Algebra & Number Theory

Volume 8
2014
No. 8

Twisted Bhargava cubes

Wee Teck Gan and Gordan Savin

msp

ALGEBRA AND NUMBER THEORY 8:8 (2014)
dx.doi.org/10.2140/ant.2014.8.1913

Twisted Bhargava cubes

Wee Teck Gan and Gordan Savin

In his reinterpretation of Gauss's composition law for binary quadratic forms, Bhargava determined the integral orbits of a prehomogeneous vector space which arises naturally in the structure theory of the split group Spin_8. We consider a twisted version of this prehomogeneous vector space which arises in quasisplit Spin_8^E, where E is an étale cubic algebra over a field F. We classify the generic orbits over F by twisted composition F-algebras of E-dimension 2.

1. Introduction

The seminal work of Bhargava [2004a; 2004b; 2004c] has extended Gauss's composition law for binary quadratic forms to far more general situations. The key step in his extension is the investigation of the integral orbits of a group over $\mathbb{Z}$ on a lattice in a prehomogeneous vector space. The prehomogeneous vector space which plays a role in elucidating the nature of the classical Gauss's composition arises from a simply connected Chevalley group G of type D_4. More precisely, let $P = MN$ be a maximal parabolic subgroup of G corresponding to the branching point of the Dynkin diagram of type D_4. As it is readily seen from the Dynkin diagram,

MSC2010: primary 11S90; secondary 17A75, 17C40.
Keywords: Bhargava's cubes, twisted composition algebras.

the derived group M_{der} of the Levi factor M is isomorphic to SL_2^3. The unipotent radical N is 9-dimensional, and is a two-step nilpotent group with 1-dimensional center Z. The adjoint action of M_{der} on the abelian quotient N/Z is isomorphic to $V = V_2 \otimes V_2 \otimes V_2$, where V_2 is the standard 2-dimensional representation of SL_2. Since Bhargava regards an element of $(\mathbb{Z}^2)^{\otimes 3}$ as a cube whose vertices are labeled by elements of $\mathbb{Z}$, we shall refer to the prehomogeneous vector space V or its elements as Bhargava's cubes.

One of Bhargava's achievements is the determination of the corresponding integral orbits, i.e., $\mathrm{SL}_2(\mathbb{Z})^3$-orbits on $\mathbb{Z}^2 \otimes \mathbb{Z}^2 \otimes \mathbb{Z}^2$. In particular, he discovered that generic orbits are in bijection with isomorphism classes of tuples (A, I_1, I_2, I_3), where A is an order in an étale quadratic $\mathbb{Q}$-algebra and I_1, I_2 and I_3 are elements in the narrow class group of A, i.e., invertible fractional ideals, such that $I_1 \cdot I_2 \cdot I_3 = 1$. More precisely, to every cube Bhargava attaches three pairs (A_i, B_i), $i = 1, 2, 3$, of 2×2 matrices by slicing the cube in the three possible ways. In this way he obtains three binary quadratic forms

$$Q_i(x, y) = -\det(A_i x + B_i y).$$

A remarkable fact, discovered by Bhargava, is that the three forms have the same discriminant Δ. It is a degree-4 polynomial on V, invariant under the action of M_{der}. The cube is generic if $\Delta \neq 0$. In this case, the ring A is the unique quadratic order of discriminant Δ and the three fractional ideals I_i correspond to the three quadratic forms Q_i by a dictionary that essentially goes back to Gauss.

We now consider the group G over a field F of characteristic different from 2 and 3. The group G is exceptional in the sense that its outer automorphism group is isomorphic to S_3: no other absolutely simple linear algebraic group has such a large outer automorphism group. In particular, since S_3 is also the group of automorphisms of the split étale cubic F-algebra $F \times F \times F$, we see that every étale cubic F-algebra E determines a quasisplit form G_E. Fixing an épinglage of G defines a splitting of the outer automorphism group S_3 to $\mathrm{Aut}(G)$, so that S_3 acts on V by a group of symmetries of the cube, fixing two opposite vertices. Then the quasisplit group G_E contains a maximal parabolic subgroup $P_E = M_E N_E$, which is a twisted form of the parabolic P mentioned above. The derived group $M_{E,\mathrm{der}}$ of M_E is isomorphic to $\mathrm{Res}_{E/F} \mathrm{SL}_2$. The adjoint action of $M_{E,\mathrm{der}}$ on N_E/Z_E, where Z_E is the center of N_E, is isomorphic to a twisted form V_E of V. We shall call $V_E(F)$ (or its elements) the E-twisted Bhargava cube.

Since the action of S_3 on V permutes the three pairs (A_i, B_i) of 2×2 matrices obtained by slicing a cube in three different ways, it follows by Galois descent that Δ gives rise to a degree-4 polynomial invariant on V_E, denoted by Δ_E. It is a quasi-invariant for M_E. More precisely, if $v \in V_E(F)$ and $g \in M_E(F)$, then

$$\Delta_E(gv) = \chi(v)^2 \cdot \Delta_E(v),$$

where χ is a character of M_E given by the adjoint action on Z_E. An $M_E(F)$-orbit $\mathcal{O} \subset V_E(F)$ is called generic if $\Delta_E(v) \neq 0$ for one and hence for all $v \in \mathcal{O}$. If $\mathcal{O}$ is generic, then the quadratic algebra $K = F\left(\sqrt{\Delta_E(v)}\right)$ is étale. It is an invariant of the generic orbit.

The purpose of this paper is to classify the generic $M_E(F)$-orbits on $V_E(F)$. The main result is:

Theorem 1.1. *Let F be a field of characteristic different from 2 or 3. Fix an étale cubic F-algebra E.*

(i) *There are natural bijections between the following sets*:

(a) *Generic $M_E(F)$-orbits $\mathcal{O}$ on the E-twisted Bhargava cube.*

(b) *E-isomorphism classes of E-twisted composition algebras (C, Q, β) over F which are of E-dimension 2.*

(c) *E-isomorphism classes of pairs (J, i), where J is a Freudenthal–Jordan algebra over F of dimension 9 and*

$$i : E \hookrightarrow J$$

is an F-algebra homomorphism. Here an E-isomorphism from (J, i) to (J', i') is a commutative diagram

$$\begin{array}{ccc} E & \xrightarrow{\ i\ } & J \\ \downarrow & & \downarrow \\ E & \xrightarrow{\ i'\ } & J' \end{array}$$

where the first vertical arrows is the identity, while the second is an F-isomorphism of J and J'.

(ii) *The bijections in* (i) *identify*

$$\mathrm{Stab}_{M_E}(\mathcal{O}) \cong \mathrm{Aut}_E(C, Q, \beta) \cong \mathrm{Aut}_E(i : E \hookrightarrow J).$$

(iii) *Let $K = F\left(\sqrt{\Delta_E(v)}\right)$ be the étale quadratic algebra K attached to a generic orbit $\mathcal{O}$ containing v. Let $L = E \otimes_F K$. The group* $\mathrm{Stab}_{M_E}(\mathcal{O})$ *in* (ii) *sits in a short exact sequence of algebraic groups*

$$1 \longrightarrow T_{E,K} \longrightarrow \mathrm{Stab}_{M_E}(\mathcal{O}) \longrightarrow \mathbb{Z}/2\mathbb{Z} \longrightarrow 1,$$

where

$$T_{E,K}(F) = \{x \in L^\times : N_{L/E}(x) = 1 = N_{L/K}(x)\}$$

is a 2-dimensional torus and where the conjugation action of the nontrivial element of $\mathbb{Z}/2\mathbb{Z}$ on $T_{E,K}$ is given by $x \mapsto x^{-1}$.

The reader is probably not familiar with some terminology in the theorem, so an explanation is necessary. In order to define twisted composition algebras, recall that the algebra E carries a natural cubic form, the norm N_E. The norm defines a quadratic map $x \mapsto x^\#$ from E to E such that $x \cdot x^\# = N_E(x)$. For example, if $E = F^3$, then

$$N_E(x_1, x_2, x_3) = x_1x_2x_3 \text{ and } (x_1, x_2, x_3)^\# = (x_2x_3, x_3x_1, x_1x_2).$$

Now, an E-twisted composition algebra (or simply twisted composition algebra) of E-dimension 2 is a triple (C, Q, β) where:

- C is an E-vector space of dimension 2.
- $Q : C \longrightarrow E$ is a quadratic form.
- $\beta : C \longrightarrow C$ is a quadratic map such that, for every $v \in C$ and $x \in E$,

$$\beta(xv) = x^\# \cdot \beta(v) \quad \text{and} \quad Q(\beta(v)) = Q(v)^\#.$$

- If b_Q is the bilinear form associated to Q, then $b_Q(v, \beta(v)) \in F$ for every $v \in C$.

This definition is due to Springer, as is the bijection of the sets (b) and (c). More precisely, suppose we have an algebra embedding $i : E \hookrightarrow J$. Then we have a decomposition

$$J = E \oplus C,$$

where C is defined as the orthogonal complement to E with respect to the trace form on J. The upshot is that the Jordan algebra J determines the structure of a twisted composition algebra on C, and vice versa.

Our contribution is the bijection between the sets (a) and (b). Starting with a twisted cube, we define a twisted composition algebra. In fact, the construction works over $\mathbb{Z}$, and can be tied to Bhargava's description as follows. Let (I_1, I_2, I_3) be a triple of ideals in a quadratic order A such that $I_1 \cdot I_2 \cdot I_3 = A$. Let $N(I)$ denote the norm of the ideal I and $z \mapsto \bar{z}$ denote the action of the nontrivial automorphism of the étale quadratic $\mathbb{Q}$-algebra containing A. Let

$$C = I_1 \oplus I_2 \oplus I_3.$$

Then C is a twisted composition algebra with quadratic form $Q : C \to \mathbb{Z} \times \mathbb{Z} \times \mathbb{Z}$ defined by

$$Q(z_1, z_2, z_3) = \left(\frac{N(z_1)}{N(I_1)}, \frac{N(z_2)}{N(I_2)}, \frac{N(z_3)}{N(I_3)} \right)$$

and quadratic map $\beta : C \to C$ defined by

$$\beta(z_1, z_2, z_3) = (\bar{z}_2\bar{z}_3N(I_1), \bar{z}_3\bar{z}_1N(I_2), \bar{z}_1\bar{z}_2N(I_3)).$$

The key parts of the paper are as follows. In order to prove the correspondence of generic $M_E(F)$-orbits and twisted composition algebras, we give a Galois cohomological argument in Theorem 8.3, based on the observation that the stabilizer of a distinguished cube is isomorphic to the automorphism group of a distinguished twisted composition algebra. This gives a conceptual explanation for the existence of the bijection. However, for arithmetic applications (such as Bhargava's), it is essential to have an explicit description of the bijection. This is done in two steps. Firstly, after reviewing the theory of twisted composition algebras, we prove in Proposition 3.5 that every twisted composition algebra C of E-dimension 2 has a reduced basis, i.e., a basis of the form $\{v, \beta(v)\}$ for some $v \in C$. Secondly, by reinterpreting Bhargava's work in the framework of twisted composition algebras in Section 10, we attach to every generic E-twisted cube a twisted composition algebra together with a good basis. In this correspondence, changing the cube by another in the same $M_E(F)$-orbit corresponds to changing the good basis. Since reduced bases are good, every twisted composition algebra is obtained in this construction.

We also consider $\widetilde{M} = M \rtimes S_3$ and its twisted form $\widetilde{M}_E$. In this case, generic $\widetilde{M}_E(F)$-orbits correspond to the F-isomorphism classes of objects in (b) and (c). The isomorphisms of the stabilizer groups in (ii) lead us to another description of $T_{E,K}$, which we view as an *exceptional Hilbert 90* theorem. This is the topic of Section 11. We conclude the paper by illustrating the main results in the case where F is a local field.

2. Étale cubic algebras

Let F be a field of characteristic different from 2 and 3. Let $\overline{F}$ be a separable closure of F, with absolute Galois group $\mathrm{Gal}(\overline{F}/F)$.

2-1. ***Étale cubic algebras.*** An étale cubic algebra is an F-algebra E such that $E \otimes_F \overline{F} \cong \overline{F}^3$. More concretely, an étale cubic F-algebra is of the form

$$E = \begin{cases} F \times F \times F; \\ F \times K, \text{ where } K \text{ is a quadratic field extension of } F; \\ \text{a cubic field.} \end{cases}$$

Since the split algebra $F \times F \times F$ has automorphism group S_3 (the symmetric group on 3 letters), the isomorphism classes of étale cubic algebras E over F are naturally classified by the pointed cohomology set $H^1(F, S_3)$, or more explicitly by the set of conjugacy classes of homomorphisms

$$\rho_E : \mathrm{Gal}(\overline{F}/F) \longrightarrow S_3.$$

2-2. ***Discriminant algebra of E.*** By composing the homomorphism ρ_E with the sign character of S_3, we obtain a quadratic character (possibly trivial) of $\mathrm{Gal}(\overline{F}/F)$

which corresponds to an étale quadratic algebra K_E. We call K_E the *discriminant algebra* of E. To be concrete,

$$K_E = \begin{cases} F \times F & \text{if } E = F^3 \text{ or a cyclic cubic field;} \\ K & \text{if } E = F \times K; \\ \text{the unique quadratic subfield in the Galois closure of } E & \text{otherwise.} \end{cases}$$

2-3. ***Twisted form of S_3.*** Fix an étale cubic F-algebra E. Then, via the associated homomorphism ρ_E, $\mathrm{Gal}(\overline{F}/F)$ acts on S_3 (by inner automorphisms) and thus defines a twisted form S_E of the finite constant group scheme S_3. For any commutative F-algebra A, we have

$$S_E(A) = \mathrm{Aut}_A(E \otimes_F A).$$

2-4. ***Quadratic map #.*** Given an étale cubic F-algebra, let $N_E : E \longrightarrow F$ be the norm map on E and let $\mathrm{Tr}_E : E \longrightarrow F$ be the trace map. Then N_E is a cubic form and Tr_E is a linear form on E. There is a quadratic map

$$\# : E \longrightarrow E$$

such that

$$a^{\#} \cdot a = a \cdot a^{\#} = N_E(a) \quad \text{for } a \in E.$$

It has an associated symmetric bilinear map

$$a \times b := (a+b)^{\#} - a^{\#} - b^{\#}.$$

For the split algebra F^3, we have:

$$N(a_1, a_2, a_3) = a_1 a_2 a_3, \quad \mathrm{Tr}(a_1, a_2, a_3) = a_1 + a_2 + a_3,$$
$$(a_1, a_2, a_3)^{\#} = (a_2 a_3, a_3 a_1, a_1 a_2).$$

We note the following identity in E:

$$(f \times y)y + f y^{\#} = \mathrm{Tr}_{E/F}(f y^{\#}). \tag{2.1}$$

This curious identity can be checked in $E \otimes_F \overline{F} \cong \overline{F}^3$; we leave it as an interesting exercise for the reader.

3. Twisted composition algebras

In this section, we introduce the E-twisted composition algebra of dimension 2 over E. This notion was introduced by Springer, and the two standard (perhaps only) references, covering many topics of this paper, are [Knus et al. 1998] and [Springer and Veldkamp 2000]. Twisted composition algebras are treated in Chapter VIII, §36 of the former and Chapter 4 of the latter.

3-1. ***Twisted composition algebras.*** A twisted composition algebra over F is a quadruple (E, C, Q, β), where:

- E is an étale cubic F-algebra.
- C is a free E-module equipped with a nondegenerate quadratic form Q, with associated symmetric bilinear form $b_Q(v_1, v_2) = Q(v_1+v_2)-Q(v_1)-Q(v_2)$.
- $\beta : C \longrightarrow C$ is a quadratic map such that

$$\beta(av) = a^{\#} \cdot \beta(v) \quad \text{and} \quad Q(\beta(v)) = Q(v)^{\#}$$

  for every $a \in E$ and $v \in C$.
- If we set

$$N_C(v) := b_Q(v, \beta(v)),$$

  then $N_C(v) \in F$ for every $v \in C$.

For a fixed E, we shall call (C, Q, β) an E-twisted composition algebra (over F), and the cubic form N_C the norm form of C. Frequently, for ease of notation, we shall simply denote this triple by C, suppressing the mention of Q and β.

