

On cubic separable algebras

M.A. Knus, E.T.H. Zurich

Foreword

These notes were prepared for a minicourse given at UNICAMP in September 1996. The idea was to present recent proofs of classical results (Wedderburn, Albert) and to describe some less classical ones (but in a classical spirit!) on involutions of the second kind. Our main sources are [H], [HK], [HKRT] and [KMRT]. Some familiarity with the theory of central simple algebras and the theory of quadratic forms was assumed. For these topics [S] is a reference.

I am very grateful to my friend Antonio Paques, who made my visit to Campinas possible. The visit was financed by a grant from the FAPESP. I thank this Institution for its support.

1. Introduction

Throughout these lectures the letter F will stand for a field. An F -algebra A is always finite dimensional as a vector space over F , has an identity 1 and is, if not further specified, associative.

Suppose that $\dim_F A = r$ and let $F(X_1, \dots, X_r)$ be the rational function field in r variables X_1, \dots, X_r . Let u_1, \dots, u_r be a basis of A . The element

$$x = \sum_{i=1}^r X_i u_i \in A \otimes F(X_1, \dots, X_r)$$

is called a *generic element of A* (even if $x \notin A$!) The set of polynomials $p(T) \in F(X_1, \dots, X_r)[T]$ such that $p(x) = 0$ in $A \otimes F(X_1, \dots, X_r)$ is an ideal of $F(X_1, \dots, X_r)[T]$, hence there is a unique monic polynomial

$$P_{A,x}[T] = T^m - s_1(x)T^{m-1} + \dots + (-1)^m s_m(x)1$$

of least degree which has x as a root. This is the *generic minimal polynomial* of A . The coefficients $s_i(x)$ are homogeneous polynomials in the variables X_i , $s_1(x)$ is the *generic trace*, denoted by t_A , s_m is the *generic norm*, denoted by n_A and m is the *degree* of A . The bilinear form

$$t_A(x, y) = t_A(xy)$$

is the *bilinear trace form* of A . Its is symmetric if A is associative. Let $\alpha : A \xrightarrow{\sim} A'$ be an isomorphism of algebras. In view of the uniqueness of the generic minimal polynomial, we have

$$P_{A',\alpha(x)}[T] = P_{A,x}[T]$$

and, in particular $t_{A'}(\alpha(x), \alpha(y)) = t_A(x, y)$. Thus α induces an isometry of the corresponding trace forms. In this way techniques of the theory of bilinear forms can be applied to algebras. We now describe the class of algebras A for which t_A is nonsingular:

Theorem 1.1. Let A be an algebra. The following conditions are equivalent:

- (1) the bilinear trace form t_A is nonsingular
- (2) for any field extension \overline{F}/F , $A \otimes \overline{F}$ is semisimple, i.e. is a direct sum of simple twosided ideals. ■

Algebras satisfying the equivalent properties of Theorem 1 are called *separable*. The structure of separable algebras is described in the following

Theorem 1.2. A separable algebra is the product of a finite number of simple algebras whose centers are finite separable field extensions of F . ■

Remark: A finite field extension L/F is separable as an F -algebra if and only if it is separable in the sense of field theory.

Since a simple algebra is central over its center, Theorem 2 reduces the study of separable algebras to

- (1) commutative separable algebras; it is usual to call them *étale algebras*
- (2) central simple algebras

Example: *Algebras of degree 2.* For convenience we assume here that F is a field of characteristic not equal to 2. A quadratic étale algebra K is either isomorphic to $F \times F$ or is a quadratic field extension. In both cases we can write $K = F[X]/(X^2 - a)$, $a \neq 0$. Denoting by i the class of X in K and putting $x = x_1 \cdot 1 + x_2 \cdot i$, we have

$$P_{K,x}[T] = T^2 - 2x_1T + (x_1^2 - ax_2^2)1 \quad \text{and} \quad t_K(x, y) = 2x_1y_1 + 2ax_2y_2.$$

A central simple algebra Q of degree 2 is a quaternion algebra i.e. Q is generated by two elements i, j with relations

$$i^2 = a, j^2 = b, \quad a, b \neq 0 \quad \text{and} \quad ij + ji = 0$$

A basis of Q is $\{1, i, j, ij\}$ and we have for $x = x_1 \cdot 1 + x_2 \cdot i + x_3 \cdot j + x_4 \cdot ij$

$$P_{Q,x}(T) = T^2 - 2x_1T + (x_1^2 - ax_2^2 - bx_3^2 + abx_4^2) \cdot 1,$$

$$t_Q(x, y) = 2x_1y_1 + 2ax_2y_2 + 2bx_3y_3 - 2abx_4y_4$$

We denote $Q = (a, b)_F$; Either $Q \simeq M_2(F)$ or Q is a division algebra. The last case occur if and only if n_Q is anisotropic.

There is another interesting class of algebras of degree 2, which however are no longer associative, but *alternative* i.e. the weaker form

$$x(xy) = (xx)y \quad \text{and} \quad (xy)y = x(yy)$$

of associativity holds. These algebras are *octonion algebras*, of dimension 8, and can be represented as

$$\mathcal{O} = Q \oplus Qz$$

as vector spaces over F , where z is a symbol such that $z^2 = c, c \in F^\times$ and Q is a quaternion algebra. If $Q = (a, b)_F$, we write $\mathcal{O} = (a, b, c)_F$.

In all these examples (quadratic, quaternion and octonion algebras) the algebra admits an *involution* (i.e. an antiautomorphism of order 2) $x \mapsto \bar{x}$ such that $x + \bar{x}$ is the generic trace t_A and $x \cdot \bar{x}$ the generic norm n_A , so that the generic minimal polynomial is obviously $T^2 - t_A(x)T + n_A(x) \cdot 1$. Summarizing, we have examples of dimension 2, 4 and 8 in degree 2. The aim of the lectures is to describe algebras of dimension 3, 9 and 27 in degree 3.

2. Etale algebras.

We follow here [KMRT]. For any finite dimensional commutative F -algebra L we denote by

$$X(L) = \text{Alg}_F(L, F_{\text{sep}})$$

the set of F -algebra homomorphisms of L to a separable closure F_{sep} of F .

Theorem 2.2. For a finite dimensional commutative F -algebra L the following conditions are equivalent

- (a) L is separable
- (b) $L \simeq K_1 \times K_2 \times \dots \times K_r$, K_i/F finite separable field extensions
- (c) $L \otimes F_{\text{sep}} \simeq F_{\text{sep}} \times \dots \times F_{\text{sep}}$
- (d) $\text{card } X(L) = \dim_F L$

If F is infinite the conditions above are also equivalent to $L \simeq F[X]/(f)$ for some polynomial $f \in F[X]$ which has no multiple roots in an algebraically closed extension of F . ■

As already mentioned an algebra satisfying these properties is called *étale*. The category \mathbf{Et}_F of étale algebras over F is closed under products $L_1 \times L_2$ and tensor products $L_1 \otimes L_2$ (this is the main reason to work with étale algebras v.s. finite separable field extensions). The algebra $F \times \dots \times F$ (n times) is the *split* étale algebra of dimension n . The generic minimal polynomial of F (with respect to the basis element 1) is $P_{F,x}(T) = T - x_1$. Since

$$P_{A \times B, (x,y)}(T) = P_{A,x}(T) \cdot P_{B,y}(T)$$

for a product algebra $A \times B$, the generic minimal polynomial of the split algebra $F \times \dots \times F$ is $(T - x_1) \dots (T - x_n)$, hence is of degree n . The degree is invariant under changes of base fields, hence it follows from Theorem 2.2, (c) that the generic minimal polynomial of an étale algebra of dimension n has degree n . Let $\rho : L \rightarrow \text{End}_F(L)$ be the regular representation. Since the characteristic polynomial $\det(T \cdot \text{Id} - \rho(x))$ has degree n , the Cayley - Hamilton theorem implies that

$$P_{L,x}(T) = \det(T \cdot \text{Id} - \rho(x))$$

and $t_L(x) = \text{tr}(\rho(x))$, where tr is the trace. Thus by Theorem 1.1 a commutative algebra L is étale if and only if the bilinear trace form $t_L(x, y) = \text{tr}(\rho(x)\rho(y))$ is nonsingular.

The extension F_{sep}/F is a Galois extension with group

$$\Gamma = \varprojlim_{\bar{\alpha}} \text{Gal}(F_{\alpha}/F),$$

where the limit is taken over all finite Galois extension $F \subset F_{\alpha} \subset F_{\text{sep}}$. The group Γ has a topology induced by the discrete topology on the groups $\text{Gal}(F_{\alpha}/F)$. It acts (on the left) on $X(L)$:

$$\gamma\xi = \gamma \circ \xi \quad \text{for } \gamma \in \Gamma \text{ and } \xi \in X(L).$$

The action is continuous, in the sense that it factors through a finite quotient $\text{Gal}(M/F)$ of Γ : take for M any finite Galois extension which contains $\xi(L)$ for all $\xi \in X(L)$.

Let \mathbf{Sets}_{Γ} be the category of finite sets with continuous left action of Γ . The correspondance $L \mapsto X(L)$ defines a contravariant functor

$$X : \mathbf{Et}_F \rightarrow \mathbf{Sets}_{\Gamma}$$

We define a functor in reverse direction. For $X \in \mathbf{Sets}_{\Gamma}$, consider the F_{sep} -algebra $\text{Map}(X, F_{\text{sep}})$ of all set-theoretic maps $f : X \rightarrow F_{\text{sep}}$ with pointwise addition and multiplication. It is convenient to write $f(\xi) = \langle f, \xi \rangle$ for $f \in \text{Map}(X, F_{\text{sep}})$ and $\xi \in X$. We define a Γ -semilinear action of Γ on $\text{Map}(X, F_{\text{sep}})$ as follows

$$\langle \gamma f, \xi \rangle = \gamma(\langle f, \gamma^{-1}\xi \rangle)$$

Let $M(X) = \text{Map}(X, F_{\text{sep}})^{\Gamma}$ denote the F -algebra of Γ -invariant maps. The algebra $M(X)$ is étale since by Galois descent

$$\text{Map}(X, F_{\text{sep}})^{\Gamma} \otimes_F F_{\text{sep}} \simeq \text{Map}(X, F_{\text{sep}}) = F_{\text{sep}} \times \dots \times F_{\text{sep}}.$$

Hence we get a contravariant functor $M : \mathbf{Sets}_{\Gamma} \rightarrow \mathbf{Et}_F$, $X \mapsto M(X)$.

Theorem 2.2. The functors X and M define an anti-equivalence of categories $\mathbf{Et}_F \equiv \mathbf{Sets}_{\Gamma}$.

“Proof.” The maps $L \rightarrow \text{Map}(X(L), F_{\text{sep}})^\Gamma$, $\ell \mapsto e_\ell$, $\langle e_\ell, \xi \rangle = \xi(\ell)$ and $X \rightarrow X(\text{Map}(X, F_{\text{sep}})^\Gamma)$, $\xi \mapsto e_\xi$, $e_\xi(f) = \langle f, \xi \rangle$ are isomorphisms. ■

Under this equivalence a direct product decomposition $L_1 \times L_2$ corresponds to a disjoint union $X(L_1) \cup X(L_2)$. We have $L \simeq F \times \dots \times F$ (i.e. L split) if and only if Γ acts trivially and L is a field if and only if Γ acts transitively on $X(L)$. In particular the decomposition of L as a direct product of fields corresponds to the decomposition of $X(L)$ in orbits under Γ .

We have a map

$$X(L_1) \times X(L_2) \rightarrow X(L_1 \otimes L_2)$$

defined by $(\xi_1, \xi_2)(x \otimes y) = \xi_1(x)\xi_2(y)$. Every F -algebra homomorphism $\varphi : L_1 \otimes L_2 \rightarrow F_{\text{sep}}$ is of this type, since $\varphi(x \otimes y) = \varphi((x \otimes 1)(1 \otimes y)) = \varphi(x \otimes 1)\varphi(1 \otimes y)$.

Thus we may identify

$$X(L_1 \otimes L_2) = X(L_1) \times X(L_2).$$

γ acting diagonally on the right. In particular we have a canonical isomorphism

$$L \otimes L \simeq \text{Map}(X(L) \times X(L), F_{\text{sep}})^\Gamma.$$

In the same way as étale algebras generalize finite separable field extensions, there is a generalization of finite Galois field extensions: let L be étale and let $G \subset \text{Aut}_F(L)$ be a finite group of F -automorphisms of L . We say that L is a *G-Galois algebra* if (1) $|G| = \dim_F L$, (2) $L^G = F$. There is a right action of G on $X(L)$, $\xi \mapsto \xi^g = \xi \circ g$, $\xi \in X(L)$, $g \in G$, which corresponds to the G -action on L through the equivalence $\mathbf{Et}_F \equiv \mathbf{Sets}_\Gamma$, and this action on $X(L)$ is Γ -equivariant. Moreover $X(L)$ is a *G-torsor*, i.e. for all $\xi, \eta \in X(L)$ there is a unique $g \in G$ such that $\eta = \xi^g$.

The Galois closure and the discriminant. Let X be a Γ -set of n elements and let

$$\Sigma(X) = \{(\xi_1, \dots, \xi_n) \mid \xi_i \in X, \xi_i \neq \xi_j \text{ for } i \neq j\}$$

The set $\Sigma(X)$ has $n!$ elements and is a Γ -set through the action $\gamma(\xi_1, \dots, \xi_n) = (\gamma\xi_1, \dots, \gamma\xi_n)$. Furthermore the group S_n of permutations of n objects acts Γ -equivariantly through permutations: $(\xi_1, \dots, \xi_n)^\sigma = (\xi_{\sigma(1)}, \dots, \xi_{\sigma(n)})$. Clearly $\Sigma(X)$ is an S_n -torsor and the projections on the various components define Γ -equivariant maps

$$\pi_i : \Sigma(X) \rightarrow X.$$

If L is étale of dimension n we can associate to L under the antiequivalence $\mathbf{Et}_F \cong \mathbf{Set}_\Gamma$ the S_n -Galois algebra

$$\Sigma(L) = \text{Map}(\Sigma(X(L)), F_{\text{sep}})^\Gamma$$

with n canonical embeddings $\varepsilon_i : L \hookrightarrow \Sigma(L)$ defined by

$$\langle \varepsilon_i(\ell), (\xi_1, \dots, \xi_n) \rangle = \xi_i(\ell)$$

The algebra $\Sigma(L)$ is called the *Galois S_n -closure of L* .

