Orthogonal determinants of characters

Gabriele Nebe

Abstract. For an irreducible orthogonal character χ of even degree there is a unique square class $\det(\chi)$ in the character field such that the invariant quadratic forms in any L-representation affording χ have determinant in $\det(\chi)(L^\times)^2$.
MSC: 20C15; 11E12; 11E57.
KEYWORDS: orthogonal representations of finite groups; Schur index.

1. Introduction

Let G be a finite group. An absolutely irreducible complex representation $\rho_{\mathbb{C}} : G \to \mathrm{GL}_n(\mathbb{C})$ fixes a non-zero quadratic form if and only if $\rho_{\mathbb{C}}$ is equivalent to a real representation $\rho : G \to \mathrm{GL}_n(\mathbb{R})$. Then $B := \sum_{g\in G} \rho(g)\rho(g)^{tr}$ is a positive definite symmetric matrix. As $\rho(g)B\rho(g)^{tr} = B$ the group $\rho(G)$ is a subgroup of the orthogonal group of B. In this case we call $\chi : G \to \mathbb{R}, \chi(g) := \mathrm{trace}(\rho(g))$ an orthogonal character. Let $K = \mathbb{Q}(\chi(g) \mid g \in G)$ be the character field of χ. The main result of this paper is Theorem 3.3 showing that for even character degree there is a unique square class $\det(\chi) \in K^\times/(K^\times)^2$ such that for any representation ρ with character χ over some extension field L of K all non-zero $\rho(G)$-invariant symmetric bilinear forms B have $\det(B) \in \det(\chi)(L^\times)^2$. The square class $\det(\chi)$ is called the orthogonal determinant of χ. The proof is immediate when the Schur index of χ is one. In this case there is a representation ρ for $L = K$ and $\det(\chi) = \det(B)(K^\times)^2$ for any non-zero $\rho(G)$-invariant form B. If the Schur index of χ is two, there is no such representation over K. Then the rational span of the matrices in $\rho(G)$ is a central simple K-algebra A and by Remark 3.1 the adjoint involution induces an involution on A whose determinant (as defined in [5, Proposition (7.1)]) is $\det(\chi)$.

In positive characteristic all Schur indices are one and the result of Theorem 3.3 holds with a direct easy proof. Therefore we restrict to characters over number fields in this short note.

In an ongoing project with Richard Parker, we aim to provide the orthogonal determinant for all irreducible orthogonal Brauer characters for all but the largest few ATLAS groups [3] over all finite fields. This is a finite (computational) problem for the primes that divide the group order. Thanks to Theorem 3.3 the infinitely many primes not dividing the group order can be treated with a characteristic zero approach as illustrated in Corollary 4.2.

ACKNOWLEDGEMENTS. I thank Richard Parker for his persisting questions and fruitful discussions that made me write this paper and Eva Bayer-Fluckiger for her interesting comments leading to Section 2.2.

2. Determinants of symmetric bilinear forms

Let K be a field of characteristic $\neq 2$, V a vector space of dimension n over K and $\tilde{B} : V \times V \to K$ a symmetric bilinear form. Any choice of a basis $(e_1, \ldots, e_n)$ of V identifies V with the row space K^n. The Gram matrix of $\tilde{B}$ with respect to this basis is

$$B := (\tilde{B}(e_i, e_j))_{i,j=1}^n \in K^{n\times n}$$

a symmetric square matrix satisfying $\tilde{B}(x, y) = xBy^{tr}$ for all $x, y \in K^n$. Base change by the matrix $T \in \mathrm{GL}_n(K)$ changes the Gram matrices into TBT^{tr} and hence the determinant of $\tilde{B}$ is

$$\det(\tilde{B}) := \det(B)(K^\times)^2 \in K/(K^\times)^2$$

well defined up to squares. The bilinear form $\tilde{B}$ is called non-degenerate, if $\det(\tilde{B}) \in K^\times/(K^\times)^2$, i.e. $\det(B) \neq 0$.

