Canad. J. Math. Vol. **54** (6), 2002 pp. 1229–1253

The Weil Character of the Unitary Group Associated to a Finite Local Ring

Roderick Gow and Fernando Szechtman

Abstract. Let $\mathbf{R}/R$ be a quadratic extension of finite, commutative, local and principal rings of odd characteristic. Denote by $\mathbf{U}_n(\mathbf{R})$ the unitary group of rank n associated to $\mathbf{R}/R$. The Weil representation of $\mathbf{U}_n(\mathbf{R})$ is defined and its character is explicitly computed.

1 Introduction

Let $\mathbf{R}/R$ be a quadratic extension of finite, commutative, local and principal rings of odd characteristic. Let $\mathbf{U}_n(\mathbf{R})$ be the unitary group of rank n associated to $\mathbf{R}/R$ and let $\mathrm{Sp}_{2n}(R)$ be the symplectic group of rank $2n$ over R. Let ψ denote the Weil character of $\mathrm{Sp}_{2n}(R)$ as defined in [CMS], and let Ψ be the restriction of ψ to $\mathbf{U}_n(\mathbf{R})$. Our main result is the following:

$$\Psi(g) = (-1)^{nl}\varepsilon(g)^l(-q)^{N(g)}, \quad g \in \mathbf{U}_n(\mathbf{R}). \tag{1}$$

Here ε is the unique linear character of order 2 of $\mathbf{U}_n(\mathbf{R})$, F_q is the residue field of R, q is a power of an odd prime p, $|R| = q^l$ and $|\ker(g-1)| = q^{2N(g)}$ for all $g \in \mathbf{U}_n(\mathbf{R})$. This extends Gérardin's formula

$$\Psi(g)\varepsilon(g) = (-1)^n(-q)^{N(g)}, \tag{2}$$

proved in [G] for the classical case $R = F_q$.

In proving (1) we shall make no use whatsoever of Gérardin's article [G], thereby giving an independent proof of (2) when q is odd. After preliminary work describing the structure of the group $\mathbf{U}_n(\mathbf{R})$ and constructing the Weil character, our method consists first of all in showing that the restriction Ψ of the Weil character ψ to $\mathbf{U}_n(\mathbf{R})$ is rational valued and that $\Psi(g) = \pm q^{N(g)}$ for all g in $\mathbf{U}_n(\mathbf{R})$. The rest of the paper is devoted to determining the sign in this formula. We first compare Ψ with a generalized permutation character of $\mathbf{U}_n(\mathbf{R})$ obtained from its action on $\mathbf{V}$. This enables us to find the values of Ψ on p'-elements of $\mathbf{U}_n(\mathbf{R})$. The values of Ψ on arbitrary elements are found by exploiting an elementary congruence relation that holds for character values of any finite group. This procedure works well provided q is not a Mersenne prime. When q is a Mersenne prime, we obtain the value of Ψ by embedding $\mathbf{U}_n(\mathbf{R})$ in a unitary group over an extension ring of $\mathbf{R}$ and then applying a comparison theorem for characters already used in the non-Mersenne case.

Received by the editors October 5, 2001.
AMS subject classification: 20G05.
©Canadian Mathematical Society 2002.

https://doi.org/10.4153/CJM-2002-047-5 Published online by Cambridge University Press

2 Basic Notions

This section fixes notation and terminology. It also proves some basic facts about hermitian spaces and unitary groups over finite local rings, which are well known in the context of finite fields.

2.1 Finite Local Rings

Let R be a finite, commutative, local and principal ring of odd characteristic. For instance, $R = \mathcal{O}/\mathfrak{p}^l$, where $\mathcal{O}$ is the ring of integers of an algebraic number field and $\mathfrak{p}$ is a prime ideal of $\mathcal{O}$ that lies over an odd rational prime.

Let max denote the unique maximal ideal of R and let ω be a generator of max. Let $F_q \cong R/max$ denote the residue class field of R. Here q is a power of an odd prime p. Note that the cardinality of every finite R-module is a power of q. As max is nilpotent, there is a positive integer l such that $max^l = 0$ but $max^{l-1} \neq 0$. (For the sake of uniformity in our notation, we assume here and elsewhere that $max^0 = R$ and $\omega^0 = 1$.) Thus $\omega^l = 0$ and $\omega^{l-1} \neq 0$. We then have $|R| = q^l$. The ideals of R have the form max^k, where $0 \leq k \leq l$. We have $|\, max^k \,| = q^{l-k}$. The unique minimal ideal of R is max^{l-1}.

Let R^* denote the group of units of R. Since max is the set of non-units of R, $R^* = R \setminus max$ and therefore $|R^*| = q^l - q^{l-1} = q^{l-1}(q-1)$. The elements in $1 + max$ form a subgroup of R^* and since $|1 + max| = q^{l-1}$, it follows that $1 + max$ is the Sylow p-subgroup of R^*. The unit group R^* is the direct product of the subgroup $1 + max$ and a cyclic subgroup of order $q-1$, isomorphic to F_q^*. We note also that if $0 \leq k < l$ and x is an element of $max^k \setminus max^{k+1}$, then we may write $x = \omega^k s$, where $s \in R^*$.

2.2 Quadratic Extensions of Finite Local Rings

Let $\mathbf{R}/R$ be a quadratic extension of finite, commutative, local and principal rings of odd characteristic. This means that R and $\mathbf{R}$ separately enjoy these properties, that $\mathbf{R}$ is a free R-module of rank two and that their residue fields form a quadratic extension F_{q^2}/F_q. An equivalent formulation is: given R, construct $\mathbf{R}$ by adjoining to R a square root $\mathbf{e}$ of a non-square unit e of R. This is possible, as R^{*2} has index 2 in R^*.

If I is an ideal of R we shall denote by $\mathbf{I} = \mathbf{R}I$ the corresponding ideal of $\mathbf{R}$. Thus the maximal ideal of $\mathbf{R}$ is $\mathbf{max}$. The element ω is also a generator of $\mathbf{max}$. We have $|\, \mathbf{max}^k \,| = q^{2(l-k)}$ for $0 \leq k \leq l$.

Associated to $\mathbf{R}/R$ one has a unique involution that fixes R elementwise:

$$r = a + b\mathbf{e} \mapsto \overline{r} = a - b\mathbf{e}, \quad a, b \in R. \tag{3}$$

The involution on $\mathbf{R}$ gives rise to a norm map $\mathbf{R}^* \to R^*$ given by $r \mapsto r\overline{r}$. We note the following property of this norm map.

Lemma 2.1 *The norm map $\mathbf{R}^* \to R^*$ is a group epimorphism. Its kernel $\mathbf{N}$ has $q^{l-1}(q+1)$ elements.*

https://doi.org/10.4153/CJM-2002-047-5 Published online by Cambridge University Press

Proof Consider the homomorphism $\tau\colon \mathbf{R}^* \to \mathbf{R}^*$ given by

$$\tau(r) = r^{-1}\overline{r}.$$

The kernel of τ is R^*. It is immediate that $\tau(\mathbf{R}^*)$ is contained in $\mathbf{N}$. We show that $\tau(\mathbf{R}^*) = \mathbf{N}$ as follows. Take $x \in \mathbf{N}$ and $\lambda \in \mathbf{R}$. Set $y = \lambda + \overline{\lambda}x$. Then $\overline{y} = \overline{\lambda} + \lambda\overline{x}$ and thus $x\overline{y} = y$. Provided $y \in \mathbf{R}^*$, we obtain $x = \tau(y^{-1})$, as required. Suppose then that y is a non-unit for all choices of λ. Then taking $\lambda = 1$, it follows that $1 + x \in \mathbf{max}$. Similarly, taking $\lambda = \mathbf{e}$ and making use of the fact that $\mathbf{e} \in \mathbf{R}^*$, we infer that $1 - x \in \mathbf{max}$. It follows that $2x \in \mathbf{max}$. As both 2 and x are units, this cannot occur. Thus $\tau(\mathbf{R}^*) = \mathbf{N}$. We deduce

$$\frac{|\mathbf{R}^*|}{|R^*|} = |\tau(\mathbf{R}^*)| = |\mathbf{N}|$$

and thus $|\mathbf{N}| = q^l(q+1)$. On the other hand, it is clear that the norm map is a homomorphism and $\mathbf{N}$ is its kernel. A comparison of orders, using $|\mathbf{N}| = q^l(q+1)$, shows that R^* is the image of the norm homomorphism. ∎

We note that $\mathbf{N}$ is the direct product of an abelian p-subgroup of order q^{l-1} and a cyclic group of order $q+1$. We also note that, since the trace map $\mathbf{R}^+ \to R^+$, given by $r \mapsto r + \overline{r}$, restricts to $r \mapsto 2r$ in R^+ and $2 \in R^*$, it is an additive group epimorphism.

2.3 Groups and Characters

Suppose that G is a finite group. A p-element of G is an element whose order is a power of p, while a p'-element is one whose order is coprime to p. Given $x \in G$, the p-decomposition of x describes the decomposition

$$x = us = su,$$

where u is a p-element and s is a p'-element. As is well known, the elements u and s are powers of x and are uniquely determined.

There is a well known concept of the determinant of a complex character. We wish to extend this concept in an obvious way to generalized characters. Let ϕ be a generalized character of G. Write

$$\phi = a_1\chi_1 + \cdots + a_r\chi_r$$

where each χ_i is an irreducible character of G and each a_i is an integer. We then define the linear character $\det\phi$ of G by

$$\det\phi = (\det\chi_1)^{a_1} \cdots (\det\chi_r)^{a_r}. \tag{4}$$

If ϕ_1 and ϕ_2 are generalized characters of G then (4) gives

$$\det(\phi_1 + \phi_2) = (\det\phi_1)(\det\phi_2). \tag{5}$$

Later, we will require a simple property of the determinant of a real-valued generalized character, which we prove below.

https://doi.org/10.4153/CJM-2002-047-5 Published online by Cambridge University Press

Lemma 2.2 *Let ϕ be a real-valued generalized character of G. Then* $\det\phi$ *has order dividing 2.*

Proof We first prove the result when ϕ is a real-valued ordinary character. Let D be a complex representation of G with character ϕ and let $\overline{D}$ be the conjugate representation of G. As ϕ is real-valued, D and $\overline{D}$ are equivalent representations. Thus there is an invertible $n \times n$ matrix A, where $n = \phi(1)$, satisfying

$$\overline{D}(g) = AD(g)A^{-1}$$

for all g in G. Taking determinants, we see that $\det D(g)$ is real-valued. It follows that $\det\phi$ is real-valued and hence has order dividing 2.

