Let $q$ be a power of an odd prime $p$, and let $G$ denote the symplectic group $Sp(2n, q)$. The Weil representation $W$ of $G$ is a complex representation of degree $q^n$ that can be obtained from the action of $G$ on an extraspecial group of order $pq^{2n}$. See, for example, [3], [5], or [11] for a more general approach. $W$ is the sum of two irreducible representations that have degrees $(q^n - 1)/2$ and $(q^n + 1)/2$. One of these representations, which we will denote by $W_1$, is faithful, and the other representation, $W_2$, has the central involution $\sigma$ of $G$ in its kernel. It is easy to see that $W_1$ is the irreducible constituent of $W$ that has even degree. Thus $W_1$ has degree $(q^n - 1)/2$ if and only if $q \equiv 1 \pmod{4}$ or $q \equiv 3 \pmod{4}$ and $n$ is even. The representation $W_2$ has odd degree. We will refer to $W_1$ and $W_2$ as Weil representations.

Suppose now that $q \equiv 3 \pmod{4}$. We will show that the characters $\psi_i$ of the $W_i$, $1 \leq i \leq 2$, each generate the field $Q(\sqrt{-p})$ over the rational field $Q$ and have Schur index 1 over $Q$. Thus, in particular, there exists a faithful irreducible $QG$-module $M$ affording the character $\psi_1 + \overline{\psi_1}$, where the bar denotes complex conjugation. Our main result (Theorem 3.2) is that when $n$ is even and $q = p$ is a prime with $p \equiv 3 \pmod{4}$, there exists a $G$-invariant rational integral lattice $L$ in $M$ that supports an even symmetric positive definite unimodular form. This means that $L$ is a free abelian group that contains a basis $e_1, \ldots, e_m$ ($m = q^n - 1$) of $M$ and there is a $G$-invariant integral symmetric form

$$f: L \times L \to \mathbb{Z}$$

such that $f(v, v) \in 2\mathbb{Z}$ for all $v \in L$ and $f(v, v) > 0$ if $v \neq 0$. The fact that $f$ is unimodular means that the determinant of the $m \times m$ integral matrix whose $i, j$ entry is $f(e_i, e_j)$, $1 \leq i, j \leq m$, is 1. More precisely, $f$ is invariant under
the action of an over-group $H$ of $G$, where $|H: G| = 2$, and $L$ is an absolutely irreducible $H$-module. Information about integral symmetric forms can be found, for example, in [6, Chapter V].

At the end of the paper, we discuss possible extensions of our main result when $n$ is odd. Section 1 of the paper contains some information of independent interest on Schur indices of irreducible characters of $Sp(2n, q)$ that are not real-valued.

1. Schur Indices of Certain Characters of $Sp(2n, q)$

In order to investigate invariant integral lattices associated with the Weil representation $W_1$, we will first determine the rational Schur indices of the characters $\psi_1, \psi_2$ when $q \equiv 3 \pmod{4}$.

Let $\text{Irr}(G)$ denote the set of complex irreducible characters of $G$. In [1], we showed that if $q \equiv 1 \pmod{4}$, any $\chi \in \text{Irr}(G)$ is real-valued and if $\chi$ is faithful, it has Schur index 2 over the real field, and hence over $Q$, by the Brauer–Speiser theorem.

When $q \equiv 3 \pmod{4}$, not all characters in $\text{Irr}(G)$ are real-valued and we intend to investigate the Schur indices over $Q$ of such characters. Let $V$ be the natural vector space of dimension $2n$ over $GF(q)$ on which $G$ acts and let

$$b : V \times V \to GF(q)$$

be the non-singular $G$-invariant alternating form. The conformal symplectic group $\bar{G}$ is the group of all automorphisms $h$ of $V$ that satisfy

$$b(hu, hv) = \lambda(h) b(u, v)$$

for all $u, v$ in $V$, where $\lambda(h)$ is a non-zero scalar in $GF(q)$. It is clear that $G$ is normal in $\bar{G}$ and it can be shown that the quotient group $\bar{G}/G$ is isomorphic to the multiplicative group of $GF(q)$. Any scalar multiple of the identity is in $\bar{G}$. Suppose now that $q \equiv 3 \pmod{4}$ and let $\mu$ be a primitive element of order $(q - 1)/2$ in $GF(q)$. Using an obvious notation, we can see that $\bar{G}$ is expressible as a direct product

