Chapter 4

The exceptional groups

4.1 Introduction

It is the aim of this Chapter to describe some of the ten families of so-called 'exceptional groups of Lie type'. There are three main ways to approach these groups. The first is via Lie algebras, as is wonderfully developed in Carter's book 'Simple groups of Lie type'. The second, more modern, approach is via algebraic groups (see for example Geck's book 'Introduction to algebraic geometry and algebraic groups'). The third is via 'alternative' algebras, as in 'Octonions, Jordan algebras and exceptional groups' by Springer and Veldkamp. I shall adopt the 'alternative' approach, for a number of reasons: although it lacks the elegance and uniformity of the other approaches, it gains markedly when it comes to performing concrete calculations. We obtain not only the smallest representations in this way, but also construct the (generic) covering groups, whereas the Lie algebra approach only constructs the simple groups.

The ten families of exceptional groups are (from the Lie algebra point of view) of three different types. Most straightforward are the five families of Chevalley (or untwisted) groups $G_2(q)$, $F_4(q)$, and $E_n(q)$ for $n = 6, 7, 8$. Next in difficulty are the Steinberg–Tits–Hertzig twisted groups ${}^3D_4(q)$ and ${}^2E_6(q)$ which also exist for any finite field $\mathbb{F}_q$, and whose construction is analogous to the construction of the unitary groups from the special linear groups. Finally there are the three families of Suzuki and Ree groups ${}^2B_2(2^{2n+1}) = \mathrm{Sz}(2^{2n+1})$, ${}^2G_2(3^{2n+1}) = R(3^{2n+1})$ and ${}^2F_4(2^{2n+1}) = R(2^{2n+1})$, which only exist in one characteristic.

4.2 Octonions and groups of type G_2

4.2.1 Quaternions

The quaternion group Q_8 consists of the 8 elements ± 1, $\pm i$, $\pm j$, $\pm k$ and is defined by the presentation

$$\langle i, j, k \mid ij = k, jk = i, ki = j\rangle, \tag{4.1}$$

from which it follows that $i^2 = j^2 = k^2 = -1$ and $ji = -k$, $kj = -i$, $ik = -j$. The (real) quaternion algebra $\mathbb{H}$ (named after Hamilton) consists of all real linear combinations of these elements (where -1 in the group is identified with -1 in $\mathbb{R}$). Thus

$$\mathbb{H} \;=\; \{a + bi + cj + dk : a, b, c, d \in \mathbb{R}\} \tag{4.2}$$

with the obvious addition, and multiplication defined by the above rules and the distributive law. This is a non-commutative algebra which has many applications in physics and elsewhere. Given a quaternion $q = a + bi + cj + dk$ we write $\overline{q} = a - bi - cj - dk$ for the (quaternion) *conjugate* of q, and $\mathrm{Re}\,(q) = a = \frac{1}{2}(q + \overline{q})$ is the *real part* of q. There is a natural norm N under which $\{1, i, j, k\}$ is an orthonormal basis, and this norm satisfies $N(q) = q\overline{q}$.

More generally, we may replace the real numbers in this definition by any field F of characteristic not 2 (fields of characteristic 2 do not work: one difficulty is that $1 = -1$ in the field but $1 \neq -1$ in the group). We obtain in this way a 4-dimensional non-commutative algebra over the field F, and we extend the definitions of $\overline{q}$, $\mathrm{Re}\,(q)$ and $N(q)$ in the obvious way to this algebra.

The group of automorphisms of this algebra must fix the identity element 1, and therefore fixes its orthogonal complement (the *purely imaginary* quaternions, spanned by i, j, k). Therefore it is a subgroup of the orthogonal group $\mathrm{O}_3(F)$, and is in fact isomorphic to the group $\mathrm{SO}_3(F) \cong \mathrm{PGL}_2(F)$. To prove this we simply need to check that if x, y, z are any three mutually orthogonal purely imaginary quaternions of norm 1, then $xy = \pm z$. (Exercise)

Indeed, the automorphism group of the quaternions consists entirely of *inner automorphisms* $\alpha_q : x \mapsto q^{-1}xq$ for invertible $q \in \mathbb{H}$. Since $\alpha_{-q} = \alpha_q$ this gives a 2-to-1 map from the group of quaternions of norm 1 to $\mathrm{SO}_3(F)$. Indeed, this group of quaternions is a double cover of $\mathrm{SO}_3(F)$ and is isomorphic to $\mathrm{SL}_2(F)$.

4.2.2 Octonions

The (real) octonion algebra $\mathbb{O}$ (also known as the Cayley numbers, even though, as Cayley himself admitted, they were first discovered by Graves) can be built from the quaternions by taking 7 mutually orthogonal square roots of -1, labelled $i_0, \ldots, i_6$ (with subscripts understood modulo 7), subject to the condition that for each t, the elements i_t, i_{t+1}, i_{t+3} satisfy the same multiplication rules as i, j, k (respectively) in the quaternion algebra. It is easy to see that this defines all of the multiplication, and that this multiplication is non-associative. For example, $(i_0i_1)i_2 = i_3i_2 = -i_5$ but $i_0(i_1i_2) = i_0i_4 = i_5$. [Strictly speaking, an algebra is associative. We emphasise the generalisation by describing $\mathbb{O}$ as a *non-associative algebra*.]