Suppose now that ϕ is a real-valued generalized character. We may write ϕ uniquely in the form $\phi = \phi_1 - \phi_2$, where ϕ_1 and ϕ_2 are ordinary characters with no irreducible constituents in common. As ϕ is real-valued, the uniqueness of this decomposition implies that both ϕ_1 and ϕ_2 are also real-valued. The result now follows from the proof in the first paragraph and the earlier observation (5). ∎

2.4 Hermitian Spaces, Unitary Groups and Symplectic Groups

We assume for the remainder of this paper that $\mathbf{V}$ is a free $\mathbf{R}$-module of finite rank n and $(\ ,\ ): \mathbf{V} \times \mathbf{V} \to \mathbf{R}$ is a non-degenerate hermitian form relative to the involution (3). Thus for each $v \in \mathbf{V}$, $f_v: \mathbf{V} \to \mathbf{R}$ defined by $f_v(w) = (v, w)$ is an $\mathbf{R}$-linear functional and $(w, v) = \overline{(v, w)}$. Furthermore, the non-degeneracy of the hermitian form means that for any v not in $\mathbf{max}\,\mathbf{V}$, f_v maps $\mathbf{V}$ onto $\mathbf{R}$. We say that $\mathbf{V}$ is an hermitian space. We proceed to prove some elementary facts about hermitian spaces over $\mathbf{R}$, which are well known in the context of finite fields.

Lemma 2.3 *There exists a vector u in V with $(u, u) = 1$.*

Proof Let v be an element of $\mathbf{V}$ not in $\mathbf{max}\,\mathbf{V}$. Since both f_v and the trace map $\mathbf{R}^+ \to R^+$ are surjective, there exists $w \in \mathbf{V}$ with

$$f_v(w) + \overline{f_v(w)} = (v, w) + \overline{(v, w)} = 1.$$

Thus we have

$$1 = (v, w) + (w, v) = (v + w, v + w) - (v, v) - (w, w).$$

It follows that at least one of the terms on the right above is not in *max*. Thus we may find $x \in \mathbf{V}$ with (x, x) a unit in R. Finally, since the norm map $\mathbf{R}^* \to R^*$ is surjective, we may find $t \in \mathbf{R}^*$ with $t\bar{t} = (x, x)^{-1}$. If we set $u = tx$, we see that $(u, u) = 1$. ∎

Lemma 2.4 *The hermitian space $\mathbf{V}$ possesses an orthonormal basis.*

https://doi.org/10.4153/CJM-2002-047-5 Published online by Cambridge University Press

Proof We proceed by induction on the rank, n, of $\mathbf{V}$. By Lemma 2.3, there is some $u \in \mathbf{V}$ with $(u,u) = 1$. Set $\mathbf{U} = \mathbf{R}u$. If $n = 1$, then $\mathbf{V} = \mathbf{U}$ and the result follows. Suppose next that $n > 1$. Then we have $\mathbf{V} = \mathbf{U} \oplus \mathbf{U}^{\perp}$, where $\mathbf{U}^{\perp}$ is defined by $\mathbf{U}^{\perp} = \{v \in \mathbf{V} : (v,u) = 0\}$. Clearly, $\mathbf{U}^{\perp}$ is a non-degenerate hermitian space of rank $n-1$ and thus has an orthonormal basis, by induction. Adjoining u to this orthonormal basis of $\mathbf{U}$, we obtain an orthonormal basis of $\mathbf{V}$, as required. ∎

Suppose now that $n \geq 2$ and u and v are linearly independent elements of $\mathbf{V}$. Let $\mathbf{U} = \mathbf{R}u \oplus \mathbf{R}v$. We say that $\mathbf{U}$ is a non-degenerate $\mathbf{R}$-submodule of $\mathbf{V}$ if the restriction of the hermitian form to $\mathbf{U} \times \mathbf{U}$ is non-degenerate. In the case that $\mathbf{U}$ is non-degenerate, we say that linearly independent elements x and y in $\mathbf{U}$ form a hyperbolic basis of $\mathbf{U}$ if

$$(x,x) = (y,y) = 0, \quad (x,y) = 1.$$

Lemma 2.5 *Let $\mathbf{U}$ be a non-degenerate $\mathbf{R}$-submodule of $\mathbf{V}$ of rank 2. Then $\mathbf{U}$ has a hyperbolic basis.*

Proof By Lemma 2.4, $\mathbf{U}$ has orthonormal basis vectors, say u and v. Let λ be an element of $\mathbf{R}$ satisfying $\lambda\overline{\lambda} = -1$. Then it is straightforward to check that

$$u + \lambda v, \quad \frac{1}{2}(u - \lambda v)$$

are hyperbolic basis vectors. ∎

We shall require the following lemma in our later investigations.

Lemma 2.6 *Suppose that $n \geq 2$. Let v be an element of $\mathbf{V}$ not in $\mathbf{max}\,\mathbf{V}$ and suppose that $(v,v) \in max$. Then there exists $z \in \mathbf{V}$ such that $v - z \in \mathbf{max}\,\mathbf{V}$ and $(z,z) = 0$.*

Proof We first note that, as $\mathbf{V}$ is a free $\mathbf{R}$-module, an equality of the form $\lambda u = 0$, where $\lambda \in \mathbf{R}$ and $u \in \mathbf{V}$, implies that either $\lambda = 0$ or $u \in \mathbf{max}\,\mathbf{V}$. Now, as we observed previously, $f_v \colon \mathbf{V} \to \mathbf{R}$ is surjective. Thus there exists $w \in \mathbf{V}$ with $(v,w) = 1$. We will show that v and w are linearly independent. For suppose that $rv + sw = 0$ for some r and s in $\mathbf{R}$. Then

$$(v, rv + sw) = 0 = r(v,v) + s(v,w) = r(v,v) + s.$$

Hence $s = -r(v,v)$ and we obtain

$$rv - r(v,v)w = r\big(v - (v,v)w\big) = 0.$$

By our opening remark, we deduce that either $r = 0$, in which case $s = 0$ also, or else $v - (v,v)w \in \mathbf{max}\,\mathbf{V}$. But since $(v,v) \in max$, the latter possibility implies that $v \in \mathbf{max}\,\mathbf{V}$, contrary to hypothesis. Hence $r = s = 0$, and v and w are indeed linearly independent.

https://doi.org/10.4153/CJM-2002-047-5 Published online by Cambridge University Press

We set $\mathbf{U} = \mathbf{R}v \oplus \mathbf{R}w$. Since $(v, v) \in max$ and $(v, w) = 1$, it is straightforward to check that $\mathbf{U}$ is non-degenerate. By Lemma 2.5, $\mathbf{U}$ has a hyperbolic basis, consisting of, say, vectors x and y. We may now write

$$v = \alpha x + \beta y,$$

where α and β are in $\mathbf{R}$. Since $v \notin \mathbf{max}\,\mathbf{V}$, at least one of α and β is a unit in $\mathbf{R}$, say α. Set $u = (\overline{\alpha})^{-1}y$. Then we have $(u, u) = 0$ and $(u, v) = 1$. Finally, set

$$z = v - \frac{(v, v)}{2}u.$$

It is easy to see that z has the required property. ■

The unitary group of rank n over $\mathbf{R}$ is by definition the group of all automorphisms g of $\mathbf{V}$ that satisfy

$$(gv, gw) = (v, w)$$

for all v and w in $\mathbf{V}$. We denote this group by $\mathbf{U}_n(\mathbf{R})$. Since Lemma 2.4 implies that all non-degenerate hermitian forms defined on $\mathbf{V} \times \mathbf{V}$ are equivalent, the isomorphism type of $\mathbf{U}_n(\mathbf{R})$ is independent of the choice of non-degenerate hermitian form.

Given u and v in $\mathbf{V}$, we may write

$$(u, v) = [u, v] + \mathbf{e}\langle u, v\rangle, \tag{6}$$

for unique $[u, v]$, $\langle u, v\rangle$ in R. If we view $\mathbf{V}$ as a free R-module, say V, of rank $2n$, then the formulation above makes $\langle\ ,\ \rangle$ into a non-degenerate alternating form on V.

Let $\mathrm{Sp}_{2n}(R)$ denote the subgroup of automorphisms of V that preserve $\langle\ ,\ \rangle$. We refer to it as the symplectic group associated to $(V, \langle\ ,\ \rangle)$. By virtue of the uniqueness of (6) and the fact that $\mathbf{U}_n(\mathbf{R})$ preserves $(\ ,\ )$, it follows that $\mathbf{U}_n(\mathbf{R})$ preserves both $\langle\ ,\ \rangle$ and $[\ ,\ ]$. Hence we have the inclusion

$$\mathbf{U}_n(\mathbf{R}) \subset \mathrm{Sp}_{2n}(R). \tag{7}$$

2.5 The Weil Representation

Let $H = \{(r, v) : r \in R, v \in V\}$ be the Heisenberg group associated to $(V, \langle\ ,\ \rangle)$, where multiplication is given by $(r_1, v_1)(r_2, v_2) = (r_1 + r_2 + \langle v_1, v_2\rangle, v_1 + v_2)$. Observe that $Z(H) = (R, 0) \simeq R^+$ and that $\mathrm{Sp}_{2n}(R)$ acts naturally on H by means of the formula

$${}^g(r, v) = (r, gv).$$

A linear character $\lambda\colon R^+ \to \mathbf{C}^*$ is said to be primitive if its kernel does not contain any non-zero ideals of R. Since max^{l-1} is the unique minimal ideal of R, the number of primitive linear characters of R^+ equals $|R| - |R/\,max^{l-1}| > 0$. We are thus allowed to choose a primitive linear character $\lambda\colon R^+ \to \mathbf{C}^*$. We view λ as a character of $Z(H)$.

Much as in the field case, one may show that $(V, \langle\ ,\ \rangle)$ admits a symplectic basis $\{u_1, \ldots, u_n, v_1, \ldots, v_n\}$. Let M be the R-span of $\{u_1, \ldots, u_n\}$. Thus M is a maximal

https://doi.org/10.4153/CJM-2002-047-5 Published online by Cambridge University Press

totally isotropic submodule of V. Consider the normal subgroup $A = (R, M)$ of H and extend λ to the linear character ρ of A by means of: $\rho(r, m) = \lambda(r)$, $r \in R$, $m \in M$. By construction, the inertia group of ρ in H is A itself. Clifford theory thus ensures that $\chi_\lambda = \operatorname{ind}_A^H \rho$ is an irreducible character of H. We have

$$\deg \chi_\lambda = [H : A] = [V : M] = |R|^n = q^{nl}. \tag{8}$$

Moreover, remark that

$$\chi_{\lambda|Z(H)} = |R|^n \lambda \quad \text{and} \quad [H : Z(H)] = |R|^{2n}.$$

It follows from [I, exercise 6.3] that χ_λ is the *only* irreducible character that lies over λ.

