Algebras with Involution That Become Hyperbolic under a Given Extension

Darrell Haile*

Department of Mathematics, Indiana University, Bloomington, Indiana 47405

and

Jean-Pierre Tignol²

Institut de Mathématique, Université Catholique de Louvain, B-1348, Louvain-La-Neuve, Belgium

Communicated by Susan Montgomery

Received September 5, 1996

1. INTRODUCTION

Let $K$ be a field of characteristic not 2 and let $(A, \sigma)$ be either a central simple $K$-algebra with an involution $\sigma$ of the first or second kind or an algebra of the form $A_0 \times A_0^{\text{op}}$, where $A_0$ is a central simple $K$-algebra and $\sigma$ is the switch involution, that is, $\sigma(a, b^{\text{op}}) = (b, a^{\text{op}})$. We will call both of these types central simple $K$-algebras with involution. Let $F$ denote the fixed field of $\sigma$ restricted to the center of $A$. Recall that $(A, \sigma)$ is said to be isotropic if $A$ contains a nonzero element $a$ such that $\sigma(a)a = 0$ and $(A, \sigma)$ is said to be hyperbolic if $A$ contains a right ideal $I$ such that $I = I^\perp$, where $I^\perp = \{ y \in A | \sigma(y)I = 0 \}$ (see Bayer-Fluckiger et al. [1] and Tignol [5]). If $A = \text{End}_F V$ where $V$ is an $F$-vector space and $\sigma$ is the adjoint involution arising from a quadratic form $q$ on $V$, then $(A, \sigma)$ is isotropic (hyperbolic) if and only if $q$ is isotropic (hyperbolic). If $A = A_0 \times A_0^{\text{op}}$ and $\sigma$ is the switch involution, then $(A, \sigma)$ is hyperbolic.

* This research was done while the first author was a visitor at the Université Catholique de Louvain. He thanks the Institut de Mathématique Pure et Appliquée for its hospitality. E-mail address: haile@ucs.indiana.edu.

² Supported in part by the National Fund for Scientific Research (Belgium). E-mail address: Tignol@agel.ucl.ac.be.

0021-8693/98 $25.00

Copyright © 1998 by Academic Press
All rights of reproduction in any form reserved.
Now let \( \pi(t) \in F[t] \) be monic and separable of even degree \( 2n \) and let
\[
F(\pi) = F[t]/\pi(t)F[t].
\]

Because \( \pi(t) \) is separable the ring \( F(\pi) \) is a direct product of separable field extensions of \( F \), \( F(\pi) = F(\pi_1) \times \cdots \times F(\pi_r) \), where the \( \pi_i \)'s are irreducible polynomials in \( F[t] \) and \( \pi(t) = \pi_1(t) \cdots \pi_r(t) \). If \((A, \sigma)\) is a central simple \( K \)-algebra with involution we say \((A, \sigma)\) becomes hyperbolic over \( F(\pi) \) if each of the algebras \((A \otimes_F F(\pi), \sigma \otimes 1)\) is hyperbolic. In Tignol [5] it was shown that there is a universal object \( H_{\pi} \) for such algebras. Namely one lets \( H_{\pi} \) be the free \( F \)-algebra on the \( 2n \) indeterminates \( a_1, a_2, \ldots, a_n, b_1, b_2, \ldots, b_n \), subject to the relations coming from the following equation, where the indeterminate \( t \) is central:
\[
\pi(t) = (t^n + a_1 t^{n-1} + \cdots + a_n)(t^n + b_1 t^{n-1} + \cdots + b_n).
\]

The algebra \( H_{\pi} \) admits a unique involution \( \sigma_{\pi} \) satisfying \( \sigma_{\pi}(b_i) = a_i \) for all \( i \). Then by [5, Proposition 10] if \((A, \sigma)\) is anisotropic then \((A, \sigma)\) becomes hyperbolic over \( F(\pi) \) if and only if there is a homomorphism \((H_{\pi}, \sigma_{\pi}) \rightarrow (A, \sigma)\) of \( F \)-algebras with involution. We will refer to the existence of such a homomorphism as the hyperbolicity criterion.

In this paper we first give a quadratic-form theoretic formulation of the hyperbolicity criterion. We then determine the structure of the algebra \( H_{\pi} \). We prove that \( H_{\pi} \) is a homomorphic image of a certain twisted polynomial ring over the free \( F \)-algebra in \( n - 1 \) variables. As a consequence we show that if the degree of \( \pi(t) \) is greater than four, then \( H_{\pi} \) contains a free algebra. However, we also show that for all \( \pi(t) \), the algebra \( H_{\pi} \) has a homomorphic image which is the Clifford algebra of a quadratic form over a polynomial ring. As an application we use this Clifford algebra to describe quaternion algebras over \( F \) with a symplectic involution that become hyperbolic over \( F(\pi) \). For such algebras hyperbolicity is equivalent to being split. In fact every quaternion algebra admits a (unique) symplectic involution, so the result classifies the quaternion algebras split by \( F(\pi) \); see Proposition 18.

2. HYPERBOLICITY CRITERIA AND THE SCHARLAU TRANSFER

Let \((V, q)\) be an anisotropic quadratic space over \( F \) and let \( \sigma \) denote the adjoint involution on \( \text{End}_F V \) associated to \( q \). Let also \( \pi \in F[t] \) be a separable polynomial. As pointed out in the Introduction, the algebra with involution \((\text{End}_F V, \sigma)\) is anisotropic, and \((V, q)\) becomes hyperbolic over \( F(\pi) \) if and only if \((\text{End}_F V, \sigma)\) becomes hyperbolic over \( F(\pi) \), if and only
if there is a homomorphism of algebras with involution \((H_{\sigma}, \sigma) \to (\text{End}_{F} V, \sigma)\).

Our aim in this section is to translate this last condition into quadratic-form theoretic terms.

We begin with the following general observation on subalgebras of anisotropic algebras:

**Lemma 1.** Let \((A, \alpha)\) be anisotropic and let \(B\) be a \(\alpha\)-invariant subalgebra of \(A\). Then \(B\) is semisimple. Moreover if \(B = B_1 \oplus \cdots \oplus B_r\) is the decomposition of \(B\) into simple components then each \(B_i\) is \(\alpha\)-invariant and \((B_i, \alpha|_{B_i})\) is anisotropic.

**Proof.** Let \(B\) be a \(\alpha\)-invariant subalgebra of \(A\). If \(J\) is the Jacobson radical of \(B\) and \(J \neq 0\), then there is a positive integer \(k\) such that \(J^k \neq 0\), but \(J^{k+1} = 0\). Because \(\alpha(J) = J\), we have \(J^k \alpha(J^k) = 0\). But \((A, \alpha)\) is anisotropic, so this is not possible. Hence \(J = 0\).

Now let \(B = B_1 \oplus \cdots \oplus B_r\) be the decomposition of \(B\) into simple components. The involution \(\alpha\) must permute the components. If for some \(i\) we have \(\alpha(B_i) = B_j\), with \(i \neq j\), then \(B_i \alpha(B_i) = 0\), a contradiction. Hence each \(B_i\) is \(\alpha\)-invariant. It follows immediately from the definition of anisotropic that each \((B_i, \alpha|_{B_i})\) must be anisotropic.

