Exceptional Groups

Maneesh Thakur

Abstract

In this mini-course, we will describe explicit constructions of some of the exceptional algebraic groups over arbitrary fields. These groups occur in Geometry, Representation theory, Number theory and so on. The constructions decribed use some natural representations of these groups. We take for granted basic notions from the theory of algebraic groups. These notes are far from being complete, are meant to provide an outline of the subject. These have been compiled from some standard texts. The list of references is not exhaustive, but contains the essential texts and papers for the material covered. The reader should watch out for mistakes in the notes, which may have crept in silently.

1 Quadratic, Hermitian and Symplectic forms

Basic references for this section are [L], [J-1], [J-2] and [L-1]. For generalities on algebraic groups, we refer to the books [H], [B] and [S-1]. Let k be a field of characteristic not 2. Let V be a finite dimensional vector space over k. Let $B : V \times V \to k$ be a map. If B is bilinear, we call B s **symmetric** form if $B(x, y) = B(y, x)$ for all $x, y \in V$. We call B **alternating** or **symplectic** if $B(x, y) = -B(y, x)$. If k has an automorphism of order 2, written as $a \mapsto \bar{a}$, we call B a **hermitian** form if B is linear in the first variable and **sesquilinear** in the second, i.e. $B(x, ay) = \bar{a}B(x, y)$ for all $x, y \in V$, moreover, $B(x, y) = \overline{B(y, x)}$ for all $x, y \in V$. A map $Q : V \to k$ is a **quadratic form** on V if there is a symmetric bilinear form B on V such that $Q(v) = B(v, v)$ for all $v \in V$. It is easy to see that the assignment $q \mapsto B_q : (v, w) \mapsto \frac{1}{2}(q(v + w) - q(v) - q(w))$ is a bijective correspondence between quadratic forms and symmetric bilinear forms on V. Let $B : V \times V \to k$ be a symmetric, alternating or hermitian form. We call B nondegenerate if $B(x, y) = 0$ for all y implies $x = 0$. We call the pair (V, B) a quadratic, symplectic or hermitian (or unitary) space if B is nondegenerate and is respectively symmetric, alternating or hermitian form on V. If B is symmetric and nonzero, then there exists an orthogonal basis for B. With respect to such a basis, the matrix of B is diagonal. This fact is stated as any nonzero symmetric bilinear form can be diagonalized. A quadratic form on V is called **universal** if it attains all values from k. We define a quadratic form Q to be **isotropic** if it has a nontrivial zero in V, **anisotropic** otherwise. Any nontrivial zero v of Q is called an **isotropic vector**. A subspace which contains only isotropic vectors for Q is called a **totally isotropic subspace**. The dimension of a maximal totally isotropic subspace is independent of the subspace and is called the **Witt index** of V. The following theorem reveals the structure of a quadratic space.

Theorem 1.1. **(Witt-decomposition)** *Let (V, Q) be a quadratic space. Then Q admits an orthogonal decomposition $Q = r\mathbb{H} \perp Q_{an}$, where r is the Witt-index of Q and Q_{an} is* *anisotropic,* $\mathbb{H}$ *denotes the* **hyperbolic plane** $\mathbb{H}((x,y)) = x^2 - y^2$*. The anisotropic part* Q_{an} *of* Q *is determined up to an isometry.*

If B is a hermitian form, one again has an othogonal basis. If B is a nondegenerate alternating form, the dimension of V is necessarily even, further, all alternating nondegenerate forms of a given dimension over k are equivalent (see Lang-Chapter XV, Section 8), see also the book by L. C. Grove, Classical Groups and Geometric Algebra. An **isometry** of a nondegenerate bilinear form B on V is an element $g \in GL(V)$ such that $B(gv, gw) = B(v, w)$ for all $v, w \in V$. An isometry is necessarily bijective, since V is finite dimensional. A **similitude** of B is an element $g \in GL(V)$ such that $B(gv, gw) = \sigma(g)B(v, w)$ for all $v, w \in V$ and a fixed $\sigma(g) \in k^*$, called the **factor of similitude** of g. The (algebraic) group of isometries is denoted by $\mathbf{O}(V, B), \mathbf{Sp}(V, B)$ or $\mathbf{U}(V, B)$ respectively, according as B is symmetric, alternating or hermitian, and are called the **orthogonal**, **symplectic** or the **unitary** group of (V, B). Let B be a bilinear form on V. For any basis $\{e_1, \cdots, e_n\}$ of V, we have the matrix associated to B, namely, $(B(e_i, e_j))$. The determinant of this matrix is called the **discriminant** of B, it is determined up to a square in k.

Clifford algebra and the Spin group : Let (V, Q) be a quadratic space (i.e. Q is a nondegenerate quadratic form on V). Then $\mathbf{SO}(Q) = \mathbf{O}(V, Q) \cap \mathbf{SL}(V)$ is a connected algebrac group defined over k. This group has a two fold covering, denoted by $\mathbf{Spin}(V, Q)$. The **Clifford algebra** of Q is a pair (C, f) where C is an associative k-algebra (k need not be algebraically closed in this discussion) with unity 1 and $f : V \to C$ is a k-linear map with $f(x)^2 = Q(x).1$ for all $x \in V$, satisfying the following **universal property**: for any pair (D, g), where D is an associative algebra over k with 1 and $g : V \to D$ is a k-linear map such that $g(x)^2 = Q(x).1$ for all $x \in V$, there exists a unique k-algebra homomorphism $\tilde{g} : C \to D$ such that $\tilde{g} \circ f = g$. The Clifford algebra $C(V, Q)$ exists and is unique upto k-isomorphism. Clearly $f(V)$ generates C as an algebra. One shows easily that f is injective. If $e_1, \cdots, e_n$ form a basis of V, the products $e_{i_1} \cdots e_{i_m},\ 1 \leq i_1 < i_2 < \cdots < i_m \leq n$ together with 1 form a basis for $C(V, Q)$, hence $Dim[C(V, Q)] = 2^n$. If n is even, C is a simple algebra with center k. If n is odd, C has a 2 dimensional center over k. In this case, C is either simple or a direct sum of two simple algebras. Let $C^+ = C^+(V, Q)$ be the **even Clifford algebra** of (V, Q), i.e., the subalgebra of C generated by products of even number of vectors in V. Hence $Dim(C^+) = 2^{n-1}$. When n is even, it can be shown that $C^+(Q)$ is seperable with center Z either a quadratic field extension of k or the split quadratic algebra $k \times k$. In the first case C^+ is simple while in the second it is direct sum of two simple algebras. If n is odd, C^+ is always central simple (defined below).

If we define $\eta : C \to C$ by $\eta(e_{i_1} \cdots e_{i_r}) = e_{i_r} e_{i_{r-1}} \cdots e_{i_1}$ on the generators $e_{i_1} \cdots e_{i_r}$ $(1 \leq i_1 < i_2 < \cdots < i_r \leq n; 1 \leq r \leq n)$ and $\eta(1) = 1$, we get a well defined involution (antiautomorphism or period 2) of C, called the **standard involution**. The **Clifford group** $\Gamma(V, Q)$ is the subgroup of the group of units in $C(V, Q)$ consisting of elements t of $C(V, Q)$ such that $tvt^{-1} \in V$ for all $v \in V$. We call $\Gamma^+(V, Q) = C^+ \cap \Gamma(V, Q)$ the **even Clifford group**. If $t \in \Gamma^+(V, Q)$, say $t = v_1 v_2 \cdots v_{2r}$, then $N(t) = t\eta(t) = \Pi Q(v_i) \in k.1$ and N is a homomorphism from Γ^+ to k^*. The group $Spin(Q)$ is defined as the kernel of N. We can now define, for any extension L/k,

$$\mathbf{Spin}(Q)(L) = \{e \in C_L^+ | tV_L t^{-1} = V_L,\ t\eta(t) = 1\}.$$

The group $\mathbf{Spin}(Q)$ defined above is a connected algebraic group defined over k, called the **Spin group** of Q and $\mathbf{Spin}(Q)(k) = Spin(Q)$. For any $t \in \mathbf{Spin}(Q)(L)$, the automorphism $v \mapsto tvt^{-1}$ of V_L belongs to $\mathbf{SO}(Q)(L)$. This gives us a map $\chi : \mathbf{Spin}(Q) \to \mathbf{SO}(Q)$ which is a k-homomorphism of algebraic groups, called the **vector representation**), is surjective with kernel $\{\pm 1\}$. The **reduced orthogonal group** of Q is, by definition, $O'(V, Q) = \chi(Spin(Q)$. For any $g \in SO(Q)$, there exists $f \in \Gamma^+$ such that $\chi(f) = g$ and f is unique up to a factor in k^*. Hence the coset $\sigma(g) = N(f)k^{*2}$ in k^*/k^{*2} is determined by g. We call $\sigma(g)$ the **spinor norm** of g. If we write $g = S_{v_1} \cdots S_{v_{2r}},\ v_i \in V,\ Q(v_i) \neq 0$, then it follows that $\sigma(g) = N(f)k^{*2} = \Pi Q(v_i)k^{*2}$. We will often need a theorem of Witt on extension of isometries, we state it below.