For X as above, let $\Delta(X)$ be the set of orbits of $\Sigma(X)$ under the action of the alternating group A_n with the induced action of Γ . This set has 2 elements. If $X = X(L)$ for L étale of dimension n

$$\Delta(L) = \text{Map}(\Delta(X(L)), F_{\text{sep}})^\Gamma$$

is a quadratic étale algebra over F . Alternatively we have

$$\Delta(L) = \Sigma(L)^{A_n}$$

An element $\gamma \in \Gamma$ acts trivially on $\Delta(X(L))$ if and only if the permutation $\xi \mapsto \gamma\xi$ is even. Therefore the kernel of the action of Γ on $\Delta(X(L))$ is the subgroup $\Gamma_0 \subset \Gamma$ which acts by even permutations on $X(L)$ and

$$\Delta(L) \simeq \begin{cases} F \times F & \text{if } \Gamma_0 = \Gamma \\ (F_{\text{sep}})^{\Gamma_0} & \text{if } \Gamma_0 \neq \Gamma. \end{cases}$$

The algebra $\Delta(L)$ is called the *discriminant algebra of L* .

Example: Let $L = F[X]/(f)$, f of degree n without multiple roots. Let x be the class of X in L and let $x_1, \dots, x_n \in F_{\text{sep}}$ be the roots of f . We have

$X(L) = \{\xi_1, \dots, \xi_n\}$ where $\xi_1(x) = x_i$. If $\text{char } F \neq 2$, $\gamma \in \Gamma$ induces an even permutation of $X(L)$ if and only if $\gamma(\prod_{i<j}(x_i - x_j)) = \prod_{i<j}(x_i - x_j)$. Thus $\Delta(L) \simeq F[T]/(T^2 - d)$, where $d = \prod_{i<j}(x_i - x_j)^2$ is the classical discriminant of f .

Exercise: If $\text{char } F \neq 2$, $\Delta(L) \simeq F[T]/(T^2 - d)$, where d represents the determinant of the bilinear trace form $t_L(x, y)$.

3. Etale algebras of dimension 3. The aim is to establish canonical isomorphisms

$$L \otimes L \xrightarrow{\sim} L \times \Sigma(L) \quad \text{and} \quad L \otimes \Delta(L) \xrightarrow{\sim} \Sigma(L)$$

for L an étale algebra of dimension 3. Let X be a Γ -set of 3 elements and

$$\Sigma(X) = \{(\xi_1, \xi_2, \xi_3) \mid \xi_i \in X, \xi_i \neq \xi_j, i \neq j\}$$

the associated S_3 -torsor. Consider the transpositions

$$\tau_1 = (2, 3), \tau_2 = (1, 3) \quad \text{and} \quad \tau_3 = (1, 2)$$

in S_3 and the corresponding subgroups $\{1, \tau_i\} = H_i$ of order 2.

Let $\Sigma(X)/A_3$, resp. $\Sigma(X)/H_i$ be the set of orbits under A_3 , resp. H_i . The canonical map

$$\Sigma(X) \rightarrow \Sigma(X)/A_3 \times \Sigma(X)/H_i$$

which carries ξ to the couple (ξ^{A_3}, ξ^{H_i}) is Γ -equivariant and is a bijection since $\xi^{A_3} \cap \xi^{H_i} = \{\xi\}$. Moreover the projection $\pi_i : \Sigma(X) \rightarrow X$ factorizes through $\Sigma(X)/H_i$; thus we get three canonical Γ -equivariant bijections

$$\hat{\pi}_i : \Sigma(X) \xrightarrow{\sim} \Delta(X) \times X.$$

Theorem 3.1. Let L be étale of dimension 3. The canonical embeddings $\varepsilon_i : L \rightarrow \Sigma(L)$ induce isomorphisms

$$\hat{\varepsilon}_i : \Delta(L) \otimes L \xrightarrow{\sim} \Sigma(L), \quad i = 1, 2, 3$$

Proof. The $\hat{\varepsilon}_i$ correspond to the $\hat{\pi}_i$ through the antiequivalence $\mathbf{Et}_F \equiv \mathbf{Sets}_\Gamma$ ■

Consider now the Γ -set $X \times X$ with Γ acting diagonally. It has a disjoint decomposition (as Γ -sets)

$$X \times X = D \cup E$$

where D is the diagonal and E is its complement. There is a canonical bijection $X \xrightarrow{\sim} D$ which maps $\xi \in X$ to (ξ, ξ) . Moreover we have three canonical bijection

$$v_i : \Sigma(X) \rightarrow E, \quad i = 1, 2, 3,$$

which each forgets the i -component. These maps are Γ -equivariant, hence we get three isomorphisms of Γ -sets

$$\hat{v}_i : X \cup \Sigma(X) \xrightarrow{\sim} X \times X$$

which corresponds to three F -algebra isomorphisms

$$\theta_i : L \otimes L \xrightarrow{\sim} L \times \Sigma(L)$$

through the antiequivalence $\mathbf{Et}_F \equiv \mathbf{Sets}_\Gamma$

Theorem 3.2. θ_i maps $x \otimes y$ to (xy, f_i) , where $f_i \in \text{Map}(\Sigma(X(L)), F_{\text{sep}})^\Gamma$ carries $(\xi_1, \xi_2, \xi_3) \in \Sigma(X(L))$ to $\theta_i(\xi_1, \xi_2, \xi_3)(x \otimes y)$. ■

The action of Γ on $X(L)$ can

- (1) be trivial, “case” 1S_3
- (2) factor over $\mathbb{Z}/2\mathbb{Z}$, “case” 2S_3
- (3) factor over A_3 , “case” 3S_3
- (4) factor over S_3 , “case” 6S_3

We consider each case separately. Since the decompositions of L as product of fields corresponds to the orbit decomposition of $X(L)$ under Γ , we have $L \simeq F \times F \times F$ in case (1), $L \simeq F \times K, K$ a quadratic field in case (2) and L is a field in case (3) and (4).

Case 1S_3 : The split algebra $L = F \times F \times F$ is obviously a A_3 -Galois algebra, A_3 acting through cyclic permutations. We have

$$\Sigma(L) = \prod_{\sigma \in S_3} F_\sigma,$$

where the F_σ are copies of F indexed by S_3 and S_3 acts by right translations. In particular we get $\Delta(L) \simeq F \times F$.

Case 2S_3 : Let $L = F \times K$ with K a quadratic étale (=Galois) field extension of F and let $z \mapsto \bar{z}$ be the conjugation in K . Assume that $K \subset F_{\text{sep}}$. The three elements of $X(L)$ are

$$r_1 : (x, z) \mapsto x, \quad c_1 : (x, z) \mapsto z, \quad c_2 : (x, z) \mapsto \bar{z}$$

The action of Γ permutes c_1 and c_2 . The isomorphism

$$L \xrightarrow{\sim} \text{Map}(X(L), F_{\text{sep}})^\Gamma$$

is given by

$$(x, z) \mapsto \begin{cases} \langle e_{(x,z)}, r_1 \rangle = x \\ \langle e_{(x,z)}, c_1 \rangle = z \\ \langle e_{(x,z)}, c_2 \rangle = \bar{z} \end{cases}$$

Let now $\Sigma(X(L)) = \{\xi_1 = (r_1, c_1, c_2), \xi_2 = (r_1, c_2, c_1), \xi_3 = (c_1, r_1, c_2), \xi_4 = (c_2, r_1, c_1), \xi_5 = (c_1, c_2, r_1), \xi_6 = (c_2, c_1, r_1)\}$

The action of Γ permutes the elements ξ_1, ξ_2 , resp. ξ_3, ξ_4 and ξ_5, ξ_6 . We claim that $\Sigma(L) = K \times K \times K$. It suffices to give a map

$$K \times K \times K \rightarrow \text{Map}(\Sigma(X(L)), F_{\text{sep}})^\Gamma.$$

We set $\langle e_{(z_1, z_2, z_3)}, \xi_1 \rangle = z_1, \langle e_{(z_1, z_2, z_3)}, \xi_2 \rangle = \bar{z}_1, \dots$

Writing S_3 as a semidirect product $S_3 = A_3 \rtimes \mathbb{Z}/2\mathbb{Z}$, according to the exact sequence

$$1 \rightarrow A_3 \rightarrow S_3 \rightarrow \mathbb{Z}/2\mathbb{Z} \rightarrow 0,$$

one sees that A_3 permutes the factors and $\mathbb{Z}/2\mathbb{Z}$ acts as $(z_1, z_2, z_3) \mapsto (\bar{z}_1, \bar{z}_2, \bar{z}_3)$.

Thus $\Delta(F \times K) \simeq K$ and the isomorphism $L \otimes \Delta(L) \simeq \Sigma(L)$ is clear, since $K \otimes K \simeq K \times K, x \otimes y \mapsto (xy, x\bar{y})$.

Case 3S_3 : L is a field and is Galois with group A_3 , i.e. L is cyclic. Let $\rho \in \text{Gal}(L/F) = A_3$ be a generator. Then

$$X(L) = \{\varepsilon, \varepsilon \circ \rho, \varepsilon \circ \rho^2\}$$

where $\varepsilon : L \rightarrow F_{\text{sep}}$ is a fixed embedding. We have

$$\Sigma(L) = L \times L$$

and, if $\sigma \in S_3$ of order 2 is such that $\sigma\rho\sigma = \rho^2$, we let ρ act as $\rho(u, v) = (\rho(u), \rho^2(v))$ and σ as the switch, $\sigma(u, v) = (v, u)$. We get in particular that $\Delta(L) \cong F \times F$.

Case 6S_3 : Here L is a separable non-normal cubic field extension. The group Γ acts as the full permutation group S_3 on $X(L)$, hence Γ acts simply transitively on $\Sigma(X(L))$ and $\Sigma(X(L)) \simeq L \otimes \Delta(L)$ is Galois of degree 6 over F with group S_3 . In particular $\Delta(L)$ is a quadratic Galois extension of F and $\Sigma(L)$ is cyclic of degree 3 over $\Delta(L)$.

Exercises: (1) Prove directly that L is a A_3 -Galois algebra over F if and only if $\Delta(L) \simeq F \times F$.

(2) Show that L étale of degree 3 has a primitive element, i.e. $L \simeq F[X]/(f)$ for some $f \in F[X]$ except if $F = \mathbb{F}_2$ and $L = F \times F \times F$.

Example: Let $L = F[X]/(f)$ with $f \in F[X]$ of degree 3 without multiple roots. If $\text{char} F \neq 3$, then f can be chosen as $f = X^3 + pX + q$ and, if furthermore $\text{char} F \neq 2$,

$$\Delta(L) \simeq F[t]/(t^2 - \delta)$$

where $\delta = -4p^3 - 27q^2$ is the classical discriminant. If $\text{char} F = 2$,

$$\Delta(L) \simeq F[t]/(t^2 + t + 1 + p^3q^{-2})$$

In particular, we have $\Delta(L) \simeq F[t]/(t^2 + t + 1)$ if $f = X^3 - b$ and $\text{char} F \neq 3$. We call a separable F -algebra of the form $L = F[X]/(X^3 - b)$ a *Kummer algebra*. Conversely we claim that L is a Kummer algebra if $\Delta(L) \simeq F[t]/(t^2 + t + 1)$. The class ω of t in $\Delta(L)$ is a primitive cubic root of 1. If $\omega \in F$, $\Delta(L) \simeq F \times F$, L is cyclic and, by Exercise (2) above, $L \not\simeq F \times F \times F$, so that L is a cyclic field extension of F . Let $\xi \in L$ be a primitive element and let $\rho \in \text{Gal}(L/F)$ be a generator of the Galois group. The Lagrange resolvent

$$x = \xi + \rho(\xi)\omega^2 + \rho^2(\xi)\omega$$

satisfies $\rho(x) = x\omega$, hence $x^3 = x\rho(x)\rho^2(x) = N_{L/F}(x) \in F$ (and $x \neq 0$ since by Dedekind, $1, \rho, \rho^2$ are linearly independent). Thus L is a Kummer extension. Assume now that $\omega \notin F$, so that $\Delta(L) = F(\omega)$ is a quadratic field over F . If L is not a field, $L = F \times F(\omega) = F[x]/(x^3 - 1)$ is a Kummer algebra. If L is a field $L \otimes \Delta(L) = L(\omega)$ is a Galois field extension of F of degree 6, cyclic of degree 3 over $F(\omega)$. Let $\rho \in \text{Gal}(L(\omega)/F(\omega))$ be a generator and let $\xi \in L$ be primitive. Let again

$$x = \xi + \rho(\xi)\omega^2 + \rho^2(\xi)\omega$$

If $x \in L$, then by the above computation, L is Kummer over F . Let τ be the automorphism of $L \otimes \Delta(L) = L(\omega)$ induced by the conjugation of $F(\omega)$, so that $\tau|_L = 1_L$, $\tau(\omega) = \omega^2$ and $\tau\rho\tau = \rho^2$. Then obviously $\tau(x) = x$ and $x \in L$ as claimed.

