Canad. Math. Bull. Vol. 28(4), 1985

ON THE ANALYTIC DETERMINATION OF THE TRACE FORM

BY
ROBERT PERLIS

Dedicated to the memory of Robert Arnold Smith

ABSTRACT. The Dedekind zeta function of an algebraic number field E determines the rational equivalence class of the trace form of E. The Hasse symbols of the trace form are related to the local Artin root numbers of the zeta function by formulas of Serre and Deligne. This is used to settle the question of which families of complex numbers appear as the local Artin root numbers of a continuous real representation of the absolute Galois group of $\mathbb{Q}$.

1. **Introduction**. The trace form of an algebraic number field E is the quadratic form

$$q_{E/\mathbb{Q}}(X) = \mathrm{trace}_{E/\mathbb{Q}}(X^2).$$

In this paper we prove a general result about permutation representations (Theorem 1) which implies that two algebraic number fields have rationally equivalent trace forms when their zeta functions coincide. The main ingredient in the proof is Serre's topological formula for the Hasse symbols of the trace form.

Combining Serre's formula with another of Deligne yields an explicit connection between the Hasse symbols of the trace form $q_{E/\mathbb{Q}}$ and the local Artin root numbers of the Galois representation defining the zeta function of E. This not only gives an analytic/arithmetic interpretation for the Hasse symbols, but also yields a general result about the root numbers. Namely, it allows the determination of those families of complex numbers which appear as the local Artin root numbers of some real (continuous) representation of the absolute Galois group $G_{\mathbb{Q}} = \mathrm{Gal}\,(\bar{\mathbb{Q}}/\mathbb{Q})$. No similar realization theorem is presently known for the local root numbers of complex representations. The proof of the realization theorem for real representations depends in an essential way on the recent characterization of trace forms in the rational Witt ring $W(\mathbb{Q})$, given in [1]. As a consequence of the realization theorem, it follows that the local Artin root numbers of any real representation are the local Artin root numbers of the very special real representations corresponding to the Dedekind zeta functions of algebraic number fields.

I would like to thank J.-P. Serre for his comments, and P. E. Conner for his suggestions concerning Section 3.

Received by the editors March 26, 1985 and, in revised form, May 13, 1985.
AMS Subject Classification (1980): 10C02.

https://doi.org/10.4153/CMB-1985-051-2 Published online by Cambridge University Press

2. **Representations and Forms**. Let K be a field of characteristic $\neq 2$ and let f be a polynomial over K with simple roots. Then the étale K-algebra

$$E = K[X]/(f)$$

is a direct sum of field extensions E_i/K, and $\Sigma_i\,[E_i : K] = n$, the degree of f. The Galois group $G_K = \mathrm{Gal}\,(\bar{K}/K)$ of the separable closure $\bar{K}$ over K permutes the roots of f, inducing a permutation representation

$$\pi_{E/K} : G_K \to S_n$$

which is transitive if and only if f is irreducible over K. We may consider $\pi_{E/K}$ as a 1-cocycle of a class in $H^1(G_K, S_n)$. Since the symmetric group S_n is not commutative when $n > 2$, H^1 is not itself a group but is only a set of cohomology classes of cocycles. It is useful to recall the definition of $H^1(G_K, A)$ for any group A on which the profinite group G_K acts. The cocycles are the continuous maps $c : G_K \to A$ satisfying $c(st) = (sc(t))c(s)$ for all s, t in G_K. Two cocycles c and c' are cohomologous when there is a fixed element a in A for which $c(s) = (sa)c'(s)a^{-1}$ for all s in G_K. Then $H^1(G_K, A)$ is the resulting set of cohomology classes of cocycles. Consider now the commutative diagram