Theorem 1.2. (Witt's Extension Theorem) : *Let $(V_i, Q_i),\ 1 \leq i \leq 2$ be a nondegenerate quadratic space and assume that Q_1 and Q_2 are isometric. Then every isometry of a subspace of V_1 onto a subspace of V_2 extends to an isometry of V_1 onto V_2.*

Corollary 1.1. (Witt's Cancellation Theorem) *Let (V, Q) and $(V'Q')$ be isometric quadratic spaces, $V = W_1 \perp W_2,\ \ V' = W_1' \perp W_2'$. Assume (W_1, Q_1) is isometric to (W_1', Q_1') with restrictions of the ambient forms. Then W_2 is isometric to W_2'.*

Pfister forms : This is a special class of quadratic forms having mulptiplicative properties (see T. Y. Lam). An r-fold **Pfister form** is a quadratic form $(x_1^2 - a_1x_2^2) \otimes (x_3^2 - a_2x_4^2) \otimes \cdots \otimes (x_r^2 - a_rx_{r+1}^2)$, i.e. a tensor product of the norm forms of quadratic extensions of k. We denote this form by $\langle\langle a_1, a_1, \cdots, a_r\rangle\rangle$. So $\langle\langle a\rangle\rangle = x_1^2 - ax_2^2$. It can be shown that a Pfister form Q is either of maximal Witt index (i.e. $Q = r\mathbb{H}$ for a suitable r) or is anisotropic over k, i.e. has no nontrivial zeros over k. Pfister forms are closely tied up with algebraic groups as we will soon see.

2 Octonion algebras and G_2

Recall that G_2 is the root system of smallest rank among the five exceptional root systems. Groups of type G_2 (i.e. twisted forms of the split group G_2) over a field k are intimately connected with certain nonassociative algebras, called **octonion algebras** or **Cayley algebras** over k. We begin this section with some preliminaries needed to describe these algebras. The material in this section and the next has been largely compiled from the texts by Springer and Veldkamp [SV] and Jacobson [J-3].

Let k denote a fixed base field. A **central simple algebra** of degree n over k is a k-algebra A such that $A \otimes k_s \simeq M_n(k_s)$, where k_s denotes a fixed separable closure of k and $M_n(k)$ is the algebra of matrices of size $n \times n$ with entries in k. We also refer to $M_n(k)$ as the **split central simple algebra** of degree n over k. We can regard central simple algebras over k as **twisted forms** of the split matrix algebra over k. Central simple algebras are equipped with twsited versions of the determinant and trace maps, called respectively the **reduced norm** and **reduced trace**. It follows that for central simple algebra A over k and $x \in A$, its reduced norm $N_A(x)$ and its reduced trace $T_A(x)$ both belong to k. It also can be shown that $N_A(xy) = N_A(x)N_A(y)$ and $T_A(x+y) = T_A(x) + T_A(y)$ for all $x, y \in A$ and T_A is a linear form on A. Degree 2 central simple algebras are called **quaternion algebras**, these are general versions of the well known **Hamilton's quaternion algebra** over $\mathbb{R}$. The reduced norm map on quaternion algebras is a nondegenerate quadratic form and is multiplicative. A k-algebra C (not necessarilyy associative) with an identity element, with a nondegenerate quadratic form Q that is multiplicative (called the **norm**), is called a **composition algebra**. Over a field k ($char(k) \neq 2$), a composition algebra C is, up to a k-isomorphism, one of the four possibilities: k with $Q(x) = x^2$, $C = K$ a quadratic étale algebra with $Q = N_{K/k}$, C a quaternion algebra A with $Q = N_A$, C an octonion algebra with Q its norm. The following will be used in the sequel:

Theorem 2.1. (Skolem-Noether Theorem) *Let A be a central simple algebra over a field k. Then every automorphism of A is given by an inner conjugation, i.e. is of the form $x \mapsto yxy^{-1}$ for a fixed $y \in A$.*

The dimension of a composition algebra is $1, 2, 4$ or 8. A composition algebra is determined by its norm up to isomorphism. Octonion algebras are 8 dimensional composition algebras. Let $\langle , \rangle$ denote the bilinear form corresponding to Q on a composition algebra C. The map $x \mapsto \overline{x} = \langle x, e\rangle - x$, where e is the identity element in C, satisfies $x\overline{x} = \overline{x}x = Q(x)$, $\overline{xy} = \overline{y}\,\overline{x}$ for all $x, y \in C$. Moreover, $\overline{x+y} = \overline{x} + \overline{y}$ and $\overline{\overline{x}} = x$ for all $x \in C$. We call this map the **canonical involution** or the **conjugation** on C. Clearly $T(x) = x + \overline{x} \in k.e$ and $Q(x).e = x\overline{x}$. We call $T(x)$ the **trace** of x. The following is easily checked:

Theorem 2.2. *Let C be a composition algebra and $a \in C$. Then a satisfies the Cayley-Hamilton equation $X^2 - T(a)X + Q(a) = 0$.*

Let C be a composition algebra and D a composition subalgebra. The form $Q|D$ being nondegenerate, we can write $C = D \oplus D^{\perp}$ with $D^{\perp}$ nondegenerate. If $D \neq C$, then there is $a \in D^{\perp}$ with $Q(a) \neq 0$. We then have

Theorem 2.3. *Let C, D and a be as above. Assume $D \neq C$. Then $S = D \oplus Da$ is a composition subalgebra of C with $Dim(S) = 2Dim(D)$. The formulae below describe the product, norm and the conjugation on S*

$$(x + ya)(x' + y'a) = (xx' + \nu\overline{y'}y) + (y'x + y\overline{x'})a,$$

$$N_S(x + ya) = N_D(x) - \nu N_D(y),\ \overline{x + ya} = \overline{x} - ya,\ \ (x, y, x', y' \in D),$$

where $\nu = -Q(a)$ and N_S and N_D denote the norms on S and D respectively. Conversely, if D is a composition algebra with norm N and $\mu \in k^*$, on the vector space $C = D \oplus D$ define a product by

$$(x, y)(x', y') = (xx' + \mu\overline{y'}y, y'x + y\overline{x'}),\ \ (x, x', y, y' \in D)$$

and a quadratic form Q by

$$Q((x, y)) = N(x) - \mu N(y).$$

If D is associative then C is a composition algebra. C is associative if and only if D is commutative and associative.

The following consequence is immediate:

Corollary 2.1. *The norm form of a composition algebra is a Pfister form.*

The construction described in the above theorem is called **doubling**. The process of doubling stops at dimension 8 and one obtains an octonion algebra. In other words, all octonion algebras can be obtained by doubling quaternion algebras. If the norm form of a composition algebra is anisotropic, i.e., has no nontrivial zeros, then every nonzero element has a multiplicative inverse, in which case we call such a composition algebra a **division** algebra. Since the norm form is either anisotropic or is hyperbolic (since it is a Pfister form), it follows that a composition algebra is either **split** (i.e. its norm has maximal Witt index) or is a division algebra.

Definition. *Let C be a composition algebra with norm N and $\lambda, \mu \in k^*$. A* **special** (λ, μ)*-pair is an ordered pair (a, b) with $a, b \in C$ such that*

$$\langle a, e\rangle = \langle b, e\rangle = \langle a, b\rangle = 0, \;\; N(a) = \lambda, \; N(b) = \mu.$$

A special $(1,1)$-pair is called a **special pair**.

We have

Lemma 2.1. *Every special (λ, μ)-pair a, b is contained in a unique quaternion subalgebra, with basis $\{e, a, b, ab\}$ and every quaternion algebra contains (λ, μ)-special pairs for suitable parameters. In particular, existence of such a pair implies that the ambient composition algebra is a quaternion or an octonion algebra.*

The following consequence of Witt's theorem is immediate:

Corollary 2.2. *Let C be a composition algebra over k, $\lambda, \mu \in k^*$ and (a, b) and (a', b') be two special (λ, μ)-pairs in C. Then there exists an automorphism ϕ of C such that $\phi(a) = a', \; \phi(b) = b'$.*

Octonion algebras : We now collect some facts specific to octonion algebras. One can construct the split octonion algebra by doubling the split quaternion algebra, i.e. by doubling $M_2(k)$, or by doubling a quaternion division algebra with $\mu = 1$, since this ensures the norm form is isotropic. We now give another model of the split octonion algebra, called the algebra of Zorn's vector matrices. Let $Zorn(k) = \begin{pmatrix} k & k^3 \\ k^3 & k \end{pmatrix}$. We fix the non-degenerate symmetric bilinear form $\langle , \rangle$ on k^3, given by

$$\langle x, y\rangle = \sum_{i=1}^{3} x_i y_i, \;\; x = (x_1, x_2, x_3), \; y = (y_1, y_2, y_3) \in k^3.$$

Fix an exterior product $\times$ on k^3 defined by

$$\langle x \times y, z\rangle = det(x, y, z), \;\; (x, y, z \in k^3).$$

Define a product $Zorn(k) \times Zorn(k) \to Zorn(k)$ by

$$\left(\begin{pmatrix} a & x \\ x' & a' \end{pmatrix}, \begin{pmatrix} b & y \\ y' & b' \end{pmatrix} \right) \mapsto \begin{pmatrix} ab + \langle x, y' \rangle & ay + b'x + x' \times y' \\ bx' + a'y' + x \times y & a'b' + \langle x', y \rangle \end{pmatrix}.$$

With this multiplication, $Zorn(k)$ is a (non-associative) k-algebra which admits $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ as the multiplicative identity element. The norm form is given by $N(\begin{pmatrix} a & x \\ x' & a' \end{pmatrix}) = aa' - \langle x, x' \rangle$. This is called the **Zorn algebra** of vector matrices and is isomorphic to the split octonion algebra over k. We can now list all the split composition algebras:

