

ORTHOGONAL REPRESENTATIONS OF TWISTED FORMS OF SL_2

SKIP GARIBALDI

ABSTRACT. For every absolutely irreducible orthogonal representation of a twisted form of SL_2 over a field of characteristic zero, we compute the “unique” symmetric bilinear form that is invariant under the group action. We also prove the analogous result for Weyl modules in prime characteristic (including characteristic 2) and an isomorphism between two symmetric bilinear forms given by binomial coefficients.

Let V be an absolutely irreducible and finite-dimensional representation of a group G over a field k . If there is a nonzero quadratic form q on V that is invariant under G , then by Schur’s Lemma q is uniquely determined up to multiplication by an element of k^\times . It is natural to ask: *What is q ?* On the one hand, the form q gives some information about G . For example, when V is the adjoint representation, q is essentially the Killing form on the Lie algebra of G . On the other hand, if G is contained in a group H , then by restricting representations of H , one reduces the problem of computing the H -invariant quadratic forms to the problem of computing those invariant under G . This is the method used in [Jac] to calculate the Killing forms of various Lie algebras.

The purpose of this paper is to answer the question “What is q ?” for the smallest groups, i.e., groups of type A_1 , meaning twisted forms of SL_2 and PGL_2 . We study Weyl modules V instead of absolutely irreducible representations. (If k has characteristic zero, this is no change at all. In prime characteristic, the results for Weyl modules imply those for irreducible representations, see 6.9.)

Recall that the group SL_2 has a unique fundamental dominant weight ω . We write $V(n)$ for the Weyl module with highest weight $n\omega$, where n is a non-negative integer. If k has characteristic zero, $V(n)$ is isomorphic to the n -th symmetric power of k^2 . For every field k , every group of type A_1 , and n even, the representation $V(n)$ is k -defined (as can easily be seen by Galois descent as in [BT, p. 139]) and has a nonzero quadratic form invariant under the group action. We compute this quadratic form. For remarks on the modules $V(n)$ with n odd, see 6.8.

We now state our main results in the case where k has characteristic $\neq 2$. The situation in characteristic 2 is very different from other characteristics, and *from here through §5, we only consider fields of characteristic $\neq 2$.*

Define a symmetric bilinear form ϕ_n^{odd} by

$$(0.1) \quad \phi_n^{\mathrm{odd}} := \bigoplus_{\substack{0 \leq i < n/2 \\ i \text{ odd}}} \left\langle \binom{n}{i} \right\rangle.$$

2000 *Mathematics Subject Classification.* 20G05 (11E04, 11E76, 20G15).
Version of June 9, 2008.

The notation $\langle \lambda \rangle$ denotes a one-dimensional vector space spanned by a vector e endowed with a symmetric bilinear form that sends $(e, e) \mapsto \lambda$ for $\lambda \in k^\times$ and \oplus means ‘orthogonal sum’. The form ϕ_2^{odd} is 0-dimensional, and ϕ_4^{odd} is $\langle 1 \rangle$. We refer to [L] for general background on symmetric bilinear forms and quaternion algebras. In particular, since the characteristic is not 2, we can and do identify symmetric bilinear forms with quadratic forms by sending a symmetric bilinear form b to the quadratic form $v \mapsto b(v, v)$.

Every semisimple algebraic group of type A_1 over k is isogenous to $\text{SL}(Q)$ for some quaternion k -algebra Q , where $\text{SL}(Q)$ denotes the group whose k -points are the norm 1 elements of Q . We write Q also for the norm form on Q ; it is a quadratic form. We write Q' for the unique 3-dimensional quadratic form such that $Q = \langle 1 \rangle \oplus Q'$.

Theorem A ($\text{char } k \neq 2$). *For n even, there is an $\text{SL}(Q)$ -invariant symmetric bilinear form on the Weyl module $V(n)$ that is isomorphic to*

$$\langle 2 \rangle \cdot \phi_n^{\text{odd}} \cdot Q \oplus \begin{cases} \left\langle \binom{n}{n/2} \right\rangle & \text{if } n \equiv 0 \pmod{4} \\ \left\langle \binom{n}{n/2} \right\rangle Q' & \text{if } n \equiv 2 \pmod{4}. \end{cases}$$

The smallest case of Theorem A is where $n = 2$, i.e., the adjoint representation of $\text{SL}(Q)$. There we find the symmetric bilinear form $\langle 2 \rangle Q'$, whereas the Killing form is $\langle -2 \rangle Q'$.

The proof of Th. A gives a result on symmetric bilinear forms as a byproduct. Define a form ϕ_n^{even} as in (0.1), except with the word ‘odd’ replaced with ‘even’ throughout. For example, ϕ_2^{even} and ϕ_4^{even} are $\langle 1 \rangle$, and ϕ_6^{even} is $\langle 1, 15 \rangle$.

Theorem B ($\text{char } k \neq 2$). *We have the following isomorphism of symmetric bilinear forms over k :*

$$\phi_n^{\text{even}} \cong \begin{cases} \phi_n^{\text{odd}} & \text{if } n \equiv 0 \pmod{4} \\ \left\langle 2 \binom{n}{n/2} \right\rangle \oplus \phi_n^{\text{odd}} & \text{if } n \equiv 2 \pmod{4}. \end{cases}$$

As an illustration, for $n = 16$, Th. B asserts the isomorphism

$$\left\langle \binom{16}{0}, \binom{16}{2}, \binom{16}{4}, \binom{16}{6} \right\rangle \cong \left\langle \binom{16}{1}, \binom{16}{3}, \binom{16}{5}, \binom{16}{7} \right\rangle,$$

i.e.,

$$\langle 1, 2^3 \cdot 3 \cdot 5, 2^2 \cdot 5 \cdot 7 \cdot 13, 2^3 \cdot 7 \cdot 11 \cdot 13 \rangle \cong \langle 2^4, 2^4 \cdot 5 \cdot 7, 2^4 \cdot 3 \cdot 7 \cdot 13, 2^4 \cdot 5 \cdot 11 \cdot 13 \rangle.$$

Note that the forms ϕ_n^{even} and ϕ_n^{odd} may be degenerate if the characteristic of k is not zero.

