ALGEBRAS OF ODD DEGREE WITH INVOLUTION, TRACE FORMS AND DIHEDRAL EXTENSIONS[1]

Darrell Haile, Max-Albert Knus, Markus Rost and Jean-Pierre Tignol[2]

Dedicated to the memory of S.A. Amitsur

Abstract

A 3-fold Pfister form is associated to every involution of the second kind on a central simple algebra of degree 3. This quadratic form is associated to the restriction of the reduced trace quadratic form to the space of symmetric elements; it is shown to classify involutions up to conjugation. Subfields with dihedral Galois group in central simple algebras of arbitrary odd degree with involution of the second kind are investigated. A complete set of cohomological invariants for algebras of degree 3 with involution of the second kind is given.

1. Introduction. Let B be a central simple algebra over a field K with an involution σ of the second kind and let F be the fixed subfield of K. Let Trd be the reduced trace and Nrd the reduced norm of B. The restriction Q_σ of the trace form Q: $(x, y) \mapsto \mathrm{Trd}(xy)$ to the F–space $(B, \sigma)_+$ of symmetric elements of B is a quadratic form with values in F. It is an invariant of σ and the aim of this paper is to study this invariant. We first describe the general form of Q_σ for algebras of arbitrary odd degree and then restrict our attention to central simple algebras of degree 3.

Consider a cubic étale F-subalgebra $L \subset (B, \sigma)_+$. The restriction of the trace form to L is nonsingular, hence we have an orthogonal decomposition:

$$(B, \sigma)_+ = L \perp V.$$

[1]The text appeared as: Israel J. Math. 96 B, 299-340 (1996) - Amitsur Volume
[2]Supported in part by the National Fund for Scientific Research (Belgium)

We give an explicit description of the restriction of the form Q_σ to V, using a special case of a construction introduced by T. Springer [19], in connection with exceptional Jordan algebras, and generalized by Petersson–Racine [11] to algebras of degree 3. Our next goal is to show that the trace form Q_σ determines the involution up to isomorphism. As a consequence we get a parametrization of all involutions of the second kind on a central simple algebra of degree 3 which leave elementwise invariant a given cubic separable subalgebra. We also associate a 3-fold Pfister form $\pi(B,\sigma)$ to Q_σ, which determines σ up to isomorphism, and characterize the class of involutions for which this 3-fold Pfister form is hyperbolic. The existence of such involutions, which we call distinguished, follows from Springer's construction, but is also related to a crossed product construction given by A.A. Albert [2]. A distinguished involution is characterized by the fact that the space $(B,\sigma)_+$ contains up to isomorphism every cubic étale F-subalgebra of B.

In the last section, we use Galois cohomology and symbols to analyze étale subalgebras of dihedral central simple algebras. As applications, we get on one hand different proofs of previous results of the paper and on the other hand we show that a dihedral algebra of degree $2n$, n odd, is cyclic if a quadratic extension of F contains a primitive n^{th}–root of 1 (see Corollary 30 for the precise statement). This is due to L. Rowen and D. Saltman [15] if F contains a primitive n^{th}–root of 1. As a last application, we give a complete set of cohomological invariants for algebras of degree three with involution of the second kind.

The second author is indebted to H.P. Petersson for useful comments on the subject.

2. Some General Results. Throughout the paper, B denotes a central simple algebra over a field K of characteristic different from 2 and σ denotes an involution of the second kind on B, i.e. a map $\sigma\colon B \to B$ such that

$$\sigma(x+y) = \sigma(x) + \sigma(y), \qquad \sigma(xy) = \sigma(y)\sigma(x), \qquad \sigma^2(x) = x$$

for all $x, y \in B$, and $\sigma|_K \neq I_K$. We let F denote the subfield of

K elementwise invariant under σ and denote by $\bar{\ }\colon K \to K$ the restriction of σ to K.

Under a scalar extension of F, the field K — hence also the algebra B — may split into a direct product of two factors. Therefore, we shall also allow K to be a split quadratic étale F-algebra:

$$K = F \times F.$$

In that case, $B = A \times A'$ for some central simple F-algebras A, A' which are exchanged under the involution σ. Therefore, there is an isomorphism of K-algebras with involution (i.e. an isomorphism which commutes with the involutions):

$$(B, \sigma) \simeq (A \times A^{\mathrm{op}}, s)$$

where A^{op} is the opposite algebra of A and s is the switch involution:

$$s(a_1, a_2^{\mathrm{op}}) = (a_2, a_1^{\mathrm{op}}).$$

Abusing the terminology, we shall also consider (B, σ) as a central simple algebra with involution in this case. (It is indeed simple as an algebra-with-involution: see Jacobson's definition in [8, p. 208]).

We let $\alpha \in F^\times$ be such that $K = F(\sqrt{\alpha}) = F[X]/(X^2 - \alpha)$. In particular, we have $\alpha \in {F^\times}^2$ if $K = F \times F$.

Let $(B, \sigma)_+$ denote the F-vector space of σ-symmetric elements:

$$(B, \sigma)_+ = \{b \in B \colon \sigma(b) = b\}.$$

We denote by Q_σ the restriction to $(B, \sigma)_+$ of the reduced trace quadratic form:

$$Q_\sigma(x) = \mathrm{Trd}_B(x^2) \qquad \text{for } x \in (B, \sigma)_+.$$

For any $u \in (B, \sigma)_+ \cap B^\times$, $\sigma' = \mathrm{Int}(u) \circ \sigma$ is again an involution of the second kind of B and conversely, if σ, σ' are involutions of the second kind of B, there exists $u \in (B, \sigma)_+ \cap B^\times$ such that $\sigma' = \mathrm{Int}(u) \circ \sigma$. Let $\langle u \rangle_B$ be the B-hermitian form on B (as a right B–module) given by

$$\langle u \rangle_B(x, y) = \sigma(x) u y,$$

for $u \in (B,\sigma)_+ \cap B^\times$ and $x, y \in B$. A right B-module automorphism $r_v\colon x \mapsto vx$, $v \in B^\times$, of B is an **isometry** $\langle u_1\rangle_B \xrightarrow{\sim} \langle u_2\rangle_B$ if $\sigma(v)u_2v = u_1$ and is a **similarity** if there is $\lambda \in F^\times$ such that $\lambda\sigma(v)u_2v = u_1$.

LEMMA 1. *Let $u_1, u_2 \in (B,\sigma)_+ \cap B^\times$ and let $\sigma_i = \mathrm{Int}(u_i)\circ\sigma$. Then*

(1) An isomorphism $(B,\sigma_1) \xrightarrow{\sim} (B,\sigma_2)$ induces an isometry $Q_{\sigma_1} \xrightarrow{\sim} Q_{\sigma_2}$.

(2) (B,σ_1) and (B,σ_2) are isomorphic (as K-algebras with involution) if and only if the hermitian spaces $\langle u_1\rangle_B$ and $\langle u_2\rangle_B$ are similar.

Proof. (1): If $\mathrm{Int}(v)\colon (B,\sigma_1) \xrightarrow{\sim} (B,\sigma_2)$ is an isomorphism, then $\mathrm{Int}(v)[(B,\sigma_1)_+] = (B,\sigma_2)_+$ and

$$Q_{\sigma_2}(vxv^{-1}, vyv^{-1}) = \mathrm{Trd}_B(vxyv^{-1}) = Q_{\sigma_1}(x,y)$$

for $x, y \in (B,\sigma)_+$.
(2): The automorphism $\mathrm{Int}(v)$ of B is an isomorphism $(B,\sigma_1) \xrightarrow{\sim} (B,\sigma_2)$, if and only if $\sigma_2(vxv^{-1}) = v\sigma_1(x)v^{-1}$ for all $x \in B$, if and only if $u_2 = \lambda v u_1 \sigma(v)$ for some $\lambda \in F^\times$, hence $\langle u_1\rangle_B$ and $\langle u_2\rangle_B$ are similar. Conversely any such similitude induces an isomorphism $(B,\sigma_1) \xrightarrow{\sim} (B,\sigma_2)$. ∎

Let $B = \mathrm{M}_n(K)$ be split and let $\tau(x_{ij}) = (\overline{x}_{ij})^t$, where t is transpose and $x \mapsto \overline{x}$ is conjugation on K. Any $u \in (\mathrm{M}_n(K),\tau)_+$ is a hermitian matrix, hence there is $v \in \mathrm{GL}_n(K)$ such that $\sigma(v)uv = a = \mathrm{diag}(\alpha_1,\ldots,\alpha_n)$, $\alpha_i \in F^\times$. Thus any involution of $\mathrm{M}_n(K)$ of the second kind is isomorphic to an involution of the form $\sigma = \mathrm{Int}(a)\circ\tau$ with $a = \mathrm{diag}(\alpha_1,\cdots,\alpha_n), \alpha_i \in F^\times$.

Let $h_a = \langle\alpha_1,\ldots,\alpha_n\rangle_K$ be the hermitian form on K^n determined by $\mathrm{diag}(\alpha_1,\cdots,\alpha_n)$, i.e. $h_a(x,y) = \sum \overline{x}_i\alpha_i y_i = \overline{x}^t a y$, $x, y \in K^n$. Any isometry $h_a \xrightarrow{\sim} h_{a'}$ of the K–space K^n can be viewed as an isometry $\langle a\rangle_{\mathrm{M}_n(K)} \xrightarrow{\sim} \langle a'\rangle_{\mathrm{M}_n(K)}$ of the $\mathrm{M}_n(K)$–space $\mathrm{M}_n(K)$.

For $\alpha_1,\ldots,\alpha_n \in F^\times$, we denote by $\langle\alpha_1,\ldots,\alpha_n\rangle$ the quadratic form on F^n determined by $\mathrm{diag}(\alpha_1,\cdots,\alpha_n)$, and by $\langle\!\langle\alpha_1,\ldots,\alpha_n\rangle\!\rangle$ the n-fold Pfister form:

$$\langle\!\langle\alpha_1,\ldots,\alpha_n\rangle\!\rangle = \langle 1,-\alpha_1\rangle\cdot\cdots\cdot\langle 1,-\alpha_n\rangle.$$

The next proposition follows by straightforward computation.

PROPOSITION 2. *Let* $K = F(\sqrt{\alpha})$. *For* $a = \operatorname{diag}(\alpha_1, \cdots, \alpha_n) \in \mathrm{M}_n(K)$ *and* $\sigma = \operatorname{Int}(a) \circ \tau$ *we have*

$$Q_\sigma \simeq n\langle 1\rangle \perp \langle 2\rangle \cdot \langle\!\langle \alpha \rangle\!\rangle \cdot (\perp_{1\le i<j\le n} \ \langle \alpha_i \alpha_j\rangle).$$

In order to get a similar result for arbitrary central simple algebras of odd degree, we first prove:

LEMMA 3. *Let* L/F *be a field extension of odd degree and let* q *be a quadratic form over* F. *Let also* q_L *denote the quadratic form over* L *derived from* q *by extending scalars to* L, *and let* $\alpha \in F^\times \smallsetminus F^{\times 2}$. *If* $q_L \simeq \langle\!\langle \alpha \rangle\!\rangle \cdot h$ *for some quadratic form* h *over* L, *of determinant* 1, *then there is a quadratic form* t *of determinant* 1 *over* F *such that*

$$q \simeq \langle\!\langle \alpha \rangle\!\rangle \cdot t.$$

Proof. Let $K = F(\sqrt{\alpha})$ and $E = L \cdot K = L(\sqrt{\alpha})$. Let also q_{an} denote an anisotropic form over F which is Witt-equivalent to q. The form $(q_{\mathrm{an}})_E$ is Witt-equivalent to the form $(\langle\!\langle \alpha \rangle\!\rangle \cdot h)_E$, hence it is hyperbolic. Since the field extension E/K has odd degree, Springer's theorem on the behaviour of quadratic forms under field extensions of odd degree [16, Theorem 2.5.3] shows that $(q_{\mathrm{an}})_K$ is hyperbolic, hence, by [16, Remark 2.5.11],

$$q_{\mathrm{an}} = \langle\!\langle \alpha \rangle\!\rangle \cdot t_0$$

for some quadratic form t_0 over F. Let $\dim q = 2d$, so that $\dim h = d$, and let w denote the Witt index of q, so that

$$q \simeq w\mathbb{H} \perp \langle\!\langle \alpha \rangle\!\rangle \cdot t_0, \tag{1}$$

where $\mathbb{H}$ is the hyperbolic plane. We then have $\dim t_0 = d - w$, hence

$$\det q = (-1)^w \, (-\alpha)^{d-w} \cdot F^{\times 2} \in F^\times / F^{\times 2}.$$

On the other hand, the relation $q_L \simeq \langle\!\langle \alpha \rangle\!\rangle \cdot h$ yields:

$$\det q_L = (-\alpha)^d \cdot L^{\times 2} \in L^\times / L^{\times 2}.$$

Therefore, $\alpha^w \in F^\times$ becomes a square in L; since the degree of L/F is odd, this implies that $\alpha^w \in F^{\times 2}$, hence w is even. Letting $t_1 = \frac{w}{2}\mathbb{H} \perp t_0$, we then derive from (1):

$$q \simeq \langle\langle \alpha \rangle\rangle \cdot t_1.$$

It remains to prove that we may modify t_1 so as to satisfy the determinant condition. Since $\dim t_1 = d$, we have modulo the square I^2F of the fundamental ideal of the Witt ring of F:

$$t_1 \equiv \begin{cases} \langle\langle (-1)^{d(d-1)/2} \det t_1 \rangle\rangle & \text{if } d \text{ is even} \\ \langle (-1)^{d(d-1)/2} \det t_1 \rangle & \text{if } d \text{ is odd.} \end{cases}$$

We may use these relations to compute the Clifford algebra of $q \simeq \langle\langle \alpha \rangle\rangle \cdot t_1$ (up to Brauer-equivalence): in both cases we get the same quaternion algebra:

$$C(q) \sim (\alpha, (-1)^{d(d-1)/2} \det t_1)_F.$$

On the other hand, since $\det h = 1$ we derive from $q_L \simeq \langle\langle \alpha \rangle\rangle \cdot h$:

$$C(q_L) \sim (\alpha, (-1)^{d(d-1)/2})_L.$$

Therefore, the quaternion algebra $(\alpha, \det t_1)_F$ is split, since it splits over the extension L/F of odd degree. Therefore, if $\delta \in F^\times$ is a representative of $\det t_1 \in F^\times/F^{\times 2}$, we have

$$\delta \in n_{K/F}(K^\times).$$

Let $\beta \in F^\times$ be a represented value of t_1, so that

$$t_1 \simeq t_2 \perp \langle \beta \rangle$$

for some quadratic form t_2 over F, and let

$$t = t_2 \perp \langle \delta\beta \rangle.$$

Then

$$\det t = \delta \cdot \det t_1 = 1.$$

On the other hand, since δ is a norm from the extension K/F we have

$$\langle\langle\alpha\rangle\rangle \cdot \langle\delta\beta\rangle \simeq \langle\langle\alpha\rangle\rangle \cdot \langle\beta\rangle,$$

hence

$$\langle\langle\alpha\rangle\rangle \cdot t \simeq \langle\langle\alpha\rangle\rangle \cdot t_1 \simeq q.$$

■

PROPOSITION 4. *Let B be a central simple K-algebra of odd degree $n = 2m - 1$ with an involution σ of the second kind. There is a quadratic form q_σ of dimension $n(n-1)/2$ and determinant 1 over F such that*

$$Q_\sigma \simeq n\langle 1\rangle \perp \langle 2\rangle \cdot \langle\langle\alpha\rangle\rangle \cdot q_\sigma.$$

Proof. Suppose first $K = F \times F$. We may then assume $(B, \sigma) = (A \times A^{\mathrm{op}}, s)$, where s is the switch involution. In that case

$$(B, \sigma)_+ = \{(a, a^{\mathrm{op}})\colon a \in A\} \simeq A,$$

and Q_σ is isometric to the reduced trace quadratic form on A. Since $\alpha \in F^{\times 2}$, we have to show that this quadratic form is Witt-equivalent to $n\langle 1\rangle$. By Springer's theorem, it suffices to prove this relation over an odd-degree field extension. Since the degree of A is odd, we may therefore assume A is split: $A = \mathrm{M}_n(F)$. In that case, the relation is easy to check. (Observe that the upper-triangular matrices with zero diagonal form a totally isotropic subspace).