Until the end of this section, we assume \((V, \alpha)\) is an anisotropic vector space over \(F\) and we denote by \(\alpha\) the adjoint involution with respect to \(\alpha\). Thus, if \(b\) is the symmetric bilinear form corresponding to \(\alpha\),

\[
b(v, f(w)) = b(f(v), w) \quad \text{for all } f \in \text{End}_{F} V \text{ and } v, w \in V.
\]

**Lemma 2.** Suppose \(B \subset \text{End}_{F} V\) is a \(\alpha\)-invariant subalgebra and let

\[B = B_1 \oplus \cdots \oplus B_r\]

be the decomposition of \(B\) into simple components. Then \(V\) decomposes into an orthogonal sum of subspaces

\[V = V_1 \perp \cdots \perp V_r\]

such that \(\text{End}_{F} V_i \supset B_i\) for all \(i = 1, \ldots, r\). Conversely, if \(V\) is an orthogonal direct sum of subspaces as above, then \(\text{End}_{F} V\) contains \(\text{End}_{F} V_1 \oplus \cdots \oplus \text{End}_{F} V_r\) as a \(\alpha\)-invariant subalgebra.

**Proof.** For \(i = 1, \ldots, r\), let \(e_i \in B_i \subset B\) be the unique nonzero central idempotent, and let \(V_i = e_i(V)\). Since \(e_1, \ldots, e_r\) are orthogonal idempotents such that \(e_1 + \cdots + e_r = 1\), we have

\[V_1 \oplus \cdots \oplus V_r = V.
\]
Since moreover $e_1, \ldots, e_r$ are symmetric, by Lemma 1, it follows that $V_1, \ldots, V_r$ are pairwise orthogonal. The relations

$$\text{End}_F V_i = e_i(\text{End}_F V) e_i \triangleright e_i B e_i = B_i$$

complete the proof of the first part.

For the converse, denote by $e_i \in \text{End}_F V$ the orthogonal projection onto $V_i$, for $i = 1, \ldots, r$. This is a symmetric idempotent such that $\text{End}_F V_i = e_i(\text{End}_F V) e_i$. Since the idempotents $e_1, \ldots, e_r$ are orthogonal and $e_1 + \cdots + e_r = 1$, it follows that $e_i(\text{End}_F V) e_1 \oplus \cdots \oplus e_r(\text{End}_F V) e_r$ is a $\sigma$-invariant subalgebra of $\text{End}_F V$.  

This lemma allows us to restrict to simple subalgebras of $(\text{End}_F V, \sigma)$. Note that any inclusion $B \subset \text{End}_F V$ endows $V$ with a (left) $B$-module structure. We want to show that stability of $B$ under $\sigma$ implies that the quadratic form $q$ is the Scharlau transfer of a hermitian form on the $B$-module $V$. We start with a few observations on hermitian forms.

Let $B$ be a simple finite-dimensional $F$-algebra with $F$-linear involution $\tau$ and let $U$ be a finitely generated $B$-module. A hermitian form on $U$ with respect to $\tau$ is a bi-additive map $h : U \times U \to B$

such that

$$h(bu, b'u') = bh(u, u')\tau(b')$$

and

$$h(u', u) = \tau(h(u, u'))$$

for all $u, u' \in U$ and $b, b' \in B$. The form $h$ is nonsingular if $h(u, u') = 0$ for all $u' \in U$ implies $u = 0$.

Let $s : B \to F$ be a nonzero $F$-linear map such that

$$s(bb') = s(b'b) \quad \text{and} \quad s(\tau(b)) = s(b) \quad \text{for all } b, b' \in B. \quad (2)$$

(If $Z$ denotes the center of $B$ and $Z_0 \supseteq F$ the subfield of $Z$ elementwise invariant under $\tau$, every such map can be obtained by composing the reduced trace $\text{Tr}_0 : B \to Z$ with the trace $\text{Tr}_{Z/Z_0} : Z \to Z_0$ and with a nonzero linear map $Z_0 \to F$.) A symmetric $F$-bilinear map $s_\ast(h)$ on $U$ may be defined by

$$s_\ast(h)(u, u') = s(h(u, u')) \quad \text{for } u, u' \in U.$$ 

Abusing notation, we also denote by $s_\ast(h)$ the corresponding quadratic form on $U$, called the Scharlau transfer of $h$ (with respect to $s$). The same
construction holds without change for skew-hermitian forms, i.e., forms for which $h(u', u) = -\tau(h(u, u'))$. Of course, in this case the form $s_\#(h)$ is alternating instead of symmetric.

**Lemma 3.** If the hermitian (or skew-hermitian) form $h$ is nonsingular, then the bilinear form $s_\#(h)$ is nonsingular. Moreover, embedding $B \rightarrow \operatorname{End}_F V$ by left multiplication, the adjoint involution with respect to $s_\#(h)$ restricts to $\tau$ on $B$ and to the adjoint involution with respect to $h$ on the centralizer $C_{\operatorname{End}_F V}B = \operatorname{End}_B U$.

**Proof.** Suppose $u \in U$ is such that $s_\#(h)(u, u') = 0$ for all $u' \in U$. Then $h(u, u')$ is a right ideal in $B$ contained in the kernel of $s$. In view of (2), $Bh(u, u')$ is then a two-sided ideal contained in $\ker s$. Since $B$ is simple and $s \neq 0$, we have $h(u, u') = (0)$, hence $u = 0$ since $h$ is nonsingular. For $b \in B$ and $u, u' \in U$ we have

$$s_\#(h)(bu, u') = s(bh(u, u'))$$

hence, in view of (2),

$$s_\#(h)(bu, u') = s(h(u, \tau(b)u')) = s_\#(h)(u, \tau(b)u').$$

Therefore, the adjoint involution with respect to $s_\#(h)$ restricts to $\tau$ on $B$. The last claim is clear. 

**Proposition 4.** Let $(V, q)$ be a quadratic space over $F$ and let $B \subset \operatorname{End}_F V$ be a simple subalgebra stable under the adjoint involution $\sigma$ with respect to $q$. We endow $V$ with the induced left $B$-module structure and pick any nonzero $F$-linear map $s : B \rightarrow F$ satisfying (2). There is a nonsingular hermitian form

$$h : V \times V \rightarrow B$$

(with respect to the involution $\sigma|_B$ on $B$) such that

$$q = s_\#(h).$$

**Proof.** Since $\sigma$ stabilizes $B$, it also stabilizes its centralizer $\operatorname{End}_B V$. By [4, Theorem 8.7.4], the restriction $\sigma|_{\operatorname{End}_B V}$ is the adjoint involution with respect to some nonsingular hermitian or skew-hermitian form

$$h_0 : V \times V \rightarrow B$$

with respect to $\sigma|_B$. Let $\theta$ denote the adjoint involution on $\operatorname{End}_B V$ with respect to $s_\#(h_0)$. There is an invertible element $g \in \operatorname{GL}(V)$ such that $\sigma(g) = \pm g$ and

$$\theta(f) = g \sigma(f) g^{-1}$$
for all $f \in \End_F V$. By Lemma 3, we have
\[ \theta|_B = \sigma|_B \quad \text{and} \quad \theta|_{\End_F V} = \sigma|_{\End_F V}, \]
hence $g$ is in the center of $B$. Define then
\[ h_1(v, v') = h_0(gv, v') \quad \text{for} \quad v, v' \in V. \]
Since $g$ is central in $B$, we have
\[ h_1(bv, b'v') = bh_1(v, v') \sigma(b') \]
for $v, v' \in V$ and $b, b' \in B$. Therefore, $h_1$ is a hermitian or skew-hamiltonian form on the $B$-module $V$. (More precisely, $h_1$ is hermitian if $h_0$ is hermitian and $\sigma(g) = g$ or if $h_0$ is skew-hermitian and $\sigma(g) = -g$, and it is skew-hermitian in the other cases.) A straightforward verification shows that $\sigma$ is the adjoint involution with respect to $s_\pi(h_1)$. In particular, since $\sigma$ is of orthogonal type (as it is the adjoint involution with respect to the quadratic form $q$), the form $h_1$ is hermitian. By [4, Sect. 8.7], involutions of orthogonal type on $\End_F V$ correspond bijectively to quadratic forms on $V$ up to a scalar factor. Therefore, multiplying $h_1$ by a suitable factor in $F^\times$, we get a hermitian form $h$ on $V$ such that $s_\pi(h) = q$.

