AN ABSTRACT OF THE THESIS OF

Dong Seung Kang for the degree of Doctor of Philosophy in Mathematics

presented on June 6, 2002.

Title: Trace Forms and Self-Dual Normal Bases in Galois Field Extensions

Signature redacted for privacy.

Abstract approved: ____________________

Zinovy Reichstein (Hal Parks)

Let G be a finite group, G_2 be a Sylow 2-subgroup of G, and L/K be a G-Galois extension. We study the trace form $q_{L/K}$ of L/K and the question of existence of a self-dual normal basis. Our main results are as follows:

(1) If G_2 is not abelian and K contains certain roots of unity then $q_{L/K}$ is hyperbolic over K.

(2) If G has a subgroup of index 2 then L/K has no orthogonal normal basis for any G-Galois extension L/K.

(3) If G has even order and G_2 is abelian then L/K does not have an orthogonal normal basis, for some G-Galois extension L/K.

We also give an explicit construction of a self-dual normal basis for an odd degree abelian extension L/K, provided K contains certain roots of unity, and study the generalized trace form for an abelian group G.

Trace Forms and Self-Dual Normal Bases in Galois Field Extensions

by

Dong Seung Kang

A THESIS

submitted to

Oregon State University

in partial fulfillment of
the requirements for the
degree of
Doctor of Philosophy

Presented June 6, 2002
Commencement June 2003

Doctor of Philosophy thesis of Dong Seung Kang presented on June 6, 2002

APPROVED:

Signature redacted for privacy.

Major Professor, representing Mathematics

Signature redacted for privacy.

Chair of Department of Mathematics

Signature redacted for privacy.

Dean of Graduate School

I understand that my thesis will become part of the permanent collection of Oregon State University libraries. My signature below authorizes release of my thesis to any reader upon request.

Signature redacted for privacy.

Dong Seung Kang

ACKNOWLEDGMENTS

Many people helped make this thesis possible–please indulge me as I thank them all, and in an order that reflects nothing of my feelings of gratitude

I would first like to thank first and foremost my advisor, Professor Zinovy Reichstein for all his help, support and above all patience. I count myself as being the most fortunate to be able to work with him.

I would like to thank professors, B. Fein, L. Chen, T.A. Schmidt, M. Flahive, Cetin Kaya Koc, and Brian D. Wood for serving my committee members. I am also grateful to J-.P. Serre, E. Bayer-Fluckiger and B. Kahn for helpful comments.

I would also like to thank all of the faculty at Oregon State University(OSU) Mathematics Department and thank the OSU Mathematics Department for financial support.

I am grateful to all of the faculty at Chung-Ang University(CAU) Mathematics Department in the early days of my undergraduate and graduate study(for a Master's degree). I am especially appreciative to professor Geun Bin Im who was my major professor at CAU.

Finally, this thesis might not exist at all without the love and support of my family. I am especially grateful to my parents for their endless love and support. My wife HeeBun Lee made countless sacrifices for her love and support I can never thank her enough. My daughter MyoungJu(Kathy) and my son Kenneth(TaeYoung) made my life much more cheerful and whenever I go to school they give me kisses and say ”GIVE ME FIVE !”

TABLE OF CONTENTS

TABLE OF CONTENTS(Continued)

Trace Forms and Self-Dual Normal Bases in Galois Field Extensions

1. Introduction

Let L be a finite Galois extension of K with Galois group G. Unless otherwise specified, we will assume that K contains a primitive 4th root of unity; in particular, $\mathrm{char}\,(K) \neq 2$. The trace form $q_{L/K} : L \times L \to K$ is the nonsingular quadratic form given by $x \mapsto \mathrm{tr}_{L/K}(x^2)$.

In this thesis we will be concerned with the following two general questions:

Question 1.1. *Given a finite group G, which quadratic forms over K are trace forms of G-Galois extensions L/K?*

Question 1.2. *Which Galois extensions L/K have a self-dual normal basis, i.e., a normal basis $e_1, \dots, e_n$, such that $\mathrm{tr}(e_i e_j) = 1$ if $i = j$ and 0 if $i \neq j$?*

Question 1.1 was studied in the mid-19th century; in particular, Sylvester [30], Jacobi [16], and Hermite [11], [12] independently proved that the number of real roots of a polynomial $p(x) \in \mathbb{R}[x]$ equals the signature of the trace form of the Galois algebra $\mathbb{R}[x]/(p(x))$; cf. [6, Preface] or [3, Section 1]. There has been a resurgence of interest in this topic at the end of the twentieth century, due in part, to an influential paper of Serre [28], relating the trace form to the extension problem in inverse Galois theory. For a survey of this topic and an extensive bibliography, see Bayer-Fluckiger [3]. Much of the work in this area was done in the case where K is a number field; for a survey of these results see [6] or [3, Section 6.3].

In spite of all this activity, Question 1.1, in its full generality remains open: a complete answer is not even known in the case where G is the cyclic group of order 16; see [7, p. 222]. Our main result shows that the situation simplifies considerably if we require K to contain certain roots of unity.

Theorem 1.3. *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.

Note that if G_2 is an abelian group of rank r and exponent e, and K contains a primitive eth root of unity then $q_{L/K}$ is an r-fold Pfister form over K. This this form is not always hyperbolic; see Lemma 3.4 or [7, Corollary 2, p. 212].

A proof of Theorem 1.3 was published in [17]. We reproduce it in Section 4, with only one substantive change. The proof of Proposition 4.7 in [17] relies on an old group-theoretic result of Rédei [23], which is actually a bit stronger than what we need. In Section 4 we give a direct proof of the special case we use (Proposition 4.5). This lengthens the argument a bit but makes it more elementary and self-contained.

An example of Serre [17, Example 6.1] shows that condition (b) of Theorem 1.3 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. We reproduce Serre's example at the end of Section 4.

Question 1.2 originated in computational problems and was initially studied in the case where L and K are finite fields; see [20], [21], [27], [14], and [15] .

My work in this area was motivated by the following result of Bayer-Fluckiger and Lenstra [4, Theorem 6.1].

Theorem 1.4. *If $|G|$ is odd then any G-Galois extension has a self-dual normal basis.*

It is natural to conjecture that the converse is also true, i.e., that for every finite group G of even order, some G-Galois extension L/K does not have a self-dual normal basis. A surprising result of Bayer-Fluckiger and Serre [5] asserts that this conjecture is false for $G = \mathrm{SL}_2(\mathbb{Z}/3\mathbb{Z})$, and more generally, any group having property [5, 9.4.1]. (Here, as usual, we assume that K contains a primitive 4th root of unity.) It is not known what other groups have this property. Our main result relating to Question 1.2 shows that the converse to the Bayer-Lenstra theorem does, indeed, hold for many groups of even order:

Theorem 1.5. *Let G be a finite group of even order.*

(a) If G has a subgroup of index 2 then L/K has no orthogonal normal basis for any G-Galois extension L/K.

(b) If the Sylow 2-subgroup G_2 of G is abelian then L/K does not have an orthogonal normal basis for some G-Galois extension L/K.

Note that Theorem 1.5 rules out "orthogonal" and not just self-dual normal bases. (Elements of an orthogonal basis are mutually orthogonal, but do not necessarily have unit norm with respect to the trace form.) A proof of Theorem 1.5 is given in Section 5. We will also show that $\mathrm{SL}_2(\mathbb{Z}/3\mathbb{Z})$ is the smallest group for which the converse to Theorem 1.4 fails; see Proposition 5.9.

The final section is devoted to the study of the generalized trace form

$$T_a(x) = \sum_{g\in G} a_g \mathrm{tr}_{L/K}(xg(x))\,. \tag{1.1}$$

Here we assume that K contains a copy of an algebraically closed field k, and that $a = (a_g)$ is a $|G|$-tuple of elements of k, chosen so that T_a is nonsingular. If L/K has a self-dual normal basis, it is easy to see that T_a is hyperbolic for every a. I hope that T_a may present an obstruction to the existence of a self-dual normal basis. In practice I do not know a single case where T_a is not isomorphic to the usual trace form for any a. The results of Section 7 should thus be viewed as preliminary; in particular, I will only consider the case where G is abelian.

The rest of this thesis is structured as follows. In Sections 2 and 3 we will review basic facts about quadratic forms and trace forms. Section 4 is devoted to proving Theorem 1.3. In Section 5 we prove Theorem 1.5. In Section 6 we give an explicit construction of a self-dual basis for an odd degree abelian extension L/K, provided K has suitable roots of unity. In Section 7, we will study the generalized trace form (1.1) for an abelian group G.

2. Preliminaries

In this section we will establish the basics to be used throughout in this thesis. Our standard reference is [18, The Algebraic Theory of Quadratic Forms]. Throughout this thesis the characteristic of a field K is not equal to 2.

2.1. **Bilinear and Quadratic Forms.**

Definition 2.1. Let V be a vector space over a field K. A bilinear form on V over K is a map

$$B : V \times V \to K$$

such that

$$\begin{aligned} B(v+v',\, w) &= B(v,\, w) + B(v',\, w),\ B(v,\, w+w') = B(v,\, w) + B(v,\, w'), \\ & B(cv,\, w) = cB(v,\, w) = B(v,\, cw)\,, \end{aligned}$$

for all $v, v', w, w' \in V$ and all $c \in K$. The form B is called symmetric if

$$B(v,\, w) = B(w,\, v)$$

for all $v, w \in V$. The pair $(V,\, B)$ is called a symmetric bilinear space over K.

2.2. **Gram Matrix.**

Let V be a vector space over a field K and let $\mathcal{B} = \{e_1, \cdots, e_n\}$ be a basis of V. For $v,\, w \in V$, we have

$$v = \sum_{i=1}^{n} v_i e_i \ \text{ and } \ w = \sum_{i=1}^{n} w_i e_i\,,$$

where all v_i and w_i are in K. Then

$$B(v,\, w) = B(\sum_{i=1}^{n} v_i e_i,\, \sum_{i=1}^{n} w_i e_i) = \sum_{i,j=1}^{n} v_i w_j B(e_i, e_j)\,.$$

Hence

$$B(v, w) = (v_1, \cdots, v_n)\; G_r\; (w_1, \cdots, w_n)^t\,,$$

where

$$G_r = \begin{pmatrix} B(e_1, e_1) & \cdots & B(e_1, e_n) \\ \vdots & \cdots & \vdots \\ B(e_n, e_1) & \cdots & B(e_n, e_n) \end{pmatrix},$$

and $(w_1, \cdots, w_n)^t$ is the transpose of $(w_1, \cdots, w_n)$. We call the matrix G_r the Gram matrix of B in the basis $\{e_1, \cdots, e_n\}$.