Proposition 2.1. *The split composition algebras over k, up to isomorphism, are the split qudratic algebra $k \times k$, the matrix algebra $M_2(k)$ and the Zorn algebra of vector matrices $Zorn(k)$.*

The group of automorphisms of an octonion algebra : Let C be an octonion algebra over k and $G = Aut(C)$ be the group of all k-linear algebra automorphisms of C. Any automorphism of C preserves the norm N of C, hence is a subgroup of the orthogonal group $O(N)$ of isometries of N. Let $K = \overline{k}$ be an algebraic closure of k and $C_K = K \otimes_k C$. Let $\mathbf{G} = Aut(C_K)$. Then G is a linear algebraic group and $G = \mathbf{G}(k)$. We need to describe the subgroup of G whose elements leave a quaternion subalgebra invariant. Let C be an octonion algebra and $D \subset C$ be a quaternion subalgebra. Let $\phi \in G$ be such that $\phi(D) = D$. Then, since ϕ preserves the norm on C, we have $\phi(D^\perp) = D^\perp$. We can write $D^\perp = Da$ for some fixed $a \in D^\perp$ with $N(a) \neq 0$. Then by Theorem 2.3, $C = D \oplus Da$ and we have, for $x, y \in D$,

$$\phi(x + ya) = \phi(x) + \phi(y)\phi(a),$$

where $\phi(x), \phi(y) \in D$ and $\phi(a) \in D^\perp$. Note that $\phi(y)\phi(a) \in D^\perp = Da$. Define maps $u, v : D \to D$ by $u(x) = \phi(x)$ and $\phi(y)\phi(a) = v(y)a$ for $x, y \in D$. Thus

$$\phi(x + ya) = u(x) + v(y)a \quad (x, y \in D).$$

It is immediate that $u = \phi|D$ is an automorphism of D and v is orthogonal for the norm on D. It follows that

$$v(xy) = v(x)u(y), \qquad (x, y \in D).$$

Let $v(e) = p$, then $N(p) = 1$. We have,

$$v(y) = pu(y) \quad (y \in D).$$

Hence we have

$$\phi(x + ya) = u(x) + (pu(y))a \quad (x, y \in D).$$

By the Skolem-Noether theorem, there exists $c \in D$ with $N(c) \neq 0$ such that $u(x) = cxc^{-1} \quad (x \in D)$. Hence

$$\phi(x + ya) = cxc^{-1} + (pcyc^{-1})a \quad (x, y \in D).$$

Let us denote this automorphism by $\phi_{c,p}$. Conversely, for any $p \in D$ with $N(p) = 1$ and any $c \in D$ with $N(c) \neq 0$, the above formula defines an automorphism leaving D invariant. We summarise this below

Proposition 2.2. *Let C be an octonion algebra over k and D a quaternion subalgebra. Then the group $Aut(C, D)$ of atomorphisms of C leaving D invariant is given by*

$$Aut(C, D) = \{\phi_{c,p} | c \in D, N(c) \neq 0,\ p \in D,\ N(p) = 1\}.$$

Corollary 2.3. *The group $G_D = Aut(C/D)$ of automorphisms fixing D pointwise can be identified with the group of norm 1 elements of D. Let $\mathbf{G}_D$ denote the algebraic group of K-automorphisms of C_K that fix D_K pointwise. Then $\mathbf{G}_D$ is a closed subgroup of $\mathbf{G}$ and $\mathbf{G}_D(k) = G_D$. The group of norm 1 elements in D_K is isomorphic to $\mathbf{SL}_2 = SL(2, K)$. Hence $\mathbf{G}_D$ is a three dimensional connected algebraic group defined over k.*

We note that $\mathbf{G}$ is a subgroup of the stabilizer of e in $\mathbf{O}(N)$. Hence $\mathbf{G}$ leaves $e^\perp$ in C_K invariant. Let N_1 denote the restriction of N to $e^\perp$ in C. Let $\mathbf{H}$ denote the stabilizer of e in $\mathbf{SO}(N)$. Then we have

Proposition 2.3. *The restriction map*

$$Res : \mathbf{H} \to \mathbf{SO}(N_1),\ g \mapsto g|e^\perp,$$

is an isomorphism of algebraic groups, defined over k. In particular, we have an induced isomorphism $H = \mathbf{H}(k) \to SO(N_1)$.

The proof follows essentially from Witt's theorem. We are now ready to compute the dimension of $\mathbf{G}$.

Theorem 2.4. *The group $\mathbf{G}$ of automorphism of C_K is a connected algebraic group of dimension 14.*

Proof. Let X denote the set of special pairs in C_K. Then $X \neq \emptyset$ since K is algebraically closed. Using Witt's theorem we see that there is a linear isometry fixing e and mapping one special pair to another. It follows that $\mathbf{H}$ acts transitively on X. Let $(a, b),\ a, b \in D_K$ be a fixed special pair. Then the stabilizer $\mathbf{S}$ of (a, b) in $\mathbf{H}$ is isomorphic to $\mathbf{SO}(N_2)$, where N_2 is the restriction of N to $(Ke \oplus Ka \oplus Kb)^\perp$. Hence we have

$$dim(X) = dim(\mathbf{H}/\mathbf{S}) = dim(\mathbf{SO}(N_1)) - dim(\mathbf{SO}(N_2)) = \frac{1}{2}(7.6) - \frac{1}{2}(5.4) = 21 - 10 = 11.$$

By Corollary 2.2, $\mathbf{G}$ acts transitively on X. We now note that $\{e, a, b, ab\}$ is a basis of D_K. Hence the stabilizer of (a, b) in $\mathbf{G}$ is precisely $\mathbf{G}_D$, the algebraic group of automorphisms of C_K whose elements fix D_K pointwise. Therefore $dim(X) = 11 = dim(\mathbf{G}) - dim(\mathbf{G}_D)$. Hence

$$dim(\mathbf{G}) = 11 + dim(\mathbf{G}_D) = 11 + 3 = 14.$$

Now X is irreducible since $\mathbf{SO}(N_1)$ is irreducible. Also $\mathbf{G}_D$ is connected. This implies that $\mathbf{G}$ is connected. □

Proposition 2.4. *The rank of the group $\mathbf{G}$ of automorphism of C_K, C an octonion algebra over k, is 2.*

To prove this, we construct an explicit maximal torus in $\mathbf{G}$ and show it has the correct dimension.

A maximal torus of $\mathbf{G}$: We have seen that the (split) octonion algebra C_K can be viewed as $D_K \oplus D_K a$ with D_K the algebra of 2×2 matrices over K, with $N((x,y)) = det(x) - det(y)$. Let, for $t \in K^*,\ c_t$ denote the 2×2 diagonal matrix $diag(t, t^{-1})$. We then have

Lemma 2.2. *The group $\mathbf{T}$ of all automorphisms of C_K given by*

$$t_{\lambda,\mu} : x + ya \mapsto c_\lambda x {c_\lambda}^{-1} + (c_\mu y {c_\lambda}^{-1})a \quad (x, y \in D_K),$$

with $\lambda, \mu \in K^*$, is a 2-dimensional torus in $\mathbf{G}$. The centralizer of $\mathbf{T}$ in $\mathbf{G}$ is $\mathbf{T}$ and hence $\mathbf{T}$ is a maximal torus in $\mathbf{G}$.

Proof. We work with the basis $\{(e_{ij}, 0), (0, e_{ij}),\ 1 \le i, j \le 2\}$ of C_K, where e_{ij} is the 2×2 matrix with (i,j)-entry equal to 1 and other entries 0. With this, one has the matrix of $t_{\lambda,\mu}$ is

$$t_{\lambda,\mu} = diag(1, \lambda^2, \lambda^{-2}, 1, \lambda^{-1}\mu, \lambda\mu, \lambda^{-1}\mu^{-1}, \lambda\mu^{-1}).$$

It then follows (by a reparametrization) that T is a 2-dimensional torus. If $t \in \mathbf{G}$ centralizes $\mathbf{T}$, then t leaves invariant the eigenspaces of all $t_{\lambda,\mu}$. If λ, μ are chosen to ensure that $t_{\lambda,\mu}$ has seven distinct eigenvalues, then its eigenspaces are

$$K(e_{11}, 0) + K(e_{22}, 0), K(e_{12}, 0), K(e_{21}, 0), \quad K(0, e_{ij}),\ 1 \le i, j \le 2.$$

Hence t must leave D_K stable and therefore $t(x + ya) = cxc^{-1} + (pcyc^{-1})a, \quad (x, y \in D_K)$, where $c, p \in D_K,\ det(c) \neq 0,\ det(p) = 1$. Further analysis of the action on the eigenspaces shows that $c = c_\alpha$ for some $\alpha \in K^*$ and p is diagonal. Hence $t = t_{\alpha,\beta}$ for suitable $\alpha, \beta \in K^*$. □

Corollary 2.4. *The center of $\mathbf{G}$ is trivial.*

Proof. Let t belong to the center of $\mathbf{G}$. Then by the above lemma, $t \in \mathbf{T}$. Hence $t = t_{\lambda,\mu}$ for suitable parameters. Also t commutes with all automorphisms of C_K that leave D_K invariant, hence it must commute with all inner automorphisms of $D_K = M_2(K)$. Hence $\lambda^2 = 1$ and $t|D_K = 1$. This holds for all quaternion subalgebras and any element of C_K imbeds in a quaternion subalgebra (this can be shown using doubling), hence $t = 1$. □

Corollary 2.5. $\mathbf{G}$ *is reductive and* $|\Phi(\mathbf{G})| = 12$.

