TRACE FORMS OF GALOIS FIELD EXTENSIONS IN THE PRESENCE OF ROOTS OF UNITY

D.-S. KANG AND Z. REICHSTEIN

Abstract. Let L/K be a Galois field extension and let G_2 be a Sylow subgroup of $\mathrm{Gal}(L/K)$. We show that if G_2 is not abelian then the trace form of L/K is hyperbolic, provided that K contains certain roots of unity.

Contents

1. Introduction

The trace form of a finite field extension (or, more generally of an etale algebra) L/K is the nonsingular quadratic form $q_{L/K}: x \mapsto \mathrm{tr}_{L/K}(x^2)$ defined over K. Trace forms have been much studied in recent years; for a survey and an extensive bibliography on the subject we refer the reader to [1].

Of special interest to us will be trace forms of Galois extensions L/K. Classifying such forms for a given $G = \mathrm{Gal}(L/K)$ (and without any further restrictions on K) is a rather delicate problem; in particular, the answer is not even known in the case where G is the cyclic group of order 16 (see [4, p. 222]). Much of the work in this area has been done in the case where K is a number field; for a survey of these results see [3] or [1, Section 6.3].

1991 *Mathematics Subject Classification.* 11E81, 12F05.
Key words and phrases. Trace forms, quadratic forms, Witt rings, Pfister forms.
Z. Reichstein was partially supported by NSF grant DMS-9801675.

In this paper we show that the situation simplifies considerably if we require K to contain certain roots of unity. Our main result is the following:

Theorem 1.1. *Let L/K be a G-Galois extension and let G_2 be a Sylow 2-subgroup of G. Assume*

(a) G_2 is not abelian, and

(b) K contains a primitive eth root of unity, where e is the minimal value of the exponent of H, as H ranges over all non-abelian subgroups of G_2.

Then the trace form $q_{L/K}$ is hyperbolic over K.

Before we proceed with the proof several remarks are in order. First of all, Theorem 1.1 may be viewed as a generalization of [4, Corollary 6, p. 227], where the same assertion is proved for $|G_2| \leq 16$.

Secondly, the theorem remains valid if we assume that L/K is a G-Galois algebra (as defined, e.g., in [2, 1.3]) and not just a field extension; see Proposition 2.5.

Thirdly, if G_2 is an abelian group of rank r and exponent e, and K contains a primitive eth root of unity then it is well-known that $q_{L/K}$ is an r-fold Pfister form over K and that this form is not always hyperbolic; see Remark 3.2 and [4, Corollary 2, p. 212].

Finally, condition (b) of the theorem cannot be substantially weakened in the following sense: for every $n = 2^i \geq 4$ there exists a non-abelian group G of order $2n$ and exponent n, and a G-Galois extension L/K such that (i) K contains a primitive root of unity of degree $n/2$ but not one of degree n and (ii) $q_{L/K}$ is not hyperbolic; see Example 6.1.

Acknowledgements

We would like to thank J.-P. Serre for supplying Example 6.1, bringing Lemma 4.5 to our attention and sending us a list of corrections to an earlier draft of this paper. We are also grateful to E. Bayer-Fluckiger, B. Fein, and B. Kahn for helpful comments.

The first author is currently a graduate student at Oregon State University. He would like to thank the OSU Mathematics Department for financial support.

2. Notation and preliminaries

The following notational conventions will be used throughout the paper.

G	finite group
G_2	Sylow 2-subgroup of G
L/K	finite field extension
$q_{L/K}$	trace form $x \mapsto \mathrm{tr}_{L/K}(x^2)$
$q^a_{L/K}$	scaled trace form $x \mapsto \mathrm{tr}_{L/K}(ax^2)$
ζ_d	primitive dth root of unity
$W(K)$	the Witt ring of K
$<<a_1, \dots, a_r>>$	the r-fold Pfister form $<1, a_1> \otimes \cdots \otimes <1, a_r>$

In the remainder of this section we present several background results on trace forms. We record them in the form suitable for subsequent use and outline the proofs.

Subextensions. Let L/K be a field extension and let $a \in L^*$. We shall denote the scaled trace form $x \mapsto \mathrm{tr}(ax^2)$ by $q^a_{L/K}$. In particular, $q^1_{L/K} = q_{L/K}$ is the usual trace form of L/K.