Combining Lemma 2 and Proposition 4, we get a quadratic-form theoretic version of the hyperbolicity criterion.

**Theorem 5.** Let $(V, q)$ be an anisotropic quadratic space over $F$. If $(V, q)$ becomes hyperbolic over $F(\pi)$, then there exist finite-dimensional simple anisotropic homomorphic images $(B_1, \sigma_1), \ldots, (B_r, \sigma_r)$ of $(H, \sigma)$, hermitian spaces $(V_1, h_1), \ldots, (V_r, h_r)$ over $(B_1, \sigma_1), \ldots, (B_r, \sigma_r)$, and $F$-linear maps $s_i : B_i \to F$ satisfying (2) such that
\[ q = s_{\pi}(h_1) \perp \cdots \perp s_{\pi}(h_r). \]
Conversely, every quadratic form of this type becomes hyperbolic over $F(\pi)$.

This theorem may be used to describe the Witt kernel
\[ W(F(\pi)/F) = \ker(WF \to WF(\pi)). \]
For each finite-dimensional simple anisotropic $F$-algebra with involution $(B, \sigma)$ which is a homomorphic image of $(H, \sigma)$, we select an $F$-linear map $s : B \to F$ satisfying (2) and we denote by $W(B, \sigma)$ the Witt group of hermitian spaces over $(B, \sigma)$. The map $s$ induces a group homomorphism
\[ s_\pi : W(B, \sigma) \to WF. \]
**Corollary 6.** The Witt kernel $W(F(\pi)/F)$ is the subgroup of $WF$ generated by the images of the transfer maps $s_n: W(B, \sigma) \to WF$, where $(B, \sigma)$ runs over the finite-dimensional simple anisotropic homomorphic images of $(H_\sigma, \sigma)$.

3. **Structure of $H_\pi$**

As in the Introduction let

$$\pi(t) = t^{2n} + s_1 t^{2n-1} + \cdots + s_{2n-1} t + s_{2n} \quad (3)$$

be monic and separable over $F$. From (1) one has

$$H_\pi = F[a_1, a_2, \ldots, a_n, b_1, b_2, \ldots, b_n]/I,$$

where $I$ is the two-sided ideal generated by the elements

$$r(k) = \begin{cases} a_k + b_k + \sum_{i+j=k} a_i b_j - s_k & \text{for } k = 1, 2, \ldots, n \\ \sum_{i+j=k} a_i b_j - s_k & \text{for } k = n + 1, n + 2, \ldots, 2n. \end{cases} \quad (4)$$

From these relations it is clear that $H_\pi$ admits a unique involution $\sigma_\pi$ satisfying $\sigma_\pi(b_i) = a_i$ for all $i$.

We want to prove that $H_\pi$ is isomorphic to a quotient ring of a certain twisted polynomial ring which we now describe. Let $R = F(x_1, x_2, \ldots, x_{n-1})$, the free algebra on $n-1$ (noncommuting) variables. The ring $R$ admits a unique $F$-algebra endomorphism $\alpha$ defined inductively by

$$\alpha(x_k) = -x_k + s_k - \sum_{i+j=k} \alpha(x_i) x_j \quad \text{for } k = 1, 2, \ldots, n-1. \quad (5)$$

In fact $\alpha$ is an automorphism; its inverse is the $F$-algebra endomorphism $\alpha'$ defined inductively by

$$\alpha'(x_k) = -x_k + s_k - \sum_{i+j=k} x_i \alpha'(x_j) \quad \text{for } k = 1, 2, \ldots, n-1. \quad (6)$$

For $k = 1, \ldots, n-1$, let

$$\delta(x_k) = \left(s_n - \sum_{i+j=n} \alpha(x_i) x_j\right) x_k + \sum_{i+j=n+k} \alpha(x_i) x_j - s_{n+k}. \quad (7)$$
Define an $F$-algebra homomorphism $R \to M_2(R)$ by mapping $x_k$ to $(\delta(x_k) \ 0 
olimits 0 \ \alpha(x_k))$. The image of an arbitrary element $a \in R$ then has the form $(\delta(a) \ a(\alpha(a)))$, where the map $\delta : R \to R$ is an $\alpha$-derivation, i.e., an $F$-linear map such that 

$$\delta(ab) = \delta(a) b + \alpha(a) \delta(b) \quad \text{for all } a, b \in R.$$ 

Let $S$ be the twisted polynomial ring $S = R[y; \alpha, \delta]$. So $S = \{ \sum r_i y^i | r_i \in R \}$ and the multiplication in $S$ is determined by $yr = \alpha(r)y + \delta(r)$. We may thus equivalently define $S$ as the factor ring 

$$S = F[x_1, \ldots, x_{n-1}, y]/J'$$

where $J'$ is the ideal generated by the relations 

$$r'(k) = yx_k - \alpha(x_k)y - \delta(x_k) \quad \text{for } k = 1, \ldots, n - 1.$$ 

Let 

$$y' = -y + s_n - \sum_{i+j=n} \alpha(x_i)x_j \in S. \quad (8)$$

We may define an $F$-linear involution $\beta_\pi$ on $R$ by 

$$\beta_\pi(x_k) = \alpha(x_k) \quad \text{for } k = 1, \ldots, n - 1; \quad (9)$$

then 

$$\beta_\pi \delta(x_k) - \delta(x_k) = \alpha(x_k) \left( s_n - \sum_{i+j=n} \alpha(x_i)x_j \right)$$

$$- \left( s_n - \sum_{i+j=n} \alpha(x_i)x_j \right) x_k$$

$$= \beta_\pi(x_k)(y + y') - (y + y')x_k.$$ 

Therefore, the relation $r'(k)$ may be rewritten as 

$$r'(k) = \beta_\pi(x_k)y' - y'x_k - \beta_\pi \delta(x_k),$$

hence $\beta_\pi$ extends to an involution on $S$ by letting 

$$\beta_\pi(y) = y'. \quad (10)$$

Now let $J$ be the ideal in $F(a_1, a_2, \ldots, a_n, b_1, b_2, \ldots, b_n)$ generated by the relations $r(k)$, for $1 \leq k \leq 2n - 1$. We will abuse notation by letting $a_i$ and $b_i$ denote their images in $F(a_1, a_2, \ldots, a_n, b_1, b_2, \ldots, b_n)/J$. 


PROPOSITION 7. There is a unique isomorphism of $F$-algebras with involution

$$\phi : (S, \beta_n) \to (F\{a_1, a_2, \ldots, a_n, b_1, b_2, \ldots, b_n\}/J, \sigma_n)$$

such that $\phi(x_i) = b_i$ for $i = 1, \ldots, n - 1$, $\phi(y) = a_n$, and $\phi(y') = b_n$.

Proof. Let $T = F\{a_1, a_2, \ldots, a_n, b_1, b_2, \ldots, b_n\}$. There is an $F$-algebra homomorphism $\phi : R \to T/J$ such that $\phi(x_k) = b_k$, for $k = 1, \ldots, n - 1$. An easy induction argument shows that $\phi(\alpha(x_k)) = a_k$, $k = 1, \ldots, n - 1$. It then follows that for each $k = 1, \ldots, n - 1$

$$\phi(\delta(x_k)) = \left(s_n - \sum_{i+j=n} a_i b_j\right)b_k + \sum_{i+j=n+k, i,j<n} a_i b_j - s_{n+k}$$

$$= b_n b_k - a_k b_n.$$

Hence $b_n \phi(x_k) = \phi(\alpha(x_k))b_n + \phi(\delta(x_k))$, so $\phi$ can be extended to $S$ by setting $\phi(y) = b_n$. Then

$$\phi(y') = -b_n + s_n - \sum_{i+j=n} a_i b_j,$$

hence relation $r(n)$ yields $\phi(y') = a_n$. Since the involution $\beta_n$ is defined by (9) and (10), and since $\sigma_n(a_k) = b_k$ for $k = 1, \ldots, n$, it is clear that $\phi$ preserves the involutions.