Proof. Grant for the moment the fact that $\mathbf{G}$ is reductive. We have shown dimension of $\mathbf{G}$ is 14 and $rank(\mathbf{G}) = 2$. Hence $|\Phi(\mathbf{G})| = 14 - 2 = 12$. For reductivity of $\mathbf{G}$, we will prove a general lemma that will be needed later for similar purpose. The proof now follows from the results below. □

Lemma 2.3. *Let V be a finite dimensional vector space and $\mathbf{G}$ a nontrivial connected algebraic subgroup of $\mathbf{GL}(V)$. Assume that G acts irreducibly on V. Then G is reductive.*

Proof. Let $\mathbf{U}$ denote the unipotent radical of $\mathbf{G}$ and let

$$V_0 = \{v \in V | \mathbf{U}v = v\} = V^{\mathbf{U}},$$

the subspace of fixed vectors of $\mathbf{U}$ in V. Then, since $\mathbf{U}$ is unipotent, $V_0 \neq 0$. If $v \in V_0$ and $g \in \mathbf{G}$, then for any $u \in \mathbf{U}$ we have, using normality of $\mathbf{U}$ in $\mathbf{G}$,

$$u(gv) = g(g^{-1}ug)(v) = gu'(v) = gv,$$

where $u' = g^{-1}ug$. Hence V_0 is $\mathbf{G}$-stable. Since V is irreducible for $\mathbf{G}$, it follows that $\mathbf{U} = \{1\}$. □

Theorem 2.5. *Let C be a composition algebra over k. Then the only invariant (nonzero) subspaces of C_K for $Aut(C_K)$ are Ke and $e^{\perp}$.*

Proof. When C is two dimensional, the assertion is trivial. So assume C is a quaternion algebra, so we may assume $C_K = M_2(K)$. By the Skolem-Noether theorem, every automorphism of $M_2(K)$ is inner. Now let V be an invariant subspace of C_K and choose $t \in M_2(K)$ a diagonal invertible matrix with distinct eigenvalues. Then by direct computation, we see that the eigenspaces of the inner automorphism $Int(t)$ are $Ke_{11} + Ke_{22}$ and $Ke_{12},\ Ke_{21}$. Hence V is spanned by vectors of the form $ae_{11} + be_{22},\ ce_{12},\ de_{21},\ \ a, b, c, d \in K$. Now we argue as follows. If $e_{12} \in V$, then for any $\alpha \in K$,

$$\begin{pmatrix} 1 & 0 \\ \alpha & 1 \end{pmatrix} e_{12} \begin{pmatrix} 1 & 0 \\ -\alpha & 1 \end{pmatrix} = \begin{pmatrix} -\alpha & 1 \\ -\alpha^2 & \alpha \end{pmatrix}$$

belongs to V. Therefore $e_{21} \in V$ and $e_{11} - e_{22} \in V$. This implies $e^{\perp} \subset V$. If $ae_{11} + be_{22} \in V$ for some $0 \neq a \neq b$, then one can show similarly that $e_{12},\ e_{21} \in V$. Therefore if neither of e_{12} and e_{21} belong to V then $V = Ke$. This settles the proof for quaternion algebras. Let now C be an octonion algebra and V be an inavriant subspace of C_K for $Aut(C_K)$. Let Q_1 be a quaternion subalgebra of C_K and let $V_1 = V \cap Q_1$. We have seen that every automorphism of Q_1 extends to an automorphism of C_K. Hence V_1 is an invariant subspace of Q_1 for $Aut(Q_1)$. Therefore $V_1 = 0, Ke, e^{\perp} \cap Q_1$ or Q_1. Let $Q_2,\ V_2$ be defined similarly for another quaternion subalgebra of C_K. But $Aut(C_K)$ acts transitively on the set of quaternion subalgebras. Hence there is $\phi \in Aut(C_K)$ such that $\phi(Q_1) = Q_2$. Then $\phi(V_1) = V_2$ and hence $V_2 = 0, Ke, e^{\perp} \cap Q_2$ or Q_2 according to the respective case for V_1. But every element of C_K is contained in some quaternion subalgebra, hence $V = 0, Ke, e^{\perp}$ or C_K. □

Corollary 2.6. $\mathbf{G} = Aut(C_K)$ *has a faithful irreducible representation (over K).*

Proof. The seven dimensional representation of $\mathbf{G}$ in $e^{\perp} \subset C_K$ is faithful and irreducible. □

We can now prove

Theorem 2.6. *The algebraic group* $\mathbf{G} = Aut(C_K)$*, for C an octonion algebra over k, is a connected simple algebraic group of type G_2.*

Proof. We have proved already that $\mathbf{G}$ is connected, reductive of rank 2 and has dimension 14. Since the center of $\mathbf{G}$ is trivial, it follows that G is in fact semisimple. We have also $|\Phi(\mathbf{G})| = 12$. Since the only the only reducible root system of rank 2 has 4 elements (namely, $A_1 \times A_1$), it follows that $\Phi(\mathbf{G})$ is irreducible. Now the list of irreducible root systems of rank 2 pins it down to type G_2. $\square$

Remark : One can show moreover that $\mathbf{G} = Aut(C_K)$ is defined over k for any octonion algebra (or composition algebra) C over k. It can be shown using Galois cohomology that all groups of type G_2 defined over k occur as above.

3 Albert algebras: $E_6,\ E_7$ and F_4

In this section we will describe an algebra whose automorphisms give a group of type F_4 defined over k and all such groups arise this way. We will then construct some groups of type E_6 and E_7 from such algerbas. We will assume now characteristic of k is different from 2 and 3. These are assumptions for the sake of simplicity of exposition, there are valid constructions over arbitrary characteristics.

Let k be a base field with characteristics other than $2, 3$. Let C be a composition algebra over k. Let $x \mapsto \overline{x}$ denote the canonical involution on C. Let $\gamma_1, \gamma_2, \gamma_3 \in k^*$ be fixed and define on $M_3(C)$, the (non-associative) algebra of 3×3 matrices with entries from C, an involution $X \mapsto X^* = \Gamma^{-1}\overline{X}^t\Gamma$, where $\Gamma = diag(\gamma_1, \gamma_2, \gamma_3)$ and $\overline{X}$ denotes the matrix obtained from X by applying the involution $x \mapsto \overline{x}$ (on C) to each entry and X^t denotes the transpose of X. Let $H_3(C, \Gamma)$ denote the set of $*$-hermitian matrices, i.e. $H_3(C, \Gamma) = \{X \in M_3(C) | X^* = X\}$. Then any $X \in H_3(C, \Gamma)$ has the form

$$X = \begin{pmatrix} \xi_1 & c_3 & \gamma_1^{-1}\gamma_3\overline{c}_2 \\ \gamma_2^{-1}\gamma_1\overline{c}_3 & \xi_2 & c_1 \\ c_2 & \gamma_3^{-1}\gamma_2\overline{c}_1 & \xi_3 \end{pmatrix}$$

where $\xi_i \in k$ and $c_i \in C$ for $1 \leq i \leq 3$. Define a product on $H_3(C, \Gamma)$ by $XY = \frac{1}{2}(X.Y + Y.X)$, where $X.Y$ denotes the usual matrix product. This is a commutative and non-associative multiplication with the 3×3 identity matrix e as multiplicative identity. On $A = H_3(C, \Gamma)$, we have a **trace** map, $T(X) = \xi_1 + \xi_2 + \xi_3$, which defines a quadratic form Q on A

$$Q(X) = \frac{1}{2}T(X^2) = \frac{1}{2}(\xi_1^2 + \xi_2^2 + \xi_3^2) + \gamma_3^{-1}\gamma_2 N(c_1) + \gamma_1^{-1}\gamma_3 N(c_2) + \gamma_2^{-1}\gamma_1 N(c_3)$$

for the coordinates of X as above. The bilinear form $\langle , \rangle$ associated to Q is nondegenerate and **associative**, i.e.,

$$\langle XY, Z\rangle = \langle X, YZ\rangle, \qquad (X, Y, Z \in A).$$

We call $A = H_3(C, \Gamma)$, for C an octonion algebra, a **reduced Albert algebra**. A k-algebra A is called an **Albert algebra** if for some field extension L of k, $A \otimes_k L \simeq H_3(C, \Gamma)$ over L, for some octonion algebra C over L and a diagonal invertible matrix $\Gamma \in M_3(L)$. Just like the usual matrix algebra, we have a **Cayley-Hamilton equation** that elements of $H_3(C, \Gamma)$ satisfy:

Proposition 3.1. *Every element $X \in H_3(C,\Gamma)$, C a composition algebra, satisfies a cubic equation*

$$X^3 - \langle X, e\rangle X^2 - (Q(X) - \frac{1}{2}\langle X, e\rangle^2)X - det(X)e = 0,$$

where det is a **cubic form** *on $H_3(C,\Gamma)$. (In fact $det(X)$ is the determinant of X computed as usual with brackets put carefully).*

The cubic polynomial that X above satisfies is called its **characteristic polynomial**. In terms of coordinates of X, one has

$$det(X) = \xi_1\xi_2\xi_3 - \gamma_3^{-1}\gamma_2\xi_1 N(c_1) - \gamma_1^{-1}\gamma_3\xi_2 N(c_2) - \gamma_2^{-1}\gamma_1\xi_3 N(c_3) + N(c_1c_2, \overline{c}_3),$$

where $N(,)$ denotes the bilinearization of N on C. The cubic form det determines a **symmetric trilinear form** $\langle\ ,\ ,\ \rangle$ with $\langle X, X, X\rangle = det(X)$. It can be shown that for any Albert algebra A there is a cubic form N on A, called its **norm form**, there is a linear form T on A, called its **trace form** (which in turn defines a quadratic form Q on A) and that every element of A satisfies its characteristic equation just as in the case of reduced Albert algebras.