Lemma 2.1. *Let L/K and K/F be finite field extensions. Suppose $q_{L/K} = \langle a_1, \dots, a_n \rangle$. Then*

(a) $q_{L/F} = q^{a_1}_{K/F} \oplus \cdots \oplus q^{a_n}_{K/F}$.

(b) If every a_i lies in F then $q_{L/F} = \langle a_1, \dots, a_n \rangle \otimes q_{K/F}$.

(c) If $q_{L/K}$ is hyperbolic over K then $q_{L/F}$ is hyperbolic over F.

Proof. (a) Suppose $q_{L/K} = \langle a_1, \dots, a_n \rangle$ in the K-basis $v_1, \dots, v_n$ of L. Then $L = Kv_1 \oplus \cdots \oplus Kv_n$ as an F-vector space. One easily checks that $Kv_i \perp Kv_j$ with respect to $q_{L/F}$ for any $i \neq j$. Moreover, $q_{L/F} = q^{a_i}_{K/F}$ on Kv_i, and part (a) follows.

(b) If $a_i \in F$ then $q^{a_i}_{K/F} = \langle a_i \rangle \otimes q_{K/F}$. The desired equality is now an immediate consequence of part (a).

(c) Follows from (b), since $0 \otimes q_{K/F} = 0$ in $W(F)$. □

Cyclic extensions.

Lemma 2.2. *Let K be a field containing a primitive nth root of unity and suppose $L = K(\sqrt[n]{a})$ is a cyclic extension of K of degree n for some $a \in K^*$. Then $q_{L/K} = \langle n, na \rangle$ in $W(K)$.*

Proof. Set $x = \sqrt[n]{a}$. An easy computation in the basis $1, x, \dots, x^{n-1}$ shows that $q_{L/K} = \langle n, na \rangle$ on $\mathrm{Span}_K\{1, x^{n/2}\}$ and is hyperbolic on $\mathrm{Span}_K\{x^i, x^{n-i}\}$ for every $i = 1, \dots, \frac{n}{2} - 1$. Thus $q_{L/K} = \langle n, na \rangle$ in $W(K)$, as claimed. □

Lemma 2.3. *Let $L = K(\sqrt{b})$ be a quadratic field extension for some $b \in K$ and let $a \in L^*$.*

(a) If $\mathrm{tr}(a) = 0$ then $q^a_{L/K}$ is hyperbolic over K.

(b) If $\mathrm{tr}(a) \neq 0$ then $q^a_{L/K} = \langle \mathrm{tr}(a) \rangle \otimes \langle 1, n(a)b \rangle$.

Here $\mathrm{tr}(a)$ and $n(a)$ denote the trace and the norm of a in L/K.

Proof. (a) Note that $q^a_{L/K}(1) = \mathrm{tr}(a) = 0$. Part (a) now follows from the fact that a 2-dimensional non-singular form is hyperbolic iff it is isotropic; see, e.g., [6, Theorem I.3.2].

(b) Let $c = \sqrt{b}$, i.e., $c \in L$ such that $c^2 = b$. The non-trivial element $^-$ of $\mathrm{Gal}(L/K) \simeq \mathbb{Z}/2\mathbb{Z}$ is given by $\overline{x + yc} = x - yc$ for any $x, y \in K$.

Recall that any non-singular 2-dimensional quadratic form q can be written as $q = <v> \otimes <1, \det(q)>$, where $v \in K^*$ is a value assumed by q; see, e.g., [6, Proposition I.5.1]. Since $q^a_{L/K}(1) = \mathrm{tr}(a)$, we can take $v = \mathrm{tr}(a)$.

The Gram matrix of $q^a_{L/K}$ in the basis $\{1, c\}$ is

$$\begin{pmatrix} a + \overline{a} & ac + \overline{ac} \\ ac + \overline{ac} & b(a + \overline{a}) \end{pmatrix} .$$

Computing the determinant of this matrix, we find that $\det(q) = 4ba\overline{a} = 4b\,n(a)$ in $(K)^*/(K^*)^2$, and the lemma follows. □

Linear representations.

