Canad. Math. Bull. Vol. **61** (1), 2018 pp. 174–190
http://dx.doi.org/10.4153/CMB-2017-046-0

A Factorization Result for Classical and Similitude Groups

Alan Roche and C. Ryan Vinroot

Abstract. For most classical and similitude groups, we show that each element can be written as a product of two transformations that preserve or almost preserve the underlying form and whose squares are certain scalar maps. This generalizes work of Wonenburger and Vinroot. As an application, we re-prove and slightly extend a well-known result of Mœglin, Vignéras, and Waldspurger on the existence of automorphisms of p-adic classical groups that take each irreducible smooth representation to its dual.

1 Introduction

For many classical groups G, we show that each element is a product of two involutions. The involutions belong to a group $\widetilde{G}$ containing G such that $[\widetilde{G}:G] \le 2$. We also prove a similar factorization for elements of the corresponding similitude groups. Our methods apply to classical (and similitude groups) over arbitrary fields with the exception of orthogonal groups (and the corresponding similitude groups) over fields of even characteristic. Our interest in such factorizations stems from an application to the representation theory of reductive groups over non-Archimedean local fields. We are interested in involutary automorphisms of such groups that take each irreducible smooth representation to its dual. Echoing [1], we call these *dualizing involutions*. They do not always exist in our setting (we give an example in §9). They do exist, however, for many classical p-adic groups by a result of Mœglin, Vignéras and Waldspurger [15, Chapter IV §II]. We re-prove this result and slightly extend its scope as explained below.

To make more precise statements, we need to define the classical and similitude groups we consider. Let E/F be a field extension with $E = F$ or $[E:F] = 2$. We assume in the quadratic case that E/F is a Galois extension. In all cases we write τ for the generator of $\mathrm{Gal}(E/F)$, so that τ has order two when $[E:F] = 2$ and $\tau = 1$ when $E = F$. Let V be a finite-dimensional vector space over E with a non-degenerate ϵ-hermitian form $\langle\cdot,\cdot\rangle$ ($\epsilon = \pm1$) which we take to be linear in the first variable. Thus

$$\langle \alpha u + \beta v, w\rangle = \alpha\langle u, w\rangle + \beta\langle v, w\rangle \quad \text{and} \quad \langle v, w\rangle = \epsilon\,\tau(\langle w, v\rangle)$$

for all $\alpha, \beta \in E$ and $u, v, w \in V$. It follows that $\langle\cdot,\cdot\rangle$ is τ-linear in the second variable:

$$\langle u, \alpha v + \beta w\rangle = \tau(\alpha)\langle u, v\rangle + \tau(\beta)\langle u, w\rangle.$$

Received by the editors August 26, 2016; revised January 9, 2017.
Published electronically October 25, 2017.
Author C. V. was supported in part by a grant from the Simons Foundation, Award #280496.
AMS subject classification: **20G15**, 22E50.
Keywords: classical group, similitude group, involution, p-adic group, dual representation.

In the case char $F = 2$ and $E = F$ we assume also that $\langle v, v\rangle = 0$ for all $v \in V$, that is, $\langle\cdot,\cdot\rangle$ is symplectic.

We write $\mathrm{U}(V)$ for the isometry group (or unitary group) of $\langle\cdot,\cdot\rangle$ and $\mathrm{GU}(V)$ for the corresponding similitude group. That is,

$$\mathrm{U}(V) = \{g \in \mathrm{Aut}_E(V) : \langle gv, gv'\rangle = \langle v, v'\rangle, \forall v, v' \in V\},$$
$$\mathrm{GU}(V) = \{g \in \mathrm{Aut}_E(V) : \langle gv, gv'\rangle = \beta\langle v, v'\rangle, \text{for some scalar } \beta, \forall v, v' \in V\}.$$

Applying τ to both sides of $\langle gv, gv'\rangle = \beta\langle v, v'\rangle$ ($g \in \mathrm{GU}(V)$) gives $\tau(\beta) = \beta$, so that $\beta \in F^\times$. For $g \in \mathrm{GU}(V)$ with associated scalar β, we often write $\mu(g) = \beta$. This is the *multiplier* of g and the resulting homomorphism $\mu\colon \mathrm{GU}(V) \to F^\times$ is the *multiplier map*.

Definition 1.1 Let $h \in \mathrm{Aut}_F(V)$. We say that h is *anti-unitary* if $\langle hv, hv'\rangle = \langle v', v\rangle$, for all $v, v' \in V$.

When $E = F$ and char $F \neq 2$, the form $\langle\cdot,\cdot\rangle$ is orthogonal ($\epsilon = 1$) or symplectic ($\epsilon = -1$). In the orthogonal case, an anti-unitary map is simply an orthogonal transformation. In the symplectic case, an anti-unitary map is a skew-symplectic transformation: $\langle hv, hv'\rangle = -\langle v, v'\rangle$.

We also need the corresponding notion for similitude groups.

Definition 1.2 Let $h \in \mathrm{Aut}_F(V)$. We say also that h is an *anti-unitary similitude* if, for some scalar β, $\langle hv, hv'\rangle = \beta\langle v', v\rangle$, for all $v, v' \in V$.

Thus an anti-unitary map is an anti-unitary similitude for which $\beta = 1$. As above, the scalar associated with any anti-unitary similitude lies in $F^\times$. Furthermore, it is straightforward to see that any anti-unitary map or similitude h is τ-linear in the sense that $h(\alpha v) = \tau(\alpha)h(v)$ for all $\alpha \in E$ and $v \in V$. In particular, a product of two anti-unitary similitudes (respectively, maps) belongs to $\mathrm{GU}(V)$ (respectively, $\mathrm{U}(V)$).

We can now state our factorization result.

Theorem A *Let $g \in \mathrm{GU}(V)$ with $\mu(g) = \beta$. Then there is an anti-unitary involution h_1 and an anti-unitary similitude h_2 with $h_2^2 = \beta$ such that $g = h_1h_2$. In particular, for any $g \in \mathrm{U}(V)$, there exist anti-unitary elements h_i with $h_i^2 = 1$ (for $i = 1, 2$) such that $g = h_1h_2$.*

For example, Theorem A says that any orthogonal transformation is a product of two orthogonal involutions and that any symplectic transformation is a product of two skew-symplectic involutions. This was originally proved by Wonenburger [26] (under the assumption char $F \neq 2$). While we ultimately obtain a new proof of her results, we borrow heavily from her approach. In particular, the arguments in §4 below are in essence those of [26] but rephrased in the language of modules. For $E = F$ and char $F \neq 2$, Theorem A in the case of similitude groups is due to Vinroot [24, 25] (by an adaptation of Wonenburger's arguments).

Our framework does not accommodate orthogonal groups in even characteristic (defined as the stabilizers of suitably non-degenerate quadratic forms) or the corresponding similitude groups. If F is perfect, then it follows readily from the work of Gow [9] or Ellers and Nolte [7] that Theorem A continues to hold in this setting.

Suppose now that F is a non-Archimedean local field and that G is the group of F-points of a reductive F-group. Let π be an irreducible smooth representation of G. For any continuous automorphism α of G, we write π^α for the (smooth) representation of G given by $\pi^\alpha(g) = \pi({}^\alpha g)$ for $g \in G$. We write $\pi^\vee$ for the smooth dual or contragredient of π.

Definition 1.3 Let ι be a continuous automorphism of G of order at most two. We say that ι is a *dualizing involution* of G if $\pi^\iota \cong \pi^\vee$ for all irreducible smooth representations π of G.

We fix an anti-unitary involution $h \in \mathrm{Aut}_F(V)$ and set ${}^\iota g = \mu(g)^{-1}hgh^{-1}$ for $g \in \mathrm{GU}(V)$. Then ι defines a continuous automorphism of $\mathrm{GU}(V)$ of order two. Further $\iota|_{\mathrm{U}(V)}$ gives the automorphism $g \mapsto hgh^{-1}$ of $\mathrm{U}(V)$ which for simplicity we again denote by ι. Our application of Theorem A hinges on the following consequence.

Corollary 1.4 *For any $g \in \mathrm{GU}(V)$, the elements ${}^\iota g$ and g^{-1} are conjugate by an element of* $\mathrm{U}(V)$.

Proof Let $g \in \mathrm{GU}(V)$ with $\mu(g) = \beta$. By Theorem A, we have $g = h_1h_2$ for an anti-unitary involution h_1 and an anti-unitary similitude h_2 with $h_2^2 = \beta$. Thus $h_2^{-1} = \beta^{-1}h_2$ and $g^{-1} = \beta^{-1}h_2h_1$. Hence

$$(h_1h){}^\iota g(h_1h)^{-1} = h_1h(\beta^{-1}h(h_1h_2)h^{-1})hh_1 = \beta^{-1}h_2h_1 = g^{-1}.$$

That is, ${}^\iota g$ and g^{-1} are conjugate by $h_1h \in \mathrm{U}(V)$. ∎

For the classical groups $\mathrm{U}(V)$, the corollary is part of [15, Chapter IV, Proposition I.2] and the early part of our proof of Theorem A mirrors the treatment in [15] (as well as [26]).

Our main result is the following.

