TAME SUPERCUSPIDAL REPRESENTATIONS OF GL_n DISTINGUISHED BY ORTHOGONAL INVOLUTIONS

JEFFREY HAKIM

ABSTRACT. For a p -adic field F of characteristic zero, the embeddings of a tame supercuspidal representation π of $G = \mathrm{GL}_n(F)$ in the space of smooth functions on the set of symmetric matrices in G are determined. It is shown that the space of such embeddings is nonzero precisely when -1 is in the kernel of π and, in this case, this space has dimension four. In addition, the space of H -invariant linear forms on the space of π is determined whenever H is an orthogonal group in n variables contained in G .

CONTENTS

1. Introduction and statement of results	121
1.1. Overview and acknowledgments	121
1.2. Dimensions of spaces of invariant linear forms	122
1.3. Pure inner forms of orthogonal groups	123
1.4. Explanation of 4-dimensionality	126
2. Quadratic spaces and orthogonal involutions	128
3. Lemmas involving tamely ramified extensions	130
4. J -symmetric embeddings	135
4.1. Preliminaries	135
4.2. Existence and construction of J -symmetric integral embeddings	137
4.3. Embeddings of degree n extensions of F stable under an outer automorphism	139
4.4. Restriction and extension of involutions	141
5. Orthogonal similitudes	145
5.1. Generalities	145
5.2. Finite fields	146
5.3. p -adic fields	147
6. Split T -orbits of orthogonal involutions	149
6.1. Generalities	149
6.2. Finite fields	150
6.3. p -adic fields	150
7. Tame supercuspidal representations	153
7.1. Buildings of general linear groups	153
7.2. Inducing data	156

Received by the editors August 16, 2011 and, in revised form, May 11, 2012, July 22, 2012, July 25, 2012 and September 11, 2012.

2010 *Mathematics Subject Classification*. Primary 22E50, 11F70; Secondary 11F67, 11E08, 11E81.

Key words and phrases. Supercuspidal representation, involution, distinguished representation, orthogonal group.

The author was supported by NSF grant DMS-0854844.

©2013 American Mathematical Society
 Reverts to public domain 28 years from publication

7.3.	Parahoric subalgebras and Moy-Prasad filtrations	159
7.4.	The character η'_θ	160
8.	Proofs of the main theorems	161
8.1.	Proof outlines	161
8.2.	Reduction to θ -split tori over the residue field	163
8.3.	Lifting finite θ -stable tori to p -adic θ -stable tori	165
8.4.	Reduction to θ -stable tori	166
8.5.	Reduction to θ -split tori	167
8.6.	Reduction to orthogonal involutions on Levi subgroups and finite groups	169
8.7.	The number of split T -orbits in a K^0 -orbit	169
8.8.	Reduction from K^0 -orbits to split T -orbits	171
8.9.	The T -orbit multiplicity formula	171
8.10.	Evaluating $\langle \zeta, \xi \rangle_T$	172
8.11.	Proofs of Theorems 1.2, 1.3 and 1.4	173
	Acknowledgements	173
	References	174

1. INTRODUCTION AND STATEMENT OF RESULTS

1.1. Overview and acknowledgments. Let $G = GL_n(F)$, where $n > 1$ and F is a finite extension of $\mathbb{Q}_p$, for some odd prime p . The space $C^\infty(\mathcal{S})$ of locally constant functions on the set $\mathcal{S}$ of symmetric matrices in G is a (nonsmooth) G -module with respect to the action

$$(g \cdot f)(\nu) = f({}^t g \nu g),$$

with $g \in G$, $f \in C^\infty(\mathcal{S})$ and $\nu \in \mathcal{S}$. Given a complex representation (π, V_π) of G , we say that a G -equivariant linear embedding of V_π in $C^\infty(\mathcal{S})$ is a *symmetric matrix model* for π . One of the main results of this paper specifies the dimension of the space $\text{Hom}_G(\pi, C^\infty(\mathcal{S}))$ of such models when π is a tame supercuspidal representation of G (as constructed in [Ho]) with central character ω_π :

Theorem 1.1. *If π is an irreducible tame supercuspidal representation of G then π has a symmetric matrix model precisely when $\omega_\pi(-1) = 1$. In this case, the dimension of $\text{Hom}_G(\pi, C^\infty(\mathcal{S}))$ is 4.*

Using Frobenius reciprocity, one sees that determining the symmetric matrix models for π is equivalent to determining, for all $\nu \in \mathcal{S}$, the space $\text{Hom}_{G_\nu}(\pi, 1)$ of linear forms λ on V_π that are invariant under the action of the orthogonal group

$$G_\nu = \{h \in G : {}^t h \nu h = \nu\},$$

in the sense that

$$\lambda(\pi(h)v) = \lambda(v),$$

for all $h \in G_\nu$ and $v \in V_\pi$.