Lemma 2.4. *Let V and V' be faithful linear representations of a finite group G over a field k and let $L = k(V)$, $K = L^G$, $L' = k(V')$ and $K' = L'^G$. If $q_{L/K}$ is hyperbolic then so is $q_{L'/K'}$.*

Proof. Let $n = \dim_k(V)$, $n' = \dim_k(V')$ and let $s_1, \dots, s_n, t_1, \dots, t_{n'}$ be independent variables. By the no-name lemma (see, e.g., [11, Appendix 3]), $L(t) \simeq L'(s)$ as G-fields, where G acts trivially on the variables $s = (s_1, \dots, s_n)$ and $t = (t_1, \dots, t_{n'})$. Thus $q_{L(t)/K(t)} = q_{L'(s)/K'(s)}$ is hyperbolic over $K(t) = K'(s)$. The desired result now follows from the fact that the natural map $W(K') \longrightarrow W(K'(s))$ is injective; see [6, Lemma IX.1.1]. □

Proposition 2.5. *Let V be a finite-dimensional faithful linear representation of a finite group G over a field k, If $q_{k(V)/k(V)^G}$ is hyperbolic then so is $q_{L/K}$, for any G-Galois algebra (and, in particular, any G-Galois field extension) L/K, where K contains k.*

Proof. By Lemma 2.4, we may assume that $V \simeq k[G]$ is the regular representation of G. Let $t = (t_1, \dots, t_n)$ be an n-tuple of independent variables, where $n = |G|$. By [8, Theorem 4.2] there exists an element $a \in L(t)$ whose n conjugates $g(a)$ are algebraically independent over k. Then $F = k(g(a) \,|\, g \in G)$ is isomorphic to $k(V)$ as a G-field. Thus $q_{F/F^G} = q_{k(V)/k(V)^G}$ is hyperbolic over F^G and hence, $q_{L(t)/K(t)}$ is hyperbolic over $K(t)$. This implies that $q_{L/K}$ is hyperbolic over K (cf. [6, Lemma IX.1.1]), as claimed. □

3. Property (*)

Definition 3.1. Let G be a 2-group of exponent d. We shall say that G has property (*) if for every G-Galois extension L/K such that K contains a primitive dth root of unity, the trace form $q_{L/K}$ is hyperbolic.

Remark 3.2. No abelian 2-group G has property $(*)$. Indeed, let $G = \mathbb{Z}/n_1\mathbb{Z} \times \cdots \times \mathbb{Z}/n_r\mathbb{Z}$ be an abelian 2-group, $K = \mathbb{C}(a_1, \dots, a_r)$ and $L = \mathbb{C}(\sqrt[n_1]{a_1}, \dots, \sqrt[n_r]{a_r})$, where $\mathbb{C}$ is the field of complex numbers and $a_1, \dots, a_r$ are algebraically independent variables over $\mathbb{C}$. Then an easy induction argument on r, using Lemmas 2.2 and Lemma 2.1(b), shows that

$q_{L/K} = <|G|> \otimes <<a_1, \ldots, a_r>>$. This form is anisotropic (and, hence, not hyperbolic) over K; see [7, Example 8.1.2(6)].

Reduction 3.3. In order to prove Theorem 1.1 it is sufficient to show that every non-abelian 2-group G has property (*).

Proof. Indeed, let G, e and L/K be as in Theorem 1.1, and let H be a non-abelian subgroup of G_2 of exponent e. Consider the intermediate extension $K \subset L^H \subset L$. Since K (and thus L^H) contains a primitive eth root of unity, and we are assuming H has property (*), q_{L/L^H} is hyperbolic. Now, by Lemma 2.1(c) $q_{L/K}$ is hyperbolic as well. $\square$

In view of Reduction 3.3, the goal of the rest of this paper will be to prove the following.

Theorem 3.4. *Every non-abelian 2-group G has property (*) (see Definition 3.1).*

We begin by showing that property (*) is inherited from subgroups and from certain quotients.

Proposition 3.5. *Let G be a 2-group and let H be a subgroup of G.*

(a) If H has property (*) then so does G.

(b) Suppose $H = <r>$ is cyclic. Assume a proper subgroup H_0 of H is normal in G. If G/H_0 has property (*) then so does G.

Proof. Let d be the exponent of G and let L/K is a G-Galois extension, and $\zeta_d \in K$. We want to show that $q_{L/K} = 0$ in $W(K)$.

(a) Consider the intermediate extension $K \subset L^H \subset L$. Since the exponent of H is $\leq d$ and $\zeta_d \in K \subset L^H$, our assumption on H implies that q_{L/L^H} is hyperbolic over L^H. Now Lemma 2.1(c) tells us that $q_{L/K}$ is hyperbolic over K, as desired.