To define a homomorphism from $T/J$ to $S$, we first consider the homomorphism $\psi : T \to S$ obtained by setting $\psi(b_k) = x_k$ and $\psi(a_k) = \alpha(x_k)$ for $k = 1, \ldots, n - 1$, and $\psi(b_n) = y$, $\psi(a_n) = y'$. To check that $\psi$ factors through $T/J$ we need to verify the relations $r(k)$ for $k = 1, \ldots, 2n - 1$. For $k = 1, \ldots, n - 1$, we have

$$\psi(a_k) + \psi(b_k) + \sum_{i+j=k} \psi(a_i) \psi(b_j) - s_k$$

$$= \alpha(x_k) + x_k - \sum_{i+j=k} \alpha(x_i) x_j - s_k = 0.$$  

For $k = n$ we have

$$\psi(a_n) + \psi(b_n) + \sum_{i+j=n} \psi(a_i) \psi(b_j) - s_n = y' + y$$

$$- \sum_{i+j=n} \alpha(x_i) x_j - s_n = 0.$$
Finally for \( k = n + 1, \ldots, 2n - 1 \) we have

\[
\sum_{i+j=k} \psi(a_i) \psi(b_j) - s_k
\]

\[
= \psi(a_n) \psi(b_{k-n}) + \psi(a_{k-n}) \psi(b_n) + \sum_{i+j=k, i, j < n} \psi(a_i) \psi(b_j) - s_k
\]

\[
= y'x_{k-n} + \alpha(x_{k-n})y + \sum_{i+j=k} \alpha(x_i)x_j - s_k
\]

\[
= -yx_{k-n} + \delta(x_{k-n}) + \alpha(x_{k-n})y
\]

\[
= 0.
\]

It follows that \( \psi \) induces an \( F \)-algebra homomorphism from \( T/J \) to \( S \). This induced map is inverse to \( \phi \).

Given this proposition it follows that \( H_p \cong S/V \) where \( V \) is the ideal in \( S \) generated by the image in \( S \) of the last relation \( r(2n) \), that is, by \( y'y - s_{2n} \).

As it turns out this ideal has a very simple form.

**Lemma 8.** The element \( y'y \) lies in the center of \( S \) and \( y'y = yy' \).

**Proof.** We consider the following two elements in the power series ring \( S[[u]] \) (in the central indeterminate \( u \)):

\[
\xi = 1 + x_1u + u_2u^2 + \cdots + x_{n-1}u^{n-1} + uy^n,
\]

\[
\eta = 1 + \alpha(x_1)u + \alpha(x_2)u^2 + \cdots + \alpha(x_{n-1})u^{n-1} + y'u^n.
\]

By Proposition 7 we have

\[
\eta \xi = 1 + s_2u + s_2u^2 + \cdots + s_{2n-1}u^{2n-1} + y'uy^{2n}.
\]

Now \( \eta, \xi \) are invertible in \( S[[u]] \) and so

\[
\xi \eta = \xi(\eta \xi^{-1}) = 1 + s_1u + \cdots + s_{2n-1}u^{2n-1} + (\xi y'\xi^{-1})u^{2n}.
\]

But since \( \xi \in 1 + uS[[u]] \) we have \( \xi y'\xi^{-1} = y'y + t_1u + t_2u^2 + \cdots \) for some \( t_j \in S \) and so

\[
\xi \eta = 1 + s_1u + \cdots + s_{2n-1}u^{2n-1} + y'uy^{2n} + t_1u^{2n+1} + \cdots.
\]

On the other hand direct calculation gives

\[
\xi \eta = 1 + (x_1 + \alpha(x_1))u + \cdots + yy'u^{2n},
\]
hence $yy' = y'y$ and $0 = t_1 = t_2 = \cdots$. Hence $\xi$ commutes with $y'y$. But then $y'y$ commutes with $x_1, x_2, \ldots, x_{n-1}, y$, so $y'y$ lies in the center of $S$.

We can now state the main structure theorem on the algebra $H_n$.

**Theorem 9.** Let $\pi(t) = t^{2n} + s_1 t^{2n-1} + \cdots + s_{2n-1} t + s_{2n}$ be monic and separable over $F$. Let $S = R[y; \alpha, \delta]$ be the twisted polynomial ring over the free $F$-algebra $R = F[x_1, \ldots, x_{n-1}]$ where $\alpha$ and $\delta$ are given by Eqs. (5) and (7). Let $y'$ be as in (8). Then the element $y'y - s_{2n}$ is central in $S$ and symmetric under the involution $\beta_x$ defined by (9) and (10), and there is a unique isomorphism of $F$-algebras with involution:

$$\phi : (S/(y'y - s_{2n})S, \beta_x) \to (H_n, \sigma_\pi)$$

such that $\phi(x_i) = b_i$ for $i = 1, \ldots, n - 1$, $\phi(y') = a_n$, and $\phi(y) = b_n$.

**Proof.** This follows immediately from Proposition 7 and Lemma 8.

The polynomial $y'y - s_{2n}$ is monic of degree 2 in $y$. It follows that every element of $S/(y'y - s_{2n})S$ has a unique expression as $r_0 + r_1 y$ where $r_0, r_1 \in R$. In particular the canonical homomorphism $R \to S/(y'y - s_{2n})S$ is an imbedding and $S/(y'y - s_{2n})S$ is a free left $R$-module of dimension 2. We therefore have the following corollary.

**Corollary 10.** The subalgebra of $H_n$ generated by $b_1, \ldots, b_{n-1}$ is free on those generators. In particular if the degree of $\pi$ is greater than four, then $H_n$ contains a free $F$-algebra on two variables.

The same method as in Lemma 8 yields the following.

**Proposition 11.** In $H_n$ we have

$$\pi(t) = (t^n + b_1 t^{n-1} + \cdots + b_n)(t^n + a_1 t^{n-1} + \cdots + a_n). \quad (11)$$

There is an automorphism of $H_n$ of order 2 which interchanges $a_k$ and $b_k$ for all $k = 1, \ldots, n$.

**Proof.** In the power series ring $H_n[[u]]$ in a central indeterminate $u$, we consider the elements

$$a = 1 + a_1 u + \cdots + a_n u^n \quad b = 1 + b_1 u + \cdots + b_n u^n.$$

From $\pi(t) = (t^n + a_1 t^{n-1} + \cdots + a_n)(t^n + b_1 t^{n-1} + \cdots + b_n)$ it follows that

$$ab = 1 + s_2 u + s_2 u^2 + \cdots + s_{2n} u^{2n},$$
hence \( ab \) is central in \( H_u[[u]] \). On the other hand, \( a \) is invertible in \( H_u[[u]] \) since it lies in \( 1 + uH_u[[u]] \); therefore
\[
ab = a^{-1}(ab)a = ba,
\]
and (11) follows. This relation shows that the relations \( r(k) \) are preserved under the map which interchanges \( a_k \) and \( h_k \) for \( k = 1, \ldots, n \). Therefore, this map induces an automorphism of \( H_u \).

4. QUATERNION ALGEBRAS

In this section we begin by examining an interesting homomorphic image \( C_\pi \) of \( H_\pi \). It will turn out that if the degree of \( \pi \) is at most four then \( C_\pi \) is isomorphic to \( H_\pi \). We will use \( C_\pi \) to obtain information about quaternion algebras which split over \( F(\pi) \).