3-2. ***Morphisms.*** An F-morphism of twisted composition algebras (E, C, Q, β) and (E', C', Q', β') is a pair $(\phi, \sigma) \in \mathrm{Hom}_F(C, C') \times \mathrm{Hom}_F(E, E')$ such that

$$\phi(av) = \sigma(a) \cdot \phi(v)$$

for $v \in C$ and $a \in E$, and

$$\phi \circ \beta = \beta' \circ \phi \quad \text{and} \quad \sigma \circ Q = Q' \circ \phi.$$

In particular, we have the automorphism group $\mathrm{Aut}_F(E, C, Q, \beta)$. The second projection gives a natural homomorphism

$$\mathrm{Aut}_F(E, C, Q, \beta) \to S_E.$$

The kernel of this map is the subgroup $\mathrm{Aut}_E(C, Q, \beta)$ consisting of those ϕ which are E-linear; we shall call these E-morphisms.

3-3. $\mathbf{Aut}_F(E, C)$***-action and isomorphism classes.*** Let us fix an E-vector space C and let $\mathrm{Aut}_E(C)$ be the automorphism group of C as an E-vector space. Let

$$\mathrm{Aut}_F(E, C) = \{(g, \sigma) \in \mathrm{Aut}_F(C) \times \mathrm{Aut}_F(E) : g \circ \lambda = \sigma(\lambda) \cdot g \text{ for all } \lambda \in E\}.$$

This is the group of E-sesquilinear automorphisms of C. The second projection induces a short exact sequence

$$1 \longrightarrow \mathrm{Aut}_E(C) \longrightarrow \mathrm{Aut}_F(E, C) \longrightarrow S_E \longrightarrow 1.$$

This short exact sequence is split. Indeed, the choice of an E-basis for C gives a splitting, with S_E acting on the coordinates with respect to the basis.

Now if (C, Q, β) is an E-twisted composition algebra, then for any $(g, \sigma) \in \mathrm{Aut}_F(E, C)$, the triple

$$(C', Q', \beta') = (C, \sigma \circ Q \circ g^{-1}, g \circ \beta \circ g^{-1})$$

is also an E-twisted composition algebra. The norm forms are related by

$$N_{C'} = N_C \circ g^{-1}.$$

Moreover, we have

$$(g, \sigma) \in \mathrm{Hom}_F((E, C, Q, \beta), (E, C', Q', \beta')).$$

Thus the map $(Q, \beta) \mapsto (Q', \beta')$ defines an action of $\mathrm{Aut}_F(E, C)$ on the set of pairs (Q, β) which define an E-twisted composition algebra structure on C. The orbits of such pairs under $\mathrm{Aut}_F(E, C)$ are precisely the F-isomorphism classes of E-twisted composition algebras of a given E-dimension $\dim_E C$, and the stabilizer of a given pair (Q, β) is precisely the automorphism group $\mathrm{Aut}_F(E, C, Q, \beta)$. Similarly, the set of orbits under $\mathrm{Aut}_E(C)$ is the set of E-isomorphism classes of such E-twisted composition algebras, and the stabilizer of a particular (Q, β) is $\mathrm{Aut}_E(C, Q, \beta)$.

3-4. ***Dimension-2 case.*** It is known, by Corollary 36.4 in [Knus et al. 1998], that for any E-twisted composition algebra (C, Q, β), $\dim_E C = 1, 2, 4$ or 8. We shall only be interested in the case when $\dim_E C = 2$.

We give an example that will feature prominently in this paper. We set $C_E = E \oplus E$, and define Q and β by

$$Q(x, y) = x \cdot y \quad \text{and} \quad \beta(x, y) = (y^{\#}, x^{\#})$$

for every $(x, y) \in E \oplus E$. It is easy to check that this defines an E-twisted composition algebra over F, with norm form

$$N_C(x, y) = N_E(x) + N_E(y).$$

The group of automorphisms of this E-twisted composition algebra is easy to describe. Let E^1 be the set of elements e in E such that $N(e) = e \cdot e^{\#} = 1$. For every element $e \in E^1$, we have an E-automorphism i_e defined by $i_e(x, y) = (ex, e^{\#}y)$. We also have an E-automorphism w defined by $w(x, y) = (y, x)$. The group of E-automorphisms is

$$\mathrm{Aut}_E(C_E, Q, \beta) = E^1 \rtimes \mathbb{Z}/2\mathbb{Z}$$

and the group of F-automorphisms is

$$\mathrm{Aut}_F(C_E, Q, \beta) = (E^1 \rtimes \mathbb{Z}/2\mathbb{Z}) \rtimes S_E = E^1 \rtimes (\mathbb{Z}/2\mathbb{Z} \times S_E).$$

If $E = F \times F \times F$, we denote the corresponding twisted composition algebra by $C_0 = (C_0, Q_0, \beta_0)$ and refer to it as the split twisted composition algebra. In this case, E^1 consists of (t_1, t_2, t_3) such that $t_1 t_2 t_3 = 1$, so that

$$\mathrm{Aut}_E(C_0, Q_0, \beta_0) \cong \mathbb{G}_m^2 \rtimes \mathbb{Z}/2\mathbb{Z}.$$

Observe that there is a natural splitting

$$S_3 \times \mathbb{Z}/2\mathbb{Z} \longrightarrow \mathrm{Aut}_F(C_0, Q_0, \beta_0). \tag{3.1}$$

3-5. ***Identities.*** It follows by [Knus et al. 1998, Proposition 36.3] that if (E, C, Q, β) is a twisted composition algebra over F, then $C \otimes_F \overline{F}$ is isomorphic to $C_0 \otimes_F \overline{F}$. This fact is useful for verifying polynomial identities in C. Indeed, any polynomial identity in C may be verified over $\overline{F}$ and thus just needs to be checked in C_0. In the following lemma, we list some useful identities which may be checked in this manner.

Lemma 3.2. *Let (E, C, Q, β) be a twisted composition algebra over F. Then*

$$\beta^2(v) = N_C(v)v - Q(v)\beta(v) \tag{3.3}$$

and

$$\beta(xv + y\beta(v)) = (y^{\#}N_C(v) - (-Q(v)x) \times y) \cdot v + (x^{\#} - Q(v)y^{\#}) \cdot \beta(v) \tag{3.4}$$

for any $v \in C$ and $x, y, \in E$.

It follows from (3.3) that Q is in fact determined by β in a twisted composition algebra. The proof of these identities can be found in [Springer and Veldkamp 2000, Lemmas 4.1.3 and 4.2.7]. We note that (3.4) looks slightly different from its counterpart there (Lemma 4.2.7), but the two are equivalent by the identity (2.1).

3-6. ***Reduced basis.*** If $\dim_E C = 2$, we call an E-basis of C of the form $\{v, \beta(v)\}$ a reduced basis of C. We note:

Proposition 3.5. *Let (C, Q, β) be an E-twisted composition algebra.*

(i) *For $v \in C$, let*

$$\Delta_C(v) = N_C(v)^2 - 4 \cdot N_E(Q(v)) \in F.$$

Then $\{v, \beta(v)\}$ is an E-basis of C if and only if $\Delta_C(v) \neq 0$.

(ii) *The degree-6 homogeneous polynomial Δ_C factors over F as*

$$\Delta_C = a \cdot P^2,$$

with $a \in F^\times$ and P an absolutely irreducible homogeneous polynomial of degree 3 over F. The square class of a is uniquely determined, and for any $g \in \mathrm{Aut}_E(C, Q, \beta)$,

$$P(gv) = \begin{cases} P(v) & \text{if } g \in \mathrm{Aut}_E(C, Q, \beta)^0, \\ -P(v) & \text{if } g \notin \mathrm{Aut}_E(C, Q, \beta)^0. \end{cases} \tag{3.6}$$

(iii) *The algebra (C, Q, β) has a reduced basis.*

(iv) *Let $\{v', \beta(v')\}$ be another reduced basis of C. Let $g \in \mathrm{Aut}_E(C)$ be such that $g(v) = v'$ and $g(\beta(v)) = \beta(v')$. Then* $\det(g) \in F^\times$.

Proof. (i) The set $\{v, \beta(v)\}$ is a basis if and only if the matrix of the symmetric bilinear form b_Q with respect to $\{v, \beta(v)\}$ has determinant in $E^\times$. Since

$$b_Q(v, v) = 2Q(v), \quad b_Q(\beta(v), \beta(v)) = 2Q(v)^\# \quad \text{and} \quad b_Q(v, \beta(v)) = N_C(v),$$

it follows that the determinant is $-\Delta_C(v)$.

(ii) We first work over $\overline{F}$, in which case we may assume that $C = E^2$, with $E = \overline{F}^3$, $Q(x, y) = xy$ and $\beta(x, y) = (y^\#, x^\#)$. Then $N_C(x, y) = N_E(x) + N_E(y)$. So

$$\Delta_C(x, y) = (N_E(x) + N_E(y))^2 - 4N_E(x)N_E(y) = (N_E(x) - N_E(y))^2.$$

The cubic polynomial $P_0(x, y) = N_E(x) - N_E(y) = x_1x_2x_3 - y_1y_2y_3$ (with $x = (x_1, x_2, x_3) \in \overline{F}^3$) is easily seen to be irreducible over $\overline{F}$.

To descend back to F, we note that for any $\sigma \in \mathrm{Gal}(\overline{F}/F)$, $\sigma(P_0) = \pm P_0$ by unique factorization of polynomials over $\overline{F}$. Thus there is a quadratic character χ_K of $\mathrm{Gal}(\overline{F}/F)$ such that $\sigma(P_0) = \chi_K(\sigma) \cdot P_0$. If K is the quadratic étale F-algebra associated to χ_K, represented by $a \in F^\times$, then we see that $P = \sqrt{a}^{-1} \cdot P_0$ is defined over F and $\Delta_C = a \cdot P^2$.

It is clear that the square class of a is uniquely determined. Equation (3.6) can be checked over $\overline{F}$; we leave it to the reader.

(iii) Since F has more than 3 elements (as we assumed that $\mathrm{char}(F) \neq 2$ or 3), there exists $v \in C$ such that $P(v) \neq 0$. Hence $\Delta_C(v) \neq 0$ by (ii) and $\{v, \beta(v)\}$ is a reduced basis by (i).

(iv) If $v' = xv + y\beta(v)$, then $\beta(v')$ is given by (3.4). So the transition matrix between the bases $\{v, \beta(v)\}$ and $\{v', \beta(v')\}$ is given by

$$g = \begin{pmatrix} x & y^\# N_C(v) - (-Q(v)x) \times y \\ y & x^\# - Q(v)y^\# \end{pmatrix}.$$

Hence

$$\begin{aligned} \det(g) &= N_E(x) - N_E(y)N_C(v) + (-Q(v)xy^\# + ((-Q(v)x) \times y)y) \\ &= N_E(x) - N_E(y)N_C(v) - \mathrm{Tr}_E(Q(v)xy^\#) \in F \end{aligned}$$

where the second equality follows by applying (2.1). □

We note that Proposition 3.5(i) and (iii) are contained in [Springer and Veldkamp 2000, Lemma 4.2.12], but (ii) seems to be new; at least we are not able to find it in [Springer and Veldkamp 2000] or [Knus et al. 1998]. The results of the proposition will be used later in the paper.

3-7. ***The quadratic algebra K_C.*** An immediate consequence of the proposition is that to every twisted composition algebra (E, C, Q, β) with $\dim_E C = 2$, we can associate an étale quadratic algebra K_C which is given by the square-class of $\Delta_C(v) \in F^\times$ as in the proof of Proposition 3.5(ii). Thus we have a map

$$\{\text{twisted composition } F\text{-algebras with } E\text{-rank } 2\} \longrightarrow \{\text{étale quadratic } F\text{-algebras}\}. \tag{3.7}$$

For example, if C_E is the twisted composition algebra introduced in Section 3-4, then

$$\Delta_C(x, y) = (N_E(x) - N_E(y))^2$$

and the quadratic algebra associated to C_E is the split algebra $F \times F$.

3-8. ***Cohomological description.*** We come now to the classification of twisted composition algebras C of rank 2 over E. Since every such C is isomorphic to C_0 over $\overline{F}$, the set of isomorphism classes of twisted composition algebras over F is classified by the pointed cohomology set

$$H^1(F, \mathrm{Aut}_F(F^3, C_0, Q_0, \beta_0)).$$

We have seen that $\mathrm{Aut}_F(F^3, C_0, Q_0, \beta_0) \cong \mathbb{G}_m^2 \rtimes (\mathbb{Z}/2\mathbb{Z} \times S_3)$, and so there is a natural map

$$H^1(F, \mathrm{Aut}_F(F^3, C_0, Q_0, \beta_0)) \longrightarrow H^1(F, \mathbb{Z}/2\mathbb{Z}) \times H^1(F, S_3). \tag{3.8}$$

Composing this with the first or second projections, we obtain natural maps

$$H^1(F, \mathrm{Aut}_F(F^3, C_0, Q_0, \beta_0)) \longrightarrow H^1(F, \mathbb{Z}/2\mathbb{Z}) = \{\text{étale quadratic } F\text{-algebras}\} \tag{3.9}$$

and

$$H^1(F, \mathrm{Aut}_F(F^3, C_0, Q_0, \beta_0)) \longrightarrow H^1(F, S_3). \tag{3.10}$$

All these projection maps are surjective, because of the natural splitting in (3.1). Indeed, (3.1) endows each fiber of the maps in (3.8), (3.9) and (3.10) with a distinguished point. We shall see in a moment that the map in (3.9) is the map defined in (3.7).

For an étale cubic F-algebra E with associated cohomology class $[E] \in H^1(F, S_3)$, the fiber of (3.10) over $[E]$ is precisely the set of F-isomorphism classes of E-twisted composition algebras. Moreover, a Galois descent argument shows that the distinguished point in this fiber furnished by the splitting (3.1) is none other than the E-twisted composition algebra C_E constructed in Section 3-4.

Using C_E as the base point, the fiber in question is identified naturally with the set $H^1(F, \mathrm{Aut}_E(C_E, Q, \beta))$ modulo the natural action of $S_E(F)$ (by conjugation). The cohomology set $H^1(F, \mathrm{Aut}_E(C_E, Q, \beta))$ classifies the E-isomorphism classes of E-twisted composition algebras C over F, and the action of $S_E(F)$ is given by

$$\sigma : (C, Q, \beta) \mapsto (C \otimes_{E,\sigma} E, \sigma \circ Q, \beta)$$

for $\sigma \in S_E(F)$.

Lemma 3.11. *The maps defined by (3.7) and (3.9) are the same.*

Proof. We fix the cubic algebra E and let $C_E = (E^2, Q, \beta)$ be the distinguished E-twisted composition algebra introduced in Section 3-4. Let $\Delta_C = P^2$ be the homogeneous polynomials as given in Proposition 3.5(ii).

Any E-twisted composition algebra C' is given by a pair of tensors (Q', β') on E^2, and there is an element $g \in \mathrm{GL}_2(E \otimes_F \overline{F})$ such that $g \cdot (Q, \beta) = (Q', \beta')$. A 1-cocycle associated to (Q', β') is given by

$$a_\sigma = g^{-1}\sigma(g) \in \mathrm{Aut}_{\overline{F}^3}(E^2, Q, \beta) \quad \text{for } \sigma \in \mathrm{Gal}(\overline{F}/F).$$

The corresponding $\Delta_{C'}$ is related to Δ_C by

$$\Delta_{C'}(v) = \Delta_C(g^{-1}v).$$

Now, the quadratic algebra associated to C' by (3.9) corresponds to the quadratic character

$$\chi : \sigma \mapsto [a_\sigma] \in \pi_0(\mathrm{Aut}_{\overline{F}^3}(E^2, Q, \beta)) = \mathbb{Z}/2\mathbb{Z}$$

of $\mathrm{Gal}(\overline{F}/F)$. By (3.6), we thus have

$$P(a_\sigma^{-1}v) = \chi(\sigma) \cdot P(v)$$

for any $v \in (E \otimes_F \overline{F})^2$.

