REALITY PROPERTIES OF CONJUGACY CLASSES IN G_2

BY

ANUPAM SINGH AND MANEESH THAKUR

Harish-Chandra Research Institute, Chhatnag Road
Jhunsi, Allahabad 211019, India
e-mail: anupam/maneesh@mri.ernet.in

ABSTRACT

Let G be an algebraic group over a field k. We call $g \in G(k)$ **real** if g is conjugate to g^{-1} in $G(k)$. In this paper we study reality for groups of type G_2 over fields of characteristic different from 2. Let G be such a group over k. We discuss reality for both semisimple and unipotent elements. We show that a semisimple element in $G(k)$ is real if and only if it is a product of two involutions in $G(k)$. Every unipotent element in $G(k)$ is a product of two involutions in $G(k)$. We discuss reality for G_2 over special fields and construct examples to show that reality fails for semisimple elements in G_2 over $\mathbb{Q}$ and $\mathbb{Q}_p$. We show that semisimple elements are real for G_2 over k with $cd(k) \leq 1$. We conclude with examples of nonreal elements in G_2 over k finite, with characteristic k not 2 or 3, which are not semisimple or unipotent.

1. Introduction

Let G be an algebraic group over a field k. It is desirable, from the representation theoretic point of view, to study conjugacy classes of elements in G. Borrowing the terminology from ([FZ]), we call an element $g \in G(k)$ **real** if g is conjugate to g^{-1} in $G(k)$. An **involution** in $G(k)$ is an element $g \in G(k)$ with $g^2 = 1$. Reality for classical groups over fields of characteristic $\neq 2$ has been studied in [MVW] by Moeglin, Vignéras and Waldspurger. That every element of a symplectic group over fields of characteristic 2 is a product of two involutions is settled in [Ni]. Feit and Zuckermann discuss reality for spin groups and symplectic groups in [FZ]. It is well known that every element of an orthogonal group is a product of two involutions (see [Wa] and [W2]). We plan to pursue

---

this for exceptional groups. In this paper, we study this property for groups of type G_2 over fields of characteristic different from 2, for both semisimple and unipotent elements. By consulting the character table of G_2 over finite fields in [CR], one sees that reality is not true for arbitrary elements of G_2 (see also Theorem 6.11 and Theorem 6.12, in this paper). Let G be a group of type G_2 over a field k of characteristic $\neq 2$. We prove that every unipotent element in $G(k)$ is a product of two involutions in $G(k)$. As it turns out, the case of semisimple elements in $G(k)$ is more delicate. We prove that a semisimple element in $G(k)$ is real in $G(k)$ if and only if it is a product of two involutions in $G(k)$ (Theorem 6.3). We call a torus in G **indecomposable** if it cannot be written as a direct product of two subtori, **decomposable** otherwise. We show that semisimple elements in decomposable tori are always real (Theorem 6.2). We construct examples of indecomposable tori in G containing non-real elements (Proposition 6.4 and Theorem 6.10). We work with an explicit realization of a group of type G_2 as the automorphism group of an octonion algebra. It is known (Chap. III, Prop. 5, Corollary, [Se]) that for a group G of type G_2 over k, there exists an octonion algebra $\mathfrak{C}$ over k, unique up to a k-isomorphism, such that $G \cong \mathrm{Aut}(\mathfrak{C})$, the group of k-algebra automorphisms of $\mathfrak{C}$. The group G is k-split if and only if the octonion algebra $\mathfrak{C}$ is split, otherwise G is anisotropic and $\mathfrak{C}$ is necessarily a division algebra. We prove that any semisimple element in $G(k)$ either leaves invariant a quaternion subalgebra or fixes a quadraticétale subalgebra pointwise (Lemma 6.1). In the first case, reality is a consequence of a theorem of Wonenburger (Th. 4, [W1]). In the latter case, the semisimple element belongs to a subgroup $SU(V,h) \subset G$, for a hermitian space (V,h) of rank 3 over a quadratic field extension L of k, or to a subgroup $SL(3) \subset G$. We investigate these cases separately in sections 6.1 and 6.2 respectively. We discuss reality for G_2 over special fields (Proposition 6.4, Theorem 6.10 and Theorem 6.11). We show that for k with $cd(k) \leq 1$ (e.g., k a finite field), every semisimple element in $G(k)$ is a product of two involutions in $G(k)$, and hence is real (Theorem 6.13). We show that nonreal elements exist in G_2 over k finite, with characteristic k not 2 or 3 (compare with [CR]); these are not semisimple or unipotent. We include a discussion of conjugacy classes of involutions in $G(k)$ over special fields. The work of [MVW] has played an important role in representation theory of p-adic groups. We hope the results in this paper will find applications in the subject.

2. The group G_2 and octonions

We begin by a brief introduction to the group G_2. Most of this material is from [SV]. Any group G of type G_2 over a given field k can be realized as the group of k-automorphisms of an octonion algebra over k, determined uniquely by G. We will need the notion of a composition algebra over a field k.

Definition: A composition algebra $\mathfrak{C}$ over a field k is an algebra over k, not necessarily associative, with an identity element 1 together with a nondegenerate quadratic form N on $\mathfrak{C}$, permitting composition, i.e., $N(xy) = N(x)N(y)\forall x, y \in \mathfrak{C}$.

The quadratic form N is called the **norm** on $\mathfrak{C}$. The associated bilinear form N is given by $N(x, y) = N(x + y) - N(x) - N(y)$. Every element x of $\mathfrak{C}$ satisfies the equation $x^2 - N(x, 1)x + N(x)1 = 0$. There is an involution (anti automorphism of order 2) on $\mathfrak{C}$ defined by $\bar{x} = N(x, 1)1 - x$. We call $N(x, 1)1 = x + \bar{x}$ the **trace** of x. The possible dimensions of a composition algebra over k are $1, 2, 4, 8$. Composition algebras of dimension 1 or 2 are commutative and associative, those of dimension 4 are associative but not commutative (called **quaternion** algebras), and those of dimension 8 are neither commutative nor associative (called **octonion** algebras).

Let $\mathfrak{C}$ be an octonion algebra and $G = \mathrm{Aut}(\mathfrak{C})$ be the automorphism group. Since any automorphism of an octonion algebra leaves the norm invariant, $\mathrm{Aut}(\mathfrak{C})$ is a subgroup of the orthogonal group $O(\mathfrak{C}, N)$. In fact, the automorphism group G is a subgroup of the rotation group $SO(N)$ and is contained in $SO(N_1) = \{t \in SO(N) \mid t(1) = 1\}$, where $N_1 = N|_{1^\perp}$. We have (Th. 2.3.5, [SV])

PROPOSITION 2.1: *The algebraic group $\mathcal{G} = \mathrm{Aut}(\mathfrak{C}_K)$, where $\mathfrak{C}_K = \mathfrak{C} \otimes K$ and K is an algebraic closure of k, is the split, connected, simple algebraic group of type G_2. Moreover, the automorphism group $\mathcal{G}$ is defined over k.*

In fact (Chap. III, Prop. 5, Corollary, [Se]), any simple group of type G_2 over a field k is isomorphic to the automorphism group of an octonion algebra $\mathfrak{C}$ over k. There is a dichotomy with respect to the norm of octonion algebras (in general, for composition algebras). The norm N is a **Pfister** form (tensor product of norm forms of quadratic extensions) and hence is either anisotropic or hyperbolic. If N is anisotropic, every nonzero element of $\mathfrak{C}$ has an inverse in $\mathfrak{C}$. We then call $\mathfrak{C}$ a **division** octonion algebra. If N is hyperbolic, up to isomorphism, there is only one octonion algebra with N as its norm, called the **split** octonion algebra. We give below a model for the split octonion algebra

over a field k. Let

$$\mathfrak{C} = \left\{ \begin{pmatrix} \alpha & v \\ w & \beta \end{pmatrix} \mid \alpha, \beta \in k; v, w \in k^3 \right\},$$

where k^3 is the three-dimensional vector space over k with standard basis. On k^3 we have a nondegenerate bilinear form, given by $\langle v, w \rangle = \sum_{i=1}^{3} v_i w_i$, where $v = (v_1, v_2, v_3)$ and $w = (w_1, w_2, w_3)$ in k^3 and the wedge product on k^3 is given by $\langle u \wedge v, w \rangle = \det(u, v, w)$ for $u, v, w \in k^3$. Addition on $\mathfrak{C}$ is entry-wise and the multiplication on $\mathfrak{C}$ is given by

$$\begin{pmatrix} \alpha & v \\ w & \beta \end{pmatrix} \begin{pmatrix} \alpha' & v' \\ w' & \beta' \end{pmatrix} = \begin{pmatrix} \alpha\alpha' - \langle v, w' \rangle & \alpha v' + \beta' v + w \wedge w' \\ \beta w' + \alpha' w + v \wedge v' & \beta\beta' - \langle w, v' \rangle \end{pmatrix}.$$

The quadratic form N, the norm on $\mathfrak{C}$, is given by

$$N \begin{pmatrix} \alpha & v \\ w & \beta \end{pmatrix} = \alpha\beta + \langle v, w \rangle.$$

An octonion algebra over a field k can be defined as an algebra over k which, after changing base to a separable closure k_s of k, becomes isomorphic to the split octonion algebra over k_s (see [T]).

2.1 OCTONIONS FROM RANK 3 HERMITIAN SPACES.

We briefly recall here from [T] a construction of octonion algebras from rank 3 hermitian spaces over a quadraticétale algebra over k. First we recall (cf. [KMRT])

Definition: Let $\mathcal{E}$ be a finite-dimensional k-algebra. Then $\mathcal{E}$ is called an étale algebra if $\mathcal{E} \otimes_k k_s \cong k_s \times \cdots \times k_s$, where k_s is a separable closure of k.

Let L be a quadratic étale algebra over k with $x \mapsto \overline{x}$ as its standard involution. Let (V, h) be a rank 3 hermitian space over L, i.e., V is an L-module of rank 3 and $h \colon V \times V \longrightarrow L$ is a nondegenerate hermitian form, linear in the first variable and sesquilinear in the second. Assume that the discriminant of (V, h) is trivial, i.e., $\bigwedge^3 (V, h) \cong (L, <1>)$, where $<1>$ denotes the hermitian form $(x, y) \mapsto x\overline{y}$ on L. Fixing a trivialization $\psi \colon \bigwedge^3 (V, h) \cong (L, <1>)$, we define a vector product $\times \colon V \times V \longrightarrow V$ by the identity

$$h(u, v \times w) = \psi(u \wedge v \wedge w),$$

for $u, v, w \in V$. Let $\mathfrak{C}$ be the 8-dimensional k-vector space $\mathfrak{C} = C(L; V, h, \psi) = L \oplus V$. We define a multiplication on $\mathfrak{C}$ by

$$(a, v)(b, w) = (ab - h(v, w), aw + \overline{b}v + v \times w), \quad a, b \in L, v, w \in V.$$

With this multiplication, $\mathfrak{C}$ is an octonion algebra over k with norm $N(a,v) = N_{L/k}(a) + h(v,v)$. Note that L embeds in $\mathfrak{C}$ as a composition subalgebra. The isomorphism class of $\mathfrak{C}$, thus obtained, does not depend on ψ. One can show that all octonion algebras arise this way. We need the following (Th. 2.2, [T])

PROPOSITION 2.2: *Let (V,h) and (V',h') be isometric hermitian spaces with trivial discriminant, over a quadratic étale algebra L. Then the octonion algebras $C(L;V,h)$ and $C(L;V',h')$ are isomorphic, under an isomorphism restricting to the identity map on the subalgebra L.*

We also need the following

LEMMA 2.1: *Let L be a quadratic field extension of k. Let (V,h) be a rank three hermitian space over L with trivial discriminant. For any trivialization ψ of the discriminant, the octonion algebra $\mathfrak{C}(L;v,h,\psi)$ is a division algebra, if and only if the k-quadratic form on V, given by $Q(x) = h(x,x)$, is anisotropic.*

We note that a similar construction for quaternion algebras can be done, starting from a rank 3 quadratic space V over k, with trivial discriminant. Let $B\colon V \times V \longrightarrow k$ be a nondegenerate bilinear form. Assume that the discriminant of (V,B) is trivial, i.e., $\bigwedge^3(V,B) \cong (k, <1>)$, where $<1>$ denotes the bilinear form $(x,y) \mapsto xy$ on k. Fixing a trivialization $\psi\colon \bigwedge^3(V,B) \cong (k, <1>)$, we define a vector product $\times\colon V \times V \longrightarrow V$ by the identity $B(u, v \times w) = \psi(u \wedge v \wedge w)$, for $u,v,w \in V$. Let Q be the 4-dimensional k-vector space $Q = Q(k;V,B,\psi) = k \oplus V$. We define a multiplication on Q by

$$(a,v)(b,w) = (ab - B(v,w), aw + bv + v \times w), \quad a,b \in k, v,w \in V.$$

With this multiplication, Q is a quaternion algebra over k, with norm $N(a,v) = a^2 + B(v,v)$. The isomorphism class of Q thus obtained does not depend on ψ. One can show that all quaternion algebras arise this way.