(1)

$$\begin{tikzcd}
H^1(G_K, O_n(\bar{K})) \arrow[r] & H^1(G_K, GL_n(\bar{K})) = \{1\} \\
\bar{\pi}_{E/K} \in H^1(G_K, S_n) \arrow[u, "i"] \arrow[r, "j"] & H^1(G_K, GL_n(\mathbb{R})) \arrow[u, "\text{trivial}"']
\end{tikzcd}$$

in which G_K operates on a matrix group by its Galois action on the entries. Here, G_K acts trivially on the field of real numbers $\mathbb{R}$, and the arrows i and j are obtained by replacing each permutation in the symmetric group S_n by its effect on the rows of the identity matrix I_n. The upper right corner of this diagram vanishes; for $n = 1$ this is Hilbert's Theorem 90. The permutation representation $\pi_{E/K}$ defined above is a 1-cocycle in the lower left corner. Its image $j(\pi_{E/K})$ in the lower right corner is a linear representation

$$\rho_{E/K} = j(\pi_{E/K})$$

of G_K. For s in G_K the character value $\mathrm{trace}(\rho_{E/K}(s))$ counts the number of fixed points of s acting on the roots of the polynomial f. The cohomology class of $\rho_{E/K}$ is the isomorphism class of the representation $\rho_{E/K}$.

By definition, the trace form of the K-algebra $E = \bigoplus E_i$ is the direct sum of forms $q_{E/K} = \bigoplus q_{E_i/K}$, where the trace form of the separable field extension E_i/K is

$$q_{E_i/K}(X) = \mathrm{trace}_{E_i/K}(X^2)$$

for X in E_i.

LEMMA 1: (a) $H^1(G_K, O_n(\bar{K}))$ *classifies the set of non-degenerate quadratic forms of rank n over K, up to K-rational equivalence.*

https://doi.org/10.4153/CMB-1985-051-2 Published online by Cambridge University Press

(b) *The image* $i(\bar{\pi}_{E/K})$ *is the K-rational equivalence class of the trace form* $q_{E/K}$.

PROOF: Part (a) is well known, but we need the details of the identification, so we give a proof. Take a cocycle c in $H^1(G_K, O_n\bar{K}))$ and map it horizontally right. Since the group $H^1(G_K, GL_n(\bar{K}))$ vanishes, the image of c is cohomologous to the identity, so $c(s) = s(B)B^{-1}$ for all s in G_K and for some fixed matrix B in $GL_n(\bar{K})$. Set $M = (B^t)B$. Then M is a symmetric matrix. Using the fact that $c(s)$ lies in $O_n(\bar{K})$ for all s, one checks that each element s of G_K fixes M. So M has coefficients in K, and defines a non-degenerate quadratic form over K. Another cocycle from the same class evidently gives rise to a K-rationally equivalent quadratic form. Following this argument backwards shows that every non-degenerate K-rational form of rank n arises in this way.

To prove (b) it suffices to consider the case $E = E_1$, the case when f is irreducible over K. In this case the matrix of the trace form $q_{E/K}$ is $(C^t)C$ where

$$C = (s_i(\theta_j)). \tag{2}$$

Here the θ_j's are the roots of f and the s_i's are the n embeddings of E into K. Now just re-read the proof of part (a). □

This then is the relationship of the trace form $q_{E/K}$ to the representation $\rho_{E/K}$: starting with the 1-cocycle $\pi_{E/K}$ and mapping horizontally right, we obtain the linear representation $\rho_{E/K} = j(\pi_{E/K})$, and mapping $\pi_{E/K}$ vertically gives the trace form $q_{E/K} = i(\pi_{E/K})$.

Now recall four important invariants of a quadratic form q over K. The rank of q is the number of variables of the form. The discriminant dis(q) is the determinant of any matrix defining q, read modulo squares in K^*. If K has embeddings into the field $\mathbb{R}$ of real numbers, then each embedding gives rise to a signature of q, obtained by diagonalizing the image of q under the given embedding and then subtracting the number of negative diagonal elements from the number of positive diagonal elements. Finally there is the Hasse invariant $h(q)$ in the Brauer group Br(K). For this, diagonalize q over K to obtain $a_1X_1^2 + \ldots + a_nX_n^2$. Then $h(q)$ is the Brauer class of the tensor product

$$\prod_{i<j} (a_i, a_j)$$

of the quaternion algebras (a_i, a_j) over K. When K is an algebraic number field, the Brauer class $h(q)$ is determined by its local invariants, so in this case $h(q)$ can be thought of as a collection $\{h_p(q)\}$, where the p runs over all primes of K, including ∞, and $h_p(q) = \pm 1$ is the local invariant at p of $h(q)$. This local invariant $h_p(q)$ can be identified with

$$\prod_{i<j} (a_i, a_j)_p$$

where $(a_i, a_j)_p$ is the classical Hilbert symbol, defined by

$$(a_i, a_j)_p = \begin{cases} 1 & \text{if } a_iX^2 + a_jY^2 \text{ represents } 1 \text{ in } K_p \\ -1 & \text{otherwise} \end{cases}$$

https://doi.org/10.4153/CMB-1985-051-2 Published online by Cambridge University Press

where K_p is the completion of K at p.