Theorem B *The maps $\iota: \mathrm{U}(V) \to \mathrm{U}(V)$ and $\iota: \mathrm{GU}(V) \to \mathrm{GU}(V)$ are dualizing involutions.*

In the case of the classical groups $\mathrm{U}(V)$, this is essentially [15, Chapter IV, Théorème II.1]. Given Harish-Chandra's theory of characters [3, 11] as recalled in Section 8, Theorem B is an immediate consequence of the corollary.

The argument in [15] does not use characters. Instead it adapts a geometric method used by Gelfand and Kazhdan to show that transpose-inverse is a dualizing involution of $\mathrm{GL}_n(F)$ [8]. As with Theorem B, this property of transpose-inverse follows immediately from the existence of characters. Indeed, by elementary linear algebra, a square matrix is conjugate to its transpose. Thus if ${}^\theta g = {}^\top g^{-1}$ for $g \in G = \mathrm{GL}_n(F)$ then, for any irreducible smooth representation π of G, the characters of π^θ and $\pi^\vee$ are equal, whence $\pi^\theta \cong \pi^\vee$. Tupan [23] found a clever and completely elementary proof

https://doi.org/10.4153/CMB-2017-046-0 Published online by Cambridge University Press

of Gelfand and Kazhdan's result. We report elsewhere [20] on a similarly elementary proof of Theorem B that builds on Tupan's approach.

Finally, let G be the isometry group of a non-degenerate hermitian or anti-hermitian form over a p-adic quaternion algebra. By [14], there is no automorphism θ of G such that ${}^{\theta}g$ is conjugate to g^{-1} for all $g \in G$. Thus the corollary above is false in this setting, which means surely that Theorem B does not extend to classical groups over p-adic quaternion algebras. In this spirit, let D be a central finite-dimensional division algebra over F. By a straightforward argument (taken from unpublished work of Roche and Spallone), we show that the group $\mathrm{GL}_n(D)$ can admit an automorphism that takes each irreducible smooth representation to its dual only in the known cases $D = F$ and when D is a quaternion algebra over F [16,18]. In particular, in contrast to the case of connected reductive groups over the reals [1], dualizing involutions in our sense do not always exist.

1.1 Organization

The proof of Theorem A takes up Sections 1 through 5. We record some special cases and applications in Section 6. In Section 7 we briefly recall some character theory and prove Theorem B. In Section 8 we show that the unit groups of finite-dimensional central simple algebras over F do not admit dualizing involutions except in the two cases noted above.

2 Proof of Theorem A: Initial Setup and First Reduction

We use the following notation throughout the proof. For R a ring with identity, we write $R^{\times}$ for the group of units of R. For any R-module M (which for us is always a unital left R-module), we write $\operatorname{ann}_R M$ for the annihilator of M. That is, $\operatorname{ann}_R M = \{r \in R : rm = 0, \forall m \in M\}$. For $m \in M$, we also write $\operatorname{ann}_R m = \{r \in R : rm = 0\}$. Thus $\operatorname{ann}_R M = \bigcap_{m \in M} \operatorname{ann}_R m$. Note that $\operatorname{ann}_R m$ is the kernel of the surjective R-module homomorphism $r \mapsto rm \colon R \to Rm$, so that $R/\operatorname{ann}_R m \cong Rm$ as R-modules.

2.1 Let $g \in \mathrm{GU}(V)$ with $\mu(g) = \beta$. The space V is a module over the polynomial ring $E[T]$ via $f(T)v = f(g)v$. Let $p = p(T)$ denote the minimal polynomial of g. We have $p = p_1^{e_1} \cdots p_n^{e_n}$ for distinct monic irreducible elements $p_1, \dots, p_n \in E[T]$ and positive integers $e_1, \dots, e_n$.

We set $\mathcal{A} = E[T]/(p)$. The ideal (p) is simply the annihilator of V as an $E[T]$-module. In particular, V carries an induced $\mathcal{A}$-module structure. The Chinese Remainder Theorem gives a canonical isomorphism of E-algebras

$$E[T]/(p) \cong E[T]/(p_1^{e_1}) \oplus \cdots \oplus E[T]/(p_n^{e_n}).$$

Thus $\mathcal{A} = \mathcal{A}_1 \oplus \cdots \oplus \mathcal{A}_n$, for ideals $\mathcal{A}_i$ in $\mathcal{A}$ with $\mathcal{A}_i \cong E[T]/(p_i^{e_i})$ $(i = 1, \dots, n)$. Setting $V_i = \mathcal{A}_i V$ $(i = 1, \dots, n)$, we have

$$V = V_1 \oplus \cdots \oplus V_n. \tag{2.1}$$

Each V_i is an $E[T]$-submodule and as such has annihilator $(p_i^{e_i})$. More concretely, each V_i is g-stable and the minimal polynomial of g on V_i is $p_i^{e_i}$.

2.2 As g is invertible, the $E[T]$-module structure on V extends to a module structure over the ring of Laurent polynomials $E[T,T^{-1}]$. It follows that each V_i in (2.1) is an $E[T,T^{-1}]$-submodule. We have $\operatorname{ann}_{E[T,T^{-1}]} V = pE[T,T^{-1}]$ and $\operatorname{ann}_{E[T,T^{-1}]} V_i = p_i^{e_i}E[T,T^{-1}]$, $(i = 1,\dots,n)$. The inclusion $E[T] \subset E[T,T^{-1}]$ induces canonical E-algebra isomorphisms

$$E[T]/(p) \cong E[T,T^{-1}]/pE[T,T^{-1}] \quad \text{and} \quad E[T]/(p_i^{e_i}) \cong E[T,T^{-1}]/p_i^{e_i}E[T,T^{-1}],$$

for $(i = 1,\dots,n)$. We use these to identify $\mathcal{A}$ with $E[T,T^{-1}]/pE[T,T^{-1}]$ and each $\mathcal{A}_i$ with $E[T,T^{-1}]/p_i^{e_i}E[T,T^{-1}]$.

The F-automorphism τ of E extends to an involution $\sum_i a_i T^i \mapsto \sum_i \tau(a_i)\beta^i T^{-i}$ on $E[T,T^{-1}]$, which we continue to denote by τ. This satisfies the adjoint relation

$$\langle v, fw\rangle = \langle \tau(f)v, w\rangle, \quad \forall v,w \in V, \forall f \in E[T,T^{-1}]. \tag{2.2}$$

It follows that $\tau(pE[T,T^{-1}]) = p\,E[T,T^{-1}]$. Hence there is a $u \in E[T,T^{-1}]^\times$ such that $\tau(p) = up$ and thus τ induces an involution on $\mathcal{A}$.

Furthermore, for $i = 1,\dots,n$,

$$(1) \quad \tau(p_i) = u_i p_{i'} \text{ for } i' \neq i \qquad \text{or} \qquad (2) \quad \tau(p_i) = u_i p_i,$$

with each $u_i \in E[T,T^{-1}]^\times$. In case (a) τ induces an isomorphism $\mathcal{A}_i \cong \mathcal{A}_{i'}$ while in case (b) it induces an involution on $\mathcal{A}_i$.

By (2.2),

$$V_k \perp V_l \text{ unless } \tau(p_k) = up_l \text{ for some } u \in E[T,T^{-1}]^\times. \tag{2.3}$$

It follows that $V = W_1 \oplus \cdots \oplus W_m$, where for a given W_j, we have $W_j = V_i \oplus V_{i'}$ for some i and i' as in (1) above or $W_j = V_i$ with i as in (2). In particular, each W_j is an $E[T,T^{-1}]$-submodule and the restriction of $\langle\cdot,\cdot\rangle$ to each W_j is non-degenerate. Thus $g \in \mathrm{GU}(V)$ decomposes as $g = g_1 \oplus \cdots \oplus g_m$ with $g_j \in GU(W_j)$ for $j = 1,\dots,m$. It suffices to prove the result for each g_j. This means we are reduced to two basic cases.

Case 1. The minimal polynomial of g is $p_1^e p_2^e$ for some positive integer e and monic irreducible polynomials $p_1, p_2 \in E[T]$ such that $\tau(p_1) = up_2$ for some $u \in E[T,T^{-1}]^\times$. We have $\mathcal{A} = \mathcal{A}_1 \oplus \mathcal{A}_2$ with

$$\mathcal{A}_i = E[T]/(p_i^e) = E[T,T^{-1}]/\,p_i^e E[T,T^{-1}], \quad (i = 1,2).$$

The space V decomposes as $V = V_1 \oplus V_2$ where $V_i = \mathcal{A}_i V$ $(i = 1,2)$. Moreover, by (2.3), each V_i is a totally isotropic subspace of V.

Case 2. The minimal polynomial of g is p^e for some positive integer e and some monic irreducible element $p \in E[T]$ such that $\tau(p) = up$ for some $u \in E[T,T^{-1}]^\times$. In this case, $\mathcal{A} = E[T]/(p^e) = E[T,T^{-1}]/p^e E[T,T^{-1}]$.