Since $\mathrm{Sp}_{2n}(R)$ acts trivially on $Z(H)$, the conjugate character χ_λ^g also lies over λ for each $g \in \mathrm{Sp}_{2n}(R)$. It follows from the uniqueness of χ_λ that $\chi_\lambda = \chi_\lambda^g$ for all $g \in \mathrm{Sp}_{2n}(R)$. If $S_\lambda \colon H \to \mathrm{GL}(X_\lambda)$ is a complex representation with character χ_λ then the $\mathrm{Sp}_{2n}(R)$-invariance of χ_λ ensures that to each $g \in \mathrm{Sp}_{2n}(R)$ there corresponds an operator, say $W_\lambda(g)$, that conjugates S_λ into S_λ^g. It is shown in [CMS, Section 3] that the operators above can be chosen so that $g \mapsto W_\lambda(g)$ is a group homomorphism. In other words, there exists a representation $W_\lambda \colon \mathrm{Sp}_{2n}(R) \to \mathrm{GL}(X_\lambda)$ such that

$$W_\lambda(g) S_\lambda(h) W_\lambda(g)^{-1} = S_\lambda({}^g h), \quad g \in \mathrm{Sp}_{2n}(R), h \in H. \tag{9}$$

We refer to W_λ as the Weil representation of $\mathrm{Sp}_{2n}(R)$ of type λ and denote its character by ψ_λ.

Since S_λ is irreducible, ψ_λ is uniquely determined by (9) whenever $\mathrm{Sp}_{2n}(R)$ is perfect, which is always the case unless $q = 3$ and $n = 1$ (see [S, Section 2.4] or [K, Section 3] for the case $q > 3$).

Definition 2.7 When $q = 3$ and $n = 1$, we shall understand by *the* Weil character of $\mathrm{Sp}_{2n}(R)$ of type λ the only character ψ_λ of this kind that satisfies (see [S, Section 5.1]):

$$\psi_\lambda(g) = \sum_{r \in R} \lambda(r^2), \tag{10}$$

where g is a symplectic transvection of the form $x \to x + \langle u, x \rangle u$ and u is any basis vector of V.

This definition makes sense because the Weil character never vanishes (see [CMS, Theorem 4.5]) and g can detect any of the three linear characters of $\mathrm{Sp}_{2n}(R)$ when $q = 3$ and $n = 1$ (see [S, Section 2.4]).

We denote the restriction of ψ_λ to $\mathbf{U}_n(\mathbf{R})$ by Ψ_λ and refer to it as the Weil character of $\mathbf{U}_n(\mathbf{R})$ of type λ. By (8) its degree is equal to

$$\deg \Psi_\lambda = \deg \psi_\lambda = \deg \chi_\lambda = q^{nl}. \tag{11}$$

https://doi.org/10.4153/CJM-2002-047-5 Published online by Cambridge University Press

2.6 Calculations in the Hermitian Space

Let r be an element of R. We set

$$\mathbf{V}(r) = \{v \in \mathbf{V} : (v, v) = r\}$$

and put $S_n^r = |\mathbf{V}(r)|$. Thus S_n^r equals the number of solutions in $\mathbf{R}$ to the equation

$$x_1\overline{x_1} + x_2\overline{x_2} + \cdots + x_n\overline{x_n} = r.$$

Let *min* denote the minimal ideal of R and let m be a generator of *min*. Set

$$T_n = S_n^0 - S_n^m.$$

Lemma 2.8

(a) *If $r \in R$ and $t \in R^*$, then $S_n^r = S_n^{tr}$.*
(b) *If $r \in R$ is different from 0 and $-m$, then $S_n^r = S_n^{r+m}$.*
(c) $T_n = (T_1)^n$.

Proof (a) Since the norm map is surjective, we may write $t = s\bar{s}$ for some $s \in \mathbf{R}^*$. The map $v \to sv$ establishes a bijection between $\mathbf{V}(r)$ and $\mathbf{V}(tr)$.

(b) If $r \in min$, then both m and $r + m$ are generators of *min*, since $r \neq 0, -m$. It follows that $r + m = tr$, where $t \in R^*$, so (a) ensures that $S_n^r = S_n^{r+m}$.

If $r \notin min$, then $m = tr$ for some $t \in max$, so $r + m = (1 + t)r$ where $1 + t \in R^*$. It follows again from (a) that $S_n^r = S_n^{r+m}$.

(c) If $n = 1$ there is nothing to prove, so we assume that $n > 1$. The equation

$$x_1\overline{x_1} + x_2\overline{x_2} + \cdots + x_{n-1}\overline{x_{n-1}} = -x_n\overline{x_n}$$

has exactly

$$\sum_{r\in R} S_1^r S_{n-1}^{-r} = \sum_{r\in R\setminus min} S_1^r S_{n-1}^{-r} + \sum_{r\in min\setminus\{0\}} S_1^r S_{n-1}^{-r} + S_1^0 S_{n-1}^0 \tag{12}$$

solutions. Since $r, -r \in R^*m$ for all $r \in min\setminus\{0\}$, (a) gives

$$\sum_{r\in min\setminus\{0\}} S_1^r S_{n-1}^{-r} = (q-1)S_1^m S_{n-1}^m. \tag{13}$$

Analogously, the equation

$$x_1\overline{x_1} + x_2\overline{x_2} + \cdots + x_{n-1}\overline{x_{n-1}} = m - x_n\overline{x_n}$$

has exactly

$$\sum_{r\in R\setminus min} S_1^r S_{n-1}^{m-r} + \sum_{r\in min\setminus\{0,m\}} S_1^r S_{n-1}^{m-r} + S_1^m S_{n-1}^0 + S_1^0 S_{n-1}^m \tag{14}$$

https://doi.org/10.4153/CJM-2002-047-5 Published online by Cambridge University Press

solutions. By (b)

$$\sum_{r\in R\setminus min} S_1^r S_{n-1}^{m-r} = \sum_{r\in R\setminus min} S_1^r S_{n-1}^{-r}, \tag{15}$$

while it follows as above from (a) that

$$\sum_{r\in min\setminus\{0,m\}} S_1^r S_{n-1}^{m-r} = (q-2)S_1^m S_{n-1}^m. \tag{16}$$

Substituting (13) in (12) and (15)–(16) in (14), and then subtracting (14) from (12) we get

$$T_n = S_n^0 - S_n^m = (S_1^0 - S_1^m)(S_{n-1}^0 - S_{n-1}^m) = T_1 T_{n-1}.$$

The result hence follows by induction. ∎

Lemma 2.9 *Suppose that l is odd. Then*

(a) $S_1^m = q^{l-1}(q+1)$.
(b) $S_1^0 = q^{l-1}$.
(c) $T_1 = -q^l$.
(d) $T_n = (-q)^{ln}$.

Proof We may assume that $m = \omega^{l-1}$, since ω^{l-1} is a generator of *min*. Suppose that $x \in \mathbf{R}$ satisfies $x\overline{x} = \omega^{l-1}$. We may write $x = \omega^k s$, where $s \in \mathbf{R}^*$. Then $x\overline{x} = \omega^{l-1} = \omega^{2k} s\overline{s}$ and it follows that $2k = l-1$ and $s\overline{s} \in 1 + max$. Conversely, any element of the form $\omega^{(l-1)/2}s$, where $s\overline{s} \in 1 + max$, has norm equal to ω^{l-1}. Now since the norm map is surjective, there are exactly $q^{l-1}(q+1)q^{l-1}$ elements $s \in \mathbf{R}^*$ with $s\overline{s} \in 1 + max$. Finally, since $\omega^{(l-1)/2}s = \omega^{(l-1)/2}s'$ if and only if $s' - s \in \omega^{(l+1)/2}\mathbf{R}$, there is a total of $q^{l-1}(q+1)q^{l-1}/(q^2)^{(l-1)/2} = q^{l-1}(q+1)$ elements $x = \omega^{(l-1)/2}s$ whose norm is equal to ω^{l-1}. This proves part (a). For part (b), the argument above implies that the set of elements of norm 0 coincides with $\mathbf{max}^{(l+1)/2}$. Since $|\,\mathbf{max}^{(l+1)/2}\,| = q^{l-1}$, part (b) follows. Parts (c) and (d) are now clear. ∎

2.7 On the Structure of the Unitary and Symplectic Groups

Let π denote the canonical ring homomorphism

$$\mathbf{R} \to \mathbf{R}/\,\mathbf{max} \cong F_{q^2}.$$

Since **max** is invariant under the involution of **R**, π induces an involution $*$ on $\mathbf{R}/\,\mathbf{max}$, defined by $\pi(r)^* = \pi(\overline{r})$. This involution is non-trivial on $\mathbf{R}/\,\mathbf{max}$, as $\mathbf{e} \notin \mathbf{max}$. Since $\mathbf{R}/\,\mathbf{max}$ is isomorphic to the field F_{q^2}, $*$ must coincide with the canonical involution $x \to x^q$ defined on F_{q^2}. We also let π denote the natural homomorphism $\mathbf{V} \to \mathbf{V}/\,\mathbf{max}\,\mathbf{V}$. Clearly, $\pi(\mathbf{V})$ is a vector space of dimension n over F_{q^2}. We may define a sesquilinear form $f\colon \pi(\mathbf{V}) \times \pi(\mathbf{V}) \to F_{q^2}$ by

$$f\big(\pi(v), \pi(w)\big) = \pi(v, w).$$

https://doi.org/10.4153/CJM-2002-047-5 Published online by Cambridge University Press

It is elementary to check that f is a non-degenerate hermitian form with respect to $*$. Finally, given g in $\mathbf{U}_n(\mathbf{R})$, we define an automorphism $\pi(g)$ of $\pi(\mathbf{V})$ by

$$\pi(g)\pi(v) = \pi(gv).$$

It is again elementary to see that $\pi(g)$ is an isometry of f and that π induces a homomorphism from $\mathbf{U}_n(\mathbf{R})$ into $\mathbf{U}_n(F_{q^2})$. We intend to investigate the kernel and image of this group homomorphism in the next few lemmas. (We trust that context will make it clear which homomorphism is signified by π.)