$$G \cong H \times \langle \mu I \rangle,$$

where $|H: G| = 2$ and $\mu I$ generates a cyclic central subgroup of order $(q - 1)/2$. The elements $h$ of $H - G$ are sometimes called skew-symplectic transformations, as we have

$$b(hu, hv) = -b(u, v)$$
for such an \( h \). We will use the group \( H \) to investigate Schur indices of characters of \( G \).

We begin by analyzing the action of \( H \) on the conjugacy classes of \( G \). We need to quote a theorem of Wonenburger [12].

(1.1) Lemma. Any element of \( G \) is expressible as a product of two involutions of \( H - G \). Thus, each element of \( G \) is a real element of \( H \).

We can now characterize the action of \( H \) on the conjugacy classes of \( G \).

(1.2) Lemma. Suppose that \( q \equiv 3 \pmod{4} \). A conjugacy class \( K \) of \( G \) remains a conjugacy class in \( H \) if and only if \( K \) is a real class in \( G \).

Proof. Let \( x \in K \). By Wonenburger's theorem, we can write

\[
x = uv,
\]

where \( u, v \) are involutions in \( H - G \). We have now

\[
x'' = uv = x^{-1}
\]

and thus \( K'' = K \) if and only if \( K \) is real, and \( K'' = K^{-1} \) precisely when \( K \) forms a class of \( H \). This proves the lemma.

It is now simple to see how \( H \) acts on \( \text{Irr}(G) \).

(1.3) Lemma. Suppose that \( q \equiv 3 \pmod{4} \). Then \( \chi \in \text{Irr}(G) \) is fixed by \( H \) if and only if \( \chi \) is real-valued.

Proof. Let \( u \in H - G \) and let \( K \) be a class of \( G \). The argument used in Lemma 1.2 shows that

\[
K'' = K^{-1},
\]

where \( K^{-1} \) is the class of \( G \) containing the inverses of the elements of \( K \). Thus we have

\[
\chi''(g) = \chi(g''') = \chi(g^{-1}) = \bar{\chi}(g),
\]

for any \( g \in G \), where \( \chi \) is the complex conjugate of \( \chi \). This proves our claim.

We are now in a position to calculate the Schur indices of certain characters in \( \text{Irr}(G) \) that are not real-valued.

(1.4) Theorem. Suppose that \( q \equiv 3 \pmod{4} \). Let \( \chi \in \text{Irr}(G) \) and suppose that \( \chi \) is not real-valued. Then if \( \chi(1) \) is relatively prime to \( p \), \( \chi \) has Schur index 1 over \( Q \).
EVEN UNIMODULAR LATTICES

Proof. By Lemma 1.3, χ is not fixed by H and hence θ = χ^H ∈ Irr(H). Moreover, θ(1) is relatively prime to p. Now consider the conformal symplectic group \( \overline{G} \) previously introduced. We know that \( \overline{G} \) is a direct product of \( H \) and a cyclic central subgroup. Therefore, θ is extendible to a character of \( \overline{G} \), which we will also denote by θ. However, \( \overline{G} \) is the group of \( GF(q) \)-rational points of a connected reductive algebraic group with connected center (namely, the conformal symplectic group over the algebraic closure of \( GF(q) \)). Therefore, a result of Green, Lehrer, and Lusztig [2, Theorem 3] shows that if \( w \) is a regular unipotent element of \( G \), we have

\[ \theta(w) = \pm 1. \]

Since \( (\theta(1), p) = 1 \), Theorems 1 and 2 of Ohmori [4] imply that \( m(\theta) = 1 \), where \( m(\theta) \) denotes the Schur index of θ over \( Q \).