For us, “orthogonal group” will mean such a group G_ν (or the associated algebraic group over F). If H is an orthogonal group in G and $\text{Hom}_H(\pi, 1)$ is nonzero, we say that π is *H-distinguished*. We show:

Theorem 1.2. *If π is an irreducible tame supercuspidal representation of G and if H is a split orthogonal group then π is H -distinguished precisely when $\omega_\pi(-1) = 1$.*

Theorems 1.3 and 1.4 below supplement Theorem 1.2 by precisely specifying the distinguished representations and the dimension of $\mathrm{Hom}_H(\pi, 1)$ for all tame supercuspidal representations π of G and all orthogonal groups H . Theorem 1.1 then follows easily from a case-by-case analysis.

To further illustrate Theorem 1.1 in the context of general symmetric spaces over F , we state it in the language of pure inner forms. More precisely, we give a formula for the total dimension of the spaces $\mathrm{Hom}_H(\pi, 1)$ as H varies over a pure inner class. This restatement in general language is not meant to suggest what should happen in all other examples, but rather to provide a baseline for comparing this example with others. As we will discuss, the examples considered in this paper are exceptional in several ways.

For simplicity, we only refer to the dimensions of the spaces $\mathrm{Hom}_G(\pi, C^\infty(\mathcal{S}))$ and $\mathrm{Hom}_{G_\nu}(\pi, 1)$ in our results, however, it is a routine matter to use our calculations and the methods of [HMu] and [HL1] to explicitly describe the elements of the latter spaces.

In the theory of distinguished representations, it has become expected that for a given F -symmetric space $H \backslash G$, the set of H -distinguished representations of G is the image of a lifting map from some other group H' to G . Ideally, the connection between H -distinction and the lifting from H' fits harmoniously within the Langlands program framework and its recent symmetric space formulation in the work of Sakellaridis and Venkatesh [SV]. Such harmony is presently lacking for the symmetric spaces we study. On the one hand, the relevant lifting is the Flicker-Kazhdan metaplectic correspondence [FK] from the double cover $\tilde{G}$ of G to G . Though the theory of local Langlands correspondences for nonlinear groups is an area of active research (see [GS, W], for example), the case of $\tilde{G}$ is still not fully understood. In addition, the notion of the L -group of a symmetric space in [SV] is undefined for our symmetric spaces. (Roughly speaking, one hopes to have a symmetric space L -group ${}^L(H \backslash G)$ such that a representation of G is H -distinguished exactly when its Langlands parameter factors through ${}^L(H \backslash G)$.)

Representations of G with symmetric matrix models arise in the local theory of automorphic representations of GL_n with orthogonal periods. Jacquet [Ja] has suggested a comparison of (global) relative trace formulas associated to the two sides of the metaplectic correspondence mentioned above. This idea has been pursued by Mao [Ma], but much work remains. A local implication of this setup is that the linear forms in $\mathrm{Hom}_H(\pi, 1)$, for suitable orthogonal groups H , should be correlated with Whittaker functionals for the corresponding representation of $\tilde{G}$. We refer the reader to the work of Chinta and Offen ([CO1] and [CO2]) for more information.

This paper is by no means self-contained. Its heavy dependence on [Ho], [Y], [HMu] and [HL1] places a burden on the reader that we have attempted to lessen by including an extended sketch of our main proofs (see §8.1) and recapitulations of some of the relevant material from the mathematical literature.

The present work uses general techniques for studying distinguished tame supercuspidal representations developed by the author and Murnaghan [HMu], together with refinements appearing in [HL1]. This paper also builds on previous work of the author with Mao [HMa] (the depth zero case) and Lansky [HL1] (the case in which n is odd) involving the specific examples considered in this paper.

1.2. Dimensions of spaces of invariant linear forms. There is an obvious necessary condition for H -distinction, for any orthogonal group H :

If an irreducible representation π of G is H -distinguished then $\omega_\pi(-1) = 1$.

Indeed, this follows from the fact that if $\lambda \in \text{Hom}_H(\pi, 1)$ then $\lambda(v) = \lambda(\pi(-1)v) = \omega_\pi(-1)\lambda(v)$, for all $v \in V_\pi$.

Given a degree n tamely ramified extension E of F and an F -admissible (in the sense of [Ho]) quasicharacter $\varphi : E^\times \rightarrow \mathbb{C}^\times$ then Howe's construction [Ho] gives an equivalence class $\pi(\varphi)$ of tame supercuspidal representations of G . The central character ω_π of $\pi \in \pi(\varphi)$ agrees with the restriction of φ to $F^\times$. So the necessary condition above can also be expressed as $\varphi(-1) = 1$. The analogue of Theorem 1.2 for nonsplit orthogonal groups is:

Theorem 1.3. *Suppose H is a nonsplit orthogonal group and π is a tame supercuspidal representation associated to an F -admissible quasicharacter $\varphi : E^\times \rightarrow \mathbb{C}^\times$ such that $\varphi(-1) = 1$. Then π is H -distinguished precisely when one of the following conditions holds:*

- E contains a unique quadratic extension L of F and $H = G_\nu$, where $(-1)^{n(n-1)/2} \det(\nu)$ lies in $N_{L/F}(L^\times) - (F^\times)^2$. In this case, H is necessarily quasisplit.
- E contains three quadratic extensions of F and H is not quasisplit.