PROPOSITION 2.3: *Let (V,B) and (V',B') be isometric quadratic spaces with trivial discriminants, over a field k. Then the quaternion algebras $Q(k;V,B)$ and $Q(k;V',B')$ are isomorphic.*

3. Some subgroups of G_2

Let $\mathfrak{C}$ be an octonion algebra over a field k of characteristic $\neq 2$. Let L be a composition subalgebra of $\mathfrak{C}$. In this section, we describe subgroups of $G =$

$\mathrm{Aut}(\mathfrak{C})$, consisting of automorphisms leaving L pointwise fixed or invariant. We define

$$G(\mathfrak{C}/L) = \{t \in \mathrm{Aut}(\mathfrak{C}) | t(x) = x \forall x \in L\}$$

and

$$G(\mathfrak{C}, L) = \{t \in \mathrm{Aut}(\mathfrak{C}) | t(x) \in L \forall x \in L\}.$$

Jacobson studied $G(\mathfrak{C}/L)$ in his paper ([J]). We mention the description of these subgroups here. One knows that two-dimensional composition algebras over k are precisely the quadratic étale algebras over k (cf. Th. 33.17, [KMRT]). Let L be a two-dimensional composition subalgebra of $\mathfrak{C}$. Then L is either a quadratic field extension of k or $L \cong k \times k$. Let us assume first that L is a quadratic field extension of k and $L = k(\gamma)$, where $\gamma^2 = c.1 \neq 0$. Then $L^\perp$ is a left L vector space via the octonion multiplication. Also,

$$h \colon L^\perp \times L^\perp \longrightarrow L$$
$$h(x, y) = N(x, y) + \gamma^{-1} N(\gamma x, y)$$

is a nondegenerate hermitian form on $L^\perp$ over L. Any automorphism t of $\mathfrak{C}$, fixing L pointwise, induces an L-linear map $t|_{L^\perp} \colon L^\perp \longrightarrow L^\perp$. Then we have (Th. 3, [J])

PROPOSITION 3.1: *Let the notation be as fixed above. Let L be a quadratic field extension of k as above. Then the subgroup $G(\mathfrak{C}/L)$ of G is isomorphic to the unimodular unitary group $SU(L^\perp, h)$ of the three-dimensional space $L^\perp$ over L relative to the hermitian form h, via the isomorphism,*

$$\psi \colon G(\mathfrak{C}/L) \longrightarrow SU(L^\perp, h)$$
$$t \longmapsto t|_{L^\perp}.$$

Now, let us assume that L is a split two-dimensional étale sublagebra of $\mathfrak{C}$. Then $\mathfrak{C}$ is necessarily split and L contains a nontrivial idempotent e. There exists a basis $B = \{1, u_1, u_2, u_3, e, w_1, w_2, w_3\}$ of $\mathfrak{C}$, called the **Peirce basis** with respect to e, such that the subspaces $U = \mathrm{span}\{u_1, u_2, u_3\}$ and $W = \mathrm{span}\{w_1, w_2, w_3\}$ satisfy $U = \{x \in \mathfrak{C} | ex = 0,\ xe = x\}$ and $W = \{x \in \mathfrak{C} | xe = 0,\ ex = x\}$. We have, for $\eta \in G(\mathfrak{C}/L)$, $x \in U$,

$$0 = \eta(ex) = \eta(e)\eta(x) = e\eta(x), \quad \eta(x)e = \eta(x)\eta(e) = \eta(xe) = \eta(x).$$

Hence $\eta(U) = U$. Similarly, $\eta(W) = W$. Then we have (Th. 4, [J])

PROPOSITION 3.2: *Let the notation be as fixed above. Let L be a split quadratic étale subalgebra of $\mathfrak{C}$. Then $G(\mathfrak{C}/L)$ is isomorphic to the unimodular linear group $SL(U)$, via the isomorphism given by*

$$\phi\colon G(\mathfrak{C}/L) \longrightarrow SL(U)$$

$$\eta \longmapsto \eta|_U.$$

Moreover, if we denote the matrix of $\eta|_U$ by A and that of $\eta|_W$ by A_1, with respect to the Peirce basis as above, then ${}^t A_1 = A^{-1}$.

In the model of the split octonion algebra as in the previous section, with respect to the diagonal subalgebra L, the subspaces U and W are respectively the space of strictly upper triangular and strictly lower triangular matrices. The above action is then given by

$$\eta \begin{pmatrix} \alpha & v \\ w & \beta \end{pmatrix} = \begin{pmatrix} \alpha & Av \\ {}^t A^{-1} w & \beta \end{pmatrix}.$$

We now compute the subgroup $G(\mathfrak{C}, L)$ of automorphisms of the split octonion algebra, leaving invariant a split quadratic étale subalgebra. We work with the matrix model for split octonions. Up to conjugacy by an automorphism, we may assume that the split subalgebra is the diagonal subalgebra. We consider the map ρ on $\mathfrak{C}$ given by

$$\rho\colon \mathfrak{C} \longrightarrow \mathfrak{C}$$

$$\begin{pmatrix} \alpha & v \\ w & \beta \end{pmatrix} \mapsto \begin{pmatrix} \beta & w \\ v & \alpha \end{pmatrix}.$$

Then ρ leaves the two-dimensional subalgebra

$$L = \left\{ \begin{pmatrix} \alpha & 0 \\ 0 & \beta \end{pmatrix} \mid \alpha, \beta \in k \right\}$$

invariant and it is an automorphism of $\mathfrak{C}$, with $\rho^2 = 1$.

PROPOSITION 3.3: *Let $\mathfrak{C}$ be the split octonion algebra as above and let L be the diagonal split quadratic étale subalgebra. Then we have*

$$G(\mathfrak{C}, L) \cong G(\mathfrak{C}/L) \rtimes H,$$

where H is the order two group generated by ρ.

Proof: Let $h \in G(\mathfrak{C}, L)$. Then $h|_L = 1$ or the nontrivial k-automorphism of L. In the first case, $h \in G(\mathfrak{C}/L)$ and in the second, $h\rho \in G(\mathfrak{C}/L)$. Hence $h = g\rho$ for

some $g \in G(\mathfrak{C}/L)$. Moreover, it is clear that H normalizes $G(\mathfrak{C}/L)$ in $\mathrm{Aut}(\mathfrak{C})$. Since $H \cap G(\mathfrak{C}/L) = \{1\}$, we get the required result. ∎

We now give a general construction of the automorphism ρ of an octonion algebra $\mathfrak{C}$, not necessarily split, as above. We first recall the Cayley–Dickson Doubling for composition algebras:

PROPOSITION 3.4: *Let $\mathfrak{C}$ be a composition algebra and $\mathfrak{D} \subset \mathfrak{C}$ a composition subalgebra, $\mathfrak{D} \neq \mathfrak{C}$. Let $a \in \mathfrak{D}^{\perp}$ with $N(a) = -\lambda \neq 0$. Then $\mathfrak{D}_1 = \mathfrak{D} \oplus \mathfrak{D}a$ is a composition subalgebra of $\mathfrak{C}$ of dimension $2\dim(\mathfrak{D})$. The product on $\mathfrak{D}_1$ is given by*

$$(x + ya)(u + va) = (xu + \lambda \overline{v}y) + (vx + y\overline{u})a, \quad x, y, u, v \in \mathfrak{D},$$

where $x \mapsto \overline{x}$ is the involution on $\mathfrak{D}$. The norm on $\mathfrak{D}_1$ is given by $N(x + ya) = N(x) - \lambda N(y)$.

Let $\mathfrak{C}$ be an octonion algebra, and $L \subset \mathfrak{C}$ a quadratic composition subalgebra of $\mathfrak{C}$. Let $a \in L^{\perp}$ with $N(a) \neq 0$. Let $\mathfrak{D} = L \oplus La$ be the double as described above. Then $\mathfrak{D}$ is a quaternion subalgebra of $\mathfrak{C}$. Define $\rho_1 : \mathfrak{D} \to \mathfrak{D}$ by $\rho_1(x + ya) = \sigma(x) + \sigma(y)a$, where σ denotes the nontrivial automorphism of L. Then ρ_1 is an automorphism of $\mathfrak{D}$, and clearly $\rho_1^2 = 1$ and $\rho_1|_L = \sigma$. We now repeat this construction with respect to $\mathfrak{D}$ and ρ_1. Write $\mathfrak{C} = \mathfrak{D} \oplus \mathfrak{D}b$ for some $b \in \mathfrak{D}^{\perp}$, $N(b) \neq 0$. Define $\rho : \mathfrak{C} \to \mathfrak{C}$ by

$$\rho(x + yb) = \rho_1(x) + \rho_1(y)b.$$

Then $\rho^2 = 1$ and $\rho|_L = \sigma$ and ρ is an automorphism of $\mathfrak{C}$. One can prove that this construction yields the one given above for the split octonion algebra and its diagonal subalgebra. We have

PROPOSITION 3.5: *Let $\mathfrak{C}$ be an octonion algebra, possibly division, and $L \subset \mathfrak{C}$ a quadratic composition subalgebra. Then $G(\mathfrak{C}, L) \cong G(\mathfrak{C}/L) \rtimes H$, where H is the subgroup generated by ρ and ρ is an automorphism of $\mathfrak{C}$ with $\rho^2 = 1$ and ρ restricted to L is the nontrivial k-automorphism of L.*

We mention a few more subgroups of $\mathrm{Aut}(\mathfrak{C})$ before closing this section. Let $\mathfrak{D} \subset \mathfrak{C}$ be a quaternion subalgebra. Then we have, by Cayley–Dickson doubling, $\mathfrak{C} = \mathfrak{D} \oplus \mathfrak{D}a$ for some $a \in \mathfrak{D}^{\perp}$ with $N(a) \neq 0$. Let $\phi \in \mathrm{Aut}(\mathfrak{C})$ be such that $\phi(x) = x$ for all $x \in \mathfrak{D}$. Then for $z = x + ya \in \mathfrak{C}$, we have $\phi(z) = \phi(x) + \phi(y)\phi(a)$. But $a \in \mathfrak{D}^{\perp}$ implies $\phi(a) \in \mathfrak{D}^{\perp} = \mathfrak{D}a$. Therefore $\phi(a) = pa$ for some $p \in \mathfrak{D}$ and, by taking norms, we see that $p \in SL_1(\mathfrak{D})$. In fact, we have (Prop. 2.2.1, [SV])

PROPOSITION 3.6: *The group of automorphisms of $\mathfrak{C}$, leaving $\mathfrak{D}$ pointwise fixed, is isomorphic to $SL_1(\mathfrak{D})$, the group of norm 1 elements of $\mathfrak{D}$. In the above notation, $G(\mathfrak{C}/\mathfrak{D}) \cong SL_1(\mathfrak{D})$.*

We describe yet another subgroup of $\mathrm{Aut}(\mathfrak{C})$. Let $\mathfrak{D}$ be as above and $\phi \in \mathrm{Aut}(\mathfrak{D})$. We can write $\mathfrak{C} = \mathfrak{D} \oplus \mathfrak{D}a$ as above. Define $\widetilde{\phi} \in \mathrm{Aut}(\mathfrak{C})$ by $\widetilde{\phi}(x + ya) = \phi(x) + \phi(y)a$. Then one checks easily that $\widetilde{\phi}$ is an automorphism of $\mathfrak{C}$ that extends ϕ on $\mathfrak{D}$. These automorphisms form a subgroup of $\mathrm{Aut}(\mathfrak{C})$, which (we will abuse notation and) we continue to denote by $\mathrm{Aut}(\mathfrak{D})$.

PROPOSITION 3.7: *With notation as fixed, we have*

$$G(\mathfrak{C}, \mathfrak{D}) \cong G(\mathfrak{C}/\mathfrak{D}) \rtimes \mathrm{Aut}(\mathfrak{D}).$$

Proof: Clearly $\mathrm{Aut}(\mathfrak{D}) \cap G(\mathfrak{C}/\mathfrak{D}) = \{1\}$ and $\mathrm{Aut}(\mathfrak{D})$ normalizes $G(\mathfrak{C}/\mathfrak{D})$. Now, for $\psi \in G(\mathfrak{C}, \mathfrak{D})$, consider the automorphism $\phi = \psi \widetilde{\psi}^{-1}$. Then ϕ fixes elements of H pointwise and we have $\psi = \phi \widetilde{\psi} \in G(\mathfrak{C}/\mathfrak{D}) \rtimes \mathrm{Aut}(\mathfrak{D})$. ∎

4. Involutions in G_2

In this section, we discuss the structure of involutions in G_2. Let G be a group of type G_2 over k and $\mathfrak{C}$ be an octonion algebra over k with $G = \mathrm{Aut}(\mathfrak{C})$. We call an element $g \in G(k)$ an **involution** if $g^2 = 1$. Hence nontrivial involutions in $G(k)$ are precisely the automorphisms of $\mathfrak{C}$ of order 2. Let g be an involution in $\mathrm{Aut}(\mathfrak{C})$. The eigenspace corresponding to the eigenvalue 1 of $g \in \mathrm{Aut}(\mathfrak{C})$ is the subalgebra $\mathfrak{D}$ of $\mathfrak{C}$ of fixed points of g and is a quaternion subalgebra of $\mathfrak{C}$ ([J]). The orthogonal complement $\mathfrak{D}^\perp$ of $\mathfrak{D}$ in $\mathfrak{C}$ is the eigenspace corresponding to the eigenvalue -1. Conversely, the linear automorphism of $\mathfrak{C}$, leaving a quaternion subalgebra $\mathfrak{D}$ of $\mathfrak{C}$ pointwise fixed and acting as multiplication by -1 on $\mathfrak{D}^\perp$, is an involutorial automorphism of $\mathfrak{C}$ (see Proposition 3.6). Let ρ be an involution in $G(k)$ and let $\mathfrak{D}$ be the quaternion subalgebra of $\mathfrak{C}$, fixed pointwise by ρ. Let $\rho' = g\rho g^{-1}$ be a conjugate of ρ by an element $g \in G(k)$. Then, the quaternion subalgebra $\mathfrak{D}' = g(\mathfrak{D})$ of $\mathfrak{C}$ is fixed pointwise by ρ'. Conversely, suppose the quaternion subalgebra $\mathfrak{D}$ of $\mathfrak{C}$ is isomorphic to the quaternion subalgebra $\mathfrak{D}'$ of $\mathfrak{C}$. Then, by a Skolem–Noether type theorem for composition algebras (Cor. 1.7.3, [SV]), there exists an automorphism g of $\mathfrak{C}$ such that $g(\mathfrak{D}) = \mathfrak{D}'$. If ρ denotes the involution leaving $\mathfrak{D}$ fixed pointwise, $\rho' = g\rho g^{-1}$ fixes $\mathfrak{D}'$ pointwise. Therefore, we have

PROPOSITION 4.1: *Let $\mathfrak{C}$ be an octonion algebra over k. Then the conjugacy classes of involutions in $G = \mathrm{Aut}(\mathfrak{C})$ are in bijection with the isomorphism classes of quaternion subalgebras of $\mathfrak{C}$.*

COROLLARY 4.1: *Assume that ${}_2Br(k)$, the 2-torsion in the Brauer group of k, is trivial, i.e., all quaternion algebras over k are split (for example, $cd(k) \leq 1$ fields). Then all involutions in $G(k)$ are conjugates.*

We need a refinement of a theorem of Jacobson (Th. 2, [J]), due to Wonenburger (Th. 5, [W1]) and Neumann ([N]),

PROPOSITION 4.2: *Let $\mathfrak{C}$ be an octonion algebra over a field k of characteristic different from 2. Then every element of G is a product of 3 involutions.*

We will study in the sequel the structure of semisimple elements in $G(k)$, in terms of involutions. We will show that a semisimple element $g \in G(k)$ is real, i.e., conjugate to g^{-1} in $G(k)$, if and only if g is a product of 2 involutions in $G(k)$.