On the other hand, the quadratic algebra associated to C' by (3.7) is defined by $\sqrt{\Delta_{C'}(v)}$ for any $v \in E^2$ such that $\Delta_{C'}(v) \neq 0$. Since

$$\sqrt{\Delta_{C'}(v)} = \sqrt{\Delta_C(g^{-1}v)} = P(g^{-1}v),$$

we need to show that

$$\sigma(P(g^{-1}v)) = \chi(\sigma)P(g^{-1}v).$$

But we have

$$\sigma(P(g^{-1}v)) = P(\sigma(g)^{-1}v) = P(a_\sigma^{-1}g^{-1}v) = \chi(\sigma)\cdot P(g^{-1}v),$$

as desired. □

3-9. ***Tits construction.*** Given an element

$$([E],[K]) \in H^1(F,S_3)\times H^1(F,\mathbb{Z}/2\mathbb{Z}),$$

we describe the composition algebras in the fiber of (3.8) over $([E],[K])$. Note that by (3.1), we have a distinguished point in this fiber. Now, we have:

Proposition 3.12. *If C is an E-twisted composition algebra, with associated étale quadratic algebra K, then we may identify C with $E\otimes_F K$, such that*

$$Q(x) = e\cdot N_{E\otimes_F K/E}(x) \quad \textit{for some } e\in E^\times$$

and

$$\beta(x) = \bar{x}^{\#}\cdot e^{-1}\cdot \bar{v} \quad \textit{for some } v\in K$$

where $x\mapsto \bar{x}$ is induced by the nontrivial automorphism of K over F. Moreover, we have:

$$N_{E/F}(e) = N_{K/F}(v).$$

The distinguished point in the fiber of (3.8) over $([E],[K])$ corresponds to taking $(e,v)=(1,1)$.

Proof. The proof of Proposition 3.5(i) shows that the quadratic discriminant algebra associated to Q is $E\otimes_F K$. Hence, we may identify C with $E\otimes_F K$ with Q given by $e\cdot N_{E\otimes_F K/E}$ for some $e\in E^\times$. On the other hand, we claim that for $x\in E\otimes_F K$ and $x_0\in C$, one has

$$\beta(x\cdot x_0) = \bar{x}^{\#}\cdot\beta(x_0).$$

Indeed, one can check this by going to $\overline{F}$, where one is reduced to checking this identity in the split algebra C_0, which is straightforward. This shows that β is determined by $\beta(1)=\bar{v}\cdot e^{-1}$ for some $v\in E\otimes_F K$. However, the identity

$$Q(1)^{\#} = Q(\beta(1))$$

implies that

$$v\cdot\bar{v} = N_{E\otimes_F K/E}(v) = N_{E/F}(e)\in F.$$

The requirement that $N(x)\in F$ for all $x\in E\otimes_F K$ implies that

$$\mathrm{Tr}_{E\otimes_F K/E}(\bar{v}\cdot N_{E\otimes_F K/K}(x))\in F.$$

In particular, taking $x = 1$ and then a trace-zero element $\delta \in K$ one obtains, respectively,

$$\nu + \bar{\nu} \in F \quad \text{and} \quad \nu\delta + \overline{\nu\delta} \in F.$$

All these conditions imply that $\nu \in K$.

Finally, it is easy to see by Galois descent that the distinguished point in the fiber over $([E], [K])$ corresponds to $(e, \nu) = (1, 1)$. □

The description of twisted composition algebras given in the above proposition is sometimes referred to as a Tits construction (though usually this terminology is reserved for the Jordan algebra associated to the above twisted composition algebra by Springer's construction, which is the subject matter of the next section).

3-10. ***Automorphism group.*** Using Proposition 3.12, it is not difficult to determine the automorphism group of any twisted composition algebra C. Indeed, if $C \cong E \otimes_F K$ as in the proposition, then the special orthogonal group

$$SO(C, Q) = \{\lambda \in E \otimes_F K : N_{E\otimes K/E}(\lambda) = 1\}$$

acts $E \otimes K$-linearly on C by multiplication and preserves Q. An element $\lambda \in SO(C, Q)$ preserves β if and only if

$$\bar{\lambda}^{\#} = \lambda.$$

But $\lambda^{\#} = \lambda^{-1}$ since $N_{E\otimes K/E}(\lambda) = \lambda \cdot \lambda^{\#} = 1$. So

$$\mathrm{Aut}_E(C, Q, \beta) \cap SO(C, Q) = \{\lambda \in L = E \otimes K : N_{L/E}(\lambda) = 1 = N_{L/K}(\lambda)\} = T_{E,K},$$

which is a 2-dimensional torus. Since we know the automorphism group of the split twisted composition algebra (C_0, Q_0, β_0), we see that

$$\mathrm{Aut}_E(C, Q, \beta)^0 = T_{E,K}$$

and $\mathrm{Aut}_E(C, Q, \beta)$ sits in short exact sequences of algebraic groups as in (iii) of Theorem 1.1.

3-11. ***Cohomology of $T_{E,K}$.*** Using Proposition 3.12 and the above description of $\mathrm{Aut}_E(C, Q, \beta)^0$, we can describe the fiber of the natural map

$$H^1(F, \mathrm{Aut}_F(F^3, C_0, Q_0, \beta_0)) \longrightarrow H^1(F, \mathbb{Z}/2\mathbb{Z}) \times H^1(F, S_3)$$

over the element $([K], [E]) \in H^1(F, \mathbb{Z}/2\mathbb{Z}) \times H^1(F, S_3)$. Indeed, this fiber is equal to

$$H^1(F, T_{E,K}) \text{ modulo the action of } S_E(F) \times \mathbb{Z}/2\mathbb{Z}.$$

The cohomology group $H^1(T_{E,K})$ classifies twisted composition algebras with fixed E and K, up to $E \otimes_F K$-linear isomorphism. With $L = E \otimes_F K$, one has a short exact sequence of algebraic tori

$$1 \longrightarrow T_{E,K} \longrightarrow L^\times \xrightarrow{N_{L/E} \times N_{L/K}} (E^\times \times K^\times)^0 \longrightarrow 1,$$

where

$$(E \times K)^0 = \{(e, v) \in E^\times \times K^\times : N_{E/F}(e) = N_{K/F}(v)\}.$$

The associated long exact sequence gives

$$H^1(F, T_{E,K}) \cong (E^\times \times K^\times)^0 / \operatorname{Im} L^\times. \tag{3.13}$$

This isomorphism is quite evident in the context of Proposition 3.12. Indeed, Proposition 3.12 tells us that any twisted composition algebra C with invariants (E, K) is given by an element $(e, v) \in (E^\times \times K^\times)^0$. Any L-linear map from C to another twisted composition algebra C' with associated pair (e', v') is given by multiplication by an element $a \in L^\times$, and this map is an isomorphism of twisted composition algebras if and only if

$$(e, v) = (e' \cdot N_{L/E}(a), v' \cdot N_{L/K}(a)).$$

This is precisely what (3.13) expresses.

4. Springer's construction

We can now relate twisted composition algebras to Freudenthal–Jordan algebras. This construction is due to Springer. Our exposition follows [Knus et al. 1998, §38A, p. 522].

4-1. ***Freudenthal–Jordan algebra of dimension 9.*** A Freudenthal–Jordan algebra J of dimension 9 over F is a Jordan algebra which is isomorphic over $\overline{F}$ to the Jordan algebra J_0 associated to the associative algebra $M_3(F)$ of 3×3-matrices, with Jordan product

$$a \circ b = \tfrac{1}{2} \cdot (ab + ba).$$

An element $a \in J$ satisfies a characteristic polynomial

$$X^3 - T_J(a)X^2 + S_J(a)X - N_J(a) \in F[X].$$

The maps T_J and N_J are called the trace and norm maps of J respectively. The element

$$a^\# = a^2 - T_J(a)a + S_J(a)$$

is called the adjoint of a. It satisfies $a \cdot a^{\#} = N_J(a)$. The cross product of two elements $a, b \in J$ is defined by

$$a \times b = (a+b)^{\#} - a^{\#} - b^{\#}.$$

4-2. ***Cohomological description.*** The automorphism group of J_0 is $\mathrm{PGL}_3 \rtimes \mathbb{Z}/2\mathbb{Z}$, with $g \in \mathrm{PGL}_3$ acting by conjugation and the nontrivial element of $\mathbb{Z}/2\mathbb{Z}$ acting by the transpose $a \mapsto a^t$. Thus, the isomorphism classes of Freudenthal–Jordan algebras of dimension 9 are parametrized by the pointed set $H^1(F, \mathrm{PGL}_3 \rtimes \mathbb{Z}/2\mathbb{Z})$, and there is an exact sequence of pointed sets

$$H^1(F, \mathrm{PGL}_3) \xrightarrow{f} H^1(F, \mathrm{PGL}_3 \rtimes \mathbb{Z}/2\mathbb{Z}) \xrightarrow{\pi} H^1(F, \mathbb{Z}/2\mathbb{Z}) \parallel \{\text{étale quadratic } F\text{-algebras}\}.$$

The map π is surjective and the fiber of π over the split quadratic algebra F^2 is the image of f. By [Serre 2002, Proposition 39(ii) and Corollary 1, p. 52], the image of f is $H^1(F, \mathrm{PGL}_3)$ modulo a natural action of $\mathbb{Z}/2\mathbb{Z}$. Now the set $H^1(F, \mathrm{PGL}_3)$ parametrizes the set of central simple F-algebras B of degree 3, and the $\mathbb{Z}/2\mathbb{Z}$ action in question is $B \mapsto B^{\mathrm{op}}$. Then the map f sends B to the associated Jordan algebra.

In general, for any étale quadratic F-algebra K, an element in the fiber of π over $[K] \in H^1(F, \mathbb{Z}/2\mathbb{Z})$ is the Jordan algebra $J_3(K)$ of 3×3-Hermitian matrices with entries in K. The automorphism group of $J_3(K)$ is an adjoint group $PGU_3^K \rtimes \mathbb{Z}/2\mathbb{Z}$. Using $J_3(K)$ as the base point, the fiber of π over $[K]$ can then be identified with $H^1(F, PGU_3^K)$ modulo the action of $\mathbb{Z}/2\mathbb{Z}$ (by [Serre 2002, pp. 50 and 52]). By [Knus et al. 1998, p. 400], $H^1(F, PGU_3^K)$ has an interpretation as the set of isomorphism classes of pairs (B_K, τ) where

- B_K is a central simple K-algebra of degree 3,
- τ is an involution of the second kind on B_K.

Moreover, the action of the nontrivial element $\tau_K \in \mathrm{Aut}(K/F) = \mathbb{Z}/2\mathbb{Z}$ is via the Galois twisting action $B \mapsto B \otimes_{K, \tau_K} K$, so that

$$H^1(F, PGU_3^K)/\mathbb{Z}/2\mathbb{Z} \longleftrightarrow \{F\text{-isomorphism classes of } (B_K, \tau)\}.$$

Then the map f sends (B_K, τ) to the Jordan algebra B_K^{τ} of τ-symmetric elements in B_K.

If J is a Freudenthal–Jordan algebra of dimension 9, we will write K_J for the étale quadratic algebra corresponding to $\pi(J)$.

4-3. ***Relation with twisted composition algebras.*** Fix an étale cubic F-algebra E and a Freudenthal–Jordan algebra J. Suppose we have an algebra embedding

$$i : E \hookrightarrow J.$$

Then, with respect to the trace form T_J, we have an orthogonal decomposition

$$J = i(E) \oplus C,$$

where $C = i(E)^{\perp}$. We shall identify E with its image under i. Then for $e \in E$ and $v \in C$, one can check that $e \times v \in C$. Thus, setting

$$e \circ v := -e \times v$$

equips C with the structure of an E-vector space. Moreover, writing

$$v^{\#} = (-Q(v), \beta(v)) \in E \oplus C = J$$

for $Q(v) \in E$ and $\beta(v) \in V$, we obtain a quadratic form Q on C and a quadratic map β on C. Then, by Theorem 38.6 in [Knus et al. 1998], the triple (C, Q, β) is an E-twisted composition algebra over F.

Conversely, given an E-twisted composition algebra C over F, the same theorem says that the space $E \oplus C$ can be given the structure of a Freuthendal–Jordan algebra over F. In particular, we have described the bijective correspondence between the objects in (b) and (c) of the main theorem:

$$\{E\text{-twisted composition algebras over } F\}$$
$$\updownarrow$$
$$\{i : E \longrightarrow J \text{ with } J \text{ Freudenthal–Jordan of dimension } 9\}.$$

It is also clear that under this identification, one has

$$\mathrm{Aut}_F(i : E \to J) = \mathrm{Aut}_F(i(E)^{\perp}).$$

4-4. ***Example.*** Let K be an étale quadratic F-algebra and consider the Jordan algebra $J_3(K)$ of 3×3 Hermitian matrices with entries in K. Let $E = F \times F \times F$ be the subalgebra of $J_3(K)$ consisting of diagonal matrices. Then C consists of matrices

$$v = \begin{pmatrix} 0 & \bar{z}_3 & z_2 \\ z_3 & 0 & \bar{z}_1 \\ \bar{z}_2 & z_1 & 0 \end{pmatrix}.$$

Thus $C = K \times K \times K$, and one checks that

$$Q(z_1, z_2, z_3) = (z_1\bar{z}_1, z_2\bar{z}_2, z_3\bar{z}_3) \quad \text{and} \quad \beta(z_1, z_2, z_3) = (\bar{z}_2\bar{z}_3, \bar{z}_3\bar{z}_1, \bar{z}_1\bar{z}_2).$$

The algebra C is the distinguished point in the fiber of $([F^3],[K])$, in the sense of Proposition 3.12. The automorphism group of C is given by

$$\mathrm{Aut}_F(C,Q,\beta) = (K^1 \times K^1 \times K^1)^0 \rtimes (\mathbb{Z}/2\mathbb{Z} \times S_3),$$

where K^1 denotes the torus of norm-1 elements in K and $(K^1 \times K^1 \times K^1)^0$ denotes the subgroup of triples (t_1,t_2,t_3) such that $t_1t_2t_3 = 1$.

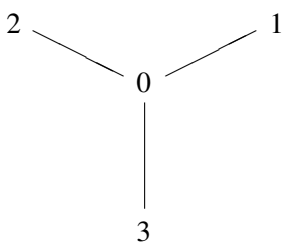
4-5. ***The quadratic algebra associated to $i : E \to J$.*** If an E-twisted composition algebra C corresponds to a conjugacy class of embeddings $i : E \longrightarrow J$, then we may ask how the quadratic algebra K_C associated to C can be described in terms of $i : E \longrightarrow J$. In this case, $C = E^{\perp}$ is an E-twisted composition algebra, and so $C = E \otimes K_C$ for a quadratic algebra K_C as in Proposition 3.12. On the other hand, we know that J is associated to a pair (B_{K_J},τ), where B_{K_J} is a central simple algebra over an étale quadratic F-algebra K_J and τ is an involution of the second kind. Now, Examples (5) and (6) on page 527 in [Knus et al. 1998] show that

$$[K_C]\cdot[K_E]\cdot[K_J] = 1 \in H^1(F,\mathbb{Z}/2\mathbb{Z}) = F^\times/F^{\times 2}.$$

5. Quasisplit groups of type D_4

In this section, we shall introduce the E-twisted Bhargava's cube by way of the quasisplit groups of type D_4.

5-1. ***Root system.*** Let Ψ be a root system of type D_4 and $\Pi = \{\alpha_0,\alpha_1,\alpha_2,\alpha_3\}$ a set of simple roots such that the corresponding Dynkin diagram is



The group of diagram automorphisms $\mathrm{Aut}(\Pi)$ is identified with S_3, the group of permutations of $\{1,2,3\}$. We denote the highest root by $\beta_0 = \alpha_1+\alpha_2+\alpha_3+2\alpha_0$.

5-2. ***Quasisplit groups of type D_4.*** Let G be a split, simply connected Chevalley group of type D_4. We fix a maximal torus T contained in a Borel subgroup B defined over F. The group G is then generated by root groups $U_\alpha \cong \mathbb{G}_a$, where $\alpha \in \Psi$. Steinberg showed that one can pick the isomorphisms $x_\alpha : \mathbb{G}_a \to U_\alpha$ such that

$$[x_\alpha(u), x_{\alpha'}(u')] = x_{\alpha+\alpha'}(\pm uu')$$

whenever $\alpha+\alpha'$ is a root. Fixing such a system of isomorphisms fixes an épinglage (or pinning) for G. As Kac noted, a choice of signs corresponds to an orientation of the Dynkin diagram. Since one can pick an orientation of the Dynkin diagram which is invariant under $\mathrm{Aut}(\Pi)$, the group of automorphisms of Π can be lifted to a group of automorphisms of G. Thus, we have a semidirect product

$$\widetilde{G} = G \rtimes \mathrm{Aut}(\Pi) = G \rtimes S_3,$$

where the action of S_3 permutes the root subgroups U_α and the isomorphisms x_α.