The cross product on A : We define a product $\times$ on A as follows: for $X, Y \in A$, we define $X \times Y$ to be the (unique) element such that

$$\langle X \times Y, Z\rangle = 3\langle X, Y, Z\rangle \quad (Z \in A),$$

where the bilinear form on the left hand is the trace bilinear form on A. It follows by direct computation that $X(X\times X) = det(X)e$. From this, the above discussion and the proposition above we have

Corollary 3.1. *Let A be an Albert algebra over k. Then $x \in A$ is invertible if and only if $det(x) \neq 0$.*

Corollary 3.2. *Every automorphism of A preserves the cubic form det, the trace form T and the quadratic form Q.*

Idempotents in A : An element $u \in A = H_3(C,\Gamma)$ is an **idempotent** if $u^2 = u$. We have

Lemma 3.1. *If $u \neq 0, e$ is an idempotent in A then $det(u) = 0$ and $Q(u) = \frac{1}{2}$ or $Q(u) = 1$. If A contains an idempotent $\neq 0, e$ then it contains an idempotent u with $Q(u) = \frac{1}{2}$.*

We will call idempotents u with $Q(u) = \frac{1}{2}$ as **primitive idempotents**. It is straight forward that primitive idempotents cannot be decomposed as a sum of two **orthogonal** idempotents.

Automorphisms fixing a primitive idempotent : Let $A = H_3(C,\Gamma)$ be a reduced Albert algebra. Since A contains idempotents $\neq 0, e$, there is a primitive idempotent $u \in A$ by the lemma above. Let us fix this idempotent for what follows. define

$$E = (ke \oplus ku)^{\perp} = \{x \in A | \langle x, e\rangle = \langle x, u\rangle = 0\}.$$

One checks easily that the restriction of the (trace) quadratic form $Q(x) = \frac{1}{2}T(x^2)$ to $ke\oplus ku$ is nondegenerate, hence Q is nondegenerate on E as well. Now, for $x \in E$ we have

$$\langle ux, e\rangle = T((ux)e) = T(ux) = \langle u, x\rangle = 0, \ \ \langle ux, u\rangle = \langle xu, u\rangle = \langle x, u^2\rangle = \langle x, u\rangle = 0,$$

where T denotes the trace form on A. Hence we can define $t : E \to E$ by $t(x) = ux$. We then have

Lemma 3.2. *t is symmetric with respect to $\langle , \rangle$, i.e., $\langle t(x), y\rangle = \langle x, t(y)\rangle$ for all $x, y \in E$, and $t^2 = \frac{1}{2}t$. Moreover $E = E_0 \oplus E_1$, where $E_i = \{x \in E | t(x) = \frac{i}{2}x\}$.*

Proof. The symmetry of t follows from that of $\langle , \rangle$. By somewhat tedious computations, one can show that for $x \in E$ we have $2u(ux) = ux$. Hence $t^2 = \frac{1}{2}t$ follows. □

The subspaces E_0 and E_1 are respectively called the **zero space** and the **half space** of u. It can be shown easily that Q is nondegenerate on these spaces. Given $u = u_1$ a primitive idempotent, we can imbed u in a **reducing** set of primitive idempotents $\{u_1, u_2, u_3\}$, i.e., $u_1 + u_2 + u_3 = 1$ and $u_i u_j = 0$ for $i \neq j$. In the case when $u_i,\ 1 \leq i \leq 3$, are the diagonal idempotents in A, we have

$$E_1 = A_{12} \oplus A_{13}, \ \ E_0 = A_0 \cap (ku_2 \oplus ku_3 \oplus A_{23}) = k(u_2 - u_3) \oplus A_{23},$$

$$A_{23} = \left\{ \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & c_1 \\ 0 & \gamma_3^{-1}\gamma_2\bar{c}_1 & 0 \end{pmatrix} | c_1 \in C \right\},$$

$A_{12},\ A_{13}$ have similar descriptions and A_0 denotes the subspace of A consisting of trace zero elements. Hence $dim(E_0) = dim(ku_2 \oplus ku_3 \oplus A_{23} - 1 = 10 - 1 = 9$ and $dim(E_1) = 16$. Let $\mathbf{G}_u$ denote the algebraic subgroup of $\mathbf{G} = Aut(A_K)$ leaving u fixed. Then $\mathbf{G}_u$ is defined over k and $\mathbf{G}_u(k) = Aut(A)_u$. Any automorphism s of A fixing u stabilizes the zero and the half spaces of u. Since s is orthogonal (for Q), it induces orthogonal transformations $t : E_0 \to E_0$ and $v : E_1 \to E_1$. It then follows from the fact that s is an automorphism of A that

$$v(xy) = t(x)v(y), \quad (x \in E_0,\ y \in E_1).$$

We have

Proposition 3.2. *For every rotation t of E_0, there exists a similitude (for Q) v of E_1 such that*

$$v(xy) = t(x)v(y), \quad (x \in E_0,\ y \in E_1).$$

If $t = s_{a_1}s_{a_2}\cdots s_{a_{2r}}$ for some $a_i \in E_0$, then one may take for v

$$v(y) = a_1(a_2(\cdots(a_{2r}y)\cdots)) \quad (y \in E_1).$$

For any rotation t of E_0, the similarity v of E_1 such that the above holds is unique up to multiplication by a nonzero scalar. The square class of the similitude factor of v equals the spinor norm of t, i.e. $n(v) = \sigma(t)$. In addition, if t is an orthogonal transformation of E_0 which is not a rotation, then there does not exist any similitude v such that $v(xy) = t(x)v(y)$ for $x \in E_0,\ y \in E_1$.

Proof. See [SV]. □

Theorem 3.1. *Let A be a reduced Albert algebra as above over k, u be a primitive idempotent and E_0 and E_1 be the zero and the half spaces for u in A. The restriction map*

$$Res|E_0 : s \mapsto s|E_0 \quad (s \in Aut(A)_u)$$

is a homomorphism of $Aut(A_u)$ onto the reduced orthogonal group $O'(E_0, Q)$ with kernel of order 2.

Proof. Let $s \in Aut(A)_u$. Then s stabilizes E_0 and E_1 and induces orthogonal transformations t on E_0 and v on E_1, with $v(xy) = t(x)v(y)$ for $x \in E_0,\ y \in E_1$. By the above proposition, t is a rotation. Since v is orthogonal, we have $n(v) = 1 = \sigma(t)$. Hence we have a homomorphism

$$Res_{E_0} : Aut(A)_u \to O'(E_0, Q),\ s \mapsto s|E_0.$$

It can be shown that this homomorphism is surjective with kernel of order 2. □

Theorem 3.2. $\mathbf{G}_u$ *is isomorphic to* $\mathbf{Spin}(E_0, Q)$.

Proof. The group $\mathbf{Spin}(E_0, Q)$ is the subgroup of the even Clifford group $\Gamma^+(E_0, Q)$ consisting of elements $s = a_1a_2 \cdots a_{2r}$ with $a_i \in E_0$ and $Q(a_i) = 1$. Define $\psi : \mathbf{Spin}(E_0, Q) \to \mathbf{G}_u$ by $\psi(s)$ to be the linear map from A_K to itself which fixes u, e, stabilizes E_0 and E_1 and such that $\psi(s)|E_0 = s_{a_1}s_{a_2} \cdots s_{a_{2r}}$ and

$$\psi(s)|E_1(y) = a_1(a_2(\cdots(a_{2r}y)\cdots)) \quad (y \in E_1).$$

Then ψ is the required isomorphism of algebraic groups. □

Now we are ready to explore the automorphism group of an Albert algebra as an algebraic group.

Automorphism group of an Albert algebra : Let A be an Albert algebra over k. Let $\mathbf{G} = Aut(A_K)$. We need

Proposition 3.3. *Let* A *be an Albert algebra over* k *and* $\mathbf{G} = Aut(A_K)$. *Then* $\mathbf{G}$ *acts transitively on the set of all primitive idempotents of* A_K.

Theorem 3.3. $\mathbf{G}$ *is a connected simple algebraic group defined over* k *and of type* F_4.