3 Proof of Theorem A: Case 1

3.1 As $V = V_1 \oplus V_2$ is non-degenerate and each V_i is totally isotropic, it follows that $\langle\cdot,\cdot\rangle$ induces an isomorphism between V_1 and the conjugate dual of V_2. That is, if we write V_2^τ for the vector space structure on V_2 obtained by twisting by τ so that $V_2^\tau = V_2$ as abelian groups and scalar multiplication on V_2^τ is given by $a.v = \tau(a)v$ (for $a \in E$ and $v \in V_2$), then $v \mapsto \langle v, -\rangle \colon V_1 \to \mathrm{Hom}_E(V_2^\tau, \mathrm{E})$ is an isomorphism of E-vector spaces.

https://doi.org/10.4153/CMB-2017-046-0 Published online by Cambridge University Press

Let $e_1, \ldots, e_n$ be any basis of V_1. By the preceding paragraph, V_2 (or V_2^{τ}) admits a dual basis $f_1, \ldots, f_n$ such that

$$\langle e_i, f_j \rangle = \begin{cases} 1 & \text{if } i = j, \\ 0 & \text{if } i \neq j. \end{cases}$$

Thus, with respect to the basis $e_1, \ldots, e_n, f_1, \ldots, f_n$, the matrix of $\langle \cdot, \cdot \rangle$ is given in block form by

$$J = \begin{bmatrix} 0 & \epsilon I_n \\ I_n & 0 \end{bmatrix}.$$

For any matrix $a = [a_{ij}]$ with entries in E, we set $\tau(a) = [\tau(a_{ij})]$ and write ${}^{\top}a$ for the transpose of a. Below we often view E-linear maps on V as (block) matrices with respect to the basis $e_1, \ldots, e_n, f_1, \ldots, f_n$.

Consider the F-linear map $c: V \to V$ given by

$$\sum_{i=1}^{n} a_i e_i + \sum_{j=1}^{n} b_j f_j \overset{c}{\longmapsto} \sum_{i=1}^{n} \epsilon\tau(a_i) e_i + \sum_{j=1}^{n} \tau(b_j) f_j.$$

Setting $a = \begin{bmatrix} a_1 \\ \vdots \\ a_n \end{bmatrix}$ and $b = \begin{bmatrix} b_1 \\ \vdots \\ b_n \end{bmatrix}$, we can write c in matrix form as $\begin{bmatrix} a \\ b \end{bmatrix} \overset{c}{\mapsto} \begin{bmatrix} \epsilon\tau(a) \\ \tau(b) \end{bmatrix}$. The map c is anti-unitary (that is, $\langle c(v), c(v') \rangle = \langle v', v \rangle$, for all $v, v' \in V$) and $c^2 = 1$. Any anti-unitary $h_1 \in \mathrm{Aut}_F(V)$ can be written as $h_1 = s_1 c$ with $s_1 \in U(V)$. Now $h_1 = s_1 c$ is an involution if and only if $s_1 {}^c s_1 = 1$ where ${}^c s_1 = c s_1 c^{-1}$. Similarly, an anti-unitary similitude h_2 can be written as $h_2 = c s_2$ with $s_2 \in \mathrm{GU}(V)$. Again $h_2^2 = \beta$ if and only if $s_2 {}^c s_2 = \beta$ with ${}^c s_2 = c s_2 c^{-1}$. In this notation, we have $h_1 h_2 = s_1 s_2$ (as $c^2 = 1$). It follows that Theorem A in Case 1 is equivalent to the following:

(∗) if $g \in \mathrm{GU}(V)$ with $\mu(g) = \beta$ then $g = s_1 s_2$ for elements $s_1 \in U(V)$ and $s_2 \in \mathrm{GU}(V)$ such that $s_1 {}^c s_1 = 1$ and $s_2 {}^c s_2 = \beta$.

3.2 We now prove (∗). Since g preserves V_1 and V_2, we have $g = \begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix}$. The condition $g \in \mathrm{GU}(V)$ says ${}^{\top}g J \tau(g) = \beta J$ with $\beta = \mu(g)$. A short matrix calculation shows that this means $b = \beta {}^{\top}\tau(a)^{-1}$, so that

$$g = \begin{bmatrix} a & 0 \\ 0 & \beta {}^{\top}\tau(a)^{-1} \end{bmatrix}.$$

We set

$$s_1 = \begin{bmatrix} 0 & d_1 \\ \epsilon {}^{\top}\tau(d_1)^{-1} & 0 \end{bmatrix}, \quad s_2 = \begin{bmatrix} 0 & \epsilon\beta {}^{\top}\tau(d_2)^{-1} \\ d_2 & 0 \end{bmatrix},$$

for elements $d_1, d_2 \in \mathrm{GL}_n(E)$. It is routine to check that ${}^{\top}s_1 J \tau(s_1) = J$ and ${}^{\top}s_2 J \tau(s_2) = \beta J$. Thus $s_1 \in \mathrm{U}(V)$ and $s_2 \in \mathrm{GU}(V)$.

To calculate ${}^c s_1$, note that for all column vectors $\begin{bmatrix} x \\ y \end{bmatrix}$ as above, we have

$$\begin{bmatrix} x \\ y \end{bmatrix} \overset{c}{\longmapsto} \begin{bmatrix} \epsilon\tau(x) \\ \tau(y) \end{bmatrix} \overset{s_1}{\longmapsto} \begin{bmatrix} 0 & d_1 \\ \epsilon {}^{\top}\tau(d_1)^{-1} & 0 \end{bmatrix} \begin{bmatrix} \epsilon\tau(x) \\ \tau(y) \end{bmatrix}$$

$$= \begin{bmatrix} d_1 \tau(y) \\ {}^{\top}\tau(d_1)^{-1}\tau(x) \end{bmatrix} \overset{c}{\longmapsto} \begin{bmatrix} \epsilon\tau(d_1) y \\ {}^{\top}d_1^{-1} x \end{bmatrix} = \begin{bmatrix} 0 & \epsilon\tau(d_1) \\ {}^{\top}d_1^{-1} & 0 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix}.$$

https://doi.org/10.4153/CMB-2017-046-0 Published online by Cambridge University Press

That is,

$$^{c}s_1 = \begin{bmatrix} 0 & \epsilon\tau(d_1) \\ {}^{\top}d_1^{-1} & 0 \end{bmatrix} = \epsilon\tau(s_1).$$

A similar computation gives

$$^{c}s_2 = \begin{bmatrix} 0 & \beta^{\top}d_2^{-1} \\ \epsilon\tau(d_2) & 0 \end{bmatrix} = \epsilon\tau(s_2).$$

By direct matrix calculations, the conditions $s_1\,{}^{c}s_1 = 1$ and $s_2\,{}^{c}s_2 = \beta$ are equivalent to $d_1{}^{\top}d_1^{-1} = I_n$ and $d_2{}^{\top}d_2^{-1} = I_n$, *i.e.*, d_1 and d_2 are symmetric. Since $g = s_1 s_2$ is equivalent to $a = d_1 d_2$, we are reduced to the following matrix statement:

($*'$) For any (invertible) $n \times n$ matrix a (with entries in E), there exist (invertible) symmetric $n \times n$ matrices d_1 and d_2 (with entries in E) such that $a = d_1 d_2$.

Now any square matrix is conjugate by a symmetric matrix to its transpose [13, p. 76]. Thus $d^{-1}ad = {}^{\top}a$ with $d \in \mathrm{GL}_n(E)$ symmetric. This means $d^{-1}a = {}^{\top}ad^{-1}$, so ${}^{\top}(d^{-1}a) = {}^{\top}ad^{-1} = d^{-1}a$. Therefore $a = d \cdot d^{-1}a$ expresses a as product of symmetric matrices (with entries in E). This completes the proof of Theorem A in Case 1.

4 Proof of Theorem A: Case 2 and Second Reduction

In this case, the minimal polynomial of g is p^e (for some positive integer e) where p is irreducible and $\tau(p) = up$ for some $u \in E[T, T^{-1}]^{\times}$. Let $\mathcal{A} = E[T, T^{-1}]/p^e E[T, T^{-1}]$. As $\mathrm{ann}_{E[T,T^{-1}]}\, V = p^e E[T, T^{-1}]$, the space V is naturally an $\mathcal{A}$-module and as such is faithful, that is, $\mathrm{ann}_{\mathcal{A}}\, V = \{0\}$. Note that $\mathcal{A}$ is a local ring with unique maximal ideal $\mathfrak{p} = pE[T, T^{-1}]/p^e E[T, T^{-1}]$. More strongly, the ideals in $\mathcal{A}$ form a chain

$$\mathcal{A} \supsetneqq \mathfrak{p} \supsetneqq \cdots \supsetneqq \mathfrak{p}^{e-1} \supsetneqq \mathfrak{p}^e = \{0\}.$$

4.1 As $\mathrm{ann}_{\mathcal{A}}\, V = \{0\}$, there is some $v \in V$ such that $\mathrm{ann}_{\mathcal{A}}\, v = \{0\}$. Below we will need to consider the restriction of $\langle\cdot,\cdot\rangle$ to the submodule $\mathcal{A}v$ generated by such an element and will make use of the following non-degeneracy criterion.

Lemma 4.1 *Let $v \in V$ with $\mathrm{ann}_{\mathcal{A}}\, v = \{0\}$; equivalently, $\mathrm{ann}_{E[T,T^{-1}]}\, v = p^e E[T, T^{-1}]$. The cyclic submodule $\mathcal{A}v$ is non-degenerate if and only if $\langle \mathfrak{p}^{e-1}v, v\rangle \neq \{0\}$.*

Proof ($\Rightarrow$) Suppose $\mathcal{A}v$ is non-degenerate. By hypothesis, $p^{e-1}v \neq 0$. Thus there is an $f \in E[T, T^{-1}]$ such that $\langle p^{e-1}v, fv\rangle \neq 0$, so that $\langle \tau(f)p^{e-1}v, v\rangle \neq 0$ and hence $\langle \mathfrak{p}^{e-1}v, v\rangle \neq \{0\}$.