2.1. The adjoint involution

Any non-degenerate symmetric bilinear form $\tilde{B}$ on V defines a K-linear involution $\iota_{\tilde{B}}$ on $\mathrm{End}_K(V)$. For $\alpha \in \mathrm{End}_K(V)$ the endomorphism $\iota_{\tilde{B}}(\alpha)$ is defined by

$$\tilde{B}(\alpha(x), y) = \tilde{B}(x, \iota_{\tilde{B}}(\alpha)(y)) \text{ for all } x, y \in V.$$

Identifying $\mathrm{End}_K(V)$ with the matrix ring $K^{n\times n}$ by choosing a basis $(e_1, \ldots, e_n)$ of V, the involution $\iota_{\tilde{B}}$ is given by

$$\iota_B(A) = BA^{tr}B^{-1}.$$

We define

$$E_-(\tilde{B}) := \{\alpha \in \mathrm{End}_K(V) \mid \iota_{\tilde{B}}(\alpha) = -\alpha\}$$

the K-space of skew adjoint endomorphisms. In matrix notation we get

$$E_-(B) := \{X \in K^{n\times n} \mid BX^{tr}B^{-1} = -X\}$$

and hence

Lemma 2.1. $E_-(B) = \{BX \mid X = -X^{tr} \in K^{n\times n}\}$.

Scaling of the bilinear form does not change the involution, $E_-(aB) = E_-(B)$ for all $a \in K^\times$. On the other hand $\det(aB) = a^n \det(B)$. So we can only read off the determinant of $\tilde{B}$ from the involution ι_B in even dimensions. The following property of skew adjoint endomorphisms is crucial.

Proposition 2.2. *$E_-(\tilde{B})$ contains invertible elements if and only if* $\dim(V)$ *is even. Then* $\det(\tilde{B}) = \det(\alpha)(K^\times)^2$ *for any invertible* $\alpha \in E_-(\tilde{B})$.

Proof. We prove the theorem in matrix notation. Let $E_-(I) := \{X \in K^{n\times n} \mid X = -X^{tr}\}$ denote the space of skew symmetric matrices. It is well known that $E_-(I)$ contains an invertible matrix, if and only if n is even and then the determinant of such a matrix is a square. By Lemma 2.1 the map $E_-(I) \to E_-(B), X \mapsto BX$ is an isomorphism. So $E_-(B)$ contains invertible elements if and only if $\dim(V)$ is even, and all such elements $Y \in E_-(B) \cap \mathrm{GL}_n(K)$ satisfy $\det(Y) \in \det(B)(K^\times)^2$. □

2.2. Determinants and isometries

For any non-degenerate symmetric bilinear form $\tilde{B}$ its orthogonal group is

$$O(V,\tilde{B}) := \{g \in \mathrm{GL}(V) \mid \tilde{B}(vg, wg) = \tilde{B}(v,w) \text{ for all } v,w \in V\}.$$

Remark 2.3. An endomorphism $g \in \mathrm{End}_K(V)$ lies in $O(V,\tilde{B})$ if and only if $g\iota_{\tilde{B}}(g) = \iota_{\tilde{B}}(g)g = \mathrm{id}_V$, i.e. $\iota_{\tilde{B}}(g) = g^{-1}$.

Proposition 2.4. *(see* [1, Proposition 5.1]*) Let $g \in O(V,\tilde{B})$ and denote by P the characteristic polynomial of g. Assume that $P(1)P(-1) \neq 0$.*

(a) $\dim(V)$ *is even.*
(b) $\det(g) = 1$.
(c) $\det(\tilde{B}) = \det(g - g^{-1})(K^\times)^2 = P(1)P(-1)(K^\times)^2$.

Proof. The (sketched) proof follows the exposition in [1].
Let $n := \dim(V) = \deg(P)$. Then $P(0) = (-1)^n \det(g) =: \epsilon \in \{1,-1\}$.
Put $P^*(X) := \epsilon X^n P(X^{-1})$ to denote the reverse polynomial of G. Then by [1, Proposition 1.1] the condition that $g \in O(V,\tilde{B})$ implies that $P = P^*$. As $P(1) \neq 0$ we hence have $\epsilon = 1$. Now $P(-1) \neq 0$ yields that n is even and so $\det(g) = 1$.
To see (c) we write $P(X) = \prod_{j=1}^n (X - \xi_j)$ over some algebraic closure of K. Then

$$P(1)P(-1) = \prod_{j=1}^n (\xi_j^2 - 1) = (\prod_{j=1}^n \xi_j) \prod_{j=1}^n (\xi_j - \xi_j^{-1}) = \det(g)\det(g - g^{-1}).$$

As $\det(g) = 1$ and $g - g^{-1} \in E_-(\tilde{B})$ is a unit, statement (c) now follows from Proposition 2.2. □

Corollary 2.5. *If there is $g \in O(V,\tilde{B})$ with $g^2 = -1$ then* $\det(\tilde{B}) = 1$.