Proof. To compute the dimension of $\mathbf{G}$ and to prove $\mathbf{G}$ is connected, we adopt an approach similar to the case of G_2. We look for an irreducible variety $\mathbf{V}$ on which $\mathbf{G}$ acts transitively and such that the stabilizer at a fixed point is a connected group whose dimension can be computed. Let $\mathbf{V}$ be the set of all primitive idempotents in A_K. It is clear that this is a closed subset of A_K. It can be shown that $\mathbf{V}$ is irreducible and $dim(\mathbf{V}) = 16$. If $u \in \mathbf{G}$, then we have seen that the stabilizer $\mathbf{G}_u$ is isomorphic to the Spin group of a 9-dimensional quadratic form, hence $dim(\mathbf{G}_u) = \frac{1}{2}9.8 = 36$. Therefore $dim(\mathbf{G}/\mathbf{G}_u) = dim(\mathbf{V}) = 16$ and hence $dim(\mathbf{G}) = 36 + 16 = 52$ and it follows from irreducibility of $\mathbf{V}$ and that $\mathbf{G}_u$ is connected that $\mathbf{G}$ is connected. We have, by a direct computation, for a fixed primitive idempotent $u \in A_K,\ \ e^\perp = K(e - 3u) \oplus E_0 \oplus E_1$. Since $\mathbf{G}$ leaves Q invariant, $\mathbf{G}$ stabilizes $W = e^\perp$. We calim that W is a faithful irreducible representation of $\mathbf{G}$, which in turn (by Lemma 2.3) would imply that $\mathbf{G}$ is reductive. Clearly $\mathbf{G}_u$ leaves $K(e - 3u), E_0$ and E_1 stable. We have seen that $\mathbf{G}_u$ acts on E_0 via rotations, hence this representation is irreducible for $\mathbf{G}_u$. The representation on E_1 of $\mathbf{G}_u$ is the **spin representation** of $\mathbf{Spin}(E_0, Q)$, which is irreducible. Hence W is the sum of three inequivalent irreducible representations of $\mathbf{G}_u$. By transitivity of $\mathbf{G}$ on $\mathbf{V}$ and the fact that any $\mathbf{G}$-invariant subspace of W is also $\mathbf{G}_u$ invariant, it follows that W is irreducible for $\mathbf{G}$. Faithfulness is immediate. We next show that the center of $\mathbf{G}$ is trivial. Let g be a central element in $\mathbf{G}$. Then g induces on W a scalar multiplication by α for some $\alpha \in K^*$. But g restricted to E_0 is a rotation, hence $\alpha = 1$ (recall $dim(E_0) = 9$).

Hence $\mathbf{G}$ is semisimple. Now we show $\mathbf{G}$ is simple. We can write (since center of $\mathbf{G}$ is trivial) $\mathbf{G} = \mathbf{G}_1 \times \mathbf{G}_2 \times \cdots \times \mathbf{G}_r$ with each $\mathbf{G}_i$ simple and $\mathbf{G}_i$ centralizes $\mathbf{G}_j$ for $i \neq j$. Since $\mathbf{G}$ is semisimple, $\mathbf{G}_i \cap \Pi_{j\neq i}\mathbf{G}_j = \{1\}$. Let π_i denote the projection of $\mathbf{G}$ onto $\mathbf{G}_i$. We have $\pi_i(\mathbf{G}_u) \neq \{1\}$ for some i, say $\pi_1(\mathbf{G}_u) \neq \{1\}$. Since $\mathbf{G}_u$ has finite center and is simple modulo center, of dimension 36, we have $dim(\pi_1(\mathbf{G}_u)) = 36$. Therefore $dim(\mathbf{G}_1) \geq 36$. But $dim(\mathbf{G}) = 52$, it follows that $\pi_i(\mathbf{G}_u) = \{1\}$ for $i > 1$. Hence $\mathbf{G}_u \subset \mathbf{G}_1$. Since $\mathbf{G}_i,\ i \neq 1$ centralize $\mathbf{G}_1$, they also centralize $\mathbf{G}_u$. For any $g \in \mathbf{G}$ that normalizes $\mathbf{G}_u$, $g(u)$ is fixed by $\mathbf{G}_u$ and $g(u)$ is an idempotent. But $\mathbf{G}_u$ fixes no other idempotent than u, hence $g(u) = u$ and hence the normalizer $N(\mathbf{G}_u) = \mathbf{G}_u$. Since $\mathbf{G}_i$'s normalize (in fact centralize) $\mathbf{G}_u$, we have $\mathbf{G}_i \subset \mathbf{G}_u \subset \mathbf{G}_1$ for $i > 1$. Hence $r = 1$ and $\mathbf{G}$ is simple. That $\mathbf{G}$ is of type F_4 follows by observing that any classical type simple group has dimension of the form $m(m-1)$ or $\frac{1}{2}m(m-1)$ for suitable m. The number 52 is not of this form and the only exceptional group of this dimension is F_4. □

Remark : Just as the case of G_2, all groups of type F_4 arise as algebraic groups of automorphisms of Albert algebras. The proof of this fact uses Galois cohomology.

The group of isometries of determinant on an Albert algebra : Let A be an albert algebra over k. We now wish to study the algebraic group $\mathbf{H}$ of linear transformations of A_K that leave the cubic form det on A_K fixed. This will shown to be connected of type E_6. Let $t : A \to A$ be an invertible linear map. Define $\widetilde{t} : A \to A$ by

$$\langle t(x), \widetilde{t}(y) \rangle = \langle x, y \rangle \quad (x, y \in A).$$

So $\widetilde{t}$ is the **contragradient** of t with respect to the trace bilinear form on A. It follows that

$$\widetilde{\widetilde{t}} = t, \ \ \widetilde{st} = \widetilde{s}\widetilde{t} \quad (s, t \in GL(A)).$$

We have

Proposition 3.4. *Let A be a reduced Albert algebra and H be the group of all invertible linear endomorphisms of A leaving $\det$ fixed. Then for $t \in GL(A),\ t \in H$ if and only if*

$$t(x) \times t(y) = \widetilde{t}(x \times y) \quad (x, y \in A).$$

Moreover, if $t \in H$ then $\widetilde{t} \in H$ and the map $t \mapsto \widetilde{t}$ is an outer automorphism of H of order 2.

We also need to know the orbits of the action of H on A.

Proposition 3.5. *Let A be a reduced Albert algebra and $a, b \in A$ with $det(a) = det(b) \neq 0$. Then there exists $t \in H$ with $t(a) = b$ if and only if the (nondegenerate) bilinear forms $det(a)^{-1}\langle x, y, a \rangle$ and $det(b)^{-1}\langle x, y, b \rangle$ are equivalent.*

We also need

Proposition 3.6. *Let A be an Albert algebra over k. Let $t \in GL(A)$. Then $t \in Aut(A)$ if and only if $t(e) = e$ and $t \in H$. In other words, $Aut(A)$ is the stabilizer subgroup of e in H.*

Theorem 3.4. $\mathbf{H}$ *is a connected (almost) simple, simply connected algebraic group of type* E_6 *defined over* k.

Proof. Observe that $dim(A_K) = 27$. One knows that det is an irreducible polynomial. Hence $\mathbf{W} = \{x \in A_K | det(x) = 1\}$ is an irreducible variety of dimension 26. By definition, $\mathbf{H}$ acts on $\mathbf{W}$. Since over an algebraically closed field any two nondegenerate symmetric bilinear forms of same dimension are equivalent, it follows from Proposition 3.5 that $\mathbf{H}$ acts transitively on A_K. By the Proposition 3.6, the stabilizer $\mathbf{H}_e$ of e in $\mathbf{H}$ is $\mathbf{G} = Aut(A_K)$, which is connected of dimension 52. Hence

$$dim(\mathbf{W}) = 26 = dim(\mathbf{H}/\mathbf{H}_e) = dim(\mathbf{H}) - dim(\mathbf{H}_e) = dim(\mathbf{H}) - 52.$$

Therefore, $dim(\mathbf{H}) = 78$. We have seen that $\mathbf{H}_e$ action on A_K has only irreducible subspaces Ke and $e^{\perp}$. It is evident that $\mathbf{H}$ leaves neither of these subspaces invariant. Hence A_K is a faithful irreducible representation of $\mathbf{H}$. By an earlier lemma, $\mathbf{H}$ is reductive. Any central element α must be a scalar (by Schur's lemma) and it follows that $\alpha^3 = 1$. Hence the center of $\mathbf{H}$ has order 3 and so $\mathbf{H}$ is semisimple. One shows with an argument similar to the F_4 case that $\mathbf{H}$ is in fact (almost) simple. The dimension of $\mathbf{H}$ combined with the simplicity allows B_6, C_6 or E_6 as possible root system types for $\mathbf{H}$. We have shown that $\mathbf{H}$ has an outer automorphism (see Proposition 3.4). Hence we rule out types B_6, C_6 and hence $\mathbf{H}$ is of type E_6. The center of $\mathbf{H}$ has order 3 implies that $\mathbf{H}$ is simply connected. □

Groups of type E_7 **:** Let A be an Albert algebra over k. Let

$$M = A \oplus A \oplus k \oplus k.$$

Then $dim(M) = 56$. Define a **quartic form** f on M as follows:

$$f((x, y, \alpha, \beta)) = T(x^{\#}y^{\#}) - \alpha N(x) - \beta N(y) - \frac{1}{4}(T(xy) - \alpha\beta)^2,$$

where $x^{\#} = x \times x$, $T(x)$ is the trace of x and $N(x)$ is the norm of x. Then f is a homogeneous polynomial function of degree 4 on M, defined over k. Under the natural action of $\mathbf{GL}(M)$ on M we have

Theorem 3.5. *The connected component (of identity) of the stabilizer of* f *in* $\mathbf{GL}(M)$ *is simply connected of type* E_7*, defined over* k.

Proof. See Springer's paper [S-2] for a proof. □

4 Tits' constructions of Albert algebras :

To make our exposition complete, we include Tits' constructions of Albert algebras. Tits gave two (rational) constructions of Albert algebras over an arbitrary field and showed that any Albert algebra arises from these constructions. These constructions put Albert algebras in a somewhat more uniform setting. We now describe these constructions.