($\Leftarrow$) Suppose now that $\langle \mathfrak{p}^{e-1}v, v\rangle \neq \{0\}$. We write $\mathrm{rad}\, \mathcal{A}v$ for the radical of $\langle\cdot,\cdot\rangle$ on restriction to $\mathcal{A}v$. It is immediate that $\mathrm{rad}\,\mathcal{A}v$ is an $\mathcal{A}$-submodule. The map $a \mapsto av\colon \mathcal{A} \to \mathcal{A}v$ is an isomorphism of $\mathcal{A}$-modules. It follows that $\mathrm{rad}\,\mathcal{A}v = \mathfrak{p}^c v$ for some non-negative integer c (as the only ideals in $\mathcal{A}$ are the powers of $\mathfrak{p}$). Our assumption $\langle \mathfrak{p}^{e-1}v, v\rangle \neq \{0\}$ implies that $c > e-1$. Thus $\mathrm{rad}\,\mathcal{A}v = \{0\}$, that is, $\mathcal{A}v$ is non-degenerate. ∎

https://doi.org/10.4153/CMB-2017-046-0 Published online by Cambridge University Press

4.2 Let $x \in V$ with $\operatorname{ann}_{\mathcal{A}} x = \{0\}$ (equivalently, $\operatorname{ann}_{E[T,T^{-1}]} x = p^e E[T, T^{-1}]$) and set $X = \mathcal{A}x$. Now $p^{e-1}x \neq 0$, so there is a $y \in V$ with $\langle p^{e-1}x, y\rangle \neq 0$. It follows that $\operatorname{ann}_{\mathcal{A}} y = \{0\}$. Assume that the subspace X is degenerate, so that $y \notin X$ (by Lemma 4.1). Setting $Y = \mathcal{A}y$, we claim that if $X \cap Y \neq \{0\}$, then Y is non-degenerate.

To prove this, let $z \in X \cap Y$ with $z \neq 0$. We have $z = p^c gx = p^{c'} g' y$, for integers c and c' with $0 \leq c < e$, $0 \leq c' < e$ and elements $g, g' \in E[T]$ that are prime to p. Thus $\operatorname{ann}_{E[T]} z = (p^{e-c}) = (p^{e-c'})$ and so $c = c'$.

Now there are elements $a, b \in E[T]$ such that $ag + bp^e = 1$. Hence

$$p^{e-c-1}az = p^{e-c-1}a(p^c gx) = p^{e-1}agx = p^{e-1}(1 - bp^e)x = p^{e-1}x \quad (\text{as} \quad p^e x = 0).$$

In addition, $p^{e-c-1}az = p^{e-c-1}a(p^c g' y) = p^{e-1}ag' y$, so that $p^{e-1}x = p^{e-1}ag' y$. As $\langle p^{e-1}x, y\rangle \neq 0$, it follows that $\langle p^{e-1}ag' y, y\rangle \neq 0$. Therefore $\langle \mathfrak{p}^{e-1}y, y\rangle \neq \{0\}$. Hence, by Lemma 4.1, $Y = \mathcal{A}y$ is non-degenerate.

4.3 We now show that if V does not admit a non-degenerate cyclic submodule (generated by an element v such that $\operatorname{ann}_{\mathcal{A}} v = \{0\}$), then it must contain a non-degenerate non-cyclic submodule of a very special kind.

Lemma 4.2 *Suppose that for any $v \in V$ such that $\operatorname{ann}_{\mathcal{A}} v = \{0\}$ the submodule $\mathcal{A}v$ is degenerate. Then there exist x and y in V such that $\langle \mathfrak{p}^{e-1}x, y\rangle \neq \{0\}$. We have $\mathcal{A}x \cap \mathcal{A}y = \{0\}$ and the submodule $\mathcal{A}x \oplus \mathcal{A}y$ is non-degenerate.*

Proof As in Section 4.2, we choose x and y in V such that $\operatorname{ann}_{\mathcal{A}} x = \{0\}$ and $\langle p^{e-1}x, y\rangle \neq 0$. We again set $X = \mathcal{A}x$ and $Y = \mathcal{A}y$. By hypothesis, X and Y are degenerate, so Lemma 4.1 gives $\langle \mathfrak{p}^{e-1}x, x\rangle = \langle \mathfrak{p}^{e-1}y, y\rangle = \{0\}$. Further, by the argument in Section 4.2, $X \cap Y = \{0\}$. We need to show that $X \oplus Y$ is non-degenerate.

Any non-zero element $z \in X \oplus Y$ can be written as $z = p^c gx + p^{c'} g' y$ for integers c and c' with $0 \leq c < e$, $0 \leq c' < e$, and elements $g, g' \in E[T]$ that are prime to p. Switching the roles of x and y if necessary, we may assume that $c' \leq c$.

To prove non-degeneracy of $X \oplus Y$, we will show that $\langle \mathfrak{p}^{e-c-1}x, z\rangle \neq \{0\}$. Writing $\overline{f}$ for the image of $f \in E[T, T^{-1}]$ under the canonical quotient map from $E[T, T^{-1}]$ to $\mathcal{A} = E[T, T^{-1}]/p^e E[T, T^{-1}]$, we have $\langle \mathfrak{p}^{e-c-1}x, z\rangle = \langle \mathfrak{p}^{e-c-1}x, \overline{p}^c \overline{g}x + \overline{p}^{c'} \overline{g}' y\rangle$. Now $\overline{p}^c \mathfrak{p}^{e-c-1} = \mathfrak{p}^{e-1}$ and $\overline{g} \in \mathcal{A}^\times$, so $\langle \mathfrak{p}^{e-c-1}x, \overline{p}^c \overline{g}x\rangle = \langle \mathfrak{p}^{e-1}x, x\rangle = \{0\}$. Thus

$$\begin{aligned} \langle \mathfrak{p}^{e-c-1}x, z\rangle &= \langle \mathfrak{p}^{e-c-1}x, \overline{p}^{c'} \overline{g}' y\rangle = \langle \mathfrak{p}^{e-c+c'-1}x, y\rangle \quad (\text{using } \overline{g}' \in \mathcal{A}^\times) \\ &\supset \langle \mathfrak{p}^{e-1}x, y\rangle \quad (\text{as } c' \leq c, \text{ so } e - c + c' - 1 \leq e - 1) \\ &\neq \{0\}. \end{aligned}$$

In particular, $\langle \mathfrak{p}^{e-c-1}x, z\rangle \neq \{0\}$, as claimed. ∎

4.4 We have established that V contains an $\mathcal{A}$-submodule of one of the following types:

(a) a non-degenerate $\mathcal{A}$-submodule $\mathcal{A}v$ with $\operatorname{ann}_{\mathcal{A}} v = \{0\}$;
(b) a non-degenerate $\mathcal{A}$-submodule as in Lemma 4.2.

Now if W is any non-degenerate $\mathcal{A}$-submodule of V, then $V = W \oplus W^\perp$ as $\mathcal{A}$-modules. Moreover, $\operatorname{ann}_{\mathcal{A}} W^\perp = \mathfrak{p}^c$ for some non-negative integer $c \leq e$. If Theorem A holds

https://doi.org/10.4153/CMB-2017-046-0 Published online by Cambridge University Press

for W and $W^\perp$, then it also holds for V. Thus we can complete the proof in Case 2 by induction on $\dim_E V$ provided we can establish the result in the two special cases (a) and (b).

5 Proof of Theorem A: Case 2(a)

5.1 This is the cyclic case in which $V = \mathcal{A}v$ with $\operatorname{ann}_{\mathcal{A}} v = \{0\}$. That is, the map

$$a \mapsto av: \mathcal{A} \to V \tag{5.1}$$

is an isomorphism of $\mathcal{A}$-modules. We will show that there is an anti-unitary involution $t: V \to V$ such that, for all $a \in \mathcal{A}$,

$$ta = \tau(a)t \tag{5.2}$$

as elements of $\operatorname{End}_F V$. Now the element $T \in E[T]$, and so also its image in $\mathcal{A}$, acts on V via $g \in \mathrm{GU}(V)$. Thus if we take a to be the image of T in $\mathcal{A}$, then (5.2) gives $tg = \beta g^{-1} t$, or $(tg)^2 = \beta$. Hence $g = t \cdot tg$ gives the requisite factorization.

5.2 To establish (5.2), we define $t: V \to V$ by $t(av) = \tau(a)v$, for all $a \in \mathcal{A}$. Thus t is simply the involution τ of $\mathcal{A}$ transported to V via the isomorphism (5.1). It is therefore immediate that t is an involution and that (5.2) holds. To check that t is anti-unitary, let $a, b \in \mathcal{A}$. By (2.2), $\langle t(av), t(bv)\rangle = \langle \tau(a)v, \tau(b)v\rangle = \langle b\tau(a)v, v\rangle = \langle bv, av\rangle$.

6 Proof of Theorem A: Case 2(b)

We have $V = \mathcal{A}x \oplus \mathcal{A}y$ with $\langle \mathfrak{p}^{e-1}x, y\rangle \neq \{0\}$. Further, $\mathcal{A}x$ and $\mathcal{A}y$ are both degenerate, so Lemma 4.1 gives $\langle \mathfrak{p}^{e-1}x, x\rangle = \langle \mathfrak{p}^{e-1}y, y\rangle = \{0\}$. This case requires a more elaborate argument.