Proof. Then the minimal polynomial of g divides $X^2 + 1$ and hence the characteristic polynomial of g is $P = (X - i)^a (X + i)^b$. Then $P(1)P(-1) = (-2)^{a+b}$. By Proposition 2.4 (a) $a + b = \dim(V)$ is even so $P(1)P(-1)$ is a square and the statement follows from Proposition 2.4 (c). □

3. Orthogonal representations of finite groups

Let G be a finite group and L be a field. An L-representation ρ is a group homomorphism $\rho : G \to \mathrm{GL}_n(L)$. Given a representation ρ we put

$$\mathcal{F}(\rho) := \{B \in L^{n\times n} \mid B = B^{tr} \text{ and } \rho(g)B\rho(g)^{tr} = B \text{ for all } g \in G\}$$

to denote the L-vector space of symmetric G-invariant bilinear forms on L^n.

Remark 3.1. Let $B \in \mathcal{F}(\rho) \cap \mathrm{GL}_n(L)$. Then the adjoint involution ι_B on $L^{n\times n}$ satisfies $\iota_B(\rho(g)) = \rho(g^{-1})$ for all $g \in G$.

Definition 3.2. *A representation ρ and also its character $\chi_\rho = trace \circ \rho$ is called* orthogonal, *if $\mathcal{F}(\rho)$ contains a non-degenerate element.*

3.1. Orthogonal determinants

Theorem 3.3. *Let $\chi \in \mathrm{Irr}_{\mathbb{C}}(G)$ be an orthogonal character of even degree $n := \chi(1) \in 2\mathbb{Z}$. Denote by K the character field of χ. Then there is a unique totally positive square class* $\det(\chi) = d(K^\times)^2 \in K^\times/(K^\times)^2$ *with the following property: Let $L \supseteq K$ be any field and $\rho : G \to \mathrm{GL}_n(L)$ a representation with character χ. Then any nonzero $B \in \mathcal{F}(\rho)$ satisfies* $\det(B) \in \det(\chi)(L^\times)^2$.

Definition 3.4. *The square class* $\det(\chi)(K^\times)^2$ *from Theorem* 3.3 *is called the* orthogonal determinant *of the character χ.*

3.2. Proof of Theorem 3.3

For the proof of Theorem 3.3 we assume that we are given a field L containing the character field K of χ and a representation $\rho : G \to \mathrm{GL}_n(L)$ with character χ. We also choose some non-zero $B \in \mathcal{F}(\rho)$. Since ρ is absolutely irreducible the matrices in $\rho(G)$ generate $L^{n\times n}$ as a vector space over L. Also $\mathcal{F}(\rho)$ is one dimensional and B is non-degenerate and unique up to scalars:

Remark 3.5. (a) $\langle \rho(g) \mid g \in G\rangle_L = L^{n\times n}$
(b) $\mathcal{F}(\rho) = \langle B\rangle_L$.
(c) $E_-(B) = \langle \rho(g) - \rho(g^{-1}) \mid g \in G\rangle_L$.

We now consider the $\mathbb{Q}$-algebra generated by the matrices in $\rho(G)$,

$$A := \langle \rho(g) \mid g \in G\rangle_{\mathbb{Q}} \leq L^{n\times n}.$$

Remark 3.6. (a) A is a central simple K-algebra of dimension n^2.
(b) The restriction ι of ι_B to A satisfies $\iota(\rho(g)) = \rho(g^{-1})$ for all $g \in G$.
(c) $E_-(\rho) := \langle \rho(g) - \rho(g^{-1}) \mid g \in G\rangle_{\mathbb{Q}} = E_-(B) \cap A$.