One might imagine that Theorem B is known, but the experts I consulted said they had never seen it before. For small n and fields of characteristic zero, one can check the theorem using the Hasse-Minkowski Principle. The proof of Theorem B given below uses neither Hasse-Minkowski nor clever manipulations of binomial coefficients.

The text through §5 is concerned with proving Theorems A and B in characteristic different from 2. Section 6 discusses orthogonal representations over all fields, with a special focus on the situation in characteristic 2. The final section, §7, states and proves analogues of Theorems A and B in characteristic 2. We remark that the version of Th. A in characteristic 2 is very different from the result in other

characteristics, in that in characteristic 2 the only Weyl module whose invariant quadratic form depends on Q is $V(2)$.

1. BINOMIAL COEFFICIENTS

This section is purely about integers, and we write n for a positive integer. Kummer proved that the power of a prime p dividing the binomial coefficient $\binom{n}{m}$ is the number of carries when you add m and $n - m$ in base p . We will use the following special case. For a non-negative integer m , the base- p expansion of m is the list of integers m_0, m_1, \dots such that $0 \leq m_j < p$ for all j and $m = \sum_j m_j p^j$.

Lemma 1.1 (Kummer, 1852). *For $0 \leq m \leq n$, the binomial coefficient $\binom{n}{m}$ is divisible by a prime p if and only if in the base- p expansions of m and n , there is some place j with $m_j > n_j$.*

Proof. See, for example, [F, Th. 1] or [Gr]. □

Lemma 1.2. *Let p be an odd prime. If n is divisible by 4, the lists*

$$\binom{n}{0}, \binom{n}{2}, \dots, \binom{n}{n/2-2} \quad \text{and} \quad \binom{n}{1}, \binom{n}{3}, \dots, \binom{n}{n/2-1}$$

have the same number of elements that are divisible by p .

If n is congruent to 2 mod 4, then the lists

$$\binom{n}{0}, \binom{n}{2}, \dots, \binom{n}{n/2-1} \quad \text{and} \quad \binom{n}{1}, \binom{n}{3}, \dots, \binom{n}{n/2-2}, \binom{n}{n/2}$$

have the same number of elements that are divisible by p .

The analogous statement is false for $p = 2$, see the characteristic 2 version of Th. B in §7 below.

Proof. We write n_j and m_j for the j -th terms in the base- p expansions of n and m .

Case 1. Suppose first that some n_ℓ of n is odd. Whether n is congruent to 0 or 2 mod 4, the two lists have the same length. So it suffices to prove that the lists have the same number of elements that are *not* divisible by p .

Write h_0, h_1, \dots for the base- p expansion of $n/2$, so $n/2 = \sum h_j p^j$ and $n = \sum (2h_j) p^j$. But since n_ℓ is odd, $2h_0, 2h_1, \dots$ cannot be the base p representation of n , and p divides $\binom{n}{n/2}$.

Let S be the set of numbers whose base- p expansion is $\sum s_j p^j$ with $0 \leq s_j \leq n_j$ for all j and s_ℓ is zero. Write \hat{S} for the collection of numbers

$$(1.3) \quad s, s + p^\ell, s + 2p^\ell, \dots, s + n_\ell p^\ell$$

as s varies over elements of S . The set \hat{S} is precisely the set of numbers m with $0 \leq m \leq n$ such that p does not divide $\binom{n}{m}$.

We note that half of the numbers in (1.3) are even and half are odd, since n_ℓ and p are both odd. As $\binom{n}{m}$ equals $\binom{n}{n-m}$, the numbers $m, n - m$ have the same parity, and $n/2$ is not in \hat{S} , we conclude that one quarter of \hat{S} belongs to each of the two lists. This proves the lemma in this case.

Case 2. Now suppose that every base- p digit n_j of n is even. We examine the set \hat{T} of numbers m such that $0 \leq m \leq n$ and p divides $\binom{n}{m}$. Such m 's are exactly those whose base- p expansion m_0, m_1, \dots has a position ℓ such that $m_j = n_j$ for

$j > \ell$,¹ $m_\ell < n_\ell$, and there is some $j < \ell$ such that $m_j > n_j$. Put T_ℓ for the set of integers t whose base- p expansion t_0, t_1, \dots has $t_j = n_j$ for $j > \ell$, has $t_\ell = 0$, and has $t_j > n_j$ for some $j < \ell$. Then \hat{T} is the union of the (disjoint) collections

$$(1.4) \quad t, t + p^\ell, t + 2p^\ell, \dots, t + (n_\ell - 1)p^\ell$$

for $t \in T_\ell$ and $0 < \ell \leq r$. Half of (1.4) is even and half is odd, so half of \hat{T} is even and half is odd. Further \hat{T} does not contain $\binom{n}{n/2}$ by the hypothesis on n . As in Case 1, we conclude that the two lists have the same number of terms that are divisible by p . \square