Definition 2.2. Let V be a vector space over a field K. The map $q : V \to K$ is a quadratic form if $q(v) = B(v, v)$, for some symmetric bilinear form B.

Note that B can be recovered from q via

$$B(v, w) = \frac{1}{4}(q(v + w) - q(v - w))\,.$$

Hence we can identify quadratic forms with symmetric bilinear forms. Thus we will call the pair $(V,\, B)$ or $(V,\, q)$ a quadratic space over K.

2.3. **Orthogonal Complement.**

Let $(V,\, B)$ be a quadratic space, and let $W \subset V$ be a subspace. Then

$$W^{\perp} = \{v \in V | B(v, w) = 0 \text{ for all } w \in W\}$$

is called the orthogonal complement of W. In particular, $V^{\perp} = \{v \in V | B(v, v') = 0 \text{ for all } v' \in V\}$ is the orthogonal complement of V.

Note that for each $v \in V$, B defines a linear map from V to V^* by $v \mapsto B(v, \cdot)$, where V^* is the dual space of V . Hence $\operatorname{Ker} B = V^\perp$.

Definition 2.3. Let $(V,\ B)$ be a quadratic space. Then B is called nonsingular on V if $\operatorname{Ker} B = (0)$.

Note that throughout this thesis we will assume quadratic forms are nonsingular.

Definition 2.4. Let (V, B), (V', B') be quadratic spaces. They are isometric, $\simeq$, if there exists a linear isomorphism $\tau : V \longrightarrow V'$ such that

$$B'(\tau(x), \tau(y)) = B(x, y)\,, \text{ for all } x, y \in V\,.$$

Note that $\simeq$ is an equivalence relation.

Definition 2.5. Let (V, q) be a quadratic space over a field K . Then the determinant of q is defined by $\det q = \det G_r$, where G_r is the Gram matrix of q .

Note that if two quadratic forms, q , q' , are equivalent, then $\det q = \det q'$ in $K^*/(K^*)^2$.

2.4. Change of Bases.

Let V be a vector space over a field K and let $C \in GL(V)$ in a basis $\mathcal{B}$ of V . Then $B_C(v, w) = B(vC, wC)$ is another symmetric bilinear form equivalent to $B(v, w)$.

$$B_C(v, w) = B(vC, wC) = v_{\mathcal{B}}C \cdot G_r \cdot (w_{\mathcal{B}}C)^t = v_{\mathcal{B}}(C \cdot G_r \cdot C^t){w_{\mathcal{B}}}^t,$$

where G_r is the Gram matrix of B and $G'_r = C \cdot G_r \cdot C^t$ is the Gram matrix of B_C.

Note that the rank is preserved because C is invertible and

$$\det G'_r = (\det C) \det G_r (\det C^t) = (\det C)^2 \det G_r \,,$$

that is, $\det G'_r = \det G_r$ in $K^*/(K^*)^2$.

2.5. **Orthogonal Sum.**

Let $(V_1, B_1)\,, (V_2, B_2)$ be quadratic spaces. We define (V, B) by $V = V_1 \oplus V_2$ and $B = B_1 \oplus B_2$. Then (V, B) is called the orthogonal sum of (V_1, B_1) and (V_2, B_2) if $B(v_1, v_2) = 0$ for all $v_1 \in V_1$ and $v_2 \in V_2$, and every element of V is uniquely written as $v_1 + v_2$ with $v_1 \in V_1$ and $v_2 \in V_2$.

Theorem 2.6. *Let (V, B) be a quadratic space over a field K of* $\dim V = n$. *Then there exists a basis $\{e_1, \cdots, e_n\}$ of V such that $B(e_i, e_j) = 0$ for $i \neq j$.*

Proof. See [18, Corollary I.2.4]. □

Note that the Gram matrix of B in this basis is diagonal, i.e.,

$$\begin{pmatrix} d_1 & & 0 \\ & \ddots & \\ 0 & & d_n \end{pmatrix},$$

where the $B(e_j, e_j) = d_j \in K^*$. We abbreviate the quadratic form by $\langle d_1, \cdots, d_n \rangle$.

2.6. Hyperbolic Spaces and Pfister Forms.

Definition 2.7. Let $(V,\ q)$ be a quadratic space over a field K, and let $d \in K^*$. We will say that q represents d if there exists $v \in V$ such that $q(v) = d$. We denote $D(q)$ the set of all values in K represented by q.

Definition 2.8. Let (V, q) be a quadratic space over a field K. It is said to be

(1) isotropic if $q(v) = 0$ for some $v \neq 0 \in V$, where v is called an isotropic vector .

(2) anisotropic if $q(v) \neq 0$ for all $v \neq 0 \in V$.

(3) totally isotropic if $q(v) = 0$ for all $v \in V$.

(4) universal if $D(q) = K$.

Lemma 2.9. *Let $a, b \in K^*$, $\dim V = 2$. $q \simeq \langle a, b\rangle$ if and only if $a \in D(q)$ and $a\,b = \det q$ in $K^*/(K^*)^2$.*

Proof. See [18, Proposition I.5.1]. □

Note that

$$\langle a, b\rangle = \langle a, a^2 b\rangle = \langle a, a \det q\rangle\,,$$

$$\langle a, -a\rangle = \langle 1, -1\rangle \text{ for all } a \in K^*\,.$$

Theorem 2.10. *Let (V, q) be a 2-dimensional nonsingular quadratic space over a field K. The following four statements are equivalent.*

(1) *q is isotropic*

(2) $\det(q) = -1$ *in* K^*/K^{*2}.

(3) $q \simeq \langle 1, -1\rangle$.

(4) *$q(x, y) = xy$ in some basis of V.*

Proof. See [18, Theorem I.3.2]. □

Definition 2.11. Let (V,q) be a 2-dimensional nonsingular quadratic space over a field K. The q is said to be hyperbolic if it satisfies one of the four statements of Theorem 2.10. Moreover, (V,q) is called a hyperbolic plane. In general, an orthogonal sum of hyperbolic planes is called a hyperbolic space.

Example 2.12. Let K be a field and $a \in K^*$.

$$\begin{aligned} q = \langle a, a\rangle \quad & \text{is hyperbolic} \\ & \text{if and only if} \quad a^2 = \det q = -1 \text{ in } K^*/K^{*2} \\ & \text{if and only if} \quad K \text{ contains a primitive 4th root of unity.} \end{aligned}$$

2.7. **Kronecker Products of Quadratic Spaces.**

Let (V_1, q_1), (V_2, q_2) be quadratic spaces over a field K. We define (V,q) by $V = V_1 \otimes V_2$ and $q = q_1 \otimes q_2$. Then (V,q) is called the kronecker product of the quadratic spaces if $q(v_1 \otimes v_2) = q_1(v_1)q_2(v_2)$, for all $v_1 \in V_1$ and $v_2 \in V_2$. In particular, if $q_1 = \langle a_1, \cdots, a_n\rangle$ and $q_2 = \langle b_1, \cdots, b_m\rangle$ then

$$q = \langle a_1b_1, a_1b_2, \cdots, a_1b_m, a_2b_1, \cdots, a_nb_1, \cdots, a_nb_m\rangle .$$

Definition 2.13. Let $a_1, \cdots, a_n \in K^*$. Suppose K does not contains a primitive 4th root of unity. We write $\langle\langle a_1, \cdots, a_n\rangle\rangle$ to denote the 2^n–dimensional form $\otimes_{i=1}^n \langle 1, -a_i\rangle$ called the n-fold Pfister form.

Note that if K contains a primitive 4th root of unity, then the n–fold Pfister form is equivalent to $\otimes_{i=1}^n \langle 1, a_i\rangle$.

Remark 2.14. A 0-fold Pfister form, by convention, taken to be $\langle 1\rangle$. A 1-fold Pfister form Pfister form $\langle\langle a\rangle\rangle = \langle 1, a\rangle$. Suppose K does not have a primitive

4th root of unity. If some a_i is 1, then $\langle\langle a_1, \cdots, a_n\rangle\rangle$ becomes hyperbolic. Also, $\langle\langle -1, a_2, \cdots, a_n\rangle\rangle = 2\langle\langle a_2, \cdots, a_n\rangle\rangle$.

Note that if K contains a primitive 4th root of unity then the form is hyperbolic whenever $a_i = 1$ or -1, for some i.

2.8. **Witt Rings.**

Let $M(K)$ be a set of all equivalent classes of finite dimensional nonsingular quadratic forms over a field K. Then $(M(K), \oplus, \otimes)$ will be a semi-ring.

We define a relation $\sim$ on $M(K) \times M(K)/\sim$ by

$$(q_1, q_2) \sim (q_1', q_2') \Leftrightarrow q_1 \oplus q_2' = q_1' \oplus q_2 \in M(K).$$

Denote (q_1, q_2) by $q_1 - q_2$. Then we have

$$WG(K) = \{q_1 - q_2 | q_1, q_2 \in M(K)\},$$

which consists of all equivalent classes. Then $(WG(K), \oplus, \otimes)$ forms a ring.

Definition 2.15. We call $WG(K)$ the Witt-Grothendieck ring.

We define the ring homomorphism

$$\dim : WG(K) \to \mathbb{Z}$$

by $q_1 - q_2 \mapsto \dim q_1 - \dim q_2$.

Lemma 2.16. *$\mathbb{Z}\langle 1, -1\rangle = \{n\langle 1, -1\rangle | n \in \mathbb{Z}\}$ is an ideal of $WG(K)$.*

Proof. See [18, Corollary I.6.1]. □

Definition 2.17. The $W(K) = WG(K)/\mathbb{Z}\langle 1, -1\rangle$ is called the Witt ring of K.

3. Preliminaries on Trace Forms

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

3.1. Subextensions.

Recall that if $F \subset K \subset L$ is a tower of finite field extensions then

$$\mathrm{tr}_{L/F}(\alpha) = \mathrm{tr}_{K/F}(\mathrm{tr}_{L/K}(\alpha))$$

for any $\alpha \in L$.

Lemma 3.1. *Let L/K and K/F be finite field extensions of degrees n and m respectively. Suppose $q_{L/K} = \langle a_1, \ldots, a_n \rangle$. 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 $q_{L/F} = \langle a_1, \ldots, a_n \rangle \otimes q_{K/F}$.

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

(d) Suppose $q_{L/K} = q_{L'/K}$ in $W(K)$ for a finite field extension L'/K. Then $q_{L/F} = q_{L'/F}$ in $W(F)$.