It is well known that the reduced norm of a central simple algebra takes values in the center of this algebra:

Lemma 3.7. *For all $X \in A$ we have that* $\det(X) \in K$.

Proof. As L is a splitting field for A the determinant is the reduced norm of the central simple K-algebra A, see for instance [6, Section 9]. Reiner also shows that the reduced norm is independent of the choice of a splitting field and takes values in K. ☐

By [5, Corollary 2.8] a central simple algebra with orthogonal involution contains invertible elements that are negated by the involution if and only if the dimension of this algebra over its center is even. In particular for our situation this yields the following proposition for which we give an independent short proof below.

Proposition 3.8. *$E_-(\rho)$ contains invertible elements.*

Proof. The fact that $E_-(\rho)$ contains an element that is invertible in the central simple K-algebra $A = \langle \rho(g) \mid g \in G\rangle_{\mathbb{Q}}$ does not depend on the choice of the splitting field L. So without loss of generality we fix an embedding $\epsilon : K \hookrightarrow \mathbb{R}$, identify K with its image $\epsilon(K) \subseteq \mathbb{R}$, and take $L = \mathbb{R}$, one of the real completions of K.

We first choose a K-basis $B = (b_1, \ldots, b_m)$ of $E_-(\rho)$. Then B is also an $\mathbb{R}$-basis of $E_-(B)$. Let $X \in E_-(B) \cap \mathrm{GL}_n(\mathbb{R})$ be an invertible element of $E_-(B)$. Write

$$X = \alpha_1 b_1 + \ldots + \alpha_m b_m \text{ with unique } \alpha_i \in \mathbb{R}.$$

Now $\mathbb{Q}$ and hence also $\epsilon(K)$ is dense in $\mathbb{R}$. So there are $a_i \in K$ such that $\epsilon(a_i)$ is arbitrary close to α_i for all $i = 1, \ldots, m$. Put

$$Y := a_1 b_1 + \ldots + a_m b_m \in E_-(\rho).$$

For Y being a unit in A, it is enough to achieve that the determinant of $\epsilon(Y) := \sum_{i=1}^{m} \epsilon(a_i) b_i$ is non zero. As det is a polynomial, in particularly continuous, and $\det(X) \neq 0$, we can find $a_i \in K$ such that $\epsilon(\det(Y)) = \det(\epsilon(Y)) \neq 0$. But then $Y \in E_-(\rho)$ is an invertible matrix. □

Proof. (of Theorem 3.3) By Proposition 2.2 we get $\det(B)(L^\times)^2 = \det(X)(L^\times)^2$ for any invertible $X \in E_-(B)$. Proposition 3.8 says that such an invertible element X can be chosen in $E_-(\rho) = E_-(B) \cap A$, so in particular its determinant is an element of K by Lemma 3.7. □

4. Some applications

4.1. An example: $\mathrm{SL}_2(\mathbb{F}_7)$

For illustration let $G := \mathrm{SL}_2(\mathbb{F}_7)$ be the special linear group of degree 2 over the field with 7 elements. The complex character table of G is given in [3]. For any faithful irreducible representation ρ of G we obtain $\rho(\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix})^2 = -\mathrm{id}$ and hence by Corollary 2.5 all faithful irreducible orthogonal characters have determinant 1. There are six complex irreducible characters of the group $L_2(7) = \mathrm{PSL}_2(7)$, of degrees 1, 3, 3, 6, 7, and 8 giving rise to three irreducible rational representations of even degree, $3ab$, 6, and 8:

3ab Restrict the representation to a Sylow-7-subgroup $\langle g\rangle$ of G. The eigenvalues of $\rho(g)$ are all primitive 7th roots of unity and hence $\det(\rho(g) - \rho(g^{-1})) = \prod_{i=1}^{6}(\zeta_7^i - \zeta_7^{-i}) = 7$. So by Proposition 2.4 the orthogonal determinant of χ is $\det(\chi) = 7(\mathbb{Q}^\times)^2$.