For reference, here is the multiplication table:

$$\begin{array}{c|ccccccc|}
1 & i_0 & i_1 & i_2 & i_3 & i_4 & i_5 & i_6 \\
\hline
i_0 & -1 & i_3 & i_6 & -i_1 & i_5 & -i_4 & -i_2 \\
i_1 & -i_3 & -1 & i_4 & i_0 & -i_2 & i_6 & -i_5 \\
i_2 & -i_6 & -i_4 & -1 & i_5 & i_1 & -i_3 & i_0 \\
i_3 & i_1 & -i_0 & -i_5 & -1 & i_6 & i_2 & -i_4 \\
i_4 & -i_5 & i_2 & -i_1 & -i_6 & -1 & i_0 & i_3 \\
i_5 & i_4 & -i_6 & i_3 & -i_2 & -i_0 & -1 & i_1 \\
i_6 & i_2 & i_5 & -i_0 & i_4 & -i_3 & -i_1 & -1 \\
\hline
\end{array} \tag{4.3}$$

It is worth pausing for a moment to consider the symmetries of this table. By definition it is invariant under the map $i_t \mapsto i_{t+1}$, and it is easy to check that it is invariant under $i_t \mapsto i_{2t}$, extending the automorphism $i \mapsto j \mapsto k \mapsto i$ of the quaternions (where $i = i_1$, $j = i_2$ and $k = i_4$). It is also invariant under the map

$$(i_0, \ldots, i_6) \quad \mapsto \quad (i_0, i_2, i_1, i_6, -i_4, -i_5, i_3) \tag{4.4}$$

which extends the automorphism $i \leftrightarrow j, k \mapsto -k$ of the quaternions. Ignoring the signs for the moment, we may recognise the permutations $(0, 1, 2, 3, 4, 5, 6)$, $(1, 2, 4)(3, 6, 5)$ and $(1, 2)(3, 6)$ generating $\mathrm{GL}_3(2)$. Thus we have a homomorphism from the group of symmetries onto $\mathrm{GL}_3(2)$. The kernel is a group of order 2^3, since we may change sign independently on i_0, i_1 and i_2, and then the other signs are determined. In fact, the resulting group $2^3\mathrm{GL}_3(2)$ is a non-split extension.

Now the set $\{\pm 1, \pm i_0, \ldots, \pm i_6\}$ is closed under multiplication, but does not form a group, since the associative law fails. In fact it is a *Moufang loop*, which means that it is a *loop* (a set with a multiplication, such that left and right multiplication by a are permutations of the set, and with an identity element) which satisfies the *Moufang laws*

$$\begin{aligned}
(xy)(zx) &= (x(yz))x \\
x(y(xz)) &= ((xy)x)z \text{ and} \\
((xy)z)x &= x(y(zx)).
\end{aligned} \tag{4.5}$$

In the loop, these laws may be verified directly: the symmetries given above reduce the work to checking the single case $x = i_0$, $y = i_1$, $z = i_2$. Since this loop has an identity element 1, the Moufang laws imply the *alternative* laws

$$(xy)x = x(yx)$$

$$\begin{aligned} x(xy) &= (xx)y \text{ and} \\ (yx)x &= y(xx). \end{aligned} \quad (4.6)$$

Indeed, the Moufang laws hold not just in the loop, but also in the algebra: this is not obvious, however, since the laws are not linear in x. It is sufficient to take $y = i_0$, $z = i_1$, and check that the cross terms cancel out in the cases $x = i_2 + i_t$, $t = 3, 4, 5, 6$. It follows from the alternative laws that any 2-generator subalgebra is associative.

Just as with the quaternions, an octonion algebra may be defined by the same rules over any field F of characteristic not 2. There is again a natural norm N, under which $\{1, i_0, \ldots, i_6\}$ is an orthonormal basis, and $N(x) = x\overline{x}$, where $^-$ is the linear map fixing 1 and negating i_0, $\ldots$, i_6. Also we define the real part $\mathrm{Re}\,(x) = \frac{1}{2}(x + \overline{x})$, so that $\overline{x} = 2\mathrm{Re}\,(x) - x$. Since $\overline{xy} = \overline{y}.\overline{x}$, and $\overline{x}$ is expressible as a linear combination of 1 and x, the alternative laws imply immediately that $N(xy) = N(x)N(y)$. The norm N is a quadratic form, and the associated bilinear form is

$$f(x, y) = N(x + y) - N(x) - N(y) \quad (4.7)$$

which is twice the usual inner product. The automorphisms of the algebra again preserve the identity element 1, so live inside the orthogonal group $\mathrm{O}_7(F)$ acting on the purely imaginary octonions. This time, however, it is clearly a proper subgroup of $\mathrm{SO}_7(F)$, since once we know the images of i_0 and i_1, we know the image of $i_3 = i_0 i_1$. Indeed, if we also know the image of i_2, then we know the images of all the basis vectors. This automorphism group is known as $G_2(F)$, or, if F is the field $\mathbb{F}_q$ of q elements, $G_2(q)$.

4.2.3 The order of $G_2(q)$

To calculate the order of $G_2(q)$ in the case q odd, we calculate the number of images under $G_2(q)$ of the list i_0, i_1, i_2 of generators for the algebra. The crux of the matter is to prove that the group is transitive on triples of elements satisfying the obvious properties of the triple (i_0, i_1, i_2), namely that they are mutually orthogonal purely imaginary octonions of norm 1, and that i_2 is orthogonal to $i_0 i_1$. We do this by showing that the multiplication is completely determined by these properties.

First, if i, j, $k = ij$ and l are mutually orthogonal norm 1 pure imaginary octonions, then $i^2 = -i.\overline{i} = -1$; second, all terms in the expansion of ij anticommute, except the terms in $i_n.i_n$, which commute and sum to 0 (since i is orthogonal to j), so that $ij = -ji$; and third, in the expansion of $(ij)l$, the terms which are associative correspond to the real parts of ij, jl, il or kl, and each of these sets of terms individually adds up to 0, so that $(ij)l = -i(jl)$. Since $N(xy) = N(x)N(y)$, multiplication by an octonion of norm 1 preserves norms, and therefore inner products. Thus we see that $\{1, i, j, ij, l, il, jl, kl\}$ is an orthonormal basis. The entire multiplication table is now determined by these relations, and is visibly the same as given in Equation 4.3.