The trace form. We denote by $\langle a_1, \dots, a_n \rangle$, $a_i \in F^\times$ the bilinear form $f(x, y) = \sum a_i x_i y_i$ and by $f \perp g$ the orthogonal sum of two bilinear forms f, g . Let L be cubic

separable. If L is not a field, say $L = F \times K$, K quadratic étale, we have for the trace form

$$t_L = t_F \perp t_K$$

Assume $\text{char} F \neq 2$, so that K has a basis $\{1, i\}$ with $i^2 = d$, $d \in K^\times$. We have $t_K \simeq \langle 2, 2d \rangle$ with respect to this basis, so that

$$t_L \simeq \langle 1, 2, 2\delta \rangle$$

since $t_F = \langle 1 \rangle$. Recall that $K \simeq \Delta(L)$, so that

$$(*) \quad t_L \simeq \langle 1, 2, 2\delta \rangle$$

where $\Delta(L) \simeq F[X]/(X^2 - \delta)$. We claim that the same holds if L is a field. We use the following

Theorem 3.3 (Springer) Let f, g be nonsingular bilinear forms over a field F with $\text{char} F \neq 2$. If $f \otimes \overline{F}$ and $g \otimes \overline{F}$ are isometric for some finite field extension \overline{F}/F of odd degree, then $f \simeq g$. ■

Proof of (*): We have $L \otimes L \simeq L \times L \otimes \Delta(L)$, hence

$$t_{L \otimes L/L} \simeq \langle 1 \rangle_L \perp t_{L \otimes \Delta(L)/L} \simeq \langle 1, 2, 2\delta \rangle_L$$

hence the claim by Springer's theorem. ■

4. Central simple algebras of degree 3. We recall that a central simple algebra A is a “form” of a matrix algebra, i.e. there exists a field extension \overline{F}/F and an isomorphism

$$\alpha : A \otimes \overline{F} \xrightarrow{\sim} M_n(\overline{F}).$$

In particular the dimension of A over F is always a square. The generic minimal polynomial of $M_n(F)$ is

$$P_{M_n(F),x}(T) = \det(T \cdot Id - x)$$

(by Cayley-Hamilton, since $\det(T \cdot Id - x)$ is irreducible. Hence

$$P_{A,x}(T) = \det(T \cdot Id - \alpha(x \otimes 1))$$

for an arbitrary central simple algebra A . Thus $\deg A = \sqrt{\dim_F A}$. Particularly nice central simple algebras are *cyclic algebras*: let C_n denote the cyclic group $\mathbb{Z}/n\mathbb{Z}$ with generator $\rho = 1 + n\mathbb{Z}$, let L be a Galois C_n -algebra and let $a \in F^\times$. The *cyclic algebra* (L, a) is defined as

$$(L, a) = L \oplus Lz \oplus \dots \oplus Lz^{n-1}$$

where z is a symbol subject to the relations

$$z\ell = \rho(\ell)z, \ell \in L \text{ and } z^n = a$$

Example: Let $L = F \times \dots \times F$ with the C_n -structure defined by $\rho(x_1, \dots, x_n) = (x_2, x_3, \dots, x_1)$. We have $(L, a) \simeq M_n(F)$ for all $a \in F^\times$. An explicit isomorphism is given by

$$(x_1, \dots, x_n) \mapsto \begin{pmatrix} x_1 & & & & \\ & x_2 & & & \\ & & \ddots & & \\ & & & x_n & \\ & & & & \end{pmatrix} \text{ and } z \mapsto \begin{pmatrix} 0 & 1 & 0 & \dots & 0 \\ 0 & 0 & 1 & \dots & 0 \\ \vdots & & & & 1 \\ a & \dots & & & 0 \end{pmatrix}$$

From this example, it follows that (L, a) is central simple for all C_n -algebras L and all $a \in F^\times$, since $(L, a) \otimes F_{\text{sep}} \simeq (L \otimes F_{\text{sep}}, a)$ and $L \otimes F_{\text{sep}} \simeq F_{\text{sep}} \times \dots \times F_{\text{sep}}$. Not every central simple algebra is cyclic. This is true in degree 2, since cyclic algebras of degree 2 are quaternion algebras, and in degree 3: (however in degree 4 there are examples of noncyclic algebras, due to Albert).

Theorem 4.1. (Wedderburn) Every central simple algebra of degree 3 is cyclic.

We give a proof due to Haile [H], assuming $\text{char} F \neq 3$. Let A^\times be the group of units of A .

Lemma 4.2. Let A be central simple of degree 3 and let $x \in A^\times$. If $t_A(x) = 0 = t_A(x^{-1})$, then $x^3 = n_A(x) \cdot 1$.

Proof. Let $T^3 - t_A(x)T^2 + s_A(x)T - n_A(x)1$ be the generic minimal polynomial (the reduced characteristic polynomial of $x \in A$). Then

$$T^3 - \frac{s_A(x)}{n_A(x)}T^2 + \frac{t_A(x)}{n_A(x)}T - \frac{1}{n_A(x)} \cdot 1$$

is the generic minimal polynomial of x^{-1} . Therefore $t_A(x^{-1}) = s_A(x)n_A(x^{-1})$ and the reduced characteristic polynomial of x has the form $T^3 - n_A(x) \cdot 1$ if $t_A(x) = 0 = t_A(x^{-1})$. \blacksquare

Proof of Theorem 4.1: In view of the above example we may assume that D is a central division algebra. We claim that it suffices to find $y, z \in D$ such that $z \notin F, y \notin F(z)$ and

$$t_D(x) = 0 = t_D(x^{-1})$$

for $x = z, yz, yz^2$. Indeed by the lemma we have

$$z^3 = n_D(z), (yz)^3 = n_D(yz) \quad (yz^2)^3 = n_D(yz^2);$$

since $n_D(yz^2) = n_D(yz)n_D(z)$, it follows that $(yz^2)^3 = (yz)^3z^3$ hence, after cancellations

$$zyz^2y = yzyz^2$$

Dividing both sides by $z^3 = n_D(z)$ we get

$$zyz^{-1}y = yzyz^{-1}$$

Hence zyz^{-1} commutes with all elements of $F(y)$. Since $y \notin F, F(y)$ is a cubic subfield of degree 3 of D , hence is maximal, so that $zyz^{-1} \in F(y)$. We have $zyz^{-1} \neq y$ since $y \notin F(z)$ and we define a C_3 -algebra structure of $F(y)$ by letting $\rho(y) = zyz^{-1}$ and

$$D \simeq (F(y), n_z(z))$$

is cyclic, as claimed. We now proceed to construct y, z as wanted. Let $L \subset D$ be an arbitrary maximal subfield. L is separable since $\text{char} F \neq 3$. Since the bilinear form t_L is nonsingular, we have

$$t_D = t_L \perp t_U$$

where $U = L^\perp = \{x \in D \mid t_D(x, y) = 0, \forall y \in L\}$. Let $0 \neq u_1 \in U$ and let $V = (Fu_1^{-1})^\perp$. Since $\dim_F V \geq 8$ and $\dim_F L = 3$, $V \cap L \neq \{0\}$, so let $0 \neq u_2 \in V \cap L$. We set $z = u_1 u_2^{-1}$; we have $t_D(z) = t_D(u_1, u_2^{-1}) = 0$ since $u_1 \in L^\perp, u_2 \in L$ and $t_D(z^{-1}) = 0$ because $u_2 \in (Fu_1^{-1})^\perp$. We cannot have $z \in F$, because $t_D(\xi) = 3\xi \neq 0$ for $\xi \in F^\times$. Next pick $v_1 \in F(z)^\perp$. Since

$$\dim(zF + z^{-1}F)^\perp = 7$$

we have

$$v_1(zF + z^{-1}F)^\perp \cap F(z) \neq \{0\}$$

we thus can find a nonzero element v_2 in the intersection and set $y = v_2^{-1}v_1$. We claim that $v_1 \notin F(z) : v_1 \in F(z)$ implies

$$F(z)^\perp \cap F(z) \neq \{0\}$$

This contradicts the fact that $t_{F(z)}$ is nonsingular, since $F(z)$ is separable. Hence $v_1 \notin F(z)$ and $y = v_2^{-1}v_1 \notin F(z)$. Since $v_1 \in F(z)^\perp$ and $v_2 \in F(z)$ we have

$$t_D(yz) = t_D(v_2^{-1}v_1z) = t_D(v_1zv_2^{-1}) = t_D(v_1, zv_2^{-1}) = 0$$

and

$$t_D(yz^2) = t_D(v_1, z^2v_2^{-1}) = 0$$

On the other hand, since $v_1^{-1}v_2 \in (zF + z^{-1}F)^\perp$ by definition of v_2 and $z^3 = n_D(z)$ we have

$$t_D(z^{-1}y^{-1}) = t_D(z^{-1}v_1^{-1}v_2) = 0 \quad \text{and} \quad t_D(z^{-2}y^{-1}) = n_D(z)t_D(zv_1^{-1}v_2) = 0$$

and y, z are as wanted. ■

Remark. Assuming Springer's theorem, the bilinear trace form of D central simple of degree 3 over F is easy to compute. The algebra D is either $M_3(F)$ or is a division algebra. If D is a division algebra, a maximal commutative subfield, which is of degree 3 will split D . Thus, by Springer's theorem $t_D \simeq t_{M_3(F)}$. An easy computation shows that

$$t_{M_3(F)} \simeq \langle 1, 1, 1 \rangle \perp \langle 1, -1, 1, -1, 1, -1 \rangle$$

5. Central simple algebras with involution. An involution σ of a ring A is an antiautomorphism of order 2, i.e. $\sigma(ab) = \sigma(b)\sigma(a)$ and $\sigma^2 = Id_A$. Examples are conjugation for quaternions and transpose $x \mapsto x^t$ for matrices. Let A be central simple over F . An involution needs of A not to be F -linear. However $\sigma(F) = F$ and one says that σ is of the *first kind* if $\sigma|_F = Id_F$ and of the *second kind* if $\sigma|_F \neq Id_F$. For example for $x \in M_n(\mathbb{C}), x \mapsto x^*$ with $x^* = (\bar{a}_{ij})^t$ if $x = (a_{ij})$ is of the second kind. If σ is of the first kind, we have an isomorphism

$$A \otimes A \xrightarrow{\sim} \text{End}_F(A), \quad a \otimes b \mapsto \ell_{a \otimes b}(x) = ax\sigma(b)$$

and A has order 2 in the Brauer group $\text{Br}(F)$ [and conversely, by a classical result of Albert]. Since a central simple algebra of degree 3 is either split, i.e. $A \simeq M_3(F)$, or has order 3 in $\text{Br}(F)$, such an algebra admits an involution of the first kind if and only if it splits. However central *division* algebras of degree 3 may admit involutions of the second kind. For such an involution σ , F is Galois quadratic over

$$F_0 = \{x \in F \mid \sigma(x) = x\}$$

It is convenient to view F_0 as base field and from now on we change notation: we give us a quadratic extension K/F with conjugation $i = i_K$ and consider central simple algebras B over K with involutions τ such that $\tau|_K = i_K$.

Examples 5.1. (1) $A = M_n(K), x \mapsto x^*, x^* = (\bar{a}_{ij})^t, \tau_a(x) = ax^*a^{-1}$ with $a^* = a$. It can be shown that any τ of second kind on $M_n(K)$ is of the form $\tau = \tau_a$.

(2) Let Q_0 be a quaternion algebra over F , let $Q = K \otimes Q_0$ and $\tau = \tau_K \otimes \sigma$, σ the conjugation of Q_0 . Then τ is of second kind and it can be shown that any quaternion

algebra Q over K with involution of second kind is of this type.

(3) It is convenient to define involutions of second kind also if $K = F \times F$: let A be central simple over F and let

$$B = A \times A^{\text{op}},$$

where A^{op} is the opposite algebra, i.e. $A = A^{\text{op}}$ as a set and $x^{\text{op}} \cdot y^{\text{op}} = (yx)^{\text{op}}$ through the identification $x \rightarrow x^{\text{op}}$. We view B as an $F \times F$ -algebra with componentwise addition and multiplication and define τ as

$$\tau(x, y^{\text{op}}) = (y, x^{\text{op}}).$$

The vector space (over F) of symmetric elements

$$H(B, \tau) = \{x \in B \mid \tau(x) = x\}$$

of a central simple algebra with involution of second kind has dimension $\dim_K B$, since we have an isomorphism of K -vector spaces

$$H(B, \tau) \otimes K \simeq B, \quad x \otimes y \mapsto xy.$$

Furthermore $H(B, \tau)$ is closed under the *Jordan multiplication*

$$x \circ y = \frac{xy + yx}{2} \quad (\text{we assume } \text{char } F \neq 2)$$

hence it is a *Jordan algebra* with identity 1 (in fact, with correct definitions it is a central simple Jordan algebra).

In particular powers x^n of elements $x \in H(B, \tau)$ lie in $H(B, \tau)$ and the reduced characteristic polynomial of B restricts to a generic polynomial $P_{H(B, \tau), x}(T)$ for the Jordan algebra $H(B, \tau)$, over F of the same degree as the reduced characteristic polynomial. In particular we have a nonsingular trace form $t_{H(B, \tau)}$ on $H(B, \tau)$. Our aim is to study $H(B, \tau)$ as an "object" of degree 3. We begin with two examples.

Examples 5.2. Let L_0 be a cubic separable field extension over F , let $K = \Delta(L_0)$ and let $M = \Sigma(L_0) = L_0 \otimes K$. Then M is cyclic over K and we get a cyclic algebra (M, a) over K_M for any $a \in K^\times$:

$$B = M \oplus Mz \oplus Mz^2$$

with $zmz^{-1} = \rho(m)$, ρ a generator of $Gal(M/K)$, and $z^3 = a$. Assume that $a \in F^\times$; let $i(\ell \otimes x) = \ell \otimes \bar{x}$ be the automorphism of M extending the conjugation of K . It is easy to check that the map $\tau : B \rightarrow B$ such that

$$(1) \tau|_M = i_M, \quad (2) \tau(z) = z \quad \text{and} \quad (3) \tau(mz) = z\tau(m)$$

is an involution of second kind of B such that

$$L_0 \subset H(B, \tau) \quad \text{and} \quad F(z) \simeq F[X]/(X^3 - a) \subset H(B, \tau)$$

Observe that the construction also makes sense if $\Delta(L_0) \simeq F \times F$, i.e. L_0 is cyclic, in which case $B = A \times A^{\text{op}}$ with $A = (L_0, a)$.

Example 5.3. Let L be cubic cyclic over F , so that $L \otimes K = M$ is cyclic over K for any quadratic étale algebra K . For any $a \in K^\times$ we get a cyclic algebra $B = (M, a)$ over K . If $a\bar{a} = 1$ in K , B admits an involution of second kind τ such that

$$1) \tau|_M = i \quad 2) \tau(z) = z^{-1} \quad \text{and} \quad 3) \tau(mz) = z^{-1}i(m).$$

Observe that, in this case $H(B, \tau)$ contains L and the extension $L' \subset K(z)$ defined by

$$L' = \{x \in K[z] \mid \tau(x) = x\}$$

In order to describe the discriminant of L' , we first define a product on quadratic algebras; for K_1, K_2 quadratic étale, we put

$$K_1 * K_2 = \{x \in K_1 \otimes K_2 \mid (i_1 \otimes i_2)(x) = x\}$$

where i_1, i_2 are the conjugation of K_1, K_2 . If $\text{char} F \neq 2$, $K_1 = F(\sqrt{\alpha})$, $K_2 = F(\sqrt{\beta})$, then $K_1 * K_2 = F(\sqrt{\alpha\beta})$. With these notations, it can be shown that

$$\Delta(L') = K * (F[t]/(t^2 + t + 1))$$

Thus $\Delta(L') = F(\sqrt{-3\alpha})$ if $K = F(\sqrt{\alpha})$ (assuming $\text{char} F \neq 2$).