6 Restriction to $\langle g\rangle$ as before allows to conclude that $\det(\chi) = 7(\mathbb{Q}^\times)^2$.

8 Let $H = C_7 : C_3 = \langle g\rangle : \langle h\rangle$ be the normaliser in G of the Sylow-7-subgroup. Then the restriction of ρ to H decomposes as $6+2$, where $\langle g\rangle$ acts fixed point free on the 6-dimensional part and trivially on the 2-dimensional summand. On the 2-dimensional summand, $\langle h\rangle$ acts faithfully. If $e = \frac{1}{7}\sum_{i=0}^{6} g^i \in \mathbb{Q}H$ is the involution invariant idempotent projecting onto the fixed space of $\langle g\rangle$, then

$$X := (\rho(g) - \rho(g^{-1})) + \rho(e)(\rho(h) - \rho(h^{-1})) \in E_-(\rho)$$

has determinant $7 \cdot 3 = 21$. So by Proposition 2.2 we get $\det(\chi) = 21(K(\chi)^\times)^2$.

Remark 4.1. Note that these techniques essentially suffice to find all orthogonal determinants for all groups $\mathrm{SL}_2(q)$ as given in [2].

4.2. Orthogonal characters with rational Schur index 2

Theorem 3.3 is particularly helpful in the case that the orthogonal character is not the character of a representation over its character field. The smallest example of a simple group G in [3] is the group $G = J_2$. This sporadic simple group has a complex irreducible orthogonal character χ of degree $\chi(1) = 336$ with rational character field. By [4] (see also [7]) the rational Schur index of χ is 2. With MAGMA [8] we realise the representation as a rational representation ρ of dimension $2 \cdot 336 = 672$ (with character 2χ). Then the central simple $\mathbb{Q}$-algebra

$$A = \langle \rho(g) \mid g \in G\rangle \cong \mathcal{Q}_{2,3}^{168\times 168}$$

is isomorphic to a matrix ring over the indefinite rational quaternion algebra $\mathcal{Q}_{2,3}$ ramified at 2 and 3. We take three random elements $g_1, g_2, g_3 \in G$ to achieve that $x := \sum_{i=1}^{3} \rho(g_i) - \rho(g_i^{-1}) \in E_-(\rho)$ has full rank. To compute the reduced norm of $x \in A$, we compute the characteristic polynomial P of x which is a square $P = p^2$ of a unique monic polynomial p. Then the reduced norm of x is $p(0)$. It turns out that $p(0)$ is a rational square, so $\det(\chi) = 1$.

Corollary 4.2. *For any finite field F of characteristic $p \geq 7$ the representation $\rho : J_2 \to \mathrm{GL}_{336}(F)$ with Brauer character χ fixes a symmetric bilinear form of determinant 1. In particular $\rho(J_2) \leq O_{336}^+(F)$.*

4.3. Split extensions $G : 2$

Let G be a finite group, $\alpha \in \mathrm{Aut}(G)$ an automorphism of order 2. Then the split extension $G : 2$ has a pseudo-presentation

$$G : 2 = \langle G, h \mid hgh^{-1} = \alpha(g), h^2 = 1\rangle.$$

Assume that there is an orthogonal character $\chi \in \mathrm{Irr}_{\mathbb{C}}(G)$ such that $\chi\circ\alpha \neq \chi$. Then there is a unique character $\mathcal{X} \in \mathrm{Irr}_{\mathbb{C}}(G : 2)$ such that $\mathcal{X}_{|G} = \chi + \chi\circ\alpha$. As $\mathcal{X}(hg) = 0$ for all $g \in G$ the character field F of $\mathcal{X}$ is contained in the character field K of χ.

Theorem 4.3. *If $K = F$ then* $\det(\mathcal{X}) = 1$.
Otherwise K is a quadratic extension of F, so $K = F[\sqrt{\delta}]$ for some $\delta \in F$ and $\det(\mathcal{X}) = \delta^{\chi(1)}$.

