JOURNAL OF ALGEBRA **192,** 209–234 (1997)
ARTICLE NO. JA966939

On the Computation of the Trace Form of Some Galois Extensions

Christof Drees

Mathematisches Institut, Universität Münster, Einsteinstrasse 62, D-48149 Münster,

Martin Epkenhans

Fb Mathematik, Universität-Gesamthochschule, D-33095 Paderborn, Germany

and

Martin Krüskemper[†]

Mathematisches Institut, Universität Münster, Einsteinstrasse 62, D-48149 Münster, Germany

Communicated by Walter Feit

Received February 15, 1996

We investigate the trace form $\mathrm{tr}_{L/K}: L \to K: x \mapsto \mathrm{tr}_{L/K} x^2$ of a finite Galois extension L/K. In particular, we study 2-extensions of degree ≤ 16. Using some reduction theorems, these results yield a classification of nearly all trace forms of Galois extensions of degree ≤ 31. Finally, we study the trace form of a cyclotomic extension and of its maximal real subfield. © 1997 Academic Press

1. INTRODUCTION AND NOTATION

If L/K is a finite, separable field extension we can associate to it the trace form $\mathrm{trace}_{L/K}(x^2)$. We want to investigate the trace form if L/K is a Galois extension with given Galois group. We will consider Galois extensions of degree ≤ 31 of arbitrary fields of characteristic $\neq 2$. We further compute the trace form of cyclotomic extensions and of their maximal real subfields.

* E-mail: martine@uni-paderborn.de.
[‡] E-mail: kruskem@uni-muenster.de

0021-8693/97 $25.00

Let us fix some notations which will be used throughout this paper. Let K be a field of characteristic $\neq 2$. As usual, K^* denotes the multiplicative group of K and K^{*2} denotes the set of all squares of K^*. Then $W(K)$ denotes the Witt ring of K and $I^r(K)$, $r \geq 1$, is the rth power of the fundamental ideal $I(K)$ of $W(K)$ (for a definition see [18]). Let $a_1, \ldots, a_l \in K^*$. Then $\langle\langle a_1, \ldots, a_l \rangle\rangle = \otimes_{i=1}^{l} \langle 1, -a_i \rangle$ denotes the l-fold Pfister form. For quadratic forms ψ, ψ' we write $\psi \simeq \psi'$ ($\psi \sim \psi'$) if ψ and ψ' are isometric (Witt equivalent). For $m \in \mathbb{N}$ let $m \times \psi$ be the m-fold orthogonal sum of ψ. Let L/K be a field extension. If ψ is a quadratic form over K, then ψ_L denotes the lifting of ψ. Let ψ be a form over L. Then $\mathrm{tr}_{L/K}\psi$ denotes the Scharlau transfer of ψ with respect to L/K. We write $\langle L \rangle \simeq \mathrm{tr}_{L/K}\langle 1 \rangle$ for the trace form. Let $\lambda \in L^*$. Then $\mathrm{tr}_{L/K}\langle \lambda \rangle$ is called scaled trace form. $\mathrm{dis}(L/K)$ is the discriminant of the trace form. The Brauer group of K is denoted $\mathrm{Br}(K)$. Let $a, b \in K^*$. Then (a, b) denotes the generalized quaternion algebra generated over K by i, j and satisfying $i^2 = a$, $j^2 = b$, $ij = -ji$. The Hasse invariant $w_2\psi$ is defined by

$$w_2\psi := \prod_{1 \leq i < j \leq n} (a_i, a_j) \in \mathrm{Br}(K),$$

where $\psi \simeq \langle a_1, \ldots, a_n \rangle$ is a diagonalization of ψ.

Let L/K be a Galois extension then $G(L/K)$ denotes its Galois group. Let $G \to G(L/K)$ be a surjective group homomorphism. Then $(L/K, G)$ denotes the associated embedding problem.

2. PRELIMINARIES AND REDUCTION THEOREMS

First we briefly want to summarize some known results on computing trace forms of Galois extensions.

PROPOSITION 1. *Let L/K be a Galois extension of degree $2^l m$, m odd and $l \geq 0$.*

1. *Then $\langle L \rangle \simeq [L : K] \times \langle 1 \rangle$, if the degree of L/K is odd.*

2. *Let $[L : K]$ be even. Then $G(L/K)$ contains a cyclic 2-Sylow subgroup if and only if $\mathrm{dis}(L/K) \notin K^{*2}$. In this case $G(L/K)$ has a normal subgroup H of order m and for the fixed field $F := L^H$ of H we have $\langle L \rangle \simeq m \times \langle F \rangle$ and F/K is a cyclic extension of degree 2^l. Further, there exists a unique quadratic subextension $K(\sqrt{a}) \subset L$ and $\mathrm{dis}(L/K) \equiv a \bmod K^{*2}$. If $2^l m \equiv 0 \bmod 4$ then $\mathrm{dis}(L/K)$ is a sum of two squares.*

3. *If $L = K(\sqrt{a_1}, \ldots, \sqrt{a_l})$ has degree 2^l over K then $\langle L \rangle \simeq \langle 2^l \rangle \otimes \langle\langle -a_1, \ldots, -a_l \rangle\rangle$.*

4. *The signature values of the trace form of a Galois extension of degree n are either* 0 *or* n.

For a proof see [4, I.3.4], or [10, Lemma 2].

DEFINITION 1. Let ψ be a quadratic form over K and let G be a finite group. Then ψ is called G-realizable if and only if there is a Galois extension L/K with Galois group G and trace form isometric to ψ.

COROLLARY 1. *Let ψ be a quadratic form over K.*

1. *If G is a group of odd order, then ψ is G-realizable if and only if $\psi \simeq \operatorname{ord}(G) \times \langle 1 \rangle$ and G is a Galois group over K.*

2. *ψ is $(\mathbb{Z}_2)^l$-realizable iff there exist elements $a_1, \ldots, a_l \in K^*$, linearly independent* mod K^{*2} *with $\psi \simeq \langle 2^l \rangle \otimes \langle\langle -a_1, \ldots, -a_l \rangle\rangle$.*

From now on we can assume that ψ has even dimension ≥ 4. Further, the preceding proposition reduces our approach to the computation of trace forms of cyclic extensions of degree 2^l if the field extension has nonsquare discriminant. Part (2) of Proposition 1 generalizes as follows.

PROPOSITION 2. *Let G be a finite group of even order $2^l m$, m odd, and let G_2 be a 2-Sylow subgroup of G. Suppose G contains a normal subgroup of order m. Let ψ be a quadratic form of dimension $2^l m$ over K. Then ψ is G-realizable if and only if there exists a Galois extension F/K with*

1. $G(F/K) \simeq G_2$,
2. $\psi \simeq m \times \langle F \rangle$,
3. *the embedding problem $(F/K, G)$ has a solution.*

This result applies for example for abelian groups, groups with cyclic 2-Sylow subgroups, groups of order $4p$, $p \geq 5$ a prime, or if a 2-Sylow subgroup of G is the modular group $M(2^l)$, $l \geq 4$. The last assertion is Wong's theorem (see [13, Satz IV.3.5]). Next we consider decomposable groups.

PROPOSITION 3. *Let G_1, G_2 be finite groups. Then the form ψ is $G_1 \times G_2$-realizable over K iff there are Galois extensions L_1/K, L_2/K with $L_1 \cap L_2 = K$, $G(L_i/K) \simeq G_i$, $i = 1, 2$, and $\psi \simeq \langle L_1 \rangle \otimes \langle L_2 \rangle$.*

Proof. $L_1 \cap L_2 = K$ gives $\langle L_1 L_2 \rangle \simeq \langle L_1 \otimes L_2 \rangle \simeq \langle L_1 \rangle \otimes \langle L_2 \rangle$. ∎

The next lemma and its application appeared in [3, 4.3.1, 4.4.1].

LEMMA 1. *Let K be a field and ψ an n-dimensional form over K. Let L/K be a field extension of odd degree*:

1. *If $n = 2^l$ and ψ is a l-fold Pfister form over L then ψ is a l-fold Pfister form over K.*

2. *If there exists some φ over L such that $\psi_L \simeq m \times \varphi$ for some odd m, then there exists some φ' over K such that $\psi \simeq m \times \varphi'$.*

COROLLARY 2. *Let L/K be a Galois extension of degree $2^l m$, m odd. Then $\langle L \rangle$ is divisible by m; that is, there exists some ψ over K of dimension 2^l such that $\langle L \rangle \simeq m \times \psi$. Let $F \subset L$ be a fixed field of a 2-Sylow subgroup of $G(L/K)$. If $\mathrm{tr}_{L/F}\langle 1 \rangle$ is a Pfister form then so is ψ. In particular, ψ is similar to a Pfister form if a 2-Sylow subgroup is elementary abelian.*

We can get some information on the invariants of the trace form from the 2-rank of the Galois group.

DEFINITION 2. Let G be a finite group. Then the 2-rank $\mathrm{rk}_2(G)$ is the maximal number r such that G contains an abelian subgroup of exponent 2 and order 2^r.

We know, for example, $\mathrm{rk}_2(G) = 0$ iff G has odd order. Further, $\mathrm{rk}_2(G) = 1$ iff the 2-Sylow subgroups of G are cyclic or generalized quaternion groups.

PROPOSITION 4. *Let L/K be a Galois extension with Galois group G. Then $\langle L \rangle \in I^r(K)$, where $r = \mathrm{rk}_2(G)$; in particular, $\mathrm{dis}(L/K) \in K^{*2}$, if $\mathrm{rk}_2(G) \geq 2$ and $w_2\langle L \rangle = 0 \in \mathrm{Br}(K)$, if $\mathrm{rk}_2(G) \geq 3$.*

Proof (*Compare* [15, 5.25]). Let F be the fixed field of a subgroup $(\mathbb{Z}/2\mathbb{Z})^r \simeq H \subset G(L/K)$. Then $\varphi := \mathrm{tr}_{L/F}\langle 1 \rangle$ is in $I^r(F)$. By [2, Theorem 3.3] $\langle L \rangle = \mathrm{tr}_{F/K}\varphi \in I^r(K)$. ∎

Let $W_{\mathrm{red}}(K) = W(K)/W_{\mathrm{tor}}(K)$ be the reduced Witt ring, where $W_{\mathrm{tor}}(K)$ denotes the torsion part of $W(K)$. Recall that elements in $W_{\mathrm{red}}(K)$ are uniquely determined by its signature values. In [19, Section 5, Theorem 2] Scheiderer showed:

PROPOSITION 5. *Let L/K be a Galois extension with Galois group G. If $\mathrm{rk}_2(G) = s$ then $\langle L \rangle = (n/2^s) \times \psi$ in $W_{\mathrm{red}}(K)$, where ψ is an s-fold Pfister form. In particular, if K is Pythagorean (that is, any sum of squares in K is a square in K) then any trace form of a Galois extension is a multiple of some Pfister form, since $W(K)$ is either $\mathbb{Z}/2\mathbb{Z}$ or is torsion-free when K is Pythagorean.*

Let us now consider abelian groups of 2-rank 2.

PROPOSITION 6. *Let L/K be an abelian 2-extension with $\mathrm{rk}_2(G(L/K)) = 2$. Then there are elements $a, b \in K^*$ such that $K(\sqrt{a}, \sqrt{b})/K$ is a biquadratic extension contained in L/K and such that $(a, -1) = 0 \in \mathrm{Br}(K)$ if $[L : K] \neq 4$. We get*

1. $w_2\langle L \rangle = (a, b) + (ab, -1) \in \mathrm{Br}(K)$ *if* $[L : K] = 4$ *and*
2. $w_2\langle L \rangle = (a, b) \in \mathrm{Br}(K)$, *if* $[L : K] \geq 8$.

