J. Korean Soc. Math. Educ. Ser. B: Pure Appl. Math. ISSN(Print) 1226-0657
http://dx.doi.org/10.7468/jksmeb.2016.23.1.53 ISSN(Online) 2287-6081
Volume 23, Number 1 (February 2016), Pages 53–59

ON TRACE FORMS OF GALOIS EXTENSIONS

Dong Seung Kang

Abstract. Let G be a finite group containing a non-abelian Sylow 2-subgroup. We elementarily show that every G-Galois field extension L/K has a hyperbolic trace form in the presence of root of unity.

1. Introduction

Let K be a field containing a primitive 4th root of unity with $\mathrm{char}(K) \neq 2$. The trace form of a finite field extension (or, more generally of an etale algebra) L is the nonsingular quadratic form $q_{L/K} \colon x \mapsto \mathrm{tr}_{L/K}(x^2)$ defined over K. In this paper we will be concerned with the following general question:

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

Question 1.1 was studied in the mid-19th century; in particular, Sylvester [14], Jacobi [7], and Hermite [5], [6] 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 $\mathbb{R}[x]/(p(x))$; see [1, 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 [13], relating the trace form to the extension problem in inverse Galois theory.

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 [4, p. 222]. But the situation simplifies considerably if we require K to contain certain roots of unity.

Definition 1.2. Let (V, q) be a 2-dimensional nonsingular quadratic space over a field K. The q is said to be *hyperbolic* if it satisfies $q \simeq \langle 1, -1 \rangle$. Moreover, (V, q)

Received by the editors January 09, 2016. Accepted January16, 2016.
2010 *Mathematics Subject Classification.* 11E04, 12F05.
Key words and phrases. trace forms, quadratic forms, hyperbolic, field extension, Galois extension.

is called a *hyperbolic plane*. In general, an orthogonal sum of hyperbolic planes is called a *hyperbolic space*.

We write $\langle\langle a_1, \cdots, a_n\rangle\rangle$ to denote the n-fold Pfister form $\langle 1, a_1\rangle \otimes \cdots \otimes \langle 1, a_n\rangle$ and $q^a_{L/K}$ is denoted by scaled trace form $x \mapsto \mathrm{tr}_{L/K}(ax^2)$, where $a \in K^*$.

Theorem 1.3 ([8, Theorem 1.1])**.** *Let L/K be a G-Galois extension and let G_2 be the 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 $\exp(H)$, as H ranges over all non-abelian subgroups of G_2.

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

Assuming only that K contains a primitive 4th root of unity, Mináč and Reichstein completely described the finite groups G which admit a $G-$Galois extension L/K with a non-hyperbolic trace form; see [9, Theorem 1.3].

In view of [8, Reduction 3.3], the Theorem 1.3 reduced to the following Theorem 1.4 :

Theorem 1.4. *Let G be a non-abelian 2-group of exponent d. Then for every $G-$Galois field extension L/K, the trace form $q_{L/K}$ is hyperbolic, provided K contains a primitive dth root of unity.*

In [8], Theorem 1.4 was proved by contradiction with a counterexample of minimal order, say G_{min}, and then [8, Propostion 4.6] gave us that $G_{min} = Q_8$ or $M(2n)$, where $n \geq 8$ is a power of 2. The proof of [8, Proposition 4.6] relied on an old group-theoretic result of Rèdei [10], which is actually a bit stronger that what we needed; see [8, Lemma 4.5].

In this paper we will reprove Theorem 1.3. The approaches are in order: first of all, we will investigate the properties of G_{min} without using the result of Rèdei and then by using these properties we will produce that $G_{min} = M(2n)$, where $n \geq 8$ is a power of 2. Finally, we will also show that the quadratic form of $M(2n)$ Galois extension L/K is hyperbolic, provided K contains a primitive nth root of unity.

2. Main Results

Throughout this paper the characteristic of any field K is not equal to 2.

Definition 2.1. 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.

2.1. Properties of G_{min} Let G_{min} be a counterexample of minimal order of Theorem 1.4.

Theorem 2.2. *(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) Immediate from [8, Proposition 3.5 (a)].

(b) Let H be a subgroup of index 2 in G_{min}; see, e.g., [11, 5.3.1(ii)]. Choose $g \in G_{min} \backslash H$; applying [11, 5.3.1(ii)] once again, we can find a subgroup $H' \subset G_{min}$ such that $q \in H'$ and $[G_{min} : H'] = 2$. By part (a) both H and H' are abelian. Thus every $x \in H \cap H'$ commutes with g and with every element of H. Since H and g generate G, we conclude that $x \in Z(G)$, i.e.,

$$H \cap H' \subset Z(G_{min})\,. \tag{2.1}$$

Since G_{min} is non-abelian,

$$[G_{min} : Z(G_{min})] \geq 4\,; \tag{2.2}$$

see, e.g., [12, 6.3.4]. On the other hand, since $[G_{min} : H] = [G_{min} : H'] = 2$, it is easy to see that

$$[G_{min} : (H \cap H')] = 4\,. \tag{2.3}$$

Part (b) now follows from (2.1-2.3). For future reference we remark that our argument also shows that

$$H \cap H' = Z(G_{min})\,. \tag{2.4}$$

(c) By [11, 5.3.1(ii)], S is contained in a subgroup H of index 2. By (2.4), $Z(G) = H \cap H'$, where H' is another subgroup of G of index 2. Then $S \cap Z(G) = S \cap H'$, and the latter clearly has index ≤ 2 in S.