5. Maximal tori in SU_n

We need an explicit description of maximal tori in the special unitary group of a nondegenerate hermitian space for our work; we discuss it in this section (cf. [R], Section 3.4). Let k be a field of characteristic different from 2 and L a quadratic field extension of k. Let V be a vector space of dimension n over L. We denote by k_s a separable closure of k containing L. Let h be a nondegenerate hermitian form on V, i.e., $h\colon V \times V \longrightarrow L$ is a nondegenerate k-bilinear map such that

$$h(\alpha x, y) = \alpha h(x,y), \quad h(x, \beta y) = \sigma(\beta)h(x,y), \quad h(x,y) = \sigma(h(y,x)),$$
$$\forall x, y \in V, \ \alpha, \beta \in L,$$

where σ is the nontrivial k-automorphism of L. Let $\mathcal{E}$ be an étale algebra over k. It then follows that the bilinear form $T\colon \mathcal{E} \times \mathcal{E} \longrightarrow k$, induced by the trace: $T(x,y) = tr_{\mathcal{E}/k}(xy)$ for $x, y \in \mathcal{E}$, is nondegenerate.

LEMMA 5.1: *Let L be a quadratic field extension of k. Let $\mathcal{E}$ be an étale algebra over k containing L, equipped with an involution σ, restricting to the non-trivial k-automorphism of L. Let $\mathcal{F} = \mathcal{E}^\sigma = \{x \in \mathcal{E} | \sigma(x) = x\}$. Let $dim_L(\mathcal{E}) = n$. For $u \in \mathcal{F}^*$, define*

$$h^{(u)}\colon \mathcal{E} \times \mathcal{E} \longrightarrow L$$
$$h^{(u)}(x,y) = tr_{\mathcal{E}/L}(ux\sigma(y)).$$

Then $h^{(u)}$ is a nondegenerate σ-hermitian form on $\mathcal{E}$, left invariant by $T_{(\mathcal{E},\sigma)} = \{\alpha \in \mathcal{E}^* | \alpha\sigma(\alpha) = 1\}$, under the action by left multiplication.

Proof: That $h^{(u)}$ is a hermitian form is clear. To check nondegeneracy, let $h^{(u)}(x,y) = 0 \forall y \in \mathcal{E}$. Then, $tr_{\mathcal{E}/L}(ux\sigma(y)) = 0 \ \forall y \in \mathcal{E}$, i.e., $tr_{\mathcal{E}/L}(xy') = 0 \ \forall y' \in \mathcal{E}$. Since $\mathcal{E}$ is étale, it follows that $x = 0$. Therefore $h^{(u)}$ is nondegenerate. Now let $\alpha \in T_{(\mathcal{E},\sigma)}$. We have

$$h^{(u)}(\alpha x, \alpha y) = tr_{\mathcal{E}/L}(u\alpha x\sigma(\alpha y)) = tr_{\mathcal{E}/L}(ux\sigma(y)) = h^{(u)}(x,y).$$

Hence the last assertion.   ∎

Remark: We note that $\mathcal{E} = \mathcal{F} \otimes_k L$. If we put $\mathcal{F}' = \{x \in \mathcal{E} | \sigma(x) = -x\}$, then $\mathcal{E} = \mathcal{F} \oplus \mathcal{F}'$. Further, if $L = k(\gamma)$ with $\gamma^2 \in k^*$, then $\mathcal{F}' = \mathcal{F}\gamma$.

Notation: In what follows, we shall often deal with situations when, for an algebraic group G defined over k, and for any extension K of k, the group $G(K)$ of K-rational points in G coincides with $G(k) \otimes_k K$. When no confusion is likely to arise, we shall abuse notation and use G to denote both the algebraic group as well as its group of k-points. We shall identify $T_{(\mathcal{E},\sigma)}$ with its image in $U(\mathcal{E}, h^{(u)})$, under the embedding via left homotheties.

LEMMA 5.2: With notation as in the previous lemma, $T_{(\mathcal{E},\sigma)}$ is a maximal k-torus in $U(\mathcal{E}, h^{(u)})$, the unitary group of the hermitian space $(\mathcal{E}, h^{(u)})$.

The proof is a tedious, straightforward computation; we omit it here.

COROLLARY 5.1: Let $T^1_{(\mathcal{E},\sigma)} = \{\alpha \in \mathcal{E}^* | \alpha\sigma(\alpha) = 1, \det(\alpha) = 1\}$. Then $T^1_{(\mathcal{E},\sigma)} \subset SU(\mathcal{E}, h^{(u)})$ is a maximal k-torus.

THEOREM 5.1: Let k be a field and L a quadratic field extension of k. We denote by σ the nontrivial k-automorphism of L. Let V be a L-vector space of dimension n with a nondegenerate σ-hermitian form h. Let $T \subset U(V,h)$ be a maximal k-torus. Then there exists $\mathcal{E}_T$, an étale L-algebra of dimension n over L, with an involution σ_h restricting to the nontrivial k-automorphism of L, such that

$$T = T_{(\mathcal{E}_T, \sigma_h)}.$$

Moreover, if $\mathcal{E}_T$ is a field, there exists $u \in \mathcal{F}^*$ such that (V,h) is isomorphic to $(\mathcal{E}_T, h^{(u)})$ as a hermitian space.

Proof: Let $A = End_L(V)$. Then A is a central simple L-algebra. Let $\mathcal{E}_T = \mathcal{Z}_A(T)$, the centralizer of T in A. Note that $T \subset \mathcal{E}_T$. The hermitian form h

defines the adjoint involution σ_h on A,

$$\sigma_h \colon A \longrightarrow A$$
$$h(\sigma_h(f)(x), y) = h(x, f(y))$$

for all $x, y \in V$. Then σ_h is an involution of second kind over L/k on A (cf. [KMRT]). We claim that σ_h restricts to $\mathcal{E}_T$: Let $f \in \mathcal{E}_T$; we need to show $\sigma_h(f) \in \mathcal{E}_T$, i.e., $\sigma_h(f)t = t\sigma_h(f) \forall t \in T$. This follows from

$$h(\sigma_h(f)t(x), y) = h(t(x), f(y)) = h(x, t^{-1}f(y)) = h(x, ft^{-1}(y))$$
$$= h(\sigma_h(f)(x), t^{-1}y) = h(t\sigma_h(f)(x), y).$$

We have $T \subset U(V, h) \subset \mathrm{End}_L(V)$ and σ_h is an involution on $\mathrm{End}_L(V)$, restricting to the nontrivial k-automorphism of L. There is a canonical isomorphism of algebras with involutions (Chap. I, Prop. 2.15, [KMRT])

$$(\mathrm{End}_L(V) \otimes_k k_s, \sigma_h) \cong (\mathrm{End}_{k_s}(V) \times \mathrm{End}_{k_s}(V), \epsilon),$$

where $\epsilon(A, B) = (B, A)$. Since $U(V, h) = \{A \in \mathrm{End}_L(V) | A\sigma_h(A) = 1\}$, we have

$$U(V, h) \otimes_k k_s \cong \{(A, B) \in \mathrm{End}_L(V) \otimes_k k_s | (A, B).\epsilon(A, B) = 1\}$$
$$= \{(A, A^{-1}) | A \in \mathrm{End}_{k_s}(V)\}.$$

We thus have an embedding

$$T \otimes_k k_s \longrightarrow \mathrm{End}_{k_s}(V) \times \mathrm{End}_{k_s}(V), A \mapsto (A, A^{-1}).$$

To prove $\mathcal{E}_T$ is étale, we may conjugate $T \otimes k_s$ to the diagonal torus in $GL_n(k_s)$. The embedding then becomes

$$T \otimes_k k_s \cong (k_s^*)^n \longrightarrow M_n(k_s) \times M_n(k_s),$$
$$(t_1 \ldots t_n) \mapsto (\mathrm{diag}(t_1, \ldots, t_n), \mathrm{diag}(t_1^{-1}, \ldots, t_n^{-1})).$$

Now, we have

$$\mathcal{E}_T \otimes_k k_s = \mathcal{Z}_A(T) \otimes_k k_s = \mathcal{Z}_{A \otimes_k k_s}(T \otimes_k k_s)$$
$$\cong \mathcal{Z}_{M_n(k_s) \times M_n(k_s)}(\{(\mathrm{diag}(t_1, \ldots, t_n), \mathrm{diag}(t_1^{-1}, \ldots, t_n^{-1})) | t_i \in k_s^*\}) = k_s^{2n}.$$

Hence $\mathcal{E}_T$ is an étale algebra of k-dimension $2n$ and L-dimension n. We have $T \subset T_{(\mathcal{E}_T, \sigma_h)}$ and, by dimension count, $T = T_{(\mathcal{E}_T, \sigma_h)}$. We have on V the natural left $\mathrm{End}_L(V)$-module structure. Since $\mathcal{E}_T$ is a subalgebra of $\mathrm{End}_L(V)$ and a field, V is a left $\mathcal{E}_T$-vector space of dimension 1. Let $V = \mathcal{E}_T.v$ for $v \neq 0$.

Let us consider the dual $V^* = \mathrm{Hom}_L(V, L)$, which is a left-$\mathcal{E}_T$-vector space of dimension 1 via the action: $(\alpha.f)(x) = f(\alpha(x))$, $\alpha \in \mathcal{E}_T$, $x \in V$. We consider the following elements in V^*:

$$\phi_1 \colon V = \mathcal{E}_T.v \longrightarrow L$$
$$fv \mapsto h(f(v), v),$$
$$\phi_2 \colon V = \mathcal{E}_T.v \longrightarrow L$$
$$fv \mapsto tr(f).$$

Since $\mathcal{E}_T$ is separable, both these are nonzero elements of V^*. Hence there exists $u \in \mathcal{E}_T^*$ such that $h(f(v), v) = tr(uf) \forall f \in \mathcal{E}_T$. We have

$$h(f.v, g.v) = h(f(v), g(v)) = h(\sigma_h(g)f(v), v) = tr(u\sigma_h(g)f) \quad \forall f, g \in \mathcal{E}_T.$$

This will prove the lemma provided we show $u \in F$. For any $f \in \mathcal{E}_T$ we have

$$tr(\sigma_h(u)f) = tr(\sigma_h(u).\sigma_h(\sigma_h(f))) = \sigma_h(tr(u\sigma_h(f)))$$
$$= \sigma_h(h(\sigma_h(f)(v), v)) = h(v, \sigma_h(f)(v)) = h(f(v), v) = tr(uf).$$

Since $\mathcal{E}_T$ is separable, the trace form is nondegenerate and hence $\sigma_h(u) = u$. The map

$$\Phi \colon (V, h) \longrightarrow (\mathcal{E}_T, h^{(u)}), \quad fv \mapsto f$$

is an isometry:

$$h^{(u)}(\Phi(fv), \Phi(gv)) = tr(u\sigma_h(g)f) = h(fv, gv)$$

by the computation done above.   ∎

COROLLARY 5.2: *Let the notation be as fixed above. Let T be a maximal torus in $SU(V, h)$. Then there exists an étale algebra $\mathcal{E}_T$ over L of dimension n, such that $T \cong T^1_{(E_T, \sigma_h)}$.*

Remark: The hypothesis in the last assertion in Theorem 5.1, that $\mathcal{E}_T$ be a field, is only a simplifying assumption. The result holds good even when $\mathcal{E}_T$ is not a field.

Let $T \subset SU(V, h)$ be a maximal torus. Then from the proof of Theorem 5.1 we get $\mathcal{E}_T = \mathcal{Z}_{\mathrm{End}(V)}(T')$ is an étale algebra with involution σ_h such that $T = T^1_{(\mathcal{E}_T, \sigma_h)}$; here, T' is a maximal torus in $U(V, h)$.

LEMMA 5.3: *With notation as above, V is an irreducible representation of T if and only if $\mathcal{E}_T$ is a field.*

Proof: Suppose $\mathcal{E}_T$ is not a field. Then $\exists\, 0 \neq f \in \mathcal{E}_T$ such that $V \neq ker(f) \neq 0$. Put $W = ker(f) \subset V$, which is a L-vector subspace. We claim that W is a T invariant subspace. Let $x \in W, t \in T$:

$$f(x) = 0 \Rightarrow t(f(x)) = 0 \Rightarrow f(t(x)) = 0 \Rightarrow t(x) \in W.$$

Hence, $T(W) = W$.

Conversely, let $\mathcal{E}_T$ be a field and $0 \neq W \subset V$ be a T-invariant L-subspace of V. We shall show that $V = W$. We know that V is a one-dimensional $\mathcal{E}_T$ vector space. Thus, it suffices to show that W is an $\mathcal{E}_T$ subspace of V. Suppose first that k is infinite. Let $t \in T(k)$ be a regular element (see [Bo], Prop. 8.8 and the Remark on page 116). Then $\mathcal{E}_T = L[t]$ and we have, for $f(t) \in \mathcal{E}_T$, $f(t)(W) = W$, since W is T-invariant. Now let k be finite. Then $\mathcal{E}_T$ is a finite field and its multiplicative group $\mathcal{E}_T^*$ is cyclic. The group $T(k)$, being a subgroup of $\mathcal{E}_T^*$, is cyclic. Then a cyclic generator t of $T(k)$ is a regular element and, arguing as above, we are done in this case too. ∎

We defined the notion of **indecomposable tori** in the introduction; these are tori which cannot be written as a direct product of subtori.