For the rest of the proof, we may thus assume K is a field. Let D be a division K-algebra Brauer-equivalent to B and let $\tau\colon D \to D$ be an involution of the second kind on D. Let also L be a field contained in $(D, \tau)_+$ and maximal for this property. The field $E = L \cdot K$ is then a maximal subfield of D, otherwise the centralizer $C_D E$ contains a symmetric element outside E, contradicting the maximality of L. We have $[L : F] = [E : K] = \deg D$, hence the degree of L/F is odd, since D is Brauer-equivalent to the algebra B of odd degree. Moreover, the algebra

$$B \otimes_F L = B \otimes_K E$$

splits, since E is a maximal subfield of D. By Proposition 2 the quadratic form $[Q_\sigma]_L$ obtained from Q_σ by scalar extension to L has the form

$$[Q_\sigma]_L \simeq n\langle 1\rangle \perp \langle 2\rangle \cdot \langle\langle \alpha \rangle\rangle \cdot h \tag{2}$$

where $h = \perp_{1\le i<j\le n} \langle \alpha_i \alpha_j \rangle$ for some $\alpha_1, \ldots, \alpha_n \in L^\times$. Therefore, the Witt index of the form $[Q_\sigma]_L \perp n\langle -1\rangle$ is at least n:

$$w([Q_\sigma]_L \perp n\langle -1\rangle) \ge n.$$

By Springer's theorem the Witt index of a form does not change under an odd-degree scalar extension. Therefore,

$$w(Q_\sigma \perp n\langle -1\rangle) \ge n,$$

and it follows that Q_σ contains a subform isometric to $n\langle 1\rangle$. Let

$$Q_\sigma \simeq n\langle 1\rangle \perp q$$

for some quadratic form q over F. Relation (2) shows that

$$(q)_L \simeq \langle 2\rangle \cdot \langle\langle \alpha \rangle\rangle \cdot h.$$

Since $\det h = 1$, we may apply Lemma 3 to the quadratic form $\langle 2\rangle \cdot q$ and get a quadratic form q_σ over F, of determinant 1, such that

$$\langle 2\rangle \cdot q \simeq \langle\langle \alpha \rangle\rangle \cdot q_\sigma,$$

hence

$$Q_\sigma \simeq n\langle 1\rangle \perp \langle 2\rangle \cdot \langle\langle \alpha \rangle\rangle \cdot q_\sigma.$$

■

We conclude with a result which will be used in the next section for algebras of degree 3.

LEMMA 5. *Let $L \subset (B,\sigma)_+$ be étale of dimension n over F and let $R = L \otimes_F L \otimes_F K$. Then B is a free R-module of rank one via left and right multiplication; the action is equivariant with respect to the involution σ on B and the action $\sigma\colon R \to R$ given by $\sigma(\lambda \otimes \mu \otimes x) = \mu \otimes \lambda \otimes \bar{x}$. In particular we have an induced action of R^σ on $(B,\sigma)_+$*

Proof. We may assume that F is separably closed, that

$$B = \mathrm{M}_n(F) \times \mathrm{M}_n(F)^{\mathrm{op}},$$

σ is the switch involution, and

$$L = \{(d, d^{\mathrm{op}}) \colon d \text{ is diagonal}\}.$$

Let L' be the set of diagonal matrices in $\mathrm{M}_n(F)$. We have

$$\mathrm{M}_n(F) = L' \oplus xL' \oplus \cdots \oplus x^{n-1}L',$$

with x a permutation matrix of order n. In this case $\xi = 1 + x \cdots + x^{n-1}$ is a free generator of $\mathrm{M}_n(F)$ as a $L' \otimes L'$-module. Thus (ξ, ξ^{op}) is a free generator of B as $L \otimes L$-module. The last claim follows by a direct verification. ∎

3. A Construction of Springer. In this section, we restrict attention to central simple algebras of degree 3 over a field of characteristic different from $2, 3$. We use the same notation as in the preceding section; in particular, we denote by B a central simple K-algebra with involution σ of the second kind. Consider a cubic étale F-subalgebra $L \subset (B, \sigma)_+$ and denote by $t_{L/F} \colon L \to F$ and $n_{L/F} \colon L \to F$ the trace, resp. the norm of L. The restriction of the trace form to L is nonsingular, hence we have an orthogonal decomposition:

$$(B, \sigma)_+ = L \perp V.$$

For $v \in V$ let

$$N(v) = \tfrac{1}{2} \operatorname{Trd}_B(v^2) - p_L(v^2) \in L,$$

where $p_L \colon (B, \sigma)_+ \to L$ denotes the orthogonal projection. We define an L-action on V such that (V, N) is a nonsingular quadratic space of rank 2 over L. We give two descriptions of the action of L on V. The first was introduced by T. Springer [19] in connection with exceptional Jordan algebras and generalized by Petersson–Racine [11] to Jordan algebras of degree 3. The second uses Lemma 5 and is specific to central simple algebras of degree 3.

LEMMA 6. (SPRINGER'S CONSTRUCTION) *The space V is a free L-module of rank 2 through the operation*

$$(\ell, v) \mapsto \ell \circ v = t_{L/F}(\ell)v - \ell v - v\ell \in V$$

and $N\colon V \to L$ is a nonsingular quadratic form for this structure. Moreover, for all $v \in V$,

$$Q_\sigma(v) = 2\, t_{L/F}(N(v)).$$

If $v \in V$ is invertible in B, then

$$\mathrm{Trd}_B(v^{-1}\ell) = -\,\mathrm{Nrd}_B(v)^{-1} t_{L/F}(N(v)\ell)$$

for all $\ell \in L$.

Proof. Extending scalars from F to an algebraic closure, we may assume that B is of the form $\mathrm{M}_3(F) \times \mathrm{M}_3(F)^{\mathrm{op}}$, σ is the switch involution, and $L = \{(d, d^{\mathrm{op}})\colon d \text{ is diagonal}\}$. In this case the lemma follows by explicit computation. ∎

We now describe the second construction: Let $D = F(\sqrt{\delta})$ be the discriminant algebra of L, i.e. δ is the determinant of the trace form $t_{L/F}(x^2) = Q_\sigma|_L(x)$. There exists a decomposition

$$L \otimes_F L = L \times L \otimes_F D, \tag{3}$$

such that the twist σ of $L \otimes_F L$ restricts on D to $a \mapsto \bar{a}$. Note that there are three natural imbeddings $L \to L \otimes_F D$. Two of them are given by $\lambda \mapsto \mathrm{pr}(\lambda \otimes 1)$ and $\lambda \mapsto \mathrm{pr}(1 \otimes \lambda)$, respectively (pr is the projection $L \otimes_F L \to L \otimes_F D$) and $L \to L \otimes_F D$, $\lambda \mapsto \lambda \otimes 1$, is the third one, which is σ-invariant. We have an induced decomposition

$$R = L \otimes_F L \otimes_F K = L \otimes_F K \times L \otimes_F D \otimes_F K. \tag{4}$$

The σ-action on R (see Lemma 5) restricts on $L \otimes_F D \otimes_F K$ to $\lambda \otimes d \otimes a \mapsto \lambda \otimes \bar{d} \otimes \bar{a}$, so the fixed subalgebra is

$$R^\sigma = L \times L \otimes_F H,$$

where $H = F(\sqrt{\alpha\delta})$.

LEMMA 7. *The decomposition of the R-module B induced by the decomposition (4) reduces to the decomposition*

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

over K. In particular $R^\sigma = L \times L \otimes_F H$ acts on $(B, \sigma)_+ = L \perp V$ componentwise and V is a free $L \otimes H$-module of rank one. Moreover the action given by the restriction $L \subset L \otimes H$ coincide with the Springer action, hence $N\colon V \to L$ is a nonsingular quadratic form on the free L-module V of rank 2. We have $N(hv) = n_{H/F}(h)N(v)$ for $h \in H$, so that N extends to a hermitian form on the $L \otimes_F H$-space V of rank one.

Proof. As for Lemma 6 it suffices to check the split case, where the claims follow by explicit computations. ∎

Let, as above, δ denote the discriminant of L. We recall that $\delta \in F^{\times 2}$ if and only if L is cyclic and that

$$Q_\sigma|_L = \langle 1, 2, 2\delta \rangle;$$

this is easy to check if L is not a field, since then $L = F \times F(\sqrt{\delta})$. The general case follows by extending scalars from F to L and applying Springer's theorem. Combining this result with Lemma 6, we get

$$Q_\sigma = \langle 1, 2, 2\delta \rangle \perp \langle 2 \rangle \cdot t_{L/F}(N), \tag{5}$$

where $t_{L/F}(N)$ denotes the Scharlau transfer of N.

PROPOSITION 8. *Let $K = F(\sqrt{\alpha})$. The following conditions are equivalent:*

(a) N is hyperbolic.

(b) $\delta = \alpha$ in $F^\times / F^{\times 2}$.

(c) LK is a cyclic extension of K and is Galois with Galois group $\mathcal{S}_3$ over F.

Moreover, if these conditions hold, then B is a crossed product:

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

for some x such that $x^3 \in F$ and $\sigma(x) = x$.

Proof. (a) $\Leftrightarrow$ (b): follows immediately from Lemma 7. Alternatively, if we only want to use Springer's Construction (Lemma 6), we get *(a) $\Rightarrow$ (b)* as follows: If N is hyperbolic, equation (5) yields:

$$\det Q_\sigma = -\delta.$$

On the other hand, Proposition 4 shows that $\det Q_\sigma = -\alpha$. Therefore, *(b)* follows.

(b) $\Rightarrow$ (c): If $\delta = \alpha$, then the discriminant of L becomes a square in K, hence LK/K is cyclic. Let ρ denote a generator of the Galois group $\mathrm{Gal}(LK/K)$. The restriction of σ to LK is an automorphism of order 2 of LK over F, hence $\sigma|_{LK}$ and ρ generate a group of automorphisms of order at least 6 of LK/K which shows that LK/F is Galois.

If $\alpha \neq 1$, then L/F is not cyclic, hence the group generated by ρ and $\sigma|_{LK}$ is not cyclic. It is therefore isomorphic to $\mathcal{S}_3$.

If $\alpha = \delta = 1$, then $B \simeq A \times A^{\mathrm{op}}$ and σ is isomorphic to the switch involution. Moreover, $LK \simeq L_0 \times L_0^{\mathrm{op}}$ for some cyclic extension L_0/F. If γ is a generator of the Galois group $\mathrm{Gal}(L_0/F)$, then we choose for ρ the automorphism of L given by:

$$\rho(\ell_1, \ell_2^{\mathrm{op}}) = (\gamma(\ell_1), \gamma^2(\ell_2)^{\mathrm{op}}).$$

Thus, σ and ρ do not commute; they generate a group isomorphic to $\mathcal{S}_3$.

Our next goal is to show that B contains an invertible element x such that $\sigma(x) = x$ and $x\ell = \rho(\ell)x$ for all $\ell \in LK$. These relations imply that x^3 centralizes LK, is σ-symmetric and commutes with x, hence $x^3 \in F$. Let

$$S = \{x \in (B, \sigma)_+ \colon x\ell = \rho(\ell)x \text{ for all } \ell \in LK\};$$

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 non-empty, we may extend scalars from F to an algebraic closure, and assume

$$B = \mathrm{M}_3(F) \times \mathrm{M}_3(F)^{\mathrm{op}},$$

σ is the switch involution, and

$$L = \{(d, d^{\mathrm{op}})\colon d \text{ is diagonal}\}.$$

We may further assume that ρ maps

$$\left(\begin{pmatrix} d_1 & & \\ & d_2 & \\ & & d_3 \end{pmatrix}, \begin{pmatrix} d_1' & & \\ & d_2' & \\ & & d_3' \end{pmatrix}^{\mathrm{op}}\right)$$

to

$$\left(\begin{pmatrix} d_3 & & \\ & d_1 & \\ & & d_2 \end{pmatrix}, \begin{pmatrix} d_2' & & \\ & d_3' & \\ & & d_1' \end{pmatrix}^{\mathrm{op}}\right);$$

we may then choose

$$x = \left(\begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}^{\mathrm{op}}\right) \in S \cap B^{\times},$$

proving the claim. It follows that B is a crossed product, as required.

(c) ⇒ (a): For every element x as above, we have $x, x^2 \in V$ (as is easily seen by scalar extension to an algebraic closure of F), hence $N(x) = 0$, proving that N is isotropic, hence hyperbolic since its dimension over L is 2. ∎

Remark. Proposition 8 can also be deduced from the Corollary of [12, Theorem 1] in relation with [11, Proposition 2.2].

In order to give an explicit description of the form N for general L, we need the following lemmas:

LEMMA 9. *Let $p_V\colon (B, \sigma)_+ \to V$ denote the orthogonal projection. For all $v \in V$,*

$$n_{L/F}(N(p_V(v^2))) = n_{L/F}(N(v))^2.$$

Proof. The lemma follows by explicit computation after extending scalars from F to an algebraic closure. ∎

LEMMA 10. *For any $\lambda \in L^\times$ such that $n_{L/F}(\lambda) \in F^{\times 2}$, the quadratic form*

$$\langle\langle \delta \rangle\rangle \cdot [t_{L/F}(\langle \lambda \rangle) \perp \langle -1 \rangle]$$

is hyperbolic.