6.1 We observe first that the subspaces $\mathcal{A}x$ and $\mathcal{A}y$ are in duality via $\langle\cdot,\cdot\rangle$. That is, the map

$$ay \longmapsto (a'x \longmapsto \langle a'x, ay\rangle): \mathcal{A}y \longrightarrow \operatorname{Hom}_E(\mathcal{A}x, E) \tag{6.1}$$

is a bijection. More precisely, if as in Section 3.1 we write $(\mathcal{A}y)^\tau$ for the E-vector space structure on $\mathcal{A}y$ obtained by twisting by τ, then (6.1) is an isomorphism of E-vector spaces between $(\mathcal{A}y)^\tau$ and $\operatorname{Hom}_E(\mathcal{A}x, E)$.

To prove this, note that the kernel of the given map is an $\mathcal{A}$-submodule and so equals $\mathfrak{p}^c y$ for some non-negative integer c. Now $\langle \mathfrak{p}^{e-1}x, y\rangle \neq \{0\}$ and hence $c > e-1$. As $\mathfrak{p}^e = \{0\}$, the kernel must be trivial and thus (6.1) is injective. Since $\dim_E \mathcal{A}x = \dim_E \mathcal{A}y (= \dim_E \mathcal{A})$, the map is also surjective.

6.2 The map $ax \mapsto \langle y, \tau(a)x\rangle = \langle ay, x\rangle$ belongs to $\operatorname{Hom}_E(\mathcal{A}x, E)$. Thus by Section 6.1, there is a unique $\gamma \in \mathcal{A}$ such that

$$\langle ay, x\rangle = \langle ax, \gamma y\rangle, \quad \forall a \in \mathcal{A}. \tag{6.2}$$

We claim that $\gamma \in \mathcal{A}^\times$. Indeed, $\langle \mathfrak{p}^{e-1}x, y\rangle \neq \{0\}$ and $\tau(\mathfrak{p}) = \mathfrak{p}$, so $\langle \mathfrak{p}^{e-1}y, x\rangle \neq \{0\}$. It follows that $\langle \mathfrak{p}^{e-1}x, \gamma y\rangle \neq \{0\}$, or equivalently $\langle \tau(\gamma)\mathfrak{p}^{e-1}x, y\rangle \neq \{0\}$. As $\mathfrak{p}^e = \{0\}$, we see that $\tau(\gamma) \notin \mathfrak{p}$. Therefore $\tau(\gamma) \in \mathcal{A}^\times$, whence also $\gamma \in \mathcal{A}^\times$.

6.3 We claim next that $\gamma\tau(\gamma) = 1$. Rewriting (6.2) as $\langle x, a\gamma y\rangle = \langle y, ax\rangle$, we have

$$\begin{aligned}\langle x, a\gamma y\rangle &= \epsilon\tau(\langle ax, y\rangle) = \epsilon\tau(\langle ax, \gamma^{-1}\gamma y\rangle) = \epsilon\tau(\langle \tau(\gamma^{-1})ax, \gamma y)\\ &= \epsilon\tau(\langle \tau(\gamma^{-1}ay, x\rangle) \quad \text{(by (6.2))}\\ &= \langle x, \tau(\gamma^{-1})ay\rangle, \quad \forall a \in \mathcal{A}.\end{aligned}$$

It follows that $\langle ax, \gamma y\rangle = \langle ax, \tau(\gamma^{-1})y\rangle$, for all $a \in \mathcal{A}$. By bijectivity of (6.1), $\tau(\gamma^{-1})y = \gamma y$, whence $\tau(\gamma^{-1}) = \gamma$, that is, $\gamma\tau(\gamma) = 1$.

6.4 Define $t: \mathcal{A}x \oplus \mathcal{A}y \to \mathcal{A}x \oplus \mathcal{A}y$ by $t(ax + by) = \tau(a)x + \tau(b)\gamma y$, for all $a, b \in \mathcal{A}$. We claim that t is an anti-unitary involution such that, for all $a \in \mathcal{A}$,

$$ta = \tau(a)t \tag{6.3}$$

as elements of $\mathrm{End}_F(\mathcal{A}x \oplus \mathcal{A}y)$. Once this is established, we can complete the argument exactly as in Section 5. That is, $(tg)^2 = \beta$, and thus as above $g = t \cdot tg$ gives the requisite factorization.

Applying t twice, we obtain

$$\begin{aligned}ax + by &\xmapsto{t} \tau(a)x + \tau(b)\gamma y\\ &\xmapsto{t} ax + b\tau(\gamma)\gamma y = ax + by \quad (\text{as } \tau(\gamma)\gamma = 1),\end{aligned}$$

and so t is an involution.

The identity (6.3) is immediate. In detail, for all $a, a', b' \in \mathcal{A}$,

$$\begin{aligned}ta(a'x + b'y) &= t(aa'x + ab'y) = \tau(a)\tau(a')x + \tau(a)\tau(b')\gamma y\\ &= \tau(a)t(a'x + b'y).\end{aligned}$$

Finally, to show that t is anti-unitary, it suffices to verify the following four identities (for all $a, b \in \mathcal{A}$):

$$\langle t(ax), t(bx)\rangle = \langle bx, ax\rangle; \tag{6.4}$$

$$\langle t(ay), t(by)\rangle = \langle by, ay\rangle; \tag{6.5}$$

$$\langle t(ax), t(by)\rangle = \langle by, ax\rangle; \tag{6.6}$$

$$\langle t(by), t(ax)\rangle = \langle ax, by\rangle. \tag{6.7}$$

Applying τ to both sides of (6.6) gives (6.7), so it is enough to check (6.4)–(6.6). We can verify (6.4) directly as in Section 5.2. The argument for (6.5) is similarly straightforward using $\gamma\tau(\gamma) = 1$. To check (6.6), note

$$\begin{aligned}\langle t(ax), t(by)\rangle &= \langle \tau(a)x, \tau(b)\gamma y\rangle = \langle b\tau(a)x, \gamma y\rangle = \langle b\tau(a)y, x\rangle \quad \text{(using (6.2))}\\ &= \langle by, ax\rangle.\end{aligned}$$

This completes the proof of Case 2(b) and so concludes the proof of Theorem A. ■

7 Some Examples and Applications

7.1 Suppose that $E = F$ and $\epsilon = -1$, so that $\mathrm{U}(V) = \mathrm{Sp}(V)$ and $\mathrm{GU}(V) = \mathrm{GSp}(V)$. Assume also that $\mathrm{char}(F) \neq 2$. As noted in the introduction, Wonenburger [26] proved Theorem A for the symplectic group $\mathrm{Sp}(V)$ and the case of the similitude

https://doi.org/10.4153/CMB-2017-046-0 Published online by Cambridge University Press

group $\mathrm{GSp}(V)$ was treated in [24]. Assume now that $\mathrm{char}(F) = 2$. Then the case of symplectic groups was proved by Gow [9] and Ellers and Nolte [7]. If F is perfect, the similitude case follows readily (as every element of F is a square). The similitude case for $\mathrm{char}(F) = 2$ and F imperfect appears to be new.

7.2 Suppose now that $[E:F] = 2$ and $\epsilon = 1$. Let $V = E^n$ and view the elements of V as column vectors. Consider the non-degenerate hermitian form $\langle \cdot, \cdot \rangle$ on V given by $\langle x, y \rangle = {}^{\top}x\tau(y)$. Here, as in Section 2.1, $\tau(y)$ is obtained by applying the automorphism τ to each coordinate of y. Similarly, for any matrix $a = [a_{ij}]$ with entries in E, we set $\tau(a) = [\tau(a_{ij})]$. We write $\mathrm{U}(n)$ for the isometry group of $\langle \cdot, \cdot \rangle$. Thus

$$\mathrm{U}(n) = \{g \in \mathrm{GL}_n(E) : {}^{\top}g\, \tau(g) = 1\}.$$

The map $x \overset{c}{\mapsto} \tau(x)\colon V \to V$ is an anti-unitary involution for $\langle \cdot, \cdot \rangle$. For any $a \in M_n(E)$ (viewed as an E-linear map on V via left multiplication), we have ${}^{c}a = cac^{-1} = \tau(a)$. The calculation that gave $(*)$ of Section 2.1 shows that Theorem A for $\mathrm{U}(n)$ is equivalent to the statement:

$(**)$ if $g \in \mathrm{U}(n)$, then $g = s_1 s_2$ for elements $s_i \in \mathrm{U}(V)$ such that $s_i\, {}^{c}s_i = 1$ for $i = 1, 2$.

From $s_i\, {}^{c}s_i = 1$ and $s_i \in \mathrm{U}(n)$, we see that $s_i^{-1} = {}^{c}s_i = \tau(s_i) = {}^{\top}s_i^{-1}$. Thus each $s_i \in \mathrm{U}(n)$ is symmetric as an element of $\mathrm{GL}_n(E)$. Hence ${}^{\top}g = {}^{\top}s_2 {}^{\top}s_1 = s_2 s_1$ and $s_1^{-1} g\, s_1 = {}^{\top}g$. In particular, we obtain the following unitary group version of a classical result in linear algebra (used in Section 3.2) that any matrix is conjugate to its transpose by a symmetric matrix.