Proof. (2) There are cyclic subextensions K_1/K, K_2/K of L/K with $K_1 \cap K_2 = K$, $L = K_1K_2$ and $[K_1 : K] \geq 4$. Let $d_i = \mathrm{dis}(K_i/K)$, $i = 1, 2$. Then $(d_1, -1) = 0 \in \mathrm{Br}(K)$. If $(d_2, -1) = 0$ we get $w_2\langle L\rangle = (d_1, (-1)^{[K_2 : K]/2}d_2) = (d_1, d_2) \in \mathrm{Br}(K)$. Since $K(\sqrt{a}, \sqrt{b}) = K(\sqrt{d_1}, \sqrt{d_2})$, the result follows from (1). If $(d_2, -1) = (d_1d_2, -1) \neq 0 \in \mathrm{Br}(K)$, then K_2/K is a quadratic extension. Then $a \equiv d_1 \bmod K^{*2}$ and we can set $K_2 = K(\sqrt{b})$. ∎

Remark 1. Proposition 1 and Corollary 2 allow us to determine the trace form of any Galois extension of degree $2^l m$, m odd and $l \leq 2$. If we have a cyclic 2-Sylow subgroup apply Proposition 1, otherwise Corollary 2.

We further need the following fact on Galois extensions.

PROPOSITION 7. *Let L/K be a Galois extension and let $\alpha \in L^* - L^{*2}$ be an element of L/K such that $L(\sqrt{\alpha})/K$ is a Galois extension and*

$$1 \to G\big(L(\sqrt{\alpha})/L\big) \to G\big(L(\sqrt{\alpha})/K\big) \to G(L/K) \to 1$$

is a nonsplit extension. Then $L(\sqrt{t\alpha})/K$ is a Galois extension with Galois group $G(L(\sqrt{\alpha})/K) \simeq G(L(\sqrt{t\alpha})/K)$ for any $t \in K^*$.

Proof. Assume $t \notin L^{*2}$. Since the group extension does not split $L(\sqrt{\alpha}, \sqrt{t})/K$ is a Galois extension with Galois group isomorphic to $G(L(\sqrt{\alpha})/K) \times G(K(\sqrt{t})/K)$. Let $\sigma \in G(L(\sqrt{\alpha})/L), \tau \in G(K(\sqrt{t})/K)$ be elements of order 2. Choose a common prolongation $\rho \in G(L(\sqrt{\alpha}, \sqrt{t})/K)$ of σ and τ. Then $L(\sqrt{t\alpha})$ is the fix field of $\langle \rho\rangle$ and $\langle \rho\rangle$ is a normal subgroup of $G(L(\sqrt{\alpha}, \sqrt{t})/K)$ since ρ corresponds to (σ, τ). ∎

3. TRACE FORMS OF DEGREE 4

By Corollary 1 it remains to consider the cyclic group of order 4.

PROPOSITION 8. 1. *Let $D \in K^* - K^{*2}$. Then $K(\sqrt{D})/K$ is contained in a cyclic field extension of degree 4 if and only if D is a sum of two squares in K. Let $D = a^2 + b^2, a, b \in K$. Then $K\Big(\sqrt{q\big(D + a\sqrt{D}\big)}\Big)$, $q \in K^*$ is a parametrization of all cyclic extensions of degree 4 with discriminant D. We get*

$$\left\langle K\left(\sqrt{q\big(D + a\sqrt{D}\big)}\right)\right\rangle \simeq \langle 1, D, q, q\rangle.$$

2. *Let ψ be a quadratic form of dimension 4 over K with discriminant $D \in K^*$. Then ψ is a cyclic trace form if and only if $D = a^2 + b^2 \notin K^{*2}$ and $\psi \simeq \langle 1, D, q, q\rangle$ for some $a, b, q \in K^*$.*

Proof. (1) Set $F := K(\sqrt{D})$. Let $F(\sqrt{\alpha})/K$, $\alpha \in F^*$ be a cyclic extension of degree 4. Then $N_{F/K}(D + a\sqrt{D}) = Db^2 \equiv \mathrm{dis}(F(\sqrt{\alpha})/K) \equiv N_{F/K}(\alpha) \equiv D \bmod K^{*2}$. Using Hilbert 90 we get $\alpha^{-1}(D + a\sqrt{D})x = \beta\sigma(\beta)^{-1}$ for some $x \in K^*$, $\beta \in F^*$ with $\langle \sigma \rangle = G(F/K)$. Set $q = N_{F/K}(\beta)\cdot x$. We easily obtain, that $K(\sqrt{q(D + a\sqrt{D})})/K$ is a cyclic extension of degree 4.

(2) Let $L = K(\sqrt{q(D + a\sqrt{D})})$ with $a, b, q \in K^*$ and $D = a^2 + b^2$. Since $\langle D, D \rangle \simeq \langle 1, 1 \rangle$ we get $\langle L \rangle \simeq \langle 1, D, q, q \rangle$. ∎

4. TRACE FORMS OF DEGREE 8

Up to isomorphism there are three abelian and two nonabelian groups of order 8. In some cases we apply a formula of Serre to determine the Hasse invariant of the trace form. To do this we first have to compute some group extensions.

LEMMA 2. *Consider the restriction map*

$$\mathrm{res}: H^2(\mathfrak{S}_d, \mathbb{Z}_2) \to H^2(G, \mathbb{Z}_2),$$

where G is a subgroup of the symmetric group $\mathfrak{S}_d$ of degree $d = 2^l \geq 4$.

1. *Let σ be a cycle of length d and set $G = \langle \sigma \rangle$.*
   (a) *Then* $\mathrm{res}(s_4)$ *is the unique nonzero element of* $H^2(G, \mathbb{Z}_2)$. *Hence,* $\mathrm{res}(s_4)$ *corresponds to the exact sequence*

$$1 \to \mathbb{Z}_2 \to \mathbb{Z}_8 \to \mathbb{Z}_4 \to 1.$$

   (b) *The restriction map is trivial for all $d = 2^l \geq 8$.*

2. *Let $G = K(\mathfrak{A}_4) \simeq \mathbb{Z}_2 \times \mathbb{Z}_2$ be the commutator subgroup of the alternating group $\mathfrak{A}_4$. Then* $\mathrm{res}(s_4)$ *corresponds to the quaternion group extension*

$$1 \to \mathbb{Z}_2 \to Q_8 \to \mathbb{Z}_2 \times \mathbb{Z}_2 \to 1.$$

3. *If $G \simeq Q_8$ is the quaternion group of order* 8, *then* $\mathrm{res}(s_8) = 0$.

4. *Let $G \simeq D_{2n}$ be a dihedral group of order $2n = 2^l \geq 8$. Then* $\mathrm{res}(s_{2n}) = 0$.

Proof. Let $\pi: \widetilde{\mathfrak{S}_d} \to \mathfrak{S}_d$ be the canonical projection. Let $\tilde{G}$ be the preimage of G in $\widetilde{\mathfrak{S}_d}$ under π. If $g \in \mathfrak{S}_d$, then $\tilde{g} \in \widetilde{\mathfrak{S}_d}$ denotes an arbitrary preimage of g.

(1) We know $\sigma^{d/2} = \tau_1 \cdots \tau_{d/2}$ with pairwise disjoint transpositions $\tau_i \in \mathfrak{S}_d$. Since $\tilde{\tau}_i\tilde{\tau}_j$ has order 4 for $i \neq j$, we get $\tilde{\tau}_i\tilde{\tau}_j = \omega\tilde{\tau}_j\tilde{\tau}_i$. This gives $(\tilde{\tau}_1 \cdots \tilde{\tau}_{d/2})^2 = \omega^{d/4}$. Now the assertion follows from $\operatorname{ord}(\tilde{\sigma}^{d/2}) = \operatorname{ord}(\tilde{\tau}_1 \cdots \tilde{\tau}_{d/2})$ (see [6, Lemma 3]).

(2) Follows immediately from the definition (see also [20, Exemple]).

(4) Let $\sigma = (1, \ldots, n)(n+1, \ldots, 2n)$ and $\tau = (1, 2n)(2, 2n-1)\cdots(n, n+1)$. Then

$$D_{2n} \simeq \langle \sigma, \tau \rangle \simeq \langle \sigma, \tau | \sigma^n = \tau^2 = \mathrm{id}, \tau\sigma\tau^{-1} = \sigma^{-1} \rangle.$$

As in (1) we get $\tilde{\sigma}^n = \tilde{\tau}^2 = 1$. Let $\tilde{\sigma}_1, \tilde{\sigma}_2 \in \widetilde{D_{2n}}$ with $\pi(\tilde{\sigma}_1) = (1, \ldots, n)$, $\pi(\tilde{\sigma}_2) = (n+1, \ldots, 2n)$. Set $\tilde{\sigma} = \tilde{\sigma}_1\tilde{\sigma}_2$. Then $\tilde{\tau}\tilde{\sigma}_1\tilde{\tau}^{-1} = \lambda\tilde{\sigma}_2^{-1}$ for some $\lambda \in \{1, \omega\}$. Hence $\tilde{\tau}\tilde{\sigma}\tilde{\tau}^{-1} = \lambda\tilde{\sigma}_2^{-1}\tilde{\tau}\tilde{\sigma}_2\tilde{\tau}^{-1} = \tilde{\sigma}^{-1}$.

The proof of (3) is left to the reader. ∎

Now we apply Serre's cohomological trace formula [20].

COROLLARY 3. *Let L/K be a Galois extension with Galois group G and* $\operatorname{dis}(L/K) = D$.

1. *If G is cyclic of order $2^l \geq 8$, then*

$$w_2\langle L \rangle = (2, D) \in \mathrm{Br}(K).$$

2. *If $G \simeq Q_8$, D_{2n}, $n = 2^l \geq 4$, then*

$$D \in K^{*2}, \qquad w_2\langle L \rangle = 0.$$

Hence, $\langle L \rangle \in I^3(K)$.

3. *If a 2-Sylow subgroup of $G(L/K)$ is a generalized quaternion group then $\langle L \rangle \in I^3(K)$.*

Proof. (1) and (2) follow immediately from Lemma 2 and Proposition 1 since Q_8 and D_{2n} are not cyclic. Later on we give direct proofs of these results (see [6, Lemma 3]).

(3) $G(L/K)$ contains a subgroup $H \simeq Q_8$. Let F be the fixed field of H. Then $\mathrm{tr}_{L/F}\langle 1 \rangle \in I^3(F)$ by (2). Now proceed as in the proof of Proposition 4. ∎

Next we consider trace forms of cyclic extensions of degree 8.

PROPOSITION 9. *Let L/K be a cyclic extension of degree 4 with* $\operatorname{dis}(L/K) = D$. *Set $L = K(\sqrt{q(D + a\sqrt{D})})$ with $a, b, q \in K^*$, $D = a^2 + b^2$. Then the following conditions are equivalent*:

1. *L/K is contained in a cyclic extension of degree* 8.
2. $w_2\langle L \rangle = (2, D) \in \mathrm{Br}(K)$.

3. $(2, D) + (q, -1) = 0 \in \mathrm{Br}(K)$.
4. -1 *is a norm of* L/K.
5. $\langle L \rangle \simeq \langle 2, 2D, 1, 1 \rangle$.

Proof. The equivalence of (2), (3), and (5) is a consequence of Proposition 8, since a trace form of dimension 4 represents 1. The equivalence of (1) and (4) is well known (see [1]). We give three different proofs of the equivalence of (1) and (3). We want to point out that this result can be proved with different methods. We give a proof which uses Serre's formula, one using the theory of central simple algebras and one by direct computation.