Proof. (a) Suppose $q_{L/K} = \langle a_1, \ldots, a_n \rangle$ in the K-basis $v_1, \ldots, v_n$ 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 $i \neq j$. Indeed, let $\alpha = xv_i, \beta = yv_j$ for some $x, y \in K$. Then for any $i \neq j$.

$$\mathrm{tr}_{L/F}(\alpha\beta) = \mathrm{tr}_{K/F}(\mathrm{tr}_{L/K}(\alpha\beta)) = \mathrm{tr}_{K/F}(xy\mathrm{tr}_{L/K}(v_iv_j)) = 0,$$

since $\mathrm{tr}_{L/K}(v_iv_j) = 0$, for any $i \neq j$. Moreover, $q_{L/F} = q^{a_i}_{K/F}$ on Kv_i. Indeed, let $\alpha = xv_i$ for some $x \in K$. Then

$$q_{L/F}(\alpha) = \mathrm{tr}_{L/F}(\alpha^2) = \mathrm{tr}_{K/F}(\mathrm{tr}_{L/K}(\alpha^2)) = \mathrm{tr}_{K/F}(a_ix^2) = q^{a_i}_{K/F}(x)\,.$$

Hence part (a) follows.

(b) If $a_i \in F$ then for any $x \in K$, $q^{a_i}_{K/F}(x) = \mathrm{tr}_{K/F}(a_ix^2) = \langle a_i\rangle \otimes q_{K/F}(x)$. The desired equality is now an immediate consequence of part (a).

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

(d) Since $q_{L/K}$ and $q_{L'/K}$ are Witt-equivalent, we may assume that $q_{L/K} = \langle a_1, \ldots, a_n\rangle$ and $q_{L'/K} = \langle a_1, \ldots, a_n\rangle \oplus m\langle 1, -1\rangle$. Then by part (b)

$$\begin{aligned} q_{L'/F} &= q^{a_1}_{K/F} \oplus \cdots \oplus q^{a_n}_{K/F} \oplus m(q_{K/F} \oplus q^{-1}_{K/F}) \\ &= q_{L/F} \oplus m\langle 1, -1\rangle \otimes q_{K/F}\,. \end{aligned}$$

Since $\langle 1, -1\rangle = 0$ in $W(F)$, part (d) follows. □

3.2. **Cyclic extensions.**

Lemma 3.2. *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*

$$q_{L/K} = \begin{cases} \langle n, na\rangle & \text{if } n \text{ even} \\ \langle n\rangle & \text{if } n \text{ odd} \end{cases}$$

in $W(K)$.

Proof. Let $G = \langle \sigma \rangle$ for L/K, ζ_n be a primitive nth root of unity, and let $x = \sqrt[n]{a}$. Since $\sigma(x) = \zeta_n x$, we have

$$\operatorname{tr}_{L/K}(x^i) = \begin{cases} 0 & \text{if } i = 1, 2, \ldots, n-1 \\ n & \text{if } i = 0. \end{cases}$$

Suppose n is even. An easy computation in the basis $1, x, \ldots, x^{n-1}$ 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 $i = 1, \ldots, \frac{n}{2} - 1$. Thus $q_{L/K} = \langle n, na \rangle$ in $W(K)$. Now suppose n is odd. Similarly, $q_{L/K} = \langle n \rangle$ on $\mathrm{Span}_K\{1\}$ and is hyperbolic on $\mathrm{Span}_K\{x^i, x^{n-i}\}$ for every $i = 1, \ldots, \frac{n-1}{2}$. Thus $q_{L/K} = \langle n \rangle$ in $W(K)$, as desired. □

3.3. **Abelian extensions.**

Lemma 3.3. *Let $G = \mathbb{Z}/n_1\mathbb{Z} \times \cdots \times \mathbb{Z}/n_r\mathbb{Z}$ be an abelian 2-group (here every $n_i \geq 2$ is a power of 2), $n = \max(n_1, \ldots, n_r)$ be the exponent of G, K be a field containing a primitive nth root of unity, and let $L = K(\sqrt[n_1]{a_1}, \ldots, \sqrt[n_r]{a_r})$ be a G-Galois extension for some $a_1, \ldots, a_r \in K$. Then $q_{L/K} = \langle |G| \rangle \otimes \langle\langle a_1, \ldots, a_r \rangle\rangle$ in $W(K)$.*

Proof. It is sufficient to consider the case where G is cyclic (i.e., $r = 1$ and $n_1 = n = |G|$); the general case will then follow from Lemma 3.1(c) and Lemma 3.2 by induction on r. Hence we have

$$\begin{aligned} \langle n_1, n_1 a_1 \rangle \otimes \cdots \otimes \langle n_r, n_r a_r \rangle &= \langle n_1 \cdots n_r \rangle \otimes \langle 1, a_1 \rangle \otimes \cdots \otimes \langle 1, a_r \rangle \\ &= \langle |G| \rangle \otimes \langle\langle a_1, \cdots, a_r \rangle\rangle, \end{aligned}$$

as desired. □

Lemma 3.4. *Let $G = \mathbb{Z}/n_1\mathbb{Z} \times \cdots \times \mathbb{Z}/n_r\mathbb{Z}$ be an abelian 2-group, $K = k(a_1, \dots, a_r)$, and $L = k(\sqrt[n_1]{a_1}, \dots, \sqrt[n_r]{a_r})$, where k is a field containing suitable roots of unity and $a_1, \dots, a_r$ are algebraically independent variables over k. Then $q_{L/K}$ is not hyperbolic over K.*

Proof. Lemma 3.3 showed that $q_{L/K} = \langle |G| \rangle \otimes \langle\langle a_1, \dots, a_r \rangle\rangle$. The desired conclusion follows from [22, Example 8.1.2(6)]. □

3.4. **Extensions of degree 2.**

Lemma 3.5. *Let $L = K(\sqrt{b})$ be a quadratic field extension for some $b \in K$ and let $a \in L^*$. Then*

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

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

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

Proof. (a) Note that $q^a_{L/K}(1) = \operatorname{tr}(a) = 0$. Part (a) now follows from the fact that a 2-dimensional nonsingular form is hyperbolic iff it is isotropic by Theorem 2.10.

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

Recall that any nonsingular 2-dimensional quadratic form q can be written as $q = \langle v \rangle \otimes \langle 1, \det(q) \rangle$, where $v \in K^*$ is a value assumed by q; see, e.g., Lemma 2.9 or [18, Proposition I.5.1]. Since $q^a_{L/K}(1) = \operatorname{tr}(a)$, we can take $v = \operatorname{tr}(a)$.

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 $\det(q) = 2ba\bar{a} - 2c\bar{c}a\bar{a} = 4ba\bar{a} = b\,n(a)$ in $(K)^*/(K^*)^2$, and the lemma follows. □

3.5. **Linear representations.**

Lemma 3.6. *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., [29, 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 [18, Lemma IX.1.1]. □

Proposition 3.7. *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 3.6, we may assume that $V = V_{\text{reg}} \simeq k[G]$ is the regular representation of G. Let $t = (t_1, \dots, t_n)$ be an n-tuple of independent variables, where $n = |G|$. By [24, Theorem 4.2] there exists an element $a \in L(t)$ whose n conjugates $g(a)$ are algebraically independent over k. Then $F = k(g(a) \mid g \in G)$ 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. [18, Lemma IX.1.1]), as claimed. □

4. Proof of Theorem 1.3

Definition 4.1. 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.

Reduction 4.2. In order to prove Theorem 1.3 it is sufficient to show that every non-abelian 2-group G has property (*).

Proof. Indeed, by Lemma 3.4, no abelian 2-group G has property(*). Now, let G, e and L/K be as in Theorem 1.3, 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 3.1(c) $q_{L/K}$ is hyperbolic as well. □

Proposition 4.3. *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 $H = \langle r \rangle$ 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 be 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 3.1(c) tells us that $q_{L/K}$ is hyperbolic over K, as desired.

(b) Suppose $H = \langle r \rangle$ is of order n and $H_0 = \langle r^{n/m} \rangle$ 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 $L^{H_0} = L^H(\sqrt[\frac{n}{m}]{a})$, and thus by Lemma 3.2, $q_{L/L^H} = \langle n, na \rangle$ and $q_{L^{H_0}/L^H} = \langle \frac{n}{m}, \frac{n}{m}a \rangle$ in $W(L^H)$. In other words,

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

and

$$q_{L^{H_0}/L^H} = \langle \frac{n}{m}, \frac{n}{m}a \rangle \oplus \frac{\frac{n}{m}-2}{2} \langle 1, -1 \rangle \,.$$

By Lemma 3.1(a),

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

Since by Lemma 3.1(b), $q_{L^H/K} \oplus q^{-1}_{L^H/K} = \langle 1, -1 \rangle \otimes q_{L^H/K} = 0$ in $W(K)$, we conclude that

$$q_{L/K} = \langle n \rangle \otimes (q_{L^H/K} \oplus q^{a}_{L^H/K}) \text{ in } W(K).$$

Similarly,

$$q_{L^{H_0}/K} = \langle \frac{n}{m} \rangle \otimes (q_{L^H/K} \oplus q^{a}_{L^H/K}) \text{ in } W(K).$$

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 $q_{L/K} = \langle m \rangle \otimes q_{L^{H_0}/K} = 0$ as well, thus proving (b). □

In view of Reduction 4.2, the goal of the rest of this section will be to prove the following.

Theorem 4.4. *Every non-abelian 2-group G has property (*).*

We will prove Theorem 4.4 by contradiction. Let G_{min} be a counterexample of minimal order.

Proposition 4.5. *(a) Every proper subgroup of G_{min} is abelian.*

(b) The center $Z(G_{min})$ has index 4 in G_{min}.

(c) If S is a proper subgroup of G_{min}, then $[S : (S \cap Z(G_{min}))] \leq 2$.

(d) $x^2 \in Z(G_{min})$ for every $x \in G_{min}$.

Let G'_{min} be the commutator subgroup of G_{min}.

(e) $G'_{min} \subset Z(G_{min})$.

(f) $|G'_{min}| = 2$. In the sequel we shall denote the non-identity element of G'_{min} by c.

(g) If $r \in G_{min}$ is an element of order $n \geq 4$ then $r^{n/2} = c$.

(h) G_{min} is generated by two elements r and s such that $rs = csr$.

(i) $|G_{min}| \geq 16$.

Proof. (a)Let H be a proper subgroup of G_{min}. Assume H is non–abelian. By the minimality of G_{min}, H should have the property (*). But this is a contradiction to Proposition 4.3. Thus every proper subgroup of G_{min} is abelian.