Corollary 7.1 *For any $g \in \mathrm{U}(n)$, there exists a symmetric matrix $s \in \mathrm{U}(n)$ such that $sgs^{-1} = {}^{\top}g$.*

When $E/F = \mathbb{C}/\mathbb{R}$, Corollary 7.1 follows immediately from the fact that any unitary matrix is unitarily diagonalizable. In the case that E/F is an extension of finite fields, Corollary 7.1 was proved in [10, Lemma 5.2].

7.3 Let $E = F = \mathbb{F}_q$ be a finite field with q elements with q odd and let $\epsilon = 1$, so that $\mathrm{GU}(V)$ is a finite group of orthogonal similitudes. We restrict attention to the case that $\dim(V) = 2m$ is even. In this setting there are two equivalence classes of non-degenerate symmetric forms on V, giving two distinct finite orthogonal similitude groups. We denote these groups by $\mathrm{GO}^{\pm}(2m, \mathbb{F}_q)$, and write $\mathrm{O}^{\pm}(2m, \mathbb{F}_q)$ for the corresponding orthogonal groups. For $\mathrm{U}(V) = \mathrm{O}^{\pm}(2m, \mathbb{F}_q)$, the element h_1 in Theorem A can be chosen so that $\det(h_1) = (-1)^m$ (see [21, Lemma 4.7]). For use in later work, we now extend this observation to the case $\mathrm{GU}(V) = \mathrm{GO}^{\pm}(2m, \mathbb{F}_q)$.

Proposition 7.2 *Let $G = \mathrm{GO}^{\pm}(2m, \mathbb{F}_q)$ with q odd and let $g \in G$ with $\mu(g) = \beta$. Then there exist $h_1, h_2 \in G$ such that $g = h_1 h_2$, $\mu(h_1) = 1$, $\mu(h_2) = \beta$, $h_1^2 = 1$, $h_2^2 = \beta$, and $\det(h_1) = (-1)^m$.*

Proof The case $\mu(g) = 1$ follows from [21, Lemma 4.7]. If $\mu(g) = \beta$ is a square in $\mathbb{F}_q$, say $\beta = \gamma^2$, then $g' = \gamma^{-1} g$ satisfies $\mu(g') = 1$, so we may write $g' = h_1 h'$ with h_1 and

https://doi.org/10.4153/CMB-2017-046-0 Published online by Cambridge University Press

h' orthogonal involutions, and $\det(h_1) = (-1)^m$. We set $h_2 = \gamma h'$, so that $g = h_1 h_2$ satisfies the desired conditions.

We now assume that $\mu(g) = \beta$ with β a non-square in $\mathbb{F}_q$ and proceed by considering Cases 1, 2(a), and 2(b) in the proof of Theorem A. In Case 1, we have $V = V_1 \oplus V_2$ where $\dim(V_1) = \dim(V_2) = m$. In this scenario, we have $E = F$ and $\epsilon = 1$, and in Section 2.2, the element s_1 satisfies $\det(s_1) = (-1)^m$ since d_1 is symmetric. Taking $s_1 = h_1$ and $s_2 = h_2$ gives the desired factorization.

In Case 2, we use Shinoda's description of conjugacy classes in $\mathrm{GO}^{\pm}(2m, \mathbb{F}_q)$ [22, §1]. In particular, Shinoda shows that Case 2(b) occurs if and only if the minimal polynomial $p(T)^e$ of g on V has the form $(T^2 - \beta)^e$ with $e = 2k - 1$ an odd positive integer [22, (1.18.2)]. Note that Wonenburger [26, Remark I] mentions the parallel exceptions in her setting, which occur in the case $\beta = 1$.

We now apply some calculations made in [24, 25]. Consider first Case 2(a), where we have $V = \mathcal{A}v$ is cyclic, and the minimal polynomial for g on V is of the form $p(T)^e$ but not of the form $(T^2 - \beta)^{2k-1}$. In particular, it follows from the fact that $\tau(p) = up$ for some $u \in F[T, T^{-1}]^\times$ that $p(T)$ has even degree. We set $2m = e \deg(p) = \dim(V)$ and define

$$P = \mathrm{span}\{(g^i + \beta^i g^{-i})v \mid 0 \le i < m\},$$
$$Q = \mathrm{span}\{(g^i - \beta^i g^{-i})v \mid 0 < i \le m\}.$$

In [24, Proposition 3(i)] and in [25, Theorem 1], it was shown that $V = P \oplus Q$, and if we define h_1 to have $+1$-eigenspace P and -1-eigenspace Q and $h_2 = h_1 g$, then we have $h_1, h_2 \in G$ with $\mu(h_1) = 1$, $\mu(h_2) = \beta$, $h_1^2 = 1$, and $h_2^2 = \beta$. Since $\dim(Q) = (-1)^m = \det(h_1)$, this gives the desired factorization.

Finally, consider Case 2(b), where we have $V = \mathcal{A}x \oplus \mathcal{A}y$, and as mentioned above, the minimal polynomial for g must be of the form $(T^2 - \beta)^{2k-1}$. In this case, we have $\dim(V) = 2m$ where $m = 4k - 2$. Define

$$P_x = \mathrm{span}\{(g^i + \beta^i g^{-i})x \mid 0 \le i \le 2k - 1\},$$
$$Q_x = \mathrm{span}\{(g^i - \beta^i g^{-i})x \mid 0 < i < 2k - 1\},$$

and define P_y and Q_y analogously. Vinroot [24, Proposition 3 (i), (iii)], [25, Theorem 1] showed that if $P = P_x \oplus Q_y$ and $Q = Q_x \oplus P_y$, and we define h_1 to have $+1$-eigenspace P and -1-eigenspace Q and $h_2 = h_1 g$, then we again have $h_1, h_2 \in G$ with $\mu(h_1) = 1$, $\mu(h_2) = \beta$, $h_1^2 = 1$, and $h_2^2 = \beta$. Since $\dim(P_y) = 2k$ and $\dim(Q_x) = 2k - 2$, then $\dim(Q) = 4k - 2 = m$, so $\det(h_1) = (-1)^m$. ∎

8 Proof of Theorem B

For the remainder of the paper, we take F to be a non-Archimedean local field. Recall that $h \in \mathrm{Aut}_F(V)$ is an anti-unitary involution and that ${}^\iota g = \mu(g)^{-1} h g h^{-1}$ for $g \in \mathrm{GU}(V)$. Thus ι is a continuous automorphism of $\mathrm{GU}(V)$ of order two. The restriction $\iota|_{\mathrm{U}(V)}$ gives the automorphism $g \mapsto hgh^{-1}$ of $\mathrm{U}(V)$, which we again denote by ι. We restate our main result.

Theorem B *The maps* $\iota\colon \mathrm{U}(V) \to \mathrm{U}(V)$ *and* $\iota\colon \mathrm{GU}(V) \to \mathrm{GU}(V)$ *are dualizing involutions.*

We recall some character theory in Section 8.1. Using this, we will see in Section 8.2 that Theorem B follows almost immediately from Theorem A.

8.1 Let G be the F-points of a reductive algebraic F-group. As usual, we write $C_c^\infty(G)$ for the space of complex-valued functions on G that are locally constant and of compact support. Let (π, V) be a smooth representation of G. For $f \in C_c^\infty(G)$, the operator $\pi(f)\colon V \to V$ is given by $\pi(f)v = \int_G f(g)\pi(g)v\,dg$, $v \in V$, where the integral is with respect to a Haar measure on G which we fix once and for all. Assume now that (π, V) is irreducible. It is well known that (π, V) is then *admissible* [12], that is, the space V^K of K-fixed vectors has finite dimension for any open subgroup K of G. It follows that the image of $\pi(f)$ has finite dimension and thus $\pi(f)$ has a well-defined trace. The resulting linear functional $f \mapsto \mathrm{tr}\pi(f)\colon C_c^\infty(G) \to \mathbb{C}$ is called the *distribution character* of π. It determines the irreducible representation π up to equivalence [4, 2.20].

It is straightforward to check that $\mathrm{tr}\pi^\vee(f) = \mathrm{tr}\pi(f^\vee)$ where $f^\vee(g) = f(g^{-1})$ for $g \in G$.

Let G_{reg} denote the set of regular semisimple elements in G. By [3, 11], the distribution character of π is represented by a locally constant function Θ_π on G_{reg} called the *character* of π. That is,

$$\mathrm{tr}\pi(f) = \int_G f(g)\Theta_\pi(g)\,dg, \quad f \in C_c^\infty(G). \tag{8.1}$$

Remark. Existence of Θ_π is established in [11] for the F-points of arbitrary connected reductive F-groups based on the submersion principle of its title. Harish-Chandra, however, only gave a proof of the principle in characteristic zero with a comment that a general proof was known. A full proof, due to G. Prasad, appears in [2, Appendix B]. Adler and Korman explained how to extend Harish-Chandra's and Prasad's arguments to the F-points of non-connected reductive F-groups [3, §13]. A similarly general treatment of characters appears in [5, Appendix].

By (8.1), the function Θ_π determines the distribution character of π and thus π is determined up to equivalence by Θ_π. In the same way, Θ_π is constant on (regular semisimple) conjugacy classes. From $\mathrm{tr}\pi^\vee(f) = \mathrm{tr}\pi(f^\vee)$ for $f \in C_c^\infty(G)$, we also have $\Theta_{\pi^\vee}(g) = \Theta_\pi(g^{-1})$ for $g \in G_{\mathrm{reg}}$, again by (8.1).