For trace forms $q_{E/K}$ these basic four invariants can be read as follows:

rank $(q_{E/K}) = \dim_K(E) =$ degree of f.

dis $(q_{E/K}) = \prod_i \mathrm{Dis}(E_i/K)$, modulo squares in K^*. Here $\mathrm{Dis}(E_i/K)$ denotes the discriminant of any field basis of E_i/K.

If $\sigma : K \to \mathbb{R}$ is an embedding of K into the reals (there may be none), then $\mathrm{sgn}_\sigma(q_{E/K}) =$ number of real roots of the embedded polynomial $\sigma(f)$.

This signature statement is a trivial generalization of a theorem of O. Taussky–Todd (see [10]).

It remains to find an interpretation for the Hasse invariant $h(q_{E/K})$. In the next section, this invariant will be related to local Artin root numbers, when E/K is an extension of algebraic number fields. Here we will give Serre's topological interpretation for the Hasse invariant.

The horizontal map $j : H^1(G_K, S_n) \to H^1(G_K, GL_n(\mathbb{R}))$ in diagram (1) factors through the orthogonal group:

$$H^1(G_K, S_n) \xrightarrow{j_0} H^1(G_K, O_n(\mathbb{R})) \xrightarrow{j_1} H^1(G_K, GL_n(\mathbb{R}))$$

so $j = j_1 \circ j_0$. The next lemma states simply that j_1 is injective.

LEMMA 2: *Let G be a profinite group and let $\rho, \rho' : G \to O_n(\mathbb{R})$ be two (continuous) orthogonal representations. If ρ and ρ' are equivalent as linear representations (i.e. if they have the same character), then they are orthogonally equivalent.*

PROOF: By hypothesis,

$$\rho(s)D = D\rho'(s)$$

for all s in G and some fixed D in $GL_n(\mathbb{R})$. The matrix D can be written uniquely in its polar form as $D = AP$ with A in $O_n(\mathbb{R})$ and P positive definite and symmetric (see, for example, [5], Th. 4.14, p. 189). Then

$$\rho(s)AP = AP\rho'(s) = A\rho'(s)\rho'(s)^{-1}P\rho'(s).$$

Since $\rho(s)A$ and $A\rho'(s)$ are orthogonal, and since P and $\rho'(s)^{-1}P\rho'(s)$ are positive definite and symmetric, uniqueness of the polar form shows

$$\rho(s)A = A\rho'(s)$$

for all s in G, with A in $O_n(\mathbb{R})$, as desired. □

Hence the map j_1 is injective, and we shall regard it as inclusion.

By analogy with the double cover $\mathrm{Spin}_n(\mathbb{R})$ of $SO_n(\mathbb{R})$, define $\mathrm{Pin}_n(\mathbb{R})$ to be a double cover of $O_n(\mathbb{R})$. By definition, $\mathrm{Pin}_n(\mathbb{R})$ is the subgroup generated by the unit sphere in the multiplicative group of units of the Clifford algebra of the standard euclidean form $X_1^2 + \ldots + X_n^2$:

$$\mathrm{Pin}_n(\mathbb{R}) = \langle a_1e_1 + \ldots + a_ne_n \quad \text{in} \quad C_n \quad \text{with} \quad a_1^2 + \ldots + a_n^2 = 1\rangle.$$

https://doi.org/10.4153/CMB-1985-051-2 Published online by Cambridge University Press

There is a canonical projection from $\mathrm{Pin}_n(\mathbb{R})$ onto $O_n(\mathbb{R})$, yielding

$$(3) \qquad 1 \to \{\pm 1\} \to \mathrm{Pin}_n(\mathbb{R}) \to O_n(\mathbb{R}) \to 1.$$