Let w be any element of $\mathbf{V}$ satisfying $(w,w) = 0$ and let λ be any element of $\mathbf{R}$ satisfying $\lambda + \overline{\lambda} = 0$. Define an automorphism $g = g_{\lambda,w}$ of $\mathbf{V}$ by

$$gv = v + \lambda(w,v)w$$

for all v in $\mathbf{V}$. We readily check that g is an element of $\mathbf{U}_n(\mathbf{R})$, which we call a unitary transvection. The image $\pi(g)$ of g is a unitary transvection in $\mathbf{U}_n(F_{q^2})$ in the usual field-theoretic sense. Here, as a matter of convenience, we consider the identity mapping to be transvection. We show now that every transvection in $\mathbf{U}_n(F_{q^2})$ is the image of a transvection in $\mathbf{U}_n(\mathbf{R})$.

Lemma 2.10 *Let ρ be a unitary transvection in $\mathbf{U}_n(F_{q^2})$. Then there is a unitary transvection g in $\mathbf{U}_n(\mathbf{R})$ with $\pi(g) = \rho$.*

Proof As ρ is a unitary transvection, it acts on $\pi(\mathbf{V})$ according to the formula

$$\rho\pi(v) = \pi(v) + \pi(\mu)f\big(\pi(w),\pi(v)\big)\,\pi(w),$$

where $v, w \in \mathbf{V}$, $f\big(\pi(w),\pi(w)\big) = 0$ and $\mu \in \mathbf{R}$ satisfies $\pi(\mu) + \pi(\mu)^* = 0$. If $\pi(w) = 0$ then $\rho = 1_{\pi(\mathbf{V})} = \pi(1_{\mathbf{V}}) = \pi(g_{0,0})$. Thus we may suppose that $\pi(w) \neq 0$. Let $\mu = a + b\mathbf{e}$, where $a, b \in R$. Then as $\pi(\mu) + \pi(\mu)^* = 0$, it follows that $2a \in max$. Thus $a \in max$, as 2 is a unit in R. If we now define $\nu = b\mathbf{e}$, we have $\nu + \overline{\nu} = 0$ and $\pi(\nu) = \pi(\mu)$. Furthermore, by Lemma 2.6, we can find $z \in \mathbf{V}$ with $(z,z) = 0$ and $\pi(z) = \pi(w)$. Then $g = g_{\nu,z}$ is a unitary transvection in $\mathbf{U}_n(\mathbf{R})$ satisfying $\pi(g) = \rho$. ∎

Lemma 2.11 *The group homomorphism $\pi\colon \mathbf{U}_n(\mathbf{R}) \to \mathbf{U}_n(F_{q^2})$ is surjective and its kernel is a p-group.*

Proof We have seen in Lemma 2.10 that all unitary transvections of $\mathbf{U}_n(F_{q^2})$ are contained in $\pi\big(\mathbf{U}_n(\mathbf{R})\big)$. Now the subgroup of $\mathbf{U}_n(F_{q^2})$ generated by the transvections is the special unitary group $\mathrm{SU}_n(F_{q^2})$ (see, for example, the proof of Theorem 10.20 of [T]). Thus, $\mathrm{SU}_n(F_{q^2})$ is contained in the image of π.

Fix now an orthonormal basis of $\mathbf{V}$ and let β be an element of order $q+1$ in $\mathbf{N}$. Let d be the element of $\mathbf{U}_n(\mathbf{R})$ whose matrix with respect to this basis is diagonal of the form $\mathrm{diag}(\beta, 1, \ldots, 1)$ and let D be the cyclic subgroup generated by d. It is straightforward to see that $\pi(d)$ is an element of order $q+1$ in $\mathbf{U}_n(F_{q^2})$, whose

https://doi.org/10.4153/CJM-2002-047-5 Published online by Cambridge University Press

determinant has order $q+1$. Thus $\pi(D)$ complements $\mathrm{SU}_n(F_{q^2})$ and $\mathbf{U}_n(F_{q^2})$ is the semi-direct product of $\mathrm{SU}_n(F_{q^2})$ and $\pi(D)$. This establishes that π is surjective.

Suppose that $g \in \ker\pi$. Then we have $gv - v \in \mathbf{max}\,\mathbf{V}$ for all $v \in \mathbf{V}$. Let A be the matrix of g with respect to the chosen basis of $\mathbf{V}$. Then $A - I = \omega B$, where ω generates $\mathbf{max}$ and B is an $n \times n$ matrix whose entries lie in $\mathbf{R}$. We will prove by induction on m that

$$A^{p^m} = I + \omega^{m+1} B_m,$$

where B_m is an $n \times n$ matrix whose entries lie in $\mathbf{R}$. This is clearly true when $m = 0$. Suppose now that

$$A^{p^r} = I + \omega^{r+1} B_r.$$

Then

$$A^{p^{r+1}} = (I + \omega^{r+1} B_r)^p = I + p\omega^{r+1} B_r + \sum_{i \geq 2} \binom{p}{i} \omega^{(r+1)i} B_r^i.$$

Since $p1$ is in $\mathbf{max}$, it is a multiple of ω and the induction step is complete. Finally, as $\omega^l = 0$, it follows that $A^{p^{l-1}} = I$ and thus the order of g is a power of p dividing p^{l-1}. This implies that $\ker\pi$ is a p-group. ∎

Corollary 2.12 *The commutator quotient group $\mathbf{U}_n(\mathbf{R})/\mathbf{U}_n(\mathbf{R})'$ is the direct product of an abelian p-group with a cyclic group of order $q+1$ that is the canonical image of the subgroup D introduced in the proof of Lemma 2.11. In particular, $\mathbf{U}_n(\mathbf{R})$ has a unique linear character ε of order 2, which is determined by its restriction to D.*

Proof Let G denote $\mathbf{U}_n(\mathbf{R})$ and L denote $\mathbf{U}_n(F_{q^2})$. The epimorphism $\pi\colon G \to L$, described in Lemma 2.11 induces an epimorphism $\overline{\pi}\colon G/G' \to L/L'$. The kernel of $\overline{\pi}$ is $(G' \ker\pi)/G' \cong \ker\pi/G' \cap \ker\pi$. Since we have seen that $\ker\pi$ is a p-group and L/L' is well known to be cyclic of order $q+1$, the first statement of the corollary follows. The existence and uniqueness of ε is straightforward. ∎

There is likewise a canonical ring homomorphism

$$\sigma\colon R \to R/\,max \cong F_q.$$

This induces a homomorphism $V \to V/\,max$, which we again denote by σ. It is clear that $\sigma(V)$ is a vector space of dimension $2n$ over F_q. We may define a non-degenerate alternating bilinear form $h\colon \sigma(V) \times \sigma(V) \to F_q$ by the formula

$$h\big(\sigma(v), \sigma(w)\big) = \sigma(\langle v, w\rangle).$$

This in turn induces a homomorphism, also denoted by σ, from $\mathrm{Sp}_{2n}(R)$ into $\mathrm{Sp}_{2n}(F_q)$. We may show that σ maps $\mathrm{Sp}_{2n}(R)$ onto $\mathrm{Sp}_{2n}(F_q)$ as follows. Let w be any element of V. Consider the automorphism g of V defined by

$$gv = v + \lambda\langle w, v\rangle w,$$

https://doi.org/10.4153/CJM-2002-047-5 Published online by Cambridge University Press

where $\lambda \in R$. A straightforward calculation shows that g is an element of $\mathrm{Sp}_{2n}(R)$. We call g a symplectic transvection. The image $\sigma(g)$ is a symplectic transvection in $\mathrm{Sp}_{2n}(F_q)$ in the usual sense. It is elementary to prove that each symplectic transvection in $\mathrm{Sp}_{2n}(F_q)$ arises as the image under σ of a symplectic transvection in $\mathrm{Sp}_{2n}(R)$. (We remark that the proof required is considerably simpler than that given in Lemma 2.10, as each element of V is isotropic with respect to the alternating form.) Since $\mathrm{Sp}_{2n}(F_q)$ is generated by its transvections (see, for example, [T, Theorem 8.5]), it follows that σ is surjective. Furthermore, $\ker\sigma$ is a p-group, as the the argument used in the proof of Lemma 2.11 implies.

The main conclusion we wish to draw from these discussions is the following, whose proof follows from the fact that $\mathrm{Sp}_{2n}(F_q)$ is perfect when q is odd, except when $q = 3$ and $n = 1$. In the exceptional case, the commutator quotient group of $\mathrm{Sp}_2(F_3)$ has order 3. (See, for example, [T, Theorem 8.7].)

Corollary 2.13 *The commutator quotient group* $\mathrm{Sp}_{2n}(R)/\mathrm{Sp}_{2n}(R)'$ *is a* p*-group.*

We remark that, in the corollary above, the commutator quotient is in fact trivial unless $q = 3$ and $n = 1$. Indeed this follows from [S, Section 2.4] or [K, Section 3] if $q > 3$. When $n = 1$ and $q = 3$, the commutator quotient is non-trivial.

2.8 The Action of $\mathbf{U}_n(\mathbf{R})$ on $\mathbf{V}$

Given $g \in \mathbf{U}_n(\mathbf{R})$, let $\mathbf{V}^g = \ker(g - I)$. It is clear that $\mathbf{V}^g$ is an $\mathbf{R}$-module and, since the residue field associated to $\mathbf{R}$ has order q^2, it follows that $|\mathbf{V}^g|$ is a power of q^2. Thus we may write $|\mathbf{V}^g| = q^{2N(g)}$ for some non-negative integer $N(g)$.

Lemma 2.14 *Let s be a p'-element of order t in $\mathbf{U}_n(\mathbf{R})$. Let*

$$P = t^{-1}\sum_{g\in\langle s\rangle} g. \tag{17}$$

Then P is a self-adjoint projection. Thus if $\mathbf{V}_0 = \mathrm{Im}\, P$ and $\mathbf{V}_1 = \ker P$, then

$$\mathbf{V}_0 \oplus \mathbf{V}_1 = \mathbf{V} \tag{18}$$

is a decomposition of $\mathbf{V}$ into the direct sum of orthogonal hermitian spaces, the first of which coincides with $\mathbf{V}^s$.