8.2 Given a smooth representation π of G and a continuous automorphism α of G, we write π^α for the smooth representation given by $\pi^\alpha(g) = \pi({}^\alpha g)$ for $g \in G$.

For any $g \in \mathrm{GU}(V)$, we noted in the introduction that the elements ${}^\iota g$ and g^{-1} are conjugate by an element of $\mathrm{U}(V)$. To prove Theorem B, it suffices therefore to observe the following.

Lemma 8.1 *Let* α *be a continuous automorphism of* G *such that* ${}^a g$ *is conjugate to* g^{-1} *for any* $g \in G$. *Then* $\pi^\alpha \cong \pi^\vee$ *for any irreducible smooth representation* π *of* G.

Proof The main detail to check is that a continuous automorphism γ of G preserves the Haar measure μ_G on G. We have $\mu_G \circ \gamma = c_\gamma \mu_G$ for some $c_\gamma > 0$. Writing $\mathrm{Aut_c}(G)$ for the group of continuous automorphisms of G and $\mathbb{R}^\times_{\mathrm{pos}}$ for the multiplicative group of positive real numbers, the assignment $\gamma \mapsto c_\gamma \colon \mathrm{Aut_c}(G) \to \mathbb{R}^\times_{\mathrm{pos}}$ is a homomorphism. Let K be a compact subgroup of G of maximal volume. (Note K exists as G has a finite non-zero number of conjugacy classes of maximal compact subgroups.) For any $\gamma \in \mathrm{Aut_c}(G)$, we have $\mu_G(\gamma(K)) = c_\gamma \mu_G(K)$, so that $c_\gamma \le 1$. Similarly $c_{\gamma^{-1}} = c_\gamma^{-1} \le 1$. Hence $c_\gamma = 1$, as required.

In particular, α preserves the Haar measure on G. Thus, for any irreducible smooth representation π of G,

$$\pi^\alpha(f) = \int_G f(g)\,\pi({}^\alpha g)\,dg = \int_G f({}^{\alpha^{-1}}g)\pi(g)\,dg, \quad f \in C_c^\infty(G).$$

That is, $\pi^\alpha(f) = \pi({}^\alpha f)$ for $f \in C_c^\infty(G)$ where ${}^\alpha f(g) = f({}^{\alpha^{-1}}g)$. It follows that $\mathrm{tr}\pi^\alpha(f) = \mathrm{tr}\pi({}^\alpha f)$, so that

$$\begin{aligned}\int_G f(g)\Theta_{\pi^\alpha}(g)\,dg &= \int_G f({}^{\alpha^{-1}}g)\Theta_\pi(g)\,dg\\ &= \int_G f(g)\Theta_\pi({}^\alpha g)\,dg, \quad \forall f \in C_c^\infty(G).\end{aligned}$$

Therefore, $\Theta_{\pi^\alpha}(g) = \Theta_\pi({}^\alpha g)$ for $g \in G_{\mathrm{reg}}$. As characters are constant on conjugacy classes, it follows that $\Theta_{\pi^\alpha}(g) = \Theta_\pi(g^{-1})$ for $g \in G_{\mathrm{reg}}$. Thus $\Theta_{\pi^\alpha} = \Theta_{\pi^\vee}$ and $\pi^\alpha \cong \pi^\vee$. ■

8.3 We record a direct consequence of Theorem B, known to experts [17, p. 305]. Suppose $E = F$, so that $\langle\cdot,\cdot\rangle$ is orthogonal or symplectic. We change notation slightly and write $\mathrm{O}(V)$ and $\mathrm{GO}(V)$ or $\mathrm{Sp}_{2n}(F)$ and $\mathrm{GSp}_{2n}(F)$ (where $\dim_F V = 2n$) for the resulting isometry and similitude groups. The center of each similitude group consists of scalar transformations. Dividing by this center gives the corresponding projective groups $\mathrm{PGO}(V)$ and $\mathrm{PGSp}_{2n}(F)$.

Corollary 8.2 (i) *Every irreducible smooth representation of* $\mathrm{O(V)}$ *is self-dual.*

(ii) *If* $-1 \in (F^\times)^2$*, then every irreducible smooth representation of* $\mathrm{Sp}_{2n}(F)$ *is self-dual.*

(iii) *For any irreducible smooth representation* π *of* $\mathrm{GO(V)}$ *or* $\mathrm{GSp}_{2n}(F)$*, we have* $\pi^\vee \cong \pi \otimes \omega_\pi \circ \mu^{-1}$ *where* ω_π *denotes the central character of* π*. In particular, every irreducible smooth representation of* $\mathrm{PGO(V)}$ *or* $\mathrm{PGSp}_{2n}(F)$ *is self-dual.*

Proof Part (i) is immediate as $h \in \mathrm{O}(V)$, so $\iota\colon \mathrm{O}(V) \to \mathrm{O}(V)$ is inner.

For part (ii), it suffices to note that $\iota(g) = hgh^{-1}$ defines an inner automorphism of $\mathrm{Sp}_{2n}(F)$ for any $h \in \mathrm{GSp}_{2n}(F)$ with $\mu(h) = -1$. Given $i \in F^\times$ with $i^2 = -1$, the homothety i satisfies $\mu(i) = i^2 = -1$ and thus $ih \in \mathrm{Sp}_{2n}(F)$. Since ${}^\iota g = (ih)g(ih)^{-1}$ for $g \in \mathrm{Sp}_{2n}(F)$, we see that ι is inner.

For part (iii), observe that $g \mapsto \mu(g)^{-1}g$ defines a dualizing involution of each similitude group. ■

https://doi.org/10.4153/CMB-2017-046-0 Published online by Cambridge University Press

9 Dualizing Involutions Do Not Always Exist

Let D be a central F-division algebra of dimension m^2 over F. Let n be a positive integer and set $G = \mathrm{GL}_n(D)$. We show that G can admit an automorphism that takes each irreducible smooth representation to its dual only in the known cases $m = 1$ [8, 23] and $m = 2$ [16, 18]. Hence it is only in these two cases that G can admit an automorphism θ such that ${}^{\theta}g$ is conjugate to g^{-1} for all $g \in G$, an observation also made by Lin, Sun, and Tan [14, Remark (c) p. 83]). Indeed, the two statements — non-existence of automorphisms that take each irreducible smooth representation to its dual and non-existence of automorphisms that invert each conjugacy class — must surely be equivalent.

Proposition 9.1 *Suppose there exists an automorphism θ of G such that $\pi^{\theta} \simeq \pi^{\vee}$ for all irreducible smooth representations π of G. Then $D = F$ or D is a quaternion algebra over F (equivalently, $m = 1$ or 2).*

We need a preliminary observation. Let $\mathfrak{o}_F$ denote the valuation ring in F and $\mathfrak{p}_F$ the unique maximal ideal in $\mathfrak{o}_F$.

Lemma 9.2 *Any field automorphism of F preserves $\mathfrak{p}_F$. In particular, field automorphisms of F are automatically continuous.*

Proof Write q for the cardinality of the residue field $\mathfrak{o}_F/\mathfrak{p}_F$ and ν_F for the normalized valuation on F. The ideals $\mathfrak{p}_F^k$ (for k a positive integer) form a neighborhood basis of $0 \in F$. Thus an automorphism that preserves $\mathfrak{p}_F$ is continuous.

Writing p for the residual characteristic of F, the set $1 + \mathfrak{p}_F$ can be characterized algebraically as follows:

$x \in 1 + \mathfrak{p}_F$ if and only if x admits an n-th root (i.e., there is a $y \in F^{\times}$ with $y^n = x$) for any n such that $p \nmid n$.

Indeed, using Hensel's Lemma or simply that $1+\mathfrak{p}_F$ is a pro-p-group, one sees that each element of $1+\mathfrak{p}_F$ admits an n-th root for any n such that $p \nmid n$. In the other direction, suppose x has this property. Then n divides $\nu_F(x)$ for infinitely many integers n, whence $\nu_F(x) = 0$, *i.e.*, $x \in \mathfrak{o}_F^{\times}$. Let y be a $(q-1)$-th root of x. Then $y \in \mathfrak{o}_F^{\times}$ and the relation $y^{q-1} = x$ implies $x \in 1 + \mathfrak{p}_F$. It follows that any field automorphism of F preserves $1 + \mathfrak{p}_F$ and so also $\mathfrak{p}_F$. ∎

Proof of Proposition 9.1 We use the isomorphism $x \mapsto x1_n : F^{\times} \to Z(G)$ to view the central character ω_π of any smooth irreducible representation π of G as a smooth character of $F^{\times}$.

Suppose first that D is not isomorphic to its opposite D°. We appeal to Dieudonné's description of the automorphism groups of general linear groups over division algebras [6]. In the case at hand, this gives a homomorphism $\eta : G \to F^{\times}$, an automorphism σ of D acting on G via ${}^{\sigma}(a_{ij}) = ({}^{\sigma}a_{ij})$, and an element $h \in G$ such that

$$ {}^{\theta}g = \eta(g) h\, {}^{\sigma}g h^{-1}, \quad g \in G. \tag{9.1}$$

(See [6, Theorems 1 and 3] for the case $n \geq 3$ and [6, §12] for the case $n = 2$.)

https://doi.org/10.4153/CMB-2017-046-0 Published online by Cambridge University Press

As $\pi^\theta \simeq \pi^\vee$, we have $\omega_\pi \circ \theta = \omega_\pi^{-1}$ (for all smooth irreducible representations π). It follows that ${}^\theta a = a^{-1}$, $a \in F^\times$. Thus, by (9.1), $a^{-1} = \eta(a)\, {}^\sigma a$, $a \in F^\times$.