Proof. By Springer's theorem, it suffices to prove that the quadratic form above is hyperbolic after extending scalars from F to L. We may thus assume $L = F \times F'$ where $F' = F(\sqrt{\delta})$. Let $\lambda = (\lambda_0, \lambda_1)$ with $\lambda_0 \in F$ and $\lambda_1 \in F'$; then

$$t_{L/F}(\langle \lambda \rangle) = \langle \lambda_0 \rangle \perp t_{F'/F}(\langle \lambda_1 \rangle). \tag{6}$$

By [16, p. 50], the image of the transfer map from the Witt ring WF' to WF is killed by $\langle\langle \delta \rangle\rangle$, hence

$$\langle\langle \delta \rangle\rangle \cdot t_{F'/F}(\langle \lambda_1 \rangle) = 0 \qquad \text{in } WF. \tag{7}$$

On the other hand,

$$n_{L/F}(\lambda) = \lambda_0 \, n_{F'/F}(\lambda_1) \in F^{\times 2},$$

hence λ_0 is a norm from F' to F, and therefore

$$\langle\langle \delta \rangle\rangle \cdot \langle \lambda_0, -1 \rangle = 0 \qquad \text{in } WF. \tag{8}$$

The lemma follows from (7) and (8), in view of the decomposition (6). ∎

PROPOSITION 11. *The quadratic form N has a diagonalization*

$$\langle\langle \alpha\delta \rangle\rangle \cdot \langle \lambda \rangle$$

for some $\lambda \in L^\times$ such that $n_{L/F}(\lambda) \in F^{\times 2}$. Consequently,

$$\begin{aligned} Q_\sigma &= \langle 1, 2, 2\delta \rangle \perp \langle 2 \rangle \cdot \langle\langle \alpha\delta \rangle\rangle \cdot t_{L/F}(\langle \lambda \rangle) \\ &= \langle 1, 1, 1 \rangle \perp \langle 2\delta \rangle \cdot \langle\langle \alpha \rangle\rangle \cdot t_{L/F}(\langle \lambda \rangle) \end{aligned}$$

for some $\lambda \in L^\times$ such that $n_{L/F}(\lambda) \in F^{\times 2}$.

Proof. Let $v \in V$ be such that $N(v)$ is invertible in L. Lemma 9 shows that $N(p_V(v^2))$ also is invertible. The element $p_V(v^2)$ is a basis of V as a $L \otimes H$-module, so that by Lemma 7, letting $\lambda = N(p_V(v^2))$, we get

$$N = \langle\langle \alpha\delta \rangle\rangle \cdot \langle \lambda \rangle$$

as wanted. Alternatively, without using Lemma 7, and letting $\lambda = N(p_V(v^2))$ as above, we have

$$N = \langle \lambda, \lambda' \rangle$$

for some $\lambda' \in L^\times$, and $n_{L/F}(\lambda) = n_{L/F}(N(v))^2 \in F^{\times 2}$, by Lemma 9. On the other hand, Proposition 8 shows that N becomes hyperbolic over $L(\sqrt{\alpha\delta})$, so $\det N = -\alpha\delta$, and therefore

$$N = \langle\langle \alpha\delta \rangle\rangle \cdot \langle \lambda \rangle.$$

The first formula for Q_σ then follows from (5) by Frobenius reciprocity. Since

$$\langle\langle \alpha\delta \rangle\rangle = \langle\langle \alpha \rangle\rangle \cdot \langle \delta \rangle + \langle\langle \delta \rangle\rangle \qquad \text{in } WF,$$

the following relation in WF follows:

$$Q_\sigma = \langle 1, 2, 2\delta \rangle + \langle 2\delta \rangle \cdot \langle\langle \alpha \rangle\rangle \cdot t_{L/F}(\langle \lambda \rangle) + \langle 2 \rangle \cdot \langle\langle \delta \rangle\rangle \cdot t_{L/F}(\langle \lambda \rangle).$$

Lemma 10 shows that the last term on the right-hand side is equal to $\langle 2 \rangle \cdot \langle\langle \delta \rangle\rangle$. Since

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

we get

$$Q_\sigma = \langle 1, 1, 1 \rangle + \langle 2\delta \rangle \cdot \langle\langle \alpha \rangle\rangle \cdot t_{L/F}(\langle \lambda \rangle) \qquad \text{in } WF.$$

Since both sides have the same dimension, these two quadratic forms are isometric, proving the second formula for Q_σ. ∎

COROLLARY 12. *The form q_σ defined in Proposition 4 may be chosen as*

$$q_\sigma = \langle\delta\rangle \cdot t_{L/F}(\langle\lambda\rangle)$$

for some $\lambda \in L^\times$ such that $n_{L/F}(\lambda) \in F^{\times 2}$.

Proof. According to [16, p. 51], we have

$$\det(t_{L/F}(\langle\lambda\rangle)) = \delta\, n_{L/F}(\lambda).$$

■

So far, the involution σ has been fixed, as well as the étale subalgebra $L \subset (B,\sigma)_+$. In the last proposition, we compare the quadratic forms Q_σ and $Q_{\sigma'}$ associated to two involutions of the second kind which leave L elementwise invariant. We denote by

$$q\colon L \to L$$

the quadratic map such that $\ell q(\ell) = n_{L/F}(\ell)$ for all $\ell \in L$.

PROPOSITION 13. *Let σ, σ' be two involutions on B such that $\sigma|_L = \sigma'|_L = I_L$:*

$$\sigma' = \mathrm{Int}(z) \circ \sigma$$

for some $z \in L^\times$. If $\lambda \in L^\times$ is such that

$$Q_\sigma = \langle 1, 2, 2\delta\rangle \perp \langle 2\rangle \cdot \langle\!\langle \alpha\delta \rangle\!\rangle \cdot t_{L/F}(\langle\lambda\rangle),$$

then

$$Q_{\sigma'} = \langle 1, 2, 2\delta\rangle \perp \langle 2\rangle \cdot \langle\!\langle \alpha\delta \rangle\!\rangle \cdot t_{L/F}(\langle q(z)\lambda\rangle).$$

Proof. The map $b \mapsto zb$ is an isomorphism $(B,\sigma)_+ \to (B,\sigma')_+$ which maps L to L; therefore, it also maps the orthogonal V of L in $(B,\sigma)_+$ to the orthogonal V' of L in $(B,\sigma')_+$. Let $N'\colon V' \to L$ denote the quadratic form

$$N'(v') = \tfrac{1}{2}\,\mathrm{Trd}(v'^2) - p'_L(v'^2) \qquad \text{for } v' \in V',$$

where $p'_L\colon (B,\sigma')_+ \to L$ denotes the orthogonal projection. An explicit computation, after extending scalars to an algebraic closure of F, shows that

$$N'(zv) = q(z)N(v) \qquad \text{for all } v \in V.$$

Therefore, multiplication by z defines a similarity $N \xrightarrow{\sim} N'$ with similarity factor $q(z)$. ■

Proposition 13 leads to the following converse of Proposition 11:

COROLLARY 14. *Let L be an arbitrary cubic étale F-subalgebra in B. For every $\lambda \in L^\times$ such that $n_{L/F}(\lambda) \in F^{\times 2}$, there is an involution σ on B leaving L elementwise invariant such that*

$$\begin{aligned} Q_\sigma &= \langle 1, 2, 2\delta\rangle \perp \langle 2\rangle \cdot \langle\langle \alpha\delta \rangle\rangle \cdot t_{L/F}(\langle\lambda\rangle) \\ &= \langle 1, 1, 1\rangle \perp \langle 2\delta\rangle \cdot \langle\langle \alpha \rangle\rangle \cdot t_{L/F}(\langle\lambda\rangle). \end{aligned}$$

Proof. By a theorem of Albert [1, p. 157], there is an involution τ leaving L elementwise invariant. Let

$$Q_\tau = \langle 1, 2, 2\delta\rangle \perp \langle 2\rangle \cdot \langle\langle \alpha\delta \rangle\rangle \cdot t_{L/F}(\langle\mu\rangle)$$

for some $\mu \in L^\times$ such that $n_{L/F}(\mu) \in F^{\times 2}$. If $\lambda \in L^\times$ is such that $n_{L/F}(\lambda) \in F^{\times 2}$, let $\xi \in F^\times$ be such that

$$n_{L/F}(\lambda\mu^{-1}) = \xi^2.$$

Since $n_{L/F}(\lambda\mu^{-1}) = \lambda\mu^{-1}q(\lambda\mu^{-1})$, the preceding equality yields:

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

Therefore, the preceding proposition shows that $\sigma = \mathrm{Int}(\xi\lambda^{-1}\mu) \circ \tau$ satisfies the required properties. ∎

4. A Classification of Involutions in Degree 3. In this section we continue to assume that B has degree 3 and that F has characteristic different from $2, 3$. By Proposition 4, the trace form of any involution σ of the second kind has the form

$$Q_\sigma = \langle 1, 1, 1\rangle \perp \langle 2\rangle \cdot \langle\langle \alpha \rangle\rangle \cdot \langle -b, -c, bc\rangle$$

where $K = F(\sqrt{\alpha})$ and $b, c \in F$. Our goal is to show that the 3-fold Pfister form $\langle\langle \alpha, b, c\rangle\rangle$ determines the involution σ up to isomorphism and to characterize the involutions for which this 3-fold Pfister form is hyperbolic.

For any Pfister form $\langle\langle a_1, \ldots, a_n\rangle\rangle$, we let $\langle\langle a_1, \ldots, a_n\rangle\rangle^\sharp = \langle 1\rangle^\perp$, so that

$$\langle\langle b, c\rangle\rangle^\sharp = \langle -b, -c, bc\rangle.$$

THEOREM 15. *Let σ, σ' be involutions of the second kind on a central simple K–algebra B of degree 3. Let*

$$Q_\sigma = \langle 1,1,1\rangle \perp \langle 2\rangle \cdot \langle\!\langle \alpha \rangle\!\rangle \cdot \langle\!\langle b,c\rangle\!\rangle^\sharp$$

and

$$Q_{\sigma'} = \langle 1,1,1\rangle \perp \langle 2\rangle \cdot \langle\!\langle \alpha \rangle\!\rangle \cdot \langle\!\langle b',c'\rangle\!\rangle^\sharp.$$

The following conditions are equivalent:

(a) The involutions σ and σ' are isomorphic.

(b) The quadratic forms Q_σ and $Q_{\sigma'}$ are isometric.

(c) The quadratic forms $\langle\!\langle \alpha \rangle\!\rangle \cdot \langle\!\langle b,c\rangle\!\rangle^\sharp$ and $\langle\!\langle \alpha \rangle\!\rangle \cdot \langle\!\langle b',c'\rangle\!\rangle^\sharp$ are isometric.

(d) 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.

(e) The quadratic forms $\langle\!\langle \alpha,b,c\rangle\!\rangle$ and $\langle\!\langle \alpha,b',c'\rangle\!\rangle$ are isometric.

Proof. *(a)* $\Rightarrow$ *(b)* is already in Lemma 1, and *(b)* $\Longleftrightarrow$ *(c)* $\Longleftrightarrow$ *(e)* follows by Witt cancellation. Moreover, *(c)* $\Rightarrow$ *(d)* is a theorem of Jacobson [7] if K is a field, and is clear if $K = F \times F$. We finally check that *(d)* $\Rightarrow$ *(a)*. If $K = F \times F$, all involutions on $B \simeq A \times A^{\mathrm{op}}$ are isomorphic to the switch involution, so *(a)* holds trivially. Thus we are reduced to the case K a field. Assume next that $B = \mathrm{M}_3(K)$ is split. Up to automorphisms of (B,σ), resp. (B,σ'), we have $\sigma = \mathrm{Int}(a)\circ\tau$, resp. $\sigma' = \mathrm{Int}(a')\circ\tau$ with $a = \mathrm{diag}(\alpha_1,\alpha_2,\alpha_3)$ and $a' = \mathrm{diag}(\alpha'_1,\alpha'_2,\alpha'_3)$. We may assume that $\alpha_1\alpha_2\alpha_3 = 1 = \alpha'_1\alpha'_2\alpha'_3$. By Proposition 2, we have

$$Q_\sigma \simeq \langle 1,1,1\rangle \perp \langle 2\rangle \cdot \langle\!\langle \alpha \rangle\!\rangle \cdot \langle \alpha_2\alpha_3^{-1}, \alpha_3\alpha_1^{-1}, \alpha_1\alpha_2^{-1}\rangle$$

and

$$Q_{\sigma'} \simeq \langle 1,1,1\rangle \perp \langle 2\rangle \cdot \langle\!\langle \alpha \rangle\!\rangle \cdot \langle \alpha'_2{\alpha'_3}^{-1}, \alpha'_3{\alpha'_1}^{-1}, \alpha'_1{\alpha'_2}^{-1}\rangle.$$

Thus

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

Since

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

we get isometries $h_a \simeq h_{a'}$ or $\langle a\rangle_{\mathrm{M}_3(K)} \simeq \langle a'\rangle_{\mathrm{M}_3(K)}$ and $(\mathrm{M}_3(K), \sigma)$ is isomorphic to $(\mathrm{M}_3(K), \sigma')$ by Lemma 1.