Observe that in example 5.2 L_0 is not cyclic over F but $L_0 \otimes K$ is cyclic over K and that $F(z)$ is Kummer over F ; in Example 5.3 L is cyclic over F , L' is not

Kummer over F but $L' \otimes K$ is Kummer over K . In view of the following result, due to Albert, case 5.2 always occurs; however there exist examples of central simple algebras of degree 3 with involution of second kind which do not contain cyclic algebras over F . Thus, the case 5.3 is “exceptional”. From now on we assume $\text{char} F \neq 2, 3$.

Theorem 5.4. (Albert) Let B be a central simple K -algebra of degree 3 which admits an involution of second kind. There exist a cubic étale F -subalgebra L_0 of B , such that $L_0 K \subset B$ is cyclic over K and is a S_3 -Galois algebra over F , and an element $z \in B$ such that $z^3 = a \in F^\times$ and $B = L_0 K \oplus L_0 K z \oplus L_0 K z^2 = (L_0 K, a)$.

The proof of Albert is quite involved and we shall give a simpler proof, which is taken from [HK]. We begin with a preliminary lemma.

Lemma 5.5. Let B be a central division algebra of degree 3 over K with an involution τ of second kind and let $S = H(B, \tau)$ be the set of symmetric elements. Let L be an étale cubic extension of F contained in S . Then

- (1) There exists $d \in S \cap B^\times$ such that $t_B(Ld) = 0$
- (2) For d as in (1) the space $V = \{\ell \in L \mid t_B(d^{-1}\ell) = 0\}$ is at least 2-dimensional over F .
- (3) The space $U = d^{-1}V$ is contained in $H(B, \text{Int}(d^{-1}) \circ \tau)$ and $u^3 = n_B(u) \in F$ for all $u \in U$.

Proof. We first observe that any element in S not in F generates an extension L as wanted. We prove (1). For any $x \in S$ the linear map

$$f(x)(\ell) = t_B(\ell x)$$

has values in F since $\tau(t_B(\ell x)) = t_B(\tau(\ell x)) = t_B(\tau(x)\tau(\ell)) = t_B(x\ell) = t_B(\ell x)$. Thus we get an F -linear map $S \rightarrow L^* = \text{Hom}(L, F)$, $x \mapsto f(x)$. Since $\dim_F S > \dim_F L$ there is d as wanted in (1).

- (2) The linear map $\ell \mapsto t_B(d^{-1}\ell)$ has values in F , hence its kernel V has dimension

≥ 2 . We prove (3). By the choice of d we have

$$t_B(d^{-1}\ell) = t_B(\ell^{-1}d) = 0 \quad \text{for all } \ell \in V \cap B^\times$$

hence $t_B(u) = t_B(u^{-1}) = 0$ for all $u \in U \cap B^\times$. Thus, by Lemma 4.2 $u^3 = n_B(u)$ for $u \in U \cap B^\times$, hence for all $u \in U$. Since $u = d^{-1}\ell$, $n_B(u) = u^3$ lies in F .

Finally we have for $u \in U$

$$d^{-1}\tau(u)d = d\tau^{-1}(d^{-1}v)d = d^{-1}vd^{-1}d = d^{-1}v = u,$$

hence $U \subset H(B, \tau)$. ■

Let $B[X] = B \otimes F[X]$. For any $\xi \in B^\times, \theta \in B$, we have

$$X - \xi^{-i}\theta\xi^i = \xi^{-1-i}(\xi X - \xi\theta)\xi^i$$

Thus

$$(X - \xi^{-2}\theta\xi^2)(X - \xi^{-1}\theta\xi)(X - \theta) = \xi^{-3}(\xi X - \xi\theta)^3$$

In particular, for $w_1, w_2 \in U$, where U is the space defined in Lemma 5.5, we have, putting $\xi = w_1$ and $\theta = w_1^{-1}w_2$

$$(w_1X - w_2)^3 = w_1^3(X - w_1^{-2}\theta w_1^2)(X - w_1^{-1}\theta w_1)(X - \theta)$$

Lemma 5.6. Let $\theta_1 = \theta = w_1^{-1}w_2$, $\theta_2 = w_1^{-1}\theta w_1$, and $\theta_3 = w_1^{-2}\theta w_1^2$.

Then

$$(1) \text{Int}(w_1^{-1})(\theta_i) = \theta_{i+1 \pmod{3}} \quad \text{and}$$

$$w_1^{-3}(w_1X - w_2)^3 = (X - \theta_3)(X - \theta_2)(X - \theta_1)$$

is the reduced characteristic polynomial of θ_i , $i = 1, 2, 3$.

$$(2) t_B(\theta_i) = \theta_1 + \theta_2 + \theta_3 = t_B(w_1^{-1}w_2) \quad \text{and} \quad n_B(\theta_i) = \theta_{i+2}\theta_{i+1}\theta_i = w_1^{-3}w_2^3.$$

(3) For the involution $\tau' = \text{Int}(d^{-1}) \circ \tau$, where d is as in Lemma 5.5 we have $\tau'(\theta_2) = \theta_2$ and $\tau'(\theta_1) = \theta_3$.

(4) There exist $w_1, w_2 \in U$ linearly independent such that $t_B(w_1^{-1}w_2) = 0$. For such a choice we have $\theta_1 + \theta_2 + \theta_3 = 0$.

Proof. The first part of (1) is clear. We compute the generic characteristic polynomial of $\theta_1 = w_1^{-1}w_2$. Using that

$$(w_1X - w_2)^3 = n_{B[X]}(w_1X - w_2) \in F$$

by the choice of w_1 and $w_2 \in U$, and similarly $n_B(w_1) = w_1^3$, we get

$$n_{B[X]}(X - w_1^{-1}w_2) = (X - \theta_3)(X - \theta_2)(X - \theta_1),$$

hence $(X - \theta_3)(X - \theta_2)(X - \theta_1)$ is the generic polynomial of $\theta_1 = w_1^{-1}w_2$. Thus $t_B(\theta_1) = \theta_3 + \theta_2 + \theta_1$ and $n_B(\theta_1) = \theta_3\theta_2\theta_1 = w_1^{-3}w_2^3$. Conjugating with w_1^{-i} , $i = 1, 2$, gives the other formulas of (2). The claims in (3) follow from

$$\theta_2 = w_1^{-3}(w_1w_2w_1), \theta_1 = w_1^{-3}(w_1^2w_2), \theta_3 = w_1^{-3}(w_2w_1^2)$$

and the fact that τ' fixes U . We finally check (4). The linear map $x \mapsto t_B(w_1^{-1}x)$ on U has values in F . Since U is at least 2-dimensional there exists $0 \neq w_2 \in U$ with $t_B(w_1^{-1}w_2) = 0$. Since $t_B(z) = 3z \neq 0$ for $0 \neq z \in F$, w_1 and w_2 are linearly independent. ■

Proof of Theorem 5.4. Let $\theta_1, \theta_2, \theta_3$ be as in Lemma 5.6. Let $M = K(\theta_2^{-1}\theta_3)$ if $\theta_2^{-1}\theta_3 \notin K$ and $M = K(\theta_2)$ if $\theta_2^{-1}\theta_3 \in K$. We claim that $M \subset B$ is cyclic over K and S_3 -Galois over F . Assume first that $\theta_2^{-1}\theta_3 \notin K$, so that $\dim_K K(\theta_2^{-1}\theta_3) = 3$. Since

$$(*) \quad \text{Int}(w_1^{-1})(\theta_2^{-1}\theta_3) = \theta_3^{-1}\theta_1 = -\theta_3^{-1}(\theta_3 + \theta_2) = -1 + \theta_3 - \theta_2 \in K(\theta_2^{-1}\theta_3),$$

$\text{Int}(w_1^{-1})$ restricts to an automorphism ρ of $K(\theta_2^{-1}\theta_3)$. If ρ is the identity, (*) shows that $\theta_2^{-1}\theta_3$ satisfies the equation $y^2 + y + 1 = 0$. Since B is of degree 3 such an equation implies $\theta_2^{-1}\theta_3 \in K$, in contradiction to the assumption. Thus ρ is nontrivial of order 3. Furthermore we have for τ' :

$$\tau'(\theta_2^{-1}\theta_3) = \theta_1\theta_2^{-1} = \theta_2(\theta_2^{-1}\theta_1)\theta_2^{-1} = -\theta_2(1 + \theta_2^{-1}\theta_3)\theta_2^{-1}$$

so that $\tau'' = \text{Int}(\theta_2^{-1}) \circ \tau'$ satisfies

$$\tau''(\theta_2^{-1}\theta_3) = -(1 + \theta_2^{-1}\theta_3)$$

and defines an automorphism of order 2 of $K(\theta_2^{-1}\theta_3)$. To show that $\rho = \text{Int}(w_1^{-1})$ and τ'' generate a group isomorphic to S_3 , it suffices to verify that $\tau'' \circ \rho = \rho^2 \circ \tau''$.

We check it on the generator $\theta_2^{-1}\theta_3$:

$$\tau'' \circ \text{Int}(w_1^{-1})(\theta_2^{-1}\theta_3) = (\theta_2^{-1}\theta_3)(\theta_1^{-1}\theta_2) = (\theta_1^{-1}\theta_2)(\theta_2^{-1}\theta_3) = \theta_1^{-1}\theta_3$$

since $\theta_1^{-1}\theta_2 \in K(\theta_2^{-1}\theta_3)$. On the other hand $\text{Int}(w_1^{-2}) \circ \tau''(\theta_2^{-1}\theta_3) = \theta_1^{-1}\theta_3$.

Assum now that $\theta_2^{-1}\theta_3 = y \in K$. By Lemma 5.6, we must have $y^3 = 1$ (since $n_B(\theta_2) = n_B(\theta_3)$). If $y = 1$, we get $\theta_1 = \theta_2 = \theta_3$, a contradiction to $\theta_1 + \theta_2 + \theta_3 = 0$. Thus $y \in K$ is a primitive cubic root of 1. It follows from $\theta_3 = y\theta_2$ that $\theta_1 = y\theta_3$ and $\theta_2 = y\theta_1$. Thus $n_B(\theta_2) = \theta_1\theta_3\theta_2 = \theta_2^3$ and $\theta_2^3 \in K$. Since $\tau'(\theta_2) = \theta_2$, we even have $\theta_2^3 \in F$. Further we deduce from $\tau'(\theta_1) = \theta_3$ and $\theta_1 = y\theta_3$ that $\theta_3 = \tau(y)\theta_1$, so that $\tau(y) = y^2$ and $K = F(y)$. Thus we have $K(\theta_2) = K(\theta_3) = K(\theta_1)$ and the restriction ρ of $\text{Int}(w_1^{-1})$ to $K(\theta_2)$ is given by $\theta_2 \mapsto \theta_3 = y\theta_2$. It is then easy to check that $\{\tau', \rho\}$ generate a group of automorphisms of $K(\theta_2)$ isomorphic to S_3 . We now define $L \subset M$ as the subfield fixed under τ'' if $M = K(\theta_2^{-1}\theta_3)$, resp. under τ' if $M = K(\theta_2)$. We finally get $z \in B$ such that

$$B = M \oplus Mz \oplus Mz^2 = (M, a)$$

by taking $z = w_1^{-1}$; by construction $\rho = \text{Int}(z)$ and, since $w_1 \in U$, $w_1^3 = n_B(w_1) \in F^\times$ by Lemma 5.5, hence $a \in F^\times$. ■

Remarks. (1) We have used the existence of an involution τ of the second kind in the proof. However the result does not say anything about τ .

(2) Wedderburn's theorem is a special case of Albert's theorem, taking $K = F \times F$ and $B = A \times A^{\text{op}}$.

6. The trace form

As already noticed, we have a 9-dimensional bilinear trace form on the F -space $S = H(B, \tau)$ of symmetric elements. The next aim will be to compute this form. We begin with two special cases:

Assume first that $B = M_3(K)$ is split. By the theorem of Skolem-Noether any involution τ of the second kind on B is of the form

$$\tau_a(x) = ax^*a^{-1}$$

with $x^* = (\bar{a}_{ij})^t$ for $x = (a_{ij})$ and $a = a^*$. Thus a is a hermitian matrix and is isometric to a diagonal matrix $a' = \text{diag}(\alpha_1, \alpha_2, \alpha_3)$ with $\alpha_i \in F^\times$. There exists $u \in \text{GL}_3(K)$ such that $a' = uau^*$ and $\int(u)$ is an isomorphism of τ_a and $\tau_{a'}$. Thus we may assume that a is diagonal. The symmetric elements of $(M_3(K), \tau_a)$ are then represented as matrices

$$a = \begin{pmatrix} x_1 & k_3 & \alpha_1^{-1}\alpha_3k_2 \\ \alpha_2^{-1}\alpha_1\bar{k}_3 & x_2 & k_1 \\ k_2 & \alpha_3^{-1}\alpha_2\bar{k}_1 & x_3 \end{pmatrix} \quad b = \begin{pmatrix} y_1 & r_3 & \alpha_1^{-1}\alpha_3r_2 \\ \alpha_2^{-1}\alpha_1\bar{r}_3 & y_2 & r_1 \\ r_2 & \alpha_3^{-1}\alpha_2\bar{r}_1 & y_3 \end{pmatrix}$$

and the bilinear trace form is given by

$$\begin{aligned} t_S(a, b) &= x_1y_1 + x_2y_2 + x_3y_3 + \alpha_3^{-1}\alpha_2b_K(k_1, r_1) + \alpha_1^{-1}\alpha_3b_K(k_2, r_2) \\ &\quad + \alpha_2^{-1}\alpha_1b_K(k_3, r_3) \end{aligned}$$

where $b_K(k, r) = k\bar{r} + \bar{k}r$. If $K = F(\sqrt{\alpha})$ (assuming $\text{char } F \neq 2$), $b_K \simeq \langle 2, -2\alpha \rangle$ and

$$t_S \simeq \langle 1, 1, 1 \rangle \perp \langle 2, -2\alpha \rangle \otimes \langle \alpha_3^{-1}\alpha_2, \alpha_1^{-1}\alpha_2, \alpha_2^{-1}\alpha_1 \rangle$$

hence is of the form

$$t_S \simeq \langle 1, 1, 1 \rangle \perp \langle 2, -2\alpha \rangle \otimes \langle \beta_1, \beta_2, \beta_3 \rangle \quad \text{with } \beta_1\beta_2\beta_3 = 1$$

We claim that this is true for an arbitrary (B, τ) . In fact a corresponding result holds for arbitrary degrees but even for degree 3 we do not have a simpler proof. The strategy will be to fix a cubic étale F -algebra $L \subset S = H(B, \tau)$ and to study the orthogonal complement $V = L^\perp$. The existence of such an algebra L

can be directly checked if $B = M_3(K)$ is split and, if B is a division algebra, any $x \in S, x \notin F$, will generate such an algebra, since we assume $\text{char } F \neq 3$. We begin with some preliminary results.