For orthogonal groups H and for H -distinguished π , the dimension of the space $\text{Hom}_H(\pi, 1)$ is given by:

Theorem 1.4. *Suppose H is an orthogonal group and π is an irreducible H -distinguished tame supercuspidal representation of G associated to an F -admissible quasicharacter $\varphi : E^\times \rightarrow \mathbb{C}^\times$.*

- (1) *If H is split then the dimension of $\text{Hom}_H(\pi, 1)$ is*
 - 1, if n is odd or, equivalently, if E contains no quadratic extensions of F ,
 - 2, if E contains a unique quadratic extension of F ,
 - 3, if E contains three quadratic extensions of F .
- (2) *If H is not split then the dimension of $\text{Hom}_H(\pi, 1)$ is 1.*

1.3. Pure inner forms of orthogonal groups. Let G act on $\mathcal{S}$ via the right action:

$$\nu \cdot g = {}^t g \nu g.$$

The stabilizer of $\nu \in \mathcal{S}$ is the orthogonal group G_ν . We let $\mathcal{S}_\nu$ denote the orbit of ν . Each orbit $\mathcal{S}_\nu$ is open and closed in $\mathcal{S}$ and thus

$$C^\infty(\mathcal{S}) \cong \bigoplus_{\nu} C^\infty(\mathcal{S}_\nu),$$

where we are summing over a set of representatives for the G -orbits (a.k.a. similarity classes) in $\mathcal{S}$. The number of G -orbits is 8, unless $n = 2$ in which case there are 7 orbits. The G -orbit of $\nu \in \mathcal{S}$ is determined by the discriminant and the Hasse invariant of ν .

For a representation π of G , we have

$$\text{Hom}_G(\pi, C^\infty(\mathcal{S})) \cong \bigoplus_{\nu} \text{Hom}_G(\pi, C^\infty(\mathcal{S}_\nu)).$$

We may identify $\mathcal{S}_\nu$ with $G_\nu \backslash G$. Then the space of smooth vectors in $C^\infty(\mathcal{S}_\nu)$ is identified with the smooth representation $\text{Ind}_{G_\nu}^G(1)$ induced from the trivial character of G_ν . Therefore, when π is smooth we have

$$\text{Hom}_G(\pi, C^\infty(\mathcal{S}_\nu)) \cong \text{Hom}_G(\pi, \text{Ind}_{G_\nu}^G(1)).$$

Applying Frobenius reciprocity, we obtain

$$(1.1) \quad \text{Hom}_G(\pi, C^\infty(\mathcal{S})) \cong \bigoplus_{\nu} \text{Hom}_{G_\nu}(\pi, 1).$$

For convenience, we now fix a tame supercuspidal representation π such that $\omega_\pi(-1) = 1$. Assume that π comes from an F -admissible quasicharacter $\varphi : E^\times \rightarrow \mathbb{C}^\times$.

Definition 1.5. An **orthogonal involution of G** is an F -automorphism of GL_n defined by

$$\theta_\nu(g) = \nu^{-1} \cdot {}^t g^{-1} \cdot \nu,$$

for some $\nu \in \mathcal{S}$.

Given an orthogonal involution θ_ν , the group G^{θ_ν} of fixed points in G of θ_ν is the orthogonal group G_ν . (See §2 for basic facts about orthogonal involutions.) The group G acts on the set of its orthogonal involutions by

$$g \cdot \theta = \text{Int}(g) \circ \theta \circ \text{Int}(g)^{-1},$$

where $(\text{Int}(g))(g') = gg'g^{-1}$.

We observe that if $\nu_1, \nu_2 \in \mathcal{S}$ then

$$G_{\nu_1} = G_{\nu_2} \Leftrightarrow \theta_{\nu_1} = \theta_{\nu_2} \Leftrightarrow \nu_1 Z = \nu_2 Z,$$

where Z is the center of G . Furthermore,

$$\begin{aligned} G_{\nu_1} \cong G_{\nu_2} &\Leftrightarrow G_{\nu_1} \text{ and } G_{\nu_2} \text{ are } G\text{-conjugate} \\ &\Leftrightarrow \theta_{\nu_1} \text{ and } \theta_{\nu_2} \text{ are in the same } G\text{-orbit} \\ &\Leftrightarrow \nu_1 Z \text{ and } \nu_2 Z \text{ are in the same } G\text{-orbit.} \end{aligned}$$

In fact, for all $g \in G$ and $\nu \in \mathcal{S}$ we have

$$G_{t_g \nu g} = g^{-1} G_\nu g.$$

The G -orbits of orthogonal involutions are given as follows. Let Θ_J be the G -orbit of θ_J , where

$$J = J_n = \begin{pmatrix} & & & 1 \\ & \ddots & & \\ & & \ddots & \\ 1 & & & \end{pmatrix}.$$

Then the involutions in Θ_J are precisely the involutions that give rise to split orthogonal groups.