Now we count the number of such triples (i, j, l): first i can be any vector of norm 1, and the number of such vectors is

$$|\mathrm{SO}_7(q)|/|\mathrm{SO}_6^{\varepsilon}(q)| \quad = \quad q^6 + \varepsilon q^3 = q^3(q^3 + \varepsilon) \tag{4.8}$$

(where $\varepsilon = \pm 1$ satisfies $\varepsilon \equiv q \bmod 4$). Then j can be any vector of norm 1 in the orthogonal space of type $\mathrm{O}_6^{\varepsilon}$, of which there are $q^5 - \varepsilon q^2 = q^2(q^3 - \varepsilon)$. Finally, l can be any vector of norm 1 orthogonal to i, j and $k = ij$, i.e. lying in the O_4^{+}-space spanned by l, il, jl, kl. There are $q^3 - q$ such vectors, so the order of $G_2(q)$ is $q^3(q^3 + \varepsilon).q^2(q^3 - \varepsilon).q(q^2 - 1)$, that is

$$|G_2(q)| = q^6(q^6 - 1)(q^2 - 1). \tag{4.9}$$

4.2.4 Another basis for the octonions

We change basis as follows. First pick elements $a, b \in \mathbb{F}_q$ such that $a^2 + b^2 = -1$ and $b \neq 0$ (this can be done for all odd q). Then our new basis is $\{x_1, \ldots, x_8\}$ defined by

$$\begin{array}{ll} 2x_1 = i_4 + ai_6 + bi_0 & 2x_8 = i_4 - ai_6 - bi_0 \\ 2x_2 = i_2 + bi_3 + ai_5 & 2x_7 = i_2 - bi_3 - ai_5 \\ 2x_3 = i_1 - bi_6 + ai_0 & 2x_6 = i_1 + bi_6 - ai_0 \\ 2x_4 = 1 + ai_3 - bi_5 & 2x_5 = 1 - ai_3 + bi_5 \end{array} \tag{4.10}$$

With respect to the norm N and the associated bilinear form f, the basis vectors are isotropic and mutually perpendicular, except that $f(x_i, x_{9-i}) = 1$. With respect to this new basis we find that all entries in the multiplication table are integers, as follows (where blank entries are 0).

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

(4.11)

This multiplication can now be interpreted over any field whatsoever, for example the real numbers, in which case the resulting algebra is called the *split form* of the octonion algebra: this is not the same as the *compact form* defined in Section 4.2.2, since there are no solutions to $a^2 + b^2 = -1$ in $\mathbb{R}$.

With respect to the basis $\{x_1, \ldots, x_8\}$ more symmetries become apparent. For example it is easy to check that the diagonal matrices which preserve the multiplication are precisely those of shape

$$\mathrm{diag}(\lambda, \mu, \lambda\mu^{-1}, 1, 1, \lambda^{-1}\mu, \mu^{-1}, \lambda^{-1}) \tag{4.12}$$

for any non-zero $\lambda, \mu \in \mathbb{F}_q$. These matrices form the (maximally split) *torus* T, which is normalized by a group $W \cong D_{12}$ generated by the maps

$$\begin{array}{rcl} r : (x_1, \ldots, x_8) & \mapsto & (-x_1, -x_3, -x_2, x_4, x_5, -x_7, -x_6, -x_8), \\ s : (x_1, \ldots, x_8) & \mapsto & (-x_2, -x_1, -x_6, x_5, x_4, -x_3, -x_8, -x_7). \end{array} \tag{4.13}$$

It is left as an Exercise to verify that these maps preserve the multiplication table in (4.11). The product of these two maps is the coordinate permutation $(1, 2, 6, 8, 7, 3)(4, 5)$. Traditionally, the normalizer of a (maximally split) torus is denoted N, and is the 'N' part of the 'BN-pair'.

4.2.5 Simplicity of $G_2(q)$

In fact $G_2(q)$ is simple for all q except for $q = 2$, when we have $G_2(2) \cong \mathrm{PSU}_3(3){:}2$. As usual, we can use Iwasawa's Lemma to prove simplicity. There are a number of primitive actions of the group which could be used. Probably the easiest is the action on isotropic 1-spaces perpendicular to 1. In this case, there are $(q^6 - 1)/(q - 1)$ points, and the point stabilizer has the shape $q^2.q.q^2.\mathrm{GL}_2(q)$. There is a normal subgroup of order q^2 consisting of so-called long root elements.

It can be shown that the subgroup generated by long root elements is transitive on the isotropic vectors, and is therefore the whole of $G_2(q)$. Then we calculate the orbits of the point stabilizer $q^2.q.q^2.\mathrm{GL}_2(q)$ on the points. We find that there are four orbits, of lengths 1, $q(q + 1)$, $q^3(q + 1)$ and q^5 (represented by $\langle x_1 \rangle$, $\langle x_2 \rangle$, $\langle x_7 \rangle$ and $\langle x_8 \rangle$ respectively). The only possibility for a block system would be $q^3 + 1$ blocks of size $q^2 + q + 1$. Some calculations rule this out. This contradiction implies that the action is primitive. Clearly long root elements are in the derived subgroup, so $G_2(q)$ is perfect. Now apply Iwasawa's Lemma.

4.3 Triality

The phenomenon known as triality plays an important role in many exceptional groups, especially $F_4(q)$, $E_6(q)$ and ${}^3D_4(q)$, but is 'really' a property of the orthogonal groups $\mathrm{O}_8^+(q)$. In this section we show how to derive triality from the octonions. We work with an octonion algebra $\mathbb{O}$, which may be the real octonion algebra, or an octonion algebra over a finite field. Most of our arguments will apply equally to all cases, but sometimes there are extra difficulties in characteristic 2 (and occasionally in characteristic 3).

To understand what triality is, it is useful first to explore what we mean by duality of vector spaces. The word is used to describe a number of related phenomena. Given a vector space V over a field F, an (external) dual space V^* may be defined as the space of linear maps from V to F. If the dimension of V is finite, then $\dim V^* = \dim V$, so V and V^* are isomorphic as vector spaces. Thus the bilinear 'evaluation' map $V^* \times V \to F$ defined by $(f, v) \mapsto f(v)$ gives rise to a bilinear 'inner product' $V \times V \to F$. This inner product can be regarded as an 'internal' version of duality. The natural action of $\mathrm{GL}(V)$ induces a 'dual' action on V^* which is different from its action on V.