If B is not split and if $\sigma' = \mathrm{Int}(u)\circ\sigma$, we have to check by Lemma 1 that the hermitian spaces $\langle u\rangle_B$ and $\langle 1\rangle_B$ are similar. Replacing u by $u \cdot \mathrm{Nrd}(u)$, we may assume that $\mathrm{Nrd}(u) \in {F^\times}^2$. Let $L = F(x)$ with $x \in (B, \sigma)_+, x \notin F$, so that L is a field extension of F of degree 3. The algebra $B \otimes_F L$ is split over $K \otimes_F L^\times$ and there is $v' \in \mathrm{GL}_3(K \otimes_F L)$ such that

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

Thus, denoting by $\bar{}\colon K \to K$ the non-trivial automorphism of K/F,

$$\mathrm{Nrd}(u \otimes 1) = \lambda^3 \,\mathrm{Nrd}(v')\overline{\mathrm{Nrd}(v')} = \mu^2$$

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

$$\lambda = (\mu\lambda^{-1}\,\mathrm{Nrd}(v')^{-1})(\overline{\mu\lambda^{-1}\,\mathrm{Nrd}(v')^{-1}}) = \nu\overline{\nu}.$$

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 [4] generalization of Springer's theorem to hermitian spaces, we have $\langle u\rangle_B \simeq \langle 1\rangle_B$ and, by Lemma 1, $(B, \sigma) \simeq (B, \sigma')$. ∎

In view of the equivalence *(a)* $\Longleftrightarrow$ *(e)* in Theorem 15, the Pfister form $\langle\langle\alpha, b, c\rangle\rangle$ classifies involutions σ on B. We denote it by $\pi(B, \sigma)$. Note that $\pi(B, \sigma)$ is isometric to the norm of the octonion algebra $\mathrm{Oct}A$ associated in [14] to any simple Jordan algebra A of degree 3 and dimension 9, if $A = (B, \sigma)_+$. Let

$$(B, \sigma)^\circ_+ = \{x \in (B, \sigma)_+\colon \mathrm{Trd}(x) = 0\} = 1^\perp \subset (B, \sigma)_+.$$

Since $Q_\sigma(1) = 3$, the restriction Q°_σ of Q_σ to $(B, \sigma)^\circ_+$ is given by

$$Q^\circ_\sigma \simeq \langle 2, 6\rangle \perp \langle 2\rangle \cdot \langle\langle\alpha\rangle\rangle \cdot \langle\langle b, c\rangle\rangle^\sharp \simeq \langle 2\rangle \cdot (\langle 1, 3\rangle \perp \langle\langle\alpha\rangle\rangle \cdot \langle\langle b, c\rangle\rangle^\sharp).$$

In the Witt ring WF, we have

$$\langle\langle\alpha\rangle\rangle \cdot \langle\langle b, c\rangle\rangle^\sharp = \langle\langle\alpha, b, c\rangle\rangle - \langle\langle\alpha\rangle\rangle;$$

therefore,

$$Q_\sigma^\circ = \langle 2\rangle \cdot (\langle 3, \alpha\rangle + \langle\langle \alpha, b, c\rangle\rangle) \qquad \text{in } WF.$$

Comparing dimensions on both sides, we see that the Witt indices of both sides are related by:

$$w(Q_\sigma^\circ) = w(\langle 3, \alpha\rangle \perp \langle\langle \alpha, b, c\rangle\rangle) - 1. \tag{9}$$

Isotropic elements of Q_σ° are elements $u \in (B, \sigma)_+$ such that $\mathrm{Trd}(u) = \mathrm{Trd}(u^2) = 0$. Since the reduced characteristic polynomial of any $a \in B$ has the form

$$X^3 - \mathrm{Trd}(a)X^2 + \tfrac{1}{2}\left[\mathrm{Trd}(a)^2 - \mathrm{Trd}(a^2)\right] X - \mathrm{Nrd}(a) \cdot 1,$$

it follows that u is isotropic if and only if $u^3 = \mathrm{Nrd}(u) \in F$.

THEOREM 16. *The following conditions are equivalent:*

(a) $\pi(B, \sigma)$ *is hyperbolic;*

(b) Either $K = F \times F$ *or* $\langle -b, -c, bc\rangle_K \simeq \langle 1, -1, -1\rangle_K$*;*

(c) $w(Q_\sigma^\circ) \geq 2$*;*

(c') $(B, \sigma)_+$ *contains a subspace* U *of dimension 2 whose elements satisfy:* $u^3 = \mathrm{Nrd}(u)$*;*

(d) $w(Q_\sigma^\circ) \geq 3$*;*

(d') $(B, \sigma)_+$ *contains a subspace* U *of dimension 3 whose elements satisfy:* $u^3 = \mathrm{Nrd}(u)$*;*

(e) $(B, \sigma)_+$ *contains an étale cubic* F*-algebra* L *of discriminant* α*.*

(f) B *is a crossed product:*

$$B = M \oplus M\,x \oplus M\,x^2,$$

where M $(\supset K)$ *is a Galois extension of* F *with Galois group* $\mathcal{S}_3$*, the involution* σ *preserves* M *and leaves* x *invariant.*

Proof. *(a)* $\Rightarrow$ *(b)* is a straightforward consequence of Theorem 15, and *(c)* $\Longleftrightarrow$ *(c')*, *(d)* $\Longleftrightarrow$ *(d')* follow from the preceding observations on isotropic elements in Q_σ°. Moreover, *(a)* $\Rightarrow$ *(d)* follows from (9), *(e)* $\Longleftrightarrow$ *(f)* from Proposition 8, and *(d)* $\Rightarrow$ *(c)* is clear. We now show *(c)* $\Rightarrow$ *(a):* if the Witt index of Q_σ° is at least 2, then (9) shows that $\langle 3, \alpha\rangle \perp \langle\langle \alpha, b, c\rangle\rangle$ contains isotropic subspaces of dimension 3. Therefore, $\langle\langle \alpha, b, c\rangle\rangle$ is isotropic, hence hyperbolic, proving *(a)*. Assuming *(e)*, the formula for Q_σ in Proposition 11 shows that $w(Q_\sigma^\circ) \geq 3$, hence *(e)* $\Rightarrow$ *(d)*. To complete the proof, we show *(c')* $\Rightarrow$ *(e)*, using results from [6]. We first consider the easy special case where B is not a division algebra. If $\alpha = 1$ in $F^\times/F^{\times 2}$, then we may assume

$$B = A \times A^{\mathrm{op}}$$

for some central simple F-algebra A of degree 3, and σ is the switch involution. A theorem of Wedderburn [1] shows that A contains a cyclic extension L of F. We may then choose

$$M = \{(\ell, \ell^{\mathrm{op}})\colon \ell \in L\}.$$

If B is split, then since *(c')* $\Rightarrow$ *(b)*, it follows that σ is the adjoint involution with respect to an isotropic hermitian form. We may thus assume $B = \mathrm{M}_3(K)$ and $\sigma = \mathrm{Int}(u) \circ \tau$, where $u = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}$. We may then choose

$$M = \left\{ \begin{pmatrix} f & 0 & 0 \\ 0 & k & 0 \\ 0 & 0 & \overline{k} \end{pmatrix} : f \in F,\ k \in K \right\}.$$

For the rest of the proof of *(c')* $\Rightarrow$ *(e)*, we now assume that B is a division algebra. Let $U \subset (B, \sigma)_+$ be a subspace of dimension 2 such that $u^3 = \mathrm{Nrd}(u)$ for all $u \in U$. According to Lemma 2 of [6], one can find a basis (w_1, w_2) of U such that

$$\mathrm{Trd}(w_1^{-1} w_2) = 0.$$

Following [6], we let

$$\theta_1 = w_1^{-1}w_2, \qquad \theta_2 = w_1^{-1}\theta_1 w_1, \qquad \theta_3 = w_1^{-1}\theta_2 w_1.$$

Note $\theta_2 = w_1^{-3}(w_1w_2w_1)$, so $\sigma(\theta_2) = \theta_2$. We let also $E = K(\theta_2^{-1}\theta_3)$ if $\theta_2^{-1}\theta_3 \notin K$ and $E = K(\theta_2)$ if $\theta_2^{-1}\theta_3 \in K$. Theorem 3 of [6] shows that E/K is cyclic and E/F is Galois with Galois group $\mathcal{S}_3$. Moreover, one of the order 2 automorphisms of E/F is the restriction of the involution

$$\sigma' = \mathrm{Int}(\theta_2^{-1}) \circ \sigma.$$

Let $L' \subset E$ denote the subfield of σ'-invariant elements. Since $L'K = E$ is cyclic over K and Galois over F with group $\mathcal{S}_3$, Proposition 8 shows that the discriminant of L'/F is α.

Observe now that

$$\theta_2 = w_1^{-3}w_2^{-3}(w_1w_2^2)(w_2^2w_1),$$

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

$$\mathrm{Int}(v)\colon (B,\sigma) \xrightarrow{\sim} (B,\sigma')$$

is an isomorphism of algebras with involution. Pulling $L' \subset (B,\sigma')_+$ back gives the wanted extension $L \subset (B,\sigma)_+$. ∎

Remark. Theorem 16 gives a positive answer to a question about Tits constructions asked in [14, (2.12)].

An involution σ satisfying the equivalent conditions of Theorem 16 is called **distinguished**. By Theorem 15, two distinguished involutions on B are isomorphic. The existence of distinguished involutions is clear if $B \simeq \mathrm{M}_3(K)$ is split: the adjoint involution with respect to any isotropic hermitian form on K^3 is distinguished. If $K = F \times F$, the switch involution on $B \simeq A \times A^{\mathrm{op}}$ is distinguished: in fact we have $\alpha = 1$, so that $\langle\langle\alpha\rangle\rangle = \langle 1, -1\rangle$ and Q_σ° has Witt index at least 3. The existence in general of distinguished involutions for algebras of degree 3 is shown next.

Proposition 17. *For every cubic étale F-algebra $L \subset B$, there is a distinguished involution σ such that $L \subset (B,\sigma)_+$.*

Proof. Let $\lambda_0 \in L^\times$ be such that $t_{L/F}(\lambda_0) = 0$, and let

$$\lambda = \lambda_0 / n_{L/F}(\lambda_0);$$

then $n_{L/F}(\lambda) = n_{L/F}(\lambda_0)^{-2} \in F^{\times 2}$ and $t_{L/F}(\lambda) = 0$. Corollary 14 shows that there is an involution σ on B such that $L \subset (B, \sigma)_+$ and

$$Q_\sigma = \langle 1, 1, 1\rangle \perp \langle 2\delta\rangle \cdot \langle\langle \alpha \rangle\rangle \cdot t_{L/F}(\langle \lambda \rangle),$$

hence

$$Q_\sigma^\circ = \langle 2\rangle \cdot (\langle 1, 3\rangle \perp \langle \delta\rangle \cdot \langle\langle \alpha \rangle\rangle \cdot t_{L/F}(\langle \lambda \rangle)).$$

Since $t_{L/F}(\lambda) = 0$, the form $t_{L/F}(\langle \lambda \rangle)$ is isotropic, hence the Witt index of $\langle\langle \alpha \rangle\rangle \cdot t_{L/F}(\langle \lambda \rangle)$ is at least 2. Therefore, condition *(c)* of Theorem 16 holds. ∎

Alternative proof. Pick an involution σ_0 such that $L \subset (B, \sigma_0)_+$ and denote by V the orthogonal of L with respect to Q_{σ_0}, as in the preceding section. By Zariski density, we may find an invertible element $v \in V$ such that $n_{L/F}(N(v)) \neq 0$, where $N\colon V \to L$ is the quadratic form defined in section 3. Lemma 6 shows:

$$\operatorname{Trd}(v^{-1}\ell) = -\operatorname{Nrd}(v)^{-1} t_{L/F}(N(v)\ell)$$

for all $\ell \in L$. Since $N(v)$ is invertible in L, we may, again by Zariski density, find $\ell \in L^\times$ such that

$$\operatorname{Trd}(v^{-1}\ell) = 0.$$

Following [6, Proposition 1], the vector space

$$U = v^{-1}L \cap \ker \operatorname{Trd}$$

is at least 2-dimensional over F and satisfies: $u^3 = \operatorname{Nrd}(u)$ for all $u \in U$. We then have $v^{-1}\ell \in U$ for $\ell \in L$ as above. Let

$$\sigma = \operatorname{Int}(\ell^{-1}) \circ \sigma_0.$$

Since $L \subset (B, \sigma_0)_+$ and $\ell \in L^\times$, it follows that $L \subset (B, \sigma)_+$. We claim that σ is distinguished. Let $y = \ell^{-1}v \in B^\times$, then

$$yU = \ell^{-1}(vU) \subset L \subset (B, \sigma)_+$$

and

$$\sigma(y) = \ell^{-1}\sigma_0(y)\ell = \ell^{-1}v\ell^{-1}\ell = y,$$

hence $(B,\sigma)_+$ contains $y^2Uy = y(yU)y$. Since $v^{-1}\ell \in U$, we have $y^{-1} \in U$, hence $y^3 = \mathrm{Nrd}(y) \in F^\times$. For $u \in U$, we have $u^3 = \mathrm{Nrd}(u) \in F$, hence

$$\begin{aligned}(y^2uy)^3 &= y^2uy \cdot y^2uy \cdot y^2uy = y^2u^3y\ \mathrm{Nrd}(y)^2\\ &= \mathrm{Nrd}(u)\,\mathrm{Nrd}(y)^3 = \mathrm{Nrd}(y^2uy).\end{aligned}$$

Therefore, $y^2Uy \subset (B,\sigma)_+$ is a subspace of dimension ≥ 2 whose elements satisfy $x^3 = \mathrm{Nrd}(x)$, hence σ is distinguished. ∎

A third proof of the existence of distinguished involutions is given in Proposition 31.

Corollary 18. *The space $(B,\sigma)_+$ contains an isomorphic copy of every cubic étale F-subalgebra L of B if and only if σ is distinguished.*

Proof. Since all the distinguished involutions on a central simple algebra B are isomorphic, the if direction follows from Proposition 17. Conversely, by Theorem 16, *(e)*, the only involutions which leave elementwise invariant étale cubic F-subalgebras of discriminant α are the distinguished involutions. ∎

The fact that the only involutions which leave elementwise invariant étale cubic F-subalgebras of discriminant α are the distinguished involutions also follows from the following general result:

Proposition 19. *Let σ be an involution on B and let L be a cubic étale F-algebra such that $L \subset (B,\sigma)_+$. Let $\delta \in F^\times$ represent the discriminant of L/F. The Pfister form $\pi(B,\sigma)$ has a factorization:*

$$\pi(B,\sigma) = \langle\langle \alpha \rangle\rangle \cdot \varphi$$

where φ is a 2-fold Pfister form whose pure subform satisfies:

$$\varphi^\sharp = t_{L/F}(\langle \ell \rangle)$$

for some $\ell \in L^\times$ such that

$$n_{L/F}(\ell) \in \delta \cdot F^{\times 2}.$$

In particular,

$$\varphi \cdot \langle\langle \delta \rangle\rangle = 0.$$

Proof. Proposition 11 shows that

$$Q_\sigma = \langle 1, 1, 1 \rangle \perp \langle 2 \rangle \cdot \langle\langle \alpha \rangle\rangle \cdot t_{L/F}(\langle \delta\lambda \rangle)$$

where $\lambda \in L^\times$ is such that $n_{L/F}(\lambda) \in F^{\times 2}$. Letting $\ell = \delta\lambda$, we get $n_{L/F}(\ell) \in \delta \cdot F^{\times 2}$ and $t_{L/F}(\langle \ell \rangle)$ is a 3-dimensional form of determinant 1. Comparing with the form of Q_σ in Theorem 15, we obtain:

$$\pi(B, \sigma) = \langle\langle \alpha \rangle\rangle \cdot (\langle 1 \rangle \perp t_{L/F}(\langle \ell \rangle)).$$

The relation $(\langle 1 \rangle \perp t_{L/F}(\langle \delta\lambda \rangle)) \cdot \langle\langle \delta \rangle\rangle = 0$ follows from Lemma 10, using the fact that $\langle -\delta \rangle \cdot \langle\langle \delta \rangle\rangle = \langle\langle \delta \rangle\rangle$. ∎

The condition $\varphi \cdot \langle\langle \delta \rangle\rangle = 0$ in the proposition above yields some restriction on the discriminants of cubic F-algebras L which lie in $(B, \sigma)_+$. It does not yield any information on cyclic extensions however, since in this case $\langle\langle \delta \rangle\rangle = 0$. Nevertheless, there are examples where $(B, \sigma)_+$ does not contain any cyclic cubic extension of F. Consider for instance the "symbol algebra" $A_\omega(s, t)$ generated over the iterated powerseries field $\mathbb{C}((s))((t))$ by two indeterminates i, j subject to the relations:

$$i^3 = s, \qquad j^3 = t, \qquad ji = \omega ij,$$

where ω is a primitive cube root of unity. This algebra carries an involution σ extending conjugation on $\mathbb{C}$ such that

$$\sigma(i) = i, \qquad \sigma(j) = j.$$

The subfield consisting of the σ-invariant elements in the center $\mathbb{C}((s))((t))$ is $\mathbb{R}((s))((t))$, which does not have any non-trivial cyclic extension of odd degree. Therefore, the space of symmetric elements

$(A_\omega(s,t),\sigma)_+$ does not contain any cyclic extension of F of degree 3. We are indebted to H.P. Petersson (see [13]) for suggesting this example.