To begin let \( \pi(t) \in F[t] \) be as in (3). Let
\[
U = F[r_1, r_2, \ldots, r_{n-1}, r_n, a_{ij}, 1 \leq i \leq j \leq n]
\]
be the polynomial ring in \( n + \binom{n}{2} \) variables. Let
\[
f(t) = t^n + r_1 t^{n-1} + \cdots + r_{n-1} t + r_n
\]
be the generic polynomial of degree \( n \) and let
\[
q(x_1, x_2, \ldots, x_n) = \sum_{i \leq j} a_{ij} x_i x_j
\]
be the generic quadratic form in \( n \) variables. Let \( D \) denote the Clifford algebra of \( q \) over \( U \), that is,
\[
D = U[y_1, \ldots, y_n]/I_q,
\]
where \( U[y_1, \ldots, y_n] \) is the free algebra in \( n \) variables over \( U \) and \( I_q \) is the ideal generated by the set of elements \( \{(c_1 y_1 + \cdots + c_n y_n)^2 - q(c_1, \ldots, c_n)c_1, \ldots, c_n \in U\} \). We then define \( C_\pi \) to be \( D/V_\pi \) where \( V_\pi \) is the ideal of \( U \) generated by the relations needed to obtain \( f(t)^3 - q(t^n-1, t^{n-2}, \ldots, t, 1) = \pi(t) \). In other words \( C_\pi \) is the Clifford algebra of the image of \( q \) over the ring \( Z_\pi = U/V_\pi \). We will let \( q_\pi \) denote this form. We first describe \( Z_\pi \).

**Proposition 12.** The canonical \( F \)-algebra homomorphism from \( F[a_{ij}, 1 \leq i \leq j \leq n-1] \) to \( Z_\pi \) is an isomorphism. In particular \( Z_\pi \) is isomorphic to a polynomial ring in \( (\frac{n}{2}) \) variables over \( F \).
Proof. By computing the coefficients of the polynomial $f(t)^2 - q(t^{n-1}, t^{n-2}, \ldots, t, 1) - \pi(t)$ one sees that the ideal $V_\pi$ is generated by the elements

$$w(k) = \sum_{i+j=k} r_ir_j - \sum_{i+j=k} a_{ij} - s_k \quad \text{for } k = 1, 2, \ldots, n, \quad (12)$$

where we let $r_0 = 1$. The relations $w(k)$ for $k = 1, 2, \ldots, n$ allow one to express (in $Z_\pi$) each $r_k$ in terms of the $a_{ij}$, $1 \leq i \leq j \leq n - 1$. Then the relation $w(k)$ for $k = n + 1, \ldots, n$ can be used to express the element $a_{n-n,n}$ in terms of the $a_{ij}$, $1 \leq i \leq j \leq n - 1$. It follows that the canonical map $F[a_{ij}, 1 \leq i \leq j \leq n - 1] \to Z_\pi$ is onto. Since $V_\pi$ is generated by $2n$ elements the Krull dimension of the ring $Z_\pi$ is at least $n$. Therefore, the kernel of the canonical map above must be reduced to 0 and the result follows.

Let $\tau_\pi$ be the standard involution on $C_\pi$, viewed as the Clifford algebra of $q_\pi$ over $Z_\pi$; that is, $\tau_\pi$ is the unique involution leaving the elements of $Z_\pi$ invariant and satisfying $\tau_\pi(y_i) = -y_i$ for all $i$.

**Proposition 13.** There is a unique $F$-algebra homomorphism $\gamma$ from $(H_\pi, \alpha_\pi)$ onto $(C_\pi, \tau_\pi)$ such that $\gamma(a_i) = r_i - y_i$ and $\gamma(b_i) = r_i + y_i$ for $i = 1, \ldots, n$. The kernel of $\gamma$ is the smallest ideal of $H_\pi$ such that in the factor ring the images of the elements $a_i b_j + a_j b_i$ are central for $1 \leq i \leq j \leq n$.

Proof. Over the polynomial ring $Z_\pi$ we have $f(t)^2 - q(t^{n-1}, t^{n-2}, \ldots, t, 1) = \pi(t)$. Hence in $C_\pi[t]$ we have

$$\pi(t) = f(t)^2 - \left(\sum_{i=1}^n y_i t^{n-i}\right)^2 = \left(f(t) - \sum_{i=1}^n y_i t^{n-i}\right)\left(f(t) + \sum_{i=1}^n y_i t^{n-i}\right).$$

Therefore

$$\left(t^n + \sum_{i=1}^n (r_i - y_i) t^{n-i}\right)\left(t^n + \sum_{i=1}^n (r_i + y_i) t^{n-i}\right) = \pi(t)$$

in $C_\pi[t]$ and so there is a map $\gamma : H_\pi \to C_\pi$ such that $\gamma(a_i) = r_i - y_i$ and $\gamma(b_i) = r_i + y_i$ for $i = 1, \ldots, n$. Clearly this uniquely determines $\gamma$. Moreover $\gamma \circ \alpha_\pi = \tau_\pi \circ \gamma$. The image of $\gamma$ contains $y_1, \ldots, y_n$. Since $a_{ij} = y_i^2$ and $a_{ij} = y_i y_j + y_j y_i$ for $i \neq j$, the map $\gamma$ is surjective. This proves the first part.

We now identify the kernel of $\gamma$. Let $W$ be the smallest ideal of $H_\pi$ such that the images of the elements $a_i b_j + a_j b_i$ are central in $H_\pi/W$ for

1 \leq i \leq j \leq n. It is easy to see that \( W \) is the ideal generated by the commutators \([a_i b_j + a_j b_i, b_m]\) for \( 1 \leq i, j, m \leq n \). We shall prove that \( W = \ker \gamma \).

If \( 1 \leq i \leq j \leq n \) then

\[
\gamma(a_i b_j + a_j b_i) = (r_i - y_j)(r_j + y_j) + (r_j - y_j)(r_i + y_i) = 2r_i r_j - a_{ij}
\]

(13)

which lies in the center of \( C_\pi \). Thus \( W \) is contained in the kernel of \( \gamma \). Let \( \overline{H_\pi} = H_\pi / W \). Thus \( \gamma \) induces a homomorphism from \( \overline{H_\pi} \) onto \( C_\pi \). We need to show that this map is an isomorphism.

For \( k = 1, \ldots, n \), let

\[
w_k = \frac{1}{2}(a_k + b_k) \in \overline{H_\pi} \quad \text{and} \quad z_k = \frac{1}{2}(b_k - a_k) \in \overline{H_\pi}.
\]

From the relations (4), we have

\[
2w_k = s_k - \sum_{i+j=k} a_i b_j \quad \text{for } k = 1, \ldots, n,
\]

hence \( w_k \) is central. Moreover for \( 1 \leq i, j \leq n \) we have

\[
z_i z_j + z_j z_i = (w_i - a_i)(b_j - w_j) + (w_j - a_j)(b_i - w_i)
\]

\[
= -a_i b_j - a_j b_i + w_i(a_i + b_j) + w_j(a_i + b_i) - 2w_i w_j
\]

\[
= -a_i b_j - a_j b_i + 2w_i w_j
\]

which lies in the center of \( \overline{H_\pi} \). From the universal property of \( D \), it follows that there is a homomorphism \( \eta: D \to \overline{H_\pi} \) such that \( \eta(y_k) = z_k \) and \( \eta(r_k) = w_k \) for all \( k \). In order to show that \( \eta \) induces a homomorphism from \( C_\pi \) to \( \overline{H_\pi} \), we show that \( \eta \) maps the ideal \( \mathcal{V}_\pi \) to 0. Let

\[
g(t) = t^n + w_1 t^{n-1} + \cdots + w_n = \eta(f(t)) \in \overline{H_\pi}[t].
\]

