Orthogonal representations of $\mathrm{SL}_2(q)$ in defining characteristic

Tobias Braun*and Gabriele Nebe†‡

Abstract

This paper determines the type of the invariant quadratic form for all irreducible modules of the groups $\mathrm{SL}_2(q)$ in defining characteristic.

1 Introduction

Let $\rho : G \to \mathrm{GL}_n(K)$ be an absolutely irreducible representation of a finite group G. Then ρ is called orthogonal, if $\rho(G)$ fixes a non-degenerate quadratic form Q; in this case $\rho(G)$ is a subgroup of the orthogonal group of Q. If K is a finite field and n is even, there are two isomorphism classes of orthogonal groups, O^+ and O^-. As field extensions are well controlled (see [6, Proposition 4.9]) it is enough to consider the minimal possible field K, the field of definition, that is generated by the traces of the matrices in $\rho(G)$.

In a long term project with Richard Parker and Thomas Breuer we aim to determine the type (+ or -) of all absolutely irreducible representations of the small finite simple groups G.

For all prime powers $q = p^f$ the paper [1] provides the relevant information for the orthogonal representations of $\mathrm{SL}_2(q)$ over fields K of characteristic 0. This immediately yields the type for all characteristics not dividing the group order. Using the methods of [5] and the decomposition matrices available in [2] one can also deduce the orthogonal type in non-defining characteristic. The present paper deals with the remaining case, where $\mathrm{char}(K) = p = \mathrm{char}(\mathbb{F}_q)$, the so-called defining characteristic. The main result is given in Theorem 3.7. Its proof is based on the observation that the restriction of all relevant representations to the cyclic subgroup $T \leq \mathrm{SL}_2(q)$ of order $|T| = q + 1$ (a non-split torus) is an orthogonal direct sum of irreducible unitary representations.

The authors acknowledge funding under Project-ID 286237555 – TRR 195 – by the Deutsche Forschungsgemeinschaft (DFG, German Research Foundation).

*tobias.braun2@rwth-aachen.de

†nebe@math.rwth-aachen.de

‡Lehrstuhl für Algebra und Zahlentheorie, RWTH Aachen University, 52056 Aachen, Germany

2 Quadratic forms over finite fields

2.1 Quadratic forms

Let K be a field and V a finite dimensional vector space over K. A quadratic form Q is a map $Q : V \to K$ such that $Q(ax) = a^2 Q(x)$ for all $a \in K$, $x \in V$ and such that the polarisation

$$B_Q : V \times V \to K, B_Q(x, y) := Q(x + y) - Q(x) - Q(y)$$

is a bilinear form. The quadratic form Q is called non-degenerate if the radical of B_Q is $\{0\}$. Note that the polarisation of a quadratic form is always a symmetric bilinear form. Also $2Q(x) = B_Q(x, x)$, so over a field of characteristic $\neq 2$ quadratic forms and symmetric bilinear forms are equivalent notions. If $\mathrm{char}(K) = 2$ then $B_Q(x, x) = 0$ for all x, so B_Q is alternating, and, in particular, the dimension of a non-degenerate quadratic form is even.

2.2 Quadratic forms over finite fields

Let $\mathbb{F}_q$ denote the field with q elements. Then it is well known that every non-degenerate quadratic form Q of dimension ≥ 3 contains isotropic vectors, i.e. vectors $v \neq 0$ with $Q(v) = 0$. It is easy to conclude that such forms split off a hyperbolic plane

$$\mathbb{H}(\mathbb{F}_q) := (\langle v, w \rangle, Q) \text{ with } Q(av + bw) = ab$$

as an orthogonal summand. There is a unique anisotropic form of dimension 2, $N(\mathbb{F}_q)$. Here the underlying space is $\mathbb{F}_{q^2}$ and the quadratic form is the norm form $Q(x) := xx^q$ for all $x \in \mathbb{F}_{q^2}$.

Hence on a vector space $V = \mathbb{F}_q^{2m}$ of even dimension there are two non-isometric quadratic forms

$$Q^+_{2m}(q) := \mathbb{H}(\mathbb{F}_q)^m \text{ and } Q^-_{2m}(q) := \mathbb{H}(\mathbb{F}_q)^{m-1} \perp N(\mathbb{F}_q), \tag{1}$$

which we call of $+$ type and of $-$ type respectively.