2. DESCRIPTION OF $V(n)$ IN THE SPLIT CASE

Suppose that Q is split, i.e., that $\mathrm{SL}(Q)$ is the split group SL_2 . Recall the well-known $\mathrm{SL}_2(\mathbb{Q})$ -invariant bilinear form on the n -th symmetric power $S^n(\mathbb{Q}^2)$: Fix a basis e_0, e_1, \dots, e_n given by

$$e_m := \binom{n}{m} \begin{bmatrix} 1 \\ 0 \end{bmatrix}^{n-m} \begin{bmatrix} 0 \\ 1 \end{bmatrix}^m$$

where $\binom{n}{m}$ denotes a binomial coefficient and $\begin{bmatrix} 1 \\ 0 \end{bmatrix}$ and $\begin{bmatrix} 0 \\ 1 \end{bmatrix}$ are the standard basis vectors for \mathbb{Q}^2 . The bilinear form f on $S^n(\mathbb{Q}^2)$ given by

$$(2.1) \quad f(e_\ell, e_m) = \begin{cases} 0 & \text{if } \ell + m \neq n \\ (-1)^\ell \binom{n}{\ell} & \text{if } \ell + m = n \end{cases}$$

is preserved by SL_2 [Bou, §VIII.1.3, Remark 3].

We view the group SL_2 as a Chevalley group defined over \mathbb{Z} as in [St] by fixing a pinning. The elements e_0, e_1, \dots, e_n in $S^n(\mathbb{Q}^2)$ span a minimal admissible lattice L in $S^n(\mathbb{Q}^2)$, see e.g. [Hum, §27, Exercise 8]. The Weyl module $V(n)$ with highest weight $n\omega$ over the field k is $L \otimes_{\mathbb{Z}} k$. In particular, it has basis e_0, e_1, \dots, e_n , and the form f extends to an SL_2 -invariant bilinear form on the k -vector space $V(n)$.

2.2. The representation $V(n)$ is irreducible if and only if

$$(2.3) \quad \begin{array}{l} k \text{ has characteristic zero or } k \text{ has prime characteristic } p \text{ and } n+1 = \\ rp^s \text{ for integers } r, s \text{ with } 0 \leq r < p, \end{array}$$

see e.g. [W, p. 240]. By Kummer (or §6 below), this condition is also equivalent to f being nondegenerate over k , i.e., that none of the binomial coefficients $\binom{n}{m}$ are divisible by the characteristic for $1 \leq m \leq n$.

From here on, we restrict to the case where n is even.

Remark 2.4. Within the line of SL_2 -invariant symmetric bilinear forms on $V(n)$, the isomorphism class of f is distinguished by the fact that

$$f(e_0, \rho \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} e_0) = f(e_0, (-1)^n e_0) = 1$$

is a square in k^\times . More generally, for every maximal torus T contained in a Borel subgroup B of SL_2 , every highest weight vector $v \in V(n)$ (relative to T and B), and every element $w \in N_{\mathrm{SL}_2}(T)(k)$ that represents the element -1 in the Weyl group, we have: *If s is an SL_2 -invariant symmetric bilinear form on $V(n)$ such that $s(v, wv)$ is a square in k^\times , then s is isomorphic to f .* This follows from the conjugacy of pairs $T \subset B$ and the fact that n is even.

¹If ℓ is such that $n_j = 0$ for $j > \ell$, then this condition just says that $m_j = 0$, which is a consequence of the hypothesis that $m \leq n$.

3. COMPUTATIONS

We now address Theorem A in the case where Q is not split. We maintain the assumptions that n is even and the characteristic of k is different from 2.

The representation $\rho: \mathrm{SL}_2 \rightarrow \mathrm{GL}(V(n))$ kills the center ± 1 of SL_2 and so induces a homomorphism $\bar{\rho}: \mathrm{PGL}_2 \rightarrow \mathrm{GL}(V(n))$, where PGL_2 denotes the (algebraic-group-theoretic) quotient $\mathrm{SL}_2/\{\pm 1\}$. As the form f defined in §2 is SL_2 -invariant, the images of ρ and $\bar{\rho}$ lie in the orthogonal group $\mathrm{O}(f)$ of f , and we obtain a map in Galois cohomology

$$(3.1) \quad H^1(k, \mathrm{PGL}_2) \rightarrow H^1(k, \mathrm{O}(f)).$$

The sets $H^1(k, \mathrm{PGL}_2)$ and $H^1(k, \mathrm{O}(f))$ classify k -forms of SL_2 and symmetric bilinear forms over k that become isomorphic to f over a separable closure of k , respectively [Se02, §III.1], and the image of a group $\mathrm{SL}(Q)$ in $H^1(k, \mathrm{O}(f))$ is an $\mathrm{SL}(Q)$ -invariant symmetric bilinear form f_n on V .

Remark 3.2. The map (3.1) is defined for every extension K/k and so leads to a morphism of functors $H^1(*, \mathrm{PGL}_2) \rightarrow H^1(*, \mathrm{O}(f))$. Suppose that f is nondegenerate, i.e., (2.3) holds. By [Se03, 28.4], the map (3.1) is necessarily of the form

$$Q \mapsto \psi_0 \oplus \psi_1 \cdot Q'$$

for uniquely-determined symmetric bilinear forms ψ_0, ψ_1 defined over k with ψ_1 anisotropic. The point of Th. A is to give ψ_0 and ψ_1 explicitly.