Since the outer automorphism group S_3 of G is also the automorphism group of the split étale cubic F-algebra F^3, we see that every cubic étale algebra E defines a simply connected quasisplit form G_E of G, whose outer automorphism group is the finite group scheme S_E. Thus,

$$\widetilde{G}_E = G_E \rtimes S_E$$

is a form of $\widetilde{G}$, and it comes equipped with a pair $B_E \supset T_E$, consisting of a Borel subgroup B_E containing a maximal torus T_E, both defined over F, as well as a Chevalley–Steinberg system of épinglage relative to this pair.

5-3. ***G_2 root system.*** The subgroup of G_E fixed pointwise by S_E is isomorphic to the split exceptional group of type G_2.

Observe that $B = G_2 \cap B_E$ is a Borel subgroup of G_2 and $T = T_E \cap G_2$ is a maximal split torus of G_2. Via the adjoint action of T on G_E, we obtain the root system Ψ_{G_2} of G_2, so that

$$\Psi_{G_2} = \Psi|_T.$$

We denote the short simple root of this G_2 root system by α and the long simple root by β. Then

$$\beta = \alpha_0|_T \quad \text{and} \quad \alpha = \alpha_1|_T = \alpha_2|_T = \alpha_3|_T.$$

Thus, the short root spaces have dimension 3, whereas the long root spaces have dimension 1. For each root $\gamma \in \Psi_{G_2}$, the associated root subgroup U_γ is defined over F and the Chevalley–Steinberg system of épinglage gives isomorphisms

$$U_\gamma \cong \begin{cases} \mathrm{Res}_{E/F}\, \mathbb{G}_a & \text{if } \gamma \text{ is short,} \\ \mathbb{G}_a & \text{if } \gamma \text{ is long.} \end{cases}$$

5-4. ***The parabolic subgroup P_E.*** The G_2 root system gives rise to two parabolic subgroups of G_E. One of these is a maximal parabolic $P_E = M_E N_E$ known as the Heisenberg parabolic. Its unipotent radical N_E is a Heisenberg group with center $Z_E = U_{\beta_0}$; see Section 2 in [Gan et al. 2002]. Moreover,

$$N_E/Z_E = U_\beta \times U_{\beta+\alpha} \times U_{\beta+2\alpha} \times U_{\beta+3\alpha} \cong \mathbb{G}_a \times \mathrm{Res}_{E/F}\, \mathbb{G}_a \times \mathrm{Res}_{E/F}\, \mathbb{G}_a \times \mathbb{G}_a$$

and

$$\widetilde{M}_E = M_E \rtimes S_E \cong \mathrm{GL}_2(E)^0 \rtimes S_E,$$

where

$$\mathrm{GL}_2(E)^0 = \{g \in \mathrm{GL}_2(E) : \det(g) \in F^\times\}.$$

We shall fix the isomorphism $M_E \rtimes S_E \cong \mathrm{GL}_2(E)^0 \rtimes S_E$ as follows. We first consider the case when $E = F^3$ is split. The pinning gives us an identification

$$M_{\mathrm{der}}(F) \cong \mathrm{SL}_2(F)^3$$

such that

$$\alpha_1^\vee(t) = \left(\begin{pmatrix} t & \\ & t^{-1} \end{pmatrix}, 1, 1\right) \in \mathrm{SL}_2(F)^3,$$

while $\alpha_2^\vee(t)$ and $\alpha_3^\vee(t)$ are defined analogously by cyclically permuting the entries of $\alpha_1^\vee(t)$. We extend this identification to $M(F)$ by

$$\alpha_0^\vee(t) = \left(\begin{pmatrix} 1 & \\ & t \end{pmatrix}, \begin{pmatrix} 1 & \\ & t \end{pmatrix}, \begin{pmatrix} 1 & \\ & t \end{pmatrix}\right) \in (\mathrm{GL}_2(F)^3)^0.$$

Note that, under the identification,

$$\beta_0^\vee(t) = \left(\begin{pmatrix} t & \\ & t \end{pmatrix}, \begin{pmatrix} t & \\ & t \end{pmatrix}, \begin{pmatrix} t & \\ & t \end{pmatrix}\right) \in (\mathrm{GL}_2(F)^3)^0.$$

Finally, since the pinning is invariant under the action of $\mathrm{Aut}(\Pi) \cong S_3$, it follows that

$$\widetilde{M}(F) \cong (\mathrm{GL}_2(F)^3)^0 \rtimes S_3,$$

where S_3 acts on $(\mathrm{GL}_2(F)^3)^0$ by permuting the components. For general E, one obtains the desired isomorphism by a Galois descent argument.

6. Bhargava's cube

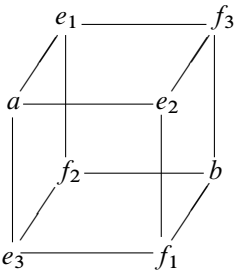
In this section, we shall examine the split case, where the pinning for G gives a $\mathbb{Z}$-structure on N/Z; for more details see Section 4 in [Gan et al. 2002].

6-1. ***Bhargava's cube.*** Let V_2 be the standard representation of SL_2. Recall that we have identified M_{der} with SL_2^3 and M with $(\mathrm{GL}_2^3)^0$. Under this identification, the representation of M_{der} on N/Z is isomorphic to the representation of SL_2^3 on $V = V_2 \otimes V_2 \otimes V_2$. Since $\beta_0^\vee(t)$ acts on N/Z as multiplication by t, it follows that $(\mathrm{GL}_2^3)^0$ acts on V by the standard action *twisted* by $\det^{-1}$. The group $S_3 \cong \mathrm{Aut}(\Pi)$ acts on $V_2 \otimes V_2 \otimes V_2$ by permuting the three factors.

Since V is an absolutely irreducible SL_2^3-module, the isomorphism of N/Z and V is unique up to a nonzero scalar. Since $\beta_0^\vee(t)$ acts on N/Z as multiplication by t, the bijection between M-orbits on N/Z and M-orbits on V does not depend

on the choice of the isomorphism. If we demand that the isomorphism preserves $\mathbb{Z}$-structures, i.e., that it gives an isomorphism of $(N/Z)(\mathbb{Z})$ and $\mathbb{Z}^2 \otimes \mathbb{Z}^2 \otimes \mathbb{Z}^2$, then it is unique up to a sign.

An element $v \in V(F)$ is represented by a cube



where $a, \ldots, b \in F$ and the vertices correspond to the standard basis in $F^2 \otimes F^2 \otimes F^2$. More precisely, we fix this correspondence so that

$$\begin{pmatrix}1\\0\end{pmatrix} \otimes \begin{pmatrix}1\\0\end{pmatrix} \otimes \begin{pmatrix}1\\0\end{pmatrix} \quad \text{and} \quad \begin{pmatrix}0\\1\end{pmatrix} \otimes \begin{pmatrix}0\\1\end{pmatrix} \otimes \begin{pmatrix}0\\1\end{pmatrix}$$

correspond to the vertices marked with letters a and b, respectively. We note that elementary matrices in $\mathrm{SL}_2(F)^3$ act on the space of cubes by the following three types of "row-column" operations on cubes:

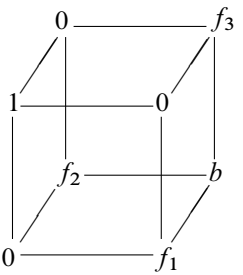
- add or subtract the front face from the rear face of the cube, and vice-versa;
- add or subtract the top face from the bottom face of the cube, and vice-versa;
- add or subtract the right face from the left face of the cube, and vice-versa.

The group $S_3 \cong \mathrm{Aut}(\Pi)$ acts as the group of symmetries of the cube fixing the two vertices marked a and b. We shall often write the cube as a quadruple

$$(a, e, f, b),$$

where $e = (e_1, e_2, e_3)$ and $f = (f_1, f_2, f_3) \in F^3$.

6-2. ***Reduced and distinguished cube.*** It is not hard to see that, using the action of $M(F)$, every cube can be transformed into a cube of the form $(1, 0, f, b)$:



We shall call such a cube a *reduced cube*. In particular, we call the cube $v_0 = (1,0,0,-1)$ the *distinguished cube*.

6-3. ***Stabilizer of distinguished cube.*** Let $\mathrm{Stab}_{\boldsymbol{M}}(v_0)$ and $\mathrm{Stab}_{\widetilde{\boldsymbol{M}}}(v_0)$ be the respective stabilizers in M and $\widetilde{M}$ of the distinguished cube $v_0 \in V$. Since $\mathrm{Aut}(\Pi)$ stabilizes v_0, the group $\mathrm{Stab}_{\widetilde{\boldsymbol{M}}}(v_0)$ is a semidirect product of $\mathrm{Stab}_{\boldsymbol{M}}(v_0)$ and $\mathrm{Aut}(\Pi)$. We shall now compute $\mathrm{Stab}_{\boldsymbol{M}}(v_0)$. Let $g = (g_1, g_2, g_3) \in M(F)$, where

$$g_i = \begin{pmatrix} a_i & b_i \\ c_i & d_i \end{pmatrix}.$$

Since

$$v_0 = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \otimes \begin{pmatrix} 1 \\ 0 \end{pmatrix} \otimes \begin{pmatrix} 1 \\ 0 \end{pmatrix} - \begin{pmatrix} 0 \\ 1 \end{pmatrix} \otimes \begin{pmatrix} 0 \\ 1 \end{pmatrix} \otimes \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

and

$$g \cdot v_0 = \det(g)^{-1} \cdot \begin{pmatrix} a_1 \\ c_1 \end{pmatrix} \otimes \begin{pmatrix} a_2 \\ c_2 \end{pmatrix} \otimes \begin{pmatrix} a_3 \\ c_3 \end{pmatrix} - \det(g)^{-1} \cdot \begin{pmatrix} b_1 \\ d_1 \end{pmatrix} \otimes \begin{pmatrix} b_2 \\ d_2 \end{pmatrix} \otimes \begin{pmatrix} b_3 \\ d_3 \end{pmatrix},$$

$g \cdot v_0 = v_0$ if and only if eight equations hold. Six of these equations are homogeneous. They are

$$a_1 c_2 a_3 = b_1 d_2 b_3, \quad a_1 c_2 c_3 = b_1 d_2 d_3,$$

with the additional four obtained by cyclically permuting the indices. If we multiply the first equation by d_3, the second by b_3, and subtract them, then

$$0 = a_1 c_2 a_3 d_3 - a_1 c_2 c_3 b_3 = a_1 c_2 (a_3 d_3 - c_3 b_3).$$

Since $a_3 d_3 - c_3 b_3 \neq 0$, we have $a_1 c_2 = 0$. A similar manipulation of these two equations gives $b_1 d_2 = 0$. By permuting the indices, we have $a_i c_j = b_i d_j = 0$ for all $i \neq j$. This implies that all the g_i are simultaneously diagonal or off-diagonal. Now it is easy to see that the remaining two equations imply that $\mathrm{Stab}_{\boldsymbol{M}}(v_0)$ has two connected components, and the identity component consists of $g = (g_1, g_2, g_3)$ such that g_i are diagonal matrices, $a_i d_i = 1$, and $a_1 a_2 a_3 = 1$. The other component of $\mathrm{Stab}_{\boldsymbol{M}}(v_0)$ contains an element $w = (w_1, w_2, w_3)$ of order 2, where

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

We now have a complete description of $\mathrm{Stab}_{\boldsymbol{M}}(v_0)$ (and of $\mathrm{Stab}_{\widetilde{\boldsymbol{M}}}(v_0)$):

$$\mathrm{Stab}_{\boldsymbol{M}}(v_0) \cong \{(a_1, a_2, a_3) \in \mathbb{G}_m^3 : a_1 a_2 a_3 = 1\} \rtimes \mathbb{Z}/2\mathbb{Z} \cong \mathbb{G}_m^2 \rtimes \mathbb{Z}/2\mathbb{Z}.$$

In particular, we have shown:

Proposition 6.1. *The stabilizer* $\mathrm{Stab}_{\widetilde{M}}(v_0)$ *in* $\widetilde{M}$ *of the distinguished cube* $v_0 = (1,0,0,-1)$ *is isomorphic to the group of* F*-automorphisms of the split twisted composition algebra* C_0*. Indeed, they give identical subgroups of* $(\mathrm{GL}_2(F)^3)^0 \rtimes S_3$*, where we fix the isomorphism* $M(F) \cong (\mathrm{GL}_2(F)^3)^0$ *as above.*

6-4. ***Three quadratic forms.*** One key observation in [Bhargava 2004a] is that one can slice the cube (given in the picture in Section 6-1) in three different ways, giving three pairs of matrices:

$$A_1 = \begin{pmatrix} a & e_2 \\ e_3 & f_1 \end{pmatrix}, \quad B_1 = \begin{pmatrix} e_1 & f_3 \\ f_2 & b \end{pmatrix},$$
$$A_2 = \begin{pmatrix} a & e_3 \\ e_1 & f_2 \end{pmatrix}, \quad B_2 = \begin{pmatrix} e_2 & f_1 \\ f_3 & b \end{pmatrix},$$
$$A_3 = \begin{pmatrix} a & e_1 \\ e_2 & f_3 \end{pmatrix}, \quad B_3 = \begin{pmatrix} e_3 & f_2 \\ f_1 & b \end{pmatrix}.$$

Note that the pairs (A_2, B_2) and (A_3, B_3) are obtained by rotating the pair (A_1, B_1) about the axis passing through a and b. For each pair (A_i, B_i), Bhargava defines a quadratic binary form by

$$Q_i = -\det(A_i x + B_i y).$$

Proposition 6.2. *Given a cube* v*, the three forms* Q_1*,* Q_2 *and* Q_3 *have the same discriminant* $\Delta = \Delta(v)$*.*

Proof. We may assume the cube is reduced. Now an easy computation show that the three forms are

$$\begin{cases} Q_1(x,y) = -f_1 x^2 - bxy + f_2 f_3 y^2, \\ Q_2(x,y) = -f_2 x^2 - bxy + f_3 f_1 y^2, \\ Q_3(x,y) = -f_3 x^2 - bxy + f_1 f_2 y^2. \end{cases}$$

These forms have the same discriminant $\Delta = b^2 + 4 f_1 f_2 f_3$. □

6-5. ***Quartic invariant.*** To every cube $v \in V$, the discriminant $\Delta(v)$ described in the previous proposition is a homogeneous quartic polynomial in v, which is invariant under the action of $\mathrm{SL}_2(F)^3$. This describes the quartic invariant of the prehomogeneous vector space V. An explicit computation gives the formula

$$\Delta = a^2 b^2 - 2ab(e_1 f_1 + e_2 f_2 + e_3 f_3) + e_1^2 f_1^2 + e_2^2 f_2^2 + e_3^2 f_3^2 + 4a f_1 f_2 f_3 + 4b e_1 e_2 e_3 - 2(e_1 e_2 f_1 f_2 + e_2 e_3 f_2 f_3 + e_3 e_1 f_3 f_1).$$

If v is reduced, then this simplifies to $\Delta(v) = b^2 + 4 f_1 f_2 f_3$. It is easy to check that for $g \in M$, one has

$$\Delta(g \cdot v) = \det(g)^2 \cdot \Delta(v).$$

Thus, we see that Δ gives a well-defined map

$$\Delta : \{\text{generic } \widetilde{M}(F)\text{-orbits on } V(F)\} \longrightarrow F^\times/F^{\times 2} = \{\text{étale quadratic } F\text{-algebras}\}.$$

7. E-twisted Bhargava cube

Now we can extend the discussion of the previous section to the case of general E, where $V_E = F \oplus E \oplus E \oplus F$ and $\widetilde{M}_E = \mathrm{GL}_2(E)^0 \rtimes S_E$, via a Galois descent using a cocycle in the class of

$$[E] \in H^1(F, \mathrm{Aut}(\Pi)) = H^1(F, S_3).$$

A cube is a quadruple $v = (a, e, f, b)$, where $e, f \in E$. As in the split case, we shall call cubes of the form $v = (1, 0, f, b)$ reduced, and the vector $v_{0,E} = (1, 0, 0, -1)$ the E-distinguished cube.