Similarly, an internal version of triality is given by the product on the octonion algebra, or more precisely by the trilinear form $\mathbb{O} \times \mathbb{O} \times \mathbb{O} \to F$ defined by $(x, y, z) \mapsto \mathrm{Re}\,(xyz)$. An 'external' version of triality has three related orthogonal 8-spaces, V, V', V'', say, with the orthogonal group (or rather its double cover the spin group) acting in three different ways on these three spaces. We shall begin by describing this external manifestation of triality. We identify V, V' and V'' with $\mathbb{O}$ for convenience, but we are regarding them only as vector spaces, not as algebras.

4.3.1 Isotopies

An *isotopy* of $\mathbb{O}$ is a map $(\alpha, \beta, \gamma) : \mathbb{O} \times \mathbb{O} \times \mathbb{O} \to \mathbb{O} \times \mathbb{O} \times \mathbb{O}$, where α, β, γ are orthogonal transformations, and which preserves the set of triples (x, y, z) with $xyz = 1$. (Here no brackets are needed as $(xy)z = 1$ implies that z is in the quaternion subalgebra generated by x and y).

Let $L_u : x \mapsto ux$ denote left multiplication by u, let $R_u : x \mapsto xu$ denote right multiplication by u, and $B_u : x \mapsto \overline{u}x\overline{u}$ denote bimultiplication by $\overline{u}$. If $u \in \mathbb{O}$ has norm 1 (i.e. $u\overline{u} = 1$) then (L_u, R_u, B_u) is an isotopy. For if $xyz = 1$ then the subalgebra generated by u and $xy = z^{-1}$ is associative (all 2-generator subalgebras are associative), so by the Moufang identity

$$\begin{aligned} ((ux)(yu))(\overline{u}z\overline{u}) &= (u(xy)u)(\overline{u}z\overline{u}) \\ &= u(xy)u\overline{u}z\overline{u} \\ &= u(xy)z\overline{u} = u\overline{u} = 1. \end{aligned} \tag{4.14}$$

In fact, the maps (L_u, R_u, B_u) generate the full group of isotopies. To see this, first note that if the characteristic is not 2 and u is purely imaginary ($\overline{u} = -u$), then B_u negates 1 and u, and fixes the orthogonal complement. Thus in $\mathrm{O}_7(q)$ these maps are reflections, and in fact generate a group $2 \times \Omega_7(q)$ on the purely imaginary octonions. Similarly, in characteristic 2, the map B_u acts on $1^\perp$ as an orthogonal transvection, and these generate $\Omega_7(q) \cong \mathrm{Sp}_6(q)$. Also, if $\omega = \frac{1}{2}(-1 + i_0 + i_1 + i_3)$ then B_ω moves the identity element to ω so extends the group to $\Omega_8^+(q)$.

Next we need to look at the group homomorphism $(\alpha, \beta, \gamma) \mapsto \gamma$ from the group of isotopies to the orthogonal group, and show that its kernel is the group of order 2 (or 1 if the field has characteristic 2) generated by $(-1,-1,1) = (L_{-1}, R_{-1}, B_{-1})$. In other words, given an isotopy $(\alpha, \beta, 1)$ we must show that $\alpha = \beta = \pm 1$.

Suppose the characteristic is not 2, and that $1^\alpha = a$, necessarily of norm 1. Applying the definition of isotopy to the triple $(x, y, z) = (1, 1, 1)$ we have $1 = 1^\alpha 1^\beta 1 = a1^\beta$ so $1^\beta = \overline{a}$. Next, taking $(x, 1, x^{-1})$ we have

$$1 = x^\alpha 1^\beta x^{-1} = x^\alpha \overline{a} x^{-1}$$

so $x^\alpha = xa$ and so $\alpha = R_a$. Similarly, taking $(1, y, y^{-1})$ we have

$$1 = 1^\alpha y^\beta y^{-1} = a y^\beta y^{-1}$$

so $y^\beta = \overline{a}y$ and so $\beta = L_{\overline{a}}$.

We wish to show that a is real, and therefore $a = \pm 1$. First define the *nucleus* of $\mathbb{O}$ to be the set of elements $a \in \mathbb{O}$ such that $(xa)w = x(aw)$ for all $x, w \in \mathbb{O}$. Clearly the nucleus is a subspace and is invariant under the automorphism group. Equally clearly, it contains 1 but not i_0. Hence the nucleus is exactly the subspace $\langle 1 \rangle$.

Therefore if a is not real, we may find x and w such that $(xa)w \neq x(aw)$. There exists y such that $\overline{a}y = w$, so

$$\begin{aligned} xy &= x((a\overline{a})y) \\ &= x(a(\overline{a}y)) \\ &\neq (xa)(\overline{a}y) \end{aligned} \tag{4.15}$$

In other words we have found x, y, z with $xyz = 1$ but $(xa)(\overline{a}y)z \neq 1$, which contradicts the assumption that $(R_a, L_{\overline{a}}, 1)$ is an isotopy.

4.3.2 The triality automorphism of $\mathrm{P}\Omega_8^+(q)$

It follows that the group of all isotopies is a double cover (except in characteristic 2) of $\Omega_8^+(q)$, namely the *spin group*. It may be extended to the full spin group $2{\cdot}\mathrm{SO}_8^+(q)$ (or $\mathrm{O}_8^+(q)$ in characteristic 2) by adjoining the duality automorphism $(x, y, z) \mapsto (\overline{y}, \overline{x}, \overline{z})$.

There is another obvious automorphism, called *triality*, which maps (x, y, z) to (z, x, y). [Clearly $xyz = 1$ implies $z = (xy)^{-1}$ and so $zxy = 1$, since inverses are 2-sided.] This extends the spin group to a group of shape $2^2{\cdot}\mathrm{P}\Omega_8^+(q){:}S_3$ (or $\Omega_8^+(q){:}S_3$ in characteristic 2). The centralizer of the triality automorphism consists of all isotopies of the form (α, α, α). This means that if $z^{-1} = xy$ then $(z^{-1})^\alpha = x^\alpha y^\alpha$: in other words, α is an automorphism of the octonion algebra. Thus this centralizer is exactly $G_2(q)$.