1. The first proof is based on Serre's cohomological trace formula. This gives $e^*(s_4) = \inf(\mathrm{res}(s_4)) = (2, D) + w_2\langle L \rangle$. By Lemma 2(1)(a) this is the obstruction to the embedding problem $(L/K, \mathbb{Z}_8)$. Hence, (1) and (2) are equivalent.

2. (3) $\Leftrightarrow$ (4) Let $L = K(\sqrt{q(D + a\sqrt{D})})$. Let L/K be a cyclic extension of degree 4. Set $F = K(\sqrt{D})$ and $\delta = D + a\sqrt{D}$. Then $N_{F/K}((a - \sqrt{D})b^{-1}) = -1$. Let

$$\psi = \langle\langle (a - \sqrt{D})b^{-1}, q\delta \rangle\rangle.$$

Now we determine the Hasse invariant of $\mathrm{tr}_{F/K}\psi$. We get $w_2(\mathrm{tr}_{F/K}\psi) = (2, D) + (q, -1)$ (note that $(D, ab) = (D, 2(a + b)^2 - D) = (D, 2) \in \mathrm{Br}(K)$). On the other hand, we know [2, Satz 4.18]

$$\begin{aligned} w_2 \,\mathrm{tr}_{F/K}\psi &= \mathrm{cor}_{F/K}\big((a - \sqrt{D})b^{-1}, q\delta\big) \\ &= \mathrm{cor}_{F/K}\big[L, {}^{-}, (a - \sqrt{D})b^{-1}\big] = [L, {}^{-}, -1]. \end{aligned}$$

Now $(2, D) + (q, -1) = 0$ if and only if the cyclic algebra $[L, {}^{-}, -1]$ splits if and only if -1 is a norm of L/K. (For notations see [18, 8.12.3, 8.12.6].)

3. Kiming [14] proved the equivalence of (1) and (3) by an explicit computation of the obstruction. We follow his ideas and give a direct proof of this result. Let L/K be a cyclic extension of degree 4 with discriminant D. Set

$$\delta := D + a\sqrt{D}, \qquad F := K(\sqrt{D}).$$

Let $\langle \sigma \rangle = G(L/K)$, where σ is the automorphism given by $\sigma(\sqrt{q\delta}) = qb\sqrt{D}\sqrt{q\delta}^{-1}$.

(4) $\Rightarrow$ (3) Let $\alpha, \beta \in F$ with $q\delta = \alpha^2 + \beta^2$. Then $N_{F/K}((a - \sqrt{D})b^{-1}) = -1$. By the assumption there is some $\gamma \in F$ with

$$\left(\frac{a - \sqrt{D}}{b}\,\frac{\gamma}{\sigma(\gamma)}, q\delta\right) = 0 \in \mathrm{Br}(F).$$

Hence, the Pfister form $\psi = \langle\langle (a - \sqrt{D})b^{-1}\gamma\sigma(\gamma), q\delta\rangle\rangle$ splits. Thus $\mathrm{tr}_{F/K}\psi \sim 0 \in W(K)$, which gives $w_2(\mathrm{tr}_{F/K}\psi) = (2, D) + (q, -1) = 0$.

(3) $\Rightarrow$ (4) Since

$$\delta = \left(\frac{a+b}{2} + \frac{1}{2}\sqrt{D}\right)^2 + \left(\frac{a-b}{2} + \frac{1}{2}\sqrt{D}\right)^2 \tag{1}$$

and $(q, -1) = (q, -1) + (2, D) = 0 \in \mathrm{Br}(F)$, there are some $\alpha, \beta \in F$ with

$$q\delta = \alpha^2 + \beta^2. \tag{2}$$

Now set

$$\Delta := q\delta + \alpha\sqrt{q\delta} \in L, \qquad C := \frac{\sigma^2(\Delta)}{\beta\sqrt{q\delta}} = \frac{\sigma^2(\Delta)}{\sqrt{N_{L/F}(\Delta)}} = -\frac{\alpha - \sqrt{q\delta}}{\beta},$$

$$A := 1 + \frac{C}{\sigma(C)}.$$

Then $C^2 = \sigma^2(\Delta)\Delta^{-1}$, $C\sigma^2(C) = -1 = \sigma(C)\sigma^3(C)$, and $\Delta = -\beta\sqrt{q\delta} \cdot \sigma^2(C) = -\beta\sqrt{q\delta}\,C^{-1}$.

Suppose $C = -\sigma(C)$. We get $\sigma^2(C) = C$, which contradicts $C = -(\alpha - \sqrt{q\delta})\beta^{-1} \notin F$. Thus $A \neq 0$. From

$$0 \neq \frac{A\sigma(A)}{C} = \left(\frac{1}{C} + \frac{1}{\sigma(C)}\right)\left(1 + \frac{\sigma(C)}{\sigma^2(C)}\right) = -\mathrm{tr}_{L/K}(C) \in K,$$

we conclude $N_{L/K}(A) = -(\mathrm{tr}_{L/K}(C))^2$.

Claim. $(2, D) + (q, -1) = 0 \in \mathrm{Br}(K)$ implies

$$\mathrm{tr}_{L/K}(C) = -2\left(\frac{\alpha}{\beta} + \frac{\sigma(\alpha)}{\sigma(\beta)}\right) \in N_{F/K}(F^*).$$

Proof. From (1) and (2) we compute elements $x, y \in K$ with $q = (1 + x^2)(y^2 + Dz^2)$. We get

$$\begin{aligned}
\left(\mathrm{tr}_{L/K}(C), D\right) &= (2, D) + \left(\mathrm{tr}_{F/K}(\alpha\sigma(\beta)), D\right) \\
&= (q, -1) + \left(\mathrm{tr}_{F/K}(\alpha\sigma(\beta)), D\right) \\
&= \left(y^2 + Dz^2, -1\right) + \left(\mathrm{tr}_{F/K}(\alpha\sigma(\beta)), D\right) \\
&= \left(\left(y^2 + Dz^2\right) \cdot \mathrm{tr}_{F/K}(\alpha\sigma(\beta)), D\right).
\end{aligned}$$

An easy computation gives

$$\mathrm{tr}_{F/K}(\alpha\sigma(\beta)) = -\big((cb-a)^2 - D\big)\big(y^2 + Dz^2\big).$$

Now let $\gamma \in F$ be an element with $N_{F/K}(\gamma) = \mathrm{tr}_{L/K}(C)$. Then $-1 = N_{L/K}(A\gamma^{-1})$. ∎

PROPOSITION 10. *Let ψ be a quadratic form of dimension 8 over K with discriminant $D \in K^*$. Then ψ is a trace form of a cyclic extension if and only if*

1. $D = a^2 + b^2 \notin K^{*2}$ *for some* $a, b \in K^*$,
2. $(D, 2) = (q, -1) \in \mathrm{Br}(K)$ *for some* $q \in K^*$ *and*
3. $\psi \simeq \langle 1, 1, 1, D\rangle \perp \langle t\rangle \otimes \langle\langle -2, -D\rangle\rangle$ *for some* $t \in K^*$.

Proof. Let L/K be a cyclic field extension of degree 8. Set $F = K(\sqrt{D})$ and let F_1 be the unique subfield of L/K with $[F_1 : K] = 4$. L/K is a solution of the embedding problem $(F_1/K, \mathbb{Z}_8)$. From Proposition 9 we get $\langle F_1\rangle \simeq \langle 2, 2D, 1, 1\rangle$ and $(2, D) = (q, -1)$ for some $q \in K^*$. Set $L = F_1(\sqrt{\Delta})$. Then

$$\langle L\rangle \simeq \langle 2\rangle \otimes \langle F_1\rangle \perp \mathrm{tr}_{F_1/K}\langle 2\Delta\rangle \simeq \langle 1, 1, 1, D\rangle \perp \langle t\rangle \otimes \varphi,$$

where φ is a two-fold Pfister form with $w_2\varphi = w_2(\langle t\rangle \otimes \varphi) = w_2\langle L\rangle = (2, D)$ by Corollary 3.

Now let ψ be a quadratic form for which the assumption of the proposition holds. By Proposition 9 $K(\sqrt{q(D + a\sqrt{D})})/K$ is a cyclic extension of degree 4 which is contained in a cyclic extension L/K of degree 8. Set $F_1 = K(\sqrt{q(D + a\sqrt{D})})$ and $L = F_1(\sqrt{\Delta})$. Then $\langle F_1\rangle \simeq \langle 2, 2D, 1, 1\rangle$ and

$$\langle L\rangle \simeq \langle 1, 1, 1, D\rangle \perp \langle t'\rangle \otimes \langle\langle 2, D\rangle\rangle$$

for some $t' \in K^*$. By Proposition 7 $F_1(\sqrt{tt'\Delta})/K$ has the desired Galois group. We already proved $\langle F_1(\sqrt{tt'\Delta})\rangle \simeq \psi$. ∎

Now we prove $w_2\langle L\rangle = (2, D)$ without Serre's trace formula (see [5, 14]). There is a tower of quadratic extensions $K \subset F = K(\sqrt{D}) \subset F_1 = K(\sqrt{q\delta}) \subset L = K(\sqrt{\tau\Delta})$ with $D = a^2 + b^2$, $\delta = D + a\sqrt{D}$, $q = (1 + x^2)(y^2 + z^2D) = (-xy + x\sqrt{D})^2 + (y + xz\sqrt{D})^2$, $q\delta = \alpha^2 + \beta^2$, $\Delta = q\delta + \alpha\sqrt{q\delta}$, $a, b, q, x, y, z \in K$, $\alpha, \beta, \tau \in F^*$. Here we calculate α and β from the given representation of q as a sum of two squares in F and from

$$\delta = \left(\frac{a+b}{2} + \frac{1}{2}\sqrt{D}\right)^2 + \left(\frac{a-b}{2} + \frac{1}{2}\sqrt{D}\right)^2.$$

As above we get $\langle L\rangle \simeq \langle 1,1,1,D\rangle \perp \mathrm{tr}_{F_1/K}\langle 2\tau\Delta\rangle$ and

$$\mathrm{tr}_{F_1/K}\langle 2\tau\Delta\rangle \simeq \mathrm{tr}_{F/K}\langle 2\tau q\delta, 2\tau q\delta\rangle \simeq \langle 1,1\rangle \otimes \mathrm{tr}_{F/K}\langle \tau\rangle$$
$$\simeq \langle 1,1\rangle \otimes \langle \mathrm{tr}_{F/K}(\tau)\rangle \otimes \langle 1, N_{F/K}(\tau)\rangle,$$

if $\mathrm{tr}_{F/K}(\tau) \neq 0$. Otherwise $\mathrm{tr}_{F_1/K}\langle 2\tau\Delta\rangle \simeq \langle 1,1\rangle \otimes \langle 1,-1\rangle$ and $N_{F/K}(\tau) \equiv -D \bmod K^{*2}$. Hence in both cases we get $\mathrm{tr}_{F_1/K}\langle 2\tau\Delta\rangle \simeq \langle t\rangle \otimes \langle\langle -1, -N_{F/K}(\tau)\rangle\rangle$ for some $t \in K^*$. Thus $w_2\langle L\rangle = (N_{F/K}(\tau), -1) \in \mathrm{Br}(K)$.

1. *Case* $-1 \in K^{*2}$. Then $w_2\langle L\rangle = 0$. Let $\zeta_4^2 = -1$. Then $(2, D) = (\zeta_4, D) = 0$ by Proposition 9.

2. *Case* $-1 \in L^{*2} - K^{*2}$. Then $D \equiv -1 \bmod K^{*2}$ which gives $w_2\langle L\rangle = 0 = (D, 2)$.