COROLLARY 5.3: *Let T be a maximal torus in $SU(V, h)$. Then T is indecomposable if and only if V is an irreducible representation of T; that is, if and only if $\mathcal{E}_T$ is a field.*

Proof: By the above lemma, if V is reducible as a representation of T, $\mathcal{E}_T$ is not a field. Hence it must be a product of at least two (separable) field extensions of L, say $\mathcal{E}_T = E_1 \times \cdots \times E_r$. Then from Corollary 5.2, $T = T^1_{\mathcal{E}_T} = T^1_{E_1} \times \cdots \times T^1_{E_r}$. Hence T is decomposable. Conversely, suppose V is irreducible as a representation of T. Then, by the above lemma, $\mathcal{E}_T$ is a field. Suppose the torus T decomposes as $T = T_1 \times T_2$ into a direct product of two proper subtori. Suppose first that k is infinite. Let $t \in T(k)$ be a regular element (see [Bo], Prop. 8.8 and the Remark on page 116). Then the minimal polynomial (= characteristic polynomial) $\chi(X)$ of t factorizes over k, as can be seen by base changing to k_s and conjugating T to the diagonal torus in $SL(n)$. Therefore $\mathcal{E}_T = L[X]/\chi(X)$ is not a field, a contradiction. Hence T is indecomposable. When k is finite, the multiplicative group $\mathcal{E}_T^*$ of $\mathcal{E}_T$ is cyclic and hence $T(k)$ is

cyclic. A cyclic generator t of $T(k)$ is then regular and we repeat the above argument to reach a contradiction. Hence T is indecomposable.   ∎

6. Reality in G_2

Let G be a group of type G_2 defined over a field k of characteristic $\neq 2$. Then, there exists an octonion algebra $\mathfrak{C}$ over k such that $G \cong \mathrm{Aut}(\mathfrak{C})$ (Chap. III, Prop. 5, Corollary, [Se]). Let t_0 be a semisimple element of $G(k)$. We will also denote the image of t_0 in $\mathrm{Aut}(\mathfrak{C})$ by t_0. We write $\mathfrak{C}_0$ for the subspace of trace 0 elements of $\mathfrak{C}$. In this section, we explore the question if t_0 is conjugate to t_0^{-1} in $G(k)$. We put $V_{t_0} = ker(t_0 - 1)^8$. Then V_{t_0} is a composition subalgebra of $\mathfrak{C}$ with norm as the restriction of the norm on $\mathfrak{C}$ ([W1]). Let $r_{t_0} = \dim(V_{t_0} \cap \mathfrak{C}_0)$. Then r_{t_0} is $1, 3$ or 7. We have

LEMMA 6.1: *Let the notation be as fixed above and let $t_0 \in G(k)$ be semisimple. Then, either t_0 leaves a quaternion subalgebra invariant or fixes a quadratic étale subalgebra L of $\mathfrak{C}$ pointwise. In the latter case, $t_0 \in SU(V, h) \subset G(k)$ for a rank 3 hermitian space V over a quadratic field extension L of k or $t_0 \in SL(3) \subset G(k)$.*

Proof: From the above discussion, we see that r_{t_0} is $1, 3$ or 7. If $r_{t_0} = 3$, t_0 leaves a quaternion subalgebra $\mathfrak{D}$ of $\mathfrak{C}$ invariant. As in Proposition 3.6, writing $\mathfrak{C} = \mathfrak{D} \oplus \mathfrak{D}a$ for $a \in \mathfrak{D}^\perp$, $N(a) \neq 0$, t_0 is explicitly given by $t_0(x + ya) = cxc^{-1} + (pcyc^{-1})a$ for some $c \in \mathfrak{D}$, $N(c) \neq 0$ and $p \in \mathfrak{D}$, $N(p) = 1$. We now assume $r_{t_0} = 7$. In this case, the minimal polynomial of t_0 on $\mathfrak{C}_0$ is $(X - 1)^7$. But since t_0 is semisimple, the minimal polynomial of t_0 is a product of distinct linear factors over the algebraic closure. Therefore $t_0 = 1$. In the case $r_{t_0} = 1$, $L = V_{t_0}$ is a two-dimensional composition subalgebra and has the form $V_{t_0} = k.1 \oplus (V_{t_0} \cap \mathfrak{C}_0)$, an orthogonal direct sum. Let $L \cap \mathfrak{C}_0 = k.\gamma$ with $N(\gamma) \neq 0$. Since t_0 leaves $\mathfrak{C}_0$ and V_{t_0} invariant, we have $t_0(\gamma) = \gamma$ and hence $t_0(x) = x \forall x \in L$, so that $t_0 \in G(\mathfrak{C}/L)$. The result now follows from Proposition 3.1 and Proposition 3.2.   ∎

If t_0 leaves a quaternion subalgebra invariant, it is a product of two involutions and hence real in $G(k)$. This follows from the following theorem (see Th. 4, [W1]).

THEOREM 6.1: *Let $\mathfrak{C}$ be an octonion algebra. If g is an automorphism of $\mathfrak{C}$ which maps a quaternion subalgebra $\mathfrak{D}$ into itself, then g is a product of two involutory automorphisms.*

COROLLARY 6.1: *If an automorphism g of $\mathfrak{C}$ leaves a nondegenerate plane of $\mathfrak{C}_0$ invariant, then it is a product of two involutory automorphisms.*

We discuss the other cases here, i.e., t_0 leaves a quadratic étale subalgebra L of $\mathfrak{C}$ pointwise fixed.

1. The fixed subalgebra L is a quadratic field extension of k

and

2. The fixed subalgebra is split, i.e., $L \cong k \times k$.

By the discussion in section 3, in the first case, t_0 belongs to $G(\mathfrak{C}/L) \cong SU(L^\perp, h)$ (Proposition 3.1) and in the second case t_0 belongs to $G(\mathfrak{C}/L) \cong SL(3)$ (Proposition 3.2). We denote the image of t_0 by A in both of these cases. We analyse further the cases when the characteristic polynomial of A is reducible or irreducible.

THEOREM 6.2: *Let t_0 be a semisimple element in $G(k)$ and suppose t_0 fixes the quadratic étale subalgebra L of $\mathfrak{C}$ pointwise. Let us denote the image of t_0 by A in $SU(L^\perp, h)$ or in $SL(3)$ as the case may be. Also assume that the characteristic polynomial of A over L in the first case and over k in the second, is reducible. Then t_0 is a product of two involutions in $G(k)$.*

Proof: Let us consider the case when L is a field extension. Let T be a maximal torus in $SU(L^\perp, h)$ containing t_0. By Corollary 5.2, there exists an étale L-algebra $\mathcal{E}_T$ with an involution σ and $u \in \mathcal{F}^*$ such that $(L^\perp, h) \cong (\mathcal{E}_T, h^{(u)})$; here, $\mathcal{F}$ is the fixed point subalgebra of σ in $\mathcal{E}_T$. Since the characteristic polynomial of A is reducible, we see that $L^\perp$ is a reducible representation of T. From Corollary 5.3 we see that $\mathcal{E}_T$ is not a field. We can write $\mathcal{E}_T \cong \mathcal{F} \otimes L$ where $\mathcal{F}$ is a cubic étale k-algebra but not a field. Let $\mathcal{F} = k \times \Delta$, for some quadratic étale k-algebra Δ. Hence $\mathcal{E}_T \cong L \times \Delta \otimes L$ and σ is given by $(\alpha, f \otimes \beta) \mapsto (\bar{\alpha}, f \otimes \bar{\beta})$. Writing $u = (u_1, u_2)$ where $u_1 \in k$, the hermitian form $h^{(u)}$ is given by $h^{(u)}((l, \delta), (l', \delta')) = tr_{L/L}(lu_1 l') + tr_{\Delta \otimes L/L}(\delta u_2 \delta') = lu_1 l' + tr_{\Delta \otimes L/L}(\delta u_2 \delta')$. Hence $L \times \{0\}$ is a nondegenerate subspace left invariant by the action of $t_0 \in T^1_{(\mathcal{E}_T, \sigma_h)} \cong T^1_L \times T^1_{\Delta \otimes L}$, which acts by left multiplication. Therefore t_0 leaves invariant a two-dimensional nondegenerate k-plane invariant in $\mathfrak{C}_0$. The result now follows from Corollary to Theorem 6.1. The proof in the case when L is split proceeds on similar lines. ∎

In general, we have the following

THEOREM 6.3: *Let G be a group of type G_2 over a field k of characteristic not 2. Then every unipotent element in $G(k)$ is a product of two involutions in*

$G(k)$. Let $g \in G(k)$ be a semisimple element. Then g is real in $G(k)$ if and only if it is a product of two involutions in $G(k)$.

Proof: The assertion about unipotents in $G(k)$ follows from a theorem of Wonenburger (Th. 4, [W1]), which asserts that if the characteristic polynomial of $t \in \text{Aut}(\mathfrak{C})$ is divisible by $(x - 1)^3$, t is a product of two involutory automorphisms of $\mathfrak{C}$.

In view of Theorem 6.2, we need to consider only the semisimple elements in $SU(L^\perp, h)$ or in $SL(3)$ with irreducible characteristic polynomials. By Corollary 5.3, it follows that such elements lie in indecomposable tori. The result follows from the following theorem.   ∎

THEOREM 6.4: Let t_0 be an element in $G(k)$ and suppose t_0 fixes a quadratic étale subalgebra L of $\mathfrak{C}$ pointwise. Let us denote the image of t_0 by A in $SU(L^\perp, h)$ or in $SL(3)$ as the case may be. Also assume that the characteristic polynomial of A over L in the first case and over k in the second is irreducible. Then t_0 is conjugate to t_0^{-1} in $G(k)$ if and only if t_0 is a product of two involutions in $G(k)$.

Proof: We distinguish the cases of both these subgroups below and complete the proof in the next two subsections; see Theorem 6.6 and Theorem 6.9.   ∎

6.1 $SU(V, h) \subset G$.   We assume that L is a quadratic field extension of k. Let t_0 be an element in $G(\mathfrak{C}/L)$ with characteristic polynomial of the restriction to $V = L^\perp$, irreducible over L. We write $\mathfrak{C} = L \bigoplus V$, where V is an L-vector space with hermitian form h induced by the norm on $\mathfrak{C}$. Then we have seen that $G(\mathfrak{C}/L) \cong SU(V, h)$ (Theorem 3.1).

LEMMA 6.2: Let the notation be as fixed above. Let t_0 be an element in $G(\mathfrak{C}/L)$ with characteristic polynomial irreducible over L. Suppose that $\exists g \in G(k)$ such that $g t_0 g^{-1} = t_0^{-1}$. Then $g(L) = L$.

Proof: Suppose that $g(L) \not\subset L$. Then we claim that $\exists x \in L \cap \mathfrak{C}_0$ such that $g(x) \notin L$. For this, let $y \in L$ be such that $g(y) \notin L$. Let $x = y - \frac{1}{2} tr(y) 1$. Then $tr(x) = 0$ and if $g(x) \in L$ then $g(y) \in L$, a contradiction. Hence we have $x \in L \cap \mathfrak{C}_0$ with $g(x) \notin L$. Also, since $t_0(x) = x$, we have

$$t_0(g(x)) = g t_0^{-1}(x) = g(x).$$

Let $g(x) = \alpha + y$, for $0 \neq y \in L^\perp$; then $t_0(g(x)) = \alpha + t_0(y) = \alpha + y$, i.e., $t_0(y) = y$. Therefore t_0 fixes an element in $L^\perp$. This implies that the

characteristic polynomial of t_0 on $L^\perp = V$ is reducible, a contradiction. Hence, $g(L) = L$. ∎

We recall a construction from Proposition 3.5. Let $a \in L^\perp$ with $N(a) \neq 0$. Let $\mathfrak{D} = L \oplus La$ and $\rho_1 \colon \mathfrak{D} \to \mathfrak{D}$ be defined by $\rho_1(x + ya) = \sigma(x) + \sigma(y)a$. Write again $\mathfrak{C} = \mathfrak{D} \oplus \mathfrak{D}b$ for $b \in \mathfrak{D}^\perp$ with $N(b) \neq 0$ and define $\rho \colon \mathfrak{C} \to \mathfrak{C}$ by $\rho(x + yb) = \sigma(x) + \sigma(y)b$. Then ρ is an automorphism of $\mathfrak{C}$ of order 2 which restricts to L to the nontrivial automorphism of L. The basis

$$\{f_1 = a, f_2 = b, f_3 = ab\}$$

of $V = L^\perp$ over L is an orthogonal basis for h. **We fix this basis throughout this section**. Let us denote the matrix of h with respect to this basis by $H = \text{diag}(\lambda_1, \lambda_2, \lambda_3)$ where $\lambda_i = h(f_i, f_i) \in k^*$. Then $SU(V, h)$ is isomorphic to $SU(H) = \{A \in SL(3, L) | {}^t A H \bar{A} = H\}$.