Moreover, the set of isotopies preserving the subset

$$\{(1, y, y^{-1}) \mid y \in \mathbb{O} \text{ invertible}\}$$

is the spin group $2^{\cdot}\Omega_7(q)$ (or just $\Omega_7(q)$ in characteristic 2). The stabilizer in this group of the triple $(1,1,1)$ consists of isotopies (α,β,γ) which simultaneously map $(1,y,y^{-1})$ to $(1,y^\beta,(y^{-1})^\gamma)$ (so that $\beta=\gamma$) and map $(x,x^{-1},1)$ to $(x^\alpha,(x^{-1})^\beta,1)$ (so that $\alpha=\beta$), so is again equal to $G_2(q)$. This leads to an alternative description of $G_2(q)$ as the stabilizer of a non-isotropic vector in the 8-dimensional spin representation of $2^{\cdot}\Omega_7(q)$ (or $\Omega_7(q)$ in characteristic 2).

4.4 Albert algebras and groups of type F_4

4.4.1 Jordan algebras

The algebra of $n\times n$ matrices has the well-known matrix product, which is associative but non-commutative. We can derive a commutative product from it, by defining $A\circ B=\frac{1}{2}(AB+BA)$. This is called the *Jordan product*, and is easily shown to be non-associative. It does however satisfy the so-called *Jordan identity*

$$((A\circ A)\circ B)\circ A \quad = \quad (A\circ A)\circ(B\circ A). \tag{4.16}$$

(Exercise) The natural inner product on the vector space of matrices can be expressed as $\mathrm{Tr}(A\circ B)$.

A *Jordan algebra* over a field of characteristic not 2 is defined abstractly to be a (non-associative) algebra with a (bilinear) commutative Jordan product $\circ$, which satisfies the Jordan identity.

Simple Jordan algebras over finite or algebraically closed fields are completely classified (at least if the characteristic is not 2 or 3), and it turns out that apart from those which arise from associative algebras in the manner just described, there is just one other Jordan algebra. It is called the *exceptional Jordan algebra*, or *Albert algebra* and has dimension 27. It may be constructed as the algebra of 3×3 Hermitian matrices over the octonions. For brevity let us define

$$(a,b,c\mid A,B,C) \quad = \quad \begin{pmatrix} a & C & \overline{B}\\ \overline{C} & b & A\\ B & \overline{A} & c\end{pmatrix}, \tag{4.17}$$

where a, b, c are real, and $\overline{}$ denotes the linear map fixing 1 and negating i_n for all n.

The Jordan product is defined in the same way as before, and it can be readily checked that the 27-dimensional space just defined is closed under multiplication. The identity matrix acts as an identity element in this algebra, and its orthogonal complement is the 26-dimensional subspace of matrices of trace 0.

4.4.2 A symmetric trilinear form

The Jordan product gives rise to three invariant forms on the Jordan algebra: a linear form $l(x) = \mathrm{Tr}(x)$, a bilinear form $b(x,y) = \mathrm{Tr}(x \circ y)$, and a trilinear form $t(x,y,z) = \mathrm{Tr}((x \circ y) \circ z)$. It is clear that the bilinear form is symmetric, i.e. $b(x,y) = b(y,x)$. It is also clear that the trilinear form satisfies $t(x,y,z) = t(y,x,z)$. What is much less obvious, but crucial, is that $t(x,y,z) = t(y,z,x)$, so that t is a symmetric trilinear form.

To prove this, note first that if u, v, w are three octonions, then $\mathrm{Re}\,(uv) = \mathrm{Re}\,(vu)$ and $\mathrm{Re}\,((uv)w) = \mathrm{Re}\,(u(vw))$, where $\mathrm{Re}\,(v)$ denotes the real part of v, i.e. $\mathrm{Re}\,(v) = \frac{1}{2}(v + \overline{v})$. This is because $\mathrm{Re}\,((uv)w)$ and $\mathrm{Re}\,(u(vw))$ are trilinear in u, v and w, and both are zero on the basis 1, i_0, ..., i_6 unless u, v, w lie in a quaternion subalgebra, which is associative. Thus we have

$$uv + \overline{uv} = 2\mathrm{Re}\,(uv) = 2\mathrm{Re}\,(vu) = vu + \overline{vu}$$

and

$$(uv)w + \overline{(uv)w} = 2\mathrm{Re}\,((uv)w) = 2\mathrm{Re}\,(u(vw)) = u(vw) + \overline{u(vw)}$$

as required. Note also that $\mathrm{Re}\,(u(vw)) = \mathrm{Re}\,((vw)u)$ so

$$\mathrm{Re}\,(uvw) = \mathrm{Re}\,(vwu) = \mathrm{Re}\,(wuv). \tag{4.18}$$

[On the other hand, beware that $\mathrm{Re}\,(uvw)$ is not in general equal to $\mathrm{Re}\,(wvu)$, even in the quaternions: for example, $\mathrm{Re}\,(ijk) = -1$ but $\mathrm{Re}\,(kji) = 1$.]

Now we calculate the trilinear form at the three matrices $(a,b,c \mid A,B,C)$, $(p,q,r \mid P,Q,R)$ and $(x,y,z \mid X,Y,Z)$ to be

$$\begin{array}{rl} & apx + bqy + crz \\ + & x\mathrm{Re}\,(C\overline{R} + \overline{B}Q) + y\mathrm{Re}\,(A\overline{P} + \overline{C}R) + z\mathrm{Re}\,(B\overline{Q} + \overline{A}P) \\ + & p\mathrm{Re}\,(Z\overline{C} + \overline{Y}B) + q\mathrm{Re}\,(X\overline{A} + \overline{Z}C) + r\mathrm{Re}\,(Y\overline{B} + \overline{X}A) \\ + & a\mathrm{Re}\,(R\overline{Z} + \overline{Q}Y) + b\mathrm{Re}\,(P\overline{X} + \overline{R}Z) + c\mathrm{Re}\,(Q\overline{Y} + \overline{P}X) \\ + & \mathrm{Re}\,(ZPB + YRA + XQC + AQZ + CPY + BRX) \end{array} \tag{4.19}$$

and observe that this is unchanged under permutations of the three matrices.