Proof Since t is coprime to p, the element t is a unit in $\mathbf{R}$, so that (17) makes sense. A straightforward calculation shows that we have $P^2 = P$ and

$$(Pv, w) = t^{-1}\sum_{g\in\langle s\rangle}(gv, w) = t^{-1}\sum_{g\in\langle s\rangle}(v, g^{-1}w) = (v, Pw), \quad v, w \in \mathbf{V}.$$

Since P is a projection, (18) holds and since P is self-adjoint, $\mathrm{Im}\, P$ and $\ker P$ are orthogonal. But $\mathbf{V}$ is non-degenerate, therefore so must be $\mathbf{V}_0$ and $\mathbf{V}_1$, and these are free $\mathbf{R}$-modules because they are projective and $\mathbf{R}$ is local. Finally, it is elementary to see that $\mathbf{V}_0 = \mathbf{V}^s$. ∎

https://doi.org/10.4153/CJM-2002-047-5 Published online by Cambridge University Press

Lemma 2.15 *If l is even and s is a p'-element of $\mathbf{U}_n(\mathbf{R})$, then $N(s)$ is even.*

Proof Consider the decomposition $\mathbf{V} = \mathbf{V}_0 \oplus \mathbf{V}_1$ of Lemma 2.14. Then

$$q^{2N(s)} = |\ker(s - I)| = |\mathbf{V}_0| = q^{2l \operatorname{rank} \mathbf{V}_0},$$

so $N(s) = l \operatorname{rank} \mathbf{V}_0$ is even. ■

Given any element α in $\mathbf{N}$, let z_α denote the central element of $\mathbf{U}_n(\mathbf{R})$ that acts on $\mathbf{V}$ according to $v \mapsto \alpha v$.

Lemma 2.16 *Let $\alpha \neq 1$ be an element of p'-order in $\mathbf{N}$ and let $z = z_\alpha$. Then $\mathbf{V}^z = \{0\}$.*

Proof If $zv = v$ then $(\alpha - 1)v = 0$. Here $\alpha - 1$ is a unit, since $\alpha \notin 1 + \mathbf{max}$. It follows that $v = 0$, as required. ■

3 Rationality of the Weil Character

Proposition 3.1 *Let λ be a primitive linear character of R^+. Then*

$$\overline{\psi_\lambda}(g)\psi_\lambda(g) = |V^g|, \quad g \in \mathrm{Sp}_{2n}(R).$$

Therefore

$$\overline{\Psi_\lambda}(g)\Psi_\lambda(g) = |\mathbf{V}^g| = q^{2N(g)}, \quad g \in \mathbf{U}_n(\mathbf{R}).$$

Proof This follows at once from [CMS, Theorem 4.5]. ■

Theorem 3.2 *Let $\lambda\colon R^+ \to \mathbf{C}$ be a primitive linear character. Let I be an ideal of R of square (0) and let $X_\lambda(I)$ be the set of fixed points in X_λ of the subgroup $B = (0, IV)$ of H. Let J be the annihilator of I in R and let K be the conductor of J in I. Let $\mathrm{Sp}_{2n}(K) = \{g \in \mathrm{Sp}_{2n}(R) \mid gv \equiv v \mod KV\}$ be the congruence subgroup of $\mathrm{Sp}_{2n}(R)$ associated to K and let $\mathbf{U}_n(\mathbf{K}) = \{g \in \mathbf{U}_n(\mathbf{R}) \mid gv \equiv v \mod \mathbf{KV}\}$ be the congruence subgroup of $\mathbf{U}_n(\mathbf{R})$ associated to $\mathbf{K}$. Then*

(a) *$X_\lambda(I)$ is a non-trivial subspace of X_λ.*
(b) *The restriction of the Weil representation of $\mathrm{Sp}_{2n}(R)$ to $\mathrm{Sp}_{2n}(K)$ is trivial on $X_\lambda(I)$.*
(c) *The restriction of the Weil representation of $\mathbf{U}_n(\mathbf{R})$ to $\mathbf{U}_n(\mathbf{K})$ is trivial on $X_\lambda(I)$.*

Proof Parts (a) and (b) are respectively proven in Sections 4 and 5 of [CMS]. The proof of part (b) given in [CMS] requires that $\mathrm{Sp}_{2n}(R)$ is perfect. A proof for the imperfect case may be found in Section 7.1 of [S]. Part (c) follows immediately from (b) and the inclusion $\mathbf{U}_n(\mathbf{K}) \subset \mathrm{Sp}_{2n}(K)$. ■

If $\lambda\colon R^+ \to \mathbf{C}^*$ is primitive and $r \in R$, we let $\lambda[r]$ denote the linear character of R^+ given by $s \mapsto \lambda(sr)$. The primitivity of λ ensures that $\lambda[r] = \lambda[s]$ if and only if $r = s$. Thus all linear characters of R^+ are of the form $\lambda[r]$, this being primitive precisely when $r \in R^*$.

https://doi.org/10.4153/CJM-2002-047-5 Published online by Cambridge University Press

Theorem 3.3 *The Weil characters of* $\mathbf{U}_n(\mathbf{R})$ *of all primitive types are equal, that is, if* λ *and* μ *are primitive linear characters of* R^+, $\Psi_\lambda = \Psi_\mu$.

Proof Let λ and μ be primitive linear characters of R^+. As noted above, there exists an element $k \in R^*$ with

$$\mu(r) = \lambda(kr)$$

for all $r \in R$. Lemma 2.1 shows that there exists an element t of $\mathbf{R}^*$ with $t\bar{t} = k$. We now define an automorphism θ of H by

$$^\theta(r, v) = (t\bar{t}r, tv) = (kr, tv).$$

We note that as every $g \in \mathbf{U}_n(\mathbf{R})$ is $\mathbf{R}$-linear, θ commutes with the action of $\mathbf{U}_n(\mathbf{R})$ on H.

Let S_λ be the irreducible complex representation of H with character χ_λ. We define the conjugate representation S_λ^θ of H by

$$S_\lambda^\theta(r, v) = S_\lambda\left(^\theta(r, v)\right).$$

It is straightforward to see that the character χ_λ^θ of S_λ^θ lies over μ, implying that S_λ^θ and S_μ are equivalent representations of H. It follows that there is an isomorphism $D\colon X_\mu \to X_\lambda$ satisfying

$$S_\mu = D^{-1}S_\lambda^\theta D.$$

Since θ commutes with the action of $\mathbf{U}_n(\mathbf{R})$ on $\mathbf{V}$, we easily see that

$$W_\mu(g)^{-1}D^{-1}W_\lambda(g)D$$

centralizes S_μ for each $g \in \mathbf{U}_n(\mathbf{R})$. Schur's Lemma implies that

$$D^{-1}W_\lambda(g)D = \eta(g)W_\mu(g), \quad g \in \mathbf{U}_n(\mathbf{R}), \tag{19}$$

where η is a linear character of $\mathbf{U}_n(\mathbf{R})$.

Consider the ideal I of R defined by

$$I = \begin{cases} max^{(l+1)/2} & \text{if } l \text{ is odd} \\ max^{l/2} & \text{if } l \text{ is even.} \end{cases}$$

Certainly, $I^2 = (0)$. Let $J = \big((0) : I\big)$ and $K = (I : J)$. Then

$$K = \begin{cases} max & \text{if } l \text{ is odd} \\ R & \text{if } l \text{ is even.} \end{cases}$$

In either case, $max \subseteq K$.

Let B be the subgroup $(0, IV)$ of H. We easily check that B is θ-invariant. We claim now that D maps $X_\mu(I)$ onto $X_\lambda(I)$. For let v be an element of $X_\mu(I)$. Then

$$S_\mu(h)v = v$$

https://doi.org/10.4153/CJM-2002-047-5 Published online by Cambridge University Press

for all h in B. It follows that

$$S_\lambda({}^\theta h)Dv = Dv.$$

Since B is θ-invariant, $Dv \in X_\lambda(I)$ and we see that $DX_\mu(I) \leq X_\lambda(I)$. Similarly, $D^{-1}X_\lambda(I) \leq X_\mu(I)$ and the equality follows.

By Theorem 3.2, $X_\mu(I)$ is non-trivial and $\mathbf{U}_n(\mathbf{max})$ acts trivially on $X_\mu(I)$. Let v be an element of $X_\mu(I)$ and g an element of $\mathbf{U}_n(\mathbf{max})$. Then $W_\mu(g)v = v$. Since $Dv \in X_\lambda(I)$, we also have $W_\lambda(g)Dv = Dv$. It follows from the equality in (19) that $\eta(g)v = v$ and thus $\eta(g) = 1$ for all g in $\mathbf{U}_n(\mathbf{max})$. Now $\mathbf{U}_n(\mathbf{max})$ is the kernel of the homomorphism π studied in Lemma 2.11. Thus $\mathbf{U}_n(\mathbf{R})/\mathbf{U}_n(\mathbf{max})$ is isomorphic to $\mathbf{U}_n(F_{q^2})$ and we may thus consider η as a linear character of $\mathbf{U}_n(F_{q^2})$. Since the commutator quotient of this group is a p'-group, it follows that η has p'-order.

We have shown in Corollary 2.13 that the commutator quotient of $\mathrm{Sp}_{2n}(R)$ is a p-group. It follows that both $\det W_\lambda$ and $\det W_\mu$ have order a power of p. Taking determinants in (19), we deduce that the order of η is also a power of p, since both W_λ and W_μ have degree q^{nl}.

It follows that η is trivial and thus the characters Ψ_λ and Ψ_μ of W_λ and W_μ are equal, as asserted. ∎

Definition 3.4 By *the* Weil character Ψ of $\mathbf{U}_n(\mathbf{R})$ we understand the restriction to $\mathbf{U}_n(\mathbf{R})$ of the Weil character of $\mathrm{Sp}_{2n}(R)$ of any primitive type.

Theorem 3.3 ensures that the definition above makes sense.

Theorem 3.5 *Ψ is rational valued and for all $g \in \mathbf{U}_n(\mathbf{R})$, we have $\Psi(g) = \pm q^{N(g)}$.*

Proof The complex conjugate of the character χ_λ lies over $\overline{\lambda} = \lambda[-1]$, whence $\overline{\chi_\lambda} = \chi_{\lambda[-1]}$ by uniqueness. It follows that $\overline{\psi_\lambda}$ is a Weil character of type $\lambda[-1]$.