The first construction : Let k be a base field as fixed before. Let D be a central simple (associative) algebra over k of degree 3. We will denote by D_+ the (special Jordan) algebra structure on D, with multiplication $x \cdot y = \frac{1}{2}(xy + yx),\ x, y \in D$. Let $\mu \in k^*$ be a scalar. Let N_D and T_D respectively denote the reduced norm and reduced trace maps on D. To this data, one associates an Albert algebra $J(D, \mu)$ as follows:

$$J(D, \mu) = D_0 \oplus D_1 \oplus D_2,$$

where $D_i,\ i = 0, 1, 2$, is a copy of D. For the multiplication on $J(D, \mu)$, we need more notation. For $a, b \in D$ define

$$a \cdot b = \frac{1}{2}(ab + ba),\ a \times b = 2a \cdot b - T_D(a)b - T_D(b)a + (T_D(a)T_D(b) - T_D(a \cdot b))$$

and $\widetilde{a} = \frac{1}{2}(T_D(a) - a)$. The multiplication on $J(D, \mu)$ is given by the formula :

$$(a_0, a_1, a_2)(b_0, b_1, b_2)$$

$$= (a_0 \cdot b_0 + \widetilde{a_1 b_2} + \widetilde{b_2 a_2}, \widetilde{a_0} b_1 + \widetilde{b_0} a_1 + (2\mu)^{-1} a_2 \times b_2, a_2 \widetilde{b_0} + b_2 \widetilde{a_0} + \frac{1}{2}\mu a_1 \times b_1).$$

It is known that $J(D, \mu)$ is an Albert algebra over k (see [KMRT] or [SV] for more details). Further, $J(D, \mu)$ is a **division algebra** if and only if μ is not a reduced norm from D. Clearly D_+ is a subalgebra of $J(D, \mu)$. Let A be an Albert algebra over k and let $D_+ \subset A$ for some degree 3 central simple algebra D. Then there exists $\mu \in k^*$ such that $A \simeq J(D, \mu)$.

Trace and Norm maps : Let $A = J(D, \mu)$ be as defined above. The trace T and the norm N on A are given by the formulae:

$$T(x, y, z) = T_D(x),\ \ N(x, y, z) = N_D(x) + \mu N_D(y) + \mu^{-1} N_D(z) - T_D(xyz).$$

From this, one gets an expression for the **trace bilinear form** on A, defined by, $T(x, y) = T(xy),\ x, y \in A$. Therefore, one has, for $x = (x_0, x_1, x_2),\ y = (y_0, y_1, y_2)$,

$$T(x, y) = T_D(x_0 y_0) + T_D(x_1 y_2) + T_D(x_2 y_1).$$

One knows that an Albert algebra A is a division algebra if and only if its norm form is anisotropic over k (see [SV],[J-3]).

The adjoint map : Let $A = J(D, \mu)$. One defines the adjoint map on A as follows. Let $x = (x_0, x_1, x_2)$. We define

$$x^{\#} = (x_0^{\#} - x_1 x_2, \mu^{-1} x_2^{\#} - x_0 x_1, \mu x_1^{\#} - x_2 x_0),$$

where, for $y \in D, 2y^{\#} = y \times y$ describes the usual adjoint map on D. One can prove that $xx^{\#} = x^{\#} x = N(x)$ for all $x \in A$ (see [J-3], [KMRT] for details).

The second construction : Let K/k be a quadratic extension and let (B, τ) be a central simple K-algebra of degree 3 over K with a unitary involution τ over K/k. Let $u \in B^*$ be such that $\tau(u) = u$ and $N_B(u) = \mu\overline{\mu}$ for some $\mu \in K^*$, here bar denotes the nontrivial k-automorphism of K and N_B is the reduced norm map on B. Let $\mathcal{H}(B, \tau)$ be the special Jordan algebra structure on the k-vector subspace of B of τ-symmetric elements in B, with multiplication as in B_+. Let $J(B, \tau, u, \mu) = \mathcal{H}(B, \tau) \oplus B$. With the notation introduced above, we define a multiplication on $J(B, \tau, u, \mu)$ by

$$(a_0, a)(b_0, b) = (a_0 \cdot b_0 + \widetilde{au\tau(b)} + \widetilde{bu\tau(a)}, \widetilde{a_0} b + \widetilde{b_0} a + \overline{\mu}(\tau(a) \times \tau(b)) u^{-1}).$$

Then $J(B,\tau,u,\mu)$ is an Albert algebra over k and is a division algebra if and only if μ is not a reduced norm from B. Clearly $\mathcal{H}(B,\tau)$ is a subalgebra of $J(B,\tau,u,\mu)$. It is known that if $\mathcal{H}(B,\tau)$ is a subalgebra of an Albert algebra A over k, then there are suitable parameters $u \in B^*$ and $\mu \in K^*$, where K is the centre of B, such that $A \simeq J(B,\tau,u,\mu)$ (see [J-3], [KMRT]).

Trace and Norm maps : Let $A = J(B,\tau,u,\mu)$ be an Albert algebra arising from the second construction. The trace T and the norm N on $J(B,\tau,u,\mu)$ are given by the formulae:

$$T(b_0,b) = T_B(b_0), \;\; N(b_0,b) = N_B(b_0) + \mu N_B(b) + \overline{\mu} N_B(\tau(b)) - T_B(b_0 b u \tau(b)).$$

From this, one gets an expression for the trace bilinear form on $J(B,\tau,u,\mu)$, defined by $T(x,y) = T(xy),\ x,y \in A$. Therefore, we have, for $x = (a_0,a), y = (b_0,b)$,

$$T(x,y) = T_B(a_0 b_0) + T_B(a u \tau(b)) + T_B(b u \tau(a)).$$

The Albert algebra $A = J(B,\tau,u,\mu)$ is a division algebra if and only if the norm form is anisotropic over k.

The adjoint map : Let $A = J(B,\tau,u,\mu)$ and $x = (a_0,a)$. In this case, the adjoint map is given by

$$x^{\#} = (a_0^{\#} - a u \tau(a), \overline{\mu}\tau(a)^{\#} u^{-1} - a_0 a),$$

where for $y \in B,\ 2y^{\#} = y \times y$ as defined above. One has $N(x) = x x^{\#} = x^{\#} x$ for all $x \in A$.

Remarks : It is known that all Albert algebras arise from the two constructions (see [KMRT]) and these constructions are not mutually exclusive: there are Albert algebras of mixed type and others are of pure type. Note that if A is a pure first construction Albert division algebra then every 9 dimensional subalgebra of A must necessarily be of the form D_+ for a degree 3 central division algebra D over k. There is a cohomological characterization of pure second construction Albert algebras. An Albert algebra A is a pure second construction if and only if $f_3(A) \neq 0$ (see [KMRT], 40.5). However, such a characterization for pure first construction Albert algebras does not seem to be available in the literature. It is well known that any cubic subfield of an Albert division algebra reduces it, i.e., if $L \subset A$ is a cubic subfield, where A is a division algebra over k, then $A \otimes L$ is reduced over L. Moreover, when A is a first construction, every cubic subfield is a splitting field for A (see [PR-1]). It is known that an Albert division algebra A over k remains division (in particular, $\mathbf{Aut}(A)$ remains anisotropic) over any extension of k of degree coprime to 3 (see [KMRT])

The structure group of Albert algebras : Recall that every Albert algebra comes equipped with a cubic form N, called the norm. The isometries of N form the k-rational points of a simply connected k-algebraic group of type E_6. This group contains the algebraic group $\mathbf{Aut}(A)$ of automorphisms of A. The group of similitudes of N is called the **structure group** of A and we denote it by $Str(A)$. This coincides with the group of k-rational points of a strict inner k-form of E_6, which we denote by $\mathbf{Str}(A)$. Let $a \in A$ and R_a denote the right multiplication by a acting on A. We let $U_a = 2R_a^2 - R_{a^2}$. Then $U_a \in Str(A)$ for all invertible $a \in A$. The (normal) subgroup generated by $U_a,\ a$ invertible, is called the **Inner structure group** of A and denoted by $Instr(A)$, this also is the group of k-points of a certain algebraic group $\mathbf{Instr(A)}$. The group $Aut(A) \cap Instr(A)$ is called the group of

inner automorphisms of A. Finally, recall that a norm isometry is an automorphism if and only if it fixes the identity element of A (see Proposition 3.6).