(see [2], proposition 5, p. 139). The group G_K is declared to act trivially on each of these groups. Then the exact cohomology sequence arising from (3) gives a coboundary map

$$H^1(G_K, O_n(\mathbb{R})) \xrightarrow{\delta} H^2(G_K, \pm 1).$$

The group $\{\pm 1\}$ lies in the multiplicative group $\bar{K}^*$, and $H^2(G_K, \pm 1)$ is the 2-torsion subgroup of the Brauer group $\mathrm{Br}(K) = H^2(G_K, \bar{K}^*)$. Thus we obtain a map from the set of isomorphism classes of orthogonal representations of G_K to the elements of order 2 in $\mathrm{Br}(K)$. Applying δ to the orthogonal representation $\rho_{E/K} = j_0(\pi_{E/K})$ yields an element $\delta(\rho_{E/K})$ in $\mathrm{Br}(K)$. Serre has proved that this element is related to the Hasse invariant of the trace form $q_{E/K}$ by the formula

$$(4) \qquad \delta(\rho_{E/K})\cdot(d_{E/K}, d_{E/K}) = h(q_{E/K})\cdot(2, d_{E/K})$$

in $\mathrm{Br}(K)$, where $d_{E/K} = \mathrm{dis}(q_{E/K})$. For a proof (using different terminology), see [8] or [4]. The product $\delta(\rho_{E/K})\cdot(d_{E/K}, d_{E/K})$ appearing on the left in (4) is called the second Stiefel–Whitney class of the representation $\rho_{E/K}$, and is denoted $w_2(\rho_{E/K})$. It has an independent, topological definition, but we won't need that here. In this notation, Serre's formula becomes

$$(5) \qquad w_2(\rho_{E/K}) = h(q_{E/K})\cdot(2, d_{E/K})$$

in $\mathrm{Br}(K)$.

The next theorem is a general result about permutation representations, stating that each of the basic four invariants of the form $q_{E/K}$ can be read from knowledge of the number of fixed points of $\pi_{E/K}(s)$, as s varies over G_K. For the statement, let

$$E = K[X]/(f) \quad \text{and} \quad E' = K[X]/(g)$$

be two étale algebras over K.

THEOREM 1: *Let E and E' be two étale K-algebras and let $\pi_{E/K}$ and $\pi_{E'/K}$ be the corresponding permutation representations. If the linear representations $\rho_{E/K} = j_0(\pi_{E/K})$ and $\rho_{E'/K} = j_0\,(\pi_{E'/K})$ are equivalent as linear representations (i.e., if they have the same trace) then the forms $q_{E/K}$ and $q_{E'/K}$ have the same rank, discriminant, Hasse invariant, and signature at any embedding of K into $\mathbb{R}$.*

PROOF: By assumption, $\rho_{E/K}$ and $\rho_{E'/K}$ are linearly equivalent, so

$$(6) \qquad \rho_E(s) = M\cdot\rho_{E'}(s)\cdot M^{-1}$$

for all s in G_K. By Lemma 2, we may take M to be in $O_n(\mathbb{R})$. It follows trivially from (6) that the matrices $\rho_{E/K}(s)$ and $\rho_{E'/K}(s)$ have the same size, hence $\mathrm{rank}(q_{E/K}) = \mathrm{rank}(q_{E'/K})$. For the signature statement, let σ be a real embedding of K, which we

https://doi.org/10.4153/CMB-1985-051-2 Published online by Cambridge University Press

extend in some fixed manner to a complex embedding of the separable colsure $\bar{K}$. Then $\text{sgn}_\sigma(q_{E/K}) = \text{trace}\,(\rho_{E/K}$ (complex conjugation)), and similarly for $\text{sgn}_\sigma(q_{E'/K})$. So (6) implies that the signatures agree.

Since $\rho_{E/K}$ is orthogonal, the kernel of the composite map

$$G_K \xrightarrow{\rho_{E/K}} O_n(\mathbb{R}) \xrightarrow{\det} \{\pm 1\}$$

has index 1 or 2 in G_K. Hence the fixed field of this kernel is an extension of degree 1 or 2 over K, and has the form $K(\sqrt{a})$ for some element a in K^*. Clearly a is determined only modulo squares in K^*.