In the perfect case there is only one such character, so $\overline{\psi_\lambda} = \psi_{\lambda[-1]}$. Suppose next that $q = 3$ and $n = 1$, and let g be the symplectic transvection used in Definition 2.7. We have

$$\overline{\psi_\lambda} = \overline{\sum_{r\in R} \lambda(r^2)} = \sum_{r\in R} \lambda(-r^2) = \psi_{\lambda[-1]}(g).$$

Thus, by definition, $\overline{\psi_\lambda}$ is *the* Weil character of type $\lambda[-1]$.

In either case $\overline{\psi_\lambda} = \psi_{\lambda[-1]}$. Thus the complex conjugate of Ψ_λ is $\Psi_{\lambda[-1]}$. Since we know from Theorem 3.3 that $\Psi_\lambda = \Psi_{\lambda[-1]}$, it follows that Ψ_λ is real-valued. The formula in Proposition 3.1 now implies that for $g \in \mathbf{U}_n(\mathbf{R})$, $\Psi(g) = \pm q^{N(g)}$, and thus $\Psi = \Psi_\lambda$ is rational-valued and takes the stated values. ∎

Corollary 3.6 $\det \Psi = 1$.

Proof This is clear when $\mathrm{Sp}_{2n}(R)$ is perfect. When $\mathrm{Sp}_{2n}(R)$ is not perfect, we know from Corollary 2.13 that the order of $\det \psi$, and hence that of $\det \Psi$, is a power of p, which is odd. But since Ψ is rational valued, so must be $\det \Psi$ and therefore the order of $\det \Psi$ divides 2. All in all, the order of $\det \Psi$ divides 1, and hence $\det \Psi$ is trivial. ∎

https://doi.org/10.4153/CJM-2002-047-5 Published online by Cambridge University Press

4 A Comparison Theorem for Characters

We prove here a slight generalization of a theorem of R. Knörr [Kn, Proposition 1.1]. We note here that in the statement of Knörr's result, the quantity z defined as the sum of the character values should be the product of these values. Our proof follows that of Knörr closely for most of its argument.

Theorem 4.1 *Let G be a finite group. Let ϕ and φ be generalized characters of G with the property that for each p'-element g of G we have*

$$\phi(g) = \pm\varphi(g) = \pm p^{m(g)},$$

where $m(g)$ is a non-negative integer. Suppose also that $\phi(1) = \varphi(1)$. Then there exists a linear character η of G of order dividing 2 such that

$$\phi(g) = \eta(g)\varphi(g)$$

for each p'-element g of G.

Proof Let W denote the complex vector space of complex-valued functions which are defined on the set of p'-elements of G and which are constant on the conjugacy classes of p'-elements. W has a basis consisting of the characteristic functions of the conjugacy classes of p'-elements and thus its dimension equals the number, r say, of conjugacy classes of p'-elements of G. W also has a basis consisting of the irreducible Brauer characters of G for the prime p by Theorem 15.10 of [I]. Let L be the integral lattice in W consisting of generalized Brauer characters of G. Thus L consists of rational integral sums of Brauer characters of G and has rank r as a lattice. We may identify L with the lattice generated by the restrictions to p'-elements of the generalized complex characters of G by Theorem 15.14 of [I]. Thus the restrictions of ϕ and φ to p'-elements of G are elements of L.

We define a linear transformation T of W by setting

$$T(\chi)(g) = \varphi(g)\chi(g)$$

for each function χ in W and each p'-element g of G. Since φ is a generalized character of G, T maps L into itself. By evaluating T on the characteristic functions of the conjugacy classes of p'-elements of G, we see that

$$\det T = \varphi(g_1)\cdots\varphi(g_r),$$

where $g_1, \ldots, g_r$ are representatives of the conjugacy classes of p'-elements of G. As each $\varphi(g_i)$ is a power of p, $\det T$ is a power of p. Since $T(L)$ is a sublattice of index $\det T$ in L, we deduce that there is an integer $a \geq 0$ with and some χ in L with

$$T(\chi) = p^a\widehat{\phi},$$

where $\widehat{\phi}$ is the restriction of ϕ to p'-elements. Our hypothesis on the values of ϕ and φ shows that $\chi(g) = \pm p^a$ for all p'-elements g. Now χ is a rational integral linear

https://doi.org/10.4153/CJM-2002-047-5 Published online by Cambridge University Press

combination of irreducible Brauer characters. Since the irreducible Brauer characters are linearly independent modulo p (see, for example, [I, Theorem 15.5]), it follows that $p^{-a}\chi$ is also in L. We set $\eta' = p^{-a}\chi$. We now have $T(\eta') = \widehat{\phi}$, $\eta'(g) = \pm 1$ for all p'-elements g and $\eta'(1) = 1$.

Finally, we extend η' to a class function η on the whole of G by setting

$$\eta(x) = \eta'(s),$$

where $x = us = su$ is the p-decomposition of x. It follows from the proof of Theorem 15.14 of [I] that η is a generalized character of G. Since η takes only the values ± 1, it is clear that the inner product of η with itself is 1. On the other hand, as η is a rational integral combination of irreducible complex characters, this is only possible if $\pm\eta$ is an irreducible complex character. Since $\eta(1) = 1$, η is a complex linear character of degree 1 whose square is trivial, as required. ∎

We note here the following elementary result, which will prove to be very effective in subsequent arguments. For a proof, see, for example, [I, Theorem 8.20].

Lemma 4.2 *Let ϱ be a rational-valued character of a finite group G. Let $x \in G$ and let $x = us = su$ be the p-decomposition of x. Then*

$$\varrho(x) \equiv \varrho(s) \mod p.$$

5 A Generalized Character of $\mathbf{U}_n(\mathbf{R})$

Recall from Section 2.6 that $\mathbf{V}(r) = \{v \in \mathbf{V} : (v, v) = r\}$ for all $r \in R$. Let m denote a generator of the minimal ideal *min* of R.

Definition 5.1 Let ν_1 be the permutation character of $\mathbf{U}_n(\mathbf{R})$ acting on $\mathbf{V}(0)$, let ν_2 be the permutation character of $\mathbf{U}_n(\mathbf{R})$ acting on $\mathbf{V}(m)$ and if l is even, let ν_3 be the permutation character of $\mathbf{U}_n(\mathbf{R})$ acting on $\mathbf{max}^{l/2}\,\mathbf{V}$. Define the generalized permutation character ν of $\mathbf{U}_n(\mathbf{R})$ by means of:

$$\nu = \begin{cases} (-1)^n(\nu_1 - \nu_2) & \text{if } l \text{ is odd} \\ \nu_3 & \text{if } l \text{ is even.} \end{cases} \tag{20}$$

Proposition 5.2 *Let s be a p'-element in $\mathbf{U}_n(\mathbf{R})$. Then*

$$\nu(s) = (-1)^{nl}(-q)^{N(s)}.$$

Proof Suppose first that l is odd. In view of Lemma 2.9 (d) and Lemma 2.14 we have:

$$\begin{aligned} \nu(s) &= (-1)^n\big(|\mathbf{V}(0)^s| - |\mathbf{V}(m)^s|\big) \\ &= (-1)^n\big(|\mathbf{V}(0)^s \cap \mathbf{V}^s| - |\mathbf{V}(m) \cap \mathbf{V}^s|\big) \\ &= (-1)^n\big(|\mathbf{V}^s(0)| - |\mathbf{V}^s(m)|\big) \\ &= (-1)^n(-q)^{l\,\mathrm{rank}\,\mathbf{V}^s} \\ &= (-1)^n(-q)^{N(s)}. \end{aligned}$$

https://doi.org/10.4153/CJM-2002-047-5 Published online by Cambridge University Press

Assume now that l is even. In view of Lemmas 2.14 and 2.15 we have:

$$\nu(s) = |(\omega^{l/2}\mathbf{V})^s| = |\omega^{l/2}\mathbf{V} \cap \mathbf{V}^s| = |\omega^{l/2}\mathbf{V}^s| = q^{l \operatorname{rank} V^s} = q^{N(s)} = (-q)^{N(s)}. \quad \blacksquare$$

Proposition 5.3 $\det \nu = \varepsilon^l$.

Proof As ν is rational-valued, it follows from Lemma 2.2 that the order of $\det \nu$ divides 2. Hence $\det \nu = \varepsilon^i$, where the parity of the integer i can be determined by examining the restriction of $\det \nu$ to the subgroup D of Corollary 2.12.

Suppose first that l is odd. Then Proposition 5.2 gives:

$$\nu_{|D}(x) = \begin{cases} -q^{l(n-1)} & \text{if } x \neq 1 \\ q^{ln} & \text{if } x = 1. \end{cases} \tag{21}$$

Let ρ_D be the regular character of D. Since D is a cyclic group of even order, $\det \rho_D$ has order 2. By virtue of (21) we have:

$$\nu_{|D} + q^{l(n-1)} \cdot 1_D = q^{l(n-1)} \frac{(q^l+1)}{q+1} \cdot \rho_D. \tag{22}$$

Since $q^{l(n-1)} \frac{(q^l+1)}{q+1}$ is an odd natural number, (5) and (22) show that $\det \nu_{|D} = \det \rho_D$ has order 2. Hence $\det \nu = \varepsilon$ by our opening remark.

Suppose now that l is even. Then Proposition 5.2 gives

$$\nu_{|D}(x) = \begin{cases} q^{l(n-1)} & \text{if } x \neq 1 \\ q^{ln} & \text{if } x = 1, \end{cases} \tag{23}$$

so

$$\nu_{|D} - q^{l(n-1)} \cdot 1_D = q^{l(n-1)} \frac{(q^l-1)}{q+1} \cdot \rho_D. \tag{24}$$

Since $q^{l(n-1)} \frac{(q^l-1)}{q+1}$ is an even natural number, (5) and (24) show that $\det \nu_{|D}$ is trivial. Hence $\det \nu = 1$ by our opening remark. $\blacksquare$

6 Computing the Weil Character of $\mathbf{U}_n(\mathbf{R})$

Theorem 6.1 *Let s be a p'-element of $\mathbf{U}_n(\mathbf{R})$. Then*

$$\Psi(s) = (-1)^{nl} \varepsilon(g)^l (-q)^{N(s)}. \tag{25}$$

Proof We have $\nu(1) = q^{nl}$ by Proposition 5.2 and $\Psi(1) = q^{nl}$. Moreover,

$$\nu(s) = \pm q^{N(s)} = \pm \Psi(s)$$

https://doi.org/10.4153/CJM-2002-047-5 Published online by Cambridge University Press

for all p'-elements s of $\mathbf{U}_n(\mathbf{R})$, due to Proposition 5.2 and Theorem 3.5. Thus the hypotheses of Theorem 4.1 are met, ensuring the existence of a linear character η of $\mathbf{U}_n(\mathbf{R})$ with $\eta^2 = 1$ that satisfies

$$\nu(s) = (\Psi\eta)(s) \tag{26}$$

for each p'-element s of $\mathbf{U}_n(\mathbf{R})$. By Corollary 2.12 we know that η is trivial or equal to ε and can be determined by its restriction to D.