3. *Case* $-1 \notin L^{*2}$. Set $\xi := \sigma(\tau)\tau^{-1}$. From $\xi \equiv N_{F/K}(\tau) \bmod F^{*2}$ we get

$$\langle \mathrm{tr}_{F/K}(\xi)\rangle \otimes \langle 2, 2D\rangle \simeq \langle 2\rangle \otimes \mathrm{tr}_{F/K}\langle \xi\rangle$$
$$\simeq \langle 2\rangle \otimes \mathrm{tr}_{F/K}\langle N_{F/K}(\tau)\rangle$$
$$\simeq \langle N_{F/K}(\tau)\rangle \otimes \langle 1, D\rangle,$$

since $\mathrm{tr}_{F/K}(\xi) = \sigma(\tau)\tau^{-1} + \tau\sigma(\tau)^{-1} \neq 0$. It follows $(2 \cdot \mathrm{tr}_{F/K}(\xi), -D) = w_2\langle L\rangle$. Now we compute ξ modulo squares of F^*. Let $\langle\sigma\rangle = G(L/K)$, where σ is the automorphism given by $\sigma(\sqrt{q\delta}) = qb\sqrt{D}\,\sqrt{q\delta}^{-1}$. Set

$$C := \frac{\sigma^2(\Delta)}{\beta\sqrt{q\delta}} = \frac{\sigma^2(\Delta)}{\sqrt{N_{L/F}(\Delta)}} = -\frac{\alpha - \sqrt{q\delta}}{\beta}, \qquad A := 1 + \frac{C}{\sigma(C)}.$$

Then $C^2 = \sigma^2(\Delta)\Delta^{-1}$, $C\sigma^2(C) = -1 = \sigma(C)\sigma^3(C)$, and $\Delta = -\beta\sqrt{q\delta} \cdot \sigma^2(C) = -\beta\sqrt{q\delta}\,C^{-1}$.

Suppose $C = -\sigma(C)$. We get $\sigma^2(C) = C$, which contradicts $C = -(\alpha - \sqrt{q\delta})\beta^{-1} \notin F$. Thus $A \neq 0$. Since

$$\phi := \frac{\sigma(\tau)\sigma(\Delta)}{\tau\Delta A^2} \in F_1$$

is invariant under σ^2, it is an element of F. From $L = K(\sqrt{\tau\Delta}) = K(\sqrt{\sigma(\tau\Delta)})$ we get $\phi \in F_1^{*2}$. Suppose $\phi \notin F^{*2}$. Then $\phi q\delta \in F^{*2}$; hence, $N_{F/K}(\phi) \equiv D \notin K^{*2}$, which contradicts

$$N_{F/K}(\phi) = \frac{\sigma^2(\Delta)}{\Delta(A\sigma(A))^2} = \left(\frac{C}{A\sigma(A)}\right)^2 = \left(\mathrm{tr}_{F/K}(C)\right)^{-4}.$$

Hence, $\xi = \sigma(\tau)\tau^{-1} \equiv \Delta A^2 \sigma(\Delta)^{-1} \bmod F^{*2}$ and

$$\begin{aligned}
\xi \equiv \frac{\Delta A^2}{\sigma(\Delta)} &= \frac{\beta\sqrt{q\delta}\,\sigma(C)A^2}{\sigma(\beta)\sigma\left(\sqrt{q\delta}\right)C} \\
&= \frac{\beta}{\sigma(\beta)}\frac{\delta}{b\sqrt{D}}\left(1 + \frac{C}{\sigma(C)}\right)\left(1 + \frac{\sigma(C)}{C}\right) \\
&= \frac{\beta}{\sigma(\beta)}\frac{a+\sqrt{D}}{b}\cdot \mathrm{tr}_{F_1/F}(A) \\
&= \frac{\beta}{\sigma(\beta)}\frac{a+\sqrt{D}}{b}\frac{2}{\beta\sigma(\beta)}\left(\beta\sigma(\beta) - \alpha\sigma(\alpha) + qb\sqrt{D}\right) \\
&\equiv 2\frac{a+\sqrt{D}}{b}\left(\beta\sigma(\beta) - \alpha\sigma(\alpha) + qb\sqrt{D}\right) \bmod F^{*2}.
\end{aligned}$$

We easily compute $\beta\sigma(\beta) - \alpha\sigma(\alpha) = (y^2 + z^2D)(ab(x^2-1) - 2xb^2)$. Hence

$$\begin{aligned}
\xi &\equiv 2\left(y^2 + z^2D\right)\frac{a+\sqrt{D}}{b}\left(ab(x^2-1) - 2xb^2 + (x^2+1)b\sqrt{D}\right) \\
&= 2\left(y^2 + z^2D\right)\left((ax-b) + x\sqrt{D}\right)^2 \equiv 2\left(y^2 + z^2D\right) \bmod F^{*2}.
\end{aligned}$$

This gives

$$\begin{aligned}
\mathrm{tr}_{F/K}\langle\xi\rangle &\simeq \mathrm{tr}_{F/K}\left\langle 2\left(y^2 + z^2D\right)\right\rangle \simeq \left\langle \mathrm{tr}_{F/K}(\xi), D\cdot\mathrm{tr}_{F/K}(\xi)\right\rangle \\
&\simeq \left\langle 2\left(y^2 + z^2D\right)\right\rangle \otimes \langle 2, 2D\rangle \simeq \langle 1, D\rangle,
\end{aligned}$$

since $\langle 1, D\rangle$ represents $y^2 + z^2D \neq 0$.

We finally conclude $w_2\langle L\rangle = (2\cdot\mathrm{tr}_{F/K}(\xi), -D) = (2, -D) = (2, D) \in \mathrm{Br}(K)$.

PROPOSITION 11. *Let ψ be a quadratic form of dimension 8 over K. Then ψ is $\mathbb{Z}_2 \times \mathbb{Z}_4$-realizable iff there are elements $a, D, q \in K^*$ such that*

1. *a, D, $aD \notin K^{*2}$ and D is a sum of two squares in K,*
2. *$\psi \simeq \langle 2\rangle \otimes \langle\langle -D, -a\rangle\rangle \perp \langle q\rangle \otimes \langle\langle -1, -a\rangle\rangle$.*

If ψ satisfies (1)–(3), *then ψ is not similar to a Pfister form iff $w_2\psi = (a, D) \neq 0$.*

The trace forms of Galois extensions with Galois group D_8 and Q_8 have been determined in [3, Section 6, Exemple]. Since there is no proof given we consider these trace forms now.

PROPOSITION 12. *Let ψ be a quadratic form of dimension 8 over K.*

1. *Then ψ is D_8-realizable if and only if there exists an element $q \in K^* - K^{*2}$ with $\psi \simeq \langle\langle -1, -q, -t\rangle\rangle$ for some $t \in K^*$ and $\langle 1, q\rangle$ represents more than two square classes.*

2. *ψ is Q_8-realizable if and only if $\psi \simeq \langle\langle -1, -1, t\rangle\rangle$ for some $t \in K^{*2}$ and Q_8 is a Galois group over K.*

Q_8 appears as Galois group over K iff there exist some $a, b \in K^*$ with $a, b, ab \notin K^{*2}$ and $(a, b) + (ab, -1) = 0 \in \mathrm{Br}(K)$.

Proof. Let L/K be a Galois extension with Galois group D_8 or Q_8. Then L/K contains a biquadratic extension field $F = K(\sqrt{a}, \sqrt{b})$. Let $\alpha \in F$ with $L = F(\sqrt{\alpha})$. We can assume that $L/K(\sqrt{ab})$ is cyclic of degree 4. From Corollary 3(2) we get $\mathrm{dis}(L/K) \in K^{*2}$ and $w_2\langle L\rangle = 0$. Since

$$\langle L\rangle \simeq \langle 2\rangle \otimes \big(\langle F\rangle \perp \mathrm{tr}_{F/K}\langle \alpha\rangle\big),$$

the quadratic forms $\langle F\rangle$ and $\mathrm{tr}_{F/K}\langle\alpha\rangle$ have the same discriminant and Hasse invariant. By [18, 2.14.1] there is some $t \in K^*$ with $\mathrm{tr}_{F/K}\langle\alpha\rangle \simeq \langle t\rangle \otimes \langle F\rangle$, which gives $\langle L\rangle \simeq \langle 2\rangle \otimes \langle 1, t\rangle \otimes \langle F\rangle \simeq \langle 2\rangle \otimes \langle\langle -t, -a, -b\rangle\rangle$. Further L/K is a solution of the embedding problem $(F/K, G(L/K))$.

Let $G(L/K) \simeq D_8$. It is Galois-theoretic folklore (see [12, Theorem 3.10]) that $(F/K, D_8)$ has a solution L/K such that $L/K(\sqrt{ab})$ is cyclic if and only if $\langle a, b\rangle \simeq \langle 1, ab\rangle$ if and only if $\langle F\rangle \simeq \langle\langle -1, -ab\rangle\rangle$. Set $q = ab$.

Now consider $G(L/K) = Q_8$. A result of Witt [22] implies, that the solvability of $(F/K, Q_8)$ is equivalent to $(a, b) + (ab, -1) = 0 \in \mathrm{Br}(K)$, which is equivalent to $\langle 1, a, b, ab\rangle \simeq 4 \times \langle 1\rangle$. This result can also be obtained by trace form considerations (see [20; 9; 7.7]; use Lemma 2(3)). This gives the necessary condition in both cases.

Now consider D_8 again. We compute the trace form of an explicit polynomial. We will apply this method in the next section. A Galois extension L/K with Galois group D_8 is a splitting field of an irreducible polynomial $f(X) = X^4 + tX^2 + b$ such that $a := t^2 - 4b \notin \mathrm{dis}(f) \equiv b \notin 1 \bmod K^{*2}$. We get $a, b, ab \in L^{*2} - K^{*2}$ and $(a, b) = 0 \in \mathrm{Br}(K)$. Hence, $\langle 1, ab\rangle \simeq \langle a, b\rangle$. Further, $L/K(\sqrt{ab})$ is a cyclic extension with discriminant $b \equiv a \bmod K(\sqrt{ab})^{*2}$.

Let $t = 0$. Then $\mathrm{tr}_{L/K(\sqrt{ab})}\langle 1\rangle \simeq \langle 1, b, 1, 1\rangle$ and $ab \equiv -1 \bmod K^{*2}$, which gives

$$\langle L\rangle \simeq \langle 1, -1\rangle \otimes \langle 1, 1, 1, b\rangle \simeq \langle\langle 1, 1, 1\rangle\rangle.$$

Now consider $t \neq 0$. From [7, Theorem 1] we get

$$\begin{aligned}\langle K[X]/(f)\rangle &\simeq \langle 1, a\rangle \perp \langle -2t\rangle \otimes \langle a, b\rangle \\ &\simeq \langle 1, a\rangle \perp \langle -2t\rangle \otimes \langle 1, ab\rangle\end{aligned}$$

which gives

$$\begin{aligned}\langle L\rangle &\simeq \mathrm{tr}_{K(\sqrt{ab})/K}\langle 1, a, -t, -t\rangle \simeq \langle 2, 2ab\rangle \otimes \langle 1, a, -t, -t\rangle \\ &\simeq \langle\langle -1, -ab, t\rangle\rangle.\end{aligned}$$

We now prove the sufficient condition. Let $\psi \simeq \langle\langle -1, -q, -t\rangle\rangle$. By assumption there is some $a \in K^*$ which is represented by $\langle 1, q\rangle$ such that $q,\ a,\ aq \notin K^{*2}$. Set $b = aq$. Then $(a, b) = 0$. Choose $u, v \in K$ with $a = u^2 - 4bv^2$. Let $u \neq 0$. Set $X^4 + tX^2 + bv^2t^2u^{-2}$ and let L be a splitting field of f. We easily obtain $\langle L\rangle \simeq \psi$ and $G(L/K) \simeq D_8$. If $u = 0$, then $ab \equiv -1 \bmod K^{*2}$ and $\psi \sim 0 \in W(K)$. Then consider the splitting field of $X^4 + b$.