This enables us to replace the trilinear form by a cubic form $c(x) = t(x,x,x)$ in the same way that we replace the bilinear form $b(x,y)$ by the quadratic form $q(x) = b(x,x)$. We recover the original forms by

$$\begin{array}{rcl} 4b(x,y) & = & q(x+y) - q(x-y) \\ 24t(x,y,z) & = & c(x+y+z) + c(x-y-z) \\ & & +c(-x+y-z) + c(-x-y+z) \end{array} \tag{4.20}$$

for example.

4.4.3 The automorphism groups of the Albert algebras

An analogous construction can be performed using the octonions over any finite field $\mathbb{F}_q$. In characteristic 2 or 3 we need to be more careful in the definitions of the quadratic and cubic forms, however. [We shall not do this here.] Thus we assume the characteristic is odd, and where necessary, not 3. We obtain in this way a finite Jordan algebra, whose automorphism group we call $F_4(q)$. This group in fact acts irreducibly on the 26-dimensional space of trace 0 matrices, except when the field has characteristic 3, in which case the identity matrix has trace 0, and $F_4(q)$ acts irreducibly on the 25-space of trace 0 matrices modulo the identity.

Now if α is any element of $G_2(q)$, i.e. automorphism of the octonions, then it induces a map $(a, b, c \mid A, B, C) \mapsto (a, b, c \mid A^\alpha, B^\alpha, C^\alpha)$ on the Albert algebra over $\mathbb{F}_q$, and it is easy to see that this map is an automorphism. It follows that $G_2(q)$ is a subgroup of $F_4(q)$.

Indeed, we can see the double cover of $\Omega_8^+(q)$, i.e. the spin group $2{\cdot}\Omega_8^+(q) \cong 2^2{\cdot}\mathrm{P}\Omega_8^+(q)$, generated by the maps $(a, b, c \mid A, B, C) \mapsto (a, b, c \mid uA, Bu, \overline{u}C\overline{u})$ where u is an octonion of norm 1. It is a straightforward, if rather tedious, calculation to show directly that this map preserves the Jordan multiplication. However, as we saw in Section 4.3.1 these maps generate the group of isotopies

$$(\alpha, \beta, \gamma) \ : \ (a, b, c \mid A, B, C) \mapsto (a, b, c \mid A^\alpha, B^\beta, C^\gamma), \tag{4.21}$$

which have the property that $ABC = 1$ implies $A^\alpha B^\beta C^\gamma = 1$. It is easy to see that these maps preserve the bilinear form, so (unless the characteristic is 2 or 3) to verify that they preserve the Jordan algebra structure, it suffices to verify that they preseve the cubic form

$$a^3 + b^3 + c^3 + 3a(B\overline{B} + C\overline{C}) + 3b(A\overline{A} + C\overline{C}) + 3c(A\overline{A} + B\overline{B}) + 6\mathrm{Re}\,(ABC).$$

But α, β and γ are orthogonal transformations, so $A\overline{A}$, $B\overline{B}$ and $C\overline{C}$ are fixed. Also we can write $C = C_1 + C_2$ such that $(AB)C_1$ is real and $(AB)C_2$ is purely imaginary, and therefore $(A^\alpha B^\beta)C_1^\gamma = (AB)C_1 = \mathrm{Re}\,((AB)C)$. Moreover, left octonion multiplication by $A^\alpha B^\beta$ is an orthogonal transformation, so $(A^\alpha B^\beta)C_2^\gamma$ is purely imaginary, and $\mathrm{Re}\,((A^\alpha B^\beta)C_1^\gamma) = \mathrm{Re}\,((AB)C)$ as required.

This group of isotopies is normalized by the triality automorphism

$$(a, b, c \mid A, B, C) \ \mapsto \ (b, c, a \mid B, C, A), \tag{4.22}$$

as well as the duality automorphism

$$(a, b, c \mid A, B, C) \ \mapsto \ (a, c, b \mid \overline{A}, \overline{C}, \overline{B}). \tag{4.23}$$

All these elements preserve the 2-dimensional space of diagonal matrices of trace 0, and generate its stabilizer, of shape $2^2{\cdot}\mathrm{P}\Omega_8^+(q){:}S_3$.

4.4.4 Primitive idempotents

To calculate the order of $F_4(q)$, consider the *primitive idempotents* in the Jordan algebra, that is elements x with $x \circ x = x$ and $x.x = 1$. (Here $x.x$ denotes the norm of x, that is, $x.x = \mathrm{Tr}(x \circ x) = \mathrm{Tr}(x)$.) First we determine how many such elements there are. Straightforward calculation shows that the primitive idempotents are precisely the elements $(a, b, c \mid A, B, C)$ which satisfy

$$\begin{aligned} a+b+c &= 1 \\ a^2 + B\overline{B} + C\overline{C} &= a \\ (a+b)\overline{C} + BA &= \overline{C}, \end{aligned} \tag{4.24}$$

and the equations derived from these by cycling a, b, c and A, B, C. The last equation can be re-written as $BA = c\overline{C}$. Eliminating $B\overline{B}$ and $C\overline{C}$ from the three images of the middle equation gives

$$2A\overline{A} = (c - c^2) + (b - b^2) - (a - a^2) = 2bc,$$

(by substituting $a = 1-b-c$) so since the characteristic is not 2 we have $A\overline{A} = bc$, $B\overline{B} = ac$ and $C\overline{C} = ab$. We now divide into three cases according as one, two or three of a, b, c are non-zero. The number of possibilities for (a, b, c) in these three cases is 3, $3(q-2)$ and $q^2 - 3q + 3$ respectively.

In each case, without loss of generality $c \neq 0$, so that C is determined by A, B and the equation $c\overline{C} = BA$. Therefore we only need to determine the number of possibilities for A and B. Note that because the norm on the octonions induces a quadratic form of plus type, there are $q^7 + q^4 - q^3$ octonions of norm 0, and $q^7 - q^3$ of any other norm.