(b)Let H be a subgroup of index 2 in G_{min}; see, e.g., [25, 5.3.1(ii)]. Choose $g \in G_{min} \backslash H$; applying [25, 5.3.1(ii)] once again with the cyclic subgroup $\langle g \rangle$, we can find a subgroup $H' \subset G_{min}$ such that $g \in H'$ and $[G_{min} : H'] = 2$. By part (a) both H and H' are abelian. Hence every $x \in H \cap H'$ commutes with g and with every element of H. Since H and g generate G_{min}, we conclude that $x \in Z(G_{min})$, i.e.,

$$H \cap H' \subset Z(G_{min})\,. \tag{4.1}$$

Since G_{min} is non-abelian, $G_{min}/Z(G_{min})$ cannot be cyclic, i.e.,

$$[G_{min} : Z(G_{min})] \geq 4\,; \tag{4.2}$$

see, e.g., [26, 6.3.4]. On the other hand, since $[G_{min} : H] = 2 = [G_{min} : H']$, we have $2 \leq [G_{min} : H \cap H'] \leq 4$. Assume $[G_{min} : H \cap H'] = 2$. Then

$$2 = [G_{min} : H \cap H'] = [G_{min} : H][H : H \cap H']$$

implies that $H = H \cap H'$. Similarly, $H' = H \cap H'$. Hence $H = H \cap H' = H'$. But this is impossible to our choice of H and H' with $g \in H' \setminus H$. Thus

$$[G_{min} : (H \cap H')] = 4\,. \tag{4.3}$$

Part (b) now follows from (4.1-4.3) and

$$4 = [G_{mni} : H \cap H'] = [G_{min} : Z(G_{min})][Z(G_{min}) : H \cap H']\,.$$

Also, we have $[Z(G_{min}) : H \cap H'] = 1$,i.e.,

$$H \cap H' = Z(G_{min})\,. \tag{4.4}$$

(c)Since S is a proper subgroup of G_{min} and apply S to [25, 5.3.1(ii)], then S is contained in a subgroup H of index 2. By (4.4), $Z(G_{min}) = H \cap H'$, where H' is another subgroup of G_{min} of index 2. Then $S \cap Z(G_{min}) = S \cap (H \cap H') = S \cap H'$, since $S \subset H$. Since $[H : H \cap H'] = 2$, $[S : S \cap Z(G_{min})] = [S : S \cap H'] \leq 2$.

(d)Let $S = \langle x \rangle$ be a cyclic subgroup of G_{min}. Applying part (c) to the cyclic group $S = \langle x \rangle$, we have $[S : S \cap Z(G_{min})] \leq 2$. If $[S : S \cap Z(G_{min})] = 1$, then $S \subset Z(G_{min})$, and $x^2 \in Z(G_{min})$. If $[S : S \cap Z(G_{min})] = 2$, then $x \notin Z(G_{min})$ because x generates S. Consider the factor group $S/(S \cap Z(G_{min})) \simeq \mathbb{Z}/2$ consisting of $(S \cap Z(G_{min}))$ and $x(S \cap Z(G_{min}))$. Hence $x(S \cap Z(G_{min}))x(S \cap Z(G_{min})) = (S \cap Z(G_{min}))$ if and only if $x^2 \in S \cap Z(G_{min})$. Thus $x^2 \in Z(G_{min})$.

(e) By part (b), the factor group $G_{min}/Z(G_{min})$ has order 4 and, hence, is abelian. Thus $G'_{min} \subset Z(G_{min})$.

(f) Since G_{min} is a non-abelian 2-group, it has an element r of order $n \geq 4$. Let $H = \langle r \rangle$ and $H_0 = \langle r^{n/2} \rangle$ be cyclic subgroups of G_{min} of orders n and 2 respectively. By part (d), H_0 is central and, hence, normal in G_{min}. By Proposition 4.3(b) G_{min}/H_0 does not have property (*) (otherwise G_{min} would have property (*) as well, contrary to our choice of G_{min}). By the minimality of G_{min}, we conclude that G_{min}/H_0 is abelian. In other words,

$$G'_{min} \subset H_0 \,. \tag{4.5}$$

Thus $|G'_{min}| \leq |H_0| = 2$. On the other hand, since G_{min} is non-abelian, $|G'_{min}| \neq 1$. Thus G'_{min} has exactly 2 elements, as claimed.

(g) By (4.5), $r^{n/2} \in G'_{min}$. Since r has order n, $r^{n/2} \neq 1$; thus $r^{n/2} = c$.

(h) By the minimality of G_{min} we can choose two non-commuting elements r and s in G_{min}. By part (a), these elements generate G_{min}. By part (f), $rsr^{-1}s^{-1} = c$.

(i) The only non-abelian 2-groups of order ≤ 8 and the dihedral group D_8 are the quaternion group Q_8. Thus it is enough to show that these groups have property (*).

If L/K is a D_8-Galois extension then $q_{L/K}$ has the form $\langle\langle -1, a, b \rangle\rangle$ for some $a, b \in K^*$; see [5, Section 6, Exemple] or [7, Proposition 12]. Note that $\exp(D_8) = 4$, and if $\zeta_4 \in K$ then -1 is a square, and thus $\langle\langle -1, a, b \rangle\rangle$ splits over K. This shows that D_8 has property (*).

Similarly, if L/K is a Q_8-Galois extension then $q_{L/K} = \langle\langle -1, -1, a \rangle\rangle$ for some $a \in K^*$; see [5, Section 6, Exemple] or [7, Proposition 12]. Note that $\exp(Q_8) = 4$, and if $\zeta_4 \in K$ then $\langle\langle -1, a, b \rangle\rangle$ splits over K. This shows that Q_8 also has property (*) and thus $|G_{min}| \geq 16$. □

4.1. The Group M(2n).

Let $n \geq 4$ be a power of 2. We define the group $M(2n)$ as the semidirect product of $\mathbb{Z}/n\mathbb{Z} \rtimes \mathbb{Z}/2\mathbb{Z}$, where the nontrivial element of $\mathbb{Z}/2\mathbb{Z}$ acts on $\mathbb{Z}/n\mathbb{Z}$ by sending 1 to $\frac{n}{2}+1$. Equivalently,

$$M(2n) = \{r, s \mid r^n = s^2 = 1, sr = r^{n/2+1}s\}\,. \tag{4.6}$$

Note that $M(8)$ is the dihedral group D_8.

Lemma 4.6. *(a) Every proper subgroup of $M(2n)$ is abelian.*

(b) For every proper normal subgroup N of $M(2n)$, the quotient $M(2n)/N$ is abelian.

Proof. (a) Let S be a proper subgroup of $M(2n)$. If S contains the index 2 subgroup $\langle r\rangle$ then $S = \langle r\rangle$ and thus S is abelian. If not, set $S_0 = S \cap \langle r\rangle$. Then, on the one hand, $S_0 \subset \langle r^2\rangle$, is central in $M(2n)$ and, on the other hand, $S/S_0 \subset M(2n)/\langle r\rangle \simeq \mathbb{Z}/2\mathbb{Z}$ is cyclic. This proves that S is abelian (see, e.g., [26, 3.2.8]).

(b) Assume the contrary,i.e., there is a non-abelian quotient group. The commutator of $M(2n)$ is $M(2n)' = \{1, r^{n/2}\}$. If $N \rhd M(2n)$ and N contains $r^{n/2}$ then $M(2n)' \leq N$ so that $M(2n)/N \leq M(2n)/M(2n)'$ are abelian. Hence we may assume N does not contain $r^{n/2}$. We know that $\langle r\rangle \rhd M(2n)$. Then

$$N \cap \langle r\rangle = \{1\}\,. \tag{4.7}$$

Otherwise, N contains $r^{n/2}$. Since $\langle r\rangle$ has index 2 in $M(2n)$, this is only possible if $|N| \leq 2$ or, equivalently, $|N| = 2$. Let $N = \langle r^i s\rangle$ for some i. Since $N \rhd M(2n)$, for all $g \in M(2n)$,

$$g(r^i s)g^{-1} = 1 \text{ or } r^i s\,.$$

But these cases imply that $s = r^{n/2+i}$, or $r^{n/2} = 1$ (for another proof, since N and $\langle r\rangle$ are complementary normal subgroups in $M(2n)$, $M(2n) \simeq N \times \langle r\rangle$, i.e., abelian). Hence this is a contradiction. Thus $M(2n)$ has no non-abelian quotient.

□

Proposition 4.7. $G_{min} = M(2n)$ *for some* $n \geq 8$.

Proof. Write $G_{min} = \langle r, s\rangle$, $G'_{min} = \{1, c\}$, and $sr = crs$, as in Proposition 4.5. Denote the orders of r and s by n and m respectively. We may assume without loss of generality that $n \geq m$. Since G_{min} is non-abelian, $m \geq 2$.

We claim that $n \geq 4$. Indeed, assume the contrary: $n = m = 2$. Then G_{min}/G'_{min} is an abelian group of order ≤ 4. Thus $|G_{min}| \leq 4|G'_{min}| = 8$, contradicting Proposition 4.5(i).

Thus $n \geq 4$. By Proposition 4.5(g), $c = r^{n/2}$. We now claim that $n \geq 8$. To prove this claim we need to show that $(n, m) \neq (4, 2)$, and $(4, 4)$.

Indeed, if $(n, m) = (4, 2)$ then $r^4 = s^2 = 1$ and $sr = crs = r^{-1}s$, i.e., r and s satisfy the defining relations of the dihedral group D_8. In other words, there exists a surjective homomorphism $D_8 \longrightarrow G_{min}$; thus $|G_{min}| \leq |D_8| = 8$, contradicting Proposition 4.5(i). If $(n, m) = (4, 4)$ then by Proposition 4.5(g), $s^2 = c = r^2$. In this case r and s satisfy the defining relations of the quaternion group Q_8, namely $r^4 = 1$, $r^2 = s^2$, and $srs^{-1} = r^{-1}$; see, e.g., [26, Example 8.2.4]. Hence there exists a surjective homomorphism $Q_8 \longrightarrow G_{min}$, and thus $|G_{min}| \leq |Q_8| = 8$, once again contradicting Proposition 4.5(i).

From now on we shall assume that $n \geq 8$. Let $\tilde{s} = r^{n/m}s$. We claim that

$$\tilde{s}^{\frac{m}{2}} = 1 \tag{4.8}$$

Indeed, recall that $r^{n/2} = s^{m/2} = c$; see Proposition 4.5(g). We now consider two cases.

Case I: $m < n$. Then $r^{n/m}$ is a square; hence, this element is central in G_{min} (see Proposition 4.5(d)) and thus

$$\widetilde{s}^{\frac{m}{2}} = r^{\frac{n}{2}} s^{\frac{m}{2}} = c^2 = 1\,,$$

as claimed.