Since in \( D[t] \), \( q(t^{n-1}, \ldots, t, 1) = (y_2 t^{n-1} + \cdots + y_n t + y_n)^2 \), we have to show

\[
g(t)^2 - \left( \sum_{k=1}^{n} z_k t^{n-k} \right)^2 = \pi(t) \quad \text{in } \overline{H_\pi}[t].
\]
This readily follows from the relation
\[ \pi(t) = \left(t^n + a_1t^{n-1} + \cdots + a_n\right)\left(t^n + b_1t^{n-1} + \cdots + b_n\right) \]
\[ = \left(g(t) - \sum_{k=1}^{n} z_k t^{n-k}\right)\left(g(t) + \sum_{k=1}^{n} z_k t^{n-k}\right). \]

Thus, there is a homomorphism \( \eta : C_\pi \to \overline{H}_x \) such that \( \eta(y_k) = z_k \) and \( \eta(r_k) = w_k \) for all \( k \).

In order to show injectivity of \( \gamma \) on \( \overline{H}_x \), it suffices now to show \( \eta \circ \gamma \) is the identity on \( \overline{H}_x \). Since this algebra is generated by \( w_1, \ldots, w_n \), and \( z_1, \ldots, z_n \), it is enough to show \( \gamma(z_k) = y_k \) and \( \gamma(w_k) = r_k \) for all \( k \). But

\[ \gamma(2z_k) = \gamma(b_k - a_k) = (r_k + y_k) - (r_k - y_k) = 2y_k \]

and

\[ \gamma(2w_k) = \gamma(a_k + b_k) = (r_k - y_k) + (r_k + y_k) = 2r_k. \]

For the next result we need to establish some additional notation. Suppose \( L \) is a finite field extension of \( F \) and \( \phi : Z_\pi \to L \) is a surjective homomorphism. The quadratic form \( \phi(q_\pi) \) is not necessarily nondegenerate. We will let \( \phi(q_\pi)' \) denote its nondegenerate part, which is uniquely determined up to isometry. The dimension of this nondegenerate form is the rank of the specialization of the matrix of the form \( q_\pi \) to \( L \).

**Proposition 14.** Let \( (A, \sigma) \) be anisotropic and let \( \phi : (C_\pi, \tau_\pi) \to (A, \sigma) \) be an \( F \)-algebra homomorphism. Then \( \phi(Z_\pi) \) is a direct sum \( L_1 \oplus \cdots \oplus L_k \) of finite field extensions of \( F \). Let \( \rho_i : \phi(Z_\pi) \to L_i \) be the canonical projection. Then \( \phi(C_\pi, \tau_\pi) = (B_1, \sigma_1) \oplus \cdots \oplus (B_k, \sigma_k) \) where for each \( i \), \( (B_i, \sigma_i) \) is the Clifford algebra of the form \( \rho_i \circ \phi(q_\pi)' \) over \( L_i \) and \( \sigma_i \) is the standard involution on \( B_i \).

**Proof.** By Lemma 1 the image of \( \phi \) must be semisimple. Because \( \phi(Z_\pi) \) lies in the center of that image it must be a direct sum of fields. Moreover \( \phi \) factors through the canonical projection of \( C_\pi \) onto \( C_\pi/IC_\pi \) where \( I \) is the kernel of the restriction of \( \phi \) to \( Z \). Let \( \rho_i \) denote the projection of \( \phi(Z) \) onto \( L_i \). Then \( C_\pi/IC_\pi = C_1 \oplus \cdots \oplus C_k \) where \( C_i \) is the Clifford algebra of \( \rho_i \circ \phi(q_\pi)' \) over \( L_i \). Let \( J_i \) denote the Jacobson radical of \( C_i \). Then \( B_i = C_i/J_i \) is precisely the Clifford algebra of the form \( \rho_i \circ \phi(q_\pi)' \) over \( L_i \). Also one checks easily that the resulting homomorphism \( C_\pi \to B_1 \oplus \cdots \oplus B_k \) preserves involutions if we use the standard involution on each \( B_i \).

For the purposes of the next corollary we will call a semisimple \( F \)-algebra \( (B, \sigma) \) \( \pi \)-special if it is a homomorphic image of \( (C_\pi, \tau_\pi) \) satisfying the conditions of the proposition, that is, \( (B, \sigma) = \phi(C_\pi, \tau_\pi) = (B_1, \sigma_1) \).
$\oplus \cdots \oplus (B_k, \sigma_k)$, where $\phi(Z_k) = L_1 \oplus \cdots \oplus L_k \subseteq Z(B)$ is a direct sum of fields and $(B_i, \sigma_i)$ is the Clifford algebra of the form $(\rho_i \circ \phi)(q_i^\prime)$ over $L_i$ with the standard involution.

**Corollary 15.** Let $(A, \sigma)$ be an anisotropic central simple algebra with involution over the field $F$ with fixed field $F$. The algebra $(A, \sigma)$ becomes hyperbolic over $F(\pi)$ if it contains a $\pi$-special, $\sigma$-invariant subalgebra.

**Proof.** This follows from Proposition 13, Proposition 14, and from [5, Proposition 10]. □

We proceed to show how the algebra with involution $(C_\pi, \tau_\pi)$ may be used to determine the quaternion $F$-algebras (and also the quadratic étale extensions of $F$) which are split by $F(\pi)$.

For every quadratic étale extension $L/F$, we denote by $-$ the non-trivial automorphism of $L/F$, which is the unique involution of the second kind on $L$. Similarly, for every quaternion $F$-algebra we denote by $-$ the quaternion conjugation on $Q$, which is the unique symplectic involution on this algebra.

**Lemma 16.** For every quadratic étale extension $L/F$, the following are equivalent:

(i) $L$ is split, i.e., $L \cong F \times F$;
(ii) the algebra with involution $(L, -)$ is hyperbolic;
(iii) the algebra with involution $(L, -)$ is isotropic.

Similarly, for every quaternion $F$-algebra $Q$, the following are equivalent:

(i) $Q$ is split;
(ii) the algebra with involution $(Q, -)$ is hyperbolic;
(iii) the algebra with involution $(Q, -)$ is isotropic.

**Proof.** The right ideal generated by a zero-divisor in a quadratic étale extension or a quaternion algebra is isotropic for $-$; this proves (i) $\Rightarrow$ (ii) in each case. The implications (ii) $\Rightarrow$ (iii) are clear and (iii) $\Rightarrow$ (i) follows in each case from the fact that an isotropic algebra with involution is not a division algebra. □

**Proposition 17.** Let $L/F$ be a quadratic field extension (necessary étale, since char. $F \neq 2$). The following are equivalent:

(i) $L$ splits over $F(\pi)$, i.e., $L \otimes F(\pi) \cong F(\pi) \times F(\pi)$;
(i') $L \subseteq F(\pi)$;
(ii) $(L, -)$ becomes hyperbolic over $F(\pi)$;
(iii) there is a homomorphism of $F$-algebras with involution $(C_\pi, \tau_\pi) \to (L, -)$. 

Moreover, if these conditions hold, then every homomorphism as in (iii) is surjective.

**Proof.** The equivalence of (i) and (i') is clear, and the equivalence of (i) and (ii) follows from the lemma. Moreover, (iii) ⇔ (ii) is a consequence of the general hyperbolicity criterion [5, Proposition 10], since \((C_π, τ_π)\) is a homomorphic image of \((H_π, σ_π)\). Conversely, if (ii) holds, then this hyperbolicity criterion yields a homomorphism

\[φ : (H_π, σ_π) → (L, −)\]

Since \(L\) is commutative, \(φ(a_bj + a_jb)\) is central for all \(i, j\), hence, by Proposition 13, the map \(φ\) factors through \((C_π, τ_π)\).