Remark 2.1. The orthogonal sums of these forms behave as expected:

$$Q^+_{2m}(q) \perp Q^+_{2n}(q) = Q^-_{2m}(q) \perp Q^-_{2n}(q) = Q^+_{2(m+n)}(q),\ Q^-_{2m}(q) \perp Q^+_{2n}(q) = Q^-_{2(m+n)}(q).$$

Fact 2.2. *(see for instance [4, Kapitel IV])*

- *The Witt index, i.e. the dimension of a maximal isotropic subspace, of $Q^+_{2m}(q)$ is m and $Q^-_{2m}(q)$ has Witt index $m - 1$.*
- *The number of non-zero isotropic vectors in $Q^+_{2m}(q)$ is $(q^m - 1)(q^{m-1} + 1)$ and for $Q^-_{2m}(q)$ one gets $(q^m + 1)(q^{m-1} - 1)$.*

Proposition 2.3. *For any non-zero $\alpha \in \mathbb{F}_{q^m}$ the quadratic form*

$$Q_\alpha : \mathbb{F}_{q^{2m}} \to \mathbb{F}_q, Q_\alpha(x) := \mathit{trace}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(\alpha x^{q^m+1})$$

is isometric to $Q^-_{2m}(q)$.

Proof. We easily check that for $x, y \in \mathbb{F}_{q^{2m}}$

$$Q_\alpha(x+y) - Q_\alpha(x) - Q_\alpha(y) = \mathrm{trace}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(x^{q^m}\alpha y + y^{q^m}\alpha x) = \mathrm{trace}_{\mathbb{F}_{q^{2m}}/\mathbb{F}_q}(x^{q^m}\alpha y)$$

by the transitivity of the trace. So the polarisation of Q_α is given by

$$B_\alpha(x,y) = \mathrm{trace}_{\mathbb{F}_{q^{2m}}/\mathbb{F}_q}(x^{q^m}\alpha y) \text{ for all } x, y \in \mathbb{F}_{q^{2m}}.$$

As the trace form of separable extensions is a non-degenerate bilinear form and the Galois automorphism $x \mapsto x^{q^m}$ of $\mathbb{F}_{q^{2m}}$ is bijective, also B_α is non-degenerate.
An easy way to see that Q_α is isometric to $Q^-_{2m}(q)$ is to count the number of isotropic vectors: The norm $N : \mathbb{F}_{q^{2m}} \to \mathbb{F}_{q^m}, x \mapsto x^{q^m}x$ is a surjective anisotropic quadratic form that restricts to a group epimorphism on the multiplicative groups. So for any $a \in \mathbb{F}_{q^m} \setminus \{0\}$ the number of $x \in \mathbb{F}_{q^{2m}} \setminus \{0\}$ with $N(x) = a$ is $q^m + 1$. The quadratic form Q_α is the composition of N with multiplication by α followed by the trace. The trace is an $\mathbb{F}_q$-linear surjective map form $\mathbb{F}_{q^m}$ to $\mathbb{F}_q$, so the kernel of the trace is an $(m-1)$-dimensional subspace of $\mathbb{F}_{q^m}$ and, in particular, contains $q^{m-1} - 1$ non-zero elements. So the number of isotropic vectors of Q_α is $(q^{m-1} - 1)(q^m + 1)$. $\square$

Proposition 2.4. *Let $Q : V \to \mathbb{F}_q$ be a non-degenerate quadratic form and $G \leq O(Q)$ be an abelian subgroup of the orthogonal group of Q such that*

(a) The $\mathbb{F}_q$-algebra A spanned by the matrices in G is semi-simple

$A = \bigoplus_{i=1}^n K_i$ for extension fields K_i of $\mathbb{F}_q$

(b) All simple summands K_i are invariant under the adjoint involution of B_Q.

(c) The restriction of this involution to K_i is non-trivial for all i.

Then Q is of $+$ type if and only if the number of composition factors of the A-module V is even.