Taking determinants in (26) applied D we get

$$\det \nu_{|D} = \det \Psi_{|D} \eta_{|D}^{q^{nl}}.$$

Since $\det \Psi = 1$ by Corollary 3.6 and q^{nl} is odd, the above translates into

$$\det \nu_{|D} = \eta_{|D},$$

hence Proposition 5.3 gives

$$\eta = \det \nu = \varepsilon^l. \tag{27}$$

By virtue of (26), (27) and Proposition 5.2 we get that for all p'-elements s of $\mathbf{U}_n(\mathbf{R})$

$$\Psi(s) = (-1)^{nl}\varepsilon(s)^l(-q)^{N(s)}. \qquad \blacksquare$$

Theorem 6.2 *Let $x \in \mathbf{U}_n(\mathbf{R})$ and let $x = us = su$ be the p-decomposition of x. Suppose that $\mathbf{V}^s = \{0\}$. Then*

$$\Psi(x) = (-1)^{nl}\varepsilon(x)^l. \tag{28}$$

Proof By Lemma 4.2 and Theorem 3.5

$$\Psi(x) \equiv \Psi(s) \mod p, \tag{29}$$

while by Theorem 6.1 and hypothesis

$$\Psi(s) = (-1)^{nl}\varepsilon(s)^l. \tag{30}$$

Thus

$$\Psi(x) \equiv (-1)^{nl}\varepsilon(s)^l \mod p. \tag{31}$$

But if $\mathbf{V}^s = \{0\}$, it follows that $\mathbf{V}^x = \{0\}$ also, since s is a power of x. Thus we have $N(s) = N(x) = 0$ and so $\Psi(x) = \pm 1$ by Theorem 3.5. Thus the only explanation for (31) is that $\Psi(x) = (-1)^{nl}\varepsilon(s)^l$. Now since u has odd order, it follows that $\varepsilon(u) = 1$ and thus $\varepsilon(x) = \varepsilon(s)$. We thus obtain the desired formula. $\blacksquare$

Before proving our next result on the Weil character, we require a well known characterization of Mersenne primes.

https://doi.org/10.4153/CJM-2002-047-5 Published online by Cambridge University Press

Lemma 6.3 *Suppose that $q+1$ has no odd prime divisor. Then $q=p$ is a Mersenne prime.*

Proof Clearly, $q+1$ must be a power of 2. Since $q=p^a$ for some positive integer a, we have $p^a+1=2^b$, for some positive integer b. It is well known, and easy to prove, that in this case a must equal 1 and b must be a prime. Thus $q=p$ is a Mersenne prime. ∎

Theorem 6.4 *Suppose that q is not a Mersenne prime. Then for $x \in \mathbf{U}_n(\mathbf{R})$,*

$$\Psi(x) = (-1)^{nl}\varepsilon(x)^l(-q)^{N(x)}.$$

Proof Write

$$\Psi(x) = \delta(x)q^{N(x)},$$

where $\delta(x) = \pm 1$, in accordance with Theorem 3.5. Let r be an odd prime divisor of $q+1$ and suppose first that r does not divide the order of x. Let $z = z_\alpha$, where α is an element of $\mathbf{N}$ of order r, and set $w = xz$. Let $w = us = su$ be the p-decomposition of w. We claim that $\mathbf{V}^s = \{0\}$. For, since x has order coprime to r, z is a power of s. Moreover, $\mathbf{V}^z = \{0\}$ by Lemma 2.16, and thus $\mathbf{V}^s = \{0\}$ also, proving our claim. It follows from Theorem 6.2 that

$$\Psi(w) = (-1)^{nl}\varepsilon(w)^l.$$

Lemma 4.2 implies that

$$\delta(x)q^{N(x)} \equiv \Psi(x) \equiv \Psi(w) \equiv (-1)^{nl}\varepsilon(w)^l \mod r. \tag{32}$$

We note that $q \equiv -1 \mod r$ and thus $q^{N(x)} \equiv (-1)^{N(x)} \mod r$. Therefore

$$\delta(x)q^{N(x)} \equiv \delta(x)(-1)^{N(x)} \mod r. \tag{33}$$

It follows from (32) and (33) that

$$\delta(x)(-1)^{N(x)} \equiv (-1)^{nl}\varepsilon(w)^l \mod r$$

and since r is odd, we must have the actual equality

$$\delta(x)(-1)^{N(x)} = (-1)^{nl}\varepsilon(w)^l.$$

Therefore,

$$\delta(x) = (-1)^{nl}(-1)^{N(x)}\varepsilon(w)^l.$$

Finally, since ε is a homomorphism and z has odd order,

$$\varepsilon(w) = \varepsilon(xz) = \varepsilon(x)\varepsilon(z) = \varepsilon(x).$$

https://doi.org/10.4153/CJM-2002-047-5 Published online by Cambridge University Press

Thus we obtain

$$\Psi(x) = (-1)^{nl}(-1)^{N(x)}q^{N(x)}\varepsilon(x)^l = (-1)^{nl}\varepsilon(x)^l(-q)^{N(x)}.$$

Suppose now that r divides the order of x. Let $x = hg = gh$ be the r-decomposition of x, where g has r'-order and the order of h is a power of r. We know that

$$\Psi(g) = (-1)^{nl}\varepsilon(g)^l(-q)^{N(g)}$$

and we have

$$\delta(x)q^{N(x)} \equiv \Psi(x) \equiv \Psi(g) \equiv (-1)^{nl}\varepsilon(g)^l(-q)^{N(g)} \mod r. \tag{34}$$

Since $(-q)^{N(g)} \equiv 1 \mod r$, $q^{N(x)} \equiv (-1)^{N(x)} \mod r$ and $\delta(x) = \pm 1$, (34) yields

$$\delta(x) = (-1)^{nl}\varepsilon(g)^l(-1)^{N(x)}.$$

Finally, we also have $\varepsilon(x) = \varepsilon(g)$, since h has odd order. Thus,

$$\delta(x) = (-1)^{nl}\varepsilon(x)^l(-1)^{N(x)}$$

and the result is proved. ∎

7 The General Case

We do not impose here any restrictions on q, except for our general assumption that q is the power of an odd prime. Note that q^3 cannot be a Mersenne prime.

Lemma 7.1 *Let $G_1 \subseteq G_2$ be finite abelian groups. Suppose that the 2-Sylow subgroups of G_1 and G_2 coincide. Then $G_1^2 = G_2^2 \cap G_1$, that is, if $a \in G_1$, then a has a square root in G_1 if and only if a has a square root in G_2.*

Proof Since G_1 and G_2 are the direct products of their Sylow subgroups and squaring is an automorphism of an odd order Sylow subgroup, we may assume without loss of generality that G_1 and G_2 coincide with their 2-Sylow subgroups. Since by assumption these Sylow subgroups are equal, the result follows. ∎

The ring epimorphism $R \to F_q$ yields a ring epimorphism of the polynomial rings $R[t] \to F_q[t]$, by reduction modulo *max*. There certainly exists a cubic irreducible polynomial in $F_q[t]$. Lift this polynomial to a cubic polynomial $p(t) \in R[t]$.

Set $T = R[t]/\big(p(t)\big)$ and $\mathbf{T} = T[t]/(t^2 - e)$. Recall at this point that $e \in R^* \setminus R^{*2}$ and that we obtained $\mathbf{R}$ by adjoining to R a square root $\mathbf{e}$. Let us now make the specific choice $\mathbf{e} = t + (t^2 - e) \in \mathbf{T}$.

https://doi.org/10.4153/CJM-2002-047-5 Published online by Cambridge University Press

Lemma 7.2

(a) $\mathbf{T}/T$ *is a quadratic extensions of finite, commutative, principal and local rings of odd characteristic.*
(b) $\mathbf{R}$ *is a subring of* $\mathbf{T}$ *and* $\mathbf{T}$ *is a free* $\mathbf{R}$*-module of rank 3.*
(c) *The involution of* $\mathbf{T}$ *that fixes* T *restricts to the involution of* $\mathbf{R}$ *that fixes* R.
(d) *The residue field of* T *is equal to* F_{q^3} *and* $|T| = (q^3)^l$.

Proof It is clear that T and $\mathbf{T}$ are finite commutative rings of odd characteristic. We claim that T is a local ring with maximal ideal $T\,max$. Indeed, let a be an element of T that does not belong to $T\,max$. Setting $\mathbf{d} = t + \big(p(t)\big) \in T$, we may write $a = r(\mathbf{d})$, where $0 \neq r(t) \in R[t]$ has degree ≤ 2 and does not vanish modulo max. Note that the reductions of $r(t)$ and $p(t)$ modulo max are coprime polynomials in $F_q[t]$. Thus, there exists $s(t) \in R[t]$ such that $r(\mathbf{d})s(\mathbf{d}) \in 1 + max[\mathbf{d}]$. Since max is nilpotent, $1 + max[\mathbf{d}] \subset T^*$, whence $a = r(\mathbf{d})$ is invertible. This proves the claim.

As max is principal, so is $T\,max$. It follows that every maximal ideal of T is principal, whence T is principal ring.

We contend that the residue field of T is F_{q^3}. Indeed, since T is a free R-module with basis $\{1, \mathbf{d}, \mathbf{d}^2\}$, we have

$$|T/T\,max| = |R[\mathbf{d}]/\,max[\mathbf{d}]| = q^3,$$

as required. Remark that the nilpotency degree of $T\,max$ is also equal to l. It follows that $|T| = (q^3)^l$ and $|T^*| = q^{3(l-1)}(q^3-1)$. Observe that part (d) has been established.

We proceed to show that $e \notin T^{*2}$. We know that the unit groups R^* and T^* have orders $q^{l-1}(q-1)$ and $q^{3(l-1)}(q^3-1) = q^{3(l-1)}(q^2+q+1)(q-1)$, respectively. As q^{l-1} and $q^{3(l-1)}(q^2+q+1)$ are odd, Lemma 7.1 applies to yield $e \notin T^{*2}$. This completes the proof of part (a).