(d) Apply part (c) to the cyclic group $S = \langle x \rangle$.

(e) Follows from the fact that the factor group $G_{min}/Z(G_{min})$ has order 4 and, hence, is abelian.

(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 of orders n and 2 respectively. By part (d), H_0 is central and, hence, normal in G_{min}. By [8, Proposition 3.5 (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,

$$G'_{min} \subset H_0\,. \tag{2.5}$$

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

(h) 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 groups of order ≤ 8 and the dihedral group D_8 and 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 [3, Section 6, Exemple] or [4, 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 [3, Section 6, Exemple] or [4, 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 $|G_{min}| \geq 16$. □

2.2. 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,

$$M(2n) = \{x, y \,|\, x^n = y^2 = 1, yx = x^{n/2+1}y\}\,. \tag{2.6}$$

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

Theorem 2.3. *$G_{min} = M(2n)$ for some $n \geq 8$.*

Proof. Write $G_{min} = \langle r, s\rangle$, $G'_{min} = \{1, c\}$, and $sr = crs$. 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 Theorem 2.2(i).

Thus $n \geq 4$. By Theorem 2.2(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 Theorem 2.2(i). If $(n, m) = (4, 4)$ then by Theorem 2.2(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., [12, Example 8.2.4]. Hence there exists a surjecive homomorphism $Q_8 \longrightarrow G_{min}$, and thus $|G_{min}| \leq |Q_8| = 8$, once again contradicting Theorem 2.2(i).

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

$$\widetilde{s}^{\frac{m}{2}} = 1 \tag{2.7}$$

Indeed, recall that $r^{n/2} = s^{m/2} = c$; see Theorem 2.2(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 Theorem 2.2(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 Theorem 2.2(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 (2.7), $\widetilde{s}$ 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 (2.6)), there exists a surjective homomorphism $M(2n) \longrightarrow G_{min}$. By [8, Lemma 4.4 (b)], this homomorphism is an isomorphism. This completes the proof of Theorem 2.3. □

2.3. Trace form of $M(2n)$-Galois extension In this section we will show the quadratic form of a $M(2n)$-Galois extension is hyperbolic. Hence it complete the proof of Theorem 1.4 (and thus of Theorem 1.3). We introduce a notation. If G is a group and $j \geq 1$ is an integer, then $G^j = \langle g^j | g \in G\rangle$ and it is a normal subgroup of G.

Lemma 2.4. *Let $n \geq 8$. $M(2n)^n = \langle 1\rangle$.*

Proof. Assume $y \in M(2n)^n$, we have $y = (s^a r^b)^n$, where $a = 0$ or 1. If $a = 0$ then $y = (r^b)^n = (r^n)^b = 1$. If $a = 1$ then

$$y = (sr^b)^n = (sr^b)^{2\frac{n}{2}} = (r^{\frac{n}{4}+2})^{b\frac{n}{2}} = (r^n)^{b(\frac{n}{8}+1)} = 1.$$

Thus $M(2n)^n = \langle 1\rangle$, as desired. □

Proposition 2.5. *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.*

Proof. Assume $q_{L/K}$ is not hyperbolic. Then the quotient group $M(2n)/M(2n)^n = M(2n)$ is not abelian. This is a contradiction to [9, Theorem 1.3]. □

Remark 2.6. By [9, Theorem 1.3], we can also conclude that condition (b) of Theorem 1.3 cannot be substantially weakened. Indeed, for any power of 2 ($2 \leq j \leq \frac{n}{2}$) $M(2n)^j$ is a normal subgroup of $M(2n)$. Then the quotient group $M(2n)/M(2n)^j$ is abelian.

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 & H.W. Lenstar Jr.: Forms in odd degree extensions and self-dual normal bases. *Amer. J. Math.* **112** (1990), no. 3, 359-373.

3. E. Bayer-Fluckiger & J.-P. Serre: Torsions quadratiques et bases normales autoduales. *Amer. J. Math.* **116** (1994), 1-64.
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. 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.
6. _____: 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.
7. 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.* **53** (1857), 275-280.
8. D.-S. Kang & Z. Reichstein: Trace forms of Galois field extensions in the presence of roots of unity. *J. Reine angew. Math.* **549** (2002), 79-89.
9. J.Ináč & Z. Reichstein: Trace forms of Galois extensions in the presence of a fourth root of unity. *Int. Math. Research Notices* **8** (2004) 389-410
10. L. Rédei: Das schiefe Produkt in der Gruppentheorie. *Comment. Math. Helvet.* **20** (1947), 225-267.
11. D.J.S. Robinson: *A Course in the Theory of Groups*. second edition, Springer-Verlag, New York, 1996.
12. W.R. Scott: *Group Theory*. Dover Publications, Inc., 1987.
13. J.-P. Serre: L'invariant de Witt de la forme $Tr(x^2)$. *Comm. Math. Helv.* **59** (1984), 651-676.
14. S. Sylvester: On the theory of syzygetic relations integral functions, comprising an application to the theory of Sturm's functions, and that of the greatest algebraic common measure. *Phil. Trans. of the Royal Society of London* **148** (1853), 407-548.

Department of Mathematical Education, Dankook University, Yongin, Gyeonggi, 448-701, Korea
Email address: dskang@dankook.ac.kr