In the first case, $c = 1$ and $a = b = 0$, so A and B have norm 0, and there are $(q^7+q^4-q^3)^2$ possibilities. In the second case, without loss of generality $b \neq 0$ and $a = 0$, so that $A\overline{A} = bc \neq 0$ and B has norm 0, and there are $(q^7-q^3)(q^7+q^4-q^3)$ possibilities. In the last case, both A and B have fixed non-zero norm, so there are $(q^7 - q^3)^2$ possibilities. Therefore the total number of primitive idempotents is

$$3(q^7 + q^4 - q^3)^2 + 3(q-2)(q^7 - q^3)(q^7 + q^4 - q^3) + (q^2 - 3q + 3)(q^7 - q^3)^2,$$

which simplifies to

$$q^8(q^8 + q^4 + 1).$$

It can be shown that, if e is a primitive idempotent, then the map

$$t_e \;:\; x \mapsto x + 4(x.e)e - 4x \circ e \tag{4.25}$$

is an automorphism of the algebra, where $x.e$ denotes the inner product, that is $x.e = \mathrm{Tr}(x \circ e)$. For example, if $e = (1, 0, 0, \mid 0, 0, 0)$ then

$$t_e \;:\; (a, b, c \mid A, B, C) \mapsto (a, b, c \mid A, -B, -C). \tag{4.26}$$

It is straightforward to deduce that the maps t_e generate a group which acts transitively on the set of primitive idempotents. Moreover, the stabilizer of a primitive idempotent is now seen to be the spin group $2{\cdot}\Omega_9(q)$.

Taking for example the primitive idempotent $e = (1, 0, 0, \mid 0, 0, 0)$ it is easy to see that it determines the 9-space $\{(0, b, -b \mid A, 0, 0)\}$ of elements y of trace 0 with $e \circ y = 0$, and the 16-space $\{(0, 0, 0 \mid 0, B, C)\}$ of elements z of trace 0 with $e \circ z = \frac{1}{2}z$ (these are just the eigenspaces of the action of e on the algebra by Jordan multiplication). In fact the orthogonal group $\Omega_9(q)$ acts on this 9-space, and its double cover acts as the spin group on the 16-space. To see that the stabilizer of e is no bigger, it suffices to check that the pointwise stabilizer of the 9-space consists only of the group of order 2 generated by the element $(a, b, c \mid A, B, C) \mapsto (a, b, c \mid A, -B, -C)$. Hence the order of $F_4(q)$ is $q^8(q^8 + q^4 + 1)q^{16}(q^8 - 1)(q^6 - 1)(q^4 - 1)(q^2 - 1)$, that is

$$|F_4(q)| = q^{24}(q^{12} - 1)(q^8 - 1)(q^6 - 1)(q^2 - 1). \qquad (4.27)$$

4.4.5 Simplicity of $F_4(q)$

To prove simplicity of $F_4(q)$ we can use Iwasawa's Lemma in the usual way. It is straightforward to show that $F_4(q)$ acts primitively on the set of primitive idempotents. The stabilizer of a primitive idempotent is the subgroup $2{\cdot}\Omega_9(q)$, which is generated by $F_4(q)$-conjugates of the central involution t_e (since it contains $2^2{\cdot}\mathrm{P}\Omega_8^+(q)$ which has normalizer $2^2{\cdot}\mathrm{P}\Omega_8^+(q){:}S_3$). Now $2{\cdot}\Omega_9(q)$ is maximal (because the action on primitive idempotents is primitive), and does not contain every conjugate of t_e, so $F_4(q)$ is generated by these elements. It follows that $F_4(q)$ is perfect, and all the conditions of Iwasawa's Lemma are satisfied. We deduce that $F_4(q)$ is simple (for q odd).

4.5 Trilinear forms and groups of type E_6

4.5.1 The determinant

The exceptional Jordan algebra (or Albert algebra) described in Section 4.4.1 can be used also to construct the groups of type E_6. These groups no longer preserve the algebra structure, or the inner product, but they do preserve a cubic form which is a type of determinant map. Of course, it is not obvious how to define a determinant even for matrices over a non-commutative ring, let alone a non-associative ring. However, for 3×3 Hermitian matrices over octonions there is a notion of determinant which makes sense, namely

$$\begin{aligned}\det(a, b, c \mid A, B, C) &= abc - aA\overline{A} - bB\overline{B} - cC\overline{C} \\ &\quad + \mathrm{Re}\,(ABC) + \mathrm{Re}\,(CBA). \qquad (4.28)\end{aligned}$$

The values of this determinant belong to the ground field $\mathbb{F}_q$, but beware that identities you are used to like $\det(xy) = \det(x)\det(y)$ may not necessarily hold.

There is even a notion of *rank* for these matrices: clearly we want

$$\begin{array}{lcl} \mathrm{rk}(x) = 3 & \Longleftrightarrow & \det(x) \neq 0 \\ \mathrm{rk}(x) = 0 & \Longleftrightarrow & x = 0 \end{array} \tag{4.29}$$

so all other matrices should have rank 1 or 2. The rank 1 matrices are (essentially) those whose rows are (left-octonion-)scalar multiples of each other. That is, if say $a \neq 0$, then the second row is $(\overline{C}, b, A) = a^{-1}(\overline{C}a, \overline{C}C, \overline{CB})$ and the third row is $(B, \overline{A}, c) = a^{-1}(Ba, BC, B\overline{B})$. (A slightly different definition is required if the diagonal of the matrix is zero.) In some of the literature the vectors of rank 1, 2 and 3 are called 'white', 'grey' and 'black' respectively.

It is possible to show (by direct, though tedious, calculation) that the numbers of white, grey and black vectors are respectively $(q^9 - 1)(q^8 + q^4 + 1)$, $q^4(q^9 - 1)(q^8 + q^4 + 1)(q^5 - 1)$ and $q^{12}(q^9 - 1)(q^5 - 1)(q - 1)$. The last case includes $q - 1$ possibilities for the determinant, so the number of vectors of determinant 1 is $q^{12}(q^9 - 1)(q^5 - 1)$. One of these is the identity matrix $(1, 1, 1 \mid 0, 0, 0)$, and if we fix this then we recover the Albert algebra. For the determinant gives rise to a trilinear form, and by substituting the identity matrix for one or two of the variables we obtain a bilinear and a linear form, and these three forms together define the algebra. (Details are left as an exercise.)