Proof. The set of isomorphism classes of simple A-modules is $\{K_i \mid 1 \leq i \leq n\}$ and the A-module V is hence the direct sum $V \cong \bigoplus_{i=1}^n K_i^{d_i}$ for some $d_i \in \mathbb{N}$. As the adjoint involution fixes each primitive idempotent of A, the summands $K_i^{d_i}$ are pairwise orthogonal. The restriction of the involution to the simple summand K_i of A is the field automorphism F_i of order 2, so the bilinear form B_Q induces Hermitian forms on these orthogonal summands. So there are $\alpha_{i1}, \dots, \alpha_{id_i}$ in the fixed field of F_i such that

$$Q = \perp_{i=1}^n \perp_{j=1}^{d_i} Q_{\alpha_{ij}}$$

for quadratic forms $Q_{\alpha_{ij}} : K_i \to \mathbb{F}_q$ as in Proposition 2.3. As these are of $-$ type, the statement follows by applying the addition formulas from Remark 2.1. $\square$

Note that the assumption from Proposition 2.4 is equivalent to the assumption that the restriction of V to G is an orthogonally stable orthogonal representation in the sense of [5, Definition 5.12]. In the language of [5] the statement of Proposition 2.4 can also be deduced from [5, Proposition 3.12].

3 The orthogonal representations of $\mathrm{SL}_2(p^f)$

In this section we fix the following notation:

- p is a prime, $q := p^f$,

$$G := \mathrm{SL}_2(q) := \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathbb{F}_q^{2\times 2} \mid ad - bc = 1 \right\}$$

  is the group of determinant 1 matrices over the finite field with q elements.

- $V := \mathbb{F}_q^2$ is the natural $\mathbb{F}_q G$-module.
- If q is odd then $Z(\mathrm{SL}_2(q)) = \langle -I_2 \rangle$ and $\mathrm{PSL}_2(q) = \mathrm{SL}_2(q)/Z(\mathrm{SL}_2(q))$ is simple for $q \geq 5$.
- If q is even, then $\mathrm{SL}_2(q)$ is simple for $q \geq 4$.
- The group $\mathrm{SL}_2(2)$ is isomorphic to S_3.

3.1 The irreducible modules and their fields of definition

For $f = 1$, the following is well known:

Fact 3.1. *The irreducible $\mathbb{F}_p \mathrm{SL}_2(p)$-modules are given by $W_0, \ldots, W_{p-1}$, where*

$$W_k := \mathrm{Sym}_k(V) = \mathbb{F}_p[x, y]_{deg=k}$$

is the space of homogeneous polynomials on V of degree k. All W_k are absolutely irreducible and the dimension of W_k is $k + 1$.

For arbitrary $f \in \mathbb{N}$ we know that $\mathbb{F}_q$ is a splitting field for $\mathrm{SL}_2(q)$ and the irreducible $\mathbb{F}_q \mathrm{SL}_2(q)$-modules are given by Steinberg's tensor product theorem: The Galois group $\mathrm{Gal}(\mathbb{F}_{p^f}/\mathbb{F}_p) = \langle F \rangle$ acts on the group $\mathrm{SL}_2(q)$ by applying the Galois automorphism to the entries of the matrices. For $0 \leq i \leq f-1$ let $V^{[i]}$ denote the natural $\mathbb{F}_q \mathrm{SL}_2(q)$-module V where the action is twisted by F^i and $W_k^{[i]} := \mathrm{Sym}_k(V^{[i]})$.

Fact 3.2. *The irreducible $\mathbb{F}_q \mathrm{SL}_2(q)$-modules are given by*

$$W(\mathbf{k}) = W(k_0, \ldots, k_{f-1}) = W_{k_0}^{[0]} \otimes \ldots \otimes W_{k_{f-1}}^{[f-1]}$$

for $\mathbf{k} := (k_0, \ldots, k_{f-1}) \in \{0, \ldots, p-1\}^f$. The $W(\mathbf{k})$ are pairwise non-isomorphic, absolutely irreducible and of dimension $\dim(W(k_0, \ldots, k_{f-1})) = \prod_{i=0}^{f-1}(k_i + 1)$.