Suppose now \(φ : (C_π, τ_π) → (L, −)\) is a homomorphism such that \(φ(C_π) = F\). Since 0 is the only skew-symmetric element in \(F\), all the skew-symmetric elements in \(C_π\) are in the kernel of \(φ\); in particular, \(φ(y_k) = 0\) for all \(k\), hence the relation

\[f(t)^2 - q(t^{n-1}, ..., t, 1) = f(t)^2 - \left(\sum_{k=1}^{n} y_k t^{n-k}\right)^2 = π(t)\]

in \(C_π[t]\) yields

\[φ(f(t))^2 = π(t) \quad \text{in } F[t].\]

This is impossible since \(π\) is separable. □

There is a similar result for quaternion algebras:

**Proposition 18.** Let \(Q\) be a non-split (hence division) quaternion \(F\)-algebra. The following are equivalent:

(i) \(Q\) splits over \(F(π)\);

(ii) \((Q, −)\) becomes hyperbolic over \(F(π)\);

(iii) there is a homomorphism of \(F\)-algebras with involution \((C_π, τ_π) → (Q, −)\).

Moreover, if these conditions hold and if \(Q\) is not split by any quadratic field extension of \(F\) contained in \(F(π)\), then every homomorphism as in (iii) is surjective.

**Proof.** The arguments for (i) ⇔ (ii) ⇔ (iii) are exactly the same as in the preceding proposition. To prove (ii) ⇒ (iii), observe that \(a_jb_j + a_jb_j = a_jσ_π(a_j) + a_jσ_π(a_j)\) is \(σ_π\)-symmetric in \(H_π\). Therefore, its image \(φ(a_jb_j + a_jb_j)\) under any homomorphism \(φ : (H_π, σ_π) → (Q, −)\) is invariant under \(−\), hence it is in \(F\). Therefore, by Proposition 13, \(φ\) factors through \((C_π, τ_π)\). This completes the proof of the equivalence of conditions (i), (ii), and (iii).
If $\phi : (C_{\pi}, \tau_{\pi}) \to (Q, -)$ is not surjective, then the argument of the last paragraph of Proposition 17 shows that its image is a quadratic field extension $L$ of $F$. Hence $\phi$ induces a homomorphism $(C_{\pi}, \tau_{\pi}) \to (L, -)$, and the preceding proposition shows that $L \subset F(\pi)$; but then $Q$ is split by the quadratic extension $L$ of $F$ contained in $F(\pi)$.  

5. EXAMPLES OF LOW DEGREE

In this final section we consider the cases where the degree of $\pi(t)$ is 2, 4, or 6. If $\deg \pi(t) = 2$, the structure of $H_{\pi}$ was determined in 5. For completeness we repeat the result here.

**Proposition 19.** If the degree of $\pi(t)$ is two then the map $\gamma : (H_{\pi}, \sigma_{\pi}) \to (C_{\pi}, \tau_{\pi})$ is an isomorphism and $(H_{\pi}, \sigma_{\pi}) \cong (F(\pi), -)$, where $-$ denotes the nonidentity automorphism of $F(\pi)$ over $F$.

**Proof.** By Theorem 9, $(H_{\pi}, \sigma_{\pi}) \cong (F[y]/(y^2 - s_2), \beta_{\pi})$, where $y$ is transcendental over $F$, $y^2 = y + s_2$, and $\beta_{\pi}(y) = y$. In particular $H_{\pi}$ is commutative so $\gamma : (H_{\pi}, \sigma_{\pi}) \to (C_{\pi}, \tau_{\pi})$ is an isomorphism by Proposition 13. Moreover $y^2 - s_2 = -y^2 + s_2 y - s_2$. Hence $(H_{\pi}, \sigma_{\pi}) \cong (F(\pi), -)$, as desired.  

We thus recover some known results:

**Corollary 20.** Suppose $\deg \pi(t) = 2$. Let $(A, \sigma)$ be a central simple $F$-algebra with involution and assume $(A, \sigma)$ is anisotropic. The algebra $(A, \sigma)$ becomes hyperbolic over $F(\pi)$ if and only if it contains a quadratic subfield $L/F$ such that $L$ is isomorphic to $F(\pi)$ and $\sigma$ induces the nonidentity automorphism $-$ on $L/F$. If $t : F(\pi) \to F$ denotes the trace map, and if we assume moreover that $\pi$ is irreducible, then the Witt kernel $W(F(\pi)/F)$ is given by

$$W(F(\pi)/F) = t(3W(F(\pi), -)).$$

**Proof.** The first part follows from the hyperbolicity criterion [5, Proposition 10] and the explicit description of $H_{\pi}$ in the preceding proposition. The second part follows from Corollary 6 since $F(\pi) = H_{\pi}$ is the only simple homomorphic image of $H_{\pi}$ if $\pi$ is irreducible.  

The first part was proved by Bayer-Fluckiger, Shapiro, and Tignol in [1, Theorem 3.3], in the case where $\sigma$ is the first kind. The description of the Witt kernel of a quadratic field extension is well known: see [4, Theorem 2.5.2].
We now turn to the case where deg $\pi(t) = 4$:

$$\pi(t) = t^4 + s_1t^3 + s_2t^2 + s_3t + s_4.$$ 

Let $u$ be a new indeterminate over $F$ and $a = \frac{1}{8}(4u + 4s_2 - s_1^2)$; let also

$$\rho(u) = 4u(a^2 - s_4) - (s_1a - s_3)^2 \in F[u].$$ 

This polynomial is the cubic resolvent of $\pi(t)$: see [2, p. 140]. Its roots are $l_1^2, l_2^2, l_3^2$, where $l_1, l_2, l_3$ are related to the roots $t_1, \ldots, t_4$ of $\pi(t)$ by

$$l_1 = \frac{1}{2}(t_1 + t_2 - t_3 - t_4)$$
$$l_2 = \frac{1}{2}(t_1 - t_2 + t_3 - t_4)$$
$$l_3 = \frac{1}{2}(t_1 - t_2 - t_3 + t_4).$$

**Proposition 21.** If the degree of $\pi(t)$ is four then the map $\gamma : (H_\omega, \alpha_\omega) \rightarrow (C_\omega, \tau_\omega)$ is an isomorphism. Therefore $H_\omega$ is isomorphic to the Clifford algebra of the form $uX_1^2 + (a - s_3)X_1X_2 + (a^2 - s_4)X_2^2$ over the polynomial ring $F[u]$. This Clifford algebra is an $F[u]$-order of (reduced) discriminant $\rho(u)$ in a quaternion algebra $(u, -\rho(u))_{F(u)}$. If $\pi(t)$ is irreducible, this order is maximal.