We claim finally that \( m(\chi) = 1 \) also. For let \( \theta_1 = \theta, ..., \theta_r \) be all the Galois conjugates of θ. As \( m(\theta) = 1 \), we have that

\[ \phi = \theta_1 + \cdots + \theta_r \]

is the character of a \( Q \)-representation of \( H \). However, as χ induces to the irreducible character θ of \( H \), it is clear that θ is the unique irreducible character of \( H \) lying over χ. Thus, \( \phi_G \) is the character of a \( Q \)-representation of \( G \) and \( \chi \) occurs exactly once as a constituent of \( \phi_G \). This proves our claim and completes the proof.

We mention a corollary of the argument above. It will not be needed in the rest of the paper.

(1.5) Corollary. Suppose that \( q \equiv 3 \pmod{4} \). Let \( w \) be a regular unipotent element of \( G \) and let \( \chi \in Irr(G) \). Suppose that \( (\chi(1), p) = 1 \). Then \( \chi(w) = \pm 1 \) if \( \chi \) is real-valued, whereas \( \chi(w) \) is not real if \( \chi \) is not real-valued.

Proof. If \( \chi \) is real-valued, we know that \( \chi \) extends to an irreducible character \( \theta \) of \( H \). The argument of Theorem 1.4 shows that

\[ \chi(w) = \theta(w) = \pm 1. \]

If, instead, \( \chi \neq \overline{\chi} \), we know that for \( u \in H - G \), \( \chi^u = \overline{\chi} \). Thus if \( \chi(w) \) is real,

\[ \chi^u(w) = \chi(w). \]

However, \( \theta = \chi^H \in Irr(H) \) and we have

\[ \theta(w) = \pm 1 = \chi(w) + \chi^u(w) = 2\chi(w). \]

This is a contradiction as the algebraic integer \( \chi(w) \) is seen to equal \( \pm \frac{1}{2} \). Thus \( \chi(w) \) is not real if \( \chi \neq \overline{\chi} \).
We finish this section by finding the fields generated over $Q$ by the characters $\psi_i$ and determining their Schur indices. Let $\psi$ be the character of the representation $W$, so that $\psi = \psi_1 + \psi_2$. The results of [3], in particular the discussion after Corollary 6.5, show that $Q(\psi) = Q(\sqrt{-p})$ when $q \equiv 3 \pmod{4}$.

(1.6) Lemma. Suppose that $q \equiv 3 \pmod{4}$. Then $Q(\psi_i) = Q(\sqrt{-p})$, $1 \leq i \leq 2$, and the $\psi_i$ both have Schur index 1 over $Q$.

Proof. If $x$ is any element of $G$ and $\sigma$ is the central involution, our choice of $\psi_1$ as the faithful constituent of $\psi$ leads to the conclusion that

$$\begin{align*}
\psi_1(x) &= (\psi(x) - \psi(x\sigma))/2 \\
\psi_2(x) &= (\psi(x) + \psi(x\sigma))/2.
\end{align*}$$

See, for example, the argument of [3, p. 621]. Thus $Q(\psi_i) \leq Q(\psi)$, $1 \leq i \leq 2$. If $w$ is a regular unipotent element of $W$, the fixed-point subspace of $w$ acting on the underlying space $V$ has dimension 1. Thus Corollary 6.4 of [3] yields that

$$\psi(w) = (-q)^{1/2}.$$ 

However as $\sigma$ acts without fixed points on $V$, rule (b) of the algorithm given for computing $\psi$ in [3, p. 619] shows that

$$\psi(w\sigma) = \pm 1.$$ 

Our earlier formulae for the $\psi_i$ clearly imply that $\psi_i(w)$ is irrational for $i = 1, 2$. It follows that $Q(\psi_i) = Q(\sqrt{-p})$, $1 \leq i \leq 2$, as required. Also, as the $\psi_i$ are not real-valued and have degree coprime to $p$, Theorem 1.4 shows that these characters have Schur index 1 over $Q$.

2. Invariant Alternating Forms Associated with $Sp(2n, q)$ Representations

In [1], we showed that any faithful complex irreducible module $M$ for $G = Sp(2n, q)$ supports a non-singular $G$-invariant alternating form whenever $q \equiv 1 \pmod{4}$. Characters of self-dual modules that support invariant alternating forms are said to be of symplectic type. When $q \equiv 3 \pmod{4}$ not all faithful $G$-modules carry invariant bilinear forms, as not all characters of $G$ are real-valued. However, we prove that any faithful absolutely irreducible $G$-module supports a non-singular $G$-invariant alternating form provided that we are working over a field of characteristic $p$. 