Lemma 6.1. Let $L \subset H(B, \tau)$ be cubic étale over F and let $R = L \otimes L \otimes K$. Then B is a free R -module via left and right multiplication; the action is equivariant with respect to the involution τ on B and the action $\sigma : R \rightarrow R$ given by $\sigma(\lambda \otimes \mu \otimes x) = \mu \otimes \lambda \otimes \bar{x}$. In particular we have an induced action of the invariant ring R^σ on $H(B, \tau)$.

Proof. Since all actions are explicitly defined it suffices to check the claimed properties over a separable closure F_{sep} of F , so that we even may assume that F is separably closed. Then $K \simeq F \times F, B = B_1 \times B_2$ and $\tau(B_1 \times \{0\}) = \tau((B_1 \times B_2)(1, 0)) = (0, 1) \cdot (B_1 \times B_2) = \{0\} \times B_2$. It follows that B_1 and B_2 are antiisomorphic. Let

$$f : B_1^{\text{op}} \xrightarrow{\sim} B_2$$

be defined by $\tau(x, 0) = (0, f(x^{\text{op}}))$. We identify now $B_1 \times B_2$ with $B_1 \times B_1^{\text{op}}$ by mapping (x_1, x_2) to $(x_1, f^{-1}(x_2))$. Under this map τ is identified with the switch

$$(x_1, x_2^{\text{op}}) \mapsto (x_2, x_1^{\text{op}})$$

(see Example 5.1., (3)) and we have $L = \{(\ell, \ell^{\text{op}}) \mid \ell \in L_2\}$ for some $L_2 \subset M_3(F)$ cubic étale. Since F is separably closed $L_2 \simeq F \times F \times F$ is given by three idempotents of $M_3(F)$. These three idempotents can be mapped by an automorphism of $M_3(F)$ to the three diagonal idempotents. Since any automorphism of $M_3(F)$ extends to an automorphism of $M_3(F) \times M_3(F)^{\text{op}}$ as algebra with involution, we may assume that

$$L = \{(\ell, \ell^{\text{op}}) \mid \ell \in M_3(F) \text{ is diagonal.}\}$$

Let L' be the set of diagonal matrices in $M_3(F)$. We have

$$M_3(F) = L' \otimes L'x + L'x^2$$

where x is a permutation matrix of order 3, for example $x = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}$ (see p.15). Then $\xi = 1 + x + x^2$ is a free generator of $M_3(F)$ as $L' \otimes L'$ -module and (ξ, ξ^{op}) is a free generator of B as $L \otimes L \otimes K$ -module. ■

Let again $L \subset H(B, \tau)$ be cubic étale over F and let t_L the trace, n_L the norm of L . The restriction of the bilinear trace form t_B to L is t_L , hence is nonsingular and we have an orthogonal decomposition

$$H(B, \tau) = L \perp V$$

For $v \in V$, let $Q(v) = \frac{1}{2}t_B(v^2) - \pi_L(v^2) \in L$ where π_L is the orthogonal projection $H(B, \tau) \rightarrow L$. We define an action of L on V such that (V, Q) is a nonsingular quadratic space of rank 2 over L . We recall that (see section 3)

$$L \otimes L = L \times L \otimes \Delta(L)$$

with the following properties:

(1) the twist $x \otimes y \mapsto y \otimes x$ restricts on $\Delta(L)$ to the conjugation $a \mapsto \bar{a}$.

(2) there are three embeddings of L in $L \otimes \Delta(L)$. Two of them are given by $x \mapsto \text{pr}(x \otimes 1)$ and $y \mapsto \text{pr}(1 \otimes y)$, where $\text{pr}: L \otimes L \rightarrow L \otimes \Delta(L)$ is the projection and the third, the L -action on $L \otimes \Delta(L)$, corresponds to

$$\ell \mapsto t_L(\ell) \cdot 1 - \text{pr}(\ell \otimes 1) - \text{pr}(1 \otimes \ell)$$

[the last claim follows from the fact that the sum of the three must be the trace] and is invariant under the twist.

We have an induced decomposition for R as in Lemma 6.1

$$R = L \otimes L \otimes K = L \otimes K \times L \otimes \Delta(L) \otimes K$$

The action σ described in Lemma 6.1 restricts on $L \otimes \Delta(L) \otimes K$ to $\lambda \otimes x \otimes y \mapsto \lambda \otimes \bar{x} \otimes \bar{y}$, so that the fixed algebra is

$$R^\sigma = L \times L \otimes H$$

where $H = \Delta(L) * K = F(\sqrt{\alpha\delta})$ if $K = F(\sqrt{\alpha})$ and $\Delta(L) = F(\sqrt{\delta})$.

Lemma 6.2. The decomposition of the R -module B induced by the decomposition $R = L \otimes K \times L \otimes \Delta(L) \otimes K$ reduces to the decomposition

$$B = L \otimes K \perp V \otimes K$$

over K . In particular $R^\sigma = L \times L \otimes H$ acts on $H(B, \sigma)$ componentwise and V is a free $L \otimes H$ -module of rank one. The action of L on V is given by

$$\ell \circ v = t_L(\ell)v - lv - v\ell.$$

Proof. By Lemma 6.1 and the consideration before Lemma 6.2. ■

Lemma 6.3. (V, Q) is a quadratic space over L for the action $\ell \circ v = t_L(\ell)v - lv - v\ell$ described in Lemma 6.2 and

$$t_{H(B, \tau)}((\ell_1, v_1), (\ell_2 v_2)) = t_L(\ell_1, \ell_2) + t_L(Q(v_1, v_2)),$$

where $Q(v_1, v_2) = Q(v_1 + v_2) - Q(v_1) - Q(v_2)$. Furthermore, we have $Q(hv) = n_H(h)Q(v)$ for $h \in H = F(\sqrt{\alpha\delta})$ and $v \in V$.

Proof. By going to a separable closure we may, as in the proof of Lemma 6.1, assume that $B = M_3(K)$, where $K = F \times F$, τ is the switch and $L = \{(\ell, \ell^{\text{op}} \mid \ell \text{ diagonal})\}$. Then V can be identified with the set of matrices

$$v = \begin{pmatrix} 0 & \bar{c}_3 & c_2 \\ c_3 & 0 & \bar{c}_1 \\ \bar{c}_2 & c_1 & 0 \end{pmatrix}, \quad c_i \in K$$

and the action of L on V is

$$(\lambda_1, \lambda_2, \lambda_3) \circ \begin{pmatrix} 0 & \bar{c}_3 & c_2 \\ c_3 & 0 & \bar{c}_1 \\ \bar{c}_2 & c_1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & \lambda_3 \bar{c}_3 & \lambda_2 c_2 \\ \lambda_3 c_3 & 0 & \lambda_1 \bar{c}_1 \\ \lambda_2 \bar{c}_2 & \lambda_1 c_1 & 0 \end{pmatrix}$$

We further have $Q(v) = (c_1\bar{c}_1, c_2\bar{c}_2, c_3\bar{c}_3)$, so that

$$t_L(Q(v)) = c_1\bar{c}_1 + c_2\bar{c}_2 + c_3\bar{c}_3$$

and the formula for $t_{H(B,\tau)}$ follows from the computation in the split case given at the beginning of this section. Finally, we have $H = K$, since $\Delta(L) \simeq F \times F$ and K acts componentwise on v , so that $Q(kv) = k\bar{k}Q(v) = n_K(k)Q(v)$ as claimed. ■

The quadratic space (V, Q) is attached to a given étale F -algebra $L \subset H(B, \tau)$. Assume now that $L \subset H(B, \tau')$ for another involution τ' . Writing $\tau' = \text{Int}(z) \circ \tau$, the fact that $\tau'|_L = \text{Id}_L$ implies that $z \in L^\times$. Let now

$$q : L \rightarrow L$$

be the quadratic map such that $\ell q(\ell) = n_L(\ell)$ for all $\ell \in L$. For example

$$q(x_1, x_2, x_2) = (x_2x_3, x_3x_1, x_1x_2)$$

if $L = F \times F \times F$.

Lemma 6.4. Let $V' = L^\perp \subset H(B, \tau')$. Putting

$$Q'(v') = \frac{1}{2}t_B(v'^2) - \pi'_L(v'^2), \quad v' \in V'$$

where π'_L is the projection $H(B, \tau') \rightarrow V'$, the map $v \mapsto zv$ is an isomorphism $V \xrightarrow{\sim} V'$ such that

$$Q'(zv) = q(z)Q(v), \quad v \in V.$$

Thus, $v \mapsto zv$ is a similitude $(V, Q) \xrightarrow{\sim} (V', Q')$ with factor $q(z) \in L^\times$.

Proof. As in the proof of Lemma 6.3 we may go to a separable closure and check the claim by explicit computations. ■

For any bilinear form b over L , let $(T_L)_*(b)$ be the form over F given by $(T_L)_*(b(x, y)) = T_L((b(x, y)))$.

Theorem 6.5. The bilinear form $Q(v_1, v_2)$ over L has a diagonalization

$$\langle 2, -2\alpha\delta \rangle \otimes \langle \lambda \rangle$$

for some $\lambda \in L^\times$ such that $n_L(\lambda) \in F^{\times 2}$, so that

$$t_{H(B,\tau)} \simeq \langle 1, 2, 2\delta \rangle \perp \langle 2, -2\alpha\delta \rangle \otimes t_L(\langle \lambda \rangle_L)$$

Proof. Let $v \in V$ be such that $Q(v)$ is invertible in L . Then v is a basis of V as $L \otimes H$ -module, hence gives a diagonalization as wanted, putting $\lambda = Q(v)$. To get $n_L(\lambda) \in F^{\times 2}$, we observe that

$$n_L(Q(\pi_V(v^2))) = n_L(Q(v))^2,$$

where $\pi_V : H(B, \tau) \rightarrow V$ is the orthogonal projection on V . This can be checked over an algebraic closure, using the explicit computation on page 30. The element $v_1 = \pi_V(v^2)$ is also a basis of V as $L \otimes H$ -module, so that we get the first claim for $\lambda = Q(\pi_V(v^2))$. The last claim follows from Lemma 6.3 and Frobenius reciprocity (see [S], Scharlau, p.48).

Theorem 6.6. There exists $\lambda \in L$ such that $n_L(\lambda) \in F^{\times 2}$ so that

$$t_{H(B,\tau)} \simeq \langle 1, 1, 1 \rangle \perp \langle 2\delta \rangle \otimes \langle 1, -\alpha \rangle \otimes t_L(\langle \lambda \rangle_L).$$

In particular $t_{H(B,\tau)}$ is of the form

$$t_{H(B,\tau)} \simeq \langle 1, 1, 1 \rangle \perp \langle 2, -2\alpha \rangle \otimes \langle \beta_1, \beta_2, \beta_3 \rangle \quad \text{with}$$

$$\beta_1\beta_2\beta_3 = 1.$$

The proof of Theorem 6.6 uses techniques from the theory of symmetric bilinear forms. We recall that the forms

$$h_n = \langle 1, -1 \rangle \perp \dots \perp \langle 1, -1 \rangle$$

of dimension $2n$ is called *hyperbolic*. Two forms f and g are *Witt equivalent* if

$$f \perp h_n \simeq g \perp h_\ell$$

for hyperbolic forms h_n, h_ℓ . We have an addition on Witt equivalence classes

$$[f] + [g] = [f \perp g]$$

Since $f \perp -f \simeq h_n$, with $n = \dim f$, we get a group structure on the set $W(F)$ of equivalence classes, putting $-[f] = [-f]$ and $0 = [h_n]$. The corresponding group is the *Witt group* of F . Since *Witt cancellation*

$$f \perp g \simeq f' \perp g \Rightarrow f \simeq f'$$

holds, we see that $[f] = [f']$ and $\dim f = \dim f'$ implies $f \simeq f'$. Furthermore, for any finite field extension \overline{F}/F the *transfer map*

$$W(\overline{F}) \rightarrow W(F).$$

defined as $f \mapsto t_{\overline{F}} \circ f$, is a group homomorphism. Let in particular $\overline{F} = F(\sqrt{\delta})$. By Scharlau [S] p. 50, the image of the transfer map

$$W(F(\sqrt{\delta})) \rightarrow W(F)$$

is killed by $\langle 1, -\delta \rangle$. Another result we shall use is the fact that if $\lambda_0 \in F^\times$ is a norm from $F(\sqrt{\delta})$, i.e. $\lambda_0 = x^2 - \delta y^2, x, y \in F$, then

$$\langle \lambda_0 \rangle \otimes \langle 1, -\delta \rangle \simeq \langle 1, -\delta \rangle.$$

Lemma 6.7. Let L be cubic étale over F and let $\lambda \in L^\times$ be such that $n_L(\lambda) \in F^{\times 2}$. Then

$$[\langle 1, -\delta \rangle \otimes t_L(\langle \lambda \rangle)] = [\langle 1, -\delta \rangle]$$

in $W(F)$.

Proof. By Springer's theorem, it suffices to check the claim over L , hence we may assume that $L = F \times K$ with $K = F(\sqrt{\delta})$. Let $\lambda = (\lambda_0, \lambda_1) \in F \times K$; then

$$t_L(\langle \lambda \rangle) = \langle \lambda_0 \rangle \perp t_K(\langle \lambda_1 \rangle)$$

and, as above observed, $t_K(\langle \lambda_1 \rangle)$ is killed by $\langle 1 - \delta \rangle$.