Let L be an arbitrary cubic étale F-subalgebra in B. Let $\Sigma(B,L)$ be the pointed set of isomorphism classes of involutions σ of B such that $\sigma|_L = I_L$, the point being given by the class of distinguished involutions.

COROLLARY 20. *The map $\mu \in L^\times \mapsto \sigma_\mu$, where σ_μ is the involution determined up to isomorphism by the trace form*

$$Q_{\sigma_\mu} = \langle 1,1,1\rangle \perp \langle 2\delta\rangle \cdot \langle\langle \alpha\rangle\rangle \cdot t_{L/F}(\langle q(\mu)\rangle_L),$$

induces a surjective map of pointed sets

$$L^\times/n_{LK/L}(LK^\times)\cdot F^\times \to \Sigma(B,L).$$

If L/F is cyclic, the map is well-defined on the set of orbits of the group $\mathrm{Gal}(L/F)$ *in*
$L^\times/n_{LK/L}(LK^\times)\cdot F^\times$.

Proof. The proof of Corollary 14 shows that the elements $\lambda \in L$ such that $n_{L/F}(\lambda) \in {F^\times}^2$ are exactly the elements of the form $q(\mu)$ for $\mu \in L^\times$. Thus, by Corollary 14, Q_{σ_μ} is the trace form of an involution σ_μ. Elements μ, $\mu' \in L^\times$ such that $\mu' = \xi n_{LK/L}(\eta)\mu$ for $\eta \in LK^\times$ and $\xi \in F^\times$ give isomorphic involutions in view of Theorem 15, *(d)*, since $q(\mu') = \xi^2\, q(\eta)\, q(\mu)\, \overline{q(\eta)}$ implies that the hermitian forms $\langle q(\mu)\rangle_{LK}$ and $\langle q(\mu')\rangle_{LK}$ are isomorphic. ∎

5. Cohomology and Symbols. Let F be a field of characteristic different from 2; let F_s denote a separable closure of F and $\Gamma = \mathrm{Gal}(F_s/F)$. For any integer n relatively prime to the characteristic of F, let

$$\mu_n = \{x \in F_s\colon x^n = 1\}$$

denote the Γ-module of n-th roots of 1. The Kummer exact sequence

$$1 \to \mu_n \to F_s^\times \xrightarrow{n} F_s^\times \to 1$$

and Hilbert's Theorem 90 yield canonical isomorphisms:

$$H^1(\Gamma, \mu_n) = F^\times / F^{\times n} \qquad \text{and} \qquad H^2(\Gamma, \mu_n) = {}_n\mathrm{Br}(F),$$

where ${}_n\mathrm{Br}(F)$ denotes the subgroup killed by n in the Brauer group $\mathrm{Br}(F)$. Since the action of Γ on μ_2 is trivial, we also have

$$H^1(\Gamma, \mu_2) = \mathrm{Hom}(\Gamma, \{\pm 1\}).$$

For any $\alpha \in F^\times$, let $\phi_\alpha\colon \Gamma \to \{\pm 1\}$ be the (continuous) homomorphism corresponding to $\alpha \cdot F^{\times 2}$ under the identification: $F^\times / F^{\times 2} = \mathrm{Hom}(\Gamma, \{\pm 1\})$; it is explicitly defined by:

$$\phi_\alpha(\gamma) = \left\{ \begin{array}{ll} +1 & \text{if } \gamma \text{ leaves invariant} \\ -1 & \text{if } \gamma \text{ permutes} \end{array} \right\} \text{the square roots of } \alpha \text{ in } F_s.$$

We then define a Γ-module $\mathbb{Z}(\alpha)$ by twisting the trivial action of Γ on $\mathbb{Z}$: for $\gamma \in \Gamma$ and $z \in \mathbb{Z}$, we let $\gamma \cdot z = \phi_\alpha(\gamma) z$. Multiplication in $\mathbb{Z}$ yields a canonical isomorphism:

$$\mathbb{Z}(\alpha) \otimes_{\mathbb{Z}} \mathbb{Z}(\beta) = \mathbb{Z}(\alpha\beta) \qquad \text{for } \alpha, \beta \in F^\times,$$

since $\phi_\alpha(\gamma)\phi_\beta(\gamma) = \phi_{\alpha\beta}(\gamma)$ for all $\gamma \in \Gamma$.

For any Γ-module M, we define a twisted module $M(\alpha)$ by:

$$M(\alpha) = M \otimes_{\mathbb{Z}} \mathbb{Z}(\alpha).$$

The Galois cohomology groups $H^\ell(\Gamma, M)$ are also denoted $H^\ell(F, M)$.

PROPOSITION 21. *Let $K = F(\sqrt{\alpha})$ be a quadratic field extension of F. For all $\ell \geq 1$ and all Γ-modules M on which multiplication by 2 is invertible, the following sequence is split exact:*

$$0 \to H^\ell(F, M(\alpha)) \xrightarrow{\text{res}} H^\ell(K, M) \xrightarrow{\text{cor}} H^\ell(F, M) \to 0$$

where res *(resp.* cor*) is the restriction (resp. the corestriction) map.*

The restriction map identifies $H^\ell(F, M(\alpha))$ with the subgroup of $H^\ell(K, M)$ consisting of the classes of cocycles which are cohomologous to the negative of their conjugate under the action of $\mathrm{Gal}(K/F)$*:*

$$H^\ell(F, M(\alpha)) = \{\varphi \in H^\ell(K, M)\colon \varphi + \overline{\varphi} = 0\}.$$

Proof. From the definition of $M(\alpha)$, it is clear that $M = M(\alpha)$ as modules over $\mathrm{Gal}(F_s/K)$. Let $G = \mathrm{Gal}(K/F) = \{1, \iota\}$ and let $IG = \mathbb{Z}\cdot(1-\iota)$ denote the augmentation ideal in the group ring $\mathbb{Z}\,G$. Denote by Σ the augmentation map:

$$\Sigma\colon\ \mathbb{Z}\,G \to \mathbb{Z}$$

and define Γ-module homomorphisms $s\colon\ \mathbb{Z} \to \mathbb{Z}\,G$ and $t\colon\ \mathbb{Z}\,G \to IG$ by:

$$s(z) = z(1+\iota), \qquad t(x) = (1-\iota)x \qquad \text{for } z \in \mathbb{Z},\ x \in \mathbb{Z}\,G.$$

These maps fit into a commutative diagram:

$$\begin{array}{ccccccccc} 0 & \leftarrow & IG & \xleftarrow{t} & \mathbb{Z}\,G & \xleftarrow{s} & \mathbb{Z} & \leftarrow & 0 \\ & & \uparrow{\scriptstyle 2\cdot} & & \| & & \downarrow{\scriptstyle 2\cdot} & & \\ 0 & \to & IG & \longrightarrow & \mathbb{Z}\,G & \xrightarrow{\Sigma} & \mathbb{Z} & \to & 0 \end{array}$$

Observe that $IG \simeq \mathbb{Z}(\alpha)$; therefore, tensoring the diagram above with M, we get the following commutative diagram:

$$\begin{array}{ccccccccc} 0 & \leftarrow & M(\alpha) & \xleftarrow{t} & M \otimes_{\mathbb{Z}} \mathbb{Z}\,G & \xleftarrow{s} & M & & \\ & & \uparrow{\scriptstyle 2\cdot} & & \| & & \downarrow{\scriptstyle 2\cdot} & & \\ & & M(\alpha) & \xrightarrow{i} & M \otimes_{\mathbb{Z}} \mathbb{Z}\,G & \xrightarrow{\Sigma} & M & \to & 0 \end{array}$$

and since multiplication by 2 is invertible on M, it follows that the sequence

$$0 \to M(\alpha) \xrightarrow{i} M \otimes_{\mathbb{Z}} \mathbb{Z}\,G \xrightarrow{\Sigma} M \to 0$$

is split exact. It yields a split exact sequence in cohomology:

$$0 \to H^\ell(F, M(\alpha)) \xrightarrow{i_*} H^\ell(F, M \otimes \mathbb{Z}\,G) \xrightarrow{\Sigma_*} H^\ell(F, M) \to 0.$$

By the lemma of Eckmann–Faddeev–Shapiro, there is an isomorphism

$$\psi\colon H^\ell(F, M \otimes \mathbb{Z}\,G) \xrightarrow{\sim} H^\ell(K, M)$$

such that $\Sigma_* = \mathrm{cor} \circ \psi$ and $\psi \circ i_* = \mathrm{res}$. This proves the first part.

Let $\mathrm{res}' : H^\ell(F, M) \to H^\ell(K, M)$ denote the restriction map. For $\varphi \in H^\ell(K, M)$, we have:

$$\mathrm{res}' \circ \mathrm{cor}(\varphi) = \varphi + \overline{\varphi}, \tag{10}$$

hence $\varphi + \overline{\varphi} = 0$ if $\mathrm{cor}(\varphi) = 0$. Conversely, applying cor to both sides of (10), we get:

$$2\ \mathrm{cor}(\varphi) = \mathrm{cor}(\varphi + \overline{\varphi}),$$

since $\mathrm{cor} \circ \mathrm{res}' = 2$. Since multiplication by 2 is invertible on M, it follows that $\mathrm{cor}(\varphi) = 0$ if $\varphi + \overline{\varphi} = 0$. Therefore, the image of $H^\ell(F, M(\alpha))$ in $H^\ell(K, M)$ can be indifferently described as the kernel of the corestriction map or as the kernel of the map $\varphi \mapsto \varphi + \overline{\varphi}$. ■

Remark. If multiplication by 2 is not invertible on M, the restriction and corestriction maps fit into a long exact sequence described by Arason and Elman in [3, Appendix].

We shall apply this proposition to the special cases where $M = \mathbb{Z}/n\,\mathbb{Z}$ (n odd) with trivial action and $M = \mu_n = \{x \in F_s\colon x^n = 1\}$ (assuming n odd and relatively prime to the characteristic of F). We first review how, for an arbitrary finite group $\mathcal{G}$, the first cohomology set $H^1(F, \mathcal{G})$, where the Galois action on $\mathcal{G}$ is trivial, is related to Galois extensions of F with Galois group $\mathcal{G}$. We recall that, in this case,

$$H^1(F, \mathcal{G}) = \mathrm{Hom}(\Gamma, \mathcal{G})/\sim,$$

where $\mathrm{Hom}(\Gamma, \mathcal{G})$ is the set of continous homomorphisms $\Gamma \to \mathcal{G}$ and $\chi' \sim \chi$ if $\chi'(\gamma) = g\chi(\gamma)g^{-1}$ for some $g \in \mathcal{G}$. In particular we have $H^1(F, \mathcal{G}) = \mathrm{Hom}(\Gamma, \mathcal{G})$ if $\mathcal{G}$ is abelian.

Let L be a finite-dimensional commutative algebra over F and let

$$X(L) = \mathrm{Alg}_F(L, F_s)$$

denote the set of F-algebra homomorphisms $L \to F_s$. Let $\mathcal{G}$ be an arbitrary finite group acting on L by F-algebra automorphisms $\ell \mapsto g * \ell$. We call L a **Galois $\mathcal{G}$-algebra** if L is étale of dimension $n = |\mathcal{G}|$ over F and the action of $\mathcal{G}$ on $X(L)$ is simply transitive.

Now, assume L is a Galois $\mathcal{G}$-algebra and fix some $\xi \in X(L)$. For every $\gamma \in \Gamma$, there is a unique $\chi_\xi(\gamma) \in \mathcal{G}$ such that

$$\gamma(\xi(\ell)) = \xi(\chi_\xi(\gamma) * \ell) \qquad \text{for all } \ell \in L.$$

The map $\chi_\xi \colon \Gamma \to \mathcal{G}$ is a continuous homomorphism:

$$\chi_\xi \in \mathrm{Hom}(\Gamma, \mathcal{G}).$$

If L, L' are Galois $\mathcal{G}$-algebras over F and $\xi \in X(L)$, $\xi' \in X(L')$, an isomorphism $\psi \colon (L, \xi) \xrightarrow{\sim} (L', \xi')$ is an isomorphism of algebras over F which commutes with the action of $\mathcal{G}$ and such that $\xi' \circ \psi = \xi$. An isomorphism of Galois $\mathcal{G}$-algebras $\psi \colon L \xrightarrow{\sim} L'$ is an isomorphism of algebras over F which commutes with the action of $\mathcal{G}$.

PROPOSITION 22. *The map $(L, \xi) \mapsto \chi_\xi$ defines a 1–1 correspondence between the set of isomorphism classes of couples (L, ξ), where L is a Galois $\mathcal{G}$-algebra and $\xi \in X(L)$, and the set* $\mathrm{Hom}(\Gamma, \mathcal{G})$. *Moreover $L \mapsto \chi_\xi$ induces a 1–1 correspondence between the set of isomorphism classes of Galois $\mathcal{G}$-algebras and the set $H^1(F, \mathcal{G})$.*

Proof. This proposition is presumably well-known (see for example [17]), but we include a sketch of proof for the reader's convenience. For $\chi \in \mathrm{Hom}(\Gamma, \mathcal{G})$, we define an action of Γ on the algebra $\mathfrak{F}(\mathcal{G}, F_s)$ of maps $\mathcal{G} \to F_s$ by:

$$(\gamma \diamond f)(x) = \gamma(f(\chi(\gamma)^{-1} x)) \qquad \text{for } \gamma \in \Gamma,\ x \in \mathcal{G}.$$

Let $\mathfrak{F}_\chi$ denote the algebra of invariant elements under this action:

$$\mathfrak{F}_\chi = \{f \colon \mathcal{G} \to F_s \colon \gamma(f(x)) = f(\chi(\gamma)x) \text{ for } \gamma \in \Gamma,\ x \in \mathcal{G}\}.$$

This algebra carries a natural $\mathcal{G}$-action defined by:

$$(g * f)(x) = f(xg) \qquad \text{for } x, g \in \mathcal{G},\ f \in \mathfrak{F}_\chi.$$

Moreover, for $g \in \mathcal{G}$, there is an F-algebra homomorphism

$$\varepsilon_g \colon \mathfrak{F}_\chi \to F_s$$

defined by:

$$\varepsilon_g(f) = f(g) \qquad \text{for } f \in \mathfrak{F}_\chi,$$

and $X(\mathfrak{F}_\chi) = \{\varepsilon_g \colon g \in \mathcal{G}\}$. It is then straightforward to check that $\mathfrak{F}_\chi$ is a Galois $\mathcal{G}$-algebra, and that $\chi_{\varepsilon_1} = \chi$.