Case II: $m = n$. Since r and s commute modulo $C'_{min} = \{1, c\}$, we have $\widetilde{s}^2 = c^i r^{2n/m} s^2$, where $i = 0$ or 1. Since c, $r^{2n/m}$ and s^2 are central elements of C_{min} (see Proposition 4.5(d) and (e)), $c^2 = 1$ and $m = n \geq 8$, we have

$$\widetilde{s}^{\frac{m}{2}} = (c^i r^{\frac{2n}{m}} s^2)^{\frac{m}{4}} = c^{\frac{mi}{4}} r^{\frac{n}{2}} s^{\frac{m}{2}} = 1 \cdot c \cdot c = 1\,.$$

This proves the claim.

Now observe that $G_{min} = \langle r, s\rangle = \langle r, \widetilde{s}\rangle$ and $rsr^{-1}s^{-1} = r\widetilde{s}r^{-1}\widetilde{s}^{-1} = c$. Thus we may replace s by $\widetilde{s}$. By (4.8), $\widetilde{s}$ has order $\leq m/2$. After repeating this process a finite number of times, we may assume $m = 2$.

Thus G_{min} is generated by elements r and s such that $r^n = s^2 = 1$ and $sr = r^{n/2+1}s$. Since these are the defining relations for $M(2n)$ (see (4.6)), there exists a surjective homomorphism $M(2n) \longrightarrow G_{min}$. By Lemma 4.6(b), this homomorphism is an isomorphism. This completes the proof of Proposition 4.7.

□

4.2. **Trace forms of M(2n)-Galois extensions.**

In this section we complete the proof of Theorem 4.4 (and thus of Theorem 1.3), by explicitly computing the trace form of an $M(2n)$-Galois extension.

Proposition 4.8. *Let $n \geq 8$. Suppose L/K be an $M(2n)$-Galois extension, and $\zeta_n \in K$. Then the trace form $q_{L/K}$ is hyperbolic.*

We remark that under the assumptions of the proposition, the primitive 8th root of unity $\zeta_8 = \zeta_n^{n/8}$ lies in K and thus

$$\sqrt{2} = \frac{2\zeta_8}{\zeta_8^2 + 1} \in K\,. \tag{4.9}$$

Proof. Set $\zeta = \zeta_n$ and let k be the field generated by the prime subfield of K and ζ. 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 3.7 we may assume without loss of generality that $L = k(V)$ and $K = k(V)^{M(2n)}$. Note that each of the elements listed below is preserved by both r and s and thus lies in $L^{M(2n)} = K$:

$$\begin{aligned} A &= x^n + y^n\,, \\ B &= (x^n - y^n)^2\,, \\ C &= x^{\frac{n}{2}} y^{\frac{n}{2}}\,, \\ D &= x^{\frac{n}{4}} y^{\frac{n}{4}} (\tfrac{x}{y} + \tfrac{y}{x})\,, \\ E_m &= (\tfrac{x}{y})^m + (\tfrac{y}{x})^m\,, \quad (m \geq 2 \text{ even}). \end{aligned} \tag{4.10}$$

We begin by explicitly computing the trace form $q_{L/K}$.

Lemma 4.9. $q_{L/K} = \langle\langle A, B \rangle\rangle$.

Proof. Consider the intermediate extension $K \subset L^H \subset L$. where $H = \langle r \rangle \subset M(2n)$. Note that $L = L^H(x) = L^H(\sqrt[n]{a})$, where $a = x^n$. By Lemma 3.2

$$q_{L/L^H} = \langle n \rangle \otimes \langle 1, a \rangle = \langle 1, a \rangle\,,$$

where the last equality follows from (4.9). Thus by Lemma 3.1(a)

$$q_{L/K} = q_{L^H/K} \oplus q^a_{L^H/K}\,. \tag{4.11}$$

Note that $[L^H : K] = [M(2n) : H] = 2$; moreover, $L^H = K(x^n - y^n) = K(\sqrt{B})$. Thus Lemma 3.5 tells us that

$$q_{L^H/K} = \langle 2 \rangle \otimes \langle 1, B \rangle = \langle 1, B \rangle \,,$$

where once again, the factor of 2 can be dropped because of (4.9), and

$$q^a_{L^H/K} = \langle \mathrm{tr}_{L^H/K}(a) \rangle \otimes \langle 1, n_{L^H/K}(a) B \rangle \,.$$

Note that $\mathrm{tr}_{L^H/K}(a) = x^n + y^n = A$ and $n_{L^H/K}(a) = x^n y^n = C^2$ is a complete square in K. Thus (4.11) can be rewritten as

$$q_{L/K} = \langle 1, B \rangle \oplus \langle A, AB \rangle = \langle\langle A, B \rangle\rangle$$

as claimed. □

Our goal is to prove that $\langle\langle A, B \rangle\rangle$ is hyperbolic over K. We shall need the following simple relations among the elements of K defined in (4.10).

Lemma 4.10. *(a)* $E_{2m} = E_m^2 - 2$.

(b) $E_2 = \frac{D^2}{C} - 2$.

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

Proof. (a) and (b) are immediate from (4.10).

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

We are now ready to complete the proof of Proposition 4.8.

$$q_{L/K} = \langle\langle x^n + y^n, (x^n - y^n)^2 \rangle\rangle = \langle\langle C E_{n/2}, C^2 (E_{n/2}^2 - 4) \rangle\rangle \,.$$

By Lemma 4.10, $E_{n/2}^2 - 4 \equiv E_{n/4}^2 - 4$ (recall that we are assuming $n \geq 8$). Thus $q_{L/K} = \langle\langle C(E_{n/4}^2 - 2), E_{n/4}^2 - 4 \rangle\rangle$. Since $E_{n/4}^2 - 2 = (E_{n/4}^2 - 4) \cdot 1^2 + (\sqrt{2})^2$, [18, Proposition X.1.3(1)] tells us that this form is equivalent (over K) to $\langle\langle C, E_{n/4}^2 -$

$4\rangle\rangle$. (Recall that $\sqrt{2} \in K$ by (4.9).) Applying Lemma 4.10(c) once again, we can replace $E_{n/4}^2 - 4$ by $E_2^2 - 4$ and thus obtain

$$q_{L/K} = \langle\langle C, E_2^2 - 4\rangle\rangle \, .$$

By Lemma 4.10(b),

$$E_2^2 - 4 = \frac{D^2}{C^2}(D^2 - 4C) \equiv D^2 - 4C \pmod{(K^*)^2} \, .$$

Thus

$$q_{L/K} = \langle\langle C, D^2 - 4C\rangle\rangle \, .$$

The latter Pfister form is clearly isotropic over K (indeed, $D^2 - C \cdot 2^2 - (D^2 - 4C) \cdot 1^2 = 0$); hence by [18, Corollary X.1.6], it is hyperbolic, as claimed. This completes the proof of Proposition 4.8, Theorem 4.4 and Theorem 1.3. □

4.3. **An example.**

We conclude this section with an example, communicated to us by J.-P. Serre, showing that for $G = M(2n)$ condition (b) of Theorem 1.3 cannot be relaxed.

Example 4.11. 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) $q_{L/K} = \langle 2n\rangle \otimes \langle\langle \zeta_{n/2}, a\rangle\rangle$, 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. (4.6). By Lemma 4.6(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 $L^{\langle r\rangle} = k'((a))$. Since $L = L^{\langle r\rangle}(\sqrt[n]{a})$ and $L^{\langle r\rangle} = K(\sqrt{\zeta_{n/2}})$, Lemma 3.2 tells us that

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

and

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

The desired formula now follows from Lemma 3.1(b).

(c) Since $\zeta_{n/2}$ is not a square in k, i.e., $\langle 1, \zeta_{n/2}\rangle$ is anisotropic over k, $q_{L/K}$ is anisotropic by [18, Proposition VI.1.9]. □

5. Non-existence of Self-Dual Normal Bases

We begin by recalling the definitions.

Definition 5.1. Let L be a finite Galois extension of a field K with a Galois group G. Suppose $\alpha \in L$. An orthogonal normal basis of L over K is a basis of the form $\{\sigma(\alpha) | \sigma \in G\}$ such that

$$\mathrm{tr}_{L/K}(\sigma(\alpha)\tau(\alpha)) = 0\,,$$

for any $\sigma, \tau \in G$ with $\sigma \neq \tau$. We call an orthogonal normal basis a self-dual normal basis if it also satisfies

$$\mathrm{tr}_{L/K}(\sigma(\alpha)\sigma(\alpha)) = 1\,,$$

for any $\sigma \in G$.

Lemma 5.2. *Let G be a finite group, L be a $G-$Galois field extension of a field K. Then the conditions to be a self-dual normal basis as in Definition 5.1 are equivalent to*

$$\mathrm{tr}_{L/K}(\alpha\sigma(\alpha)) = \begin{cases} 0 & \textit{if } \sigma \neq id \\ 1 & \textit{if } \sigma = id\ . \end{cases} \tag{5.1}$$

Proof. For all $g \in G$, and $x \in L$, $\mathrm{tr}_{L/K}(gx) = \mathrm{tr}_{L/K}(x)$. Hence

$$\mathrm{tr}_{L/K}(g_1(\alpha)g_2(\alpha)) = \mathrm{tr}_{L/K}(g_1^{-1}(g_1(\alpha)g_2(\alpha))) = \mathrm{tr}_{L/K}(\alpha g(\alpha))\,,$$

where $g_1, g_2 \in G$ and $g = g_1^{-1}g_2$. □

Lemma 5.3. *Let K contain a primitive 4th root of unity, and let L/K be a $G-$Galois field extension of even degree. If L/K has an orthogonal normal basis, then $q_{L/K}$ is hyperbolic.*

Proof. Let $\{\sigma(\alpha) | \sigma \in G\}$ be an orthogonal normal basis of L over K, where $\alpha \in L$. Since for any $\sigma, \tau \in G$,

$$\tau G = G, \text{ and } \operatorname{tr}(\sigma(\alpha)\tau(\sigma)) = \begin{cases} 0 & \text{if } \sigma \neq \tau \\ 1 & \text{if } \sigma = \tau, \end{cases}$$

then for all $\sigma \in G$,

$$\operatorname{tr}(\sigma(\alpha)\sigma(\alpha)) = a,$$

where $a \in K^*$. By Example 2.12, $\langle a, a \rangle$ is hyperbolic since K contains 4th root of unity. Hence $q_{L/K} = \langle a, \cdots, a \rangle$ is the sum of hyperbolic planes. Thus $q_{L/K}$ is hyperbolic. □

5.1. **Proof of Theorem 1.5(a).**

Proposition 5.4. *Let L be a Galois extension of a field K with Galois group G. Suppose that G has a normal subgroup N.*

(1) *If L has an orthogonal normal basis over K then L^N has an orthogonal normal basis over K.*

(2) *If L has a self-dual normal basis over K, then L^N has a self-dual normal basis over K.*

Proof. Let $\alpha \in L$, $G = \{g_1, \cdots, g_n\}$, and let $B = \{g_1(\alpha), \cdots, g_n(\alpha)\}$. Since N is a normal subgroup of G with $|N| = t$, consider the quotient group, $G/N = \{a_1 N, \cdots, a_r N\}$, where the $a_i \in G$. Then we write

$$\begin{aligned} y_1 &= a_1 n_1 \alpha + \cdots + a_1 n_t \alpha, \\ \cdots & \quad \cdots \\ y_r &= a_r n_1 \alpha + \cdots + a_r n_t \alpha, \end{aligned}$$

where $\{a_j n_i\}_{1\leq j\leq r, 1\leq i\leq t} = G$. Note that for each $j = 1, \cdots, r$, $y_j \in L^N$.