The action of the Galois group on these irreducible modules is given by cyclic permutation:

$$W(k_0,\dots,k_{f-1})^F \cong W(k_{f-1},k_0,\dots,k_{f-2}).$$

As the modules $W(\mathbf{k})$ are pairwise non isomorphic, the representation on $W(\mathbf{k})$ can be realised over the fixed field of F^ℓ if and only if

$$(k_0,\dots,k_{f-1}) = (k_{f-\ell},k_{f-\ell+1},\dots,k_{f-\ell-1}).$$

Remark 3.3. Let $\ell \geq 1$ be minimal such that

$$\mathbf{k} := (k_0,\dots,k_{f-1}) = (k_{f-\ell},k_{f-\ell+1},\dots,k_{f-\ell-1}).$$

Then ℓ divides f. Put $\mathbb{F}(\mathbf{k}) := \mathbb{F}_{p^\ell}$ to be the fixed field of F^ℓ in $\mathbb{F}_q$. Then $\mathbb{F}(\mathbf{k})$ is the field of definition of the module $W(\mathbf{k})$.
By abuse of notation we denote the corresponding $\mathbb{F}(\mathbf{k})\,\mathrm{SL}_2(q)$-module again by $W(\mathbf{k})$.

3.2 Invariant quadratic forms

For $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathbb{F}_{p^f}^{2\times 2}$ and $J := \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ we have $AJA^{tr} = \det(A)J$, so the natural $\mathbb{F}_q\,\mathrm{SL}_2(q)$-module $V = \mathbb{F}_q^2$ carries a non-degenerate alternating G-invariant bilinear form. This yields a non-degenerate G-invariant bilinear form B_k on the space of homogenous polynomials

$$B_k : \mathbb{F}_q[x,y]_{deg=k} \times \mathbb{F}_q[x,y]_{deg=k} \to \mathbb{F}_q : B_k(g,h) := g\left(-\frac{\partial}{\partial y}, \frac{\partial}{\partial x}\right)(h(x,y)).$$

The form B_k is symmetric if k is even and alternating if k is odd.

Remark 3.4. There is a special case for $q = 2$. Here V carries a non-degenerate quadratic form of $-$ type and $\mathrm{SL}_2(2) \leq O_2^-(2)$.

Remark 3.5. (see [6, Proposition 3.4], [3, Proposition 9.1.2]) Let G be a group and let (V,B) and (W,B') be G-invariant alternating non-degenerate bilinear forms on the KG-modules V and W. Then

$$Q : V \otimes W \to K,\ Q\left(\sum_{i=1}^{n} v_i \otimes w_i\right) := \sum_{i<j} B(v_i,v_j)B'(w_i,w_j)$$

is a G-invariant quadratic form on $V \otimes W$ with polarisation $B \otimes B'$. If $U \leq V$ is an isotropic subspace, i.e. $B(U,U) = \{0\}$, then $Q(U \otimes W) = \{0\}$. In particular, the Witt index of Q is $m := \dim(V \otimes W)/2$. If $K = \mathbb{F}_q$ is a finite field, this shows that Q is isometric to $Q_{2m}^+(q)$.

Proposition 3.6. *Assume that $q \neq 2$. Let $\mathbf{k} := (k_0, \ldots, k_{f-1})$ and $\mathbb{F}(\mathbf{k})$ be as in Remark 3.3 and put $e(\mathbf{k}) := |\{i \mid k_i \text{ is odd }\}|$. Then the $\mathbb{F}(\mathbf{k})G$-module $W(\mathbf{k})$ carries a non-degenerate G-invariant quadratic form $Q_{\mathbf{k}}$ if and only if either*

(i) q is odd and $e(\mathbf{k})$ is even.

(ii) q is even and $\dim(W(\mathbf{k})) \geq 4$.

If $[\mathbb{F}_q : \mathbb{F}(\mathbf{k})]$ is odd, then $Q_{\mathbf{k}}$ has maximal Witt index and hence is of $+$ type.