For any Galois $\mathcal{G}$-algebra L and any $\xi \in X(L)$, there exists a unique isomorphism $(L, \xi) \xrightarrow{\sim} (\mathfrak{F}_{\chi_\xi}, \varepsilon_1)$: this isomorphism maps $\ell \in L$ to $f_\ell \in \mathfrak{F}_\chi$ defined by:

$$f_\ell(g) = \xi(g * \ell) \qquad \text{for } g \in \mathcal{G}.$$

Let now $\xi, \eta \in X(L)$. By definition of Galois algebra, there is a unique element $g \in \mathcal{G}$ such that $\eta(\ell) = \xi(g * \ell)$ for all $\ell \in L$. Then, for $\gamma \in \Gamma$ and $\ell \in L$,

$$\gamma(\eta(\ell)) = \gamma(\xi(g * \ell)) = \xi(\chi_\xi(\gamma) g * \ell) = \xi(g * (g^{-1}\chi_\xi(\gamma) g * \ell)),$$

hence

$$\chi_\eta(\gamma) = g^{-1}\chi_\xi(\gamma) g.$$

This implies the last claim of Proposition 22. ∎

We now consider the particular case where $\mathcal{G}$ is dihedral: let $\mathcal{D}_n$ be the group generated by two elements r, s subject to the relations:

$$r^n = 1, \qquad s^2 = 1 \qquad \text{and} \qquad rsr = s,$$

and let $\mathcal{Z}_n$ denote the cyclic (normal) subgroup of $\mathcal{D}_n$ generated by r. The group $\mathcal{D}_n$ is the semidirect product $\mathcal{D}_n = \mathcal{Z}_n \rtimes \mu_2$ and we have a split exact sequence

$$1 \to \mathcal{Z}_n \to \mathcal{D}_n \xrightarrow{\rho} \mu_2 \to 1. \tag{11}$$

Proposition 23. *Let L be a Galois $\mathcal{D}_n$-algebra over F and let*

$$L_0 = \{\ell \in L \colon r * \ell = \ell\}, \qquad L_1 = \{\ell \in L \colon s * \ell = \ell\}.$$

Then $L_0 \simeq F(\sqrt{\alpha})$ for some $\alpha \in F^\times$. For all $\xi \in X(L)$, the homomorphism $\rho \circ \chi_\xi \in \mathrm{Hom}(\Gamma, \mu_2)$ corresponds to $\alpha \cdot F^{\times 2}$ under the identification $\mathrm{Hom}(\Gamma, \mu_2) = H^1(F, \mu_2) = F^\times / F^{\times 2}$. Moreover, if n is odd, $\alpha \cdot F^{\times 2}$ is the discriminant of L/F, so that the map $H^1(F, \mathcal{D}_n) \to H^1(F, \mu_2)$, induced in cohomology by ρ, associates to L the discriminant of L. The discriminant of L_1/F is 1 if $n \equiv 1 \bmod 4$ and $\alpha \cdot F^{\times 2}$ if $n \equiv 3 \bmod 4$.

Proof. The first statement is clear, since Galois theory shows L_0 is a quadratic étale algebra over F. Since the action of $\mathcal{Z}_n$ on L_0 is trivial, the action of $\mathcal{D}_n$ factors through μ_2: we may set

$$\rho(g) * \ell = g * \ell \qquad \text{for } g \in \mathcal{D}_n \text{ and } \ell \in L_0.$$

For all $\xi \in X(L)$, we then have

$$\gamma(\xi(\ell)) = \xi(\rho \circ \chi_\xi(\gamma) * \ell) \qquad \text{for } \gamma \in \Gamma \text{ and } \ell \in L_0,$$

proving that $\rho \circ \chi_\xi \in H^1(F, \mu_2)$ is the homomorphism corresponding to the Galois μ_2-algebra L_0/F.

For the rest of the proof, assume n is odd. The discriminant of L_1/F is represented by the determinant

$$\det(\mathrm{tr}_{L_1/F}(e_i e_j))_{1 \le i,j \le n},$$

where $(e_i)_{1 \le i \le n}$ is a basis of L_1 over F. Since, for $\ell \in L_1$,

$$\mathrm{tr}_{L_1/F}(\ell) = \sum_{i=1}^{n} \xi(r^i * \ell),$$

we have

$$(\mathrm{tr}_{L_1/F}(e_i e_j))_{1 \le i,j \le n} = m^t \cdot m$$

where

$$m = (\xi(r^i * e_j))_{1 \le i,j \le n}.$$

Therefore, if $\delta_1 = \det m \in \xi(L)$, the discriminant of L_1/F is represented in $F^\times/F^{\times 2}$ by δ_1^2. For $\gamma \in \Gamma$, we have

$$\gamma(\delta_1) = \xi(\det(\chi_\xi(\gamma) r^i * e_j)_{1 \le i,j \le n}) = \xi(\det(\chi_\xi(\gamma) r^i s * e_j)_{1 \le i,j \le n}).$$

If $\chi_\xi(\gamma) \in \mathcal{Z}_n$, multiplication by $\chi_\xi(\gamma)$ is an even permutation of $\mathcal{Z}_n$, hence

$$\det(\chi_\xi(\gamma) r^i * e_j)_{1 \le i,j \le n} = \det(r^i * e_j)_{1 \le i,j \le n},$$

and therefore $\gamma(\delta_1) = \delta_1$. If $\chi_\xi(\gamma) \notin \mathcal{Z}_n$, the map $z \mapsto \chi_\xi(\gamma) z s$ is a permutation of $\mathcal{Z}_n$ of signature $(-1)^{(n-1)/2}$, hence

$$\gamma(\delta_1) = (-1)^{(n-1)/2} \delta_1.$$

Therefore, if $n \equiv 1 \bmod 4$ we have $\delta_1 \in F$, hence the discriminant of L_1/F is trivial. If $n \equiv 3 \bmod 4$, we have

$$\gamma(\delta_1) = \rho \circ \chi_\xi(\gamma)\, \delta_1,$$

hence the discriminant of L_1/F corresponds to $\rho \circ \chi_\xi \in H^1(F, \mu_2)$, hence it is $\alpha \cdot F^{\times 2}$.

The discriminant of L/F is calculated in a similar way: multiplication by $g \in \mathcal{D}_n$ defines on $\mathcal{D}_n$ a permutation of signature $\rho(g)$, hence the discriminant of L/F corresponds to $\rho \circ \chi_\xi \in H^1(F, \mu_2)$. ∎

Suppose now $K = F(\sqrt{\alpha})$ is a quadratic field extension of F contained in F_s. We denote by Γ_K the Galois group $\Gamma_K = \mathrm{Gal}(F_s/K)$ of F_s over K.

PROPOSITION 24. *Suppose n is odd. The group $H^1(F, \mathcal{Z}_n(\alpha))$ classifies the Galois $\mathcal{Z}_n$-algebras L over K which can be endowed with a Galois $\mathcal{D}_n$-algebra structure over F extending the action of $\mathcal{Z}_n$.*

Proof. Let $\sigma \in \Gamma \smallsetminus \Gamma_K$. Proposition 21 shows that

$$\begin{aligned} H^1(F, \mathcal{Z}_n(\alpha)) &= \{\chi \in H^1(K, \mathcal{Z}_n) \colon \chi\overline{\chi} = 1\} \\ &= \{\chi \in \mathrm{Hom}(\Gamma_K, \mathcal{Z}_n) \colon \chi\overline{\chi} = 1\}, \end{aligned}$$

where $\overline{\chi}$ is defined by:

$$\overline{\chi}(\gamma) = \chi(\sigma\gamma\sigma^{-1}) \qquad \text{for } \gamma \in \Gamma_K.$$

Let L be a Galois $\mathcal{Z}_n$-algebra over K which also has a Galois $\mathcal{D}_n$-algebra structure over F extending the action of $\mathcal{Z}_n$. Let $\xi \in X(L)$. We may assume ξ is a K-algebra homomorphism; the restriction to Γ_K of the associated homomorphism $\chi_\xi \colon \Gamma \to \mathcal{D}_n$ is then the element $\chi_\xi|_{\Gamma_K} \in H^1(K, \mathcal{Z}_n)$ associated to L, viewed as a Galois $\mathcal{Z}_n$-algebra over K.

If $\chi_\xi(\sigma) \in \mathcal{Z}_n$, then ρ maps the image of χ_ξ to $1 \in \mu_2$, hence Proposition 23 shows that the subalgebra L_0 of invariant elements under r splits as $F \times F$. This is a contradiction since $L_0 = K$. Therefore, $\chi_\xi(\sigma) \notin \mathcal{Z}_n$, hence, for $\gamma \in \Gamma_K$,

$$\chi_\xi|_{\Gamma_K}(\sigma\gamma\sigma^{-1}) = \chi_\xi(\sigma)\chi_\xi(\gamma)\chi_\xi(\sigma)^{-1} = \chi_\xi|_{\Gamma_K}(\gamma)^{-1}.$$

This shows that $\chi_\xi|_{\Gamma_K}\overline{\chi_\xi|_{\Gamma_K}} = 1$, hence $\chi_\xi|_{\Gamma_K} \in H^1(F, \mathcal{Z}_n(\alpha))$.

Conversely, to every $\chi \in H^1(F, \mathcal{Z}_n(\alpha))$ we associate the Galois $\mathcal{Z}_n$-algebra over K:

$$\mathfrak{F}_\chi = \{f \in \mathfrak{F}(\mathcal{Z}_n, F_s)\colon \gamma(f(x)) = f(\chi(\gamma)x) \text{ for all } x \in \mathcal{Z}_n\}.$$

Since $\chi\overline{\chi} = 1$, we may extend the $\mathcal{Z}_n$-action on $\mathfrak{F}_\chi$ to an action of $\mathcal{D}_n$ by letting:

$$(s * f)(x) = \sigma(f(x^{-1})) \qquad \text{for } f \in \mathfrak{F}_\chi,\ x \in \mathcal{Z}_n.$$

■

Remark. Another proof of the proposition above can be obtained by defining a twisted action of Γ on $\mathcal{D}_n$ extending the action on $\mathcal{Z}_n$. There is an exact sequence corresponding to (11):

$$1 \to \mathcal{Z}_n(\alpha) \to \mathcal{D}_n(\alpha) \to \mu_2 \to 1,$$

and the associated cohomology sequence:

$$1 \to H^1(F, \mathcal{Z}_n(\alpha)) \to H^1(F, \mathcal{D}_n(\alpha)) \to H^1(F, \mu_2)$$

yields an alternative (equivalent) description of $H^1(F, \mathcal{Z}_n(\alpha))$.

As observed in the proof, all Galois $\mathcal{Z}_n$-algebras L over K which can be endowed with a Galois $\mathcal{D}_n$-algebra structure over F extending the $\mathcal{Z}_n$-action have discriminant $\alpha \cdot F^{\times 2}$. It is also clear from the proof that the $\mathcal{D}_n$-algebra structure on L is not uniquely determined, since it depends on the choice of σ. However, the subalgebra L_1 of invariant elements under the element s of $\mathcal{D}_n$ does not depend on the choice of the $\mathcal{D}_n$-algebra structure up to F-isomorphism. Therefore, for $\chi \in H^1(F, \mathcal{Z}_n(\alpha))$, we may denote by F_χ an F-algebra which is isomorphic to the subalgebra of s-invariant elements in the algebra L corresponding to χ under the correspondence of Proposition 24. According to Proposition 23, the discriminant of F_χ is 1 if $n \equiv 1 \bmod 4$ and $\alpha \cdot F^{\times 2}$ if $n \equiv 3 \bmod 4$.

Any $\chi \in H^1(F, \mathcal{Z}_n)$ defines a Galois $\mathcal{Z}_n$-algebra over F which we will also denote by F_χ. The discriminant of this extension is 1.

We now turn to the Galois module μ_n of n-th roots of unity, assuming that n is relatively prime to the characteristic of F. As above, we denote

$$\mu_n(\alpha) = \mu_n \otimes_{\mathbb{Z}} \mathbb{Z}(\alpha).$$

PROPOSITION 25. *Let $K = F(\sqrt{\alpha})$ be a quadratic field extension of F. For any odd integer n relatively prime to the characteristic of F,*

$$H^1(F, \mu_n(\alpha)) = \{x \cdot K^{\times n} \in K^\times/K^{\times n} \colon x\overline{x} = 1\}$$

and $H^2(F, \mu_n(\alpha))$ classifies up to Brauer-equivalence central simple K-algebras of exponent n which admit involutions of the second kind leaving F elementwise invariant.

Proof. Applying Proposition 21 with $M = \mu_n$ and $\ell = 1$ yields:

$$H^1(F, \mu_n(\alpha)) = \{x \cdot K^{\times n} \in K^\times/K^{\times n} \colon x\overline{x} \in F^{\times n}\}.$$

If $x \in K^\times$ is such that $x\overline{x} = \lambda^n$ with $\lambda \in F^\times$, then

$$x' = x(\lambda^{(n-1)/2}x^{-1})^n$$

represents the same element of $K^\times/K^{\times n}$ and satisfies: $x'\overline{x'} = 1$. This proves the first claim.

For $\ell = 2$, Proposition 21 yields a split exact sequence:

$$1 \to H^2(F, \mu_n(\alpha)) \to {}_n\mathrm{Br}(K) \xrightarrow{\mathrm{cor}} {}_n\mathrm{Br}(F) \to 1.$$

The proposition follows, since by the theorem of Albert–Riehm–Scharlau [16] a central simple K-algebra admits an involution of the second kind leaving F elementwise invariant if and only if its corestriction is trivial. ∎

For $a \in K^\times$ with $a\overline{a} = 1$, we denote the class of a in $H^1(F, \mu_n(\alpha))$ by $[a]$ and we define a commutative étale F-algebra F_a of dimension n as follows: on the K-algebra $K(y)$ where y is an indeterminate subject to $y^n = a$, define an F-automorphism θ extending $\bar{}$ on K by letting $\theta(y) = y^{-1}$. Then F_a is the F-subalgebra $K(y)^\theta$ of invariant elements under θ. It is easily seen that $F_a \simeq F_{a'}$ if $[a] = [a'] \in$

$H^1(F, \mu_n(\alpha))$. For $[a] \in H^1(F, \mu_n) = F^\times/F^{\times n}$, $a \in F^\times$, we also denote by F_a the F-algebra $F(y)$ where $y^n = a$.