(1)Suppose B is an orthogonal normal basis for L over K. For each $1 \leq i \neq j \leq r$, the transitivity formula for the trace (see Section 3[Subextensions]) tells us that

$$\begin{aligned}
\mathrm{tr}_{L^N/K}(y_i\, y_j) &= 1/|N|\; \mathrm{tr}_{L/K}(y_i\, y_j) \\
&= 1/|N|\; \mathrm{tr}_{L/K}((h^i_1\alpha + \cdots + h^i_t\alpha)(h^j_1\alpha + \cdots + h^j_t\alpha)) \\
&= 1/|N| \sum_{k,l=1}^{t} \mathrm{tr}_{L/K}(h^i_k\alpha\, h^j_l\alpha) \\
&= 0,
\end{aligned}$$

where $h^j_i = a_j\, n_i$. Thus $y_1, \cdots, y_r$ form an orthogonal normal basis for L^N over K.

(2) Suppose B is a self-dual normal basis for L over K. From (1), it is enough to show that $\mathrm{tr}_{L^N/K}(y_i^2) = 1$, for each $j = 1, \cdots, r$. Indeed,

$$\begin{aligned}
\mathrm{tr}_{L^N/K}(y_i^2) &= 1/|N| \sum_{k,l=1}^{t} \mathrm{tr}_{L/K}(h^i_k\alpha\, h^i_l\alpha) \\
&= 1/|N| \sum_{k=1}^{t} \mathrm{tr}_{L/K}(h^i_k\alpha)^2 \\
&= 1/|N|\; t \\
&= 1,
\end{aligned}$$

where $h^j_i = a_j\, n_i$. Thus $y_1, \cdots, y_r$ form a self-dual normal basis for L^N over K. □

Lemma 5.5. *Suppose L/K is a Galois extension of a field K of degree 2. Then L does not have orthogonal normal basis over K.*

Proof. Since $[L : K] = 2$, we can let $L = K(\sqrt{b})$ for some $b \in K^*$. Apply $a = 1$ to Lemma 3.5, we have

$$q_{L/K} = \langle 2 \rangle \otimes \langle 1, b \rangle .$$

Let ζ_4 be a primitive 4th root of unity. Assume $q_{L/K}$ is hyperbolic. By Example 2.12,

$$q_{L/K} = \langle 2 \rangle \otimes \langle 1, b \rangle \quad \text{is hyperbolic}$$

$$\text{if and only if} \quad b = \det q_{L/K} = -1 \text{ in } K^*/K^{*2}.$$

Hence $\zeta_4 \notin K$; (otherwise, $L = K$).

If $\zeta_4 \in L$, then the quadratic form $q_{L/K}$ is hyperbolic. However, if L/K has an orthogonal normal basis then the quadratic form for L/K is of the form $\langle a, a \rangle$ as in the proof of Lemma 5.3. By Example 2.12, $\langle a, a \rangle$ is not hyperbolic since $\zeta_4 \notin K$. This is a contradiction. Suppose $\zeta_4 \notin L$. Then $q_{L/K}$ is not hyperbolic, i.e., L/K has no orthogonal normal basis. □

Proof. We are now ready to complete the proof of Theorem 1.5(a). Suppose N is a subgroup of G of index 2. Assume that L has an orthogonal normal basis for L/K. By Proposition 5.4, the field extension L^N has an orthogonal normal basis over K, with $[L^N : K] = 2$. But Lemma 5.5 tells us that L^N cannot have an orthogonal normal basis over K. This contradiction completes the proof. □

Example 5.6. The following groups have subgroups of an index 2.

(1) Let G be a nontrivial 2-group; see,e.g., [26, 6.3.11].

(2) Let $G = S_n$, for $n \geq 2$.

(3) Let $G = \mathrm{GL}_n(K)$, where K is a finite field with $\mathrm{char}(K) \neq 2$, and $n \geq 1$. The K^* has a subgroup H of index 2 because K^* is a cyclic group of even order. Then the preimage of H under the surjective homomorphism $\det : \mathrm{GL}_n(K) \to K^*$ is a subgroup of $\mathrm{GL}_n(K)$ of index 2.

In all of these cases Theorem 1.5(a) tells us that no G−Galois extension L/K can have an orthogonal normal basis.

5.2. **Proof of Theorem 1.5(b).**

We will now prove Theorem 1.5(b) by explicitly constructing a G-Galois extension which does not have an orthogonal normal basis.

Proposition 5.7. *Let V be faithful linear representation of a finite group G over a field k, $L = k(V)$, $K = L^G$, and let $G_2 \leq G$ be an abelian 2-group. Suppose n is the exponent of G_2 and K contains a primitive nth root of unity. Then the Galois extension L of L^G has no orthogonal normal basis.*

Proof. The Proposition 3.7, [5, Theorem 6.1.2], and Lemma 3.4 tell us that the trace form $q_{L/K}$ is not hyperbolic. The desired result now follows from Lemma 5.3 . □

Example 5.8. Let $G = A_n$ $(n = 4, 5)$. Then the group G has an abelian Sylow 2-subgroup. Thus the G-Galois extension of Proposition 5.7 has no orthogonal normal basis.

5.3. **Groups of small order.**

We will now use Theorem 1.5 to show that the converse to the Bayer-Lenstra Theorem 1.4 holds for "almost all" groups of small order.

Proposition 5.9. *Let G be a group of even order ≤ 47. Assume $G \not\simeq$ $\mathrm{SL}_2(\mathbb{Z}/3\mathbb{Z})$. Then there exists a G-Galois field extension L/K, such that L*

does not have an orthogonal normal basis over K. In fact, K can be taken to be a finitely generated extension of an algebraically closed field.

Proof. By Theorem 1.5 it suffices to show that $\mathrm{SL}_2(\mathbb{Z}/3\mathbb{Z})$ is the only group of order ≤ 47 which has the following two properties:

(1) G does not have a subgroup of index 2, and

(2) the Sylow 2-subgroup of G is not abelian.

If $|G| \neq 24, 40$ then G is either 2-group (and thus (1) fails) or $|G| = 2^i m$, where $i \leq 2$ and m is odd (and thus (2) fails).

Suppose G is a group of order 40, satisfying (1) and (2). Every group of order 40 is solvable; hence G has a normal subgroup H of index 2 or 5. The former is impossible by (1); thus we may assume $|H| = 8$. By (2), H is isomorphic to D_8 or Q_8. Let K be a Sylow 5-subgroup of G. Then $G = H \rtimes_\phi K$, where ϕ is a homomorphism $K \to \mathrm{Aut}(H)$. By [8, Proposition 4.4.17], $\mathrm{Aut}(D_8) = D_8$ and $\mathrm{Aut}(Q_8) = S_4$. Since the orders of these groups are not divisible by 5, ϕ is trivial, i.e., $G = H \times K$. Consequently, G has a subgroup of index 2, contradicting (1). This shows that no subgroup of order 40 satisfies (1) and (2).

Now, assume G is a subgroup of order 24, satisfying (1) and (2). Then G is solvable and, hence, has a subgroup H of index 2 or 3. The former is impossible by (1); thus $|H| = 8$. By (2), H is either D_8 or Q_8. Let K be a subgroup of G of order 3. Then $G = H \rtimes_\phi K$, where ϕ is a homomorphism $K \to \mathrm{Aut}(H)$. As noted above, $\mathrm{Aut}(D_8) = D_8$ and $\mathrm{Aut}(Q_8) = S_4$. If $H = D_8$ then $|K| = 3$ and $|\mathrm{Aut}(H)| = 8$; this implies that ϕ is trivial. Then $G = H \times K$, so that G has a subgroup of index 2, a contradiction.

From now on we will assume $G = H \rtimes_\phi K$, where $H = Q_8$, $K = \mathbb{Z}/3$, and $\phi\colon K \to \mathrm{Aut}(H)$ is nontrivial (otherwise $G = H \times K$, and G has a subgroup of index 2, as above.) Then ϕ is an isomorphism between K and the subgroup of $\mathrm{Aut}(Q_8) = S_4$ generated by a 3-cycle. Since S_4 has 8 3-cycles, there are

8 possibilities for ϕ. We claim that the resulting semidirect products are all isomorphic to each other (and thus isomorphic to $\mathrm{SL}_2(\mathbb{Z}/3\mathbb{Z})$, which has order 24 and satisfies (1) and (2)). Since any two 3-cycles in S_4 are conjugates, the proposition is a consequence of the following:

Lemma 5.10. *Let K and H be groups, f and f' be homomorphisms $K \to \mathrm{Aut}(H)$, and S and S' be the semidirect products of H and K formed via f and f', respectively. Assume that f and f' are conjugates, i.e., there exists a r in $\mathrm{Aut}(H)$ such that $f'(x) = r\,f(x)\,r^{-1}$ for any $x \in K$. Then $(h,x) \mapsto (r(h),x)$ is an isomorphism between S and S'.*

To prove the lemma, define $\Phi : S \to S'$ by $(h,x) \mapsto (r(h),x)$ for any $h \in H$ and $x \in K$. Then for any $h_1, h_2 \in H$ and $x_1, x_2 \in K$

$$\begin{aligned}\Phi((h_1,x_1)(h_2,x_2)) &= \Phi((h_1 f(x_1)h_2, x_1x_2)) = (r(h_1 f(x_1)h_2), x_1x_2) \\ &= (r(h_1)(f'(x_1)r)(h_2), x_1x_2) = \Phi(h_1,x_1)\Phi(h_2,x_2)\,.\end{aligned}$$

Hence Φ is a homomorphism. Since $|S| = |S'|$, we need to show that Φ is one-to-one. Indeed, $(h,x) \in \operatorname{Ker}\Phi$, i.e., $(r(h),x) = 0$. Since $r \in \mathrm{Aut}(H)$, $\operatorname{Ker}\Phi = (0)$. This completes the proof of Lemma 5.10 and thus of Proposition 5.9. □

Remark 5.11. The argument of the case where $|G| = 40$ shows that no subgroup of order 56 can satisfy the properties (1) and (2).

