgroups $\mathscr{H}$, isomorphic with $\mathrm{SL}_3(2)$, a element of which is given by

$$H = \left\langle \begin{pmatrix} w^5 & w^2 & 1 \\ \omega & 0 & \omega^6 \\ 2 & \omega^3 & \omega^7 \end{pmatrix}, \begin{pmatrix} \omega^6 & 0 & 2 \\ \omega^6 & 2 & 2 \\ \omega^5 & 1 & \omega \end{pmatrix} \right\rangle .$$

We produce a graph Γ, consisting of a hundred vertices, $\{\star\}\cup\mathscr{I}\cup\mathscr{H}$, where $\star$ is connected to every vertex in $\mathscr{H}$, two elements of $\mathscr{I}$ are connected if their product has order 4, two elements of $\mathscr{H}$ are connected if their intersection is S_4, and joining an element of $\mathscr{I}$ to and element of $\mathscr{H}$ whenever the subgroup contains the involution. Let G denote the group of automorphisms of this graph. It can be thought of as a permutation group on 100 points. We need $|G|$: since G is transitive on Γ (not obvious), we simply need the size of a vertex stabilizer, which is $\mathrm{PSU}_3(3) : 2$. Hence $|G| = 1209600$.

[There is an odd permutation: if one fixes a point in the 36-orbit, it breaks up as $1+7+7+21$ under the action of $\mathrm{SL}_3(2)$, and the 63-orbit breaks up as three 21-orbits. There is a symmetry in $\mathrm{SL}_3(2)$ that fixes the 7-orbits pointwise, swaps the four 21-orbits in pairs, and commutes with the action of $\mathrm{SL}_3(2)$.]

This action is not contained within A_{100}, and so we see that G has a subgroup of index 2. It is this group that we will denote by J_2.

By construction, J_2 contains a (maximal) subgroup isomorphic with $\mathrm{PSU}_3(3) = G_2(2)'$. Also, J_2 is contained as a maximal subgroup in $G_2(4)$. This 'sandwiching' considerably restricts its representation theory. Here is the table of J_2's simple modules in characteristic 2.

Block	Simple Modules	Defect Group
1	$\{1, 6_1, 6_2, 14_1, 14_2, 36, 84\}$	Sylow
2	$\{64_1, 64_2, 160\}$	Defect 2

Each of these simple modules, with the exception of the 160-dimensional module, is the restriction of a simple module for $G_2(4)$. To finish off, there is a 196-dimensional representation of $G_2(4)$ that restricts to the direct sum of the 160-dimensional representation and the 36-dimensional representation.

Now let us go in the opposite direction, restricting J_2-modules down to $\mathrm{PSU}_3(3) = G_2(2)'$. Firstly, we need a table of $\mathrm{PSU}_3(3)$-modules.

Block	Simple Modules	Defect Group
1	$\{1, 6, 14\}$	Sylow
2,3	$\{32\}$, $\{32^*\}$	Defect 0

The two 6-dimensional modules for J_2 have simple restriction, as do the two 14-dimensional modules. The two 64-dimensional modules have semisimple restriction. The 36- and 160-dimensional modules have complicated restriction, and the 84-dimensional module restricts to the two 32-dimensionals plus a 20-dimensional uniserial module, with socle layers 6, K, 6, K, 6.

We can now quite easily read off facts about J_2 from this: the three modules in the unique block of defect V_4 are all algebraic, by general results that will be published at some point. The 6- and 14-dimensional modules for $\mathrm{PSU}_3(3)$ are both non-algebraic, and so therefore are all except perhaps for the 36- and 84-dimensional modules for J_2. These two can easily be dealt with by restricting down to a V_4-subgroup and applying the fact that an indecomposable V_4-module is algebraic if and only if it is trivial or even-dimensional. Hence we get the following theorem.

Theorem 5.1 Let $G = J_2$, and let M be a simple KG-module, where K is a splitting field of characteristic 2. Then M is algebraic if and only if M is trivial or M lies in a block of defect V_4.