Let L/K be a Galois extension with Galois group Q_8 and let F/K be the biquadratic subextension of L/K. Then $L = F(\sqrt{\alpha})$ for some $\alpha \in F^* - F^{*2}$ and $\mathrm{tr}_{F/K}\langle\alpha\rangle \simeq \langle q\rangle \otimes \langle\langle -1, -1\rangle\rangle$. The Galois group of $F(\sqrt{tq^{-1}\alpha})/K$ is isomorphic to Q_8 and its trace form is $\langle\langle -1, -1, t\rangle\rangle$. ∎

Let us denote some observation which we will use later.

Remark 2. Let L/K be a Galois extension of degree 8 with $G(L/K) \in \{\mathbb{Z}_8, D_8, Q_8\}$ and let F be an intermediate field of L/K such that F/K is a normal extension of degree 4. Let $L = F(\sqrt{\alpha})$. Then the parameter $t \in K^*$ in Propositions 10 and 12 can be any element which is represented by $\mathrm{tr}_{F/K}\langle\alpha\rangle$. If $\mathrm{tr}_{F/K}(\alpha) \neq 0$, we can choose $t = \mathrm{tr}_{F/K}(\alpha)$. Otherwise we can take $t = 1$.

Proof. $\mathrm{tr}_{F/K}\langle\alpha\rangle$ is similar to a Pfister form. ∎

5. TRACE FORMS OF DEGREE 16

There are 14 different groups of order 16, five of which are abelian. (In [12] we find a list of all these groups. See also [21].) We are not able to compute the trace form of a cyclic extension of degree 16 and of an extension with Galois group Q_{16}. If G is a noncyclic abelian group we can use the results of Sections 3 and 4 to classify the G-realizable forms. We omit stating these results here.

First we determine trace forms of Galois extensions L/K with Galois group D_{16}, the quasidihedral group QD_8 and the modular group $M(16)$,

each of order 16. We know

$$D_{16} = \langle \sigma, \tau \mid \sigma^8 = \tau^2 = \mathrm{id}, \tau^{-1}\sigma\tau = \sigma^{-1} \rangle,$$
$$QD_8 = \langle \sigma, \tau \mid \sigma^8 = \tau^2 = \mathrm{id}, \tau^{-1}\sigma\tau = \sigma^3 \rangle,$$
$$M(16) = \langle \sigma, \tau \mid \sigma^8 = \tau^2 = \mathrm{id}, \tau^{-1}\sigma\tau = \sigma^5 \rangle.$$

Each of these groups contains an element of order 8 (see [13, I.14.9]). Let L/K be a Galois extension with Galois group $G = G(L/K) \in \{D_{16}, QD_8, M(16)\}$. We have a tower of quadratic subextensions,

$$K \subset K_1 := K(\sqrt{a}) := L^{\langle \tau, \sigma^2 \rangle} \subset L^{\langle \tau, \sigma^4 \rangle} =: K_2 \subset L^{\langle \tau \rangle} =: K_3 \subset L.$$

Set $K(\sqrt{b}) := L^{\langle \sigma \rangle}$. Then $K(\sqrt{b}) \cap K_3 = K$. Further $L/K(\sqrt{b})$ is a cyclic extension of degree 8 with discriminant $a \equiv ab \bmod K(\sqrt{b})^{*2}$. Let $\alpha \in K_2$ be any element with $K_3 = K_2(\sqrt{\alpha})$. Then $L = K_2(\sqrt{b})(\sqrt{\alpha})$. From Proposition 10 and Remark 2 we know

$$\begin{aligned} \mathrm{tr}_{L/K(\sqrt{b})}\langle 1 \rangle &\simeq \langle 1, 1, 1, ab \rangle \perp \langle t \rangle \otimes \langle\langle -2, -ab \rangle\rangle \\ &\simeq \langle 1, 1, 1, a \rangle \perp \langle t \rangle \otimes \langle\langle -2, -a \rangle\rangle \end{aligned}$$

with $t = 1$ or $t = \mathrm{tr}_{K_2(\sqrt{b})/K(\sqrt{b})}(\alpha) = \mathrm{tr}_{K_2/K}(\alpha) \in K$. Suppose $G \neq M(16)$. Then $\langle \sigma^4 \rangle$ is a normal subgroup of G with $G/\langle \sigma^4 \rangle \simeq D_8$. From $K_2(\sqrt{b}) = L^{\langle \sigma^4 \rangle}$ we get $G(K_2(\sqrt{b})/K) \simeq D_8$. Hence, $K_2(\sqrt{b})/K$ is a solution of the embedding problem $(K(\sqrt{a}, \sqrt{b})/K, D_8)$, where $F/K(\sqrt{b})$ is cyclic of order 4. From Proposition 3.10 in [12] we get $\langle a, ab \rangle \simeq \langle 1, b \rangle$. Now Frobenius reciprocity (see [18, 2.5.6]) gives

$$\begin{aligned} \langle L \rangle &\simeq \langle 2, 2b \rangle \otimes (\langle 1, 1, 1, ab \rangle \perp \langle t \rangle \otimes \langle\langle -2, -ab \rangle\rangle) \\ &\simeq \langle\langle -1, -1, -b, -t \rangle\rangle. \end{aligned}$$

PROPOSITION 13. *Let ψ be a quadratic form of dimension* 16 *over K. Let $G \in \{D_{16}, QD_8\}$. Then ψ is G-realizable if and only if there exist $b, t \in K^*$, $b \neq -1$ with*

1. $\psi \simeq \langle\langle -1, -1, -b, -t \rangle\rangle$,
2. $b, b+1, b(b+1) \notin K^{*2}$, *and*
3. *there is an element $q \in K^*$ with*

$$(b+1, 2) + (q, -b) = 0 \in \mathrm{Br}(K), \qquad \text{if } G = D_{16}$$
$$[\text{resp. } (b+1, -2) + (q, -b) = 0 \in \mathrm{Br}(K), \text{ if } G = QD_8.]$$

There exists some $q \in K^*$ *with* $(b+1,2)+(q,-b)=0 \in \mathrm{Br}(K)$ *iff*

$$X_1^2-(b+1)X_2^2-2X_3^2-2(b+1)bX_4^2=0$$

has a solution $x_1, x_2, x_3, x_4 \in K$ *with* $(x_1,x_2)\neq(0,0)$.

Proof. For the last assertion see [14, Theorem 6]. L/K is a solution of the embedding problem $(F/K,G)$ with $L/K(\sqrt{b})$ is cyclic. If $G=D_{16}$, apply [14, Theorem 6]. If $-1\in K^{*2}$ we can also use [9, 7.11]. Hence, $(a,ab)=0=(a,-b)$ and $(a,2)+(q,-b)=0$. We get $a=x^2+by^2$ with $x,y\in K^*$. Replace b by by^2x^{-2} and a by ax^{-2}. Now let $G=QD_8$. Then $G(L/K(\sqrt{a}))\simeq\langle\tau,\sigma^2\rangle\simeq D_8$. Apply [14, Theorem 7]. ∎

PROPOSITION 14. *Let* ψ *be a quadratic form of dimension* 16 *over* K. *Then* ψ *is* $M(16)$ *realizable if and only if there exist* $a, b, q, t \in K^*$ *with*

1. $a, b, ab \notin K^{*2}$, $(a,-1)=0\in\mathrm{Br}(K)$,
2. $(a,2b)+(q,-1)=0\in\mathrm{Br}(K)$,
3. $\psi\simeq\langle 2,2b\rangle\otimes(\langle 1,1,1,a\rangle\perp\langle t\rangle\otimes\langle\langle -2,-a\rangle\rangle)$.

Proof. Since $\langle\sigma^4,\tau\rangle$ is a normal subgroup of $M(16)$ with cyclic quotient we get $(a,-1)=0$. Use the same calculation as above and apply [12, Theorem 4.8.1]. ∎

Let us now consider the two pullbacks

$$D_8\curlywedge\mathbb{Z}_4=\langle\sigma,\tau,\rho\,|\,\sigma^4=\tau^2=\rho^2=1,[\sigma,\tau]=[\rho,\tau]=1,\sigma\rho=\rho\sigma^3\tau\rangle$$

and

$$Q_8\curlywedge\mathbb{Z}_4=\langle\sigma,\tau\,|\,\sigma^4=\tau^4=1,\tau^{-1}\sigma\tau=\sigma^{-1}\rangle.$$

PROPOSITION 15. *The quadratic form* ψ *over* K *is* $D_8\curlywedge\mathbb{Z}_4$*-realizable if and only if there are elements* $a, t, q \in K^*$, $a\notin K^{*2}$ *such that*

1. $\psi\simeq\langle\langle -1,-a,-t,-q\rangle\rangle$ *and*
2. $\langle 1,-a\rangle$ *represents some* $b\in K^*$ *with* $b, ab\notin K^{*2}$ *and* $(b,-1)=0\in\mathrm{Br}(K)$.

Proof. Set $G:=D_8\curlywedge\mathbb{Z}_4$. Then $\langle\tau\rangle\triangleleft G$ with $G/\langle\tau\rangle\simeq D_8$. Further $H:=\langle[\sigma,\rho],\sigma^2\rho\rangle$ is a normal subgroup of G with cyclic quotient of order 4. Let N/K be a Galois extension with Galois group G. Set $L:=N^{\langle\tau\rangle}$ and $F:=N^H$. Then there are elements $a,b\in K^*$ such that $K(\sqrt{a},\sqrt{b})/K$ is a biquadratic extension contained in L and $K(\sqrt{b})=L\cap F$. Hence, $b=x^2+y^2$ with $x,y\in K^*$ and $F=K(\sqrt{q(b+x\sqrt{b})})$ for some $q\in K^*$ (see Proposition 8). Since $\langle H,\tau\rangle\simeq\mathbb{Z}_2\times\mathbb{Z}_2\times\mathbb{Z}_2$ the extension $L/K(\sqrt{b})$ is

not cyclic and we can assume that $L/K(\sqrt{ab})$ is cyclic. Hence, $(a, b) = 0$ by Proposition 3.10 in [12]. L is a splitting field of an irreducible polynomial $f = X^4 - tX^2 + b \in K[X]$ with $a \equiv t^2 - 4b \not\equiv \operatorname{dis}(f) \equiv b \not\equiv 1 \bmod K^{*2}$. Now f is irreducible in $F[X]$. If $t \neq 0$ we get $\operatorname{tr}_{N/F}\langle 1\rangle \simeq \langle\langle -a, -2t\rangle\rangle$, which implies

$$\langle N\rangle \simeq \langle\langle -a, -2t\rangle\rangle \otimes \langle F\rangle \simeq \langle\langle -1, -a, -t, -q\rangle\rangle.$$

If $t = 0$, then $\langle N\rangle \sim 0 \in W(K)$. ∎

PROPOSITION 16. *The quadratic form ψ over K is $Q_8 \rtimes \mathbb{Z}_4$-realizable if and only if there are elements $a, t, q \in K^*$, $a \notin K^{*2}$ with*

1. $\psi \simeq \langle\langle -1\rangle\rangle \otimes (\langle\langle -1, -t\rangle\rangle \perp \langle q\rangle \otimes \langle 1, a, t, t\rangle)$ *and*
2. $\langle 1, -a\rangle$ *represents some element $b \in K^*$ with b, $ab \notin K^{*2}$ and* $(ab, -1) = 0 \in \operatorname{Br}(K)$.