The k -algebra Q is generated by elements i, j such that $i^2 = a$, $j^2 = b$, and $ij = -ji$ for some $a, b \in k^\times$. As Q is not split, a is not a square in k and $k(\sqrt{a})$ is a proper extension. The algebra Q is isomorphic to the k -subalgebra of $M_2(k(\sqrt{a}))$ generated by

$$\begin{pmatrix} \sqrt{a} & 0 \\ 0 & -\sqrt{a} \end{pmatrix} \quad \text{and} \quad \begin{pmatrix} 0 & b \\ 1 & 0 \end{pmatrix},$$

which we may identify with i and j respectively. For ι the nonidentity k -automorphism of $k(\sqrt{a})$, Q is obtained from $M_2(k)$ by twisting by the cocycle $\eta \in Z^1(k(\sqrt{a})/k, \mathrm{PGL}_2)$ given by

$$(3.3) \quad \eta_\iota = \mathrm{Int} \begin{pmatrix} 0 & b \\ 1 & 0 \end{pmatrix},$$

where we write $\mathrm{Int}(g)$ for the map $x \mapsto gxg^{-1}$ on M_2 . (Recall that for an extension K/k , the K -points of PGL_2 are of the form $\mathrm{Int}(g)$ for $g \in \mathrm{GL}_2(K)$.)

We now compute $\bar{\rho}(\eta_\iota) \in \mathrm{O}(f)(k(\sqrt{a}))$. Write k_{sep} for a separable closure of k . The element

$$\beta := \begin{pmatrix} 0 & -\sqrt{-b} \\ 1/\sqrt{-b} & 0 \end{pmatrix} \in \mathrm{SL}_2(k_{\mathrm{sep}})$$

is a scalar multiple of η_ι , hence has the same image in $\mathrm{PGL}_2(k)$ and $\bar{\rho}(\eta_\iota)$ equals $\rho(\beta)$. We find:

$$\bar{\rho}(\eta_\iota)e_m = \rho(\beta)e_m = (-1)^{n/2}b^{m-(n/2)}e_{n-m}.$$

The action of $\bar{\rho}(\eta_\iota)$ preserves the line spanned by $e_{n/2}$ and the hyperbolic planes spanned by e_m, e_{n-m} for $m \neq n/2$. We compute separately the restriction of f_n to each of these subspaces.

(Here is an alternative view on this computation. The orthogonal group O_2 of the 2-dimensional quadratic form $\begin{bmatrix} x \\ y \end{bmatrix} \mapsto xy$ has identity component SO_2 the torus of diagonal matrices in SL_2 ; write PO_2 for the image of O_2 in PGL_2 . The 1-cocycle η takes values in $\mathrm{PO}_2(k_{\mathrm{sep}})$, and twisting SO_2 by η gives the norm 1 torus for the quadratic extension $k(\sqrt{a})/k$ —equivalently the special orthogonal group

$\text{SO}(\langle 1, -a \rangle)$ of the quadratic form $\langle 1, -a \rangle$ —as a subgroup of $\text{SL}(Q)$. If we twist ρ also by η , we find a representation of $\text{SO}(\langle 1, -a \rangle)$ that is a direct sum of a trivial 1-dimensional representation and $n/2$ copies of the natural representation. We calculate the restriction of f_n to each of these subspaces.)

For the line spanned by $e_{n/2}$, we have $\bar{\rho}(\eta_\iota)e_{n/2} = (-1)^{n/2}e_{n/2}$, so the fixed k -subspace of the line is spanned by $e_{n/2}$ if $n/2$ is even and by $\sqrt{a}e_{n/2}$ if $n/2$ is odd. Therefore the restriction of f_n to this subspace is

$$\left\langle (-a)^{n/2} \binom{n}{n/2} \right\rangle.$$

For the $k(\sqrt{a})$ -plane spanned by e_m, e_{n-m} with $m \neq n/2$, the $\bar{\rho}(\eta_\iota)$ -fixed k -subspace is spanned by

$$e_m + (-1)^{n/2} b^{m-(n/2)} e_{n-m} \quad \text{and} \quad \sqrt{a}e_m - (-1)^{n/2} b^{m-(n/2)} \sqrt{a}e_{n-m}.$$

These vectors are orthogonal and the restriction of f_n to this subspace is

$$\langle 2 \rangle \langle 1, -a \rangle \left\langle (-b)^{m-(n/2)} \binom{n}{m} \right\rangle.$$

Summarizing the previous two paragraphs, we find that f_n is isomorphic to

$$\langle 2 \rangle \langle 1, -a \rangle \left[\bigoplus_{\substack{0 \leq m < n/2 \\ m - (n/2) \text{ odd}}} \left\langle -b \binom{n}{m} \right\rangle \oplus \bigoplus_{\substack{0 \leq m < n/2 \\ m - (n/2) \text{ even}}} \left\langle \binom{n}{m} \right\rangle \right] \oplus \left\langle (-a)^{n/2} \binom{n}{n/2} \right\rangle.$$

That is:

If n is divisible by 4, then f_n is isomorphic to

$$\langle 2 \rangle \langle 1, -a \rangle [\langle -b \rangle \phi_n^{\text{odd}} \oplus \phi_n^{\text{even}}] \oplus \left\langle \binom{n}{n/2} \right\rangle.$$

(3.4) *If n is congruent to 2 mod 4, then f_n is isomorphic to*

$$\langle 2 \rangle \langle 1, -a \rangle [\langle -b \rangle \phi_n^{\text{even}} \oplus \phi_n^{\text{odd}}] \oplus \left\langle -a \binom{n}{n/2} \right\rangle.$$

4. PROOF OF THEOREM B

This purpose of this section is to prove Theorem B. We put $q := \phi_n^{\text{odd}}$ if 4 divides n and $q := \phi_n^{\text{odd}} \oplus \left\langle 2 \binom{n}{n/2} \right\rangle$ if n is congruent to 2 mod 4; we want to show that ϕ_n^{even} and q are isomorphic.