Now a equals $\text{dis}(q_{E/K})$, modulo squares in K^*. To verify this, write the matrix of $q_{E/K}$ as $(C')C$, with C as in display (2). Fix s in G_K. Then from Lemma 1 we see that the matrix $\rho_{E/K}(s)$ can be written as $s(C)C^{-1}$. So $\det(\rho_{E/K}(s)) = 1$ if and only if $s(\det C) = \det C$. That is, s belongs to $\ker(\det \rho_{E/K})$ if and only if s fixes $\det C$. This being true for all s, we see that $\det C$ generates the fixed field of $\ker(\det \rho_{E/K})$. So $\det C$ plays the role of $\sqrt{a}$, and $(\det C)^2$ plays the role of a. So $a = (\det C)^2 = \det((C')C) = \text{dis}\,(q_{E/K})$, mod squares. From (6), $\det \rho_{E/K}$ and $\det \rho_{E'/K}$ have the same kernel, from which it follows that the discriminants of the two quadratic forms agree, modulo squares.

Finally, since the discriminants $d_{E/K}$ and $d_{E'/K}$ agree modulo squares, and since the representations $\rho_{E/K}$ and $\rho_{E'/K}$ give rise to the same class in $H^1(G_K, O_n(\mathbb{R}))$ and hence have the same coboundry, Serre's formula (4) implies that the Hasse invariants of the forms coincide as well. This establishes Theorem 1. □

COROLLARY: *Let E and E' be two algebraic number fields. If the Dedekind zeta functions $\zeta_E(z)$ and $\zeta_{E'}(z)$ coincide for all complex numbers z, then the trace forms $q_{E/\mathbb{Q}}$ and $q_{E'/\mathbb{Q}}$ are rationally equivalent.*

PROOF: The Dedekind zeta function $\zeta_E(z)$ is the Artin L-series of the representation $\rho_{E/K}$. It is well-known (and essentially due to Artin) that $\zeta_E(z)$ and $\zeta_{E'}(z)$ coincide if and only if the representations $\rho_{E/\mathbb{Q}}$ and $\rho_{E'/\mathbb{Q}}$ are linearly equivalent. (For a detailed proof, see [7]). Theorem 1 then shows that $q_{E/\mathbb{Q}}$ and $q_{E'/\mathbb{Q}}$ share ranks, signatures, discriminants, and Hasse invariants. But these four invariants completely classify a rational quadratic form up to rational equivalence. □

3. **Local root numbers**. Let $\rho : G_K \to GL_n(\mathbb{C})$ be a (continuous) representation of the absolute Galois group $G_K = \text{Gal}\,(\bar{K}/K)$ of an algebraic number field K. Then the Artin L-series $L(\rho, z)$ can be enlarged to a meromorphic function $\Lambda(\rho, z)$ satisfying

$$\Lambda(\rho, z) = W(\rho)\cdot\Lambda(\bar{\rho}, 1 - z)$$

where $\bar{\rho}$ is the complex conjugate representation, and $W(\rho)$ is the global Artin root number. The root number $W(\rho)$ depends only on the character of ρ, and can be written canonically as a product

$$W(\rho) = \prod_p W_p(\rho)$$

https://doi.org/10.4153/CMB-1985-051-2 Published online by Cambridge University Press

where p runs over all primes of K, and the local root numbers $W_p(\rho)$ are complex numbers. For details, see [6] and [9].

This section concerns the local root number $W_p(\rho)$ when $K = \mathbb{Q}$ and the representation ρ is real. In this case, ρ is always linearly equivalent to an orthogonal representation, and the local Artin root numbers $W_p(\rho) = a_p$ are complex numbers satisfying

(1) a_p is a fourth root of unity;

(2) $a_p = 1$ with at most finitely-many exceptions;

(3) $a_p = \pm 1$ whenever $p \equiv 1 \pmod 4$;

(4) $\prod_p a_p = 1$.

(see [9], p. 109, (ii) and (iii) of Cor. 1, and set $\rho = \bar{\rho}$. Property (4) is the theorem of Fröhlich–Queyrut, and is given in [9], Cor. 1, p. 124).

THEOREM 2: *Let $\{a_p\}$ be any family of complex numbers indexed by $p = 2, 3, \ldots, \infty$ and satisfying properties* (1) *through* (4). *Then there is an extension $E/\mathbb{Q}$ with $W_p(\rho_{E/\mathbb{Q}}) = a_p$ for all p.*

This theorem settles the question of realizing local Artin root numbers for real representations of $G_{\mathbb{Q}}$. No similar result seems to be known for complex representations. Before proving Theorem 2, we single out an immediate consequence: the local root numbers of any real representation ρ of $G_{\mathbb{Q}}$ are also the root numbers of the representation $\rho_{E/\mathbb{Q}}$ corresponding to the Dedekind zeta function of some algebraic number field E.