If n is odd there is only one other G -orbit of orthogonal involutions. We denote it by Θ_{nqs} . When n is even and greater than two, we let Θ_{nqs} denote the G -orbit consisting of all orthogonal involutions θ_ν associated to symmetric matrices ν not similar to J but having the same discriminant as J . Whether n is odd or even, the elements of Θ_{nqs} are the involutions that yield orthogonal groups that are not quasisplit.

When n is even there are three additional G -orbits of orthogonal involutions corresponding to the three possible discriminants other than the discriminant of J .

In other words, if θ_ν is not in Θ_J or Θ_{nqs} then its G -orbit is determined by the discriminant of ν . The associated orthogonal groups are quasisplit but not split.

Another elementary fact is that we have an isomorphism

$$\mathrm{Hom}_{G_\nu}(\pi, 1) \cong \mathrm{Hom}_{g^{-1}G_\nu g}(\pi, 1)$$

given by mapping $\lambda \in \mathrm{Hom}_{G_\nu}(\pi, 1)$ to the linear form $w \mapsto \lambda(\pi(g)w)$. This shows that, for a given π , the dimension of $\mathrm{Hom}_{G^\theta}(\pi, 1)$ is constant as θ varies over a G -orbit of involutions.

Throughout this paper, unless otherwise specified, we use boldface letters for algebraic groups defined over F and we use the corresponding nonbold letters for the associated groups of rational points. In particular, we now take $\mathbf{G}$ be the F -group GL_n and $G = \mathrm{GL}_n(F)$. Given $\sigma \in \Gamma = \mathrm{Gal}(\overline{F}/F)$ and $g \in \mathbf{G}$, we use the notation $\sigma(g)$ for the standard Galois action. Fix $\nu \in \mathcal{S}$ such that the orthogonal group

$$\mathbf{H} = \{g \in \mathbf{G} : {}^t g \nu g = \nu\}$$

is split over F . (For example, take $\nu = J$.) Then $H = \mathbf{H}(F) = G_\nu$. Suppose $z \in Z^1(F, \mathbf{H})$ is a Galois 1-cocycle. In other words, if $\overline{F}$ is an algebraic closure of F then z is a map $\sigma \mapsto z_\sigma$ from Γ to $\mathbf{H}$ such that $z_{\sigma\tau} = z_\sigma \sigma(z_\tau)$, for all $\sigma, \tau \in \Gamma$.

We may also view z as an element of $Z^1(F, \mathbf{G})$. Since $H^1(F, \mathbf{G})$ is trivial, we can choose $\zeta \in \mathbf{G}$ such that $z_\sigma = \zeta \sigma(\zeta)^{-1}$, for all $\sigma \in \Gamma$. The coset ζG is canonically associated to z and it consists of all possible choices of ζ . Note that for any element ζ in $\mathbf{G}$, if we define $z_\sigma = \zeta \sigma(\zeta)^{-1}$ then we have

$$\begin{aligned} {}^t \zeta \nu \zeta \in \mathcal{S} &\Leftrightarrow \sigma({}^t \zeta \nu \zeta) = {}^t \zeta \nu \zeta, \forall \sigma \\ &\Leftrightarrow \nu = {}^t z_\sigma \nu z_\sigma, \forall \sigma \\ &\Leftrightarrow z_\sigma \in \mathbf{H}, \forall \sigma \\ &\Leftrightarrow z \in Z^1(F, \mathbf{H}). \end{aligned}$$

This gives a canonical bijection between $H^1(F, \mathbf{H})$ and the set of G -orbits in $\mathcal{S}$ that sends the cohomology class of z to the G -orbit of ${}^t \zeta \nu \zeta$. (This also follows from Corollary 1 of Proposition I.5.36 and Lemma III.1.1 in [Se].)

Associated to $\mathbf{H}$ and z is the group $\mathbf{H}_z^*$ which is the same as $\mathbf{H}$ with the modified Galois action

$$\sigma_*(g) = z_\sigma \sigma(g) z_\sigma^{-1}.$$

Consider the group $\zeta^{-1} \mathbf{H}_z^* \zeta$ with the standard Galois action inherited from $\mathbf{G}$. Then $h \mapsto \zeta h \zeta^{-1}$ determines an F -isomorphism between $\zeta^{-1} \mathbf{H}_z^* \zeta$ and $\mathbf{H}_z^*$. On the other hand, if $\nu_* = {}^t \zeta \nu \zeta$ then

$$\zeta^{-1} \mathbf{H}_z^* \zeta = \{g \in \mathbf{G} : {}^t g \nu_* g = \nu_*\}.$$

If $\omega \in H^1(F, \mathbf{H})$ is the cohomology class of z then we let H_ω denote the G -conjugacy class of G_{ν_*} .