Proof. If N/K is a Galois extension with Galois group $Q_8 \rtimes \mathbb{Z}_4$, then N contains subfields L, F such that L/K and F/K are Galois extensions with $G(L/K) \simeq D_8$ and $G(F/K) \simeq \mathbb{Z}_4$. Further, $L/L \cap F$ is cyclic of degree 4. Now proceed as in the proof of Proposition 15. ∎

Let

$$DC = \left\langle \sigma, \rho, \tau \,\middle|\, \sigma^4 = \rho^2 = \tau^2 = 1, [\sigma, \rho] = [\sigma, \tau] = 1, [\rho, \tau] = \sigma^2 \right\rangle.$$

PROPOSITION 17. *The quadratic form ψ is DC-realizable over K if and only if there are elements $a, b, c, t \in K^*$ with*

1. $\psi \simeq \langle\langle -1, -1, -abc, -t\rangle\rangle$ *and*
2. $a, b, c \notin K^{*2}$ *and* $(a, b) = (c, c) \in \operatorname{Br}(K)$.

Proof. We use the notation of [17, Theorem 2.A], where an explicit construction of a DC-extension is given. Let L/K be a Galois extension with Galois group DC and let $K(\sqrt{a}, \sqrt{b}, \sqrt{c})/K$ be an extension of degree 8 contained in L. Then $H := \langle \sigma_c^2, \sigma_c \circ \sigma_a, \sigma_c \circ \sigma_b\rangle \simeq Q_8$ and $DC = \langle H, \sigma_b\rangle$. Set $K_3 := L^{\langle \sigma_b\rangle}$ and $K_2 = L^{\langle \sigma_b, \sigma_c\rangle}$. Then $K(\sqrt{abc}) = L^H$, $L = K_3(\sqrt{abc})$, and $K_3 \cap K(\sqrt{abc}) = K$. Choose $\alpha \in K_2$ with $K_3 = K_2(\sqrt{\alpha})$. Since $L = K_2(\sqrt{abc})(\sqrt{\alpha})$, Proposition 12 and Remark 2 give

$$\operatorname{tr}_{L/K(\sqrt{abc})}\langle 1\rangle \simeq \langle\langle -1, -1, -t\rangle\rangle$$

with $t \in K^*$. ∎

By Propositions 3 and 12 the trace form of a $D_8 \times \mathbb{Z}_2$ (resp. $Q_8 \times \mathbb{Z}_2$) extension is a Pfister form.

6. SOME CONSEQUENCES

COROLLARY 4. *Let L/K be a cyclic field extension of degree $2^l \geq 4$ with discriminant D.*

1. *If L/K is contained in a cyclic field extension of degree 2^{l+1}, then*
$$\langle L\rangle \simeq \langle 2, 2D\rangle \perp (2^l - 2) \times \langle 1\rangle.$$
2. *If $l \geq 3$ and $-1 \in L^{*2}$, then $\langle L\rangle \simeq \langle D\rangle \perp (2^l - 1) \times \langle 1\rangle$.*

Proof. (1) If $l = 2$, see Proposition 9. Now consider $l \geq 3$. Let F be the unique subfield of L/K with $[L : F] = 4$. Since L/F is contained in a cyclic extension of degree 8 we get $\mathrm{tr}_{L/K}\langle 1\rangle \simeq \langle 2, 2\Delta\rangle \perp \langle 1, 1\rangle$. Now induction gives

$$\begin{aligned}\langle L\rangle &\simeq \mathrm{tr}_{F/K}\langle 2, 2\Delta\rangle \perp \mathrm{tr}_{F/K}\langle 1, 1\rangle \simeq \left\langle F\left(\sqrt{\Delta}\right)\right\rangle \perp \langle 1, 1\rangle \otimes \langle F\rangle \\ &\simeq \langle 2, 2D\rangle \perp (2^{l-1} - 2) \times \langle 1\rangle \perp \langle 1, 1\rangle \\ &\quad \otimes \left(\langle 2, 2D\rangle \perp (2^{l-2} - 2) \times \langle 1\rangle\right) \\ &\simeq \langle 2, 2D\rangle \perp (2^l - 2) \times \langle 1\rangle.\end{aligned}$$

(2) Let F be as above. Then $-1 \in F^{*2}$ and $\mathrm{tr}_{L/F}\langle 1\rangle \simeq \langle 1, \Delta, 1, 1\rangle$. Hence, $\langle L\rangle \simeq \langle 2\rangle \otimes \left\langle F\left(\sqrt{\Delta}\right)\right\rangle \perp \langle 1, 1\rangle \otimes \langle F\rangle \simeq \langle 1, D\rangle \perp (2^l - 2) \times \langle 1\rangle$ by part (1). ∎

COROLLARY 5. *Let L/K be a Galois extension with Galois group G. Suppose the Hasse invariant of $\langle L\rangle$ is nontrivial. Then either $\mathrm{rk}_2(G) = 2$ or the 2-Sylow subgroups are cyclic.*

Proof. If $\mathrm{rk}_2(G) \geq 3$ then $\langle L\rangle \in I^3(K)$ by Proposition 4. It is well known that if $\mathrm{rk}_2(G) = 1$ and G is a 2-group then G is either cyclic or a generalized quaternion group (see [11, 5.4.10]). We know from Corollary 3 that $\langle L\rangle \in I^3(K)$ if L/K is a Galois extension with generalized quaternion group as its Galois group. ∎

We determined the Hasse invariant of the trace form of a cyclic extension of degree 8 without Serre's formula. Using induction we are able to extend this method to all cyclic field extensions of degree $2^l \geq 8$. Let L/K be a cyclic field extension of degree $2^{l+1} \geq 16$ with discriminant D. Set $F := K(\sqrt{D})$. Let $\delta \in F^*$ be the discriminant of L/F and set $\varphi := \langle 2, 2\delta\rangle \perp 6 \times \langle 1\rangle \in W(F)$. Then by the induction hypothesis $\mathrm{tr}_{L/F}\langle 1\rangle \equiv \varphi \bmod I^3(F)$. From [2, Satz 3.3] we get $\langle L\rangle \equiv \mathrm{tr}_{F/K}\varphi \bmod I^3(K)$. Now $\mathrm{tr}_{F/K}\varphi \simeq \mathrm{tr}_{F/K}\langle 2, 2\delta\rangle \perp 6 \times \langle 2, 2D\rangle \simeq \langle 2, 2D\rangle \perp 14 \times \langle 1\rangle$, since $\mathrm{tr}_{F/K}\langle 2, 2\delta\rangle$ is the trace form of the cyclic extension $F(\sqrt{\delta})/K$ of degree 4 and by Proposition 9.

COROLLARY 6. *Let K be a field with $-1 \in K^{*2}$ and let L/K be a Galois extension.*

1. *If $G(L/K)$ contains a nonabelian group of order 8, then*

$$\langle L\rangle \sim 0 \in W(K).$$

2. *Let L/K be a nonabelian extension of degree 16. Then*

$$\langle L\rangle \sim 0 \in W(K)$$

if $G(L/K) \neq M(16)$. If $G(L/K) \simeq M(16)$, then $\langle L\rangle \sim \langle\langle 2, a\rangle\rangle$.

Proof. Let $H < G(L/K)$ be a nonabelian subgroup of order 8. Since $H \simeq D_8$, Q_8 we get $\mathrm{tr}_{L/L^H}\langle 1\rangle \sim 0 \in W(L^H)$ from Proposition 12. $M(16)$, $Q_8 \curlywedge \mathbb{Z}_4$, $D_8 \curlywedge \mathbb{Z}_4$ are the only nonabelian groups of order 16 with abelian subgroups of order 8 only. Apply Propositions 15, 16 in these cases. ∎

7. ON TRACE FORMS OF DEGREE ≤ 31

We apply our results to the classification of quadratic forms of dimension ≤ 31 which are trace forms of Galois extensions with prescribed Galois group. In [21] we find a list of all groups of order ≤ 31. We are not able to handle all cases. By Corollary 1 we can assume that G has even order. We do not discuss decomposable groups of order ≤ 31 here. We deduce from Proposition 2:

PROPOSITION 18. *Let ψ be a quadratic form of dimension $2m$, m odd over K with discriminant D. Let G be a group of order $2m$. Then ψ is G-realizable if and only if*

1. *$\psi \simeq m \times \langle 2, 2D\rangle$ with $D \notin K^{*2}$ and*
2. *the embedding problem $(K(\sqrt{D})/K, G)$ has a solution.*

This covers forms of dimensions 6, 10, 14, 18, 22, 26, 30. Let us discuss $G \simeq \mathfrak{S}_3$ in more detail. Suppose $\mathrm{char}(K) \neq 3$ and let L/K be a Galois extension with $G(L/K) \simeq \mathfrak{S}_3$. Then L is the splitting field of some irreducible trinomial $f(X) = X^3 + aX + b \in K[X]$ with discriminant $D = -27b^2 - 4a^3 \in L^{*2} - K^{*2}$. Suppose $-3D \notin K^{*2}$. Then $ab \neq 0$. Set

$$F(X, T) := X^3 - 3(3DT^2 + 1)X - 2(3DT^2 + 1) \in K(T)[X].$$

Then $F(X, T)$ is irreducible and has discriminant D mod $K(T)^{*2}$. We get $f(X) = (3b)^3(2a)^{-3} \cdot F(2a(3b)^{-1}X, (3^2b)^{-1})$. Hence, f is a specialization of $F(X, T)$. We conclude:

COROLLARY 7. *Let K be a Hilbertian field with* $\mathrm{char}(K) \neq 3$, *ψ a quadratic form of dimension* 6 *over K with discriminant D. Then ψ is $\mathfrak{S}_3$-realizable if $D \notin K^{*2}$ and $\psi \simeq 3 \times \langle 2, 2D \rangle$.*

Hence, the solvability of the embedding problem $(K(\sqrt{D})/K, \mathfrak{S}_3)$ does not provide any further restriction on ψ.

Let us consider another example. Let K be a local field such that the residue class field has characteristic $\neq 3$. Then any nonnormal extension of degree 3 is tamely ramified. Hence $\mathfrak{S}_3$ is a Galois group over K iff K does not contain the third roots of unity, i.e., iff $-3 \notin K^{*2}$. We conclude that ψ is $\mathfrak{S}_3$-realizable iff $\psi \simeq 3 \times \langle 2, -6 \rangle$ and $-3 \notin K^{*2}$.

Let us now consider forms of dimension 12. There are five different groups of order 12, two of which have a cyclic 2-Sylow subgroup, further, $\mathbb{Z}_2 \times \mathbb{Z}_6$, $\mathbb{Z}_2 \times \mathfrak{S}_3$, and $\mathfrak{A}_4$. We only consider $\mathfrak{A}_4$.