Proof. Let L be some extension of K and $\rho : G \to \mathrm{GL}_n(L)$ a representation affording the character χ, so $n = \chi(1)$. Then the induced representation $\mathcal{R}$ with character $\mathcal{X}$ is given by

$$\mathcal{R}(g) = \mathrm{diag}(\rho(g), \rho(\alpha(g))) \text{ for all } g \in G \text{ and } \mathcal{R}(h) = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.$$

In particular $\mathcal{R}$ is also an L-representation and

$$\mathcal{F}(\mathcal{R}) = \{\mathrm{diag}(B, B) \mid B \in \mathcal{F}(\rho)\}.$$

This shows that $\det(\mathcal{X})(K^\times)^2 = \det(\chi)^2$. In particular $\det(\mathcal{X}) = 1$ if $K = F$. Now assume that $K = F[\sqrt{\delta}]$. Let $g_0 \in G$ be such that $K = F[\chi(g_0)]$ and put $C_0 := \sum_{g \in g_0^G} g$ the class sum of g_0. Then C_0 and $\alpha(C_0)$ are central elements in $\mathbb{Q}G$. Adding some element of F and multiplying by some element in $F^\times$ we find C in the center of $\mathbb{Q}G$, such that

$$\chi(C) = \chi(\iota(C)) = n\sqrt{\delta}, \chi(\alpha(C)) = \chi(\alpha(\iota(C))) = -n\sqrt{\delta}.$$

As $h = h^{-1}$ and also $\iota(C) = C$ we compute

$$\begin{array}{lll} \iota(\mathcal{R}(h)\,\mathcal{R}(C)) = & \mathcal{R}(\iota(C))\,\mathcal{R}(h) = & \mathcal{R}(C)\,\mathcal{R}(h) = \\ \mathcal{R}(h)\,\mathcal{R}(\alpha(C)) = & \mathcal{R}(h)(-\mathcal{R}(C)) = & -\mathcal{R}(h)\,\mathcal{R}(C). \end{array}$$

So $\mathcal{R}(h)\,\mathcal{R}(C) \in E_-(\mathcal{R})$ and $\det(\mathcal{R}(h)\,\mathcal{R}(C)) = (-1)^n \sqrt{\delta}^n (-\sqrt{\delta})^n = \delta^n$. Thanks to Proposition 2.2 and Theorem 3.3 we get $\det(\mathcal{X}) = \delta^n (F^\times)^2$. □

Example 4.4. Let $\mathcal{X}_n \in \mathrm{Irr}_{\mathbb{C}}(J_2 : 2)$ be the irreducible characters of degree $2n$ of the automorphism group of J_2, for $n = 14, 21, 70, 189, 224$ (see [3]). In all cases the character field of $\mathcal{X}_n$ is $\mathbb{Q}$ and the restriction of $\mathcal{X}_n$ to the simple group J_2 is the sum of two irreducible orthogonal characters of degree n and with character field $\mathbb{Q}[\sqrt{5}]$. As $J_2 : 2$ is a split extension Theorem 4.3 tells us that $\det(\mathcal{X}_n) = 5^n (\mathbb{Q}^\times)^2$.

References

[1] Eva Bayer-Fluckiger, Isometries of quadratic spaces. J. EMS **17** (2015) 1629–1656

[2] Oliver Braun and Gabriele Nebe, The orthogonal character table of $\mathrm{SL}_2(q)$. J. Algebra 486 (2017) 64-79

[3] John H. Conway, Robert T. Curtis, Simon P. Norton, Richard A. Parker and Robert A. Wilson, Atlas of Finite Groups. Oxford University Press (1985)

[4] Walter Feit, The computations of some Schur indices, Isr. J. Math. 46 (1983) 274–300.

[5] Max-Albert Knus, Alexander Merkurjev, Markus Rost, and Jean-Pierre Tignol, The Book of Involutions. AMS Coll. Publications **44** (1998)

[6] Irving Reiner, Maximal Orders. Lond. Math. Soc. Monogr. 5 (1975) Academic Press, London.

[7] William R. Unger, An algorithm for computing Schur indices of characters, J. Symb. Comput. 93 (2019) 148–160

[8] The Magma Computational Algebra System for Algebra, Number Theory and Geometry, http://www.maths.usyd.edu.au:8000/u/magma/

Gabriele Nebe
e-mail: nebe@math.rwth-aachen.de
Lehrstuhl für Algebra und Zahlentheorie, RWTH Aachen University, 52056 Aachen, Germany