(b) Suppose $H = <r>$ is of order n and $H_0 = <r^{n/m}>$ is of order m, where m and n are powers of 2. Since $H_0 \neq H$, we may assume $n > m$. We may also assume without loss of generality that $H_0 \neq \{1\}$, i.e., $m \geq 2$.

Consider the tower of extensions $K \subset L^H \subset L^{H_0} \subset L$. By our assumption, $\zeta_n \in K$; hence, we can write $L = L^H(\sqrt[n]{a})$ for some $a \in L^H$. Then $L^{H_0} = L^H(\sqrt[m]{a})$, and thus by Lemma 2.2, $q_{L/L^H} = <n, na>$ and $q_{L^{H_0}/L^H} = <m, ma>$ in $W(L^H)$. In other words,

$$q_{L/L^H} = <n, na> \oplus \frac{n-2}{2} <1, -1>$$

and

$$q_{L^{H_0}/L^H} = <m, ma> \oplus \frac{m-2}{2} <1, -1> .$$

By Lemma 2.1(d),

$$q_{L/K} = q^n_{L^H/K} \oplus q^{na}_{L^H/K} \oplus \frac{n-2}{2}(q_{L^H/K} \oplus q^{-1}_{L^H/K}) .$$

Since $q_{L^H/K} \oplus q^{-1}_{L^H/K} = <1,-1> \otimes q_{L^H/K} = 0$ in $W(K)$, we conclude that

$$q_{L/K} = <n> \otimes (q_{L^H/K} \oplus q^a_{L^H/K}) \text{ in } W(K).$$

Similarly,

$$q_{L^{H_0}/K} = <m> \otimes (q_{L^H/K} \oplus q^a_{L^H/K}) \text{ in } W(K).$$

Since the exponent of G/H_0 is $\leq d$, and G/H_0 has property (*), we know that $q_{L^{H_0}/K} = 0$ in $W(K)$. Then $q_{L/K} = <\frac{n}{m}> \otimes q_{L^{H_0}/K} = 0$ as well, thus proving (b). □

4. Barely non-abelian groups

Definition 4.1. We shall call a finite group G *barely non-abelian* if satisfies the following conditions:

(a) G is not abelian,

(b) every proper subgroup of G is abelian,

(c) if H is a cyclic subgroup, H_0 is a non-trivial proper subgroup of H, and H_0 is normal in G then G/H_0 is abelian.

Remark 4.2. In view of Proposition 3.5, a counterexample to Theorem 3.4 of minimal order is a barely non-abelian 2-group. Our strategy in proving Theorem 3.4 will thus be to

(i) obtain a complete list of barely non-abelian 2-groups,

(ii) prove property (*) for each group on this list.

In this section we will carry out step (i).

Example 4.3. Q_8 and D_8 are barely non-abelian, since all of their proper subgroups and quotients have order ≤ 4.

We will now introduce a more sophisticated example. Let $n \geq 4$ be a power of 2 and let

$$M(2n) = \{r, s \mid r^n = s^2 = 1, sr = r^{n/2+1}s\}. \tag{4.1}$$

It is easy to see that $M(2n)$ is isomorphic to the semidirect product of $\mathbb{Z}/n\mathbb{Z}$ and $\mathbb{Z}/2\mathbb{Z}$, where the nontrivial element of $\mathbb{Z}/2\mathbb{Z}$ acts on $\mathbb{Z}/n\mathbb{Z}$ by sending 1 to $\frac{n}{2}+1$. Note that $M(8)$ is the dihedral group D_8.

Lemma 4.4. *(a) Every proper subgroup of $M(2n)$ is abelian.*

(b) Every proper quotient of $M(2n)$ is abelian.

(c) $M(2n)$ is barely non-abelian for any $n \geq 4$.

Proof. (a) Let S be a proper subgroup of $M(2n)$. If S contains the index 2 subgroup $<r>$ then $S = <r>$ and thus S is abelian. If not, set $S_0 = S \cap <r>$. Then, on the one hand, $S_0 \subset <r^2>$, is central in $M(2n)$ and, on the other hand, $S/S_0 \subset M(2n)/<r> \simeq \mathbb{Z}/2\mathbb{Z}$ is cyclic. This proves that S is abelian (see, e.g., [10, 3.2.8]).