We consider the “generic” case of Th. A, i.e., where k is $\mathbb{F}(a, b)$ where \mathbb{F} is a prime field (of characteristic $\neq 2$) and a, b are independent indeterminates. We write f_n for the form computed in (3.4). Recall that a symmetric bilinear form s on a vector space V induces a nondegenerate form — the *nondegenerate part* of s — on V modulo the radical of s . By Springer’s Theorem (twice), the coefficients of $\langle a \rangle$ and $\langle b \rangle$ in the nondegenerate part of f_n — namely, the nondegenerate parts of $\langle -2 \rangle \phi_n^{\text{even}}$ and $\langle -2 \rangle q$ or vice versa — are determined up to Witt equivalence. The isomorphism class of the form f_n depends only on the isomorphism class of Q and not on the choice of η . In particular, f_n is unchanged when we interchange the roles of a and b , and we conclude that ϕ_n^{even} and q have Witt-equivalent nondegenerate parts. By Lemma 1.2, the forms ϕ_n^{even} and q have nondegenerate parts of the same

dimension. Since the total dimension of ϕ_n^{even} and q is also the same, we conclude that the two forms are isomorphic. This completes the proof of Th. B. \square

5. PROOF OF THEOREM A

We now prove Theorem A for fields of characteristic $\neq 2$. In the case where Q is not split, one combines Theorem B with (3.4) and the fact that the norm of Q is $\langle 1, -a, -b, ab \rangle$. Therefore, we assume that Q is split, in which case the form f from (2.1) is an invariant quadratic form on $V(n)$. For $0 \leq m < n/2$, the elements e_m, e_{n-m} in $V(n)$ span a hyperbolic plane \mathcal{H} if $\binom{n}{m}$ is nonzero and a 2-dimensional subspace of the radical otherwise. We conclude that f is isomorphic to

$$[\mathcal{H} \cdot (\phi_n^{\text{even}} \oplus \phi_n^{\text{odd}})] \oplus \left\langle (-1)^{n/2} \binom{n}{n/2} \right\rangle.$$

(Specialists in symmetric bilinear forms are used to ignoring hyperbolic planes. Here we must keep careful track, because some are multiplied by zero.) By Theorem B, this is isomorphic to

$$[(\mathcal{H} \oplus \mathcal{H}) \cdot \phi_n^{\text{odd}}] \oplus \begin{cases} \left\langle \binom{n}{n/2} \right\rangle & \text{if } n \equiv 0 \pmod{4} \\ \left\langle \binom{n}{n/2} \right\rangle [(-1) \oplus \mathcal{H}] & \text{if } n \equiv 2 \pmod{4}. \end{cases}$$

As Q is split, its quadratic norm form is $\mathcal{H} \oplus \mathcal{H}$ and Q' is isomorphic to $\langle -1, 1, -1 \rangle$. This completes the proof of Th. A. \square

Remark. We proved Theorem A using Galois descent. Alternately, one could in principle prove it—at least in characteristic zero—using the Clebsch-Gordan formula

$$V(n) \otimes V(2) \cong V(n-2) \oplus V(n) \oplus V(n+2)$$

and induction on n , together with a precise description of the inclusion $V(n+2) \subset V(n) \otimes V(2)$.

6. INVARIANT QUADRATIC FORMS ON WEYL MODULES

In this section, k is any field (including the possibility of characteristic 2) and G is a split semisimple linear algebraic group over k . We extend some results on G -invariant bilinear forms on an irreducible representation $L(\lambda)$ with highest weight λ to the case of a Weyl module $V(\lambda)$. Although the extensions are straightforward, we write them explicitly for lack of a better reference. The results are mostly interesting in characteristic 2, but we state them as much as possible in a characteristic-free way.

6.1. First, a clarification. We say that a form f on a representation V of G over k is G -invariant if f is fixed by the algebraic group G (and not merely by the group of k -points $G(k)$). As G is reductive, this is equivalent to saying that $G(K)$ fixes the form f on $V \otimes K$ for some infinite field K containing k . As an example of the difference, the form $\begin{bmatrix} x \\ y \end{bmatrix} \mapsto x^2 + xy + y^2$ on $(\mathbb{F}_2)^2$ is invariant under $SL_2(\mathbb{F}_2)$, but one can check by hand that there is no nonzero $SL_2(K)$ -invariant quadratic form on K^2 for any infinite field K . So there is no nonzero SL_2 -invariant quadratic form on k^2 for any field k . Obviously the distinction between G and $G(k)$ -invariance exists only for k finite.

6.2. The usual proofs for irreducible representations in characteristic zero from [Bou] or [GW] show that a Weyl module $V(\lambda)$ has a nonzero G -invariant bilinear

form if and only if $\lambda = -w_0\lambda$ for w_0 the longest element of the Weyl group, and that a nonzero G -invariant bilinear form is uniquely determined up to a factor in k^\times . (The uniqueness comes from the fact that $\text{Hom}_G(V(\lambda), V(\lambda)^*)$ is k ; in characteristic 0 this is Schur's Lemma, here we use [Jan, p. 183].)

Fix a surjection $\pi: V(\lambda) \rightarrow L(\lambda)$. Its kernel is the (*representation-theoretic*) *radical* of $V(\lambda)$, i.e., the intersection of the maximal proper submodules [Jan, II.2.14]. Every nonzero G -invariant bilinear form \bar{s} on $L(\lambda)$ gives a nonzero G -invariant bilinear form s on $V(\lambda)$ by setting $s(x, y) := \bar{s}(\pi(x), \pi(y))$. As \bar{s} is necessarily nondegenerate, the radical of s equals the kernel of π . By uniqueness, the radical of every nonzero G -invariant bilinear form on $V(\lambda)$ is $\ker \pi$.