On the other hand

$$n_L(\lambda) = \lambda_0 n_K(\lambda_1) \in F^{\times 2},$$

hence λ_0 is a norm from K , so that

$$\langle 1, -\delta \rangle \otimes \langle \lambda_0, -1 \rangle = 0$$

which implies the claim. ■

Proof of Theorem 6.6. We have

$$\langle 1, -\alpha\delta \rangle = \langle 1, -\alpha \rangle \cdot \langle \delta \rangle + \langle 1, -\delta \rangle$$

in $W(F)$, hence

$$\begin{aligned} t_{H(B,\tau)} &= \langle 1, 2, 2\delta \rangle + \langle 2 \rangle \cdot \langle 1, -\alpha\delta \rangle \cdot t_L(\langle \lambda \rangle) \\ &= \langle 1, 2, 2\delta \rangle + \langle 2\delta \rangle \langle 1, -\alpha \rangle \cdot t_L(\langle \lambda \rangle) + \langle 2 \rangle \cdot \langle 1, -\delta \rangle \cdot t_L(\langle \lambda \rangle) \\ &= \langle 1, 2, 2\delta \rangle + \langle 2\delta \rangle \langle 1, -\alpha \rangle t_L(\langle \lambda \rangle) + \langle 2 \rangle \langle 1, -\delta \rangle \end{aligned}$$

by Lemma 6.7. Further we have in the Witt group

$$\langle 2\delta \rangle + \langle 2 \rangle \cdot \langle 1 - \delta \rangle = \langle 2 \rangle \quad \text{and} \quad \langle 1, 2, 2 \rangle = \langle 1, 1, 1 \rangle$$

which implies that

$$t_{H(B,\tau)} \simeq \langle 1, 1, 1 \rangle \perp \langle 2\delta \rangle \otimes \langle 1, -\alpha \rangle \otimes t_L(\langle \lambda \rangle_L)$$

In particular $t_{H(B,\tau)}$ is of the form

$$t_{H(B,\tau)} \simeq \langle 1, 1, 1 \rangle \perp \langle 2, -2\alpha \rangle \otimes \langle \beta_1, \beta_2, \beta_3 \rangle$$

putting $\langle \delta \rangle \otimes T_L(\langle \lambda \rangle_L) = \langle \beta_1, \beta_2, \beta_3 \rangle$. The fact that $\beta_1\beta_2\beta_3 = 1$ follows from

Lemma 6.8. For L/F cubic étale and $\lambda \in L^\times$ we have

$$\det(t_L(\langle \lambda \rangle_L)) \equiv \delta n_L(\lambda) \pmod{F^{\times 2}}$$

where $\Delta(L) = F(\sqrt{\delta})$.

Proof. As in the proof of Lemma 6.7 we may assume that $L = F \times K$ with $K = F(\sqrt{\delta})$. Let $\lambda = (\lambda_0, \lambda_1)$, $\lambda_0 \in F$, $\lambda_1 \in K$ and put $\lambda_1 = \xi_1 + \xi_2\sqrt{\delta}$ with $\xi_1, \xi_2 \in F$. The matrix of $t_L(\langle \lambda \rangle)$ with respect to the basis $\{(1, 0), (0, 1), (0, \sqrt{\delta})\}$ of L is

$$\begin{pmatrix} \lambda_0 & 0 & 0 \\ 0 & 2\xi_1 & 2\delta\xi_2 \\ 0 & 2\delta\xi_2 & 2\delta\xi_1 \end{pmatrix}$$

so that $\det(t_L(\langle \lambda \rangle)) = 4\lambda_0\delta(\xi_1^2 - \delta\xi_2^2) = 4\delta\lambda_0n_K(\lambda_1) = 4\delta n_L(\lambda)$. \blacksquare

Theorem 6.9. Let τ, τ' be two involutions on B such that $\tau|_L = \tau'|_L = Id_L$ so that $\tau' = \text{Int}(z) \circ \tau$ for $z \in L^\times$. If $\lambda \in L^\times$ is such that

$$t_{H(B, \tau)} \simeq \langle 1, 1, 1 \rangle \perp \langle 2\delta \rangle \otimes \langle 1, -\alpha \rangle \otimes t_L(\langle \lambda \rangle_L)$$

then

$$t_{H(B, \tau')} \simeq \langle 1, 1, 1 \rangle \perp \langle 2\delta \rangle \otimes \langle 1, -\alpha \rangle \otimes t_L(\langle q(z)\lambda \rangle_L)$$

Proof. By Lemma 6.4 and Theorem 6.5 $\lambda = Q(v_1)$ has to be replaced by $Q(zv_1) = q(z)\lambda$. \blacksquare

Theorem 6.6. has the following converse, which shows that the expression given for the trace form is not as exotic as it may appear first.

Theorem 6.10. Let B central simple of degree 3 with an involution of second kind. Let L be an arbitrary étale F -algebra in B . For every $\lambda \in L^\times$ such that $n_L(\lambda) \in F^{\times 2}$, there is an involution τ on B leaving L elementwise invariant and such that

$$t_{H(B, \tau)} \simeq \langle 1, 1, 1 \rangle \perp \langle 2\delta \rangle \otimes \langle 1, -\alpha \rangle \otimes t_L(\langle \lambda \rangle_L)$$

Proof. We first check that there exists an involution τ_1 which leaves L invariant. Let τ_2 be a involution of second kind of B (such a τ_2 exists by hypothesis). Let

$L = F(\xi)$, $\xi \in B$, and let

$$W = \{x \in L \mid \tau_2(x) = x \text{ and } x\tau_2(\xi) = \xi x\}$$

If W contains an invertible element z , then $\text{Int}(z) \circ \tau_2 = \tau_1$ leaves ξ , hence L invariant. W is a vector space over F in which the invertible elements form a Zariski open set. In order to prove that this set is not empty we may extend scalars from F to an algebraic closure and assume that $B = M_3(F) \times M_3(F)^{\text{op}}$. Let $\xi = (y_1, y_2^{\text{op}})$ and let $u \in M_3(F)$ be such that $uy_2u^{-1} = y_1$. If ε is the switch involution on B , then $\text{Int}(u, u^{\text{op}}) \circ \varepsilon$ leaves ξ invariant. This involution is of the form $\text{Int}(z) \circ \tau_2$ and z is as wanted. Let now $\mu \in L^\times$ be such that $n_L(\mu) \in F^{\times 2}$ and

$$t_{H(B, \tau_1)} \simeq \langle 1, 1, 1 \rangle \perp \langle 2\delta \rangle \otimes \langle 1, -\alpha \rangle \otimes t_L(\langle \mu \rangle_L)$$

Let $\nu \in F^\times$ be such that $n_L(\lambda\mu^{-1}) = \nu^2$. We have

$$\lambda\mu^{-1} = \nu^2 q(\lambda\mu^{-1}) = q(\nu\lambda^{-1}\mu)$$

where $q(\ell) \cdot \ell = n_L(\ell)$. Then $\tau = \text{Int}(\nu\lambda^{-1}\mu) \circ \tau_1$ has by Theorem 6.9 the wanted trace form. ■

Example. Let (B, τ) be as in Example 5.2, i.e.

$$B = M \oplus Mz \oplus Mz^2$$

where M is cyclic over $K = F(\sqrt{\alpha})$ and is an S_3 -Galois algebra over F . Furthermore we have $M = L \otimes K$ where

$$L = \{x \in M \mid \tau(x) = x\} \subset H(B, \tau)$$

has discriminant algebra K . The involution τ is such that $\tau(z) = z$. For $x \in M$ we have $\tau(xz) = \rho\tau(x)z$, where $\rho(x) = zxz^{-1}$ and similarly $\tau(xz^2) = \rho^2\tau(x)z$. It follows that

$$H(B, \tau) = L \oplus \rho^2(L)z \oplus \rho(L)z^2$$

and $V = \rho^2(L)z \oplus \rho(L)z^2$ is an L -module through the action

$$\ell \circ v = \rho^2(\ell)x_1z + \rho(\ell)x_2z \text{ if } v = x_1z + x_2z^2$$

Observe that we have in fact $\ell \circ v = t_L(\ell)v - \ell v - v\ell$ since

$$\ell v = \ell x_1 z + \ell x_2 z^2 \quad \text{and} \quad v\ell = \rho(\ell)x_1 z + \rho^2(\ell)x_2 z^2$$

and $t_L(\ell) = \ell + \rho(\ell) + \rho^2(\ell)$ since $t_M|_L = t_L$ and

$$t_M(x) = x + \rho(x) + \rho^2(x),$$

M being Galois over K . We next compute $Q(v)$. We have

$$v^2 = [\rho^2(\ell_1 \ell_2) + \rho(\ell_1 \ell_2)]a + a\rho(\ell_2)\ell_2 z + \rho^2(\ell_1)\ell_1 z^2$$

for $v = \rho^2(\ell_1)z + \rho(\ell_2)z^2$. Since

$$(xz)^3 = n_B(x)a \in K \quad \text{and} \quad (xz^2)^3 = n_B(x)a^2 \in K$$

for $x \in M$, we have $t_B(xz) = 0 = t_B(xz^2)$ and

$$Q(v) = \frac{1}{2}t_B(v^2) - \pi_L(v^2) = \ell_1 \ell_2 \quad \text{for} \quad v = \rho^2(\ell_1)z + \rho(\ell_2)z^2.$$

Thus $(V, Q) \simeq h_1 \simeq \langle 1, -1 \rangle$ is hyperbolic of rank 2. Observe that $\alpha \equiv \delta \pmod{F^{\times 2}}$ since $\Delta(L) = K$, so that, taking $\lambda = 1$ in Theorem 6.6, we get

$$\begin{aligned} \langle 2 \rangle \otimes \langle 1, -\alpha \rangle \otimes t_L(\langle 1 \rangle) &= \langle 2, -2\delta \rangle \otimes \langle \delta, 2\delta, 2 \rangle \\ &\simeq \langle 2\delta, -2, 4\delta, -4, 4, -4\delta \rangle \\ &\simeq \langle 2, -2\delta \rangle \otimes \langle -1, -1, 1 \rangle \end{aligned}$$

using that $\langle x, -x \rangle \simeq \langle 1, -1 \rangle$ for any $x \in F^\times$. Thus

$$t_{H(B, \tau)} \simeq \langle 1, 1, 1 \rangle \perp \langle 2, -2\alpha \rangle \otimes \langle -1, -1, 1 \rangle$$

in this example. The condition Q hyperbolic over L is in fact characteristic for algebras as in Example 5.2:

Theorem 6.11. Let $K = F(\sqrt{\alpha})$ be a field and let $L \subset H(B, \tau)$ be such that $\Delta(L) \simeq F(\sqrt{\delta})$. The following conditions are equivalent

- (1) (V, Q) is hyperbolic over L ;
- (2) $\delta = \alpha$ in $F^\times / F^{\times 2}$;

(3) LK is cyclic over K and S_3 -Galois over F .

Moreover, if these conditions hold, then B is a cyclic algebra

$$B = LK \oplus LKz \oplus LKz^2$$

for some z such that $z^3 \in F$ and $\tau(z) = z$.

Proof. (1) \Leftrightarrow (2) follows from Theorem 6.5, since $\langle x, y \rangle$ is hyperbolic if and only if $xy = -1$ in $F^\times/F^{\times 2}$.

(2) \Rightarrow (3): The discriminant of LK over K is $\Delta(L) \otimes K$ and $\Delta(L) \otimes K \simeq K \times K$ if $\delta = \alpha$ in $F^\times/F^{\times 2}$. Hence LK is cyclic since it has trivial discriminant. Let $\rho \in \text{Aut}_K(LK)$ be a generator of the Galois group $\text{Gal}(LK/K)$. The restriction σ of τ to LK is an automorphism of order 2 and $\sigma\rho \neq \rho\sigma$, since L/F is not Galois (having discriminant $K \not\cong F \times F$). Thus $\{\rho, \tau\}$ generates a group of automorphisms of LK of order at least 6; since $[LK : F] = 6$ it must be S_3 . We next show that B contains an invertible element z such that $\tau(z) = z$ and $z\ell = \rho(\ell)z$ for all $\ell \in LK$. These relations imply that z^3 centralizes LK , is τ -symmetric and commutes with z , hence $z^3 \in F$. Let

$$Z = \{z \in H(B, \tau) \mid z\ell = \rho(\ell)z \text{ for all } \ell \in LK\}$$

This is a vector space over F in which the invertible elements form a Zariski open set. In order to prove that this set is not empty we may extend scalars from F to an algebraic closure and assume $B = M_3(F) \times M_3(F)^{\text{op}}$, σ is the switch involution and $L = \{d, d^{\text{op}} \mid d \in M_3(F) \text{ diagonal}\}$. We may further assume that

$$\rho(\text{diag}(\alpha_1, \alpha_2, \alpha_3), \text{diag}(\alpha'_1, \alpha'_2, \alpha'_3)^{\text{op}}) = (\text{diag}(\alpha_3, \alpha_1, \alpha_2), \text{diag}(\alpha'_2, \alpha'_3, \alpha'_1)^{\text{op}})$$

We may then choose

$$z = \left(\left(\begin{array}{ccc} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{array} \right), \left(\begin{array}{ccc} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{array} \right)^{\text{op}} \right)$$

It follows that B is a cyclic algebra, as claimed. Finally (3) \Rightarrow (1) follows from the explicit computations given in the example above \blacksquare .