(b) Assume the contrary: $M(2n)/N$ is not abelian for some non-trivial normal subgroup N of $M(2n)$. Then N cannot contain $r^{n/2}$; otherwise r and s will commute in the quotient. Consequently,

$$N \cap {<}r{>} = \{1\}\,. \tag{4.2}$$

Since ${<}r{>}$ has index 2 in $M(2n)$, (4.2) implies $|N| = 2$. Moreover, N and ${<}r{>}$ are complementary normal subgroups in $M(2n)$. Consequently, $M(2n) \simeq N \times {<}r{>}$ is abelian, a contradiction.

(c) Immediate from (a) and (b). □

We now proceed to give a complete list of barely non-abelian 2-groups. Our starting point is the following classification, due to Rédei, of 2-groups satisfying conditions (a) and (b) of Definition 4.1 (but not necessarily condition (c)).

Lemma 4.5. *(Rédei [9], see also [5, p. 309]) Let G be a finite non-abelian 2-group all of whose proper subgroups are abelian. Then G is isomorphic to one of the following groups:*

(i) The quaternion group Q_8 of order 8.

(ii) $A(n,m) = {<}r,s \,|\, r^n = s^m = 1\,, sr = r^{\frac{n}{2}+1}s{>}$ of order mn. Here $n \geq 4$ and $m \geq 2$ are powers of 2.

(iii) $B(n,m) = {<}r,s \,|\, r^n = s^m = t^2 = 1\,, sr = trs{>}$ of order $2mn$. Here $n,m \geq 2$ are powers of 2. □

We are now ready to prove the main result of this section.

Proposition 4.6. *A 2-group G is barely non-abelian if and only if G is isomorphic to the quaternion group Q_8 or to $M(2n)$, where $n \geq 4$ is a power of 2.*

Proof. The groups Q_8 and $M(2n)$ are barely non-abelian; see Example 4.3 and Lemma 4.4(c).

To prove the converse, suppose G is barely non-abelian. Then G is isomorphic to one of the groups listed in Lemma 4.5. Observe that $A(n,2) = M(2n)$ and $B(2,2) = D_8 = M(8)$. (Indeed, D_8 is the only non-abelian group of order 8 that has at least 3 elements of order 2.) It remains to show that $A(n,m)$ and $B(n,m)$ are not barely non-abelian for all other values of n and m.

First assume $m \geq 4$ and consider the group $A(n,m)$. Since $|A(n,m)| = mn$, the elements r^is^j are all distinct for $i = 0,1,\ldots,m-1$ and $j = 0,1,\ldots,n-1$. (This is also easy to see directly by identifying $A(n,m)$ with a semidirect product of $\mathbb{Z}/n\mathbb{Z}$ and $\mathbb{Z}/m\mathbb{Z}$.) Let $H = {<}s{>} \subset A(n,m)$ and $H_0 = {<}s^2{>}$. Then H_0 is central (and, hence, normal) in $A(n,m)$. Since $r^{n/2+1} \notin H_0$, we conclude that r and s do not commute in $A(n,m)/H_0$. This shows that $A(n,m)$ does not satisfy condition (c) of Definition 4.1 for any $m \geq 4$.

A similar argument shows that $B(m,n)$ is not barely non-abelian for $(n,m) \neq (2,2)$. Indeed, since $|B| = 2mn$, the elements $t^i r^j s^k$ are all distinct for $i = 0,1$, $j = 0,1,\dots,n-1$ and $k = 0,1,\dots,m-1$. If $n \geq 4$, let $H = <r>$ and $H_0 = <r^2>$. Then the same argument as above shows that H_0 is central and $B(m,n)/H_0$ is not abelian. Similarly if $m \geq 4$, then $B(m,n)/H_0$ is not abelian for $H = <s>$ and $H_0 = <s^2>$. $\square$

5. Proof of Theorem 1.1

By Reduction 3.3 it is sufficient to prove Theorem 3.4. We now follow the strategy outlined in Remark 4.2. We have shown that if G is a minimal counterexample to Theorem 3.4 then $G \simeq Q_8$ or $M(2n)$ for some $n \geq 4$. It remains to prove that these groups have property (*). For $G = Q_8$ and $G = M(8) \simeq D_8$ this is known; see, e.g., [2, Section 6, Exemple] or [4, Corollary 6, p. 227]. Thus it remains to prove the following:

Proposition 5.1. *Let $n \geq 8$ be a power of 2 and $G = M(2n)$. Suppose L/K be an G-Galois extension, where K contains a primitive nth root of unity ζ. Then the trace form $q_{L/K}$ is hyperbolic.*

Proof. Let k be the field generated by the prime subfield of K and ζ and let V be the 2-dimensional k-representation of $M(2n)$ given by

$$\begin{aligned} r &\colon (x,y) \longrightarrow (\zeta x, \zeta^{\frac{n}{2}+1} y) \text{ and} \\ s &\colon (x,y) \longrightarrow (y,x)\,. \end{aligned}$$

By Proposition 2.5 we may assume without loss of generality that $L = k(V)$ and $K = k(V)^{M(2n)}$. Since $n \geq 8$, k contains primitive 8th root of unity; hence,

$$\sqrt{2}, \sqrt{-2} \in K\,. \tag{5.1}$$

Note that $a = x^n$ lies in $L^{<r>}$, and

$$\begin{aligned} A &= x^n + y^n\,, \\ B &= (x^n - y^n)^2\,, \\ C &= x^{\frac{n}{2}} y^{\frac{n}{2}}\,, \\ D &= x^{\frac{n}{4}} y^{\frac{n}{4}} (\tfrac{x}{y} + \tfrac{y}{x})\,, \\ E_m &= (\tfrac{x}{y})^m + (\tfrac{y}{x})^m \quad (m \text{ even}) \end{aligned} \tag{5.2}$$

lie in $L^{<r,s>} = L^{M(2n)} = K$. Since $L = L^{<r>}(x) = L^{<r>}(\sqrt[n]{a})$, Lemma 2.2 tells us that

$$q_{L/L^{<r>}} = <n> \otimes <1,a> = <1,a>\,,$$

where the last equality follows from (5.1). Thus by Lemma 2.1(a)

$$q_{L/K} = q_{L^{<r>}/K} \oplus q^a_{L^{<r>}/K}\,. \tag{5.3}$$

Note that $[L^{<r>} : K] = [M(2n) : <r>] = 2$; moreover, $q_{L^{<r>}/K} = K(x^n - y^n) = K(\sqrt{B})$. Thus Lemma 2.3 tells us that

$$q_{L^{<r>}/K} = <2> \otimes <1,B> = <1,B>\,,$$

where once again, the factor of 2 can be dropped because of (5.1), and

$$q^a_{L^{<r>}/K} = <\mathrm{tr}_{L^{<r>}/K}(a)> \otimes <1, n_{L^{<r>}/K}(a)B>\,.$$

Since $\mathrm{tr}_{L^{<r>}/K}(a) = x^n + y^n = A$ and $n_{L^{<r>}/K}(a) = x^n y^n = C^2$ is a complete square in K, (5.3) can be rewritten as

$$q_{L/K} = <1, B> \oplus <A, AB> = <<A, B>>\,.$$

It remains to show that $<<A, B>>$ is hyperbolic over K. We shall need the following simple relations among the elements of K defined in (5.2).

Lemma 5.2. *If $m \geq 2$ a power of 2 then $E_m^2 - 4 \equiv E_2^2 - 4 \pmod{(K^*)^2}$.*

Proof. Induction on m, starting from $m = 2$. The induction step is given by $E_m^2 - 4 = (E_{m/2}^2 - 2)^2 = E_{m/2}^2(E_{m/2}^2 - 4)$. □

Now $A = CE_{n/2} = C(E_{n/4}^2 - 2)$ and $B = C^2(E_{n/2}^2 - 4)$. By Lemma 5.2,

$$q = <<A, B>> = <<C(E_{n/4}^2 - 2), E_{n/4}^2 - 4>> = <<C, E_{n/4}^2 - 4>>\,,$$

where we removed the factor of $E_{n/4}^2 - 2$ in the first position because it is of the form $(E_{n/4}^2 - 4)v^2 + w^2$, with $v = 1$ and $w = \sqrt{2}$; cf. [6, Proposition X.1.3(1)]. (Note that we are using the assumption that $n \geq 8$ here, so that $n/4$ is even and thus $E_{n/4}$ lies in K.)