7-1. ***Quartic invariant.*** By Galois descent, we see that the basic polynomial invariant Δ_E is given by

$$\Delta_E(a, e, f, b) = a^2b^2 - 2ab\,\mathrm{Tr}_{E/F}(ef) + \mathrm{Tr}_{E/F}(e^2f^2) + 4aN_{E/F}(f) + 4bN_{E/F}(e) - 2\,\mathrm{Tr}_{E/F}(e^\# f^\#).$$

If v is reduced, then this simplifies to

$$\Delta_E(1, 0, f, b) = b^2 + 4 \cdot N_{E/F}(f).$$

7-2. ***Group action.*** It is useful to note the action of certain elements of $\mathrm{GL}_2(E)^0$ on V_E. Specifically, $\sigma \in S_E$ acts by $\sigma(a, e, f, b) = (a, \sigma(e), \sigma(f), b)$. Moreover, the diagonal torus elements

$$t_{\alpha,\beta} = \begin{pmatrix} \alpha & 0 \\ 0 & \beta \end{pmatrix} \quad \text{with } \alpha\beta \in F^\times$$

act by

$$(a, e, f, b) \mapsto (\alpha^\#\beta^{-1}a, \alpha^\#\alpha^{-1}e, \beta^\#\beta^{-1}f, \beta^\#\alpha^{-1}b).$$

It is easy to check that

$$\Delta_E(t_{\alpha,\beta} \cdot v) = (\alpha\beta)^2 \cdot \Delta_E(v).$$

Since the actions of $\mathrm{SL}_2(E)$ and S_E preserve Δ_E, we see that

$$\Delta_E(g \cdot v) = (\det g)^2 \cdot \Delta_E(v),$$

so that Δ_E induces a map

$$\{\widetilde{M}_E\text{-orbits on } V_E\} \longrightarrow F^\times/F^{\times 2} = \{\text{étale quadratic algebras}\}.$$

In addition, the standard Weyl group element

$$w = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \in \mathrm{GL}_2(E)^0$$

acts by

$$w : (a, e, f, b) \mapsto (-b, -f, -e, -a).$$

7-3. ***Stabilizer of distinguished E-cube.*** We can readily determine the stabilizer of the E-distinguished cube . Namely, under the action described in Section 7-2, it is easy to see that the subgroup

$$E^1 = \left\{ \begin{pmatrix} \alpha & \\ & \alpha^{-1} \end{pmatrix} : \alpha \in E^1 \right\} \subset \mathrm{SL}_2(E)$$

fixes the E-distinguished cube $v_{0,E}$. So does the Weyl group element w. Thus, we see that

$$\mathrm{Stab}_{M_E}(v_{0,E}) \cong E^1 \rtimes \mathbb{Z}/2\mathbb{Z} \quad \text{and} \quad \mathrm{Stab}_{\widetilde{M}_E}(v_{0,E}) = E^1 \rtimes (\mathbb{Z}/2\mathbb{Z} \times S_E).$$

In particular, we have shown:

Proposition 7.1. *The stabilizer* $\mathrm{Stab}_{\widetilde{M}_E}(v_{0,E})$ *in* $\widetilde{M}_E$ *of the* E*-distinguished cube* $(1, 0, 0, -1)$ *is isomorphic to the group of* F*-automorphisms of the twisted composition algebra* C_E *introduced in* Section 3-4. *Indeed, they are identical as subgroups of* $\mathrm{GL}_2(E)^0 \rtimes S_E(F)$ *under the fixed isomorphism* $M_E(F) \cong \mathrm{GL}_2(E)^0$.

8. Generic orbits

We come now to the main result of this paper: the determination of the generic $\widetilde{M}_E(F)$-orbits in $V_E(F)$.

8-1. ***A commutative diagram.*** We have the following commutative diagram

$$\begin{array}{ccc} H^1(F, \mathrm{Stab}_{\widetilde{M}}(v_0)) & \longrightarrow & H^1(F, \widetilde{M}) \\ \downarrow & & \downarrow \\ H^1(F, \mathrm{Aut}_F(C_0, Q_0, \beta_0)) & \longrightarrow & H^1(F, S_3) \end{array} \tag{8.1}$$

We make several observations about this commutative diagram.

Lemma 8.2. (i) *The first vertical arrow is bijective.*
(ii) *The second vertical arrow is bijective.*
(iii) *The horizontal arrows are surjective.*

Proof. (i) This follows by Proposition 6.1.

(ii) Let the second vertical arrow be denoted by ψ. Since $\widetilde{M}$ is a semidirect product of M and S_3, the map ψ is surjective. For injectivity, we shall use the exact sequence of pointed sets

$$1 \longrightarrow H^1(F, M) \longrightarrow H^1(F, \widetilde{M}) \longrightarrow H^1(F, S_3) \longrightarrow 1.$$

Let $c \in H^1(F, S_3)$ and let E be the étale cubic algebra corresponding to c. Then M_E is the twist of M by c. In order to prove that $\psi^{-1}(c)$ consists of one element, it suffices to show that $H^1(F, M_E)$ is trivial, by the twisting argument on page 50 of [Serre 2002]. We have an exact sequence of algebraic groups

$$1 \longrightarrow M_{E,\mathrm{der}} \longrightarrow M_E \longrightarrow \mathrm{GL}_1 \longrightarrow 1,$$

where $M_{E,\mathrm{der}} \cong \mathrm{Res}_{E/F} \mathrm{SL}_2$. By Hilbert's theorem 90, $H^1(F, \mathrm{GL}_1)$ is trivial. Since

$$H^1(F, \mathrm{Res}_{E/F} \mathrm{SL}_2) = H^1(E, \mathrm{SL}_2) = 0$$

(see [Serre 2002, p. 130]), it follows that $H^1(F, M_E)$ is trivial.

(iii) This follows because $\mathrm{Stab}_{\widetilde{M}}(v_0) = \mathrm{Stab}_M(v_0) \rtimes \mathrm{Aut}(\Pi)$, hence

$$H^1(F, \mathrm{Stab}_{\widetilde{M}}(v_0)) \to H^1(F, \mathrm{Aut}(\Pi))$$

has a natural splitting. □

8-2. ***Determination of orbits.*** We can now determine the generic $\widetilde{M}_E(F)$-orbits on $V_E(F)$.

Theorem 8.3. *Fix an étale cubic F-algebra E.*

(i) *The generic $\widetilde{M}_E(F)$-orbits on $V_E(F)$ are in bijective correspondence with the set of F-isomorphism classes of E-twisted composition algebras over F, with the orbit of $v_{0,E} = (1, 0, 0, 1)$ corresponding to the twisted composition algebra C_E introduced in Section 3-4.*

(ii) *The generic $M_E(F)$-orbits on $V_E(F)$ are in bijective correspondence with the set of E-isomorphism classes of E-twisted composition algebras over F.*

(iii) *There is a commutative diagram*

$$\begin{array}{ccc} \{E\text{-twisted composition algebras}\} & \longrightarrow & \{\text{étale quadratic } F\text{-algebras}\} \\ \downarrow & & \downarrow \\ \{\text{generic } \widetilde{M}_E\text{-orbits on } V_E\} & \longrightarrow & F^\times / F^{\times 2} \end{array}$$

where the bottom arrow is the map induced by Δ_E (see Section 7-2).

Proof. (i) Given a cohomology class $[E] \in H^1(F, S_3)$ corresponding to an étale cubic F-algebra, we consider the fibers of the two horizontal arrows in the commutative diagram (8.1) over $[E]$. Since the map $\mathrm{Stab}_{\widetilde{M}}(v_0) \longrightarrow S_3$ splits, the fiber of the second horizontal arrow has a distinguished element which corresponds to the twisted composition algebra C_E. Similarly, the fiber over $[E]$ of the first horizontal arrow has a distinguished point which corresponds to the orbit of $v_{0,E} = (1, 0, 0, -1)$. Moreover, these two distinguished point correspond under the first vertical arrow.

By the twisting argument [Serre 2002, p. 50] we see that both fibers in question are naturally identified with

$$\mathrm{Ker}(H^1(F, \mathrm{Stab}_{\widetilde{M}_E}(v_{0,E})) \longrightarrow H^1(F, \widetilde{M}_E)).$$

Thus, the fiber of the first horizontal map over $[E]$ are the generic $\widetilde{M}_E$-orbits in V_E, while the fibers of the second map are F-isomorphism classes of E-twisted composition algebras.

(ii) The bijection follows because both sets are in natural bijection with the set $H^1(F, \mathrm{Stab}_{M_E}(v_{0,E}) = H^1(F, \mathrm{Aut}_E(C_E))$.

(iii) Suppose an E-twisted composition algebra is represented by a cocycle

$$(a_\sigma) \in H^1(F, \mathrm{Stab}_{M_E}(v_{0,E})).$$

Then the associated étale quadratic F-algebra K corresponds to the group homomorphism

$$\eta_K : \mathrm{Gal}(\bar{F}/F) \longrightarrow \mathrm{Stab}_{M_E}(v_{0,E})(\bar{F}) \longrightarrow \mathbb{Z}/2\mathbb{Z}$$

given by $\sigma \mapsto a_\sigma \mapsto \pi(a_\sigma)$, where $\pi : \mathrm{Stab}_{M_E}(v_{0,E}) \to \mathbb{Z}/2\mathbb{Z}$ is the natural projection. In fact, regarding $\mathrm{Stab}_{M_E}(v_{0,E}) \subseteq M_E$ as described in Section 7-3, we see that the map π is simply given by the determinant map on $M_E = \mathrm{GL}_2(E)^0$.

On the other hand, the cocycle splits in $H^1(F, M_E) = 0$, so that we may write

$$a_\sigma = g^{-1} \cdot \sigma(g) \quad \text{for some } g \in M_E(\bar{F}).$$

Then the $\widetilde{M}_E$-orbit associated to (a_σ) is that of $g \cdot v_{0,E}$. Now, we have

$$\Delta_E(g \cdot v_{0,E}) = \det(g)^2 \cdot \Delta_E(v_{0,E}) = \det(g)^2$$

and

$$\eta_K(\sigma) = \det(a_\sigma) = \det(g)^{-1} \cdot \sigma(\det(g))$$

for any $\sigma \in \mathrm{Gal}(\bar{F}/F)$. This shows that $\det(g)$ is a trace-zero element in K, so that K is represented by the square class of $\det(g)^2 \in F^\times$, as desired. □

In particular, we have established Theorem 1.1. However, the bijection between the generic $\widetilde{M}_E(F)$-orbits on $V_E(F)$ and the F-isomorphism classes of twisted composition algebras is obtained by a Galois cohomological argument, which is

quite formal and not at all explicit. For applications, it is necessary to have an explicit description of the bijection. We shall arrive at such an explicit description in the following sections.

9. Reinterpreting Bhargava

In this section, revisiting the case when $E = F^3$ is split, we shall reinterpret [Bhargava 2004a] in the framework of twisted composition algebras, leading to an explicit recipe for the bijection in Theorem 8.3.

9-1. ***Bhargava's result.*** We first review briefly Bhargava's results and, following him, we shall work over $\mathbb{Z}$. Note that we have an action of the group $\mathrm{SL}_2(\mathbb{Z})^3$ on the set of integer-valued cubes, by the "row-column" operations described in Section 6-1.

In order to state the main result of Bhargava, we need a couple of definitions. Fix a discriminant Δ. Let $K = \mathbb{Q}(\sqrt{\Delta})$ and R the unique order of discriminant Δ. A module M is a full lattice in K. In particular, it is a $\mathbb{Z}$-module of rank 2. We shall write $M = \{u, v\}$ if u and v span M. For example,

$$R = \left\{1, \frac{\Delta + \sqrt{\Delta}}{2}\right\}.$$

By fixing this basis of R, we have also fixed a preferred orientation of bases of modules. An oriented module is a pair (M, ϵ), where ϵ is a sign. If $M = \{u, v\}$, then M becomes an oriented module (M, ϵ), where $\epsilon = 1$ if and only if the orientation of $\{u, v\}$ is preferred. The norm of an oriented module (M, ϵ) is $N(M) = \epsilon \cdot [R : M]$.

Then:

- A triple of oriented modules (M_1, M_2, M_3), with R as the multiplier ring, is said to be *colinear* if there exists $\delta \in K^\times$ such that the product of the three oriented modules is a principal oriented ideal $((\delta), \epsilon)$, where $\epsilon = \mathrm{sign}(N(\delta))$, i.e., $M_1 M_2 M_3 = (\delta)$, as ordinary modules, and $N(M_1)N(M_2)N(M_3) = N(\delta)$.
- A cube is *projective* of discriminant Δ if the three associated forms are primitive and have discriminant Δ.
- Two triples of oriented modules (M_1, M_2, M_3) and (M_1', M_2', M_3') are equivalent if there exist μ_1, μ_2, μ_3 in $K^\times$ with $M_i' = \mu_i M_i$ and $\epsilon_i' = \mathrm{sign}(N(\mu_i))\epsilon_i$ for $i = 1, 2, 3$.

Then, Bhargava [2004a] showed:

Theorem 9.1. *There is a bijection, to be described in the proof, between the equivalence classes of oriented colinear triples of discriminant Δ and the $SL_2(\mathbb{Z})^3$-equivalence classes of projective cubes of discriminant Δ.*

Sketch of proof. Let v be a projective cube. Again, without any loss of generality we can assume that the cube is reduced and that the numbers f_1, f_2 and f_3 are nonzero. Define three modules by

$$M_1 = \left\{1, \frac{b-\sqrt{\Delta}}{2f_1}\right\}, \quad M_2 = \left\{1, \frac{b-\sqrt{\Delta}}{2f_2}\right\} \quad \text{and} \quad M_3 = \left\{1, \frac{b-\sqrt{\Delta}}{2f_3}\right\}.$$

The norms of the three modules are $-1/f_1, -1/f_2$ and $-1/f_3$, respectively, if we take the given bases to be proper. For δ, we shall take

$$\delta = -\frac{2}{b+\sqrt{\Delta}},$$

which has the correct norm $-1/(f_1 f_2 f_3)$.

The modules M_i, with given oriented bases, correspond to the quadratic forms Q_i. More precisely, if

$$z_i = x_i + y_i \frac{b-\sqrt{\Delta}}{2f_i} \in M_i,$$

then

$$-f_i N(z_i) = Q_i(x_i, y_i) = -f_i x_i^2 - b x_i y_i + f_i^{\#} y_i^2,$$

where $f^{\#} = (f_2 f_3, f_3 f_1, f_1 f_2)$. □

9-2. ***Integral twisted composition algebras.*** We can now give a reinterpretation of Bhargava's results, in particular of Bhargava's triples (M_1, M_2, M_3), in the framework of twisted composition algebras. Assume the notation from the previous subsection, so that $M_1 M_2 M_3 = (\delta)$. Set

$$C = M_1 \oplus M_2 \oplus M_3.$$

We shall define a pair of tensors (Q, β) on C as follows:

- Define a quadratic form $Q : C \to \mathbb{Z} \times \mathbb{Z} \times \mathbb{Z}$ by

$$Q(z_1, z_2, z_3) = (-f_1 N(z_1), -f_2 N(z_2), -f_3 N(z_3)) = -f \cdot (N(z_1), N(z_2), N(z_3)).$$

- Define a quadratic map $\beta : C \to C$ by

$$\beta(z_1, z_2, z_3) = \delta(f_2 f_3 \bar{z}_2 \bar{z}_3, f_3 f_1 \bar{z}_3 \bar{z}_1, f_1 f_2 \bar{z}_1 \bar{z}_2) = \delta \cdot f^{\#} \cdot (\bar{z}_1, \bar{z}_2, \bar{z}_3)^{\#}.$$

The relations $M_1 M_2 M_3 = (\delta)$ and $M \bar{M} = N(M)$ imply that β is well defined. Moreover, using $N(\delta) = -1/(f_1 f_2 f_3)$, one checks that

$$Q(\beta(z_1, z_2, z_3)) = Q(z_1, z_2, z_3)^{\#}$$

and

$$N_C(z_1, z_2, z_3) = \mathrm{Tr}\left(\frac{z_1 z_2 z_3}{\delta}\right).$$

Thus the triple (C, Q, β) is a twisted composition algebra over $\mathbb{Z}$.