Moufang Hexagons of type $27/F$ and E_8 : We reproduce below some of the material from [TH], suited for this exposition. Let A be an Albert division algebra over k with norm map N and trace map T. Let U_1, U_3, U_5 be three groups isomorphic to the additive group $(A, +)$ and let U_2, U_4, U_6 be three groups isomorphic to the additive group $(k, +)$. Let x_i denote the isomorphism of $(A, +)$ or $(k, +)$ with U_i. We define a group U_+, generated by the U_i subject to the commutation relations as follows (see [TW] 8.13):

$$[U_1, U_2] = [U_2, U_3] = [U_3, U_4] = [U_4, U_5] = [U_5, U_6] = 1,$$

$$[U_2, U_4] = [U_4, U_6] = 1,$$
$$[U_1, U_4] = [U_2, U_5] = [U_3, U_6] = 1,$$
$$[x_1(a), x_3(b)] = x_2(T(a, b)),$$
$$[x_3(a), x_5(b)] = x_4(T(a, b)),$$
$$[x_1(a), x_5(b)] = x_2(-T(a^{\#}, b))x_3(a \times b)x_4(T(a, b^{\#})),$$
$$[x_2(t), x_6(u)] = x_4(tu),$$
$$[x_1(a), x_6(t)] = x_2(-tN(a))x_3(ta^{\#})x_4(t^2N(a))x_5(-ta),$$

for all $a, b \in A$ and all $t, u \in k$. Here, $[x, y]$ denotes the commutator $xyx^{-1}y^{-1}$ and $[U_i, U_j] = 1$ means U_i centralizes U_j. We construct a (bipartite) graph Γ from this data as follows: Let ϕ be a map from $\{1, 2, \cdots, 6\}$ to the set of subgroups of U_+ defined by :

$$\phi(i) = U_{[1,i]},\ 1 \leq i \leq 3,\ \ \phi(i) = U_{[i-3,3]}, 4 \leq i \leq 6,$$

where

$$U_{[i,j]} =< U_i, U_{i+1}, \cdots, U_j >,\ \ i \leq j < i + n;\ \ U_{[i,j]} = 1 \text{ otherwise}.$$

Let the vertex set of Γ be defined by

$$V(\Gamma) = \{(i, \phi(i)g) | 1 \leq i \leq 6,\ g \in U_+\},$$

where $\phi(i)g$ is the right coset of $\phi(i)$ containing g. The edge set of Γ is defined by

$$E(\Gamma) = \{((i, R), (j, S))|\ |i - j| = 1,\ R \cap S \neq \emptyset\},$$

here $|i-j|$ is computed modulo 6. This gives a graph $\Gamma = (V(\Gamma), E(\Gamma))$, which is completely determined (up to isomorphism) by the 7-tuple $(U_+, U_1, \cdots, U_6)$. We call the subgroups $U_i,\ 1 \leq i \leq 6$ the **root groups** of Γ. The graph Γ is the Tits building associated to the k-algebraic group of type E_8 (with index $E_{8,2}^{78}$, see [T] for the index notation) with anisotropic kernel the strict inner k-form of E_6 corresponding to the structure group of A. This graph is called a **Moufang hexagon** of type $27/F$, where $F = k$ if A is a first construction and a Moufang hexagon of type K/k if K/k is a separable quadratic extension of k and A is a second construction $J(B, \sigma, u, \mu)$ Albert division algebra, B a degree 3 central division algebra with a unitary involution σ over K/k .

Let G be the group of type preserving automorphisms of Γ and let $G^\dagger$ denote the subgroup of G generated by the root groups $U_i,\ 1 \leq i \leq 6$ of Γ (see [TW] for definition). Then, by (37.8, [TW]),

$$G/G^\dagger \simeq H/H^\dagger,$$

where H is the pointwise stabilizer in G of a 12-circuit in Γ and $H^\dagger = G^\dagger \cap H$.

In (37.41, [TW]) is proved that there is a canonical homomorphism from H to $Aut(k)$. Let H_0 be the kernel of this map. Then $H^\dagger \subset H_0$. Let G_0 be the subgroup of G containing $G^\dagger$ such that

$$G_0/G^\dagger = H_0/H^\dagger.$$

Then G_0 is the group of k-rational points $\mathbf{G}(k)$ for an algebraic group defined over k of types E_8 (and Tits index $E_{8,2}^{78}$). Following the notations in [TW], let X_1 denote the structure group of A ($Str(A)$ in our notation) and let $X_1^\dagger$ be the subgroup of X_1 generated by the U-operators $U_a,\ a \in A^*$ and the the scalar multiplications $x \mapsto tx,\ t \in k^*$ (note that $X_1^\dagger = C.Instr(A)$ in our notation). Then it is shown in (37.41, [TW]) that

$$H_0/H^\dagger \simeq X_1/X_1^\dagger.$$

By ([TW], 42.3.6), the root groups of Γ are precisely the groups $\mathcal{U}_\alpha(k)$, where α is a (nondivisible) root corresponding to a maximal split k-torus S in $\mathbf{G}$ and $\mathcal{U}_\alpha$ is the unipotent k-group corresponding to α. Also,

$$\mathbf{G}(k)/\mathbf{U}(k) = G_0/G^\dagger = H_0/H^\dagger \simeq X_1/X_1^\dagger = Str(A)/C.Instr(A),$$

where $\mathbf{U}(k)$ denotes the subgroup of $\mathbf{G}(k) = G_0$ generated by the k-rational points of the unipotent radicals of parabolic k-subgroups of $\mathbf{G}$. The **Kneser-Tits problem** is to determine if the quotient $\mathbf{G}(k)/\mathbf{U}(k)$ is trivial. The **Tits-Weiss conjecture** asserts that the quotient $G_0/G^\dagger \simeq Str(A)/C.Instr(A)$ is trivial. The conjecture is open in its full generality.

Invariants of Albert algebras : Let k be as before. Let k_s denote the separable closure of k and let $\Gamma = Gal(k_s/k)$. Let for any Γ-module M, $H^n(k, M)$ denote the nth **cohomology group** with coefficients in M (see [J-2]). The **cup product**

$$\cup : H^i(\Gamma, M_1) \times H^j(\Gamma, M_2) \to H^{i+j}(\Gamma, M_1 \otimes_{\mathbb{Z}} M_2)$$

is a bilinear map satisfying $c_i \cup c_j = (-1)^{ij} c_j \cup c_i$. Consider $\mathbb{Z}/2\mathbb{Z}$ with trivial Γ action. Then

$$H^1(k, \mu_2) \simeq H^1(k, \mathbb{Z}/2\mathbb{Z}) \simeq k^*/k^{*2}.$$

Let J be an Albert algebra over k with other notation as before. There exists a 3-fold Pfister form ϕ_3 and a 5-fold Pfister form ϕ_5 over k such that

$$Q \perp \phi_3 \simeq < 2, 2, 2 > \perp \phi_5$$

over k (cf. [S]). Further, this property characterizes ϕ_3 and ϕ_5 up to isometry. For an n-fold Pfister form $\phi_n = << a_1, a_2, \cdots, a_n >> = < 1, -a_1 > \otimes \cdots \otimes < 1, -a_n >$, one has the **Arason invariant** $A(\phi_n) \in H^n(k, \mathbb{Z}/2\mathbb{Z})$ given by

$$A(\phi_n) = (-a_1) \cup (-a_2) \cdots \cup (-a_n),$$

where, for $a \in k^*,\ (a)$ denotes the class of a in $H^1(k, \mathbb{Z}/2\mathbb{Z})$. The mod 2 invariants for J are defined as

$$f_3(J) = A(\phi_3),\ \ f_5(J) = A(\phi_5).$$

If $J = \mathcal{H}_3(C, \Gamma)$ then $f_3(J) = A(n_C)$ and $f_5(J) = A(< 1, \gamma_1^{-1}\gamma_2 > \otimes < 1, \gamma_2^{-1}\gamma_3 > \otimes n_C)$, where n_C is the norm on the Cayley algebra C, which is known to be a 3-fold Pfister form. Rost ([R]) attached an invariant mod 3 to J, denoted by $g_3(J)$, which is defined as follows. If $J = J(B, \sigma, u, \mu)$ for some central simple algebra B of degree 3 over a quadratic filed extension K of k, with an involution of second kind, then define

$$g_3(J) = -Cor_{K/k}([B] \cup [\mu]) \in H^3(k, \mathbb{Z}/3\mathbb{Z}),$$

and if $J = J(A, \nu)$ for a central simple algebra A of degree 3 over k, then define

$$g_3(J) = ([A] \cup [\nu]) \in H^3(k, \mathbb{Z}/3\mathbb{Z}).$$

These are independent of the expression of J as a first or a second Tits' construction (cf. [R], [PR-2]). Rost showed ([R]) that J is a division algebra if and only if $g_3(J) \neq 0$. Further, g_3 is compatible with base change. One of the questions on Albert algebras that is of central interest is if the isomorphism class of an Albert algebra is determined by its invariants. It is also of importance to find relations among the invariants and compute the image of the invariant map $J \mapsto (f_3(J), f_5(J), g_3(J))$.

Acknowledgement : I thank my student Miss Neha Hooda for her comments and suggestions, these were very helpful in making the exposition readable.

5 References

[B] A. Borel: Linear Algebraic Groups

[H] J. Humphreys: Linear Algebraic Groups

[J-1] Nathan Jacobson: Basic Algebra, Volume-1

[J-2] Nathan Jacobson: Basic Algebra, Volume-2

[J-3] Nathan Jacobson: Structure and Representations of Jordan Algebras

[KMRT] Max Knus, Merkurjev, Rost and Tignol: The Book of Involutions

[L] Serge Lang: Algebra

[L-1] T. Y. Lam: Algebraic Theory of Quadratic Forms

[PR-1] H. P. Petersson, M. Racine: Springer forms and the First Tits construction of Exceptional Jordan Division Algebras

[PR-2] H. P. Petersson, M. Racine: The Mod-3 Invariant of Albert algebras, an elementary approach

[R] Marcus Rost: A Mod-3 invariant for exceptional Jordan algebras

[S] J. P. Serre: Cohomology Galoisienne: Progress et problemes.

[SV] T. A. Springer and F. D. Veldkamp: Octonions, Jordan algebras and exceptional groups

[S-1] T. A. Springer: Linear Algebraic Groups

[S-2] T. A. Springer: Some Groups of Type E_7

[T] J. Tits: Classicfication of algebraic semisimple groups

[TH] Tom De Medts and Hendrik Van Maldeghem: Moufang Generalized Polygons

[TW] J. Tits and R. M. Weiss: Moufang Polygons