Using Lemma 5.2 again, $q = <<C, E_2^2 - 4>>$. Finally, $E_2^2 - 4 = (D/C)^2(D^2 - 4C^2)$ so that $q = <<C, D^2 - 4C>> = <<C, 1>>$, where we removed a the factor of $D^2 - 4C$ in the second position because it is of the form $Cv^2 + w^2$, where $v = \sqrt{-2}$ and and $w = D$. The form $<<C, 1>>$ is clearly hyperbolic over K. This completes the proof of Proposition 5.1, and thus of Theorem 1.1. □

6. An example

We conclude this paper with an example, communicated to us by J.-P. Serre, showing that for $G = M(2n)$ condition (b) of Theorem 1.1 cannot be relaxed.

Example 6.1. Let $n \geq 4$ be a power of 2. Suppose that a field k contains a primitive root of unity $\zeta_{n/2}$ of degree $n/2$ but does not contain a primitive root of unity ζ_n of degree n. Set $k' = k(\zeta_n)$, $L = k'((t))$ and $K = k((a))$, where $a = t^n$. Then

(a) L/K is an $M(2n)$-Galois extension,
(b) $q_{L/K} = <2n> \otimes <<\zeta_{n/2}, a>>$, and
(c) $q_{L/K}$ is anisotropic (and hence, not hyperbolic) over K.

Proof. (a) Let $r, s \in \mathrm{Gal}(L/K)$ be given by

$$r\colon \begin{array}{ccc} t & \mapsto & \zeta_n t \\ \zeta_n & \mapsto & \zeta_n \end{array} \quad \text{and} \quad s\colon \begin{array}{ccc} t & \mapsto & t \\ \zeta_n & \mapsto & -\zeta_n \end{array}\,.$$

It is easy to see that $r^n = s^2 = 1$ and $sr = r^{n/2+1}s$ in $\mathrm{Gal}(L/K)$. Thus we have a homomorphism $f\colon M(2n) \longrightarrow \mathrm{Gal}(L/K)$; cf. (4.1). By Lemma 4.4(b), f is injective. Since $\mathrm{Gal}(L/K) \leq [L:K] = 2n = M(2n)$, f is an isomorphism. This proves (a).

(b) Note that $L^{<r>} = k'((a))$. Since $L = L^{<r>}(\sqrt[n]{a})$ and $L^{<r>}(\sqrt{\zeta_{n/2}})$, Lemma 2.2 tells us that

$$q_{L/k'((a))} = <n> \otimes <1, a>\,,$$

and

$$q_{k'((a))/K} = <2, 2\zeta_{n/2}>\,,$$

The desired formula now follows from Lemma 2.1(b).

(c) Since $\zeta_{n/2}$ is not a square in k, i.e., $<1, \zeta_{n/2}>$ is anisotropic over k, the desired conclusion follows from [6, Proposition VI.1.9]. $\square$

References

[1] E. Bayer-Fluckiger, *Galois cohomology and the trace form*, Jahresber. Deutch. Math.-Verein. **96** (1994), no. 2, 35–55.

[2] E. Bayer-Fluckiger, J.-P. Serre, *Torsions quadratiques et bases normales autoduales*, Americal J. Math. **116** (1994), 1–64.

[3] P.E. Conner, R. Perlis, A Survey of Trace Forms of Algebraic Number Fields, World Scientific, Singapore, 1998.

[4] C. Drees, M. Epkenhans, M. Krüskemper, *On the computation of the trace form of some Galois extensions*, J. Algebra **192** (1997), 209–234.

[5] B. Hupper, Endliche Gruppen I, Springer-Verlag, 1967.

[6] T. Y. Lam, The Algebraic Theory of Quadratic Forms, W. A. Benjamin, Inc., 1973.

[7] A. Pfister, Quadratic Forms with Applications to Geometry and Topology, Cambridge University Press, 1995.

[8] Z. Reichstein, *On a theorem of Hermite and Joubert*, Canadian J. Math. **51** (1) (1999), 69–95.

[9] L. Rédei, *Das schiefe Produkt in der Gruppentheorie*, Comment. Math. Helvet. **20** (1947), 225–267.

[10] W. R. Scott, Group Theory, Dover Publications, Inc., 1987.

[11] I. R. Shafarevich, Basic Algebraic Geometry, vol. 1, second edition, Springer-Verlag, 1994.

Department of Mathematics, Oregon State University, Corvallis, OR 97331
E-mail address: `zinovy@math.orst.edu`

Department of Mathematics, Oregon State University, Corvallis, OR 97331
E-mail address: `kangdo@math.orst.edu`