Proof. (i) As $W(\mathbf{k})$ is absolutely irreducible any G-invariant bilinear form is a scalar multiple of $B_{\mathbf{k}} := B_{k_0} \otimes \ldots \otimes B_{k_{f-1}}$. This form is symmetric if and only if $e(\mathbf{k})$ is even.
(ii) If q is even and $W(\mathbf{k})$ is a proper tensor product, then Remark 3.5 yields such an invariant quadratic form $Q_{\mathbf{k}}$. Since both orthogonal groups of dimension 2 are solvable, there cannot be an invariant quadratic form on $W(\mathbf{k})$ if $\dim(W(\mathbf{k})) = 2$ and $q > 2$.
In both cases (q even or odd) Remark 3.5 states that $Q_{\mathbf{k}}$ is of maximal Witt index over the splitting field $\mathbb{F}_q$. As odd degree extensions do not change the type of a quadratic form (see for instance [6, Proposition 4.9]) they are of the same type, if $[\mathbb{F}_q : \mathbb{F}(\mathbf{k})]$ is odd. □

3.3 The type of $Q_{\mathbf{k}}$

This section finishes the proof of our main result:

Theorem 3.7. *Let $q \neq 2$. The quadratic form $Q_{\mathbf{k}} : W(\mathbf{k}) \to \mathbb{F}(\mathbf{k})$ from Proposition 3.6 is of $+$ type except for the case that $\dim(W(\mathbf{k})) \equiv 4 \pmod 8$ and $[\mathbb{F}_q : \mathbb{F}(\mathbf{k})] = 2$ where this form is of $-$ type.*

The case $q = 2$ is given in Remark 3.4.

Proposition 3.6 proves Theorem 3.7 in the case that $[\mathbb{F}_q : \mathbb{F}(\mathbf{k})]$ is odd so it remains to consider the case where this degree is even, i.e. f is even and

$$\mathbf{k} = (k_0, \ldots, k_{f/2-1}, k_0, \ldots, k_{f/2-1})$$

where at least one of the k_i is odd. In this case we show that the non-split torus T of $\mathrm{SL}_2(q)$ acts on $W(\mathbf{k})$ such that the image A of $\mathbb{F}(\mathbf{k})T$ in $\mathrm{End}(W(\mathbf{k}))$ is a semi-simple subalgebra that is a direct sum of even degree extension fields of $\mathbb{F}(\mathbf{k})$. Then Proposition 2.4 allows us to conclude that the type of $Q_{\mathbf{k}}$ is $-$ if and only if the number of composition factors of the A-module $W(\mathbf{k})$ is odd.

Let $t \in \mathrm{SL}_2(q)$ denote an element of order $q + 1$. Put $\tau, \tau^q \in \mathbb{F}_{q^2}$ to denote the two eigenvalues of t on the natural $\mathrm{SL}_2(q)$ module $V = \mathbb{F}_q^2$.

Lemma 3.8. *Let $\mathbf{k} = (k_0, \dots, k_{f-1}) \in \{0, \dots, p-1\}^f$ and put $s(\mathbf{k}) := \sum_{i=0}^{f-1} k_i p^i$. Then $s(\mathbf{k}) \leq p^f - 1$.*
The eigenvalues of t on $W(\mathbf{k})$ are exactly the elements τ^e with

$$e \in E(\mathbf{k}) := \left\{ s(\mathbf{k}) - 2\sum_{i=0}^{f-1} x_i p^i \mid x_i \in \{0, \dots, k_i\}\} \subseteq \{-s(\mathbf{k}), \dots, s(\mathbf{k}) \right\}.$$

Proof. After extending the field to $\mathbb{F}_{q^2}$ we choose a basis of V consisting of eigenvectors of t. Then the monomials in $W_k^{[i]}$ are eigenvectors of t where the eigenvalue of $x^{k-j}y^j$ is τ^e with $e = (k-2j)p^i$. So the eigenvalues of t on $W(\mathbf{k})$ are the elements τ^e where

$$e \in E(\mathbf{k}) := \{\sum_{i=0}^{f-1} m_i p^i \mid -k_i \leq m_i \leq k_i, k_i - m_i \text{ even}\}.$$

Replacing m_i by $k_i - 2x_i$ yields the description in the lemma. □

Lemma 3.9. *We have $0 \in E(\mathbf{k})$ if and only if all k_i are even.*
If p is odd, f is even, and one of $\pm(p^f+1)/2 \in E(\mathbf{k})$ then $s(\mathbf{k})$ is odd.