6.3. In characteristic 2, quadratic forms—not symmetric bilinear forms—are the objects naturally associated with algebraic groups of types B and D , see [Ti 68, §3]. Every quadratic form q gives a symmetric bilinear form b_q by setting $b_q(x, y) := q(x + y) - q(x) - q(y)$. The *radical* of q is defined to be the radical of b_q .

Proposition 6.4. *Let q be a nonzero G -invariant quadratic form on $V(\lambda)$. Then:*

- (1) *If $\lambda \neq 0$ or $\text{char } k \neq 2$, the radical of q is the representation-theoretic radical of $V(\lambda)$.*
- (2) *If q' is a G -invariant quadratic form on $V(\lambda)$, then $q' = cq$ for some $c \in k$.*

If $\lambda = 0$ and k has characteristic 2, then $V(\lambda)$ is the irreducible 1-dimensional representation and the radical of every G -invariant quadratic form q on $V(\lambda)$ is all of $V(\lambda)$.

Proof of Prop. 6.4. In characteristic $\neq 2$, the proposition is a restatement of observations about bilinear forms from 6.2, so we assume that k has characteristic 2. To prove (1), we may enlarge k and so assume that every element of k is a square. For sake of contradiction, suppose that (1) is false, which by 6.2 is equivalent to b_q being identically zero. Then $q(x + y) = q(x) + q(y)$ for all $x, y \in V(\lambda)$ and the elements of $V(\lambda)$ on which q vanishes form a subspace W invariant under G .

We claim that $\dim V/W$ is at most 1. Otherwise, there are elements $v_1, v_2 \in V(\lambda)$ whose images in V/W are linearly independent; in particular, $q(v_1), q(v_2)$ are not zero. Multiplying v_1 by an element of k^\times , we may assume that $q(v_1) = q(v_2)$, so that $v_1 + v_2$ belongs to W . This contradicts the linear independence, proving the claim.

If W is a proper subspace, then it is contained in the radical of $V(\lambda)$, hence maps to zero in $L(\lambda)$. It follows that the dimension of V/W is at least the dimension of $L(\lambda)$, which is at least 2 because $\lambda \neq 0$. We conclude that W is all of V , i.e., that q is zero, a contradiction.

Claim (2) follows easily from the proof of (1), as uniqueness for bilinear forms on $L(\lambda)$ gives a $c \in k$ such that $cb_q - b_{q'}$ is the zero form. \square

We have shown that a G -invariant quadratic form on $V(\lambda)$ —if it exists—is unique (up to scaling) and we have determined the radical. But what about existence? Consider the following:

Example 6.5. For a nonnegative integer n , the irreducible representation $L(n)$ of SL_2 has a nonzero SL_2 -invariant quadratic form if and only if n is even ($\text{char } k \neq 2$) or n is not a power of 2 ($\text{char } k = 2$). To prove the characteristic 2 result for $n \neq 0$, one writes $L(n)$ as a tensor product $\otimes L(1)^{[j]}$ where the product runs over those j such that the term n_j in the base-2 expansion of n is not zero and $L(1)^{[j]}$ denotes the

j -th Frobenius twist of $L(1)$, i.e., the composition of the standard 2-dimensional representation of SL_2 with the map $SL_2 \rightarrow SL_2$ induced by the homomorphism $x \mapsto x^{2^j}$ of k . There is no nonzero SL_2 -invariant quadratic form on $L(1)$ by 6.1, hence none on $L(1)^{[j]}$ for all j . Conversely, $L(1)^{[j]}$ has a nonzero SL_2 -invariant alternating bilinear form for all j , so $\otimes L(1)^{[j]}$ has a nonzero SL_2 -invariant quadratic form if there are at least two terms in the product by, e.g., [KMRT, p. 67, Exercise 21] or [SW, 3.4].

6.6. In general, we have: *There is a nonzero G -invariant quadratic form on the irreducible representation $L(\lambda)$ if and only if there is a nonzero G -invariant quadratic form on the Weyl module $V(\lambda)$ that is zero on the radical of $V(\lambda)$.* Indeed, you can lift a G -invariant quadratic form on $L(\lambda)$ to one on $V(\lambda)$ that is zero on the radical, so the if direction is trivial and the only if direction follows from Prop. 6.4(1).

Example 6.7. For a non-negative integer n , the Weyl module $V(n)$ of SL_2 has a nonzero SL_2 -invariant quadratic form if and only if n is even ($\text{char } k \neq 2$) or $n \neq 1$ ($\text{char } k = 2$). To check this in characteristic 2, one constructs a quadratic form on $V(n)$ for n even by reducing a form defined over \mathbb{Z} , see the next section. The claim for n odd follows from the two preceding paragraphs.

Remark 6.8. In the rest of this paper, we have ignored the Weyl modules $V(n)$ of groups of type A_1 with n odd. We have done so for two reasons. First, *these modules are defined only for SL_2* , that is, they are defined for $SL(Q)$ only if Q is split. Indeed, suppose that there is a representation W of $SL(Q)$ defined over k that is equivalent to $V(n)$ over a separable closure k_{sep} of k . The radical of $V(n)$ is a characteristic submodule, so by Galois descent, there is a k -defined submodule R of W such that W/R is equivalent to the irreducible representation $L(n)$ over k_{sep} . This implies that $n[Q] = 0$ in the Brauer group of k [Ti 71, 3.5], hence that Q is split (because n is odd).