We have $G/(G,G) \simeq D^\times/(D^\times, D^\times)$ via Dieudonné's non-commutative determinant Det. Furthermore, the reduced norm Nrd from D to F induces an isomorphism $D^\times/(D^\times, D^\times) \simeq F^\times$. Thus there is a character $\eta_1\colon F^\times \to F^\times$ such that $\eta(g) = \eta_1(\mathrm{Nrd} \circ \mathrm{Det}\, g)$, for $g \in G$. Using $\mathrm{Det}\, a = a^n(D^\times, D^\times)$ and $\mathrm{Nrd}\, a = a^m$, it follows that $a^{-1} = \eta_1(a)^{mn\sigma} a$, $a \in F^\times$. Taking $a = \varpi$, a uniformizer in F, and applying ν_F, we obtain $-1 = mn\nu_F(\eta_1(\varpi)) + \nu_F({}^\sigma\varpi)$. By Lemma 9.2, $\nu_F({}^\sigma\varpi) = 1$, and hence $m \mid 2$. Thus $D = F$ or D is a quaternion algebra over F, which contradicts our assumption that D is not isomorphic to D°. It follows that there is an isomorphism $\alpha\colon D \to D^\circ$. If α is F-linear, then D represents an element of order at most two in the Brauer group of F. As the only such elements are the class of F and the class of the unique quaternion division algebra over F, the result follows. In general, however, we can only say that α preserves the center F of D. By Lemma 9.2, it must also preserve $\mathfrak{o}_F$. The ring D contains a unique maximal $\mathfrak{o}_F$-order $\mathfrak{O}$ consisting of the elements of D that are integral over $\mathfrak{o}_F$. From this description, we see that α preserves $\mathfrak{O}$. Thus α also preserves the unique maximal (left or right) ideal $\mathfrak{q}$ in $\mathfrak{O}$, and hence induces an automorphism of the quotient $\mathfrak{O}/\mathfrak{q}$, a finite field of order q^m. Let ϖ_D be a generator of $\mathfrak{q}$, *i.e.*, $\mathfrak{q} = \varpi_D\mathfrak{O} = \mathfrak{O}\varpi_D$. Then, for $D \neq F$, there is a unique integer r with $1 < r < m$ and $(r,m) = 1$ such that

$$\varpi_D x \varpi_D^{-1} \equiv x^{q^r} \pmod{\mathfrak{q}}, \quad x \in \mathfrak{O}. \tag{9.2}$$

Moreover the congruence is independent of the choice of generator ϖ_D. (This all follows, for example, from [19, 14.5].) Applying α to (9.2) and rearranging (and using the fact that $\mathfrak{O}/\mathfrak{q}$ has order q^m), we obtain

$$\alpha(\varpi_D) x \alpha(\varpi_D)^{-1} \equiv x^{q^{m-r}} \pmod{\mathfrak{q}}, \quad x \in \mathfrak{O}.$$

Since (9.2) holds for all generators of $\mathfrak{q}$, we deduce that $r = m - r$ or $2r = m$, whence $r = 1$ and $m = 2$. Thus D is a quaternion algebra over F and we have completed the proof. ∎

Acknowledgements We are grateful to Steven Spallone and an anonymous referee for several helpful comments.

References

[1] J. Adams, *The real Chevalley involution.* Compositio Math. **150**(2014), 2127–2142. http://dx.doi.org/10.1112/S0010437X14007374

[2] J. Adler and S. DeBacker, *Murnaghan-Kirillov theory for supercuspidal representations of tame general linear groups, with appendices by G. Prasad and R. Huntsinger.* J. Reine Angew. Math. **575**(2004), 1–35. http://dx.doi.org/10.1515/crll.2004.080

[3] J. Adler and J. Korman, *The local character expansion near a tame, semisimple element.* Amer. J. Math. **129**(2007), no. 2, 381–403. http://dx.doi.org/10.1353/ajm.2007.0005

[4] J. Bernstein and A. Zelevinsky, *Representations of the group* $\mathrm{GL}(n,F)$ *where* F *is a non-Archimedean local field.* Russian Math. Surveys **31**(1976), no. 3, 1–68.

[5] C. Bushnell and G. Henniart, *Local tame lifting for* $\mathrm{GL}(n)$*. I. Simple characters*. Inst. Hautes Études Sci. Publ. Math. (1996), no. 83, 105–233.

[6] J. Dieudonné, *On the automorphisms of the classical groups.* Mem. Amer. Math. Soc. (2). Corrected reprint of the 1951 original. American Mathematical Society, Providence, RI, 1980.

[7] E. W. Ellers and W. Nolte, *Bireflectionality of orthogonal and symplectic groups.* Arch. Math. **39**(1982), 113–118. http://dx.doi.org/10.1007/BF01899190
[8] I. M. Gelfand and D. A. Kazhdan, *Representations of the group* $\mathrm{GL}(n, K)$ *where* K *is a local field.* In: Lie groups and their representations. Halsted, New York, 1975, pp. 95–118.
[9] R. Gow, *Products of two involutions in classical groups of characteristic 2.* J. Algebra **71**(1981), no. 2, 583–591. http://dx.doi.org/10.1016/0021-8693(81)90198-8
[10] R. Gow and C. R. Vinroot, *Extending real-valued characters of finite general linear and unitary groups on elements related to regular unipotents.* J. Group Theory **11**(2008), no. 3, 299–331. http://dx.doi.org/10.1515/JGT.2008.017
[11] Harish-Chandra, *A submersion principle and its applications.* In: Geometry and analysis: papers dedicated to the memory of V. K. Patodi. Indian Academy of Sciences, Bangalore, 1980, pp. 95–102.
[12] H. Jacquet, *Sur les représentations des groupes réductifs* p*-adiques.* C. R. Acad. Sci. Paris Sér. A-B **280**(1975), Aii, A1271–A1272.
[13] I. Kaplansky, *Linear algebra and geometry: a second course.* 2nd. edition. Chelsea Publishing Company, New York, 1974.
[14] Y. Lin, B. Sun, and S. Tan, *MVW-extensions of quaternionic classical groups.* Math. Z. **277**(2014), 81–89. http://dx.doi.org/10.1007/s00209-013-1246-6
[15] C. Mœglin, M.-F. Vignéras, and J.-L. Waldspurger, *Correspondances de Howe sur un corps* p*-adique.* Lecture Notes in Mathematics, 1291. Springer-Verlag, Berlin, 1987.
[16] G. Muić and G. Savin, *Complementary series for Hermitian quaternionic groups.* Canad. Math. Bull. **43**(2000), no. 1, 90–99. http://dx.doi.org/10.4153/CMB-2000-014-5
[17] D. Prasad, *On the self-dual representations of finite groups of Lie type.* J. Algebra **210**(1998), no. 1, 298–310. http://dx.doi.org/10.1006/jabr.1998.7550
[18] A. Raghuram, *On representations of* p*-adic* $\mathrm{GL}_2(D)$. Pacific J. Math. **206**(2002), no. 2, 451–464. http://dx.doi.org/10.2140/pjm.2002.206.451
[19] I. Reiner, *Maximal orders.* Corrected reprint of the 1975 original. With a foreword by M. J. Taylor. London Math. Soc. Monographs. New Series, 28. Oxford University Press, Oxford, 2003.
[20] A. Roche and C. R. Vinroot, *Dualizing involutions for classical and similitude groups over local non-Archimedean fields.* J. Lie Theory **27**(2017), no. 2, 419–434.
[21] A. A. Schaeffer Fry and C. R. Vinroot, *Real classes of finite special unitary groups.* J. Group Theory **19**(2016), no. 5, 735–762. http://dx.doi.org/10.1515/jgth-2016-0009
[22] K.-I. Shinoda, *The characters of Weil representations associated to finite fields.* J. Algebra **66**(1980), no. 1, 251–280. http://dx.doi.org/10.1016/0021-8693(80)90123-4
[23] A. Tupan, *A triangulation of* $\mathrm{GL}(n, F)$. Represent. Theory **10**(2006), 158–163. http://dx.doi.org/10.1090/S1088-4165-06-00224-X
[24] C. R. Vinroot, *A factorization in* $\mathrm{GSp}(V)$. Linear and Multilinear Algebra **52**(2004), no. 6, 385–403. http://dx.doi.org/10.1080/03081080412331316079
[25] ———, *A note on orthogonal similitude groups.* Linear and Multilinear Algebra **54**(2006), no. 6, 391–396. http://dx.doi.org/10.1080/03081080500209588
[26] M. J. Wonenburger, *Transformations which are products of two involutions.* J. Math. Mech. **16**(1966), 327–338.

Dept. of Mathematics, University of Oklahoma, Norman, OK 73019-3103, USA
e-mail: aroche@math.ou.edu

Dept. of Mathematics, College of William and Mary, P.O. Box 8795, Williamsburg, VA 23187-8795, USA
e-mail: vinroot@math.wm.edu