Proof. If $0 \in E(\mathbf{k})$ then there are $x_i \in \{0, \dots, k_i\}$ such that $\sum_{i=0}^{f-1} k_i p^i = \sum_{i=0}^{f-1} 2x_i p^i$. Taking the equation mod p, we get that $2x_0 \equiv_p k_0$. As $2x_0 \in \{0, 2, \dots, 2k_0\}$ and $k_0 < p$, we hence have $2x_0 = k_0$ so k_0 is even and $x_0 = k_0/2$. Continuing like this, we obtain that $x_i = k_i/2$ for all i.
Now assume that p is odd, f is even, and $\pm(p^f+1)/2 \in E(\mathbf{k})$. Then $s(\mathbf{k}) = 2\sum_{i=0}^{f-1} x_i p^i \pm (p^f+1)/2$. As f is even, $(p^f+1)/2$ is odd and so is $s(\mathbf{k})$. □

Proof. (of Theorem 3.7) Under the assumptions of the lemma $s(\mathbf{k}) = (1+p^{f/2})\sum_{i=0}^{f/2-1} k_i p^i$ is even and hence Lemma 3.9 shows that t has no eigenvalues ± 1 on $W(\mathbf{k})$. Now the order of t is $p^f + 1$. As $\gcd(p^f - 1, p^f + 1) = 2$ (or 1) all eigenvalues of t that are not ± 1 generate a quadratic extension of $\mathbb{F}_q$. Let $A := \mathbb{F}(\mathbf{k})[t] \leq \mathrm{End}(W(\mathbf{k}))$ be the $\mathbb{F}(\mathbf{k})$-subalgebra generated by the endomorphism t of $W(\mathbf{k})$. Then $A = \bigoplus_{i=1}^n K_i$ is semi-simple and commutative. As the adjoint involution of B_Q inverts the elements of $O(Q)$ and inverting the eigenvalues of t is non-trivial on K_i, this involution is the field automorphism of order 2 on each of the K_i. To apply Proposition 2.4 it is hence enough to determine the parity of the number of composition factors of the A-module $W(\mathbf{k})$. If $d := [\mathbb{F}_q : \mathbb{F}(\mathbf{k})] = 2^a b$ with $a \geq 1$ and b odd then

$$2^{a+1} \text{ is the 2-part of } [K_i : \mathbb{F}(\mathbf{k})] \text{ for all } i \tag{2}$$

because the subfields of 2-power index of $\mathbb{F}_{q^2}$ are linearly ordered.
As $\mathbf{k}$ consists of the d-fold juxtaposition of a squence of length f/d and one of the k_i is odd, at least d of the k_i are odd and hence

$$\dim(W(\mathbf{k})) = \prod_{i=0}^{f-1}(k_i + 1) \tag{3}$$

is divisible by 2^d.
So the number of composition factors of V is odd, if and only if 2^{a+1} is the maximal 2-power that divides $\dim(W(\mathbf{k}))$. In particular,

$$a + 1 \geq d = 2^a b,$$

which implies that $a = 1 = b$, i.e. $d = 2$, so $\mathbb{F}(\mathbf{k}) = \mathbb{F}_{p^{f/2}}$. Moreover $\dim(W(\mathbf{k})) \equiv 4 \pmod 8$. $\square$

References

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

[2] Rainer Burkhardt, Die Zerlegungsmatrizen der Gruppen $\mathrm{PSL}(2, p^f)$. J. Algebra 40, 75-96 (1976).

[3] Skip Garibaldi and Daniel K. Nakano, Bilinear and quadratic forms on rational modules of split reductive groups. Can. J. Math. 68, No. 2, 395-421 (2016).

[4] Martin Kneser, Quadratische Formen. Neu bearbeitet und herausgegeben in Zusammenarbeit mit Rudolf Scharlau. Springer (Berlin) (2002)

[5] Gabriele Nebe and Richard Parker, Orthogonal Stability, J. Algebra 614, 362–391 (2023).

[6] Peter Sin and Wolfgang Willems, G-invariant quadratic forms, J. Reine Angew. Math. **420** (1991) 45–59.