7. A Classification of involutions in degree 3. Let (B, τ) be central simple of degree 3 over $K = F(\sqrt{\alpha})$ with τ an involution of the second kind. We assume that $\text{char} F \neq 2, 3$. By Theorem 6.6, we have

$$t_{H(B, \tau)} \simeq \langle 1, 1, 1 \rangle \perp \langle 2 \rangle \otimes \langle 1, -\alpha \rangle \otimes \langle -b, -c, bc \rangle$$

for some $b, c \in F^\times$. We introduce some new notations. We set

$$\langle \langle \alpha \rangle \rangle = \langle 1, -\alpha \rangle \quad \text{and} \quad \langle \langle \alpha_1, \dots, \alpha_n \rangle \rangle = \langle \langle \alpha_1 \rangle \rangle \otimes \dots \otimes \langle \langle \alpha_n \rangle \rangle$$

for $\alpha_1, \dots, \alpha_n \in F^\times$. The bilinear form $\langle \langle \alpha_1, \dots, \alpha_n \rangle \rangle$ is 2^n -dimensional and is called a n -Pfister form. Examples are given by the norm of quadratic, quaternion and octonion algebras. Let $n_K, n_Q, n_{\mathcal{O}}$ resp. be the norm $n(x) = x\bar{x}$ of such an algebra and let $b_K, b_Q, b_{\mathcal{O}}$ resp. be defined by

$$b(x, y) = \frac{1}{2}[n(x+y) - n(x) - n(y)]$$

Then $b_K = \langle \langle a \rangle \rangle$ if $K = F(\sqrt{a})$, $b_Q = \langle \langle a, b \rangle \rangle$ if $Q = (a, b)_F$ and $b_{\mathcal{O}} = \langle \langle a, b, c \rangle \rangle$ if $\mathcal{O} = (a, b, c)_F$. Observe that in these cases the Pfister form is either anisotropic (if the algebra is a division algebra) or hyperbolic. This is true in general (see Scharlau). We further set

$$\langle \langle \alpha_1, \dots, \alpha_n \rangle \rangle' = \langle 1 \rangle^\perp,$$

so that, for example, $\langle \langle b, c \rangle \rangle' = \langle -b, -c, bc \rangle$. It follows that the trace bilinear form of $H(B, \tau)$ has the form

$$t_{H(B, \tau)} = \langle 1, 1, 1 \rangle \perp \langle 2 \rangle \otimes \langle \langle \alpha \rangle \rangle \otimes \langle \langle b, c \rangle \rangle'$$

Finally we need one more notation. If $\langle a_1, \dots, a_n \rangle$ is a bilinear form over F , we denote by $\langle a_1, \dots, a_n \rangle_K$ its extension to K as a hermitian form, i.e

$$(x, y) \mapsto \sum \bar{x}_i a_i y_i, \quad x = (x_1, \dots, x_n), \quad y = (y_1, \dots, y_n).$$

The main result of this section is:

Theorem 7.1. Let τ, τ' be involutions of the second kind on a central simple K -algebra B of degree 3. Let

$$t_{H(B,\tau)} = \langle 1, 1, 1 \rangle \perp \langle 2 \rangle \otimes \langle \langle \alpha \rangle \rangle \otimes \langle \langle b, c \rangle \rangle'$$

and

$$t_{H(B,\tau')} = \langle 1, 1, 1 \rangle \perp \langle 2 \rangle \otimes \langle \langle \alpha \rangle \rangle \otimes \langle \langle b', c' \rangle \rangle'$$

The following conditions are equivalent:

- (1) the involutions τ and τ' are isomorphic, i.e. there exists an automorphism φ of B such that $\tau' \circ \varphi = \varphi \circ \tau$;
- (2) the bilinear forms $t_{H(B,\tau)}$ and $t_{H(B,\tau')}$ are isometric;
- (3) the bilinear forms $\langle \langle \alpha \rangle \rangle \otimes \langle \langle b, c \rangle \rangle'$ and $\langle \langle \alpha \rangle \rangle \otimes \langle \langle b', c' \rangle \rangle'$ are isometric;
- (4) either $K = F \times F$ or the K -hermitian forms $\langle -b, -c, bc \rangle_K$ and $\langle -b', -c', b'c' \rangle_K$ are isometric
- (5) the Pfister forms $\langle \langle \alpha, b, c \rangle \rangle$ and $\langle \langle \alpha, b', c' \rangle \rangle$ are isometric.

Proof. (1) \Rightarrow (2) let $\varphi(x) = uxu^{-1}, x \in B$, by Skolem-Noether. Then φ maps $H(B, \tau)$ to $H(B, \tau')$ and

$$\begin{aligned} t_{H(B,\tau')}(\varphi(x), \varphi(y)) &= t_{H(B,\tau)}(uxu^{-1}, uyu^{-1}) \\ &= t_B\left(\frac{uxu^{-1}uyu^{-1} + uyu^{-1}uxu^{-1}}{2}\right) \\ &= t_B\left(\frac{xy + yx}{2}\right) = t_{H(B,\tau)}(x, y) . \end{aligned}$$

Now (2) \Leftrightarrow (3) \Leftrightarrow (5) follows by Witt cancellation for quadratic forms and (3) \Leftrightarrow (4) is a theorem of Jacobson ([J]) if K is a field and is clear if $K = F \times F$. We finally check that (4) \Rightarrow (1). If $K = F \times F$ all involutions on $B \simeq A \times A^{\text{op}}$ are isomorphic to the switch involution so (1) is clear. Thus we may assume that K is a field. Assume next that $B = M_3(K)$ is split. Up to automorphisms of (B, τ) , resp. (B, τ') , we may assume that $\tau = \tau_a$, i.e $\tau(x) = ax^*a^{-1}$ with $a = \text{diag}(\alpha_1, \alpha_2, \alpha_3)$ and

$\tau' = \tau_{a'}$ with $a' = \text{diag}(\alpha'_1, \alpha'_2, \alpha'_3)$. We may further assume $\alpha_1\alpha_2\alpha_3 = \alpha'_1\alpha'_2\alpha'_3$, since a , resp. a' , is only determined up to a scalar. In view of the example at the very beginning of section 6 we have

$$t_{H(B,\tau)} \simeq \langle 1, 1, 1 \rangle \perp \langle 2 \rangle \otimes \langle \langle \alpha \rangle \rangle \otimes \langle \alpha_2\alpha_3^{-1}, \alpha_3\alpha_1^{-1}, \alpha_1\alpha_2^{-1} \rangle$$

and

$$t_{H(B,\tau')} \simeq \langle 1, 1, 1 \rangle \perp \langle 2 \rangle \otimes \langle \langle \alpha \rangle \rangle \otimes \langle \alpha'_2\alpha_3'^{-1}, \alpha'_3\alpha_1'^{-1}, \alpha'_1\alpha_2'^{-1} \rangle$$

so that, by Witt cancellation, we have an isomorphism

$$\langle \alpha_1\alpha_3^{-1}, \alpha_3\alpha_1^{-1}, \alpha_1^{-1}\alpha_2 \rangle_K \simeq \langle \alpha'_2\alpha_3^{-1}\alpha'_3\alpha_1^{-1}, \alpha'_1\alpha_2'^{-1} \rangle_K$$

of K -hermitian forms. Since

$$\langle \alpha_1\alpha_2\alpha_3 \rangle \otimes \langle \alpha_2\alpha_3^{-1}, \alpha_3\alpha_1^{-1}, \alpha_1^{-1}\alpha_2 \rangle \simeq \langle \alpha_1, \alpha_2, \alpha_3 \rangle_K$$

the two K -hermitian forms $\langle \alpha_1, \alpha_2, \alpha_3 \rangle_K$ and $\langle \alpha'_1, \alpha'_2, \alpha'_3 \rangle_K$ are isometric; let $u \in GL_3(K)$ be such that

$$a = ua'u^*$$

Then $\tau_a(uxu^{-1}) = a(uxu^{-1})^*a^{-1} = au^{*-1}x^*u^*a^{-1} = ua'x^*a'^{-1}u^{-1} = u\tau_{a'}(x)u^{-1}$ and the two involutions are isometric. Assume that B is a division algebra. For any $u \neq 0$ in $H(B, \tau)$ we have a τ -hermitian space.

$$\langle u \rangle_B(x, y) = \tau(x)uy$$

A right B -module automorphism $x \mapsto xv, v \in B^\times$, is a *similitude* $\langle u_1 \rangle_B \xrightarrow{\sim} \langle u_2 \rangle_B$ if there is $\lambda \in F^\times$ such that $\lambda\tau(v)u_1v = u_2$. Let now $\tau_i = \text{Int}(u_i) \circ \tau$. It follows from Skolem-Noether that $(B, \tau_1) \simeq (B, \tau_2)$ if and only if $\langle u_1 \rangle_B$ and $\langle u_2 \rangle_B$ are similar: in fact if $\text{Int}(v)$ is an isomorphism $(B, \tau_1) \xrightarrow{\sim} (B, \tau_2)$, then $u_2 = \lambda v u_1 \tau(v)$ for some $\lambda \in F^\times$ and conversely any similitude induces an isomorphism.

Let now $\tau' = \text{Int}(u) \circ \tau$. By the above consideration we have to check that $\langle u \rangle_B$ and $\langle 1 \rangle_B$ are similar to conclude that τ and τ' are isomorphic. Replacing u by $un_B(u)$ we may assume that $n_B(u) \in F^{\times 2}$. Let $x \in H(B, \tau), x \notin F$, so that $L = F(x)$ is cubic over F . The algebra $B \otimes L$ is split over $K \otimes L$ and by the split

case $\langle u \rangle_{B \otimes L}$ and $\langle 1 \rangle_{B \otimes L}$ are similar, i.e. there is $v' \in GL_3(K \otimes L)$ and $\lambda \in L$ such that

$$u \otimes 1 = \lambda v'(\sigma \otimes 1)(v')$$

Denoting by $x \mapsto \bar{x}$ the conjugation in K we get

$$n_{B \otimes L}(u \otimes 1) = \lambda^3 n_{B \otimes L}(v') \overline{n_{B \otimes L}(v')} = \mu^2$$

with $\mu \in F^\times$ since $n_B(u) \in F^{\times 2}$ and we can write

$$\lambda = (\mu \lambda^{-1} n_{B \otimes L}(v')^{-1}) \overline{(\mu \lambda^{-1} n_{B \otimes L}(v')^{-1})} = \nu \bar{\nu}$$

It follows that $u \otimes 1 = v(\sigma \otimes 1)v$ with $v = \nu v'$, so

$$\langle u \rangle_{B \otimes L} \simeq \langle 1 \rangle_{B \otimes L}$$

By the Bayer-Lenstra [BL] generalization of the theorem of Springer to hermitian spaces we have $\langle u \rangle_B \simeq \langle 1 \rangle_B$ and by the above consideration $(B, \tau) \simeq (B, \tau')$. ■

8. Distinguished involutions. Let (B, τ) as above and let $t_{H(B, \tau)} \simeq \langle 1, 1, 1 \rangle \perp \langle 2 \rangle \otimes \langle \langle \alpha \rangle \rangle \otimes \langle \langle b, c \rangle \rangle'$. In view of Theorem 7.1, the isometry class of the Pfister form $\langle \langle \alpha, b, c \rangle \rangle$ determines the isomorphism class of τ . We denote it by $\pi(\tau)$. Furthermore, since two 3-Pfister forms which are isotropic, are hyperbolic, hence isometric. Thus by Albert's theorem and Theorem 6.11 any central simple algebra of degree 3 which admits an involution of second kind, carries an involution such that $\pi(\tau)$ is hyperbolic. We call such an involution *distinguished*. Distinguished involutions can be characterized by different properties. We first need some notations. Let

$$H(B, \tau)^0 = \{x \in H(B, \tau) \mid t_{H(B, \tau)}(x) = 0\}$$

Since $t_{H(B, \tau)}(x) = t_B(x) = t_B(x, 1)$ we have $H(B, \tau)^0 = 1^\perp$ and since $t_B(1) = t_B(1, 1) = 3 \neq 0$, we see that $H(B, \tau)^0$ is a nonsingular bilinear space for the restriction of the trace form. We denote the restriction by $t_{H(B, \tau)}^0$.

Lemma 8.1. Putting $t_{H(B, \tau)} \simeq \langle 1, 1, 1 \rangle \perp \langle 2 \rangle \otimes \langle \langle \alpha \rangle \rangle \otimes \langle \langle b, c \rangle \rangle'$ we have

$$t_{H(B, \tau)}^0 \simeq \langle 2 \rangle \otimes (\langle 1, 3 \rangle \perp \langle \langle \alpha \rangle \rangle \otimes \langle \langle b, c \rangle \rangle')$$

Proof. We have $t_{H(B,\tau)}(1,1) = 3$. Further the bilinear form $\langle 1, 1, 1 \rangle = f$ obviously contains x such that $f(x, x) = 3$. By Witt theorem (see Scharlau) there exists an isometry of $t_{H(B,\tau)}$ which maps 1 to x . This isometry maps 1^\perp to x^\perp . However the orthogonal of x inside $\langle 1, 1, 1 \rangle$ is isometric to $\langle 2, 6 \rangle$ since

$$\langle 1, 1, 1 \rangle \simeq \langle 3 \rangle \perp \langle 2, 6 \rangle$$

Writing $\langle 2, 6 \rangle$ as $\langle 2 \rangle \otimes \langle 1, 3 \rangle$, we get the claim \blacksquare

In the Witt group we have

$$\langle \langle \alpha \rangle \rangle \cdot \langle \langle b, c \rangle \rangle' = \langle \langle \alpha, b, c \rangle \rangle - \langle \langle \alpha \rangle \rangle$$

hence

$$(*) \quad t_{H(B,\tau)}^0 = \langle 2 \rangle \cdot (\langle 3, \alpha \rangle + \langle \langle \alpha, b, c \rangle \rangle) \text{ in } W(F).$$

Any symmetric bilinear form f can be decomposed in a unique way up to isometry as

$$f \simeq h_n \perp f_{an}$$

where f_{an} is anisotropic, i.e. $f_{an}(x, x) = 0 \Rightarrow x = 0$ and h_n is hyperbolic of rank $2n$. The number n is called the *Witt index* of f and is denoted by $w(f)$. Comparing dimensions on both sides of (*) we have

$$w(t_{H(B,\tau)}^0) = w(\langle 3, \alpha \rangle \perp \langle \langle \alpha, b, c \rangle \rangle) - 1.$$

Isotropic elements of $t_{H(B,\tau)}^0$ are elements $x \in H(B, \tau)$ such that $t_B(x) = 0 = t_B(x^2)$ (since $t_B(x^2) = t_B(x, x)$). Since the characteristic reduced polynomial of B can also be written as (exercise!)

$$X^3 - t_B(b)X^2 + \frac{1}{2}[t_B(b)^2 - t_B(b^2)]X - n_B(b) \cdot 1$$

we see that $x \in H(B, \tau)^0$ is isotropic if and only if

$$x^3 = n_B(x) \in F$$

We now get to the announced equivalent properties of distinguished involutions:

Theorem 8.2. Let (B, τ) be central simple of degree 3 over K with τ an involution of second kind. The following properties are equivalent:

- (1) τ is distinguished;
- (2) either $K = F \times F$ or $\langle -b, -c, bc \rangle_K \simeq \langle 1, -1, 1 \rangle_K$
- (3) $w(t_{H(B, \tau)}^0) \geq 2$
- (3') $H(B, \tau)$ contains a subspace of dimension 2 whose elements satisfy $u^3 = n_B(u)$
- (4) $w(t_{H(B, \tau)}^0) \geq 3$
- (4') $H(B, \tau)$ contains a subspace of dimension 3 whose elements satisfy $u^3 = n_B(u)$
- (5) $H(B, \tau)$ contains an étale cubic F -algebra whose discriminant algebra is isomorphic to K
- (6) B is a cyclic algebra

$$B = M \oplus Mz \oplus Mz^2$$

where M is cyclic over K , τ preserves M , M is a S_3 -Galois algebra over F and $\tau(z) = z$