For our purposes, a *pure inner form* of H is a pair (ω, H_ω) , with $\omega \in H^1(F, \mathbf{H})$. By abuse of notation, we also use the notation H_ω for a specific group in the conjugacy class of H_ω . The connection between $\mathrm{Hom}_G(\pi, C^\infty(\mathcal{S}))$ and pure inner forms (as we have defined them) is now given by

$$\mathrm{Hom}_G(\pi, C^\infty(\mathcal{S})) \cong \bigoplus_{\omega \in H^1(F, \mathbf{H})} \mathrm{Hom}_{H_\omega}(\pi, 1).$$

Therefore Theorem 1.1 may be stated as:

$$(1.2) \quad \sum_{\omega \in H^1(F, \mathbf{H})} \dim \operatorname{Hom}_{H_\omega}(\pi, 1) = 4.$$

One can also consider the sum

$$\bigoplus_{\omega \in H^1(F, \mathbf{H}^\circ)} \operatorname{Hom}_{H_\omega}(\pi, 1),$$

where $\mathbf{H}^\circ$ is the identity component of $\mathbf{H}$. So $\mathbf{H}^\circ$ is a split special orthogonal group. In the above discussion, to require $z \in Z^1(F, \mathbf{H}^\circ)$ means that $\nu_* = {}^t\zeta \nu \zeta \in \mathcal{S}$ and $\det(\zeta \sigma(\zeta)^{-1}) = 1$ for all $\sigma \in \Gamma$. But the latter condition is equivalent to $\det \zeta \in F^\times$. It is also equivalent to $(\det \zeta)^2 = (F^\times)^2$. So $z \in Z^1(F, \mathbf{H}^\circ)$ if and only if the element ν_* lies in $\mathcal{S}$ and has the same discriminant as ν . When $n = 2$, $H^1(F, \mathbf{H}^\circ)$ is trivial, but otherwise $H^1(F, \mathbf{H}^\circ)$ has order two. When $n \neq 2$ and ω is the nontrivial cohomology class then H_ω is a non-quasisplit orthogonal group. Theorems 1.2, 1.3 and 1.4 imply:

$$(1.3) \quad \sum_{\omega \in H^1(F, \mathbf{H}^\circ)} \dim \operatorname{Hom}_{H_\omega}(\pi, 1) = [E^\times : (E^\times)^2 F^\times].$$

1.4. Explanation of 4-dimensionality. It is a routine matter to deduce Theorem 1.1 from Theorems 1.2, 1.3, and 1.4 and equation (1.1). Nevertheless, we consider this matter in detail in this section because the explanation of the source of 4-dimensionality in Theorem 1.1 appears to be quite different depending on how many quadratic extensions of F are contained in E . At the end of this section, we provide some uniformity by considering things in a more general context. However, even with this extra generality, there is no obvious way to extrapolate from our results reliable conjectures that predict the behavior of other symmetric spaces.

Assume n is odd. Then there are eight G -orbits in $\mathcal{S}$. Four of these orbits have representatives of the form zJ , with $z \in Z$. These G -orbits project to the single G -orbit Θ_J of orthogonal involutions. This, in turn, corresponds to the unique conjugacy class of split orthogonal groups in G . For such an orthogonal group H , the dimension of $\operatorname{Hom}_H(\pi, 1)$ is one, according to the results of [HL1]. The other four G -orbits in $\mathcal{S}$ yield a single conjugacy class of non-quasisplit orthogonal groups. the representation π is not H -distinguished for such orthogonal groups H , according to [HL1]. Therefore, equation (1.1) implies

$$\dim \operatorname{Hom}_G(\pi, C^\infty(\mathcal{S})) = 4 \cdot 1 + 4 \cdot 0 = 4,$$

which is consistent with Theorem 1.1.

If n is even and greater than 2, then there are again eight G -orbits in $\mathcal{S}$. The G -orbit of J projects to a unique G -orbit of orthogonal involutions, namely, Θ_J . The orthogonal groups in this case are split. There is also a unique G -orbit in $\mathcal{S}$ consisting of the symmetric matrices ν that have the same discriminant as J but do not lie in $\mathcal{S}_J$. This G -orbit projects to Θ_{nqs} . The remaining six G -orbits in $\mathcal{S}$ collapse in pairs to form three G -orbits of involutions. Two of these G -orbits in $\mathcal{S}$ merge precisely when they have the same discriminant. All of the associated orthogonal groups are quasisplit but not split. When $n = 2$, the situation is similar, except that there are only seven G -orbits in $\mathcal{S}$. The orbit that projects to Θ_{nqs} is missing.

According to Lemma 3.3, when n is even the field E contains at least one quadratic extension of F . Let us consider first the case in which E contains a unique quadratic extension L of F . According to Theorems 1.2 and 1.4, if H is a split orthogonal group then $\mathrm{Hom}_H(\pi, 1)$ has dimension two. According to Theorems 1.3 and 1.4, there is a single conjugacy class of quasisplit, nonsplit orthogonal groups H such that π is H -distinguished. For this H , the dimension of $\mathrm{Hom}_H(\pi, 1)$ is 1. However, since the conjugacy class of H comes from two G -orbits in $\mathcal{S}$, we count it twice in the tally of dimensions coming from equation (1.1). For all other orthogonal groups H , the representation π is not H -distinguished. We obtain

$$\dim \mathrm{Hom}_G(\pi, C^\infty(\mathcal{S})) = 2 + 2 = 4,$$

which is again consistent with Theorem 1.1.