This fact could probably be proved using the representation theory of algebraic groups. However, we will prove the result using characteristic zero representation theory. We need some preparatory lemmas.

(2.1) **Lemma.** Each p-regular element of \( G \) is real.

*Proof.* Let \( k \) denote the algebraic closure of \( GF(q) \) and put \( S = Sp(2n, k) \). By a result of Springer, [7, IV, 2.15], two elements of \( S \) are conjugate in \( S \) if and only if they are conjugate in \( GL(2n, k) \). As centralizers of semisimple elements of \( S \) are connected [7, II, 3.9] we see from [7, I. 3.4] that two semisimple (= p-regular) elements of \( G \) are conjugate in \( G \) if and only if they are conjugate in \( S \). However, elements of \( S \) are certainly conjugate to their inverses in \( GL(2n, k) \), as they preserve a non-singular bilinear form. Thus, all elements of \( S \) are conjugate in \( S \) to their inverses, by Springer's theorem, and our lemma follows by the observations above.

(2.2) **Corollary.** Each absolutely irreducible \( G \)-module \( M \) over a field of characteristic \( p \) is self-dual and hence supports a non-singular \( G \)-invariant symmetric or alternating form.

*Proof.* The isomorphism type of \( A_4 \) is determined by its Brauer character, \( \phi \), say. The Brauer character of the dual, \( M^* \), of \( M \) has Brauer character \( \phi^\ast \), the complex conjugate of \( \phi \). However, \( \phi = \phi^\ast \), as all p-regular elements of \( G \) are real. Thus \( M \) is isomorphic to \( M^* \). By well-known arguments, \( M \) supports a non-singular \( G \)-invariant form, which is either symmetric or alternating.

(2.3) **Theorem.** Let \( M \) be a faithful absolutely irreducible \( G \)-module over a field of characteristic \( p \). Then \( M \) supports a non-singular \( G \)-invariant alternating form and any other non-zero \( G \)-invariant bilinear form defined on \( M \) is a scalar multiple of this form.

*Proof.* We use a result of W. Willems, also proved by Thompson in [9]. Let \( \phi \) be the Brauer character of \( M \). There exists a real-valued \( \chi \in \text{Irr}(G) \) such that the \( p \)-modular decomposition number \( d_{\chi \phi} \) is odd. As \( \phi \) is faithful, \( \chi \) must also be faithful, and thus by Theorem 1 of [1], \( \chi \) is of symplectic type. By [9, p. 227], \( \phi \) is also of symplectic type, implying that \( M \) supports a non-singular \( G \)-invariant alternating form. The uniqueness of the form, up to scalar multiples, is a consequence of Schur's lemma, given that \( M \) is absolutely irreducible.
3. INVARIANT UNIMODULAR FORMS ASSOCIATED WITH THE WEIL REPRESENTATION $W$

The irreducible constituent of degree $(q^n - 1)/2$ of the Weil representation is known to define an irreducible Brauer character modulo any prime $r \neq p$, as shown in [5]. The character of degree $(q^n + 1)/2$ is irreducible modulo any prime $r \neq p$, but it is reducible modulo 2. See [11, Theorem 2.5]. For our main theorem, we need the following theorem of I. Suprunenko and A. Zaleskii [8].

(3.1) THEOREM. Suppose that $q = p$ is a prime. Then the irreducible characters $\psi_1, \psi_2$ of $G = Sp(2n, p)$ arising from the Weil representation define irreducible Brauer characters modulo $p$.