In terms of the coordinates (x_i, y_i) given by

$$z_i = x_i + y_i \frac{b - \sqrt{\Delta}}{2f_i},$$

we have seen in the sketch proof of Theorem 9.1 that

$$Q_i(z_i) = -f_i N(z_i) = -f_i x_i^2 - b x_i y_i + f_i^{\#} y_i^2.$$

We shall now do the same for β. Write $\beta(z_1, z_2, z_3) = (z_1', z_2', z_3')$, and let (x_i', y_i') be the coordinates of z_i'. A short calculation shows that

$$x_1' = -\begin{pmatrix} x_3 & y_3 \end{pmatrix} \begin{pmatrix} 0 & f_3 \\ f_2 & b \end{pmatrix} \begin{pmatrix} x_2 \\ y_2 \end{pmatrix} \quad \text{and} \quad y_1' = \begin{pmatrix} x_3 & y_3 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & f_1 \end{pmatrix} \begin{pmatrix} x_2 \\ y_2 \end{pmatrix},$$

while the expressions for (x_2', y_2') and (x_3, y_3) are obtained by cyclically permuting the indices.

There are two important observations to be made here:

- Firstly, these formulas make sense for any triple (f_1, f_2, f_3) and any b, i.e., the f_i can be zero. The axioms of twisted composition algebra are satisfied for formal reasons. For example, if $(f_1, f_2, f_3) = (0, 0, 0)$ and $b = -1$, we get the split algebra C_0.
- Secondly, the two matrices are two opposite faces of the cube. This gives a hint how to directly associate a composition algebra to any cube in general (i.e., not just a reduced cube).

9-3. ***From cubes to twisted composition algebras.*** The above discussion suggests an explicit recipe for associating a twisted composition algebra over $F \times F \times F$ to any cube $v \in V(F)$.

Let $C = F^2 \times F^2 \times F^2$. An element $z \in C$ is a triple (z_1, z_2, z_3) of column vectors $z_i = \binom{x_i}{y_i}$. Slice a cube into three pairs of 2×2-matrices (A_i, B_i), as before, and let

$$Q_i(z_i) = -\det(A_i x_i + B_i y_i).$$

Then, we set:

- $Q : C \to F \times F \times F$, defined by

$$Q(z_1, z_2, z_3) = (Q_1(z_1), Q_2(z_2), Q_3(z_3)).$$

- $\beta : C \to C$, defined by

$$\beta(z_1, z_2, z_3) = (z_1', z_2', z_3'),$$

where $z_i' = \binom{x_i'}{y_i'}$,

$$x_1' = -z_3^\top B_1 z_2, \quad x_2' = -z_1^\top B_2 z_3, \quad x_3' = -z_2^\top B_3 z_1$$

and

$$y_1' = z_3^\top A_1 z_2, \quad y_2' = z_1^\top A_2 z_3, \quad y_3' = z_2^\top A_3 z_1.$$

Thus, starting from a cube v, we have defined a pair of tensors (Q, β) on $C = F^2 \times F^2 \times F^2$. Let

$$\tilde{\phi} : V(F) \longrightarrow \{\text{tensors } (Q, \beta) \text{ on } C\}$$

be the resulting map. We may express this map using the coordinates (a, e, f, b) of a cube. A short calculation gives

$$\begin{aligned} Q(x, y) &= (e^\# - af)x^2 + (-ab - 2ef + \mathrm{Tr}(ef))xy + (f^\# - be)y^2, \\ \beta(x, y) &= (-ex^\# - by^\# - (fx) \times y, ax^\# + fy^\# + (ey) \times x). \end{aligned}$$

In the next section, we shall study the properties of the map $\tilde{\phi}$; for example, we shall show that a (Q, β) in the image of $\tilde{\phi}$ does define a twisted composition algebra on C.

10. Explicit parametrization

Using the results of the previous section, we can now give an explicit description of the bijection between $\tilde{M}_E(F)$-orbits of nondegenerate cubes and F-isomorphism classes of E-twisted composition algebras.

10-1. ***Definition of $\tilde{\phi}$.*** Let us write $C = E \cdot e_1 \oplus E \cdot e_2$. Motivated by the case where $E = F^3$, studied in the previous section, we define the map

$$\tilde{\phi} : V_E(F) \longrightarrow \{\text{tensors } (Q, \beta) \text{ on } C\}$$

using the coordinates $v = (a, e, f, b)$ of a cube, with $a, b \in F$ and $e, f \in E$, by

$$\begin{aligned} Q(x, y) &= (e^\# - af)x^2 + (-ab - 2ef + \mathrm{Tr}(ef))xy + (f^\# - be)y^2, \\ \beta(x, y) &= (-ex^\# - by^\# - (fx) \times y, ax^\# + fy^\# + (ey) \times x). \end{aligned} \tag{10.1}$$

In particular, for a reduced cube $(1, 0, f, b)$, one has

$$\begin{aligned} Q(x, y) &= -fx^2 - bxy + f^\# y^2, \\ \beta(x, y) &= (-by^\# - (fx) \times y, x^\# + fy^\#). \end{aligned} \tag{10.2}$$

Thus, the image of the distinguished cube $v_{E,0} = (1, 0, 0, -1)$ is the algebra C_E. Observe also that one has

$$\beta(1, 0) = (0, 1) \quad \text{and} \quad \beta(0, 1) = (-b, f). \tag{10.3}$$

Thus, the standard basis $\{e_1, e_2\}$ is a reduced basis with respect to (Q, β), in the sense of Section 3-6.

Proposition 10.4. (i) *The map $\tilde{\phi}$ is injective.*

(ii) *For $g \in \mathrm{GL}_2(E)^0$ and $\sigma \in S_E(F)$, one has*

$$\tilde{\phi}(g \cdot v) = {}^t g^{-1} \cdot \tilde{\phi}(v) \quad \text{and} \quad \tilde{\phi}(\sigma \cdot v) = \sigma \cdot \tilde{\phi}(v)$$

for any $v \in V_E(F)$.

Thus, the map $\tilde{\phi}$ is $\mathrm{GL}_2(E)^0 \rtimes S_E$-equivariant, with respect to the outer automorphism $(g, \sigma) \mapsto ({}^t g^{-1}, \sigma)$ of $\mathrm{GL}_2(E)^0 \rtimes S_E$, and where the action of $\mathrm{GL}_2(E)^0 \rtimes S_E$ on the set of (Q, β) is given as in Section 3-3.

(iii) *For any nondegenerate cube v, $\tilde{\phi}(v) = (Q, \beta)$ defines a twisted composition algebra on C.*

Proof. (i) If $\tilde{\phi}(a, e, f, b) = (Q, \beta)$, then

$$\beta(1, 0) = (-e, a) \quad \text{and} \quad \beta(0, 1) = (-b, f).$$

Hence the cube (a, e, f, b) is uniquely determined by β.

(ii) We can verify this equivariance property over $\overline{F}$; thus we only need to check it for $E = F^3$. For the central element $(t, t, t) \in \mathrm{GL}_2(E)^0$ or the element $\sigma \in S_E$, the desired equivariance property is clear. Thus, it remains to verify it for elementary matrices such as

$$g = (E_u, 1, 1) = \left(\begin{pmatrix} 1 & u \\ 0 & 1 \end{pmatrix}, 1, 1 \right) \in (\mathrm{GL}_2(F) \times \mathrm{GL}_2(F) \times \mathrm{GL}_2(F))^0.$$

Now, if the cube v has a pair of faces (A_1, B_1), then the corresponding pair for $g \cdot v$ is

$$(A_1', B_1') = (A_1 + uB_1, B_1).$$

Slicing the cube in the other two ways, we obtain

$$(A_2', B_2') = (E_u A_2, E_u B_2) \quad \text{and} \quad (A_3', B_3') = (A_3 E_u^t, B_3 E_u^t).$$

Hence, if $\tilde{\phi}(g \cdot v) = (Q', \beta')$, then β' is given on $(z_1, z_2, z_3) \in F^2 \times F^2 \times F^2$ by

$$\begin{pmatrix} x_1' & x_2' & x_3' \\ y_1' & y_2' & y_3' \end{pmatrix} = \begin{pmatrix} -z_3^t B_1 z_2 & -z_1^t E_u B_2 z_3 & -z_2^t B_3 E_u^t z_1 \\ z_3^t (A_1 + uB_1) z_2 & z_1^t E_u A_2 z_3 & z_2^t A_3 E_u^t z_1 \end{pmatrix}.$$

On the other hand, ${}^tg^{-1}$ acts on β by precomposing by $({}^tg^{-1})^{-1} = g^t$, and post-composing by ${}^tg^{-1}$:

$$\begin{aligned}
{}^tg^{-1}\cdot\beta(g^t(z_1,z_2,z_3)) &= {}^tg^{-1}\cdot\beta(E_u^t z_1, z_2, z_3)\\
&= {}^tg^{-1}\cdot\begin{pmatrix} -z_3^tB_1z_2 & -z_1^tE_uB_2z_3 & -z_2^tB_3E_u^tz_1\\ z_3^tA_1z_2 & z_1^tE_uA_2z_3 & z_2^tA_3E_u^tz_1\end{pmatrix}\\
&= \begin{pmatrix} -z_3^tB_1z_2 & -z_1^tE_uB_2z_3 & -z_2^tB_3E_u^tz_1\\ z_3^t(A_1+uB_1)z_2 & z_1^tE_uA_2z_3 & z_2^tA_3E_u^tz_1\end{pmatrix}\\
&= \beta'(z_1,z_2,z_3).
\end{aligned}$$

(iii) Again, we may work over $\overline{F}$, and hence we may assume that $E = F^3$. If v is a reduced cube, we have seen in Section 9-2 that (Q,β) defines a twisted composition algebra on E^2. Since every $\widetilde{M}(F)$-orbit contains a reduced cube, the result follows by (ii). □

The occurrence of the outer automorphism $g \mapsto {}^tg^{-1}$ is natural here. Indeed, assume that $E = F^3$ and regard $\mathrm{GL}_2(F)$ as $\mathrm{GL}(V)$ for a 2-dimensional F-vector space V. Then the quadratic map β is an element of $(V^*)^{\oplus 3}\otimes_F (V^*)^{\oplus 3}\otimes_F V^{\oplus 3}$, whereas its associated cube is an element in $V\otimes_F V\otimes_F V\otimes_F \det(V)^{-1}$. Thus scaling a cube by $t\in F^\times$ corresponds to scaling β by t^{-1}.

10-2. ***Reduced cubes and bases.*** To describe the image of $\tilde{\phi}$, we examine the case of reduced cubes more carefully.

Proposition 10.5. *Suppose that the pair (Q,β) defines a twisted composition algebra structure on E^2 such that the standard basis $\{e_1,e_2\}$ is reduced (i.e., $\beta(e_1)=e_2$). Then (Q,β) is the image under $\tilde{\phi}$ of the reduced cube*

$$v = (1,0,-Q(e_1),-N_{Q,\beta}(e_1)).$$

Moreover, $\Delta_E(v) = \Delta_{Q,\beta}(e_1)$ (where the Δ on the left side is the quasi-invariant form on the space V_E of cubes while the one on the right is defined in Proposition 3.5).

Proof. We need to show that Q and β are uniquely determined by $f = -Q(e_1)$ and $b = -N_{Q,\beta}(e_1)$. Since

$$Q(e_2) = Q(\beta(e_1)) = f^{\#} \quad\text{and}\quad b_Q(e_1,e_2) = b_Q(e_1,\beta(e_1)) = N(e_1) = -b,$$

we see that Q is uniquely determined. Then $\beta(xe_1+ye_2)$ is uniquely determined by (3.4) in Lemma 3.2. Finally, observe that

$$\Delta_E(v) = \Delta_{Q,\beta}(e_1) = b^2 + 4N_E(f).$$ □

10-3. ***Good bases.*** We call a basis of C a *good basis* if it is in the $\mathrm{Aut}_E(C)^0 \cong \mathrm{GL}_2(E)^0$-orbit of a reduced basis. By Proposition 3.5(iv), this notion is independent of the choice of the reduced basis. Similarly, since the action of S_E preserves the set of reduced cubes, the notion of good bases does not depend on whether one uses $\mathrm{Aut}_E(C)^0$ or $\mathrm{Aut}_F(E,C)^0 \cong \mathrm{GL}_2(E)^0 \rtimes S_E$.

As a consequence of the proposition, we have:

Corollary 10.6. (i) *The map $\tilde{\phi}$ gives a bijection between the set of reduced (nondegenerate) cubes and the set of (Q,β) on E^2 such that the standard basis $\{e_1,e_2\}$ is reduced.*

(ii) *The image of $\tilde{\phi}$ consists precisely of those (Q,β) such that the standard basis $\{e_1,e_2\}$ of $C = E^2$ is a good basis for (Q,β).*

The definition we have given for a good basis $\{e_1,e_2\}$ may not seem very satisfactory. It would have been more satisfactory if one defines a good basis for (C,Q,β) using purely the forms (Q,β) rather than using the action of $\mathrm{Aut}_E(C)^0$. Indeed, it will not be easy to check that a given basis is good by our definition. However, by Corollary 10.6, one knows *a posteriori* that a basis $\{e_1,e_2\}$ is good for (C,Q,β) if and only if $\beta(xe_1+ye_2)$ has the form given in (10.1) with $a,b \in F$. We would have taken this as a definition, but it would have seemed completely unmotivated without the results of this section!

10-4. ***A commutative diagram.*** As a summary of the above discussion, we have the following refinement and explication of Theorem 8.3:

Theorem 10.7. (i) *The bijective map $\tilde{\phi}$ descends to give a commutative diagram*

$$\begin{array}{ccc}
V_E(F)^0 = \{c \in V_E(F) : \Delta_E(c) \neq 0\} & \longrightarrow & \tilde{M}_E(F)\text{-orbits on } V_E(F)^0 \\
\downarrow{\scriptstyle \tilde{\phi}} & & \downarrow{\scriptstyle \phi} \\
\{\text{pairs } (Q,\beta) \text{ on } E^2\text{: standard basis is good}\} & \longrightarrow & \{\mathrm{GL}_2(E)^0 \rtimes S_E(F)\text{-orbits of } (Q,\beta)\} \\
\downarrow & & \downarrow \\
\{F\text{-isomorphism classes of pairs } (C,b)\} & \longrightarrow & \{F\text{-isomorphism classes of } C\}
\end{array}$$

where all vertical arrows are $\mathrm{GL}_2(E)^0 \rtimes S_E(F)$-equivariant bijections and, in the last row, C denotes an E-twisted composition algebra and b denotes a good basis of C. Moreover the action of $\mathrm{GL}_2(E)^0 \rtimes S_E(F)$ on a pair $(C,\{e_1,e_2\})$ is given as follows: $g \in \mathrm{GL}_2(E)^0$ sends the pair to $(C,\{e_1',e_2'\})$, where

$$\begin{pmatrix} e_1' \\ e_2' \end{pmatrix} = g \cdot \begin{pmatrix} e_1 \\ e_2 \end{pmatrix},$$

whereas $\sigma \in S_E$ sends the pair to $(E \otimes_{E,\sigma} C, \{e_1,e_2\})$.

(ii) *The bijection ϕ agrees with the one given in Theorem 8.3.*

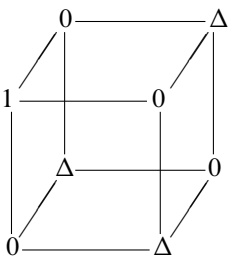
Proof. (i) Our discussion above already shows that $\tilde{\phi}$ is bijective and descends to give the map ϕ. It remains to show that the induced map ϕ is bijective. The surjectivity of ϕ follows from Proposition 3.5(iii) and (iv) and Corollary 10.6(i). The injectivity of ϕ follows from Proposition 10.4(i) and (ii). We leave the bijection and the equivariance of the lower half of the diagram to the reader.