THEOREM 6.5: *With notation fixed as above, let A be the matrix of t_0 in $SU(H)$ with respect to the fixed basis described above. Let the characteristic polynomial of A be irreducible over L. Then t_0 is conjugate to t_0^{-1} in $G(k)$, if and only if $\bar{A}$ is conjugate to A^{-1} in $SU(H)$, where the entries of $\bar{A}$ are obtained by applying σ on the entries of A.*

Proof: Let $g \in G(k)$ be such that $g t_0 g^{-1} = t_0^{-1}$. In view of Lemma 6.2, we have $g(L) = L$. We have (Prop. 3.5) $G(\mathfrak{C}, L) \cong G(\mathfrak{C}/L) \rtimes N$ where $N = <\rho>$ and ρ is an automorphism of $\mathfrak{C}$, described above. Clearly g does not belong to $G(\mathfrak{C}/L)$. For if so, we can conjugate t_0 to t_0^{-1} in $G(\mathfrak{C}/L) \cong SU(H)$. But then the characteristic polynomial $\chi(X) = X^3 - \bar{a}X^2 + aX - 1$, where $a \in L$, and $\bar{a} = a$. Hence $\chi(X)$ is reducible, a contradiction. We write $g = g'\rho$ where $g' \in G(\mathfrak{C}/L)$. Let B be the matrix of g' in $SU(H)$. Then, by a direct computation, it follows that

$$g t_0 g^{-1}(\alpha_0.1 + \alpha_1 f_1 + \alpha_2 f_2 + \alpha_3 f_3)$$
$$= \alpha_0.1 + \alpha_1 B \bar{A} B^{-1} f_1 + \alpha_2 B \bar{A} B^{-1} f_2 + \alpha_3 B \bar{A} B^{-1} f_3.$$

Also,

$$t_0^{-1}(\alpha_0.1 + \alpha_1 f_1 + \alpha_2 f_2 + \alpha_3 f_3) = (\alpha_0.1 + \alpha_1 A^{-1} f_1 + \alpha_2 A^{-1} f_2 + \alpha_3 A^{-1} f_3).$$

Therefore, if t_0 is conjugate to t_0^{-1} in $G = \text{Aut}(\mathfrak{C})$, then $\bar{A}$ is conjugate to A^{-1} in $SU(H)$. Conversely, let $B \bar{A} B^{-1} = A^{-1}$ for some $B \in SU(H)$. Let $g' \in G(\mathfrak{C}/L)$ be the element corresponding to B. Then $g'\rho$ conjugates t_0 to t_0^{-1}. ∎

Let V be a vector space over L of dimension n with a nondegenerate hermitian form h. Let H denote the diagonal matrix of h with respect to some fixed orthogonal basis. Then, for any $A \in U(H)$, we have ${}^tAH\bar{A} = H$. Let $A \in SU(H)$ with characteristic polynomial $\chi_A(X) = X^n + a_1 X^{n-1} + \cdots + a_{n-1}X + (-1)^n$. Then $(-1)^n a_i = \bar{a}_{n-i}$ for $i = 1, \ldots, n-1$.

LEMMA 6.3: *With notation as above, let $A \in SU(H)$ with its characteristic polynomial over L be the same as its minimal polynomial. Suppose $A = A_1 A_2$ with $A_1, A_2 \in GL(n, L)$ and $\bar{A}_1 A_1 = I = \bar{A}_2 A_2$. Then $A_1, A_2 \in U(H)$.*

Proof: Let $H = \operatorname{diag}(\lambda_1, \lambda_2, \ldots, \lambda_n)$, where $\lambda_1, \ldots, \lambda_n \in k$. We have ${}^tAH\bar{A} = H$. Then

$$(HA_1^{-1})A(HA_1^{-1})^{-1} = HA_1^{-1}A_1 A_2 A_1 H^{-1} = H\bar{A}^{-1}H^{-1} = {}^tA.$$

Since the characteristic polynomial of A equals its minimal polynomial, by (Th. 2 [TZ]), HA_1^{-1} is symmetric, i.e., $HA_1^{-1} = {}^t(HA_1^{-1}) = {}^tA_1^{-1}H$. This implies, $H = {}^tA_1 HA_1^{-1} = {}^tA_1 H\bar{A}_1$. Hence $A_1 \in U(H)$. By similar analysis we see that $A_2 \in U(H)$.   ∎

LEMMA 6.4: *With notation as above, let $A \in SU(H)$ with characteristic polynomial $\chi_A(X) = X^n + a_1 X^{n-1} + \cdots + a_{n-1}X + (-1)^n$ over L, equal to its minimal polynomial. Then, $A = B_1 B_2$ with $B_1, B_2 \in GL(n, L)$ and $\overline{B}_1 B_1 = I = \overline{B}_2 B_2$.*

Proof: Let A_χ denote the companion matrix of A, namely

$$A_\chi = \begin{pmatrix} 0 & 0 & \ldots & 0 & -(-1)^n \\ 1 & 0 & \ldots & 0 & -a_{n-1} \\ \vdots & \vdots & & & \vdots \\ 0 & 0 & \ldots & 1 & -a_1 \end{pmatrix}.$$

We have

$$A_\chi = \begin{pmatrix} (-1)^n & 0 & \ldots & 0 & 0 \\ a_{n-1} & 0 & \ldots & 0 & -1 \\ \vdots & \vdots & & & \vdots \\ a_1 & -1 & \ldots & 0 & 0 \end{pmatrix} \begin{pmatrix} 0 & 0 & \ldots & 0 & -1 \\ 0 & 0 & \ldots & -1 & 0 \\ \vdots & \vdots & & & \vdots \\ -1 & 0 & \ldots & 0 & 0 \end{pmatrix} = A_1 A_2,$$

and $\bar{A}_1 A_1 = I = \bar{A}_2 A_2$, using $(-1)^n a_i = \bar{a}_{n-i}$ for $i = 1, \ldots, n-1$. Since the characteristic polynomial of A equals its minimal polynomial, there exists $T \in GL(n, L)$ such that $A = TA_\chi T^{-1}$. We put $B_1 = TA_1 \bar{T}^{-1}$, $B_2 = \bar{T}A_2 T^{-1}$. Then $A = B_1 B_2$, where $\bar{B}_1 B_1 = I = \bar{B}_2 B_2$.   ∎

COROLLARY 6.2: *Let $A \in SU(H)$ with characteristic polynomial $\chi_A(X)$ over L the same as its minimal polynomial. Then, $A = B_1 B_2$ with $B_1, B_2 \in U(H)$ and $\overline{B}_1 B_1 = I = \overline{B}_2 B_2$.*

From this corollary, we get the following

LEMMA 6.5: *Let $A \in SU(H)$, with characteristic polynomial over L equal to its minimal polynomial. Then,*

1. *$\bar{A}$ is conjugate to A^{-1} in $U(H)$, if and only if $A = A_1 A_2$ with $A_1, A_2 \in U(H)$ and $\bar{A}_1 A_1 = I = \bar{A}_2 A_2$;*

2. *$\bar{A}$ is conjugate to A^{-1} in $SU(H)$, if and only if $A = A_1 A_2$ with $A_1, A_2 \in SU(H)$ and $\bar{A}_1 A_1 = I = \bar{A}_2 A_2$.*

The following proposition is due to Neumann ([N], Lemma 5). Recall that we have fixed a basis $\{f_1, f_2, f_3\}$ for $V = L^{\perp}$ over L in Theorem 6.5.

PROPOSITION 6.1: *Let $\mathfrak{C}$ be an octonion algebra over k and let L be a quadratic field extension of k, which is a subalgebra of $\mathfrak{C}$. An element $t \in G(\mathfrak{C}/L)$ is a product of two involutions in $\mathrm{Aut}(\mathfrak{C})$, if and only if the corresponding matrix $A \in SU(H)$ is a product of two matrices $A_1, A_2 \in SU(H)$, satisfying $\bar{A}_1 A_1 = \bar{A}_2 A_2 = I$.*

We now have

THEOREM 6.6: *Let t_0 be an element in $G(\mathfrak{C}/L)$ and let A denote the image of t_0 in $SU(H)$. Suppose the characteristic polynomial of A is irreducible over L. Then t_0 is conjugate to t_0^{-1}, if and only if t_0 is a product of two involutions in $G(k)$.*

Proof: From Theorem 6.5 we have, t_0 is conjugate to t_0^{-1}, if and only if $\bar{A}$ is conjugate to A^{-1} in $SU(H)$. From Lemma 6.5 above, $\bar{A}$ is conjugate to A^{-1} in $SU(H)$ if and only if $A = A_1 A_2$ with $A_1, A_2 \in SU(H)$ and $\bar{A}_1 A_1 = I = \bar{A}_2 A_2$. Now, from Proposition 6.1, it follows that t_0 is a product of two involutions. ∎

Let V be a vector space over L of dimension n together with a nondegenerate hermitian form h. Let $A \in SU(H)$. Let us denote the conjugacy class of A in $U(H)$ by C and the centralizer of A in $U(H)$ by $\mathcal{Z}$ and let

$$L_A = \{\det(X) | X \in \mathcal{Z}\}.$$

LEMMA 6.6: *With notation as fixed above, for $X, Y \in U(H)$, XAX^{-1} is conjugate to YAY^{-1} in $SU(H)$ if and only if $\det(X) \equiv \det(Y) \pmod{L_A}$.*

Proof: Suppose there exists $S \in SU(H)$ such that $SXAX^{-1}S^{-1} = YAY^{-1}$. Then, $Y^{-1}SX \in \mathcal{Z}$ and $\det(X) \equiv \det(Y) \pmod{L_A}$.

Conversely, let $\det(XY^{-1}) = \det(B)$ for $B \in \mathcal{Z}$. Put $S = YBX^{-1}$. Then $\det(S) = 1$, $S \in SU(H)$ and $Y^{-1}SX = B \in \mathcal{Z}$. Then, $Y^{-1}SXA = AY^{-1}SX$ gives $SXAX^{-1}S^{-1} = YAY^{-1}$.   ∎

LEMMA 6.7: *Let t_0 be an element in $G(\mathfrak{C}/L)$ for L a quadratic field extension of k and A be the corresponding element in $SU(H)$. Suppose the characteristic polynomial of A is irreducible over L. Then, t_0 is conjugate to t_0^{-1} in $G(k)$, if and only if for every $X \in U(H)$ such that $X\bar{A}X^{-1} = A^{-1}$, $\det(X) \in L_{\bar{A}}$.*

Proof: We have, by Theorem 6.5, t_0 is conjugate to t_0^{-1} in $G(k)$ if and only if $\bar{A}$ is conjugate to A^{-1} in $SU(H)$. Let $X \in U(H)$ be such that $X\bar{A}X^{-1} = A^{-1}$. Then from the above lemma, $\bar{A}$ is conjugate to A^{-1} in $SU(H)$ if and only if $\det(X) \in L_{\bar{A}}$.   ∎

COROLLARY 6.3: *With notation as fixed above whenever $L^1/L_{\bar{A}}$ is trivial, t_0 is conjugate to t_0^{-1} in $G(k)$, where $L^1 = \{\alpha \in L | \alpha\bar{\alpha} = 1\}$.*

Proof: We have $L^1 = \{\alpha \in L | \alpha\bar{\alpha} = 1\} = \{\det(X) | X \in U(H)\}$. Now let us fix $X_0 \in U(H)$ such that $X_0\bar{A}X_0^{-1} = A^{-1}$. Then, for any $X \in U(H)$ such that $X\bar{A}X^{-1} = A^{-1}$, we have $X_0^{-1}X \in \mathcal{Z}_{U(H)}(\bar{A})$. Hence $\det(X) \in \det(X_0)L_{\bar{A}}$. But since $L^1/L_{\bar{A}}$ is trivial, we have $\det(X) \in L_{\bar{A}}$. From the above lemma, it now follows that t_0 is conjugate to t_0^{-1} in $G(k)$.   ∎

Remark: From the proof above, for any $X \in U(H)$ such that $X\bar{A}X^{-1} = A^{-1}$, we get $X \in X_0\mathcal{Z}_{U(H)}(\bar{A})$. Since the characteristic polynomial of A is irreducible, that of $\bar{A}$ is irreducible as well. Therefore $\mathcal{Z}_{U(H)}(\bar{A}) \subset \mathcal{Z}_{\mathrm{End}_L(V)}(\bar{A}) = L[\bar{A}] \cong L[T]/ < \chi_{\bar{A}}(T) >$. In fact, $\mathcal{Z}_{U(H)}(\bar{A}) = \{x \in \mathcal{Z}_{\mathrm{End}_L(V)}(\bar{A}) | x\sigma_h(x) = 1\}$. Hence we can write $X = X_0f(\bar{A})$ for some polynomial $f(T) \in L[T]$.

LEMMA 6.8: *Let $A \in SU(H)$ and its characteristic polynomial $\chi_A(X)$ be irreducible over L. Let $\mathcal{E} = L[X]/\chi_{\bar{A}}(X)$, a degree three field extension of L. Then $L^1/L_{\bar{A}} \hookrightarrow L^*/N(\mathcal{E}^*)$.*

Proof: Define a map $\phi: L^1 \longrightarrow L^*/N(\mathcal{E}^*)$ by $x \mapsto xN(\mathcal{E}^*)$. We claim that $\ker(\phi) = \{x \in L^1 | x \in N(\mathcal{E}^*)\} = L_{\bar{A}} = \{N(x) | x \in \mathcal{E}^*, x\sigma(x) = 1\}$. Let $x \in$

$ker(\phi)$, i.e., $x = N(y)$ for some $y \in \mathcal{E}^*$ and $x\sigma(x) = 1$. Let $\tilde{y} = xy^{-1}\sigma(y) \in \mathcal{E}^*$, then $N(\tilde{y}) = x, \tilde{y}\sigma(\tilde{y}) = 1$. Hence $x \in L_{\bar{A}}$. Conversely, if $N(x) \in L_{\bar{A}}$ for some $x \in \mathcal{E}^*$ such that $x\sigma(x) = 1$ then $N(x) \in ker(\phi)$. ∎

Hence if the field k is C_1 (for example, a finite field) or it does not admit degree three extensions (real closed fields, algebraically closed fields etc.), $L^*/N(E^*)$ is trivial. From Corollary 6.3, it follows that every element in $G(\mathfrak{C}/L)$, with irreducible characteristic polynomial, is conjugate to its inverse. In particular, combining with Theorem 6.2, it follows that every semisimple element in $G(k)$ is conjugate to its inverse.