Second, if k has characteristic different from 2, the nonzero SL_2 -invariant bilinear form on $V(n)$ is skew-symmetric and its isomorphism class is uniquely determined by the fact that its radical is the radical of $V(n)$. If k has characteristic 2 and $n \geq 3$, then there is a nonzero SL_2 -invariant quadratic form on $V(n)$ that vanishes on the radical of $V(n)$ by the preceding example. This form is always hyperbolic, because 0 is not a weight of $L(n)$.

6.9. The material in this section implies that—for answering the question “What is q ?” posed at the beginning of this article for absolutely irreducible representations—it suffices to consider the Weyl modules. Suppose that you know a G -invariant quadratic form q on a Weyl module $V(\lambda)$. If the field k has characteristic $\neq 2$, then obviously the invariant form on the irreducible representation $L(\lambda)$ is the nondegenerate part of q . If k has characteristic 2, one applies the criterion 6.6 to determine if $L(\lambda)$ has a nonzero G -invariant quadratic form; if it does, then again it is the nondegenerate part of q .

7. THEOREMS A AND B IN CHARACTERISTIC 2

In this section, the field k has characteristic 2. We prove analogues of Theorems A and B in this setting.

We adopt the notation of [Ba] for symmetric bilinear forms and quadratic forms over k . In particular, $\langle \alpha_1, \dots, \alpha_n \rangle$ denotes the bilinear form $(x, y) \mapsto x^t A y$ on k^n where A is the diagonal matrix whose (i, i) -entry is α_i .

Write $s(n)$ for the number of 1's appearing in the binary expansion of the natural number n . We have:

Theorem B ($\text{char } k = 2$). *For n even, the bilinear form ϕ_n^{odd} is identically zero and the bilinear form ϕ_n^{even} has nondegenerate part $2^{s(n)-1}\langle 1 \rangle$.*

The theorem says the nondegenerate part of ϕ_n^{even} is $\langle 1 \rangle$ if n is a power of 2 and is metabolic otherwise.

Proof. The binomial coefficient $\binom{n}{m}$ is even if and only if some 1 in the binary expansion of m appears where there is a 0 in the binary expansion of n . Hence $\binom{n}{m}$ is even for all odd m , which proves that ϕ_n^{odd} is identically zero. Further, the coefficient $\binom{n}{n/2}$ is even and the number of $\binom{n}{m}$ that are odd is $2^{s(n)}$. The $2^{s(n)}$ odd binomial coefficients are divided evenly between those even m with $0 \leq m < n/2$ and those even m with $n/2 < m \leq n$. Hence the first collection has exactly $2^{s(n)-1}$ members. This proves the claim about ϕ_n^{even} . \square

We fix notations in order to state Theorem A. A quaternion algebra Q over k is generated by elements i, j such that

$$i^2 + i = a, \quad j^2 = b, \quad \text{and} \quad ij = ji + j$$

for some $a \in k$ and $b \in k^\times$. The element i generates a quadratic étale k -algebra K in Q isomorphic to $k[\alpha]/(\alpha^2 + \alpha - a)$, and the norm from this extension is a 2-dimensional quadratic form denoted by $[1, a]$. We write $[c]$ for the 1-dimensional space with basis e endowed with the quadratic form sending $e \mapsto c$.

The norm of Q restricted to the trace zero elements is

$$Q' := [1] \oplus \langle b \rangle [1, a].$$

This can be calculated by identifying $Q \otimes K$ with $M_2(K)$ via

$$(7.1) \quad i \mapsto \begin{pmatrix} \alpha & 0 \\ 0 & \alpha+1 \end{pmatrix} \quad \text{and} \quad j \mapsto \begin{pmatrix} 0 & b \\ 1 & 0 \end{pmatrix}$$

and restricting the determinant of $M_2(K)$ to the k -subspace spanned by $1, j, ij$.

Recall that every quadratic form can be written uniquely as $q_0 \oplus q_{\text{nd}}$, where q_0 is the zero quadratic form and q_{nd} is nondefective, see e.g. [HL, 2.4]; we call q_{nd} the *nondefective part* of q . We write \mathcal{H} for the hyperbolic plane $[0, 0]$.

Theorem A ($\text{char } k = 2$). *Let n be even. There is an $\text{SL}(Q)$ -invariant quadratic form on the Weyl module $V(n)$ that is isomorphic to*

$$\begin{cases} Q' & \text{if } n = 2, \text{ and} \\ [1] \oplus \mathcal{H} \oplus (n-2)[0] & \text{if } n \text{ is a power of 2 and } n \geq 4. \end{cases}$$

Otherwise, the nondefective part of the $\text{SL}(Q)$ -invariant form is $2^{s(n)-1}$ hyperbolic planes.

The form given by the theorem is uniquely determined (up to a scalar factor) by the property of being $\text{SL}(Q)$ -invariant, see Prop. 6.4(2).