(ii) The map $\tilde{\phi}$ sends the distinguished cube $v_{E,0} = (1, 0, 0, -1)$ to the pair (Q_0, β_0) on E^2, which defines the algebra C_E. Moreover, $\tilde{\phi}$ is equivariant with respect to the automorphism $g \mapsto {}^t g^{-1}$ of $\mathrm{GL}_2(E)$, which preserves the subgroup $\mathrm{Stab}_{\mathrm{GL}_2(E)^0}(v_{E,0}) = \mathrm{Aut}_E(Q_0, \beta_0) \subset \mathrm{GL}_2(E)^0$. Finally, since $\tilde{\phi}$ is algebraic, it is Galois-equivariant with respect to base field extension. All these imply that we have a commutative diagram

$$\begin{array}{ccc} \{\mathrm{GL}_2(E)^0\text{-orbits on } V_E(F)^0\} & \longrightarrow & H^1(F, \mathrm{Stab}_{\mathrm{GL}_2(E)^0}(v_{E,0})) \\ \downarrow{\scriptstyle \phi} & & \downarrow{\scriptstyle g \mapsto {}^t g^{-1}} \\ \{E\text{-isomorphism classes of twisted composition algebras}\} & \longrightarrow & H^1(F, \mathrm{Aut}_E(C_E)) \end{array}$$

Since the map $g \mapsto {}^t g^{-1}$ of $\mathrm{Stab}_{\mathrm{GL}_2(E)^0}(v_{E,0}) = \mathrm{Aut}_E(Q_0, \beta_0)$ is given by conjugation by the element $w \in \mathrm{Aut}_E(Q_0, \beta_0)(F)$, we see that the induced map on H^1 is trivial. Hence ϕ agrees with the bijection given in Theorem 8.3 by a Galois cohomological argument. □

10-5. ***An example.*** As an example, assume that $K = F(\sqrt{\Delta})$ and consider the composition algebra given by the example in Section 4-4. (This is the distinguished point in the fiber of $([F^3], [K])$.) Then $v = (\sqrt{\Delta}, \sqrt{\Delta}, \sqrt{\Delta})$ and $\beta(v) = (\Delta, \Delta, \Delta)$ is a reduced basis. The corresponding reduced cube is



10-6. ***Relation with Tits' construction.*** If $f \in E^\times$, we can relate the construction of $\tilde{\phi}$ attached to the reduced cube $(1, 0, -f, b)$ to Proposition 3.12. Identify $E \oplus E$ with $E \otimes K$ using the E-linear isomorphism given by

$$(x, y) \mapsto x \otimes 1 + \frac{y}{f} \otimes \frac{b - \sqrt{\Delta}}{2} = x + y\frac{b - \sqrt{\Delta}}{2f},$$

where, in the last expression, we omitted tensor product signs for readability. Then Q can be written as

$$Q\left(x+y\frac{b-\sqrt{\Delta}}{2f}\right)=-f\cdot N_{E\otimes K/E}\left(x+y\frac{b-\sqrt{\Delta}}{2f}\right)$$

and β as

$$\beta\left(x+y\frac{b-\sqrt{\Delta}}{2f}\right)=-\frac{2}{b+\sqrt{\Delta}}\cdot f^{\#}\cdot\left(x+y\frac{b+\sqrt{\Delta}}{2f}\right)^{\#}.$$

Indeed, if $E=F^3$, these formulae are exactly the same as those in Section 9-2 . Let

$$e=-f\quad\text{and}\quad \nu=-\frac{b+\sqrt{\Delta}}{2}.$$

Using $e^{-1}\cdot\bar{\nu}=\nu^{-1}\cdot e^{\#}$ (since $N_{E/F}(e)=N_{K/F}(\nu)$) this composition algebra is the algebra attached to the pair (e,ν), as in Proposition 3.12. Conversely, a composition algebra given by a pair (e,ν), as in Proposition 3.12, arises from the cube $(1,0,-e,b)$ where $b=-\operatorname{Tr}_{K/F}(\nu)$.

11. Exceptional Hilbert 90

Assume that E is an étale cubic F-algebra with corresponding étale quadratic discriminant algebra K_E, and let K be an étale quadratic F-algebra. Recall that

$$T_{E,K}=\{x\in E\otimes_F K: N_{E/F}(x)=1=N_{K/F}(x)\}.$$

Suppose, for example, that $[K_E]=[K]=1$, so E is a Galois extension, and $T_{E,K}$ is the group of norm-one elements in $E^\times$. Let σ be a generator of the Galois group $G_{E/F}$. Then Hilbert's theorem 90 states that the map

$$x\mapsto\sigma(x)/\sigma^2(x)$$

induces an isomorphism of $E^\times/F^\times$ and $T_{E,K}(F)$. Our goal in this section is to generalize this statement to all tori $T_{E,K}$, thus obtaining an exceptional Hilbert's theorem 90. As an application, we give an alternative description of $H^1(F,T_{E,K})$.

11-1. ***The torus $T_{E,K}$.*** We first describe the torus $T_{E,K}$ by Galois descent. Over $\bar{F}$, we have the identification

$$T_{E,K}(\bar{F})=\{(\underline{a},\underline{b})\in\bar{F}^3\otimes\bar{F}^2: a_ib_i=1\text{ for all }i\text{ and }a_1a_2a_3=1\}.$$

The F-structure is given by the twist of the Galois action on coordinates by the cocycle

$$\rho_E\times\rho_K:\operatorname{Gal}(\bar{F}/F)\longrightarrow\operatorname{Aut}(\bar{F}^3)\times\operatorname{Aut}(\bar{F}^2)\cong S_3\times\mathbb{Z}/2\mathbb{Z},$$

where S_3 and $\mathbb{Z}/2\mathbb{Z}$ act on $\mathbb{Z}^3$ and $\mathbb{Z}^2$, respectively, by permuting the coordinates.

We may describe $T_{E,K}$ using its cocharacter lattice X. We have

$$X = \{(\underline{a}, -\underline{a}) \in \mathbb{Z}^3 \otimes \mathbb{Z}^2 : a_1 + a_2 + a_3 = 0\},$$

equipped with the Galois action given by

$$\rho_E \otimes \rho_K : \mathrm{Gal}(\overline{F}/F) \longrightarrow S_3 \times \mathbb{Z}/2\mathbb{Z}.$$

11-2. ***The torus $T'_{E,K}$.*** Now we introduce another torus $T'_{E,K}$ over F. Let K_J be the étale quadratic F-algebra such that $[K_J] \cdot [K] \cdot [K_E] = 1$ in $H^1(F, \mathbb{Z}/2\mathbb{Z})$. We define the tori

$$\widetilde{T}'_{E,K} = \{x \in E \otimes_F K_J : N_{E \otimes K_J/E}(x) \in F^\times\}$$

and

$$T'_{E,K} = \widetilde{T}'_{E,K}/K_J^\times,$$

where the last quotient is taken in the sense of algebraic groups. If $J = B^\tau$, where B is a degree-3 central simple K_J-algebra with an involution τ of the second kind, and $E \to J$ is an F-embedding or, equivalently, $E \otimes_F K_J \to B$ is a K_J-embedding such that τ pulls back to the nontrivial element of $\mathrm{Aut}(E \otimes_F K_J/E)$, then $T'_{E,K}$ acts naturally as a group of automorphisms of the embedding $E \to J$.

We may again describe these tori by Galois descent. Over $\overline{F}$, we may identify

$$\widetilde{T}'_{E,K}(\overline{F}) = \{(\underline{a}, \underline{b}) \in (\overline{F}^\times)^3 \otimes (\overline{F}^\times)^2 : a_1 b_1 = a_2 b_2 = a_3 b_3\},$$

and $T'_{E,K}(\overline{F})$ is the quotient of this by the subgroup consisting of the elements $(a \cdot \underline{1}, b \cdot \underline{1})$. The action of $\mathrm{Gal}(\overline{F}/F)$ which gives the F-structure of $\widetilde{T}'_{E,K}$ is then described as follows. Let $\rho_E : \mathrm{Gal}(\overline{F}/F) \longrightarrow S_3$ be the cocycle associated to E, so that $\mathrm{sign} \circ \rho_E : \mathrm{Gal}(\overline{F}/F) \longrightarrow \mathbb{Z}/2\mathbb{Z}$ is the homomorphism associated to K_E. On the other hand, we let ρ_K be the homomorphism associated to K, so that

$$(\mathrm{sign} \circ \rho_E) \cdot \rho_K : \mathrm{Gal}(\overline{F}/F) \longrightarrow \mathbb{Z}/2\mathbb{Z}$$

is the homomorphism associated to K_J. Now the action of $\mathrm{Gal}(\overline{F}/F)$ on $\overline{F}^3 \otimes \overline{F}^2$ is the twist of the action on coordinates by the cocycle

$$\rho_E \times (\mathrm{sign} \circ \rho_E) \cdot \rho_K : \mathrm{Gal}(\overline{F}/F) \longrightarrow S_3 \times \mathbb{Z}/2\mathbb{Z}.$$

As before, we may describe the tori $\widetilde{T}'_{E,K}$ and $T'_{E,K}$ by their cocharacter lattice. The cocharacter lattice $\widetilde{Y}$ of $\widetilde{T}'_{E,K}$ is given by

$$\widetilde{Y} = \{(\underline{a}, \underline{b}) \in \mathbb{Z}^3 \otimes \mathbb{Z}^2 : a_1 + b_1 = a_2 + b_2 = a_3 + b_3\},$$

equipped with the Galois action given by

$$\rho_E \times (\mathrm{sign} \circ \rho_E) \cdot \rho_K : \mathrm{Gal}(\overline{F}/F) \longrightarrow S_3 \times \mathbb{Z}/2\mathbb{Z}.$$

This contains the Galois-stable sublattice

$$Z = (1,1,1) \otimes \mathbb{Z}^2,$$

so that $Y = \widetilde{Y}/Z$ is the cocharacter lattice of $T'_{E,K}$.

11-3. ***A homomorphism.*** We are going to construct a morphism of tori from $\widetilde{T}'_{E,K}$ to $T_{E,K}$. We shall first define this morphism over $\overline{F}$ and then shows that it descends to F.

Now we may define a morphism over $\overline{F}$,

$$f : \widetilde{T}'_{E,K}(\overline{F}) \longrightarrow T_{E,K}(\overline{F}),$$

by

$$f : \begin{pmatrix} a_1 & a_2 & a_3 \\ b_1 & b_2 & b_3 \end{pmatrix} \mapsto \begin{pmatrix} a_2/a_3 & a_3/a_1 & a_1/a_2 \\ b_2/b_3 & b_3/b_1 & b_1/b_2 \end{pmatrix}.$$

It is easy to see that this defines an $\overline{F}$-isomorphism of tori

$$f : T'_{E,K}(\overline{F}) \cong T_{E,K}(\overline{F}).$$

Moreover, if $\sigma \in S_e(\overline{F}) = S_3$ is the cyclic permutation

$$(a_1, a_2, a_3) \mapsto (a_2, a_3, a_1),$$

then the map f is given by

$$f(x) = \sigma(x)/\sigma^2(x).$$

Now the morphism f induces a map

$$f_* : \widetilde{Y} \longrightarrow X,$$

given by

$$\begin{pmatrix} a_1 & a_2 & a_3 \\ b_1 & b_2 & b_3 \end{pmatrix} \mapsto \begin{pmatrix} a_2 - a_3 & a_3 - a_1 & a_1 - a_2 \\ b_2 - b_3 & b_3 - b_1 & b_1 - b_2 \end{pmatrix}.$$

This induces an isomorphism of $\mathbb{Z}$-modules $Y \cong X$.

11-4. ***Exceptional Hilbert 90.*** The main result of this section is:

Theorem 11.1. *The isomorphism $f : T'_{E,K} \times_F \overline{F} \longrightarrow T_{E,K} \times_F \overline{F}$ is defined over F, and thus gives an isomorphism of tori*

$$T'_{E,K} \longrightarrow T_{E,K}$$

given by

$$x \mapsto \sigma(x)/\sigma^2(x).$$

Proof. It remains to prove that f is defined over F. For this, we may work at the level of cocharacter lattices, and we need to show that f_* is Galois-equivariant. For this, regard $\mathbb{Z}^3 \otimes \mathbb{Z}^2$ as a $S_3 \times \mathbb{Z}/2\mathbb{Z}$-module with the permutation of the coordinates in $\mathbb{Z}^3$ and $\mathbb{Z}^2$. Then observe that f_* is not equivariant with respect to $S_3 \times \mathbb{Z}/2\mathbb{Z}$. On the other hand, we have the automorphism of $S_3 \times \mathbb{Z}/2\mathbb{Z}$ given by

$$(g, h) \mapsto (g, \mathrm{sign}(g) \cdot h)$$

If we twist the $S_3 \times \mathbb{Z}/2\mathbb{Z}$-module structure on the domain of f_* by this automorphism, then f_* is easily seen to be equivariant. Together with our description of the $\mathrm{Gal}(\overline{F}/F)$-actions on the domain and codomain of f_*, the desired $\mathrm{Gal}(\overline{F}/F)$-equivariance follows. □

11-5. ***Cohomology of $T_{E,K}$.*** As an application of the exceptional Hilbert 90, we may give an alternative description of the cohomology group $H^1(F, T_{E,K})$, which classifies twisted composition algebras with fixed invariants (E, K) up to $E \otimes_F K$-linear isomorphisms.

In order to state our results, we need additional notation. For every quadratic extension K_J of F, let $\mathrm{Res}^1_{K_J/F} \mathbb{G}_m$ be the 1-dimensional torus defined by the short exact sequence of algebraic tori

$$1 \longrightarrow \mathrm{Res}^1_{K_J/F} \mathbb{G}_m \longrightarrow \mathrm{Res}_{K_J/F} \mathbb{G}_m \longrightarrow \mathbb{G}_m \longrightarrow 1.$$

By the classical Hilbert theorem 90, the associated long exact sequence gives the exact sequence

$$1 \longrightarrow H^2(F, \mathrm{Res}^1_{K_J/F} \mathbb{G}_m) \longrightarrow H^2(K_J, \mathbb{G}_m) \longrightarrow H^2(F, \mathbb{G}_m),$$

where the last map is the corestriction. By a theorem of Albert, Riehm, and Scharlau [Knus et al. 1998, Theorem 3.1], the kernel of the corestriction map is the set of Brauer equivalence classes of central simple algebras over K_J that admit an involution of the second kind, and so we can view $H^2(F, \mathrm{Res}^1_{K_J/F} \mathbb{G}_m)$ as the set of Brauer equivalence classes of such algebras.

Proposition 11.2. *Let K_J be an étale quadratic algebra with $[K_J] \cdot [K] \cdot [K_E] = 1$, and set $M = E \otimes_F K_J$.*

(i) *If K_J is a field, then we have an exact sequence*

$$1 \longrightarrow E^\times / F^\times N_{M/E}(M^\times) \longrightarrow H^1(F, T_{E,K}) \longrightarrow H^2(F, \mathrm{Res}^1_{K_J/F} \mathbb{G}_m) \longrightarrow H^2(E, \mathrm{Res}^1_{M/E} \mathbb{G}_m).$$

The image of $H^1(F, T_{E,K})$ consists of those central simple algebras over K_J which contain M as a K_J-subalgebra and which admit an involution of the second kind fixing E (or equivalently, restricting to the nontrivial automorphism of M over E).

(ii) *If $K_J = F^2$, then we have a simplified version of the above sequence:*

$$H^1(F, T_{E,K}) = \mathrm{Ker}(H^2(F, \mathbb{G}_m) \longrightarrow H^2(E, \mathbb{G}_m)).$$

Proof. (i) By the exceptional Hilbert theorem 90, we have a short exact sequence of algebraic tori

$$1 \longrightarrow \mathrm{Res}^1_{K_J/F}\, \mathbb{G}_m \longrightarrow \mathrm{Res}_{E/F}\, \mathrm{Res}^1_{M/E}\, \mathbb{G}_m \longrightarrow T_{E,K} \longrightarrow 1.$$

Now, (i) follows from the associated long exact sequence, using

$$H^1(F, \mathrm{Res}^1_{K_J/F}\, \mathbb{G}_m) = F^\times / N_{K_J/F} K_J^\times,$$
$$H^1(E, \mathrm{Res}^1_{M/E}\, \mathbb{G}_m) = E^\times / N_{M/E} M^\times.$$

(ii) One argues as above, except that since $K_J = F^2$, we have

$$1 \longrightarrow \mathbb{G}_m \longrightarrow \mathrm{Res}_{E/F}\, \mathbb{G}_m \longrightarrow T_{E,K} \longrightarrow 1.$$

Thus the long exact sequence gives

$$1 \longrightarrow H^1(F, T_{E,K}) \longrightarrow H^2(F, \mathbb{G}_m) \longrightarrow H^2(E, \mathbb{G}_m). \qquad \square$$

11-6. ***Interpretation.*** The above description of $H^1(F, T_{E,K})$ fits beautifully with the correspondence between E-twisted composition algebras and conjugacy classes of embeddings $E \hookrightarrow J$, where J is a Freudenthal–Jordan algebra of dimension 9.