PROPOSITION 6.2: *With notation as above, let L be a quadratic field extension of k and let $S \in SU(H)$ be an element with irreducible characteristic polynomial over L, satisfying $\bar{S} = S^{-1}$. Let $\mathcal{E} = L[X]/\chi_S(X)$, a degree three field extension of L, and assume $L^1/N(\mathcal{E}^1)$ is nontrivial, where $L^1 = \{x \in L | x\sigma(x) = 1\}$, $\mathcal{E}^1 = \{x \in \mathcal{E} | x\sigma(x) = 1\}$ and σ is the extension of the nontrivial automorphism of L to $\mathcal{E}$. Then there exists an element $A \in SU(H)$ with characteristic polynomial the same as the characteristic polynomial of S, which cannot be written as $A = A_1 A_2$ where $\bar{A}_i = A_i^{-1}$ and $A_i \in SU(H)$. The corresponding element t in $G(\mathfrak{C}/L)$ is not a product of two involutions in $G = \mathrm{Aut}(\mathfrak{C})$ and hence not real in G.*

Proof: Let $b \in L^1$ such that $b^2 \notin N(\mathcal{E}^1)$. Put $D = \mathrm{diag}(b, 1, 1)$ and $A = DSD^{-1}$; then A belongs to $SU(H)$. Now suppose $A = A_1 A_2$ with $\bar{A}_i = A_i^{-1}$ and $A_i \in SU(H)$. Then $A = A_1 A_2 = DSD^{-1} = DSDD^{-2}$. Put $T_1 = DSD$ and $T_2 = D^{-2}$; then $\bar{T}_i = T_i^{-1}$. Since $A_2 A A_2^{-1} = \bar{A}^{-1}$ and $T_2 A T_2^{-1} = \bar{A}^{-1}$, we have $T_2^{-1} A_2 \in \mathcal{Z}_{U(V,h)}(A)$, i.e., $T_2^{-1} A_2 = f(A)$ for some $f(X) \in L[X]$ (see the Remark after Corollary 6.3). Then $b^2 = \det(T_2^{-1}) = \det(T_2^{-1}A_2) = \det(f(A)) \in N(\mathcal{E}^*)$, a contradiction. ∎

Remark: If we choose S in the theorem above with characteristic polynomial separable, then the element A, constructed in the proof, is a semisimple element in an indecomposable maximal torus, contained in $SU(H)$, which is not real.

We recall that any central division algebra of degree three is cyclic (Theorem, Section 15.6, [P]). Let L be a quadratic field extension of k. Let F be a degree three cyclic extension of k and we denote $E = F.L$. Let us denote the generator of the Galois group of F over k by τ. Let $A = F \oplus Fu \oplus Fu^2$ with $udu^{-1} = \tau(d)$ for all $d \in F$ and $u^3 = a \in k^*$. Then A, denoted by (F, τ, a), is a cyclic algebra of degree three over k. Recall also that (F, τ, a) is a division algebra if and only if

$a \notin N_{F/k}(F^*)$. We denote the relative Brauer group of F over k by $B(F/k)$, i.e., the group of Brauer classes of central simple algebras over k, which split over F. We define a map $\phi\colon B(F/k) \longrightarrow B(E/L)$ by $[(F, \tau, a)] \mapsto [(E, \tau, a)]$ (which is the same as the map $[D] \mapsto [D \otimes L]$). This map is well defined (Section 15.1, Cor. c, [P]) and is an injective map since

$$\ker(\phi) = \{[(F, \tau, a)] \in B(F/k) | a \in k^*, a \in N_{E/L}(E^*)\}$$
$$= \{[(F, \tau, a)] \in B(F/k) | a \in N_{F/k}(F^*)\}.$$

We have a commutative diagram,

$$
\begin{array}{ccc}
k^*/N_{F/k}(F^*) & \xrightarrow{\;\cong\;} & B(F/k) \\
\downarrow & & \downarrow{\scriptstyle \phi} \\
L^*/N_{E/L}(E^*) & \xrightarrow{\;\cong\;} & B(E/L)
\end{array}
$$

The vertical maps are injective in the above diagram. We have the following exact sequence,

$$1 \longrightarrow (N_{E/L}(E^*)k^*)/N_{E/L}(E^*) \longrightarrow L^*/N_{E/L}(E^*) \longrightarrow L^1/N_{E/L}(E^1) \longrightarrow 1$$

where $(N_{E/L}(E^*)k^*)/N_{E/L}(E^*) \cong k^*/N_{F/k}(F^*)$. Hence, from the commutativity of the above diagram, we get $B(E/L)/\phi(B(F/k)) \cong L^1/N_{E/L}(E^1)$.

This shows $L^1/N_{E/L}(E^1)$ is nontrivial, if and only if there exists a central division algebra D over L which splits over E, and it does not come from a central division algebra over k, split by F. We recall a proposition from [K] (Chapter V, Prop. 1).

PROPOSITION 6.3: *Let k be a number field and L a quadratic field extension of k. Let F be a cyclic extension of degree m over k, which is linearly disjoint from L, over k. Then there exists a central division algebra $(FL/L, \tau, a)$ over L of degree m, with an involution of second kind, with $a \in L^1$.*

COROLLARY 6.4: *Let k be a number field and L a quadratic field extension of k. Let F be a cyclic extension of degree 3 over k. Let us denote $E = F.L$. Then $L^1/N_{E/L}(E^1)$ is nontrivial.*

Proof: By the proposition above, there exists a degree three central division algebra (E, τ, a) over L with $a \in L^1$. Therefore $a \notin N_{E/L}(E^*)$. ∎

We proceed to construct an example of the situation required in Proposition 6.2.

PROPOSITION 6.4: *Let k be a number field. There exist octonion algebras $\mathfrak{C}$ over k such that not every (semisimple) element in $\mathrm{Aut}(\mathfrak{C})$ is real.*

Proof: We use Proposition 6.2 here. Let L be a quadratic field extension of k. Let F be a degree three cyclic extension of k. Then we have $E = F.L$, a degree three cyclic extension of L. We denote the extension of the nontrivial automorphism of L over k to E over L by σ, which is the identity automorphism when restricted to F. Sometimes we write $\bar{x} = \sigma(x)$ for $x \in E$. Let us consider E as a vector space over L. We consider the trace hermitian form on E defined as follows:

$$tr: E \times E \longrightarrow L$$

$$tr(x, y) = tr_{E/L}(x\bar{y}).$$

The restriction of this form to F is the trace form $tr: F \times F \longrightarrow k$, given by $tr(x, y) = tr_{F/k}(xy)$. We choose an orthogonal basis of F over k, say $\{f_1, f_2, f_3\}$, with respect to the trace form, and extend it to a basis of E/L. Then the bilinear form tr with respect to this basis has diagonalization $< 1, 2, 2 >$ (Section 18.31, [KMRT]). We have $disc(tr) = 4 \in N_{L/k}(L^*)$. Hence (E, tr) is a rank 3 hermitian space over L with trivial discriminant and $SU(E, tr)$ is isomorphic to $SU(H)$ where $H = diag(1, 2, 2)$. We choose an element $1 \neq a \in T^1 - L^1$, where $T^1 = \{x \in E | x\bar{x} = 1, N_{E/L}(x) = 1\}$. Let us consider the left homothety map,

$$l_a: E \longrightarrow E$$

$$l_a(x) = ax.$$

Since $a \in T^1 - L^1$, the characteristic polynomial $\chi(X)$ of l_a is the minimal polynomial of a over L, which is irreducible of degree 3 over L. Next we prove that $l_a \in SU(E, tr)$. This is so since

$$tr(l_a(x), l_a(y)) = tr(ax, ay) = tr_{E/L}(ax\bar{a}\bar{y}) = tr_{E/L}(x\bar{y}) = tr(x, y).$$

Let $S = (s_{ij})$ denote the matrix of l_a with respect to the chosen basis $\{f_1, f_2, f_3\}$ of F over k. Then the matrix of $l_{\bar{a}}$ is $\bar{S} = (\bar{s}_{ij})$. Also, since $a\bar{a} = 1$, we have $S\bar{S} = 1$. Thus we have a matrix S in $SU(H)$, for $H = < 1, 2, 2 >$, satisfying the conditions of Proposition 6.2.

Now, let $L = k(\gamma)$ with $\gamma^2 = c \in k^*$. We write $Q = k \oplus F$. Since (F, tr) is a quadratic space with trivial discriminant, we can define a quaternionic multiplication on Q (Prop. 2.3); denote its norm by N_Q. We double Q with $\gamma^2 = c \in k^*$ to get an octonion algebra $\mathfrak{C} = Q \oplus Q$ with multiplication

$$(x, y)(u, v) = (xu + c\bar{v}y, vx + y\bar{u})$$

and the norm $N((x,y)) = N_Q(x) - cN_Q(y)$. We choose a basis $\{1, a, b, ab\}$ of Q, orthogonal for N_Q, so that N_Q has diagonalization $< 1, 1, 2, 2 >$ with respect to this basis. This gives a basis

$$\{(1,0), (a,0), (b,0), (ab,0), (0,1), (0,a), (0,b), (0,ab)\}$$

of $\mathfrak{C}$ and the diagonalization of N with respect to this basis is

$$< 1, 1, 2, 2, -c, -c, -2c, -2c > .$$

We observe that the subalgebra $k \oplus k \subset \mathfrak{C}$ is isomorphic to L and $L^\perp = F \times F$ is a three-dimensional vector space over L with hermitian form $< 1, 2, 2 >$. Hence $SU(L^\perp, h)$, with respect to the basis $\{(a,0), (b,0), (ab,0)\}$ of $L^\perp$, is $SU(H)$ for $H =< 1, 2, 2 >$. Hence, from the discussion in previous paragraph, we have an element of required type in $SU(L^\perp, h)$.

By Corollary 6.4, $L^1/N(E^1)$ is nontrivial. It follows from Proposition 6.1 and Proposition 6.2 that not all (semisimple) elements in $\mathrm{Aut}(\mathfrak{C})$, which are contained in the subgroup $SU(E, tr)$, are real.   ∎

COROLLARY 6.5: *Let k be a totally real number field. Then there exists an octonion division algebra $\mathfrak{C}$ over k such that not every element in $\mathrm{Aut}(\mathfrak{C})$ is real. Hence there exist (semisimple) elements in $\mathrm{Aut}(\mathfrak{C})$ which are the product of three involutions but not the product of two involutions.*

Proof: We recall from Lemma 2.1 that if the k-quadratic form Q_B, corresponding to the bilinear form $B: E \times E \longrightarrow k$, defined by $B(x,y) = tr_{E/L}(x\bar{y}) + tr_{E/L}(\bar{x}y)$, is anisotropic, then the octonion algebra $\mathfrak{C}$, as constructed in the proof of the above proposition, is a division algebra. In case when k is a totally real number field and $L = k(i)$, the diagonalization of q_B is $< 1, 2, 2, 1, 2, 2 >$, which is clearly anisotropic over k.   ∎

Remark: We note that the quadratic form Q_B as above can be isotropic for imaginary quadratic number fields. For example, if $k = \mathbb{Q}(\sqrt{-2})$, Q_B has diagonalization $< 1, -1, -1, -c, c, c >$, which is isotropic. Hence the octonion algebra $\mathfrak{C}$ in this case is split. Therefore, indecomposable tori in subgroups $SU(V, h) \subset \mathrm{Aut}(\mathfrak{C})$ exist in all situations, whether $\mathfrak{C}$ is division or not. And in either case, there are nonreal elements.

6.2 $SL(3) \subset G$. Let us assume now that $L \cong k \times k$. We have seen in section 3 that $G(\mathfrak{C}/L) \cong SL(U) \cong SL(3)$. Let t_0 be an element in $G(\mathfrak{C}/L)$ and denote

its image in $SL(3)$ by A. We assume that the characteristic polynomial of $A \in SL(3)$ is irreducible over k. In this case, the characteristic polynomial equals the minimal polynomial of A.

LEMMA 6.9: *Let the notation be fixed as above. Let t_0 be an element in $G(\mathfrak{C}/L)$ and its image in $SL(3)$ be denoted by A. Let the characteristic polynomial of A be irreducible over k. Suppose that $\exists h \in G = \mathrm{Aut}(\mathfrak{C})$, such that $h t_0 h^{-1} = t_0^{-1}$. Then $h(L) = L$.*

Proof: Suppose that $h(L) \not\subset L$. Then we claim that $\exists x \in L \cap \mathfrak{C}_0$ such that $h(x) \notin L$. For this, let $y \in L$ be such that $h(y) \notin L$. Let $x = y - \frac{1}{2} tr(y)1$. Then $tr(x) = 0$, and if $h(x) \in L$ then $h(y) \in L$, a contradiction. Hence we have $x \in L \cap \mathfrak{C}_0$ with $h(x) \notin L$. Also, since $t_0(x) = x$, we have

$$t_0(h(x)) = h t_0^{-1}(x) = h(x).$$

Therefore, t_0 fixes $h(x) \in \mathfrak{C}_0$ and hence fixes a two-dimensional subspace $\mathrm{span}\{x, h(x)\}$ pointwise, which is contained in $\mathfrak{C}_0 \subset \mathfrak{C}$. Hence the characteristic polynomial of t_0 on $\mathfrak{C}_0$ has a degree 2 factor. But the characteristic polynomial $f(X)$ of t_0 on $\mathfrak{C}_0$ has the factorization

$$f(X) = (X - 1)\chi(X)\chi^*(X),$$

where $\chi(X)$ is the characteristic polynomial of t_0 on the three-dimensional k-subspace U of $\mathfrak{C}_0$ and $\chi^*(X)$ is its dual polynomial (see Sec. 3, [W1]). Since $\chi(X)$ is irreducible by hypothesis, this leads to a contradiction. Hence any $h \in \mathrm{Aut}(\mathfrak{C})$, conjugating t_0 to t_0^{-1} in G, leaves L invariant. ∎

THEOREM 6.7: *With notation fixed as above, let A be the matrix of t_0 in $SL(3)$ with irreducible characteristic polynomial. Then t_0 is conjugate to t_0^{-1} in $G = \mathrm{Aut}(\mathfrak{C})$, if and only if A is conjugate to ${}^t A$ in $SL(3)$.*

Proof: Let $h \in G$ be such that $h t_0 h^{-1} = t_0^{-1}$. In view of the lemma above, we have $h(L) = L$. We may, without loss of generality (up to conjugacy by an automorphism), assume that

$$\mathfrak{C} = \left\{ \begin{pmatrix} \alpha & v \\ w & \beta \end{pmatrix} | \alpha, \beta \in k; v, w \in k^3 \right\} \quad \text{with } L = \left\{ \begin{pmatrix} \alpha & 0 \\ 0 & \beta \end{pmatrix} | \alpha, \beta \in k \right\}.$$