6. Explicit Self-Dual Normal Bases

By Theorem 1.4 every odd degree Galois extension L/K has a self-dual normal basis. In this section we give an explicit formula constructing such a basis in the case where G is cyclic and K contains suitable roots of unity and the characteristic of K can be 2.

We remark that Lempel and Weinberger [20] found a general construction for self-dual normal basses in the case where K and L are finite fields; see in [20, p. 196]. Our construction works for both finite and infinite fields; however, in the finite field case, K rarely contains the required roots of unity.

Lemma 6.1. *Let $G = G_1 \times G_2$. Suppose that $L \supseteq F \supseteq K$ are Galois extensions with a Galois group G, where $F = L^{G_1}$ and $K = L^G$. If $\{a_1, \cdots, a_m\}$ is a self-dual normal basis for L/F, and $\{b_1, \cdots, b_n\}$ is a self-dual normal basis for F/K, then $\{a_i b_j\}$ $(1 \le i \le m; 1 \le j \le n)$ forms a self-dual normal basis for L/K.*

Proof. Since

$$\begin{aligned} \mathrm{tr}_{L/K}(a_i b_j a_k b_l) &= \mathrm{tr}_{F/K}(b_j b_l \, \mathrm{tr}_{L/F}(a_i a_k)) \\ &= \delta_{jl}\delta_{ik}\,, \end{aligned}$$

for $1 \le i, k \le m$, and $1 \le j, l \le n$, the conditions to be self-dual normal basis are satisfied. Since L is $G-$Galois extension of K, where $G = G_1 \times G_2$ is the direct product of two subgroups G_1 and G_2, then L is the composite of two Galois extensions with their intersection equal to K. The lemma follows. □

Theorem 6.2. *Let $G = \mathbb{Z}/m_1\mathbb{Z} \times \cdots \times \mathbb{Z}/m_s\mathbb{Z}$ be a finite abelian group of odd order, $n = lcm(m_1, \cdots, m_s)$ be the exponent of G, K be a field containing a* *primitive nth root of unity, and let* $L = K(\sqrt[m_1]{r_1}, \cdots, \sqrt[m_s]{r_s})$ *be a* $G-$*Galois extension for some* $r_1, \cdots, r_s \in K$. *Then* $\{g(x_1 \cdots x_s) \,|\, g \in G\}$ *forms a self-dual normal basis of* L *over* K, *where for each* $j = 1, \cdots, s$, $t_j = (m_j - 1)/2$, $c_{j\,i} \in K^*(i = 1, \cdots, t_j)$, $\alpha_j = \sqrt[m_j]{r_j} \in L$, *and*

$$x_j = m_j^{-1}(1 + c_{j\,1}\alpha_j + \cdots + c_{j\,t_j}\alpha_j^{t_j} + (r_j c_{j\,1})^{-1}\alpha_j^{t_j+1} + \cdots + (r_j c_{j\,t_j})^{-1}\alpha_j^{m_j-1}).$$

Proof. Consider the intermediate extensions

$$L = K(\sqrt[m_1]{r_1}, \cdots, \sqrt[m_s]{r_s}) \supset \cdots \supset K(\sqrt[m_s]{r_s}) \supset K,$$

since each intermediate field extension has a primitive *nth* root of unity. If each cyclic intermediate Galois extension has a self-dual normal basis, the proof follows from the Lemma 6.1. Hence it is enough to show the following lemma.

Lemma 6.3. *Let* G *be a finite cyclic group of odd order* n, K *be a field containing a primitive nth root of unity, and let* $L = K(\sqrt[n]{r})$ *be a* $G-$*Galois extension for some* $r \in K$. *Then* $\{g(x) \,|\, g \in G\}$ *forms a self-dual normal basis of* L *over* K, *where* $\alpha = \sqrt[n]{r} \in L$, $t = (n-1)/2$, $c_i \in K^*(i = 1, \cdots, t)$, *and*

$$x = n^{-1}(1 + c_1\alpha + \cdots + c_t\alpha^t + (rc_1)^{-1}\alpha^{t+1} + \cdots + (rc_t)^{-1}\alpha^{n-1}).$$

To prove the lemma, let $\zeta = \zeta_n$ be a primitive *nth* root of unity in K, and $G = \langle\sigma\rangle$. Then for $i = 1, \cdots, n-1$,

$$\begin{aligned} \sigma(\alpha^i) &= \zeta^i\alpha^i \\ \mathrm{tr}_{L/K}(\sigma(\alpha^i)) &= \mathrm{tr}_{L/K}(\zeta^i\alpha^i) = \zeta^i\mathrm{tr}_{L/K}(\alpha^i). \end{aligned}$$

Since $\mathrm{tr}_{L/K}(\alpha^k(\beta)) = \mathrm{tr}_{L/K}(\beta)$ for any $\beta \in L$ and $k \in \mathbb{Z}$, then for each $i = 1, \cdots, n-1$,

$$\mathrm{tr}_{L/K}(\alpha^i) = \zeta^i\mathrm{tr}_{L/K}(\alpha^i).$$

Hence $\mathrm{tr}_{L/K}(\alpha^i) = 0$ for all $i = 1, \cdots, n-1$. Let $y = a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1}$, where $a_j \in K$. Then we have

$$y^2 = a_0^2 + ra_1a_{n-1} + ra_2a_{n-2} + \cdots + ra_{n-1}a_1 + f_0(\alpha)\,,$$

and for each $k = 1, \cdots, n-1$,

$$y \cdot \sigma^k(y) = a_0^2 + ra_1a_{n-1}\zeta^{k\cdot(n-1)} + \cdots + ra_{n-1}a_1\zeta^{k\cdot 1} + f_k(\alpha)\,,$$

where $f_0(\alpha)$ and $f_k(\alpha)$ have no constant terms in $K[\alpha]$. The system of equations (5.1) can be written as

$$\begin{aligned}
\mathrm{tr}_{L/K}(y^2) &= n(a_0^2 + 2ra_1a_{n-1} + \cdots + 2ra_ta_{t+1}) = 1 \\
\mathrm{tr}_{L/K}(y \cdot \sigma^k(y)) &= n(a_0^2 + r(\zeta^{k\cdot 1} + \zeta^{k\cdot(n-1)})a_1a_{n-1} + \cdots \\
&\quad \cdots + r(\zeta^{k\cdot t} + \zeta^{k\cdot(t+1)})a_ta_{t+1}) = 0
\end{aligned}$$

for $k = 1, \cdots, n-1$. Let

$$x = n^{-1}(1 + c_1\alpha + \cdots + c_t\alpha^t + (rc_1)^{-1}\alpha^{t+1} + \cdots + (rc_t)^{-1}\alpha^{n-1})\,, \tag{6.1}$$

where the c_i are arbitrary elements in K^*. Then x is in L and

$$\mathrm{tr}_{L/K}(x^2) = n[(\frac{1}{n})^2(1 + 2 + \cdots + 2)] = 1$$

$$\mathrm{tr}_{L/K}(x \cdot \sigma^k(x)) = n[(\frac{1}{n})^2 \sum_{j=0}^{n-1} \zeta^{k\cdot j}] = 0$$

for $k = 1, \cdots, n-1$ (this geometric series sums to $\frac{1-(\zeta^k)^n}{1-\zeta^k} = 0$ because $\zeta^{k\cdot n} = 1$ and $\zeta^k \neq 1$). Hence x is a solution of the system of equations (5.1). Moreover, the set $\{g(x) | g \in G\}$ is linearly independent because nonzero mutually orthogonal vectors are linear independent. This completes the proof of Lemma 6.3 and thus of Theorem 6.2. □

7. Generalized Trace Forms of Galois Field Extensions

Throughout this section, we assume that K contains a copy of an algebraically closed field k, unless otherwise specified. Let G be a finite group, L/K be a $G-$Galois field extension. We recall the generalized trace form $T_a : L \times L \to K$ defined by

$$x \mapsto \sum_{\sigma \in G} a_\sigma \mathrm{tr}_{L/K}(x\sigma(x)),$$

for every choice of constants $a_\sigma \in K$ for which the trace form T_a is nonsingular.

We will determine whether or not the generalized trace form of Galois field extension is equivalent to the usual trace form $x \mapsto \mathrm{tr}_{L/K}(x^2)$.

Let G be a finite group, let and V be an 1-dimensional vector space over k, where $\{b\}$ is a basis of V over k. Suppose $\phi : G \to \mathrm{GL}(V)$ is a representation defined by, for each $\sigma \in G$,

$$\phi(\sigma) = \phi_\sigma \in \mathrm{GL}(V)$$

$$\phi_\sigma(b) = \chi(\sigma)b,$$

where $\chi : G \to k^*$ is a character of G. Note that $\chi(\sigma) \neq 0$ because σ induces an automorphism of V. Since G is finite, for each $\sigma \in G$, there exists a positive integer n such that $\sigma^n = id$ and

$$\chi(\sigma)^n = \chi(\sigma^n) = \chi(id) = 1.$$

Hence the values of 1-dimensional characters are certain roots of unity. Here we will consider the case where G is a finite abelian group.

Lemma 7.1. *Let G be a finite group and L/K be a $G-$Galois extension. Then*

(1) *L is isomorphic to the regular representation V_{reg} as a K-representation of G.*

(2) *Suppose G is an abelian group of exponent e and K contain a primitive eth root of unity. Then V_{reg} is isomorphic to the direct sum of the characters of G; each character appears with multiplicity* 1.

Proof. (1) is equivalent to the normal basis theorem. Indeed, V_{reg} is, by definition, a $|G|$-dimensional vector space with a basis $\{e_h | h \in G\}$, where the $G-$action on V_{reg} is given by linearly extending $g(e_h) = e_{gh}$ to all of V_{reg}. If $\{h(\alpha) | h \in G\}$ is a normal basis of L/K for some $\alpha \in L$ then there is an isomorphism of representations given by $e_h \mapsto h(\alpha)$. Conversely, if $\phi : V_{\mathrm{reg}} \to L$ is an isomorphism of $K-$representations then $\phi(e_h)$ is a normal basis of L/K.