Proof. The quadratic form $v \mapsto f(v, v)$ over \mathbb{Z} defined by (2.1) is divisible by 2 because $\binom{n}{n/2}$ is even. Dividing by 2 and extending scalars to k , we find that the quadratic form

$$(7.2) \quad \left(\frac{1}{2}\binom{n}{n/2}\right)x_{n/2}^2 + \sum_{\substack{0 \leq m < n/2 \\ m \text{ even}}} \binom{n}{m}x_mx_{n-m}$$

is SL_2 -invariant, where x_0, x_1, \dots, x_n is a basis of $V(n)^*$ dual to e_0, e_1, \dots, e_n . (The terms $\binom{n}{m}x_mx_{n-m}$ with m odd are zero as in the proof of Th. B.) The isomorphism class of (7.2) is

$$\left[\frac{1}{2}\binom{n}{n/2}\right] \oplus (\phi_n^{\text{even}} \cdot \mathcal{H}).$$

The integer $\frac{1}{2}\binom{n}{n/2}$ is odd if and only if n is a power of 2 by Kummer's criterion from §1 or [KMRT, 10.29]. Applying Th. B completes the proof of Th. A in case Q is split.

Suppose now that Q is not split, and in particular that the subalgebra K of Q generated by the element i is a separable field extension of k . Write ι for the non-identity k -automorphism of K , i.e., the map such that $\iota(\alpha) = \alpha + 1$. Via (7.1), Q is identified with the k -subalgebra of $M_2(K)$ fixed by $\text{Int}(\eta_\iota)\iota$ for η_ι as in (3.3). The same computations as in §3 show that the $SL(Q)$ -invariant form on $V(n)$ has the same nondefective part as

$$(7.3) \quad \left[\frac{1}{2}\binom{n}{n/2}\right] \oplus \phi_n^{\text{even}} \cdot \langle b^{n/2} \rangle \cdot [1, a].$$

This verifies the theorem in case $n = 2$. If n is not a power of 2, we are done by Th. B because ‘metabolic tensor quadratic is hyperbolic’ [Ba, I.4.7].

Finally, if n is a power of 2 and not 2, the nondefective part of (7.3) is $[1] \oplus [1, a]$. But this is the norm on the trace zero elements of the quaternion algebra with $b = 1$, i.e., on $M_2(k)$, hence this form is isomorphic to $[1] \oplus \mathcal{H}$. \square

Acknowledgment. I thank George McNinch and Pham Tiep for their helpful remarks on representations and Jean-Pierre Serre for suggesting the problem and for his comments on an earlier version of this note. My research was partially supported by NSF grant DMS-0654502.

REFERENCES

[Ba] R. Baeza, *Quadratic forms over semilocal rings*, Lecture Notes in Mathematics, vol. 655, Springer, 1978.

[Bo] N. Bourbaki, *Lie groups and Lie algebras: Chapters 7–9*, Springer-Verlag, Berlin, 2005.

[BT] A. Borel and J. Tits, *Groupes réductifs*, Inst. Hautes Études Sci. Publ. Math. **27** (1965), 55–150.

[F] N.J. Fine, *Binomial coefficients modulo a prime*, Amer. Math. Monthly **54** (1947), 589–592.

[Gr] A. Granville, *Arithmetic properties of binomial coefficients. I. Binomial coefficients modulo prime powers*, Organic mathematics (Burnaby, BC, 1995), CMS Conf. Proc., vol. 20, Amer. Math. Soc., Providence, RI, 1997, pp. 253–276.

[GW] R. Goodman and N. Wallach, *Representations and invariants of the classical groups*, Cambridge University Press, 1998.

[HL] D.W. Hoffmann and A. Laghribi, *Quadratic forms and Pfister neighbors in characteristic 2*, Trans. Amer. Math. Soc. **356** (2004), 4019–4053.

- [Hum] J.E. Humphreys, *Introduction to Lie algebras and representation theory*, Graduate Texts in Mathematics, vol. 9, Springer-Verlag, 1980, Third printing, revised.
- [Jac] N. Jacobson, *Exceptional Lie algebras*, Lecture notes in pure and applied mathematics, vol. 1, Marcel-Dekker, New York, 1971.
- [Jan] J.C. Jantzen, *Representations of algebraic groups*, second ed., Amer. Math. Soc., 2003.
- [KMRT] M.-A. Knus, A.S. Merkurjev, M. Rost, and J.-P. Tignol, *The book of involutions*, Colloquium Publications, vol. 44, Amer. Math. Soc., 1998.
- [L] T.Y. Lam, *Introduction to quadratic forms over fields*, Graduate Studies in Mathematics, vol. 67, Amer. Math. Soc., Providence, RI, 2005.
- [Se 02] J.-P. Serre, *Galois cohomology*, Springer-Verlag, 2002, originally published as *Cohomologie galoisienne* (1965).
- [Se 03] ———, *Cohomological invariants, Witt invariants, and trace forms*, Cohomological invariants in Galois cohomology, University Lecture Series, vol. 28, Amer. Math. Soc., 2003, notes by Skip Garibaldi.
- [St] R. Steinberg, *Lectures on Chevalley groups*, Yale University, New Haven, Conn., 1968.
- [SW] P. Sin and W. Willems, *G-invariant quadratic forms*, J. Reine Angew. Math. **420** (1991), 45–59.
- [Ti 68] J. Tits, *Formes quadratiques, groupes orthogonaux et algèbres de Clifford*, Invent. Math. **5** (1968), 19–41.
- [Ti 71] ———, *Représentations linéaires irréductibles d'un groupe réductif sur un corps quelconque*, J. Reine Angew. Math. **247** (1971), 196–220.
- [W] P.W. Winter, *On the modular representation theory of the two-dimensional special linear group over an algebraically closed field*, J. London Math. Soc. (2) **16** (1977), no. 2, 237–252.

DEPARTMENT OF MATHEMATICS & COMPUTER SCIENCE, EMORY UNIVERSITY, ATLANTA, GA 30322, USA

E-mail address: skip@member.ams.org

URL: <http://www.mathcs.emory.edu/~skip/>