We assume now that $G = Sp(2n, p)$, where $p \equiv 3 \pmod{4}$, and recall that $\psi_1$ is the character of the faithful irreducible constituent of $W$. Let $H$ be the extension of $G$ consisting of all symplectic and skew-symplectic transformations. As $Q(\psi_1) = Q(\sqrt{-p})$, we know that $\theta = \psi_1''$ is irreducible by Lemma 1.3 and this character has Schur index 1 over $Q$ by the proof of Theorem 1.4. Now we claim that $\theta$ is rational-valued, for $\theta$ vanishes on $H - G$ and equals $\psi_1 + \overline{\psi_1}$ on $G$. As $\psi_1$ has the single Galois conjugate $\overline{\psi_1}$, $\psi_1 + \overline{\psi_1}$ is rational-valued on $G$, as required. It follows therefore that $\theta$ is the character of an absolutely irreducible $Q$-representation of $H$. Let $M$ be a $QH$-module affording the character $\theta$ and let $L$ be an $H$-invariant rational integral lattice in $M$. We can find a non-singular positive definite integral symmetric form

$$f: L \times L \to \mathbb{Z}$$

that is $H$-invariant. For all primes $r$, we induce a symmetric form

$$\tilde{f}: \tilde{L} \times \tilde{L} \to GF(r),$$

where $\tilde{L} = L/rL$, and we can scale $f$ so that $\tilde{f}$ is not identically zero. Then $\tilde{f}$ is an $H$-invariant symmetric form defined on $\tilde{L}$. Assuming this notation, we can prove our main result. The argument is derived from the proof of a theorem of Thompson [10].

(3.2) THEOREM. Suppose that $n$ is even. Let $f$ be a non-singular positive definite integral symmetric form defined on $L \times L$. Assume that $f$ is scaled so that $\tilde{f}$ is non-zero for all primes. Then $\tilde{f}$ is unimodular and even.

Proof. Take any prime $r \neq p$. We claim that $\tilde{L}$ is an absolutely irreducible module for $H$ over $GF(r)$. To see this, we note that as $n$ is even, $\psi_1$ has degree $(p^n - 1)/2$ and hence defines an absolutely irreducible $r$-modular Brauer character $\phi$, by our remarks at the beginning of this
section. Now the $H$-conjugate Brauer character $\phi^u$ equals $\psi_1^u$ on $r$-regular elements of $G$, for $u \in H - G$. We note that if $w$ is a regular unipotent element of $G$, $w$ has order coprime to $r$, and $\psi_1(w) \neq \overline{\psi_1(w)}$. It follows that $\phi(w) \neq \phi^u(w)$ and thus $\phi, \phi^u$ are distinct Brauer characters of $G$. Since we have $\theta_G = \psi_1 + \psi_1^u$, the decomposition

$$\theta_G = \phi + \phi^u$$

holds for $r$-regular elements of $G$. It follows easily from Clifford's theorem that $\theta$ must define an irreducible Brauer character for $H$ and hence $L$ is absolutely irreducible.

Now the radical of $f$ on $L$ is $H$-invariant and not equal to $L$. As $L$ is irreducible, this forces the radical to be zero and hence the discriminant of $f$ is relatively prime to $r$. Thus the discriminant of $f$ can only be a power of $p$ and we will show that it is actually 1 by considering the reduction of $L$ modulo $p$.

We set $\overline{L} = L/pL$ now and again note that the radical $R$ of $f$ on $\overline{L}$ is $H$-invariant and not equal to $L$. Moreover, $\overline{L}/R$ is a module for $H$ that supports a non-singular $H$-invariant symmetric form. We know that $\psi_1$ defines an irreducible Brauer character, $\phi$ say, modulo $p$, by Theorem 3.1, and $\phi$ must be real-valued by Lemma 2.1. Therefore $\overline{\psi_1} = \phi$ on $p$-regular elements of $G$ and it follows that the Brauer character of $G$ acting on $\overline{L}$ is $2\phi$. If $R$ is non-zero, the Brauer character of $G$ acting on $\overline{L}/R$ can only be $\phi$. However we know from Theorem 2.3 that $\phi$ is of symplectic type, which contradicts the fact that $\overline{L}/R$ supports a non-singular $G$-invariant symmetric form. Thus $R$ must be zero and consequently $f$ is non-singular. This forces the discriminant of $f$ to be coprime to $p$, and hence to be 1, which means that $f$ is unimodular. Finally, the fact that $f$ is even follows from the argument of Thompson [10]. This completes the proof.