More precisely, Proposition 11.2 exhibits $H^1(F, T_{E,K})$ as the set of isomorphism classes of triples (B, τ, i), where:

- B is a central simple K_J-algebra of degree 3.
- τ is an involution of the second kind on B.
- $i : E \longrightarrow B^\tau$ is an F-algebra embedding, or equivalently a K_J-algebra embedding $i : M = E \otimes_F K_J \longrightarrow B$ such that τ pulls back to the nontrivial element of $\mathrm{Aut}(M/E)$.

The map $\pi : H^1(F, T_{E,K}) \to H^2(F, \mathrm{Res}^1_{K_J/F}\, \mathbb{G}_m)$ sends (B, τ, i) to B. For a fixed

$$[B] \in \mathrm{Ker}(H^2(F, \mathrm{Res}^1_{K_J/F}\, \mathbb{G}_m) \longrightarrow H^2(E, \mathrm{Res}^1_{M/E}\, \mathbb{G}_m)),$$

so that B contains $M = E \otimes_F K_J$ as an K_J-subalgebra, the fiber of π over $[B]$ is the set of $\mathrm{Aut}_{K_J}(B)$-conjugacy classes of pairs (τ, i). The Skolem–Noether theorem says that any two embeddings $M \hookrightarrow B$ are conjugate, and on fixing an embedding $i : M \hookrightarrow B$, the fiber of π over $[B]$ is then the set of $\mathrm{Aut}_{K_J}(B, i)$-conjugacy classes of involutions of the second kind on B which restricts to the nontrivial automorphism of M over E. Therefore, the exact sequence in Proposition 11.2(i) says that the set of such $\mathrm{Aut}_{K_J}(B, i)$-conjugacy classes of involutions is identified with $E^\times / F^\times N_{M/E}(M^\times)$. One has a natural map on the fiber $\pi^{-1}([B])$ sending a

$\mathrm{Aut}_{K_J}(B,i)$-conjugacy class of involutions to its $\mathrm{Aut}_{K_J}(B)$-conjugacy class. This is the surjective map described in Corollary 19.31 in [Knus et al. 1998].

On the other hand, the map sending the triple (B,τ,i) to the pair (B,τ) is the natural map

$$H^1(F,T_{E,K}) \longrightarrow H^1(F,PGU_3^{K_J})$$

induced by the map $T_{E,K} \hookrightarrow PU_3^{K_J}$ where $PGU_3^{K_J}$ is the identity component of the automorphism group of the Freuthendal–Jordan algebra associated to the distinguished twisted composition algebra with invariants (E,K).

12. Local fields

In this section, we specialize and explicate the main result in the case of local fields.

12-1. ***Local fields.*** Let F be a local field, E an étale cubic F-algebra, and K_E the corresponding discriminant algebra. Let K be an étale quadratic F-algebra. We consider

$$\widetilde{\Omega}_{E,K} = \{\text{generic } \widetilde{M}_E\text{-orbits on } V_E \text{ with associated quadratic algebra } K\},$$

$$\Omega_{E,K} = \{\text{generic } M_E\text{-orbits on } V_E \text{ with associated quadratic algebra } K\}.$$

We have seen that $\widetilde{\Omega}_{E,K}$ has a distinguished element: this is the distinguished point of $H^1(T_{E,K})$ which is fixed by $S_E(F)\times\mathbb{Z}/2\mathbb{Z}$. Moreover, by Galois cohomological arguments,

$$\widetilde{\Omega}_{E,K} = H^1(F,T_{E,K})/S_E(F)\times\mathbb{Z}/2\mathbb{Z} \quad \text{and} \quad \Omega_{E,K} = H^1(F,T_{E,K})/\mathbb{Z}/2\mathbb{Z}.$$

We would like to explicate the sets $\widetilde{\Omega}_{E,K}$ and $\Omega_{E,K}$.

12-2. ***Cohomology of tori.*** Recall that in (3.13), we have shown

$$H^1(F,T_{E,K}) = (E^\times\times K^\times)^0/\operatorname{Im}(L^\times),$$

where $L = E\otimes_F K$,

$$(E^\times\times K^\times)^0 = \{(e,v)\in E^\times\times K^\times : N_{E/F}(e) = N_{K/F}(v)\}$$

and the map from $L^\times$ to $(E^\times\times K^\times)^0$ is given by

$$a \mapsto (N_{L/E}(a), N_{L/K}(a)).$$

This description of $H^1(F,T_{E,K})$ is natural but may not be so explicit. When F is a local field, we can further explicate this description.

Since the case when E or K is not a field is quite simple, we consider the case when E and K are both fields. In that case, the norm map induces an isomorphism

$$E^\times/N_{L/E}(L^\times) \longrightarrow F^\times/N_{K/F}(K^\times) \cong \mathbb{Z}/2\mathbb{Z},$$

so that any $(e, \nu) \in (E^\times \times K^\times)^0$ has $e = N_{L/E}(a)$ for some $a \in L^\times$. Hence any element in $H^1(F, T_{E,K})$ is represented by $(1, \nu)$ for $\nu \in K^1 = \{\nu \in K^\times : N_{K/F}(\nu) = 1\}$. We thus deduce that, with $L^1 = \{a \in L^\times : N_{L/E}(a) = 1\}$,

$$H^1(F, T_{E,K}) = K^1/N_{L/K}(L^1) \cong K^\times/F^\times N_{L/K}(L^\times),$$

where the last isomorphism is induced by the usual Hilbert theorem 90. Using this last expression, we easily see that

$$H^1(F, T_{E,K}) = \begin{cases} 1 & \text{if } K \neq K_E, \\ \mathbb{Z}/3\mathbb{Z} & \text{if } K = K_E. \end{cases}$$

Exchanging the roles of E and K in the above argument, one also has

$$H^1(F, T_{E,K}) = E^1/N_{L/E}(L_1),$$

where now $L_1 = \{a \in L^\times : N_{L/K}(a) = 1\}$. If E/F is Galois (and K is a field), it follows by the usual Hilbert theorem 90 that

$$H^1(F, T_{E,K}) = E^1/N_{L/E}(L_1) \cong E^\times/F^\times N_{L/E}(E^\times) = 1,$$

thus partially recovering the result of the last section.

Alternatively, we could use Proposition 11.2 to compute $H^1(F, T_{E,K})$. If K_J is a field, then the only central simple K_J-algebra which admits an involution of the second kind is the split algebra $M_3(K_J)$. Thus we deduce from Proposition 11.2(i) that

$$H^1(F, T_{E,K}) \cong E^\times/F^\times N_{M/E}(M^\times),$$

where $M = E \otimes_F K_J$. On the other hand, if K_J is split, Proposition 11.2(ii) gives

$$H^1(F, T_{E,K}) \cong \mathrm{Ker}(H^2(F, \mathbb{G}_m) \longrightarrow H^2(E, \mathbb{G}_m)),$$

which is $\mathbb{Z}/3\mathbb{Z}$ when E is a field.

12-3. ***Fibers.*** With the various computations of $H^1(F, T_{E,K})$ given above, it is not difficult to show the following proposition which determines $|\widetilde{\Omega}_{E,K}|$ and $|\Omega_{E,K}|$.

Proposition 12.1. *We have*

E	K	$T_{E,K}$	$H^1(F, T_{E,K})$	$\lvert\widetilde{\Omega}_{E,K}\rvert$	$\lvert\Omega_{E,K}\rvert$
$F \times K_E$	$K = K_E$	$K^\times$	1	1	1
$F \times K_E$, K_E *a field*	*field* $\neq K_E$	$(K \otimes K_E)^\times/K_E^\times$	$\mathbb{Z}/2\mathbb{Z}$	2	2
$F \times K_E$, K_E *a field*	$F \times F$	$K_E^\times$	1	1	1
F^3	*field*	$K^\times/F^\times \times K^\times/F^\times$	$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$	2	4
field	$K = K_E$	$E^\times/F^\times$	$\mathbb{Z}/3\mathbb{Z}$	2	2
field	$K \neq K_E$		1	1	1

Here, the difference in the last two columns reflects the fact that $S_E(F)$ acts trivially on $H^1(F, T_{E,K})$ except when $E = F^3$ and K is a field.

12-4. ***Embeddings into J.*** The main theorem says that the elements of $\Omega_{E,K}$ are in bijection with the conjugacy classes of embeddings

$$E \hookrightarrow J,$$

where J is a 9-dimensional Freudenthal–Jordan algebra associated to a pair (B, τ), where B is a central simple algebra over the quadratic algebra K_J and τ is an involution of the second kind on B. We now describe the elements of $\Omega_{E,K}$ in terms of such embeddings.

- When F is p-adic and $K = K_E$, so that $K_J = F \times F$ is split, then

$$(B, \tau) = (D \times D^{\mathrm{op}}, \mathrm{sw})$$

where D is a central simple F-algebra of degree 3 and sw denotes the involution which switches the two factors. Thus, there are two possible J in this case: the Jordan algebra J^+ attached to $M_3(F)$ or the Jordan algebra J^- attached to a cubic division F-algebra (and its opposite). In either case, the set of embeddings $E \longrightarrow J$ is either empty or a single conjugacy class, and it is empty if and only if $J = J^-$ and E is not a field. Thus when $K = K_E$, we have

$$\widetilde{\Omega}_{E,K} = \Omega_{E,K} = \begin{cases} \{E \to J^+, E \to J^-\} & \text{if } E \text{ is a field;} \\ \{E \to J^+\} & \text{if } E \text{ is not a field.} \end{cases}$$

On the other hand, when K_J is a field, then $B = M_3(K_J)$, and there is a unique isomorphism class of involution of the second kind on B, given by conjugation by a nondegenerate hermitian matrix, so that J is isomorphic to the Jordan algebra of 3×3-Hermitian matrices with entries in K_J. According to the proposition, there is a unique conjugacy class of embedding $E \hookrightarrow J$ unless $E = F \times K_E$ and K is a field with $K \neq K_E$. In the exceptional case, there are two subalgebras $E \subset J$ up to conjugacy. We may write down the 2 non-F-isomorphic twisted composition algebras corresponding to these. The twisted composition algebra can be realized on

$$E \otimes_F K = K \times (K_E \otimes K).$$

Let $\{1, \alpha\}$ denote representatives of $F^\times / NK^\times$. Then the two twisted composition algebras correspond to

$$(e, \nu) = ((1, 1), 1) \quad \text{or} \quad ((1, \alpha), \alpha) \in (F \times K_E)^\times \times K^\times.$$

We see that these two twisted composition algebras are not isomorphic because they are not isomorphic as quadratic spaces over E (even allowing for twisting by $S_E(F)$).

Further, when $E = F^3$, there are in fact four conjugacy classes of embeddings $E \hookrightarrow J$. This corresponds to the fact that the F-isomorphism class of the twisted composition algebras associated to $((1,\alpha),\alpha)$ above breaks into three E-isomorphism classes. These are associated to

$$(e_1,\nu_1) = ((1,\alpha,\alpha),\alpha), \quad (e_2,\nu_2) = ((\alpha,1,\alpha),\alpha), \quad (e_3,\nu_3) = ((\alpha,\alpha,1),\alpha).$$

- When $F = \mathbb{R}$, then $E = \mathbb{R}^3$ or $\mathbb{R}\times\mathbb{C}$. When $K_J = \mathbb{R}^2$ is split, then there is a unique J, namely the one associated to $M_3(\mathbb{R})$, and there is a unique conjugacy class of embeddings $E \hookrightarrow J$.

When $K_J = \mathbb{C}$, then there are two possible J, associated to $B = M_3(\mathbb{C})$ and the involution τ given by the conjugation action of two Hermitian matrices with signature $(1,2)$ and $(3,0)$. We denote these two Jordan algebras by $J_{1,2}$ and $J_{3,0}$.

When $E = \mathbb{R}^3$ and $K = \mathbb{C}$, we have $|\Omega_{E,K}| = 2$. However, the two elements in question correspond to embeddings

$$\mathbb{R}^3 \hookrightarrow J_{3,0} \quad \text{and} \quad \mathbb{R}^3 \hookrightarrow J_{1,2}.$$

Thus, we see that these subalgebras are unique up to conjugacy. When $E = \mathbb{R}\times\mathbb{C}$ and $K = \mathbb{R}^2$, we have $|\Omega_{E,K}| = 1$. This reflects the fact that there is no embedding $\mathbb{R}\times\mathbb{C} \hookrightarrow J_{3,0}$, and there is a unique conjugacy class of embeddings $\mathbb{C} \hookrightarrow J_{1,2}$.

Acknowledgment

This work began when both authors participated in the program "Branching Laws" at the Institute for Mathematical Sciences at the National University of Singapore in March 2012, and was completed during Savin's stay at the Hong Kong University of Science and Technology in May 2013. Both authors thank Chengbo Zhu for his invitation to the IMS program. Savin would like to thank Jianshu Li for the invitation, and HKUST for excellent working environment.

Gan is partially supported by AcRF Tier One grant R-146-000-155-112, and Savin is supported by a National Science Foundation grant DMS-0852429.

References

[Bhargava 2004a] M. Bhargava, "Higher composition laws, I: A new view on Gauss composition, and quadratic generalizations", *Ann. of Math.* (2) **159**:1 (2004), 217–250. MR 2005f:11062a Zbl 1072.11078

[Bhargava 2004b] M. Bhargava, "Higher composition laws, II: On cubic analogues of Gauss composition", *Ann. of Math.* (2) **159**:2 (2004), 865–886. MR 2005f:11062b Zbl 1169.11044

[Bhargava 2004c] M. Bhargava, "Higher composition laws, III: The parametrization of quartic rings", *Ann. of Math.* (2) **159**:3 (2004), 1329–1360. MR 2005k:11214 Zbl 1169.11045

[Gan et al. 2002] W. T. Gan, B. Gross, and G. Savin, "Fourier coefficients of modular forms on G_2", *Duke Math. J.* **115**:1 (2002), 105–169. MR 2004a:11036 Zbl 1165.11315

[Knus et al. 1998] M.-A. Knus, A. Merkurjev, M. Rost, and J.-P. Tignol, *The book of involutions*, American Mathematical Society Colloquium Publications **44**, Amer. Math. Soc., Providence, RI, 1998. MR 2000a:16031 Zbl 0955.16001

[Serre 2002] J.-P. Serre, *Galois cohomology*, Springer, Berlin, 2002. MR 2002i:12004 Zbl 1004.12003

[Springer and Veldkamp 2000] T. A. Springer and F. D. Veldkamp, *Octonions, Jordan algebras and exceptional groups*, Springer, Berlin, 2000. MR 2001f:17006 Zbl 1087.17001

Communicated by Efim Zelmanov
Received 2014-02-24 Revised 2014-07-23 Accepted 2014-07-26

matgwt@nus.edu.sg *Department of Mathematics, National University of Singapore, Block S17, 10 Lower Kent Ridge Road, Ridge Road, Singapore 119076, Singapore*

savin@math.utah.edu *Department of Mathematics, University of Utah, Salt Lake City, UT 84112, United States*

Algebra & Number Theory

msp.org/ant

See inside back cover or msp.org/ant for submission instructions.

The subscription price for 2014 is US $225/year for the electronic version, and $400/year (+$55, if shipping outside the US) for print and electronic. Subscriptions, requests for back issues and changes of subscribers address should be sent to MSP.

Algebra & Number Theory (ISSN 1944-7833 electronic, 1937-0652 printed) at Mathematical Sciences Publishers, 798 Evans Hall #3840, c/o University of California, Berkeley, CA 94720-3840 is published continuously online. Periodical rate postage paid at Berkeley, CA 94704, and additional mailing offices.

ANT peer review and production are managed by EditFLOW® from MSP.

PUBLISHED BY

mathematical sciences publishers

nonprofit scientific publishing

http://msp.org/

Algebra & Number Theory

Volume 8 No. 8 2014