We now relate by cup-product the special cases $\mathcal{Z}_n$ and μ_n considered above. There is a canonical isomorphism: $\mathcal{Z}_n \otimes_{\mathbb{Z}} \mu_n = \mu_n$ defined by: $r^i \otimes \zeta \mapsto \zeta^i$. Therefore, for $\delta_1, \delta_2 \in F^\times$,

$$\mathcal{Z}_n(\delta_1) \otimes_{\mathbb{Z}} \mu_n(\delta_2) = \mathcal{Z}_n \otimes \mu_n \otimes \mathbb{Z}(\delta_1) \otimes \mathbb{Z}(\delta_2) = \mu_n(\delta_1\delta_2).$$

Thus the cup-product defines a map:

$$H^1(F, \mathcal{Z}_n(\delta_1)) \times H^1(F, \mu_n(\delta_2)) \to H^2(F, \mu_n(\delta_1\delta_2)).$$

PROPOSITION 26. *Let $K = F(\sqrt{\alpha})$ be a quadratic field extension of F and let $\delta_1, \delta_2 \in F^\times$ be such that $\delta_1\delta_2 \equiv \alpha \bmod F^{\times 2}$. Let $\chi \in H^1(F, \mathcal{Z}_n(\delta_1))$ and $a \in F(\sqrt{\delta_2})^\times$ such that $n_{F(\sqrt{\alpha_2})/F}(a) = 1$, with cohomology class $[a] \in H^1(F, \mu_n(\delta_2))$. There exists a central simple K-algebra $B(\chi, a)$ of degree n such that*

(1) $[B(\chi, a)] = \chi \cup [a] \in H^2(F, \mu_n(\alpha))$;

(2) $B(\chi, a)$ admits an involution σ of the second kind such that $(B(\chi, a), \sigma)_+$ contains subalgebras isomorphic to F_χ and to F_a.

Proof. We first consider the special cases where $\delta_1 \in F^{\times 2}$ or $\delta_2 \in F^{\times 2}$. If $\delta_1 \in F^{\times 2}$, we have $\chi \in H^1(F, \mathcal{Z}_n)$ and $[a] \in H^1(F, \mu_n(\alpha))$ with $a \in K^\times$ such that $a\overline{a} = 1$. The algebra F_χ is a Galois $\mathcal{Z}_n$-algebra over F. The central simple algebra $B(\chi, a)$ is the crossed product:

$$B(\chi, a) = \bigoplus_{i=0}^{n-1} (F_\chi \otimes_F K) z^i,$$

where the indeterminate z is subject to the relations:

$$z(\ell \otimes k) \;=\; [(r * \ell) \otimes k]z \quad \text{for } \ell \in F_\chi,\ k \in K, \quad \text{and} \quad z^n = a.$$

An involution of the second kind σ on $B(\chi, a)$ is defined by:

$$\sigma(\ell \otimes k) \;=\; \ell \otimes \overline{k} \quad \text{for } \ell \in F_\chi,\ k \in K, \quad \text{and} \quad \sigma(z) = z^{-1}.$$

Clearly, $(B,\sigma)_+$ contains F_χ and the subalgebra $F_a \subset K(z)$.

If $\delta_2 \in {F^\times}^2$, then $\chi \in H^1(F, \mathcal{Z}_n(\alpha))$ and $a \in F^\times$, $[a] \in H^1(F,\mu_n)$. Let L be a Galois $\mathcal{Z}_n$-algebra over K corresponding to χ. According to Proposition 24, we may also choose a Galois $\mathcal{D}_n$-algebra structure on L, viewed as an algebra over F. The algebra $B(\chi,a)$ is the crossed product:

$$B(\chi,a) = \bigoplus_{i=0}^{n-1} L\, z^i$$

where the indeterminate z is subject to the relations:

$$z\ell \;=\; (r*\ell)z \quad \text{for } \ell \in L, \quad \text{and} \;\; z^n = a.$$

An involution of the second kind σ on $B(\chi,a)$ is defined by:

$$\sigma(\ell) \;=\; s*\ell \quad \text{for } \ell \in L, \quad \text{and} \;\; \sigma(z) = z.$$

By definition, it is clear that $F_a = F(z) \subset (B,\sigma)_+$ and that the subalgebra $L_1 \subset L$ of invariant elements under s, which is isomorphic to F_χ, lies in $(B,\sigma)_+$.

Suppose now $\delta_1, \delta_2 \notin {F^\times}^2$. Let $F' = F(\sqrt{\delta_1})$ and $K' = K(\sqrt{\delta_1})$. Let L be a Galois $\mathcal{Z}_n$-algebra over F' which corresponds to $\chi \in H^1(F, \mathcal{Z}_n(\delta_1))$; according to Proposition 24, we may endow it with a Galois $\mathcal{D}_n$-algebra structure over F. Since $\delta_1\delta_2 \equiv \alpha \bmod {F^\times}^2$, we may identify $F(\sqrt{\delta_2})$ with a subfield of K'. Consider the following crossed product algebra over K':

$$B' = \bigoplus_{i=0}^{n-1} (L \otimes_F K)\, z^i$$

where z is subject to:

$$z(\ell \otimes k) \;=\; [(r*\ell)\otimes k]z \quad \text{for } \ell \in L,\; k \in K \;\; \text{and} \;\; z^n = a.$$

This algebra represents the restriction $\mathrm{res}(\chi \cup [a]) \in H^1(F', \mu_n(\alpha))$. We define an involution σ' on B' by:

$$\sigma'(\ell \otimes k) \;=\; (s*\ell)\otimes \overline{k} \quad \text{for } \ell \in L,\; k \in K, \;\; \text{and} \;\; \sigma'(z) = z.$$

On the other hand, we define a K-algebra automorphism θ on B' by:

$$\theta(\ell \otimes k) \;=\; (s * \ell) \otimes k \quad \text{for } \ell \in L,\ k \in K, \quad \text{and} \quad \theta(z) = z^{-1}.$$

The restriction of θ to the center K' is the non-trivial automorphism over K, and $\theta^2 = I$; therefore, the subalgebra $B = B'^{\theta}$ of invariant elements under θ is a central simple K-algebra such that

$$B' = B \otimes_K K'.$$

Since the restriction map $\operatorname{res}\colon H^2(F, \mu_n(\alpha)) \to H^2(F', \mu_n(\alpha))$ is injective (since n is odd), it follows that B represents the cup product $\chi \cup [a] \in H^2(F, \mu_n(\alpha))$ and we define $B(\chi, a) = B$. Moreover, θ and σ' commute, hence the restriction of σ' to $B(\chi, a)$ defines an involution σ of the second kind. The subalgebra L_1 of L elementwise invariant under s and the subalgebra $K'(z)^{\theta}$ invariant under θ both lie in $(B(\chi, a), \sigma)_+$; the involution σ thus satisfies the required properties, since $L_1 \simeq F_\chi$ and $K'(z)^{\theta} \simeq F_a$. ∎

Proposition 27. *Let B be a central simple K-algebra of degree n (odd) which admits involutions of the second kind leaving F elementwise invariant, and let $\delta \in F^\times$. If B contains a subfield isomorphic to F_χ for some $\chi \in H^1(F, \mathcal{Z}_n(\delta))$, then $B \simeq B(\chi, a)$ for some $a \in F(\sqrt{\alpha\delta})^\times$ such that $n_{F(\sqrt{\alpha\delta})/F}(a) = 1$.*

Proof. Suppose first $\delta \in F^{\times 2}$. Then $F_\chi \otimes K$ is a maximal subfield of B which is cyclic over K, hence B is a cyclic algebra:

$$[B] = \operatorname{res}_{K/F}(\chi) \cup [b] \in H^2(K, \mu_n) \tag{12}$$

for some $b \in K^\times$ (so that $[b] \in H^1(K, \mu_n)$), where $[B]$ denotes the image of B in $H^2(K, \mu_n)$. Since B admits involutions of the second kind over F, we have $\operatorname{cor}_{K/F}(B) = 0$; therefore,

$$\chi \cup \operatorname{cor}_{K/F}([b]) = 0 \quad \text{in } H^2(F, \mu_n). \tag{13}$$

Since n is odd, we may find $m \in \mathbb{Z}$ such that $2m \equiv 1 \bmod n$. Then

$$b \equiv b^{2m} = (b\overline{b}^{-1})^m n_{K/F}(b)^m \mod K^{\times n};$$

therefore, letting $a = (b\overline{b}^{-1})^m$, we have $[a] \in H^1(F, \mu_n(\alpha))$ and

$$[b] = [a] + m \ \mathrm{res}_{K/F} \circ \mathrm{cor}_{K/F}([b]) \quad \text{in } H^1(K, \mu_n).$$

Substituting in equation (12), we get:

$$[B] = \mathrm{res}_{K/F}(\chi) \cup [a] + m \ \mathrm{res}_{K/F}(\chi \cup \mathrm{cor}_{K/F}([b])),$$

hence $B \simeq B(\chi, a)$, in view of (13). Suppose next $\delta \notin F^{\times 2}$ and let $F' = F(\sqrt{\delta})$. Since $\delta \in F'^{\times 2}$, the case already considered yields:

$$[B \otimes F'] = \mathrm{res}_{F'/F}(\chi) \cup [a']$$

for some $[a'] \in H^1(F', \mu_n(\alpha\delta))$. Applying the corestriction map to both sides of this equation, we get by the projection formula:

$$2[B] = \chi \cup \mathrm{cor}_{F'/F}([a']).$$

Therefore, if $2m \equiv 1 \bmod n$,

$$[B] = m\,\chi \cup \mathrm{cor}_{F'/F}([a']),$$

hence $B \simeq B(\chi, a)$ for $[a] = m \ \mathrm{cor}_{F'/F}([a']) \in H^1(F, \mu_n(\alpha\delta))$. ∎

In a different direction, we have the following result on the Galois cohomology of the twisted modules $\mu_n(\alpha)$:

PROPOSITION 28. *Let $\delta_1, \delta_2 \in F^\times$. In $H^2(F, \mu_n^{\otimes 2}(\delta_1\delta_2))$, we have:*

$$H^1(F, \mu_n(\delta_1)) \cup H^1(F, \mu_n(\delta_2)) \subset H^1(F, \mu_n) \cup H^1(F, \mu_n(\delta_1\delta_2)),$$

where the left-hand side is

$$\{x \cup y \colon x \in H^1(F, \mu_n(\delta_1)),\ y \in H^1(F, \mu_n(\delta_2))\}.$$

Proof. Assume first that $\delta_1, \delta_2, \delta_1\delta_2 \notin F^{\times 2}$. For $i = 1, 2$, let $F_i = F(\sqrt{\delta_i}) \subset F_s$ and let $a_i \in F_i^\times$ be such that $n_{F_i/F}(a_i) = 1$, so that $[a_i] \in H^1(F, \mu_n(\delta_i))$. If $a_i \in F^{\times n}$, then $[a_i] = 0$, hence $[a_1] \cup [a_2] =$

$0 \in H^1(F, \mu_n) \cup H^1(F, \mu_n(\delta_1\delta_2))$. For the rest of the proof, we may thus assume $a_i \neq \pm 1$ for $i = 1, 2$. Let

$$u = \frac{a_1 - 1}{a_1 + 1} \in F_1^\times \quad \text{and} \quad v = \frac{a_2 + 1}{a_2 - 1} \in F_2^\times,$$

so that

$$a_1 = \frac{1 + u}{1 - u} \quad \text{and} \quad a_2 = \frac{v + 1}{v - 1}.$$

Since $n_{F_i/F}(a_i) = 1$, it follows that u and v have trace zero. Therefore, $u^2, v^2 \in F^\times$ and $uv^{-1} \in F(\sqrt{\delta_1\delta_2})^\times$. Let

$$[b] = \frac{1 - v^2}{1 - u^2} \cdot F^{\times n} \in H^1(F, \mu_n)$$

and

$$[c] = \frac{1 + uv^{-1}}{1 - uv^{-1}} \cdot F\left(\sqrt{\delta_1\delta_2}\right)^{\times n} \in H^1(F, \mu_n(\delta_1\delta_2)).$$

We claim that

$$[a_1] \cup [a_2] = [b] \cup [c] \quad \text{in } H^2(F, \mu_n^{\otimes 2}(\delta_1\delta_2)).$$

Let $M = F(\sqrt{\delta_1}, \sqrt{\delta_2}) \subset F_s$. Since the degree of the extension M/F is relatively prime to n, the restriction map

$$\mathrm{res}_{M/F} : H^2(F, \mu_n^{\otimes 2}(\delta_1\delta_2)) \to H^2(M, \mu_n^{\otimes 2}(\delta_1\delta_2)) = H^2(M, \mu_n^{\otimes 2})$$

is injective; therefore, it suffices to prove the claim over M. The identity

$$\left\{\frac{1 + u}{1 - u}; \frac{v + 1}{v - 1}\right\} = \left\{\frac{1 - v^2}{1 - u^2}; \frac{1 + uv^{-1}}{1 - uv^{-1}}\right\}.$$

holds for symbols $\{a, b\}$ in Milnor's K_2, a proof is given in the following Lemma 29.

Applying the norm residue homomorphism $K_2M \to H^2(M, \mu_n^{\otimes 2})$ to both sides, we get

$$[a_1] \cup [a_2] = [b] \cup [c] \quad \text{in } H^2(M, \mu_n^{\otimes 2}) = H^2(M, \mu_n^{\otimes 2}(\delta_1\delta_2)),$$

completing the proof in the case where $\delta_1, \delta_2, \delta_1\delta_2 \notin F^{\times 2}$. If δ_1 or $\delta_2 \in F^{\times 2}$, the proposition is obvious. If $\delta_1\delta_2 \in F^{\times 2}$, we may use the same arguments as above, substituting F for $F(\sqrt{\delta_1\delta_2})$, except if $u = \pm v$. In this case however, we have $a_1 = -a_2^{\pm 1}$, hence $[a_1] = [a_2]^{\pm 1}$ and therefore $[a_1] \cup [a_2] = 0$. ∎

LEMMA 29. *For $u, v \neq \pm 1 \in F^\times, u \neq \pm v$, the relation*

$$\left\{\frac{1+u}{1-u}; \frac{v+1}{v-1}\right\} = \left\{\frac{1-v^2}{1-u^2}; \frac{1+uv^{-1}}{1-uv^{-1}}\right\}$$

holds in K_2F.