PROPOSITION 19. *A quadratic form of dimension* 12 *over K is $\mathfrak{A}_4$-realizable if and only if there is an irreducible polynomial $f \in K[X]$ of degree* 4 *with Galois group $\mathfrak{A}_4$ and $\psi \simeq 3 \times \langle K[X]/(f) \rangle$. In particular, $\psi \simeq 3 \times \langle\langle -a, -b \rangle\rangle$ for some $a, b \in K^*$.*

Let K be a Hilbertian field with $\mathrm{char}(K) = 0$. *Then ψ is $\mathfrak{A}_4$-realizable iff $\psi \simeq 3 \times \langle\langle -a, -b \rangle\rangle$ for some $a, b \in K^*$.*

Proof. Let L/K be a Galois extension with Galois group $\mathfrak{A}_4$. Let $F = K(\alpha)$ be an intermediate field of L/K with $[F : K] = 4$. Then L is a splitting field of the minimal polynomial of α over K. Further, $\langle L \rangle \simeq 3 \times \langle F \rangle$. From Lemma 1 we get $\langle L \rangle \simeq 3 \times \langle\langle -a, -b \rangle\rangle$ for some $a, b \in K^*$. If K is Hilbertian apply [8, Theorem 1, and Theorem 3]. ∎

Let $n = 20, 28$. Then $n = 4p$ for some prime $p > 3$. From Sylow theory we get

LEMMA 3. *Let G be a group of order $4p$, $p > 3$ a prime. Then G has a unique p-Sylow subgroup G_p. Further, G is the semidirect product $G_p \rtimes_\alpha G_2$ of G_p with a 2-Sylow subgroup G_2, where $\alpha : G_2 \to \mathrm{Aut}(G_p)$ is a homomorphism.*

If $p \equiv 1 \bmod 4$, then there are five types of groups, if $p \equiv 3 \bmod 4$ then there are four types of groups of order $4p$. In both cases the dihedral group D_{4p} is the unique nonabelian group of order $4p$ with noncyclic 2-Sylow subgroup.

PROPOSITION 20. *Let $p > 3$ be a prime. The quadratic form ψ is D_{4p}-realizable iff there are elements $a, b \in K^*$, linearly independent* mod K^{*2} *with*

1. $\psi \simeq p \times \langle\langle -a, -b \rangle\rangle$ *and*
2. $(K(\sqrt{a}, \sqrt{b})/K, D_{4p})$ *has a solution.*

There are 15 groups of order 24 (see [21]), three of which are abelian. Further, six nonabelian groups are decomposable. There are the two

semidirect products $\mathbb{Z}_3 \rtimes \mathbb{Z}_8$ and $\mathbb{Z}_3 \rtimes D_8$, both having a unique 3-Sylow subgroup. The dihedral group and the dicyclic group of order 24 both have a unique 3-Sylow subgroup. Apply Proposition 2 in these cases. It remains to consider $\mathrm{SL}_2(\mathbb{F}_3)$ and $\mathfrak{S}_4$.

PROPOSITION 21. *Let q be a prime power with $q \equiv \pm 3 \bmod 8$. Then the quadratic form ψ is $\mathrm{SL}_2(\mathbb{F}_q)$-realizable iff $\psi \simeq (q(q^2-1)/8) \times \langle\langle -1, -1, -t\rangle\rangle$ for some $t \in K^*$ and $\mathrm{SL}_2(\mathbb{F}_q)$ is a Galois group over K.*

Proof. The 2-Sylow subgroup of $\mathrm{SL}_2(\mathbb{F}_q)$ is a quaternion group of order 8 (see [11, Chap. 2, Theorem 8.3]). Let L/K be a Galois extension with Galois group $\mathrm{SL}_2(\mathbb{F}_q)$ and let F be the fix field of a 2-Sylow subgroup G_2. Then $\mathrm{tr}_{L/F}\langle 1\rangle \simeq \langle\langle -1, -1, t'\rangle\rangle$ for some $t' \in F^*$ and $\langle L\rangle \simeq ([L:K]/8) \times \psi$ for some Pfister form ψ over K with $\psi_F \simeq \langle\langle -1, -1, t'\rangle\rangle$ (apply Proposition 12 and Corollary 2). By [3, 4.5.2] there is some $t \in K^*$ with $\psi \simeq \langle\langle -1, -1, t\rangle\rangle$.

Since

$$1 \to \left\langle \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} \right\rangle \to \mathrm{SL}_2(\mathbb{F}_q) \to \mathrm{PSL}_2(\mathbb{F}_q) \to 1$$

is a nonsplit extension we can apply Proposition 7. Then proceed as in the proof of Proposition 12. ∎

Now let L/K be a Galois extension with Galois group $\mathfrak{S}_4$. Since $\mathfrak{S}_4$ has a dihedral group of order 8 as a 2-Sylow subgroup we get $\langle L\rangle \simeq 3 \times \langle\langle -1, -a, -b\rangle\rangle$ for some $a, b \in K^*$ (use Proposition 12, Lemma 1, and [3, 4.5.2]).

Consider a Galois extension L/K. Let G_2 be a 2-Sylow subgroup of its Galois group. Suppose that L/L^{G_2} is noncyclic and its trace form is not similar to a Pfister form. In general we do not get much information on the trace form of L/K. If $[L:K] \equiv 8 \bmod 16$ then G_2 must be $\mathbb{Z}_2 \times \mathbb{Z}_4$. If G has order 24, then the classification of all these groups implies that G has a normal subgroup of order 3 in this situation. Hence no problem arise for $n \le 31$. If G_2 has order 16, then $G_2 \simeq Q_8 \wedge \mathbb{Z}_4$, $G_2 \simeq Q_{16}$, or $G_2 \simeq M(16)$. In the latter case G_2 has a normal complement in G (see [13, Wong's theorem]).

8. THE TRACE FORM OF A CYCLOTOMIC EXTENSION AND ITS MAXIMAL REAL SUBFIELD

Next we apply our results to determine the trace form of a cyclotomic extension $K_n/\mathbb{Q}$ and the trace form of its maximal real subfield K_n^+. The trace form of a cyclotomic extension has been computed in [4, pp. 47–49]. We are able to give a shorter proof.

PROPOSITION 22. *Let $n \in \mathbb{N}$, $n \not\equiv 2 \bmod 4$. Let ζ_n be a primitive nth root of unity. Set $K_n := \mathbb{Q}(\zeta_n)$ and let $\Phi_n(X)$ be the minimal polynomial of ζ_n over $\mathbb{Q}$. We get*

1. $\langle K_n \rangle \sim 0$, *if $n \equiv 0 \bmod 4$ and if n has at least three distinct prime divisors*,
2. $\langle K_n \rangle \sim \langle p, -1 \rangle \otimes \langle q, -1 \rangle$, *if $n = p^r q^s \equiv 1 \bmod 2$ with $r, s \geq 1$*,
3. $\langle K_n \rangle \sim \langle (-1)^{r-1} \rangle \otimes \langle p, -1 \rangle$, *if $n = p^r \equiv 1 \bmod 2$, $r \geq 1$.*

Proof. *Case* 1. $n = 2^l \geq 4$. Then $\varphi(n) = 2^{l-1}$ and $\Phi_n(X) = X^{2^{l-1}} + 1$. Hence, $\langle K_n \rangle \sim 0$ by [4, III,4.1].

Case 2. $n = p^r$, $p \neq 2$, $r \geq 1$. Then $K_p/\mathbb{Q}$ is a subextension of $K_n/\mathbb{Q}$ with $[K_n : K_p] = p^{r-1} \equiv 1 \bmod 2$. Hence by Proposition 1 $\langle K_n \rangle \simeq p^{r-1} \times \langle K_p \rangle$. Now $X^p - 1 = (X-1)\Phi_p(X)$ gives

$$\langle p \rangle \sim \langle \mathbb{Q}[X]/(X^p - 1) \rangle \simeq \langle \mathbb{Q}[X]/(X-1) \rangle \perp \langle K_p \rangle \simeq \langle 1 \rangle \perp \langle K_p \rangle.$$

Thus $\langle K_p \rangle \sim \langle p, -1 \rangle$.

Case 3. $n = p_1^{e_1} \cdots p_t^{e_t}$, $e_1, \ldots, e_t \geq 1$. Then $K_n = K_{p_1^{e_1}} \cdots K_{p_t^{e_t}}$ and $K_{p_i^{e_i}} \cap \prod_{i \neq j} K_{p_j^{e_j}} = \mathbb{Q}$ gives $\langle K_n \rangle \simeq \otimes_{i=1}^t \langle K_{p_i^{e_i}} \rangle$. If n is even, then $\langle K_n \rangle \sim 0$ by case (1). If $t \geq 3$, then $\langle K_n \rangle \in I^t(\mathbb{Q})$ by Proposition 4. We further know sign $\langle K_n \rangle = 0$. ∎

Next we consider the trace form of $K_n^+/\mathbb{Q}$.

PROPOSITION 23. *Set $m := \varphi(n)/2 =: 2^e m_0$ with m_0 odd. Let t be the number of odd prime divisors of n. Then the trace form of the maximal real subfield K_n^+ inside K_n over $\mathbb{Q}$ is given as follows*:

1. $\langle K_2^+ \rangle \simeq \langle K_4^+ \rangle \simeq \langle 1 \rangle$ *and*

$$\langle K_n^+ \rangle \simeq \langle 2, 10 \rangle \perp (2^{l-1} - 2) \times \langle 1 \rangle, \qquad \text{if } n = 2^l \geq 8.$$

2. *Let $n = 4p^r$, $p \neq 2$, $r \geq 1$. Then*

$$\langle K_n^+ \rangle \simeq m \times \langle 2, 2p \rangle, \qquad \text{if } p \equiv 3 \bmod 4.$$
$$\langle K_n^+ \rangle \simeq \langle p \rangle \perp (m-1) \times \langle 1 \rangle, \qquad \text{if } p \equiv 1 \bmod 4.$$

3. *Let $n = 2^l p^r$, $p \neq 2$, $l \geq 3$, $r \geq 1$. Then*

$$\langle K_n^+ \rangle \simeq \langle 1, 5, p, p, p, 5p \rangle \perp (m-6) \times \langle 1 \rangle, \quad \text{if } p \equiv 3 \bmod 4 \text{ and } l > 3.$$
$$\langle K_n^+ \rangle \simeq \langle 1, 5, p, 5p \rangle \perp (m-4) \times \langle 1 \rangle, \quad \text{else}.$$

4. *Let* $n = 4p^r q^s$ *with* $p \neq q$ *odd and* $r, s \geq 1$. *Then*

$$\langle K_n^+ \rangle \simeq \langle 1, p, p, p, q, pq \rangle \perp (m-6) \times \langle 1 \rangle, \qquad \text{if } q \not\equiv p \equiv 3 \bmod 4.$$
$$\langle K_n^+ \rangle \simeq \langle 1, p, q, pq \rangle \perp (m-4) \times \langle 1 \rangle, \qquad \text{else}.$$

5. *Let* $n \equiv 0 \bmod 8$, $t \geq 2$; *or* $n \equiv 4 \bmod 8$, $t \geq 3$; *or* $n \equiv 1 \bmod 2$, $t \geq 4$; *or* $n \equiv 1 \bmod 2$, $t = 3$ *and* $p \equiv 1 \bmod 4$ *for all* $p \mid n$. *Then*

$$\langle K_n^+ \rangle \simeq m \times \langle 1 \rangle.$$

6. *Let* $n = p_1^{e_1} p_2^{e_2} p_3^{e_3}$ *odd and* $p_3 \equiv 3 \bmod 4$. *Then*

$$\langle K_n^+ \rangle \simeq \langle 1, p_1 p_2, p_2 p_3, p_1 p_3 \rangle \perp (m-4) \times \langle 1 \rangle,$$
$$\text{if } p_1 \equiv p_2 \equiv p_3 \equiv 3 \bmod 4.$$
$$\langle K_n^+ \rangle \simeq \langle 1, p_1, p_2, p_1 p_2 \rangle \perp (m-4) \times \langle 1 \rangle,$$
$$\text{if } p_1 \equiv p_2 \not\equiv p_3 \equiv 3 \bmod 4.$$
$$\langle K_n^+ \rangle \simeq \langle 1, 1, 1, p_1 \rangle \otimes \langle p_2, p_3 \rangle \perp (m-8) \times \langle 1 \rangle,$$
$$\text{if } p_1 \not\equiv p_2 \equiv p_3 \equiv 3 \bmod 4.$$