By Proposition 3.3, h belongs to $G(\mathfrak{C}/L) \rtimes H$. Clearly h does not belong to $G(\mathfrak{C}/L)$, for if so, we can conjugate t_0 to t_0^{-1} in $SL(U)$, which implies in particular that the characteristic polynomial $\chi(X)$ of t_0 on U is reducible, a contradiction. Hence $h = g\rho$ for some $g \in G(\mathfrak{C}/L)$. Let A denote the matrix of t_0 on

U in $SL(3)$ and B that of g. Then, a direct computation gives

$$ht_0h^{-1}\begin{pmatrix} \alpha & v \\ w & \beta \end{pmatrix} = \begin{pmatrix} \alpha & B^tA^{-1}B^{-1}v \\ {}^tB^{-1}A^tBw & \beta \end{pmatrix},$$

and

$$t_0^{-1}\begin{pmatrix} \alpha & v \\ w & \beta \end{pmatrix} = \begin{pmatrix} \alpha & A^{-1}v \\ {}^tAw & \beta \end{pmatrix}.$$

Therefore,

$$ht_0h^{-1} = t_0^{-1} \Leftrightarrow A = B^tAB^{-1}.$$

Hence, t_0 is conjugate to t_0^{-1} in $G(k)$ if and only if A is conjugate to ${}^tA$ in $SL(3)$.   ∎

We now derive a necessary and sufficient condition that a matrix A in $SL(3)$, with irreducible characteristic polynomial, be conjugate to ${}^tA$ in $SL(3)$. We have, more generally,

THEOREM 6.8: *Let A be a matrix in $SL(n)$ with characteristic polynomial $\chi_A(X)$ irreducible. Let $E = k[X]/\chi_A(X) \cong k[A]$ be the field extension of k of degree n given by $\chi_A(X)$. Then A is conjugate to ${}^tA$ in $SL(n)$, if and only if, for every $T \in GL(n)$ with $TAT^{-1} = {}^tA$, $\det(T)$ is a norm from E.*

Proof: Fix a $T_0 \in GL(n)$ such that $T_0AT_0^{-1} = {}^tA$ and define a map,

$$\{T \in M_n(k)|TA = {}^tAT\} \longrightarrow k[A]$$
$$T \mapsto T_0^{-1}T.$$

This map is an isomorphism of vector spaces, since if $T \in M_n(k)$ is such that $TA = {}^tAT$ then $T_0^{-1}T$ belongs to $\mathcal{Z}(A)$ $(= k[A]$, as the characteristic polynomial of A is the same as its minimal polynomial). To prove the assertion, suppose $T_0 \in SL(n)$ conjugates A to ${}^tA$. But with the above bijection, $T_0^{-1}T = p(A)$ for some $p(A) \in k[A]$, $p(X) \in k[X]$. Hence $\det(p(A)) = \det(T)$, i.e., $\det T$ is a norm from E.

Conversely, suppose there exists $T \in GL(n)$ with $TAT^{-1} = {}^tA$ and $\det(T)$ is a norm from E. Then there exists $p(X) \in k[X]$ such that $\det(p(A)) = \det(T)^{-1}$. Thus $\det(Tp(A)) = 1$ and $(Tp(A))A(p(A)^{-1}T^{-1}) = TAT^{-1} = {}^tA$.   ∎

In the case under discussion, $A \in SL(3)$ has an irreducible characteristic polynomial. Hence, $E \cong k[A] \cong \mathcal{Z}_{M_3(k)}(A)$ is a cubic field extension of k. We combine the previous two theorems to get

COROLLARY 6.6: *Let A be a matrix in $SL(3)$ with irreducible characteristic polynomial. With notation as above, suppose $k^*/N(E^*)$ is trivial. Then A can be conjugated to ^tA in $SL(3)$ and hence t_0 can be conjugated to t_0^{-1} in* Aut$(\mathfrak{C})$.

If k a C_1 field (e.g., a finite field) or k does not admit cubic field extensions (e.g., k real closed, algebraically closed), the above criterion is satisfied automatically. Hence every element in $G(\mathfrak{C}/L)$, for $L = k \times k$, with irreducible characteristic polynomial over k, is conjugate to its inverse in $G(k)$. In particular, combining this with Theorem 6.2, we see that every semisimple element in $G(k)$ is real.

We shall give a cohomological proof of reality for G_2 over fields k with $cd(k) \leq 1$ (see the remarks later in this section).

LEMMA 6.10: *Let A be a matrix in $SL(n)$ with irreducible characteristic polynomial. Then A is conjugate to ^tA in $SL(n)$ if and only if A is a product of two symmetric matrices in $SL(n)$.*

Proof: Any matrix conjugating A to ^tA is necessarily symmetric (Th. 2 [TZ]). Let S be a symmetric matrix which conjugates A to ^tA in $SL(n)$, i.e., $SAS^{-1} = {}^tA$. Let $B = SA = {}^tAS$. Then B is symmetric and belongs to $SL(n)$. Hence $A = S^{-1}B$ is a product of two symmetric matrices in $SL(n)$. Conversely, let A be a product of two symmetric matrices from $SL(n)$, say $A = S_1 S_2$. Then S_2 conjugates A to ^tA. ∎

We need the following result from ([W1]) (cf. also [L]),

PROPOSITION 6.5: *Let $\mathfrak{C}$ be a (split) Cayley algebra over a field k of characteristic not 2. Let L be a split two-dimensional subalgebra of $\mathfrak{C}$. An element $\eta \in G(\mathfrak{C}/L)$ is a product of two involutory automorphisms if and only if the corresponding matrix in $SL(3)$ can be decomposed into a product of two symmetric matrices in $SL(3)$.*

We have

THEOREM 6.9: *Let t_0 be an element in $G(\mathfrak{C}/L)$, with notation as in this section. Let us assume that the matrix A of t_0 in $SL(3)$ has irreducible characteristic polynomial. Then t_0 can be conjugated to t_0^{-1} in $G = $ Aut$(\mathfrak{C})$, if and only if t_0 is a product of two involutions in $G(k)$.*

Proof: The element t_0 can be conjugated to t_0^{-1} in G if and only if A can be conjugated to ^tA in $SL(3)$ (Theorem 6.7). This is if and only if A is a product

of two symmetric matrices in $SL(3)$ (Lemma 6.10). By Proposition 6.5, this is if and only if t_0 is a product of two involutions in $\text{Aut}(\mathfrak{C})$.   ∎

In view of these results, to produce an example of a semisimple element of $G = \text{Aut}(\mathfrak{C})$ that is not conjugate to its inverse in $\text{Aut}(\mathfrak{C})$, we need to produce a semisimple element which is a product of three involutions but not a product of two involutions. We shall show that, for the split form G of G_2 over $k = \mathbb{Q}$ or $k = \mathbb{Q}_p$, there are semisimple elements in $G(k)$ which are not conjugate to their inverses in $G(k)$. We shall end this section by exhibiting explicit elements in G_2 over a finite field, which are not real. These necessarily are not semisimple or unipotent (see the remarks at the end of this section). We adapt a slight variant of an example in ([W1], [L]) for our purpose; there, the issue is bireflectionality of G_2.

LEMMA 6.11: *Let k be a field and let S be a symmetric matrix in $SL(3)$ whose characteristic polynomial $p(X)$ is irreducible over k. Let $E = k[X]/ < p(X) >$, the degree three field extension of k given by $p(X)$. Further, suppose that $k^*/N(E^*)$ is not trivial. Then there exists a matrix in $SL(3)$, with characteristic polynomial $p(X)$, which is not a product of two symmetric matrices in $SL(3)$.*

Proof: Let $b \in k^*$ such that $b^2 \notin N(E^*)$. Consider $D = diag(b, 1, 1)$, a diagonal matrix, and put $A = DSD^{-1}$. Then $A \in SL(3)$. We claim that A is not a product of two symmetric matrices from $SL(3)$. Assume the contrary. Suppose $A = DSD^{-1} = S_1 S_2$ where $S_1, S_2 \in SL(3)$ and symmetric. Then

$$A = DSD^{-1} = (DSD)D^{-2} = S_1 S_2.$$

Let $T_1 = DSD$, $T_2 = D^{-2}$. Then ${}^t T_i = T_i$, $i = 1, 2$ and $A = T_1 T_2 = S_1 S_2$. Therefore,

$$^t A = T_2 T_1 = T_2 A T_2^{-1} = S_2 S_1 = S_2 A S_2^{-1}.$$

Since the characteristic polynomial of A is irreducible, by the proof of Theorem 6.8, $D^2 S_2 = T_2^{-1} S_2 \in \mathcal{Z}(A) = k[A] \cong E$, which implies $S_2 = D^{-2} f(A)$ for some polynomial $f(X) \in k[X]$. Taking determinants, we get

$$1 = \det S_2 = \det D^{-2} \det(f(A)),$$

i.e., $b^2 = \det(f(A)) \in N(E^*)$, contradicting the choice of $b \in k$. Hence A cannot be written as a product of two symmetric matrices from $SL(3)$.   ∎

Remark: In view of Theorem 6.9 and its proof, the element A corresponds to an element in $\text{Aut}(\mathfrak{C})$ which cannot be conjugated to its inverse. If we choose the matrix S, as in the statement of the lemma above, to have separable characteristic polynomial, the matrix A, as constructed in the proof, corresponds to a semisimple element in an indecomposable torus contained in $SL(3) \subset G = \text{Aut}(\mathfrak{C})$, which is not real.

THEOREM 6.10: *Let G be a split group of type G_2 over $k = \mathbb{Q}$ or $\mathbb{Q}_p$. Then there exists a semisimple element in $G_2(k)$ which is not conjugate to its inverse.*

Proof: **Reality over $\mathbb{Q}_p$:** Let $k = \mathbb{Q}_p$, $p \neq 2$. Let $p(X)$ be an irreducible monic polynomial of degree n, with coefficients in $\mathbb{Q}_p$. By a theorem of Bender ([Be1]), there exists a symmetric matrix with $p(X)$ as its characteristic polynomial, if and only if, for the field extension $E = \mathbb{Q}_p[X]/(p(X))$, there exists α in E^* such that $(-1)^{n(n-1)/2}N(\alpha)$ belongs to $(\mathbb{Q}_p^*)^2$. We choose E as the (unique) unramified extension of $\mathbb{Q}_p$ of degree 3. Then, E is a cyclic extension of $\mathbb{Q}_p$. We choose $\beta \in E^*$, $N(\beta) = 1$ so that $E = \mathbb{Q}_p(\beta)$. Let $p(X)$ be the minimal polynomial of β over $\mathbb{Q}_p$. Then, applying Bender's result, there is a symmetric matrix A over $\mathbb{Q}_p$, with characteristic polynomial $p(X)$. Since $N(\beta) = 1$, A belongs to $SL(3, \mathbb{Q}_p)$. We have $\mathbb{Q}_p^*/N(E^*) \cong \mathbb{Z}/3\mathbb{Z}$ (see Sec. 17.9, [P]), hence $(\mathbb{Q}_p^*)^2 \not\subset N(E)$. Therefore we are done by Lemma 6.11, combined with Proposition 6.5 and Theorem 6.9.   ∎

This example shows that there exist semisimple elements in $G = \text{Aut}(\mathfrak{C})$ over $k = \mathbb{Q}_p$, which are not a product of two involutions and hence must be a product of three involutions, by ([W1]). In particular, reality for G_2 fails over $\mathbb{Q}_p$ (Theorem 6.3).

Reality over $\mathbb{Q}$: A polynomial $p(X) \in K[X]$ is called K-real if every real closure of K contains the splitting field of $p(X)$ over K. Bender (Th. 1, [Be2]) proves that whenever we have K, an algebraic number field, and $p(X)$ a monic K-polynomial with an odd degree factor over K, then $p(X)$ is K-real if and only if it is the characteristic polynomial of a symmetric K-matrix.

Let $p(X) = X^3 - 3X - 1$. Then all roots of this polynomial are real but not rational. This polynomial is therefore irreducible over $\mathbb{Q}$ and, by Bender's theorem stated above, $p(X)$ is the characteristic polynomial of a symmetric matrix. Note that $K = \mathbb{Q}[X]/ < p(X) >$ is a degree 3 cyclic extension of $\mathbb{Q}$.

We recall that for a cyclic field extension K of a k, the relative Brauer group $B(K/k) \cong k^*/N_{K/k}(K^*)$ (ref. Sec. 15.1, Prop. b, [P]). It is known that if K/k is a nontrivial extension of global fields, then $B(K/k)$ is infinite (ref. Cor. 4,

[FKS]). Therefore, for K chosen as above, $\mathbb{Q}^*/N(K^*)$ is not trivial. Hence all conditions required by Lemma 6.11 are satisfied by the polynomial $p(X)$ and we get a semisimple element $t_0 \in G_2(\mathbb{Q})$ which is not conjugate to its inverse, using Lemma 6.11, Proposition 6.5 and Theorem 6.9. ∎

Reality over $\mathbb{F}_q$: Let $k = \mathbb{F}_q$ be a finite field. We have shown (Theorem 6.3) that semisimple elements and unipotent elements in $G(k)$ are real in $G(k)$. We now construct an element in $G(k)$ which is not conjugate to its inverse. Let $\mathfrak{C}$ be the split octonion algebra over k; assume that the characteristic of k is not 2 or 3. We use the matrix model for the split octonions, as introduced in section 2. Let L be the split diagonal subalgebra of $\mathfrak{C}$. We assume that k contains primitive third roots of unity. We have $G(\mathfrak{C}/L) \cong SL(3)$. Let ω be a primitive third root of unity in k. Let

$$A = \begin{pmatrix} \omega & -1 & 0 \\ 0 & \omega & 1 \\ 0 & 0 & \omega \end{pmatrix}.$$

Then $A \in SL(3)$ and the minimal polynomial (=characteristic polynomial) of A is $p(X) = (X-\omega)^3$. Let $b \in k$ be such that the polynomial $X^3 - b^2$ is irreducible over k (this is possible due to characteristic assumptions). Let $D = \operatorname{diag}(b,1,1)$ and $B = DAD^{-1}$. Then $B \in SL(3)$ and has the same minimal polynomial as A. Note that B is neither semisimple nor unipotent. Let $t \in G(\mathfrak{C}/L)$ be the automorphism of $\mathfrak{C}$ corresponding to B. It is clear that the fixed point subalgebra of t is precisely L.