(2) follows from [26, 12.2.15]. □

Let G be a finite abelian group, L/K be a $G-$Galois field extension, and let G^* be a set of all characters of G. By Lemma 7.1

$$L \simeq \oplus_{\chi \in G^*} L(\chi),$$

where $L(\chi) = \{\alpha | \sigma(\alpha) = \chi(\sigma)\alpha \text{ for all } \sigma \in G\}$, and $\dim_K L(\chi) = 1$.

For a convenience, we abbreviate the trace form $\mathrm{tr}_{L/K}$ for L/K by tr, unless otherwise specified and for each $\chi \in G^*$ we will denote b_χ a basis element of $L(\chi)$.

Lemma 7.2. *For each $\chi_1, \chi_2 \in G^*$,*

$$\mathrm{tr}(b_{\chi_1} b_{\chi_2}) = \begin{cases} 0 & \text{if } \chi_2 \neq {\chi_1}^{-1} \\ |G| b_{\chi_1} b_{{\chi_1}^{-1}} & \text{if } \chi_2 = {\chi_1}^{-1}. \end{cases}$$

Proof. For any $\sigma \in G$,

$$\mathrm{tr}(b_{\chi_1} b_{\chi_2}) = \mathrm{tr}(\sigma(b_{\chi_1}) \sigma(b_{\chi_2})) = \mathrm{tr}(\chi_1(\sigma) \chi_2(\sigma) b_{\chi_1} b_{\chi_2}) = \chi_1(\sigma)\chi_2(\sigma)\mathrm{tr}(b_{\chi_1} b_{\chi_2}).$$

If $\chi_1(\sigma)\chi_2(\sigma) = 1$ for all $\sigma \in G$, i.e., $\chi_2 = {\chi_1}^{-1}$, then

$$\begin{aligned}\mathrm{tr}(b_{\chi_1}\, b_{\chi_1^{-1}}) &= \sum_{\sigma\in G} \sigma(b_{\chi_1} b_{\chi_1^{-1}}) = \sum_{\sigma\in G} \chi_1(\sigma){\chi_2}^{-1}(\sigma) b_{\chi_1} b_{\chi_2^{-1}} \\ &= \sum_{\sigma\in G} b_{\chi_1} b_{\chi_1^{-1}} = |G| b_{\chi_1} b_{\chi_1^{-1}}\,;\end{aligned}$$

otherwise $\mathrm{tr}(b_{\chi_1} b_{\chi_2}) = 0$. □

Note that for all $g \in G$,

$$g(b_\chi b_{\chi^{-1}}) = \chi(g)\chi^{-1}(g) b_\chi b_{\chi^{-1}} = b_\chi b_{\chi^{-1}}\,,$$

i.e., $b_\chi b_{\chi^{-1}} \in K$.

Let $\sigma \in G$, define $B_\sigma : L \times L \to K$ by

$$B_\sigma(x, y) = \frac{1}{2}\mathrm{tr}(x\sigma(y) + y\sigma(x))\,.$$

Then B_σ will be a symmetric $K-$bilinear form over K.

Lemma 7.3. *For each $\sigma \in G$, and $\chi_1, \chi_2 \in G^*$,*

$$B_\sigma(b_{\chi_1}, b_{\chi_2}) = \begin{cases} 0 & \textit{if } \chi_2 \neq {\chi_1}^{-1} \\ \frac{|G|}{2}(\chi_1(\sigma) + {\chi_1}^{-1}(\sigma)) b_{\chi_1} b_{\chi_1^{-1}} & \textit{if } \chi_2 = {\chi_1}^{-1}\,. \end{cases}$$

Proof.

$$\begin{aligned}B_\sigma(b_{\chi_1}, b_{\chi_2}) &= \frac{1}{2}\mathrm{tr}(b_{\chi_1} \cdot \sigma(b_{\chi_2}) + b_{\chi_2} \cdot \sigma(b_{\chi_1})) \\ &= \frac{1}{2}\mathrm{tr}(\chi_2(\sigma) b_{\chi_1} b_{\chi_2} + \chi_1(\sigma) b_{\chi_1} b_{\chi_2}) = \frac{1}{2}(\chi_1(\sigma) + \chi_2(\sigma))\mathrm{tr}(b_{\chi_1}\, b_{\chi_2})\,.\end{aligned}$$

The desired results follow from Lemma 7.2. □

For each $\chi \in G^*$, define $c_\chi = \sqrt{\frac{1}{2}(\chi(\sigma) + \chi^{-1}(\sigma))}\; b_\chi$. Then $\{c_\chi | \chi \in G^*\}$ forms a new basis of L over K. Then the Gram matrix of B_σ in the basis $\{b_\chi | \chi \in G^*\}$ and the Gram matrix of the usual trace form in the basis $\{c_\chi | \chi \in G^*\}$ are equivalent up to change of bases. Hence we have the following result:

Lemma 7.4. *Let G_r be a Gram matrix of the usual trace form in the basis $\{c_\chi | \chi \in G^*\}$. Then for each $\sigma \in G$, the Gram matrix M_σ of B_σ is*

$$M_\sigma = D_\sigma G_r D_\sigma^t ,$$

where $D_\sigma = (d^\sigma_{\chi_1,\chi_2})_{\chi_1,\chi_2 \in G^*}$ with all $d^\sigma_{\chi_1,\chi_2} \in K$, and

$$d^\sigma_{\chi_1,\chi_2} = \begin{cases} 0 & \text{if } \chi_2 \neq {\chi_1}^{-1} \\ \sqrt{\frac{1}{2}(\chi_1(\sigma) + {\chi_1}^{-1}(\sigma))} & \text{if } \chi_2 = {\chi_1}^{-1} . \end{cases}$$

Theorem 7.5. *Let L be a Galois extension of K with a Galois group G which is an abelian group. Then the generalized trace form and the usual trace form are equivalent.*

Proof. Let $\{b_\chi | \chi \in G^*\}$ be a basis of L over K. Then for any $\chi_1, \chi_2 \in G^*$, we have

$$\begin{aligned} T_a(b_{\chi_1} b_{\chi_2}) &= \sum_{\sigma \in G} a_\sigma B_\sigma(b_{\chi_1}, b_{\chi_2}) \\ &= \begin{cases} 0 & \text{if } \chi_2 \neq {\chi_1}^{-1} \\ \frac{1}{2}\sum_{\sigma\in G} a_\sigma(\chi_1(\sigma) + {\chi_2}^{-1}(\sigma))\mathrm{tr}(b_{\chi_1} b_{{\chi_2}^{-1}}) & \text{if } \chi_2 = {\chi_1}^{-1} , \end{cases} \end{aligned}$$

where all $a_\sigma(\chi_1(\sigma) + {\chi_2}^{-1}(\sigma))$ are in K. Let for each $\chi \in G^*$,

$$\gamma_\chi = \frac{1}{2}\sum_{\sigma \in G} a_\sigma(\chi(\sigma) + \chi^{-1}(\sigma)) .$$

Then we have a new basis $\{c_\chi = \sqrt{\gamma_\chi}\, b_\chi | \chi \in G^*\}$. Let $P = (p_{\chi_1,\chi_2})$ be a matrix over K such that

$$p_{\chi_1,\chi_2} = \begin{cases} 0 & \text{if } \chi_2 \neq {\chi_1}^{-1} \\ \sqrt{\gamma_{\chi_1}} & \text{if } \chi_2 = {\chi_1}^{-1} . \end{cases}$$

Hence we have $M_a = P G_r P^t$, where M_a is the generalized Gram matrix in the basis $\{b_\chi | \chi \in G^*\}$ and G_r is the usual Gram matrix in the basis $\{c_\chi | \chi \in G^*\}$. Thus two trace forms are equivalent up to change of bases. □

BIBLIOGRAPHY

[1] J.L. Alperin, Rowen B. Bell *Groups and Representations*, Springer, 1995.

[2] E. Bayer-Fluckiger, *Self-dual normal bases*, Indag. Math., **51** (1989), 379–383.

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

[4] E. Bayer-Fluckiger, H. W., Jr. Lenstar, *Forms in odd degree extensions and self-dual normal bases*, Amer. J. Math. **112** (1990),no.3, 359–373.

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

[6] P.E. Conner, R. Perlis, *A Survey of Trace Forms of Algebraic Number Fields*, World Scientific, Singapore, 1984.

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

[8] D. S. Dummit and R. M. Foote, *Abstract Algebra*, Prentice-Hall, 1991.

[9] M. Epkenhans, *Trace forms of normal extensions of algebraic number fields*, Lin. Multilin. Algebra **25** (1989), 309–320.

[10] V. P. Gallagher, *Local trace forms*, Lin. Multilin. Algebra **7** (1979), 167–174.

[11] C. Hermite, *Extrait d'une lette de Mr. ch. Hermite de paris à Mr. Borchardt de Berlin sur le nombre des racines d'une équation algébrique comprises entre des limites données* J. Reine angew. Math. **52** (1856), 39–51.

[12] C. Hermite, *Extrait d'une lettre des M.C. Hermite à M. Borchardt sur l'invariabilité du nombres des carrés positifs et des carrés négatifs dans la transformation des polynômes homogères du second degré* J. Reine angew. Math. **53** (1857), 271–274.

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

[14] K. Imamura, *On Self-complementary bases of* $GF(q^n)$ *over* $GF(q)$ Trans. IECE Japan(section E) E66, **121**(1983), 717–721.

[15] K. Imamura and M. Morii, *Two classes of finite fields which have no Self-complementary norma bases* IEEE International Symposium on Information Theory, Brighton, England, June 1985.

[16] C.G. Jacobi,*Uber einen algebraischen Fundamentalsatz und seine Anwendungen (Aus den hinterlassenen Papieren von C.G. J. Jacobi migethelt durch C. W. Borchardt).*, J. Reine Angew. Math. bf 53 (1857), 275–280.

[17] D.-S. Kang, Z. Reichstein, *Trace forms of Galois field extensions in the presence of roots of unity*, Reine Angew. Math., to appear.

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

[19] S. Lang, *Algebra*, third edition, Addison-Wesley, 1993.

[20] A. Lempel, M. J. Weinberger, *Self-complementary normal basis in finite fields*, SIAM J. Disc. Math. **1** (1988), no.2, 193–198.

[21] F.J. MacWilliams and N.J.A. Sloane *The theory of Error-Correcting Codes*, North-Holland, Amsterdam, 1977.

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

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

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

[25] D. J. S. Robinson, *A Course in the Theory of Groups*, second edition, Springer-Verlag, New York, 1996.

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