In other words, the stabilizer of a black vector is $F_4(q)$, and provided we can prove transitivity of our group on vectors of determinant 1, we deduce that its order is $q^{12}(q^9 - 1)(q^5 - 1)|F_4(q)|$, that is

$$q^{36}(q^{12} - 1)(q^9 - 1)(q^8 - 1)(q^6 - 1)(q^5 - 1)(q^2 - 1). \tag{4.30}$$

Now this group in general is not simple, as it may contain non-trivial scalars—this is so if and only if $\mathbb{F}_q$ contains a cube root ω of 1, for $\det(\omega x) = \omega^3 \det(x)$ which equals $\det(x)$ if and only if $\omega^3 = 1$. We define $E_6(q)$ to be the (simple!) group obtained by factoring out the scalars of order 3, when $q \equiv 1 \bmod 3$.

By analogy with the linear groups, let $SE_6(q)$ denote the original matrix group, so that $SE_6(q) \cong 3{\cdot}E_6(q)$ if $q \equiv 1 \bmod 3$ and $SE_6(q) \cong E_6(q)$ otherwise. Similarly, let $GE_6(q)$ denote the group of matrices which multiply the determinant by a scalar, so that $GE_6(q) \cong 3.(C_{(q-1)/3} \times E_6(q)).3$ if $q \equiv 1 \bmod 3$, and let $PGE_6(q)$ denote the quotient of $GE_6(q)$ by scalars. Thus $PGE_6(q) \cong E_6(q).3$ if $q \equiv 1 \bmod 3$, and $PGE_6(q) \cong E_6(q)$ otherwise.

4.5.2 Dickson's construction

It is not well-known that the simple groups $E_6(q)$, and their triple covers when they exist, were first constructed by L. E. Dickson around 1901. He constructed the 27-dimensional representation with respect to a basis which is essentially the same as the one we use, and wrote down a large number of elements generating the group. He calculated the group order, as well as constructing the permutation representation of the simple group $E_6(q)$ on $(q^9-1)(q^8+q^4+1)/(q-1)$ points, although he did not prove simplicity of the group.

Dickson's construction is more elementary than ours, but more or less equivalent. He takes 27 coordinates labelled x_i, y_i and $z_{ij} = -z_{ji}$ where i and j are distinct elements of the set $\{1,2,3,4,5,6\}$, and defines his group as the stabilizer of a cubic form with 45 terms:

$$\sum_{i\neq j} x_i y_j z_{ij} + \sum z_{ij} z_{kl} z_{mn} \tag{4.31}$$

where $(ij \mid kl \mid mn)$ ranges over the 15 partitions of $\{1,2,3,4,5,6\}$ into three pairs, ordered so that $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ i & j & k & l & m & n \end{pmatrix}$ is an even permutation.

It is a straightforward exercise to show that this is the same cubic form as the determinant defined above, for example by taking $x_1, \ldots, x_6$ to correspond to w_1, w_1', w_1'', w_2, w_2', w_2'' and $y_1, \ldots, y_6$ to correspond to $w_7, \ldots, w_8''$ (in that order).

An alternative description of the cubic form may be obtained by defining the 27-space as the space of triples (x, y, z) of 3×3 matrices over $\mathbb{F}_q$, with the cubic form

$$\det x + \det y + \det z - \operatorname{Tr}(xyz). \tag{4.32}$$

Again, this is easily seen to be a cubic form with 45 terms in 27 variables, and it is a straightforward exercise to show it is essentially the same cubic form.

4.6 Twisted groups of type ${}^3D_4$

Recall that the unitary groups may be defined by identifying the duality (or inverse-transpose) automorphism $x \mapsto (x^{-1})^T$ of the general linear groups $\mathrm{GL}_n(q^2)$ with the field automorphism $x \mapsto \overline{x} = x^q$ of order 2, so that the group consists of the matrices x satisfying $x^{-1} = \overline{x}^T$. We may apply the same principle to the groups $\mathrm{P}\Omega_8^+(q^3)$, identifying the triality automorphism with the field automorphism $x \mapsto x^q$ of order 3.

In other words, we consider those isotopies (α, β, γ) on the octonion algebra over $\mathbb{F}_{q^3}$ which commute with the map $(x, y, z) \mapsto (y^q, z^q, x^q)$. The group of such isotopies is denoted ${}^3D_4(q)$, because the triality automorphism can be thought of as an automorphism of order 3 of the Dynkin diagram $\mathtt{D}_4$.

A more concrete way to look at this group is to 'twist' the octonion algebra (see Section 4.2.2) over $\mathbb{F}_{q^3}$ by the field automorphism $x \mapsto x^q$ of order 3. That is, replace the ordinary octonion product by a new product $*$ which takes the same values on our standard basis (either $\{1, i_0, \ldots, i_6\}$ or $\{x_1, \ldots, x_8\}$), but instead of the bilinearity condition $(\lambda a)(\mu b) = (\lambda\mu)(ab)$ we now have

$$(\lambda a) * (\mu b) \quad = \quad (\lambda^q \mu^{q^2})(a * b) \tag{4.33}$$

for all $\lambda, \mu \in \mathbb{F}_{q^3}$ and all a, b in the algebra. Notice that the twisted algebra has no identity element, since $1 * x = x$ would imply $1 * (\lambda x) = \lambda^{q^2} x \neq \lambda x$. Indeed, we shall see that the automorphism group of the twisted algebra acts irreducibly on it. It is immediate from this construction that ${}^3D_4(q)$ contains $G_2(q)$.

The algebra still has a norm and inner product defined over $\mathbb{F}_{q^3}$. The norm is still a quadratic form but now it satisifies

$$N(a * b) \quad = \quad N(a)^q N(b)^{q^2} \tag{4.34}$$

instead of $N(ab) = N(a)N(b)$.