**Proof.** For $\pi(t)$ of degree four defining relations for $H_\omega$ are

$$s_1 = a_1 + b_1$$
$$s_2 = a_2 + b_2 + a_1b_1$$
$$s_3 = a_1b_2 + a_2b_1$$
$$s_4 = a_2b_2.$$

By Lemma 8 the elements $a_2$ and $b_2$ commute in $H_\omega$. From the expression for $s_2$ it follows that $a_1b_1$ commutes with $b_2$ and the expression for $s_3$ shows that $a_1b_2$ commutes with $b_1$. Therefore, $a_1b_1$ is in the center of $H_\omega$. The elements $a_1b_2 + a_2b_1$ and $a_2b_2$ also lie in the center. From Proposition 13 we infer that $\gamma$ is an isomorphism. To compute the quadratic form we use the relations (12) for $n = 2$. We obtain

$$2r_1 = s_1$$
$$2r_2 + r_1^2 - a_{11} = s_2$$
$$2r_1r_2 - a_{12} = s_3$$
$$r_2^2 - a_{22} = s_4.$$
Combining the first two relations, we obtain \( r_2 = \frac{1}{p}(4a_{11} + 4s_2 - s_3^2) = \frac{1}{p}(4u + 4s_2 - s_3^2) = a \), where \( u \) and \( a \) are as defined above. The third and fourth relations then give \( a_{22} = s_1a - s_3 \) and \( a_{22} = a^2 - s_4 \). Hence the quadratic form is as stated. Diagonalizing this form (over the field of fractions \( F(u) \)) yields the quadratic form \( \langle u, u^{-1}p(u) \rangle \), whose Clifford algebra is \( (u, -\rho(u))_{F(u)} \). The reduced discriminant of the order \( C_\pi \) is the square root of the determinant of reduced trace form. It can be computed by using the standard basis \( 1, y_1, y_2, y_1y_2 \) for \( C_\pi \). If \( p(t) \) is irreducible, then the formula given above for the roots \( l_1^2, l_2^2, l_3^2 \) of \( \rho \) show that for each \( i \) one has \( l_i \notin F(l_i^2) \). It follows that the quaternion algebra \( (u, -\rho(u))_{F(u)} \) ramifies exactly at the irreducible factors of \( \rho \). Since \( \rho \) is the discriminant of \( C_\pi \), viewed as an order in \( (u, -\rho(u))_{F(u)} \), this order is maximal.

**Corollary 22.** The quaternion \( F \)-algebra which are split by \( F(\pi) \) but not by a quadratic extension of \( F \) contained in \( F(\pi) \) (if any) are of the form

\[
(x, -\rho(x))_F
\]

for \( x \in F^\times \).

**Proof.** Proposition 18 shows that the quaternion \( F \)-algebras which are split by \( F(\pi) \) but not by a quadratic extension of \( F \) contained in \( F(\pi) \) are homomorphic images of \( (C_\pi, \tau_\pi) \). Let \( (Q, -) \) be such an algebra and let \( \phi : (C_\pi, \tau_\pi) \to (Q, -) \) be a surjective homomorphism.

In the description of Proposition 21, \( C_\pi \) is an \( F[u] \)-order in a quaternion algebra \( (u, -\rho(u))_{F(u)} \). Let \( x = \phi(u) \in Q \). Since \( \tau_\pi(u) = u \), it follows that \( x = x \), hence \( x \in F \). Note that the algebra \( C_\pi \) contains an element with square \( u \); therefore, if \( x = 0 \), then \( \phi(C_\pi) \) is split. Moreover, if \( \rho(x) = 0 \), the image under \( \phi \) of a basis of \( C_\pi \) over \( F[u] \) is not linearly independent (since \( \rho \) is the discriminant of \( C_\pi \)), hence \( \phi \) is not onto, a contradiction. It is then easy to check that \( Q \) has the required form.

The corollary readily yields a description of the 2-fold Pfister forms over \( F \) which become hyperbolic over \( F(\pi) \), in view of the well-known relation between quaternion algebras and 2-fold Pfister forms. When \( F(\pi) \) contains a quadratic extension of \( F \), these 2-fold Pfister forms are determined by different arguments by Lam, Leep, and Tignol in [3, Theorem 3.9].

From the explicit description of \( H_\pi \) in Proposition 21, it follows that the finite-dimensional anisotropic homomorphic images of \( H_\pi \) are of the following two types:

- \( (L(\sqrt{r}), -) \) where \( L \) is a finite field extension of \( F \) containing a root \( r \) of \( \rho \) and \( - \) is the non-trivial automorphism of \( L(\sqrt{r})/L \);
- \( (Q, -) \) where \( Q \) is a quaternion algebra over a finite field extension
$L$ of $F$, of the form

$$Q = (l, -\rho(l))_L,$$

where $l \in L^\times$ is not a root of $\rho$.

If the degree of $\pi(t)$ is six, then $H_\pi$ is no longer the same as $C_\pi$ and so we can say no more than is contained in the general hyperbolicity criterion. However, there is one special case worth noting. For $\pi(t)$ of arbitrary degree we can always assume without loss of generality that the coefficient $s_1$ is zero. However, in the degree six case if we assume in addition that the coefficients $a_1$ and $b_1$ of the factorization of $\pi(t)$ are also zero then we get a surprising result.

**Proposition 23.** Assume that $\pi(t) = t^6 + s_4 t^4 + s_3 t^3 + s_2 t^2 + s_1 t + s_0$ and let $J$ be the ideal in $H_\pi$ generated by $b_1$. Then $H_\pi/J$ is isomorphic to the Clifford algebra of the following quadratic form over $F$:

$$\left(\frac{s_2^2}{4} - s_4\right)x_2^2 + \left(\frac{s_2 s_3}{2} - s_5\right)x_2 x_3 + \left(\frac{s_3^2}{4} - s_6\right)x_3^2.$$

In particular, $H_\pi/J$ is either a quaternion algebra over $F$ or a quadratic étale extension of $F$.

**Proof.** If we set $b_1 = 0$ in the defining relations (4) we obtain

$$s_2 = a_2 + b_2,$$

$$s_3 = a_3 + b_3,$$

$$s_4 = a_2 b_2,$$

$$s_5 = a_2 b_3 + a_3 b_2,$$

$$s_6 = a_3 b_3.$$

From these relations it follows immediately that the image of every element of the form $a_i b_j + a_j b_i$ lies in the center of $H_\pi/J$ and so by Proposition 13, $H_\pi/J$ is isomorphic to $C_\pi/I$ where $I$ is the image of $J$ in $C_\pi$, that is, $I$ is the ideal generated by the image of $b_1$. By Proposition 13 the image of $b_1$ is $r_1 + y_1$, but by the relations (12), $r_1 = s_1/2 = 0$. It follows that $I$ is the ideal in $C_\pi$ generated by $y_1$. Hence in $C_\pi/I$ all of the terms $a_{ij}$ where $i = 1$ or $j = 1$ are zero. Hence by (12) we have

$$r_2 = s_2/2, \quad r_3 = s_3/2$$

$$a_{22} = r_2^2 - s_4$$

$$a_{23} = 2r_2 r_3 - s_5$$

$$a_{33} = r_3^2 - s_6.$$

In particular all of these elements lie in $F$. The result follows. \qed
Let $\delta$ denote the discriminant of the quadratic form of the proposition.

**Corollary 24.** Let $\pi(t) = t^6 + s_2t^4 + s_3t^3 + s_4t^2 + s_5t + s_6$ over $F$ and assume $\delta \neq 0$. If $A$ is a central simple $F$-algebra then $\pi(t)$ can be factored into two factors $(t^3 + a_2t + a_3)(t^3 + b_2t + b_3)$ in $A[t]$ iff $A$ can be decomposed into a tensor product of central simple $F$-algebras $C \otimes_F B$ where $C$ is the Clifford algebra of the form

$$\left(\frac{s_2^2}{4} - s_4\right)x_2^2 + \left(\frac{s_2s_3}{2} - s_5\right)x_2x_3 + \left(\frac{s_3^2}{4} - s_6\right)x_3^2.$$

**Proof.** The condition on $A$ is equivalent to saying that there is an $F$-algebra homomorphism from $H_2$ to $A$ with $b_2 = 0$. By the proposition and the assumption that $\delta \neq 0$ it follows that $A$ contains an $F$-subalgebra isomorphic to the Clifford algebra $C$. But $C$ is an $F$-central simple algebra and so must split off as a tensor factor of $A$. 

**References**