THEOREM 6.11: *The element $t \in G(\mathfrak{C}/L)$ as above is not real.*

Proof: If not, suppose for $h \in G(k)$, $hth^{-1} = t^{-1}$. Then, since t fixes precisely L pointwise, we have $h(L) = L$. Therefore $h \in G(\mathfrak{C}, L) \cong G(\mathfrak{C}/L) \rtimes H$, where $H =< \rho >$ is as in Proposition 3.3. If $h \in G(\mathfrak{C}/L)$, conjugacy of t and t^{-1} by h would imply conjugacy of B and B^{-1} in $SL(3)$. But this cannot be, since ω is the only root of $p(X)$. Thus $h = g\rho$ for $g \in G(\mathfrak{C}/L)$. Now, by exactly the same calculation as in the proof of Theorem 6.7, conjugacy of t and t^{-1} in $G(k)$ is equivalent to conjugacy of B and ^tB in $SL(3)$. Let $CBC^{-1} = {}^tB$ with $C \in SL(3)$. Let

$$T = \begin{pmatrix} 0 & 0 & 1 \\ 0 & -1 & 0 \\ 1 & 0 & 0 \end{pmatrix}.$$

Then $T \in SL(3)$ is symmetric and $TAT^{-1} = {}^tA$. Hence A is a product of two symmetric matrices in $SL(3)$, say $A = T_1 T_2$ with $T_i \in SL(3)$, symmetric (see

the proof of Lemma 6.10). But $CBC^{-1} = {}^tB$ gives $(DCD)A = {}^tA(DCD)$. Therefore, by an argument used in the proof of Theorem 6.8, using the fact that the characteristic polynomial is equal to the minimal polynomial of A, we have $DCD = T_2 f(A)$ for some polynomial $f \in k[X]$. Taking determinants, we get $b^2 = \det(f(A)) = f(\omega)^3$. But this contradicts the choice of b. Hence t is not real. ∎

A similar construction can be done for the subgroup $SU(V, h) \subset G$. We continue to assume that k is a finite field with characteristic different from $2, 3$. We first note that the (split) octonion algebra contains all quadratic extensions of k. We assume that 2 is a square in k and that k contains no primitive cube roots of unity. Let L be a quadratic extension of k containing a primitive cube root of unity ω. Let $b \in L$ with $N_{L/k}(b) = 1$ such that the polynomial $X^3 - b^2$ is irreducible over L. Let $\alpha \in L$ with $N_{L/k}(\alpha) = -1$. Let

$$A = \begin{pmatrix} \omega + \frac{1}{4} & \frac{1}{2} & -\frac{1}{4}\alpha \\ -\frac{1}{2}\omega^2 & \omega & \frac{1}{2}\alpha\omega^2 \\ -\frac{1}{4}\overline{\alpha} & -\frac{1}{2}\overline{\alpha} & \omega - \frac{1}{4} \end{pmatrix};$$

then $A \in SU(3)$ and the minimal polynomial (=characteristic polynomial) of A over L is $(X - \omega)^3$. Let F be a cubic extension of k and $E = F.L$. Then E is a cyclic extension of L and we have the trace hermitian form as defined in Proposition 6.4, on E. We fix an orthogonal basis for F over k for the trace bilinear form and extend it to a basis of E over L. Then the trace hermitian form has diagonalization $< 1, 1, 1 >$. We construct $\mathfrak{C} = L \oplus E$ with respect to the hermitian space (E, tr), as in Section 3. Then $SU(L^\perp, h) \cong SU(3)$. Let $D = diag(b, 1, 1)$ and $B = DAD^{-1}$. Then $B \in SU(3)$ and has the same minimal polynomial as A. Note that B is neither semisimple nor unipotent. Let t denote the automorphism of $\mathfrak{C}$ corresponding to B. Then the fixed point subalgebra of t in $\mathfrak{C}$ is precisely L. We have

THEOREM 6.12: *The element $t \in G(\mathfrak{C}/L)$ as above is not real.*

Proof: Suppose t is real in $G(k)$. Then there is $h \in G(k)$ such that $hth^{-1} = t^{-1}$. Since the fixed point subalgebra of t is L, we have $h(L) = L$. Thus, by Proposition 3.5, $h \in G(\mathfrak{C}, L) \cong G(\mathfrak{C}/L) \rtimes H$, where $H = < \rho >$ is as in Proposition 3.5. If $h \in G(\mathfrak{C}/L)$, then B and B^{-1} would be conjugate in $SU(3)$, but that cannot be since ω is the only eigenvalue for B. Hence $h = g\rho$ for $g \in G(\mathfrak{C}/L)$. Then, conjugacy of t and t^{-1} in $G(k)$ is equivalent to conjugacy of $\overline{B}$ and B^{-1} in $SU(3)$, by the same calculation as in the proof of Theorem 6.5. By

Lemma 6.5, this is if and only if $B = B_1 B_2$ with $B_i \in SU(3)$ and $\overline{B_i} B_i = 1$. But then $B = DAD^{-1} = B_1 B_2$ and hence $A = (D^{-1} B_1 D^{-1})(DB_2 D) = A_1 A_2$, say. Then $A_i \in U(3)$ and $\overline{A_i} A_i = 1$. Let $C \in SU(3)$ be such that $C\overline{B}C^{-1} = B^{-1}$. Then $C\overline{DAD^{-1}}C^{-1} = DA^{-1}D^{-1}$. This gives $(D^{-1}CD^{-1})\overline{A}(DC^{-1}D) = A^{-1}$. Hence, by Lemma 6.5, $A = T_1 T_2$ with $T_i \in SU(3)$, $\overline{T_i} T_i = 1$. Therefore, by a similar argument as in the remark following Corollary 6.3, we must have $T_1 A_1^{-1} = f(A)$ for a polynomial $f(X) \in L[X]$. Taking determinants, we get $b^{-2} = f(\omega)^3$, contradicting the choice of b. Therefore t is not real in $G(k)$. ∎

Remarks:

1. Our results in fact show that if a semisimple element in $G(k)$, for a group G of type G_2, is conjugate to its inverse in $G(k)$, the conjugating element can be chosen to be an involution. The same is true for unipotents (these are always conjugate to their inverses).

2. One can give a simple cohomological proof of reality for G_2 over k with $cd(k) \leq 1$. Recall that $cd(k) \leq 1$, if and only if, for every algebraic extension K of k, $Br(K) = 0$ ([Se] Chap. 3, Prop. 5). Let $g \in G(k)$ be semisimple and T be a maximal k-torus of G containing g (cf. [Sp], Corollary 13.3.8). Let $N(T)$ be the normalizer of T in G and $W = N(T)/T$ the Weyl group of G relative to T. We have the exact sequence of groups

$$1 \to T \to N(T) \to W \to 1.$$

The corresponding Galois cohomology sequence is

$$1 \to T(k) \to N(T)(k) \to W(k) \to H^1(k,T) \to \cdots.$$

Now, if $cd(k) \leq 1$, by Steinberg's theorem (see [S]), $H^1(k,T) = 0$. Hence the last map above is surjective homomorphism of groups. Therefore the longest element w_0 in the Weyl group W of G_2, which acts as -1 on the set of positive roots with respect to T ([B], Plate IX), lifts to an element h of $N(T)(k)$. Hence, over k_s, we have $hth^{-1} = t^{-1}$ for all $t \in T$. But $h \in G(k)$, hence the conjugacy holds over k itself. Using Theorem 6.3, we get the following interesting result.

THEOREM 6.13: *Let $cd(k) \leq 1$ and G be a group of type G_2 over k. Then every semisimple element in $G(k)$ is a product of two involutions in $G(k)$.*

3. **The obstruction**: From our results, we see that semisimple elements belonging to decomposable tori are always product of two involutions and hence real in $G(k)$. For semisimple elements belonging to an indecomposable maximal torus T, the obstruction to reality is measured by $L^1/N(\mathcal{E}^1)$, where $T \subset SU(V,h) \cong SU(\mathcal{E},h^{(u)})$ is given by $T = \mathcal{E}^1$ and $\mathcal{E}$ is a cubic field extension of L. In the other case, when $T \subset SL(3)$, the obstruction is measured by $k^*/N(\mathcal{F}^*)$, where $\mathcal{F}$ is a cubic field extension of k. In both cases, the obstruction has a Brauer group interpretation. When $T \subset SL(3) \subset G$ is an indecomposable maximal torus, coming from a cyclic cubic field extension $\mathcal{F}$ of k, the obstruction to reality for elements in $T(k)$ is the relative Brauer group $B(\mathcal{F}/k)$. For an indecomposable torus $T \subset SU(\mathcal{E},h^u) \subset G$, where $\mathcal{E}$ is a cubic cyclic field extension of L, the obstruction is the quotient $B(\mathcal{E}/L)/\phi(B(\mathcal{F}/k))$, where $\mathcal{F}$ is the subfield of $\mathcal{E}$, fixed by the involution σ on $\mathcal{E}$, and ϕ is the base change map $B(\mathcal{F}/k) \longrightarrow B(\mathcal{E}/L)$.

References

[B]   N. Bourbaki, *Lie Groups And Lie Algebras*, Chapters 4–6, Springer-Verlag, Berlin, 2000.

[Be1]   E. A. Bender, *Symmetric matrices, characteristic polynomials and hilbert symbols over local number fields*, Bulletin of the American Mathematical Society **79** (1973), 518–520.

[Be2]   E. A. Bender, *Characteristic polynomial of symmetric matrices*, Pacific Journal of Mathematics **25** (1968), 433–441.

[Bo]   A. Borel, *Linear Algebraic Groups*, GTM 126, Springer-Verlag, Berlin, 1991.

[CR]   B. Chang and R. Ree, *The characters of $G_2(q)$*, Symposia Mathematica, Vol. XIII (Convegno di Gruppi e loro Rappresentazioni, INDAM, Rome, 1972), Academic Press, London, 1974, pp. 395–413.

[FKS]   B. Fein, W. Kantor and M. Schacher, *Relative Brauer groups II*, Journal für die reine und angewandte Mathematik **328** (1981), 39–57.

[FZ]   W. Feit and G. J. Zuckermann, *Reality properties of conjugacy classes in spin groups and symplectic groups*, in *Algebraists' Homage: Papers in Ring Theory and Related Topics* (S. A. Amitsur, D. J. Saltman and G. B. Seligman, eds.), Contemporary Mathematics **13** (1982), 239–253.

[J]   N. Jacobson, *Composition algebras and their automorphisms*, Rendiconti del Circolo Matematico di Palermo (2) **7** (1958), 55–80.

[K]   M. Kneser, *Lectures on Galois Cohomology of Classical Groups, With an Appendix by T. A. Springer, Notes by P. Jothilingam*, Tata Institute of Fundamental Research Lectures on Mathematics, No. 47, Tata Institute of Fundamental Research, Bombay, 1969.

[KMRT]   M. A. Knus, A. Merkurjev, M. Rost and J. P. Tignol, *The Book of Involutions*, American Mathematical Society Colloquium Publications, Vol. 44, The American Mathematical Society, Providence, RI, 1998.

[L]   H. Lausch, *Generators of automorphism groups of Cayley algebras*, in *Generators and Relations in Groups and Geometries (Lucca, 1990)*, Kluwer Academic, Dordrecht, 1991, pp. 69–94.

[MVW]   C. Moeglin, M.-F. Vignéras and J.-L. Waldspurger, *Correspondences de Howe sur un corps p-adique*, Lecture Notes in Mathematics **1291**, Springer-Verlag, Berlin, 1987.

[N]   A. Neumann, *Bedingungen für die Zweispiegeligkeit der Automorphismengruppen von Cayleyalgebren*, Geometriae Dedicata **34** (1990), 145–159.

[Ni]   K. Nielsen, *On bireflectionality and trireflectionality of orthogonal groups*, Linear Algebra and its Applications **94** (1987), 197–208.

[P]   R. S. Pierce, *Associative Algebras*, Graduate Texts in Mathematics 88, Springer-Verlag, New York–Berlin, 1982.

[R]   J. D. Rogawski, *Automorphisc Representations of Unitary Groups in Three Variables*, Annals of Mathematics Studies 123, Princeton University Press, 1990.

[S]   R. Steinberg, *On Galois Cohomology of Linear Algebraic Groups*, Proceedings of an International Conference on the Theory of Groups, Canberra (1965), Gordon and Breach, London, 1967, pp. 315–319.

[St]   R. Steinberg, *Conjugacy classes in algebraic groups*, Notes by Vinay V. Deodhar, Lecture Notes in Mathematics **366**, Springer-Verlag, Berlin–New York, 1974.

[Se]   J. P. Serre, *Galois Cohomology*, Springer-Verlag, Berlin, 1997.

[Sp]   T. A. Springer, *Linear Algebraic Groups*, second edition, Progress in Mathematics 9, Birkhäuser Boston, Boston, MA, 1998.

[SV]   T. A. Springer and F. D. Veldkamp, *Octonions, Jordan Algebras and Exceptional Groups*, Springer Monographs in Mathematics, Springer-Verlag, Berlin, 2000.

[T]   M. Thakur, *Cayley algebra bundles on $\mathbf{A}_K^2$ revisited*, Communications in Algebra **23** (1995), 5119–5130.

[TZ]   O. Taussky and H. Zassenhaus, *On the similarity transformation between a matrix and its transpose*, Pacific Journal of Mathematics **9** (1959), 893–896.

[W1]   M. J. Wonenburger, *Automorphisms of Cayley algebras*, Journal of Algebra **12** (1969), 441–452.

[W2]   M. J. Wonenburger, *Transformations which are products of two involutions*, Journal of Mathematics and Mechanics **16** (1966), 327–338.

[Wa]   G. E. Wall, *On the conjugacy classes in the unitary, symplectic and orthogonal groups*, Journal of the Australian Mathematical Society **3** (1963), 1–63.