As an illustration of the theorem we take $G = Sp(4, 3)$ and $H$ the corresponding group of symplectic and skew-symplectic transformations. By Theorem 3.2, we have an absolutely irreducible $H$-invariant integral lattice $L$ of rank 8 that supports an $H$-invariant positive definite even unimodular form $f$. By a theorem of Mordell [6, p. 55], $f$ is unique up to integral equivalence and we can identify $L$ with the root lattice of type $E_8$. In particular, $H$ is isomorphic to a subgroup of the derived group of the Weyl group of type $E_8$. We note that $H/\langle \sigma \rangle$, where $\sigma$ is the central involution, is isomorphic to the Weyl group of type $E_6$.

4. Possible Extensions and Comments

We consider whether an analogue of Theorem 3.2 exists when $n$ is odd and $p \equiv 3 \pmod{4}$. The faithful irreducible character $\psi_1$ of $G = Sp(2n, p)$ of
the Weil representation $W_i$ has degree $(p^n+1)/2$ and we can obtain an $H$-invariant integral lattice $L$ of rank $p^n+1$, where $H$ is defined as previously, whose character on $G$ equals $\psi_1 + \overline{\psi}_1$. Now $\psi_1$ defines an irreducible Brauer character modulo any prime different from 2 by [11, Theorem 2.5] and Theorem 3.1 of the previous section. Thus the discriminant of the $H$-invariant integral form $f$ defined on $L$ can be shown to equal a power of 2 by the arguments used to prove Theorem 3.2. However, we cannot necessarily prove that $f$ is even and unimodular, as $\psi_1$ is reducible modulo 2, its modular constituents having degree $(p^n-1)/2$ and 1 [11, Theorem 2.5]. Indeed, as the rank of an even positive definite unimodular lattice is divisible by 8, by [6, p. 53, Corollary 2], $f$ can only be even and unimodular if $p \equiv -1 \pmod{8}$. We do not know if this necessary condition for $f$ to be even and unimodular is also sufficient, except in the rather simple case described in the next theorem.

(4.1) Theorem. Let $G = \text{Sp}(2, p)$, where $p$ is a prime with $p \equiv -1 \pmod{8}$. There exists a $G$-invariant even unimodular integral lattice $L$ of rank $p + 1$ that affords the character $\psi_1 + \overline{\psi}_1$.

Proof. The normalizer $B$ of a Sylow $p$-subgroup $U$ of $G$ has order $p(p-1)$ and $B/U$ is cyclic. Let $\lambda$ be a linear character of $B$ of order 2. As $p \equiv 3 \pmod{4}$, $\lambda$ is non-trivial on the central involution of $G$, which is contained in $B$. The induced character $\lambda^G$ is then faithful for $G$ and the known character theory of $G$ shows that $\lambda^G = \psi_1 + \overline{\psi}_1$.

We can see that $G$ acts as group of signed permutation matrices in the monomial representation defined by $\lambda^G$. Let $M$ be the corresponding rational vector space on which $G$ acts. It is clear that there is naturally a $G$-invariant integral lattice $L$ in $M$ and the identity matrix defines a $G$-invariant unimodular form on $L$. As 8 divides the rank of $L$, a theorem of Thompson [13, Theorem 2.8] shows that there is an even unimodular lattice $L_0$ in $M$ which is invariant under a subgroup $G_0$ of $G$, where $|G:G_0| \leq 2$. As $G$ contains no subgroup of index 2, $L_0$ is a $G$-invariant lattice of the required type. This completes the proof.

Finally, we remark that when $p \equiv 1 \pmod{4}$, the fact that the faithful irreducible characters of degree $(p^n-1)/2$ of the group $\text{Sp}(2n, p)$ have Schur index 2 over $Q$ makes an analogue of Theorem 3.2 for this group impossible to prove by our methods.

Acknowledgment

I thank Professor Zaleskii for helpful discussions on Theorem 3.1.
REFERENCES

1. R. Gow, Real representations of the finite orthogonal and symplectic groups of odd characteristic, *J. Algebra* 96 (1985), 249–274.