Finally, we assume that E contains more than one quadratic extension of F . Note that if E contains two quadratic extensions of F then it must in fact contain all three possible quadratic extensions of F . Theorems 1.2, 1.3, and 1.4 imply that $\mathrm{Hom}_H(\pi, 1)$ has dimension three, when H is split, and has dimension one when H is not quasisplit. Otherwise, π is not H -distinguished. We have

$$\dim \mathrm{Hom}_G(\pi, C^\infty(\mathcal{S})) = 3 + 1 = 4.$$

In the above discussion, the explanation of why $\mathrm{Hom}_G(\pi, C^\infty(\mathcal{S}))$ has dimension 4 (when it is nonzero) is quite different depending on the number of quadratic extensions of F contained in E . For a more uniform explanation of the number 4, we describe things now in a more general setting.

Let $\mathbf{G}$ be the F -group GL_n . Let θ be the involution θ_J . We have a tame supercuspidal representation π of $G = \mathbf{G}(F)$ that is associated to an F -admissible quasicharacter of the multiplicative group of a degree n tamely ramified extension E of F . We choose a maximal F -torus $\mathbf{T}$ in $\mathbf{G}$ such that $T = \mathbf{T}(F) \cong E^\times$ and $\mathbf{T}$ is θ -split in the sense that $\theta(t) = t^{-1}$ for all $t \in \mathbf{T}$. The fact that such a $\mathbf{T}$ exists is a very special feature of our example. (See [Sp2] for more details.)

Let $\mathbf{H} = \mathbf{G}^\theta$, $H = \mathbf{H}(F)$, $\underline{\mathcal{S}} = \mathbf{H} \backslash \mathbf{G}$ and $\mathcal{S} = \underline{\mathcal{S}}^\Gamma$. We let $\mathbf{G}$ act by right translations on $\underline{\mathcal{S}}$. Suppose $\nu \in \mathcal{S}$. Then $\nu = \mathbf{H}g$, where $g \in \mathbf{G}$ and $\sigma \mapsto g\sigma(g)^{-1}$ defines a cocycle in $Z^1(F, \mathbf{H})$. This yields a canonical bijection between $H^1(F, \mathbf{H})$ and the set of G -orbits in $\mathcal{S}$. We define $\theta_\nu = g^{-1} \cdot \theta$ and $G_\nu = G^{\theta_\nu} = g^{-1}Hg$.

Theorem 1.1 asserts that the space

$$\mathrm{Hom}_G(\pi, C^\infty(\mathcal{S})) = \bigoplus_{\nu \in H^1(F, \mathbf{H})} \mathrm{Hom}_{G_\nu}(\pi, 1)$$

has dimension four. This can be proved by showing that the set $\mathcal{X}/T$ of T -orbits in the set

$$\mathcal{X} = \{\nu \in \mathcal{S} : \mathbf{T} \text{ is } \theta_\nu\text{-split}\}$$

has cardinality four and parametrizes a basis of $\mathrm{Hom}_G(\pi, C^\infty(\mathcal{S}))$. This is essentially what we do.

It is elementary to verify that there is a bijection between T/T^2 and $\mathcal{X}/T$ given by mapping the coset tT^2 to $\mathbf{H}s$ where s is any square root of t in $\mathbf{T}$. Thus $\mathcal{X}/T$ has cardinality four since it is in bijection with $E^\times/(E^\times)^2$. (This argument was suggested to us by Jeffrey Adams. Another argument is given later.)

Given $\nu \in \mathcal{S}$, let $\mathcal{X}_\nu = \{\eta \in \mathcal{S}_\nu : \mathbf{T} \text{ is } \theta_\eta\text{-split}\}$. It suffices to show that

$$\dim \mathrm{Hom}_{G_\nu}(\pi, 1) = \#(\mathcal{X}_\nu/T).$$

Suppose $\eta \in \mathcal{S}_\nu$. Let ζ be the T -orbit of θ_η . Let $m_T(\zeta)$ be the number of T -orbits in $\mathcal{S}_\nu$ that project to ζ . Then we have

$$\#(\mathcal{X}_\nu/T) = \sum_{\zeta} m_T(\zeta),$$

where we are summing over the T -orbits ζ in the G -orbit of θ_ν such that $\mathbf{T}$ is θ -split for some (hence all) $\theta' \in \zeta$.

The fact that

$$\dim \operatorname{Hom}_{G_\nu}(\pi, 1) = \sum_{\zeta} m_T(\zeta),$$

follows from Proposition 8.12.

2. QUADRATIC SPACES AND ORTHOGONAL INVOLUTIONS

Sections 2 through 7 contain background material that is needed in §8 for the proofs of the main theorems. To motivate the material in §2–7, the reader may find it advisable to skip directly to the proofs in §8, referring back to the preceding sections as needed.