7. *Let* $n = p^r q^s, r, s \geq 1$, $p \neq q$ *odd. Then*

$$\langle K_n^+ \rangle \simeq \langle 1, p, q, pq \rangle \perp (m-4) \times \langle 1 \rangle, \qquad \text{if } p \equiv q \equiv 1 \bmod 4.$$
$$\langle K_n^+ \rangle \simeq m_0 \times \langle 2, 2pq \rangle, \qquad \text{if } p \equiv q \equiv 3 \bmod 4.$$
$$\langle K_n^+ \rangle \simeq \langle 2, 2q \rangle \perp (m-2) \times \langle 1 \rangle, \qquad \text{if } p \not\equiv q \equiv 1 \bmod 4,\ q \equiv 1 \bmod 8.$$
$$\langle K_n^+ \rangle \simeq \langle 1, q, p, p \rangle \perp (m-4) \times \langle 1 \rangle, \qquad \text{if } p \not\equiv q \equiv 1 \bmod 4,\ q \equiv 5 \bmod 8.$$

8. *Let* $n = p^r$, $r \geq 1$ *odd. Then*

$$\langle K_n^+ \rangle \simeq m \times \langle 1 \rangle, \qquad \text{if } p \equiv 3 \bmod 4.$$
$$\langle K_n^+ \rangle \simeq \langle 2, 2p \rangle \perp (m-2) \times \langle 1 \rangle, \qquad \text{if } p \equiv 1 \bmod 4.$$

Proof. Let $G_n := G(K_n/\mathbb{Q})$ and $G_n^+ = G(K_n^+/\mathbb{Q})$. We know $\dim\langle K_n^+ \rangle = [K_n^+ : \mathbb{Q}] = \operatorname{sign}\langle K_n^+ \rangle = \varphi(n)/2$. Let $n = 2^l p_1^{e_1} \dots p_t^{e_t}, e_1, \dots, e_t \geq 1, l \geq 0$ be the prime decomposition of n. By Proposition 4 we have to study the 2-rank of G_n^+ to get more information on $\langle K_n^+ \rangle$. We use the following facts from basic algebra and from number theory.

Fact I,

$$\mathrm{rk}_2(G_n) = \begin{cases} t, & \text{if } n \text{ is odd;} \\ t+1, & \text{if } n \equiv 4 \bmod 8; \\ t+2, & \text{if } n \equiv 0 \bmod 8. \end{cases}$$

Fact II. $\mathrm{rk}_2(G_n) - 1 \le \mathrm{rk}_2(G_n^+) \le \mathrm{rk}_2(G_n)$ and $\mathrm{rk}_2(G_n^+) = \mathrm{rk}_2(G_n) - 1$ if and only if $G_n \simeq \mathbb{Z}/2\mathbb{Z} \times H$ for some abelian group H if and only if n is even or n has a prime divisor $p \equiv 3 \bmod 4$; ($\mathrm{rk}_2(G)$ is the minimal number of a set of generators of the 2-Sylowgroup of G).

Fact III. Let p be a prime divisor of n. Then $\sqrt{(-1)^{(p-1)/2}p} \in K_n$. If n is even, then $\sqrt{p} \in K_n^+$. If $8 \mid n$, then $\sqrt{5} \in K_n^+$.

Fact IV. We further use Proposition 8. Let $K/\mathbb{Q}$ be a cyclic extension of degree 4. Then the local Hasse-invariant $H_p\langle K\rangle$ is trivial for primes $p \equiv 1 \bmod 4$ and for odd primes p that are unramified in $K/\mathbb{Q}$.

Let $K_n^+(2)$ be the maximal 2-extension inside K_n^+. Let $m := \varphi(n)/2 = 2^e m_0$ with m_0 odd.

Case 1. $n = 2^l \ge 2$. Then $\langle K_2^+\rangle \simeq \langle K_4^+\rangle \simeq \langle 1\rangle$. Let $l \ge 3$. Then G_n^+ has a cyclic 2-Sylowgroup. Since $K_n^+(2)$ is contained in the cyclic extension $K_{2n}^+(2)$ and $[K_{2n}^+(2) : K_n^+(2)] = 2$, we can apply Corollary 4. By Fact III we get

$$\langle K_n^+\rangle \simeq \langle 2, 10\rangle \perp (m-2) \times \langle 1\rangle.$$

Case 2. $n = 4p^r$, $r \ge 1$, $p \ne 2$. Then $\mathrm{rk}_2(G_n^+) = 1$ and $\mathrm{dis}(K_n^+/\mathbb{Q}) = p$ by Fact III. If $p \equiv 3 \bmod 4$, then $[K_n^+ : \mathbb{Q}] \equiv 2 \bmod 4$. Now apply Proposition 18. If $p \equiv 1 \bmod 8$ apply Corollary 3. Now consider $p \equiv 5 \bmod 8$. Only the primes 2 and p are ramified in K_n (see [16, IV, Section 1, Theorem 1]). By Fact IV all local Hasse-invariants at odd primes are trivial. Now Hilbert reciprocity gives

$$\langle K_n^+\rangle \simeq \langle p\rangle \perp (m-1) \times \langle 1\rangle.$$

Case 3 *and* 4. $n = 2^l p^r$, $l \ge 3$, $p \ne 2$, or $n = 4p^r q^s$ with p, q odd and $r, s \ge 1$. Then $\mathrm{rk}_2(G_n^+) = 2$. Hence, $\mathrm{dis}(K_n^+/\mathbb{Q}) = 1$. Now (III) gives $\sqrt{5}$, $\sqrt{p} \in K_n^+$ (resp. $\sqrt{p}$, $\sqrt{q} \in K_n^+$). Now apply Proposition 6.

Case 5. Then Facts I, II and Proposition 4 give

$$\langle K_n^+\rangle \simeq m \times \langle 1\rangle.$$

Case 6. Then $\mathrm{dis}(K_n^+/\mathbb{Q}) = 1$, since $\mathrm{rk}_2(G_n^+) = 2$. Let $p_1 \not\equiv p_2 \equiv 3 \bmod 4$. We get $\sqrt{p_1}$, $\sqrt{p_2 p_3} \in K_n^+$ by (III). Proposition 6 gives $w_2\langle K_n^+\rangle =$

$(p_1, p_2 p_3) \in \mathrm{Br}(\mathbb{Q})$. Extending this approach we get

$$w_2\langle K_n^+\rangle = \frac{p_1-1}{2}(p_2,p_3) + \frac{p_2-1}{2}(p_1,p_3) + \frac{p_3-1}{2}(p_1,p_2) + \frac{p_1-1}{2}\frac{p_2-1}{2}\frac{p_3-1}{2}(p_1p_2p_3,-1) \in \mathrm{Br}(\mathbb{Q}).$$

Case 7. If $p \equiv q \equiv 1 \bmod 4$, then $\mathrm{rk}_2(G_n^+) = 2$ and $\sqrt{p}, \sqrt{q} \in K_n^+$ by Facts I–III. We get $w_2\langle K_n^+\rangle = (p,q)$ by Proposition 6. Let $p \equiv q \equiv 3 \bmod 4$. Then $\sqrt{pq} \in K_n^+$ and $\mathrm{ord}(G_n^+) \equiv 2 \bmod 4$. Now apply Proposition 18. Next consider $p \not\equiv q \equiv 1 \bmod 4$. Then $\mathrm{rk}_2(G_n^+) = 1$ and $\sqrt{q} \in K_n^+$. If $q \equiv 1 \bmod 8$, then

$$\langle K_n^+\rangle \simeq \langle 2, 2q\rangle \perp (m-2) \times \langle 1\rangle$$

by Corollary 4. Let $q \equiv 5 \bmod 8$. $K_n^+(2)/\mathbb{Q}$ is a cyclic extension of degree 4 and $\mathbb{Q}(\sqrt{q})$ is its unique nontrivial subfield. Then p and q are the only ramified primes in $K_n^+(2)/\mathbb{Q}$. We get $H_l\langle K_n^+\rangle = 1$ if $l \neq 2, p$ by (IV). Since $q \equiv 5 \bmod 8$, the prime 2 does not split in the quadratic extension $K_n^+(2)/\mathbb{Q}$. Further, 2 is unramified. Thus Proposition 4(2)(c) of [6] gives $H_2\langle K_n^+\rangle = -1 = H_p\langle K_n^+\rangle$ by Hilbert reciprocity.

Case 8. If $p \equiv 3 \bmod 4$ then m is odd. If $p \equiv 1 \bmod 4$ then $K_n^+/\mathbb{Q}$ is contained in the cyclic extension $K_n/\mathbb{Q}$ of degree $2[K_n^+ : \mathbb{Q}]$. Now use Corollary 4. ∎

REFERENCES

1. A. A. Albert, "Modern Higher Algebra," University Press, Chicago, 1937.
2. J. Kr. Arason, Cohomologische Invarianten quadratischer Formen, *J. Algebra* **36** (1975), 448–491.
3. E. Bayer-Fluckiger and J. P. Serre, Torsions quadratiques et bases normales autoduales, *Amer. J. Math.* **116** (1994), 1–64.
4. P. E. Conner and R. Perlis, A Survey of Trace Forms of Algebraic Number Fields, World Scientific, Singapore, 1984.
5. C. Drees, Spurformen von Körpererweiterungen kleinen Grades, Diplomarbeit, Westfälische Wilhelms-Universität Münster, 1994.
6. M. Epkenhans, Trace forms of normal extensions of algebraic number fields, *Linear and Multilinear Algebra* **25** (1989), 309–320.
7. M. Epkenhans, Trace forms of trinomials, *J. Algebra* **155** (1993), 211–220.
8. M. Epkenhans and M. Krüskemper, On Trace Forms of étale Algebras and Field Extensions, *Math. Z.* **217** (1994), 421–434.
9. A. Fröhlich, Orthogonal representation of Galois groups, Stiefel–Whitney classes and Hasse–Witt invariants, *J. Reine Angew. Math.* **360** (1984), 84–123.
10. V. P. Gallagher, Local Trace Forms, *Lin. Multilin. Alg.* **7** (1979), 167–174.

11. D. Gorenstein, Finite Groups, Harper and Row, New York, 1968.
12. H. G. Grundman, T. L. Smith, and J. R. Swallow, Groups of Order 16 as Galois Groups, *Exposition. Math.* **13** (1995), 289–319.
13. B. Huppert, "Endliche Gruppen I," Grundlagen Math. Wiss. Springer-Verlag, Berlin/Heidelberg/New York, 1967.
14. I. Kiming, Explicit classifications of some 2-extensions of a field of characteristic different from 2, *Canad. J. Math.* **42** (1990), 825–855.
15. M. Krüskemper, The quadratic form transfer, *Schriftenr. Math. Inst. Univ. Münster*, 15, 1995. 3. Serie.
16. S. Lang, Algebraic Number Theory, Addison–Wesley, Reading, MA, 1970.
17. J. Mináč and T. Smith, A characterization of C-fields via Galois groups, *J. Algebra* **137** (1991), 1–11.
18. W. Scharlau, "Quadratic and Hermitian Forms," Grundlehren der mathematischen Wissenschaften, Springer-Verlag, Berlin, Heidelberg, New York, Tokyo, 1985.
19. C. Scheiderer, Spaces of orderings of fields under finite extensions, *Manuscripta Math.* **72** (1991), 27–47.
20. J. P. Serre, L'invariant de Witt de la forme $Tr(x^2)$, *Comment. Math. Helv.* **59** (1984), 651–676.
21. A. D. Thomas and G. V. Wood, Group Tables, Shiva Publishing Limited, 1980.
22. E. Witt, Konstruktion von galoisschen Körpern der Charakteristik p zu vorgegebener Gruppe der Ordnung p^f. *J. Reine Angew. Math.* **174** (1936), 237–245.