The proof of Theorem 2 depends on a formula of Deligne and on the Witt characterization of trace forms in the Witt ring $W(\mathbb{Q})$. Consider an orthogonal representation ρ of $G_{\mathbb{Q}}$. Combining ρ with the determinant yields a 1-dimensional orthogonal representation

$$G_{\mathbb{Q}} \xrightarrow{\rho} O_n(\mathbb{R}) \xrightarrow{\det} O_1(\mathbb{R})$$

where $O_1(\mathbb{R}) = \{\pm 1\}$. Then $\det \rho$ has local root numbers $W_p(\det \rho)$. Deligne has proved that the p-part of the second Stiefel–Whitney class of ρ is given by the quotient

$$w_2(\rho)_p = \frac{W_p(\rho)}{W_p(\det \rho)} \tag{7}$$

so this Stiefel–Whitney class may be thought of as a normalized local root number (see [9]). Now fix a number field E. Putting $\rho = \rho_{E/\mathbb{Q}}$ in (7) and recalling Serre's formula (5) yields an explicit connection between the Hasse invariant of the trace form $q_{E/\mathbb{Q}}$ and normalized local root numbers:

$$h_p(q_{E/\mathbb{Q}}) = \frac{W_p(\rho_{E/\mathbb{Q}})}{W_p(\det \rho_{E/\mathbb{Q}})} \cdot (2, d_{E/\mathbb{Q}})_p\,. \tag{8}$$

To prove Theorem 2, we adopt the notation of [1]. Thus for a Witt class X in the Witt ring $W(\mathbb{Q})$ the stable Hasse–Witt invariant is $c_p(X)$; this is just h_p of a representative

https://doi.org/10.4153/CMB-1985-051-2 Published online by Cambridge University Press

of the class X having rank 0 or 1 (mod 8). Also, the Witt class of the trace form $q_{E/\mathbb{Q}}$ is denoted by $\langle E \rangle$. With this, we can now prove Theorem 2.

PROOF OF THEOREM 2: Define a square-free rational integer d as follows:

1. If all $a_p = \pm 1$, then set $d = 1$.

2. If $a_p = \pm 1$ for all odd finite p but $a_\infty = \pm\, i$, set $d = -1$.

3. If $a_p = \pm\, i$ for odd finite primes $p_1, \ldots, p_K$ and for no other odd finite p but $a_\infty = \pm\, 1$, set $d = p_1 p_2 \ldots p_K$.

4. If $a_p = \pm\, i$ for the odd finite primes $p_1, \ldots, p_K$ and for no other odd finite p but $a_\infty = \pm\, i$, then set $d = -p_1 p_2 \ldots p_K$.

There is a real orthogonal 1-dimensional representation

$$\delta : G_{\mathbb{Q}} \to O_1(R)$$

associated with d, given by $\delta(s) = s(\sqrt{d})/\sqrt{d}$. This representation has local root numbers $W_p(\delta)$. Cor. 1, (ii) of [9] shows that $W_p(\delta)^2$ is given by Hilbert symbol $(-1, d)_p$. By our choice of d we therefore have

$$a_p = \pm W_p(\delta)$$

for all $p \neq 2$, including $p = \infty$. Since $\Pi_p\, a_p = \Pi_p\, W_p(\delta) = 1$, it follows that $a_2 = \pm W_2(\delta)$ also.

Now define a Witt class X in the rational Witt ring $W(\mathbb{Q})$ by declaring the four basic invariants to be

1. $rk(X) \equiv 1 \pmod 2$;
2. $\operatorname{dis}(X) = d$ modulo rational squares;
3. $c_p(X) = (2, d)_p \cdot a_p / W_p(\delta)$;

$$(9) \qquad 4.\ \operatorname{sgn}(X) = \begin{cases} 1 & \text{if } d > 0 \text{ and } c_\infty(X) = 1; \\ 3 & \text{if } d < 0 \text{ and } c_\infty(X) = -1; \\ 5 & \text{if } d > 0 \text{ and } c_\infty(X) = -1; \\ 7 & \text{if } d < 0 \text{ and } c_\infty(X) = 1. \end{cases}$$