It is clear that $\mathbf{R}$ is a subring of $\mathbf{T}$. Moreover, $\mathbf{T}$ is a free R-module of rank 6 with basis $\{1, \mathbf{d}, \mathbf{d}^2, \mathbf{e}, \mathbf{ed}, \mathbf{ed}^2\}$, whence $\mathbf{T}$ is a free $\mathbf{R}$-module of rank 3 with basis $\{1, \mathbf{d}, \mathbf{d}^2\}$. This demonstrates part (b). As part (c) is obvious, the proof is complete. ∎

Lemma 7.3 *For all* $g \in \mathbf{U}_n(\mathbf{R})$ *we have*

$$\varepsilon(g) = \begin{cases} 1 & \text{if } \det g \in \mathbf{N}^2 \\ -1 & \text{otherwise.} \end{cases} \tag{35}$$

Proof As $\mathbf{N}$ has order $q^{l-1}(q+1)$ and the subgroup of $\mathbf{N}$ of order $q+1$ is isomorphic to the one-norm subgroup of F_{q^2} and hence cyclic, it follows that $\mathbf{N}^2$ has index 2 in $\mathbf{N}$. Since the determinant map of $\mathbf{U}_n(\mathbf{R})$ takes values in $\mathbf{N}$, we deduce that the right hand side of (35) does define a linear character of $\mathbf{U}_n(\mathbf{R})$ of order 2, hence equality prevails in (35) by uniqueness (*cf.* Corollary 2.12). ∎

Fix an orthonormal $\mathbf{R}$-basis $\{v_1, \ldots, v_n\}$ of $\mathbf{V}$. Set $\mathbf{Y} = \mathbf{T} \otimes_{\mathbf{R}} \mathbf{V}$ and define a non-degenerate hermitian $\mathbf{T}$-form on $\mathbf{Y}$ by declaring $\{1 \otimes v_1, \ldots, 1 \otimes v_n\}$ to be an

https://doi.org/10.4153/CJM-2002-047-5 Published online by Cambridge University Press

orthonormal basis of $\mathbf{Y}$. Given $g \in \mathbf{U}_n(\mathbf{R})$ let $\overline{g} \in \mathbf{U}_n(\mathbf{T})$ be defined by

$$\overline{g}(\mathbf{t} \otimes v) = \mathbf{t} \otimes g(v), \quad \mathbf{t} \in \mathbf{T}, v \in \mathbf{V}.$$

Observe that $\mathbf{U}_n(\mathbf{R}) \ni g \mapsto \overline{g} \in \mathbf{U}_n(\mathbf{T})$ is a group monomorphism.

Lemma 7.4 *Let $\varepsilon_{\mathbf{T}}$ denote the linear character of order 2 of $\mathbf{U}_n(\mathbf{T})$. Then for all $g \in \mathbf{U}_n(\mathbf{R})$ we have*

$$\varepsilon_{\mathbf{T}}(\overline{g}) = \varepsilon(g).$$

Proof Clearly $\det \overline{g} = \det g$. Also, the one-norm groups $\mathbf{N}$ and $\mathbf{N}_{\mathbf{T}}$ of $\mathbf{R}$ and $\mathbf{T}$ have orders $q^{l-1}(q+1)$ and $q^{3(l-1)}(q^3+1) = q^{3(l-1)}(q^2-q+1)(q+1)$, respectively. As q^{l-1} and $q^{3(l-1)}(q^2-q+1)$ are odd and $\mathbf{N} \subset \mathbf{N}_{\mathbf{T}}$ by Lemma 7.2 (c), we may apply Lemmas 7.1 and 7.3 to obtain the desired result. ∎

Lemma 7.5 *For all $g \in \mathbf{U}_n(\mathbf{R})$ we have*

$$|\ker(\overline{g} - I_{\mathbf{Y}})| = |\ker(g - I_{\mathbf{V}})|^3.$$

Proof Note that $\ker(\overline{g} - I_{\mathbf{Y}}) = \ker(\overline{g - I_{\mathbf{V}}})$. We claim that $\ker(\overline{g - I_{\mathbf{V}}})$ is equal to $\mathbf{T} \otimes_{\mathbf{R}} \ker(g - I_{\mathbf{V}})$. The inclusion $\mathbf{T} \otimes_{\mathbf{R}} \ker(g - I_{\mathbf{V}}) \subseteq \ker(\overline{g - I_{\mathbf{V}}})$ is clear. To see the reverse inclusion, let $w \in \ker(\overline{g - I_{\mathbf{V}}})$. In view of Lemma 7.2 (b) there exists an $\mathbf{R}$-basis $\{\mathbf{t}_1, \mathbf{t}_2, \mathbf{t}_3\}$ of $\mathbf{T}$. Accordingly, we may write w uniquely as

$$w = \mathbf{t}_1 \otimes v_1 + \mathbf{t}_2 \otimes v_2 + \mathbf{t}_3 \otimes v_3,$$

where the $v_i \in \mathbf{V}$. Now

$$0 = (\overline{g - I_{\mathbf{V}}})w = \mathbf{t}_1 \otimes \big(g(v_1) - v_1\big) + \mathbf{t}_2 \otimes \big(g(v_2) - v_2\big) + \mathbf{t}_3 \otimes \big(g(v_3) - v_3\big),$$

whence $g(v_i) = v_i$ for all i by uniqueness. This proves our claim. It follows that

$$|\ker(\overline{g} - I_{\mathbf{Y}})| = |\ker(\overline{g - I_{\mathbf{V}}})| = |\mathbf{T} \otimes_{\mathbf{R}} \ker(g - I_{\mathbf{V}})| = |\ker(g - I_{\mathbf{V}})|^3.$$ ∎

Lemma 7.6 *For all $g \in \mathbf{U}_n(\mathbf{R})$ we have*

$$N(\overline{g}) = N(g).$$

Proof In light of Lemma 7.5 we have

$$(q^3)^{2N(\overline{g})} = |\ker(\overline{g} - I_{\mathbf{Y}})| = |\ker(g - I_{\mathbf{V}})|^3 = (q^{2N(g)})^3.$$ ∎

Let $\Psi_{\mathbf{T}}$ denote the Weil character $\mathbf{U}_n(\mathbf{T})$.

Lemma 7.7 *For all $g \in \mathbf{U}_n(\mathbf{R})$ we have*

$$\Psi_{\mathbf{T}}(\overline{g}) = (-1)^{nl}\varepsilon(g)^l(-q^3)^{N(g)}.$$

https://doi.org/10.4153/CJM-2002-047-5 Published online by Cambridge University Press

Proof As q^3 is not a Mersenne prime, this follows at once from Theorem 6.4 and Lemmas 7.2 (d), 7.4 and 7.6. ■

Lemma 7.8 *For all $g \in \mathbf{U}_n(\mathbf{R})$ we have*

$$\Psi_{\mathbf{T}}(\overline{g}) = \Psi(g)^3.$$

Proof By Lemma 7.7 and Theorem 3.5 we have

$$\Psi_{\mathbf{T}}(\overline{g}) = \pm\Psi(g)^3, \quad g \in \mathbf{U}_n(\mathbf{R}).$$

Moreover, note that

$$\Psi_{\mathbf{T}}(\overline{1}) = \Psi(1)^3.$$

In view of Theorem 4.1 there exists a linear character η of $\mathbf{U}_n(\mathbf{R})$ of order dividing 2 such that for all $g \in \mathbf{U}_n(\mathbf{R})$,

$$\Psi_{\mathbf{T}}(\overline{g}) = \eta(g)\Psi(g)^3.$$

Taking determinants above and making use of the fact that the Weil character has determinant 1 we get $\eta^{q^{3nl}} = 1$. Since 2 and q^{3nl} are coprime it follows that $\eta = 1$, as desired. ■

Theorem 7.9 *Let $\mathbf{R}/R$ be a quadratic extension of finite, commutative, local and principal rings of odd characteristic. Let $\mathbf{U}_n(\mathbf{R})$ be the unitary group of rank n associated to $\mathbf{R}/R$. Let F_q be the residue field of R. Let ε be the only linear character of $\mathbf{U}_n(\mathbf{R})$ of order 2, that is*

$$\varepsilon(g) = \begin{cases} 1 & \text{if } \det g \in \mathbf{N}^2 \\ -1 & \text{otherwise,} \end{cases}$$

where $\mathbf{N}$ is the subgroup of $\mathbf{R}^*$ of all elements having norm equal to 1. Write $|R| = q^l$ and $|\ker(g - I)| = q^{2N(g)}$ for each $g \in \mathbf{U}_n(\mathbf{R})$. Let Ψ be the Weil character of $\mathbf{U}_n(\mathbf{R})$. Then for all g in $\mathbf{U}_n(\mathbf{R})$,

$$\Psi(g) = (-1)^{nl}\varepsilon(g)^l(-q)^{N(g)}.$$

Proof As Ψ is rational valued, this follows at once from Lemmas 7.7 and 7.8. ■

References

[CMS] G. Cliff, D. McNeilly and F. Szechtman, *Weil representations of symplectic groups over rings.* J. London Math. Soc. **62**(2000), 423–436.

[G] P. Gérardin, *Weil representations associated to finite fields.* J. Algebra **46**(1977), 54–101.

[I] I. M. Isaacs, *Character Theory of Finite Groups.* Academic Press, New York, 1976.

[K] W. Klingenberg, *Symplectic groups over local rings.* Amer. J. Math. **85**(1963), 232–240.

[Kn] R. Knörr, *On the number of characters in a p-block of a p-solvable group.* Illinois J. Math. **28**(1984), 181–210.

https://doi.org/10.4153/CJM-2002-047-5 Published online by Cambridge University Press

[S] F. Szechtman, *Weil representations of finite symplectic groups*. Ph. D. thesis, University of Alberta, 1999.
[T] D. E. Taylor, *The Geometry of the Classical Groups.* Heldermann Verlag, Berlin, 1992.

Department of Mathematics
University College Dublin
Belfield, Dublin 4
Ireland
email: rod.gow@ucd.ie

Instituto de Matemática y Estadística
Universidad de la República
Julio Herrera y Reissig 565
CP 11300 Montevideo
Uruguay

Current address:
Department of Pure Mathematics
University of Waterloo
Waterloo, Ontario
N2L 3G1
email: fszechtm@herod.uwaterloo.ca

https://doi.org/10.4153/CJM-2002-047-5 Published online by Cambridge University Press