In this section, we recall well-known facts about quadratic forms, quadratic spaces, orthogonal involutions, and orthogonal groups over a field F that is either:

- a finite field of odd characteristic,
- a finite extension of $\mathbb{Q}_p$ with $p \neq 2$.

Assume we have fixed such a field F . For convenience, we give a unified treatment of these two cases.

Definition 2.1. The **Hilbert symbol** is the pairing $F^\times \times F^\times \rightarrow \{\pm 1\}$ defined by

$$\operatorname{Hilbert}(a, b) = \begin{cases} 1, & \text{if } z^2 = ax^2 + by^2 \text{ has a solution } (x, y, z) \in F^3 - \{0\}, \\ -1, & \text{otherwise.} \end{cases}$$

When F is finite, $\operatorname{Hilbert}(a, b) = 1$ for all $a, b \in F^\times$ since every quadratic form in three variables is isotropic.

Let $G = \operatorname{GL}_n(F)$, where $n > 1$, and let $\mathcal{S}$ be the set of symmetric matrices in G . Then G acts on the right of $\mathcal{S}$ by $\nu \cdot g = {}^t g \nu g$. Two elements of $\mathcal{S}$ are said to be **similar** when they are in the same G -orbit. It is well known that the group A of diagonal matrices in $\mathcal{S}$ contains a set of representatives for the similarity classes in $\mathcal{S}$.

Definition 2.2. The **discriminant** $\operatorname{disc}(\nu)$ of $\nu \in \mathcal{S}$ is the image of $\det \nu$ in $F^\times / (F^\times)^2$. The **Hasse invariant** (a.k.a., **Hasse-Witt invariant**) $\operatorname{Hasse}(\nu)$ of $\nu \in \mathcal{S}$ is given by

$$\operatorname{Hasse}(\nu) = \prod_{i \leq j} \operatorname{Hilbert}(a_i, a_j),$$

where $\operatorname{diag}(a_1, \dots, a_n)$ is a diagonal matrix similar to ν .

The latter definitions are motivated by the following standard result:

Lemma 2.3. *Two elements $\nu_1, \nu_2 \in \mathcal{S}$ are similar precisely when $\operatorname{disc}(\nu_1) = \operatorname{disc}(\nu_2)$ and $\operatorname{Hasse}(\nu_1) = \operatorname{Hasse}(\nu_2)$.*

Unfortunately, the literature is not consistent in its use of the terminology “discriminant” or “Hasse invariant”. The “discriminant” of $\nu \in \mathcal{S}$ is sometimes defined as

$$\mathrm{disc}_0(\nu) = (-1)^{n(n-1)/2} \mathrm{disc}(\nu) = \det(J_n) \mathrm{disc}(\nu).$$

The “Hasse invariant” is sometimes defined as above except that the product is over $i < j$ instead of $i \leq j$, that is,

$$\mathrm{Hasse}_0(\nu) = \prod_{i < j} \mathrm{Hilbert}(a_i, a_j).$$

We have

$$\mathrm{Hasse}(\nu) = \mathrm{Hasse}_0(\nu) \prod_{i=1}^n (a_i, a_i) = \mathrm{Hasse}_0(\nu) \cdot \mathrm{Hilbert}(-1, \mathrm{disc} \nu).$$

Note that Lemma 2.3 would still be true regardless of which variants of the definitions one chooses. More precisely, if $\nu_1, \nu_2 \in \mathcal{S}$ then the statement “ ν_1 and ν_2 have the same discriminant” is independent of which of the two definitions of “discriminant” one chooses. Moreover, if ν_1 and ν_2 have the same discriminant then the statement “ ν_1 and ν_2 have the same Hasse invariant” is independent of which of the two definitions of “Hasse invariant” one chooses. (Therefore, to avoid confusion, we try to make such comparative statements rather than referring directly to the discriminant or Hasse invariant of an element of $\mathcal{S}$.)

Of the many identities regarding Hilbert symbols and Hasse invariants, we emphasize the following fact:

If F is a finite extension of $\mathbb{Q}_p$ with p odd and $\nu \in \mathcal{S} \cap \mathrm{GL}_n(\mathfrak{D}_F)$
then $\mathrm{Hasse}(\nu) = \mathrm{Hasse}_0(\nu) = 1$.

(See Lemma 5.9 [HL1].)

Suppose F is p -adic. Then $F^\times / (F^\times)^2$ has order four (since $p \neq 2$) and thus there are four possibilities for the discriminant of an element of $\mathcal{S}$. On the other hand, there are two possibilities for the Hasse invariant. Therefore, if $\nu \in \mathcal{S}$ there are eight possibilities for $(\mathrm{disc}(\nu), \mathrm{Hasse}(\nu))$. Hence, there are at most eight G -orbits (or, in other words, similarity classes) in $\mathcal{S}$. Using diagonal matrices, it is easy to see that there are exactly eight G -orbits in $\mathcal{S}$ when $n > 2$, but there are only seven orbits when $n = 2$ since in this case if $\mathrm{disc}(\nu) = \mathrm{disc}(J_n)$ then ν is similar to J_n .