Since $\operatorname{sgn}(X) > 0$, there is an extension $F/\mathbb{Q}$ with $\langle F \rangle = X$ in $W(\mathbb{Q})$ (see [1], Theorem III.6.1, p. 146, and the remark at the end of p. 125). Then $m = [F : \mathbb{Q}] \equiv rk(X) \pmod 2$ is odd, so there is an odd integer $k > 3$ with $km \equiv 1 \pmod 8$. By [1], Lemma VI.2.8, p. 293 there is an irreducible trinomial f of degree k giving a field extension $F' = \mathbb{Q}[T]/f(T)$ with F' disjoint from F and $\operatorname{dis}\langle F' \rangle = 1$, modulo rational squares. By [1], Theorem VI.2.1, page 286, $\langle F' \rangle = \langle 1 \rangle$, the multiplicative identity in $W(\mathbb{Q})$. Then the composite $E = F \cdot F'$ has $\langle E \rangle = \langle FF' \rangle = \langle F \rangle \langle F' \rangle = X \langle 1 \rangle = X$, and $[E : \mathbb{Q}]$ is congruent to 1 (mod 8). Now Dis $(E/\mathbb{Q}) = d$ modulo rational squares, so the 1-dimensional representations $\det \rho_{E/\mathbb{Q}}$ and δ coincide. Hence

$$W_p(\det \rho_{E/\mathbb{Q}}) = W_p(\delta).$$

Furthermore, $c_p\langle E_p \rangle = h_p(q_{E/\mathbb{Q}})$ since the trace form is a representative of the Witt class $\langle E \rangle$ having rank 1 (mod 8). From condition (3) of display (9) we have

https://doi.org/10.4153/CMB-1985-051-2 Published online by Cambridge University Press

$$h_p(q_{E/\mathbb{Q}}) = (2,d)_p \cdot a_p / W_p(\det \rho_{E/\mathbb{Q}}).$$

Then by the Serre/Deligne formula (8)

$$(2,d)_p \cdot \frac{W_p(\rho_{E/\mathbb{Q}})}{W_p(\det \rho_{E/\mathbb{Q}})} = h_p(q_{E/\mathbb{Q}}) = (2,d)_p \cdot a_p / W_p(\det \rho_{E/\mathbb{Q}})$$

and hence $W_p(\rho_{E/\mathbb{Q}}) = a_p$ for all p. This proves Theorem 2. □

In closing, we note that it is not known whether Theorem 2 remains valid when $\mathbb{Q}$ is replaced by a number field K. For in that case, it is presently unknown which Witt classes in $W(K)$ are represented by trace forms.

References

1. P. E. Conner and R. Perlis, *A Survey of Trace Forms of Algebraic Number Fields*, World Scientific Publishing Company, Singapore (1984).

2. M. Curtis, *Matrix Groups*, Springer-Verlag, New York (1979).

3. P. Deligne, *Les constantes locales de l'équation fonctionnelle de la fonction L d'Artin d'une représentation orthogonale*, Inv. Math. **35** (1976), pp. 296–316.

4. A. Fröhlich, *Orthogonal representations of Galois groups, Stiefel–Whitney classes, and Hasse–Witt invariants*, preprint (1984), p. 1–60.

5. M. Marcus and H. Minc, *Introduction to Linear Algebra*, Macmillan, New York (1965).

6. J. Martinet, *Character theory and Artin L-functions, in Algebraic Number Fields*, Academic Press, New York (1977), pp. 1–87.

7. R. Perlis, *On the equation* $\zeta_K(s) = \zeta_{K'}(s)$, J. Number Theory **9** (1977), pp. 342–360.

8. J.-P. Serre, *L'invariant de Witt de la forme* $\mathrm{Tr}(x^2)$, Commentarii Mathematici Helvetici **59** (1984), pp. 651–676.

9. J. Tate, *Local Constants, in Algebraic Number Fields*, Academic Press, New York (1977), pp. 89–131.

10. O. Taussky-Todd, *The discriminant matrices of an algebraic number field*, J. London Math. Soc., **43** (1968), pp. 152–154.

Department of Mathematics
Louisiana State University
Baton Rouge, Louisiana 70803
U.S.A.

https://doi.org/10.4153/CMB-1985-051-2 Published online by Cambridge University Press