Proof (1) \Rightarrow (2) follows from Theorem 6.11 and Theorem 7.1. (3) \Leftrightarrow (3') and (4) \Leftrightarrow (4') are consequences of the preceding observation on isotropic elements of $t_{H(B, \tau)}^0$. (1) \Rightarrow (3) follows from the above formula

$$W(t_{H(B, \tau)}^0) = W(\langle 3, \alpha \rangle \perp \langle \langle \alpha, b, c \rangle \rangle) - 1$$

(5) \Leftrightarrow (6) is part of Theorem 6.11, (4) \Rightarrow (3) is clear. We now show (3) \Rightarrow (1): if $W(t_{H(B, \tau)}^0) \geq 2$, then $\langle 3, \alpha \rangle \perp \langle \langle \alpha, b, c \rangle \rangle$ contains isotropic subspaces of dimension 3. Therefore $\langle \langle \alpha, b, c \rangle \rangle$ is isotropic, hence hyperbolic, proving (1). To show that (5) \Rightarrow (4), recall that

$$t_{H(B, \tau)} \simeq \langle 1, 2, 2\delta \rangle \perp \langle 2, -2\alpha\delta \rangle \otimes t_L(\langle \lambda \rangle_L)$$

by Theorem 6.5; (5) implies that $\alpha\delta \equiv 1$, so that $\langle 2, -2\alpha\delta \rangle \simeq \langle 2, -2 \rangle \simeq \langle 1, -1 \rangle$ is hyperbolic, hence

$$\langle 2, -2\alpha\delta \rangle \otimes t_L(\langle \lambda \rangle_L) \simeq h_3$$

and since on the other hand $\langle 1, 2 \rangle \simeq \langle 3, 6 \rangle$, we get (4). To complete the proof we show that (3') \Rightarrow (6). Assume first that $K = F \times F$, so that $B = A \times A^{\text{op}}$ and τ is the switch involution. By Wedderburn's theorem A contains a cyclic extension L of F and we put

$$M = \{(\ell, \ell^{\text{op}}) | \ell \in L\}.$$

If $B = M_3(K)$, then since (3) \Rightarrow (2), we may assume that $\tau = \text{Int}(a) \circ *$, where a defines an isotropic hermitian form. We may take up to isomorphism

$$a = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}$$

then

$$M = \left\{ \begin{pmatrix} f & 0 & 0 \\ 0 & k & 0 \\ 0 & 0 & \bar{k} \end{pmatrix} \mid f \in F, k \in K \right\}$$

Thus we are reduced to the case where B is a central division algebra. We use computation made in the proof of Albert's theorem (p.24-25). Since we have by assumption a 2-dimensional subspace $U \subset H(B, \tau)$ of elements u such that $u^3 = n_B(u) \in F$, we may take $\tau' = \tau$ in the proof of Albert's theorem (see the remark p.23). With the notations in p.24, let $\tau'' = \text{Int}(\theta_2^{-1}) \circ \tau$ and let $L' \subset M$ denote the subfield of τ'' -invariant elements. Since $L'K = M$ is cyclic over K and S_3 -Galois over F , Theorem 6.11 shows that L' has discriminant algebra K . Observe now that

$$\theta_2 = w_1^{-3} w_2^{-3} (w_1 w_2^2) (w_2^2 w_1),$$

hence $\theta_2^{-1} = \lambda v \tau(v)$ for $\lambda = w_1^3 w_2^3$ and $v = w_1^{-1} w_2^{-2}$ so that

$$\text{Int}(v) : (B, \tau) \xrightarrow{\sim} (B, \tau'')$$

is an isomorphism of algebras with involution. Pulling $L' \subset H(B, \tau'')$ back to $H(B, \tau)$ gives the wanted étale algebra L . ■

Theorem 8.3. For every cubic étale F -algebra $L \subset B$, there is a distinguished involution τ such that $L \subset H(B, \tau)$.

Proof. Let $\lambda_0 \in L^\times$ be such that $t_L(\lambda_0) = 0$ and let $\lambda = \lambda_0 n_L(\lambda_0)^{-1}$, so that

$$n_L(\lambda) = n_L(\lambda_0)^{-2} \in F^{\times 2}$$

By Theorem 6.10 there is an involution τ on B such that $L \subset H(B, \tau)$ and

$$t_{H(B, \tau)} \simeq \langle 1, 1, 1, \rangle \perp \langle 2\delta \rangle \otimes \langle \langle \alpha \rangle \rangle \otimes t_L(\langle \lambda \rangle_L)$$

hence

$$t_{H(B, \tau)}^0 \simeq \langle 2 \rangle \otimes \langle \langle 1, 3 \rangle \perp \langle \delta \rangle \otimes \langle \langle \alpha \rangle \rangle \otimes t_L(\langle \lambda \rangle_L)$$

Since $t_L(\lambda) = 0$, $t_L(\langle \lambda \rangle)$ is isotropic and the Witt index of $\langle \langle \alpha \rangle \rangle \otimes t_L(\langle \lambda \rangle_L)$ is at least 2.

Therefore condition (3) of Theorem 8.2 is satisfied and τ is distinguished.

Corollary 8.4. The space $H(B, \tau)$ contains an isomorphic copy of every cubic étale F -algebra of B if and only if τ is distinguished.

Proof. Since all distinguished involutions of B are isomorphic, the if direction follows from Theorem 8.3. Conversely, by Theorem 8.2 the only involutions which leave elementwise invariant étale cubic F -subalgebras of discriminant algebra K are the distinguished involutions ■

9. Some complements

9.1. In section 7 we showed that the isomorphism class of the hermitian form

$$h = \langle -b, -c, bc \rangle_K$$

correspond to the isomorphism class of the 3-Pfister form $\langle\langle\alpha, b, c\rangle\rangle$. On the other hand a 3-Pfister form $\langle\langle\alpha, b, c\rangle\rangle$ determines an isomorphism class of octonions, represented by the algebra $\mathcal{O} = (\alpha, b, c)_F$, (see the introduction). There is a way to describe directly the correspondence. Let

$$\langle -b, -c, bc \rangle_K = (W, h) \quad , W = K^3$$

Since $(-b)(-c)bc \in F^{\times 2}$ we may fix an isomorphism

$$\varphi : \Lambda^3(W, h) \xrightarrow{\sim} \langle 1 \rangle_K$$

of hermitian forms ((W, h) has trivial hermitian discriminant). Let $v \times w \in W$ be defined by $h(u, v \times w) = \phi(u \wedge v \wedge w)$ Then

$$\mathcal{O} = K \oplus W$$

is an octonian algebra under the product

$$(a, v) \cdot (b, w) = (ab - h(v, w), aw + \bar{b}v + v \times w)$$

Conversely, given $K \subset \mathcal{O}$, \mathcal{O} any octonian algebra, we put $W = K^\perp$ for the scalar product induced by the norm. It can be shown that W is a K -space and admits a 3-dimensional nonsingular hermitian form h which has trivial hermitian discriminant. Observe the similarity with the situation $L \subset H(B, \tau)$ and $V = L^\perp$.

9.2. Exceptional Jordan algebras

Let (B, τ) of degree 3 over K with involution τ of second kind. As observed in section 5, $H(B, \tau)$ is closed under the product

$$(*) \quad x \cdot y = \frac{xy + yx}{2}$$

This product satisfies

$$((a \cdot a) \cdot b) \cdot a = (a \cdot a)(b \cdot a),$$

is commutative and has an identity 1. In fact $(*)$ defines the structure of a Jordan algebra, denoted A^+ for any associative algebra A . A Jordan algebra J is *special* if $J \subset A^+$ for some A associative, exceptional otherwise. There is a notion of central simple Jordan algebras and it can be shown (Albert) that there exist exceptional Jordan algebras which are central simple only in dimension 27. These algebras are of degree 3. We give two examples:

Examples 1. Let \mathcal{O} be an octonian algebra over F , let $a = \text{diag}(\alpha_1, \alpha_2, \alpha_3) \in M_3(F)$, $\alpha_1\alpha_2\alpha_3 \neq 0$. On

$$M_3(F) \otimes \mathcal{O} = M_3(\mathcal{O})$$

we define $\tau(x) = a\bar{x}^t a^{-1}$ and put

$$H_3(\mathcal{O}, \tau) = \{x \in M_3(\mathcal{O}) \mid \tau(x) = x\}$$

Then $x \cdot y = \frac{xy + yx}{2}$ defines on $H_3(\mathcal{O}, \tau)$ the structure of an exceptional Jordan algebra of degree 3.

Example 2. Let (B, τ) be of degree 3 with involution of second kind. On

$$J = (B, \tau) \oplus H(B, \tau)$$

one can define the structure of a central simple Jordan algebra of degree 3 which is exceptional (Tits construction) and Tits has shown that any central simple exceptional Jordan algebra of dimension 27 is of that kind.

9.3. Galois cohomology

Let F_{sep} be a separable closure of F and let $\Gamma = \text{Gal}(F_{\text{sep}}/F)$. If A is a Γ -module (with continuous action) one can define cohomology groups

$$H^n(\Gamma, A)$$

Typical examples are $A = C_n$ (cyclic of order n) with trivial action, $A = \mu_n(F_{\text{sep}})$, where

$$\mu_n(F') = \{x \in F' \mid x^n = 1\}$$

for any field F' . Assume $\text{char} F \neq 2$. We have

$$H^1(\Gamma, \mathbb{Z}/2\mathbb{Z}) = H^1(\Gamma, \mu_2) \simeq F^\times / F^{\times 2}$$

and this group classifies quadratic étale F -algebras. If the action of Γ on A is trivial, we have

$$H^1(\Gamma, A) = \text{Hom}(\Gamma, A),$$

in particular $H^1(\Gamma, \mathbb{Z}/2\mathbb{Z}) = \text{Hom}(\Gamma, \mathbb{Z}/2\mathbb{Z})$. Thus to a quadratic étale F algebra K , we may associate a homomorphism $\varphi_K : \Gamma \rightarrow \mathbb{Z}/2\mathbb{Z}$. If A is a Γ -module which admits an automorphism α of order 2, we may twist the action of Γ by putting

$$\gamma \circ \alpha = \varphi_K(\gamma)\alpha$$

We denote the new action by $A_{[K]}$. In particular we have

$$\mu_3 = C_{3[F(\omega)]}.$$

where $F(\omega) = F[X]/(X^2 + X + 1)$. Assume that $\text{char} F \neq 3$.

Then

$$H^1(\Gamma, \mu_3) \simeq F^\times / F^{\times 3}$$

and $H^2(\Gamma, \mu_3)$ is the subgroup of the Brauer group $Br(F)$ of F of elements of order 3. Let K/F be quadratic étale not split and let

$$\Gamma_K = \text{Gal}(F_{\text{sep}}/K)$$

(we assume that $K \subset F_{\text{sep}}$). The norm map $n_K : K \rightarrow F$ induces a group homomorphism

$$H^2(\Gamma_K, \mu_3) \rightarrow H^2(\Gamma, \mu_3)$$

and, by a result of Albert-Riehm-Scharlau [S], its kernel consists of classes of algebras of exponent 3 over K which admit involutions of second kind. Using the Lemma of Eckmann-Faddeev-Shapiro, it can be shown that this kernel is isomorphic to $H^2(\Gamma, \mu_{3[K]})$. In the description of Albert of algebras of degree 3 which admit an

involution of second kind, two typical étale algebras of degree 3 over F occur: the algebra $F(z)$ with $z^3 = a \in F^\times$, which corresponds to an element $[a] \in H^1(\Gamma, \mu_3)$, and an algebra L of discriminant K . Such an algebra corresponds to a class

$$[L] \in H^1(\Gamma, (C_3)_{[K]}).$$

We have an isomorphism

$$\mu_3 \otimes (C_3)_{[K]} \simeq \mu_{3[K]}$$

of Galois modules, so that the cup-product induces a pairing

$$\cup : H^1(\Gamma, \mu_3) \times H^1(\Gamma, (C_3)_{[K]}) \rightarrow H^2(\Gamma, \mu_{3[K]})$$

and $[a] \cup [L] \in H^2(\Gamma, \mu_{3[K]})$ is the class of the algebra (B, τ) . Finally the classification of involution through Pfister forms can also be described in cohomology terms. A 1-Pfister form $\langle\langle \alpha \rangle\rangle$ corresponds to a quadratic étale algebra, hence an element in $H^1(\Gamma, \mu_2)$. To a n -Pfister form $\langle\langle \alpha_1, \dots, \alpha_n \rangle\rangle$ we associate the cup-product $[\alpha_1] \cup \dots \cup [\alpha_n] \in H^n(\Gamma, \mu_2)$ and it is known that n -Pfister forms are classified by their cohomology class. This is “classical” for $n \leq 3$ and was proven recently by Voesvodsky in general. Thus we see that triples (B, K, τ) viewed as objects over F are classified up to isomorphisms by three cohomological invariants: the class of K in $H^2(\Gamma, \mu_2)$, the class of B (as an algebra which admits an involution) in $H^2(\Gamma, \mu_{3[K]})$ and the class of the Pfister form $\pi(\tau)$ in $H^3(\Gamma, \mu_2)$, which classifies the involutions.

References

- : [A] A.A. Albert. On involutorial associative division algebras, Scripta Math. 26 (1963), 309-316.
- : [BL] E. Bayer Fluckiger, H.W. Lenstra. Forms in odd-degree extensions and self-dual normal bases, Amer. J. Math. 112 (1990), 359-373.
- : [H] D. Haile, A useful proposition for division algebras of small degree, Proc. Amer. Math. Soc 106 (1989), 317-319.

- : [J] N. Jacobson. A note on hermitian forms. Bull. Amer. Math. Soc. 46(1940), 264-268.
- : [HK] D. Haile, M.-A. Knus. On division algebras of degree 3 with involution. J. Algebra? (1996).
- : [HKRT] D. Haile, M.-A. Knus, M. Rost, J.-P. Tignol. Algebras of odd degree with involution, trace forms and dihedral extensions, Israel J. Math.(1996).
- : [HKRT] M.-A. Knus, A.A. Merkurjev, M. Rost, J.-P. Tignol, The book of involutions.
- : [S] W. Scharlau. Quadratic and Hermitian Form. Springer, 1985.
- : [W] J.H.M. Wedderburn. On division algebras. Trans. Amer. Math. Soc. (1921), 129-135.