Proof. We have $\{1-u; 1+uv^{-1}\} + \{1-u; v\} = \{1-u; u+v\}$. On the other hand the basic relation $\{a; b\} = \{a; b-a\} + \{a-b; b\}$ in K_2 (see for example [9, p. 75]) implies that

$$\begin{aligned} \{1-u; u+v\} &= \{1-u; 1+v\} - \{-u-v; 1+v\} \\ &= \{1-u; 1+v\} + \{1+v; -u-v\}. \end{aligned}$$

Subtracting $0 = \{1+v; -v\}$ we get

$$\{1-u; 1+uv^{-1}\} - \{1+v; 1+uv^{-1}\} = \{1-u; 1+v\} - \{1-u; v\}.$$

Replacing u, v by $\pm u, \pm v$, we get four expressions which adds to the wanted relation. Another proof is to check the formula in the function field $F(u, v)$ by using the exact sequence of Milnor for $K_2F(t)$ (see [10]) to show that

$$\left\{\frac{1+u}{1-u}; \frac{v+1}{v-1}\right\} - \left\{\frac{1-v^2}{1-u^2}; \frac{1+uv^{-1}}{1-uv^{-1}}\right\}$$

lies in $K_2F(u)$, K_2F and then to show that it is 0 by specialization at some places. ∎

Remark. The Galois module μ_n plays a special rôle in the preceding proposition. Suppose that δ_1, δ_2, ε_1, $\varepsilon_2 \in F^\times$ are such that

$$\mu_n(\delta_1) \otimes \mu_n(\delta_2) = \mu_n(\varepsilon_1) \otimes \mu_n(\varepsilon_2),$$

and that the sets $\{\mu_n(\delta_1), \mu_n(\delta_2)\}$ and $\{\mu_n(\varepsilon_1), \mu_n(\varepsilon_2)\}$ are disjoint (up to isomorphism). If $\mu_n(\varepsilon_1)$ and $\mu_n(\varepsilon_2)$ are different from μ_n, then there is an extension $\tilde{F}$ of F such that

$$H^1(\tilde{F}, \mu_n(\delta_1)) \cup H^1(\tilde{F}, \mu_n(\delta_2)) \not\subset H^1(\tilde{F}, \mu_n(\varepsilon_1)) \cup H^1(\tilde{F}, \mu_n(\varepsilon_2))$$

Indeed, after a biquadratic extension of F we may assume that $\delta_1, \delta_2 \in F^{\times 2}$. Let then $\tilde{F}$ be the iterated powerseries extension $F((s))((t))$. Then

$$s \cdot \tilde{F}^{\times n} \cup t \cdot \tilde{F}^{\times n} \in H^1(\tilde{F}, \mu_n) \cup H^1(\tilde{F}, \mu_n)$$

has non-trivial residue. On the other hand,

$$\partial(H^1(\tilde{F}, \mu_n(\varepsilon))) \subset H^0(F, \mathcal{Z}_n(\varepsilon)) = 0$$

for nontrivial ε, hence $s \cdot \tilde{F}^{\times n} \cup t \cdot \tilde{F}^{\times n}$ cannot be a sum of cup-products of elements of $H^1(\tilde{F}, \mu_n(\varepsilon_1))$ and $H^1(\tilde{F}, \mu_n(\varepsilon_2))$.

COROLLARY 30. *Let n be an odd integer and let F be a field of characteristic relatively prime to n. Assume that $\mu_n = \mathcal{Z}_n(\varepsilon)$ for some $\varepsilon \in F^\times$; then every central simple F-algebra split by a Galois extension of degree $2n$ with dihedral Galois group is cyclic.*

Proof. Let A be a central simple F-algebra split by a Galois extension L/F with dihedral Galois group of order $2n$. The index of A then divides $2n$. Since n is odd, we may decompose the Brauer class of A:

$$[A] = \alpha_1 + \alpha_2$$

where α_1 has index 1 or 2 and α_2 has index dividing n. The element α_1 is split by an cyclic extension C_1/F of degree 1 or 2. If we show that $2[A]$ is split by a cyclic extension C_2/F of degree dividing n, then α_2 is also split by C_2, hence A is split by the cyclic extension $C_1 \otimes C_2/F$. Therefore, it suffices to show that $A^{\otimes 2}$ is cyclic. Let $\delta \in F^\times$ be a representative of the discriminant of L. Proposition 23 shows that L is a cyclic extension of $F(\sqrt{\delta})$. Choosing a Galois $\mathcal{Z}_n$-algebra structure of L over $F(\sqrt{\delta})$, we may associate to L an element $\chi \in H^1(F, \mathcal{Z}_n(\delta))$ by Proposition 24. Since $A \otimes F(\sqrt{\delta})$ is split by L, we have

$$[A \otimes_F F(\sqrt{\delta})] = \mathrm{res}_{F(\sqrt{\delta})/F}(\chi) \cup [a] \quad \text{in } H^2(F(\sqrt{\delta}), \mu_n)$$

for some $[a] \in H^1(F(\sqrt{\delta}), \mu_n) = H^1(F(\sqrt{\delta}), \mu_n(\delta))$. Taking the corestriction of both sides, we get

$$2[A] = \chi \cup [a'] \quad \text{in } H^2(F, \mu_n), \tag{14}$$

where $[a'] = \mathrm{cor}_{F(\sqrt{\delta})/F}([a]) \in H^1(F, \mu_n(\delta))$. Since $\mu_n = \mathscr{Z}_n(\varepsilon)$, we have $\mathscr{Z}_n(\delta) = \mu_n(\varepsilon\delta)$, hence relation (14) yields:

$$2[A] \in H^1(F, \mu_n(\varepsilon\delta)) \cup H^1(F, \mu_n(\delta)).$$

From Proposition 28, it follows that

$$2[A] = [b] \cup [c]$$

for some $[b] \in H^1(F, \mu_n)$ and some $[c] \in H^1(F, \mu_n(\varepsilon)) = H^1(F, \mathscr{Z}_n)$. The element $[c]$ then defines a cyclic extension of F which splits $A^{\otimes 2}$. ∎

We conclude by discussing the special features of the case where $n = 3$ (assuming that the characteristic of F is not 2 nor 3). Every cubic field extension L of F is of the form F_χ and also of the form F_a: more precisely, if the discriminant of L/F is represented by $\alpha \in F^\times$, then the field $L \otimes_F F(\sqrt{\alpha})$ is cyclic over $F(\sqrt{\alpha})$, hence $L = F_\chi$ for any $\chi \in H^1(F, \mathscr{Z}_3(\alpha))$ representing $L \otimes_F F(\sqrt{\alpha})$. Since $\mu_3 = \mathscr{Z}_3(-3)$, we may also view $L = F_a$ for $[a] = \chi \in H^1(F, \mu_3(-3\alpha))$.

Proposition 31. *Let $K = F(\sqrt{\alpha})$ be a quadratic field extension of F and let B be a central division K-algebra of degree 3 which admits involutions of the second kind leaving F elementwise invariant. Let also L be a cubic field extension of F with discriminant δ and let $\chi \in H^1(F, \mathscr{Z}_3(\delta))$ be such that $L = F_\chi$. The algebra B contains an isomorphic image of L if and only if $B \simeq B(\chi, a)$ (i.e. $[B] = \chi \cup [a]$ in $H^2(F, \mu_3(\alpha))$) for some $[a] \in H^1(F, \mu_3(\alpha\delta))$. The algebra B then contains a cubic field extension $L' = F_a$ of discriminant $-3\alpha\delta$. Moreover, there exists an involution σ such that $L, L' \subset (B, \sigma)_+$.*

The algebra B always contains cubic field extensions L_*, L'_* of discriminant -3, α respectively, and carries an involution σ_* such that $L_*, L'_* \subset (B, \sigma_*)_+$.

Proof. The first part follows from Propositions 26 and 27. In order to prove that B always contains extensions L_*, L'_* as stated, we use Proposition 28: let L be any cubic field extension of F contained in

B; then, letting $\delta \in F^\times$ denote a representative of the discriminant of L/F, we have

$$B \simeq B(\chi, a)$$

for some $\chi \in H^1(F, \mathcal{Z}_3(\delta))$ and some $[a] \in H^1(F, \mu_3(\alpha\delta))$. Since $\mathcal{Z}_3(\delta) = \mu_3(-3\delta)$, it follows that

$$[B] \in H^1(F, \mu_3(-3\delta)) \cup H^1(F, \mu_3(\alpha\delta)),$$

hence Proposition 28 shows that $B \simeq B(\chi_*, a_*)$ for some $\chi_* \in H^1(F, \mu_3) = H^1(F, \mathcal{Z}_3(-3))$ and some $[a_*] \in H^1(F, \mu_3(-3\alpha)) = H^1(F, \mathcal{Z}_3(\alpha))$. We then let $L_* = F_{\chi_*}$ and $L'_* = F_{a_*}$. ∎

Note that, according to condition *(e)* of Theorem 16, the involution σ_* is distinguished; the proposition above thus yields another proof of the existence of distinguished involutions.

Note also that the pair $(-3, \alpha)$ is the only pair of discriminants that occurs for every central division $F(\sqrt{\alpha})$-algebra of degree 3 which admits involutions of the second kind: given a pair $(\varepsilon_1, \varepsilon_2)$ with $\varepsilon_1\varepsilon_2 \in (-3\alpha) \cdot F^{\times 2}$, the remark following Proposition 25 together with Proposition 27 shows that there is an algebra B over some extension of F which does not contain any cubic separable extension of discriminant ε_1 or ε_2. For example, there are algebras B which do not contain a cyclic cubic field extension, i.e. a cubic field extension of discriminant 1, as already observed in the example at the end of section 4.

Since 3-fold Pfister forms are classified up to isometry by their Arason invariant:

$$\mathrm{Ar}(\langle\langle a, b, c\rangle\rangle) = (a \cdot F^{\times 2}) \cup (b \cdot F^{\times 2}) \cup (c \cdot F^{\times 2}) \in H^3(F, \mu_2),$$

(see [5]), Theorem 15 (together with Proposition 25) yields a classification of central simple algebras of degree 3 with involution by cohomological invariants:

Corollary 32. *Triples (K, B, σ) where $K = F(\sqrt{\alpha})$ is a quadratic étale F-algebra, B is a central simple K-algebra of degree 3 and σ is*

an involution of the second kind on B leaving F elementwise invariant, are classified over F by the three cohomological invariants:

$$\begin{aligned} f_1(K,B,\sigma) &= \alpha \cdot F^{\times 2} \in H^1(F,\mu_2), \\ g_2(K,B,\sigma) &= [B] \in H^2(F,\mu_3(\alpha)), \\ f_3(K,B,\sigma) &= \mathrm{Ar}(\pi(B,\sigma)) \in H^3(F,\mu_2). \end{aligned}$$

Proof.

Indeed we have seen that f_1 determines K, g_2 determines B and f_3 determines the involution σ. ∎

Remark. Let K_0/F_0 be a separable quadratic field extension and let B_0 be a central division K_0-algebra of degree 3 which admits an involution of the second kind. Let $F = F_0((t))$, $K = K_0((t))$ and $B = B_0((t))$. Let σ be any involution on B, not necessarily defined over B_0. We claim that the second residue $\varphi^t(Q_\sigma)$ is always trivial, i.e. Q_σ is induced from F_0. A cubic étale F-subalgebra L of B is either unramified or totally ramified, i.e. $L = F[X]/(X^3 - ut)$ for $u \in F_0^\times$. Thus in both cases the discriminant of L is a class defined over F_0. On the other hand, an element $\lambda \in L$ such that $n_{L/F}(\lambda)$ is a square in $F^\times$ must be a unit in $F_0[[t]]$. This, together with Proposition 11, implies that $\varphi^t(Q_\sigma) = 0$. It follows that the invariant $f_3(B,\sigma)$ cannot in general be arbitrary. In particular the three invariants f_1, g_2 and f_3 are not independent. A corresponding question for invariants of exceptional Jordan algebras is discussed in [18].

References

[1] A.A. Albert, *Structure of Algebras*, Colloquium Publ. 24, Amer. Math. Soc. Providence, R.I., 1939.

[2] A.A. Albert, On involutorial associative division algebras, *Scripta Mathematica* **26** (1963), 309–316.

[3] J.K. Arason; R. Elman, Nilpotence in the Witt ring, *Amer. J. Math.* **113** (1991), 861–875.

[4] E. Bayer-Fluckiger; H.W. Lenstra Jr., Forms in odd-degree extensions and self-dual normal bases, *Amer. J. Math.* **112** (1990), 359–373.

[5] R. Elman; T.Y. Lam, Pfister forms and K-theory of fields, *J. Algebra* **23** (1972) 181–213.

[6] D.E. Haile; M.-A. Knus, On division algebras of degree 3 with involutions, Preprint (1995).

[7] N. Jacobson, A note on hermitian forms, *Bull. Amer. Math. Soc.* **50** (1944), 645–648.

[8] N. Jacobson, *Structure and Representations of Jordan Algebras*, AMS Colloquium Publ. Vol. 39, Amer. Math. Soc., Providence, R.I., 1968.

[9] I. Kersten, *Brauergruppen von Körpern*, Aspekte der Mathematik, Vieweg, Braunschweig, 1990.

[10] J. Milnor, Algebraic K-theory and quadratic forms, *Invent. Math.* **9** (1970), 318–344.

[11] H.P. Petersson; M.L. Racine, Springer forms and the first Tits construction of exceptional Jordan division algebras, *manuscripta mathematica* **45** (1984), 249–272.

[12] H.P. Petersson; M.L. Racine, The toral Tits process of Jordan algebras, *Abh. Math. Sem. Hamburg* **54** (1984), 251–256.

[13] H.P. Petersson; M.L. Racine, Cubic subfields of exceptional simple Jordan algebras, *Proc. Amer. Math. Soc.* **91** (1984), 31–36.

[14] H.P. Petersson; M.L. Racine, Reduced models of Albert algebras, to appear.

[15] L.H. Rowen; D.J. Saltman, Dihedral algebras are cyclic, *Proc. Amer. Math. Soc.* **84** (1982), 162–164.

[16] W. Scharlau, *Quadratic and Hermitian Forms*, Grundlehren Math. Wiss. 270, Springer-Verlag, Berlin, 1985.

[17] J-P. Serre, *Cohomologie Galoisienne*, Lecture Notes in Mathematics 5, Springer-Verlag, Berlin, 1964 and 1994.

[18] J-P. Serre, Cohomologie galoisienne: Progrès et Problèmes, *Sém. Bourbaki* (1993–1994), exposé 783.

[19] T.A. Springer, *Oktaven, Jordan-Algebren und Ausnahmegruppen*, Lecture Notes, Göttingen, 1963.

Darrell E. Haile
Department of Mathematics
Indiana University
Bloomington, IN 47405
USA
haile@ucs.indiana.edu

Max-Albert Knus
Departement Mathematik
ETH-Zentrum
CH-8092 Zürich
Switzerland
knus@math.ethz.ch

Markus Rost
NWFI-Mathematik
Universität Regensburg
D-93053 Regensburg
Germany
markus.rost@mathematik.uni-regensburg.de

Jean-Pierre Tignol
Institut de Mathématique Pure et Appliquée
Université catholique de Louvain
B-1348 Louvain-la-Neuve
Belgium
tignol@agel.ucl.ac.be