When F is finite, $F^\times / (F^\times)^2$ has two elements and the Hasse invariant is always trivial. It turns out that there are always two G -orbits in $\mathcal{S}$ and they are characterized by the discriminant.

We now consider the orthogonal involutions θ_ν associated to $\nu \in \mathcal{S}$, as in Definition 1.5. Given $\nu_1, \nu_2 \in \mathcal{S}$, it is elementary to see that $\theta_{\nu_1} = \theta_{\nu_2}$ precisely when $\nu_1 Z = \nu_2 Z$, where Z is the center of G . So $\nu Z \mapsto \theta_\nu$ determines a bijection between the set $\mathcal{S}/Z$ and the set of orthogonal involutions of G .

The group G acts on the set of its orthogonal involutions by:

$$g \cdot \theta = \mathrm{Int}(g) \circ \theta \circ \mathrm{Int}(g^{-1}).$$

We have

$$g \cdot \theta_\nu = \theta_{t_{g^{-1}} \nu g^{-1}}.$$

The (right) action of G on $\mathcal{S}$ yields a right action of G on $\mathcal{S}/Z$.

Lemma 2.4. *The map that sends the G -orbit of θ_ν to the G -orbit of νZ defines a bijection between the set of G -orbits of orthogonal involutions and the set of G -orbits in $\mathcal{S}/Z$.*

Suppose F is finite. If n is odd then the two G -orbits in $\mathcal{S}$ merge into a single G -orbit in $\mathcal{S}/Z$, but when n is even they remain separate. We obtain:

Lemma 2.5. *Suppose F is finite. If n is odd there is a single G -orbit of orthogonal involutions. If n is even there are two G -orbits.*

When F is p -adic, we have:

Proposition 2.6. *Suppose F is p -adic. If $n > 1$ is odd then there are precisely two G -orbits of orthogonal involutions of G . If two elements of $\mathcal{S}$ have the same discriminant but different Hasse invariants then their cosets in $\mathcal{S}/Z$ lie in different G -orbits.*

If $n \geq 2$ is even then the discriminant determines a map from $\mathcal{S}/Z$ onto $F^\times/(F^\times)^2$. If $n = 2$ then there are four G -orbits in $\mathcal{S}/Z$ and they are precisely the fibers of the discriminant map $\mathcal{S}/Z \rightarrow F^\times/(F^\times)^2$. If $n > 2$ and even then there are five G -orbits in $\mathcal{S}/Z$. Three of these orbits are fibers of the discriminant map $\mathcal{S}/Z \rightarrow F^\times/(F^\times)^2$. But the fiber containing the matrix J_n breaks up into two orbits and these orbits are distinguished from each other by the Hasse invariant.

We refer the reader to §63C of [O] for the latter description of the the G -orbits in $\mathcal{S}$. From this, it is routine to deduce the orbit structure on $\mathcal{S}/Z$.

Let $\mathbf{G}$ be the F -group GL_n . If θ is an orthogonal involution of G then we let $\mathbf{G}^\theta$ denote the F -group consisting of the the fixed points of θ in $\mathbf{G}$. We let $G^\theta = \mathbf{G}^\theta(F)$ denote the group of fixed points of θ in G .

Lemma 2.7. *Suppose θ_1 and θ_2 are orthogonal involutions of $G = \mathrm{GL}_n(F)$ such that $G^{\theta_1} = G^{\theta_2}$. Then $\theta_1 = \theta_2$. Consequently, $\theta \mapsto G^\theta$ leads to a bijection between the set of G -orbits of orthogonal involutions of G and the set of G -conjugacy classes of orthogonal groups in n variables in G .*

Proof. We begin by recalling Proposition 1.2 [HW]:

Let $\mathbf{G}$ be a connected semi-simple algebraic group and θ_1 and θ_2 be involutions of $\mathbf{G}$. If the identity components of the fixed point groups $\mathbf{G}^{\theta_1}$ and $\mathbf{G}^{\theta_2}$ are identical, then $\theta_1 = \theta_2$.

Now suppose, under the hypotheses of our lemma, $G^{\theta_1} = G^{\theta_2}$. Then $H^{\theta_1} = H^{\theta_2}$, where $H = \mathrm{SL}_n(F)$. We deduce that $\mathbf{H}^{\theta_1} = \mathbf{H}^{\theta_2}$, where $\mathbf{H} = \mathrm{SL}_n$, since, according to Corollary 13.3.9 [Sp1], H^{θ_i} is dense in $\mathbf{H}^{\theta_i}$. This implies $\theta_1|_{\mathrm{SL}_n} = \theta_2|_{\mathrm{SL}_n}$, which implies $\theta_1 = \theta_2$. $\square$

3. LEMMAS INVOLVING TAMELY RAMIFIED EXTENSIONS

This section contains a collection of basic, and presumably well-known, facts about tamely ramified extensions. These facts will be needed in the proofs of our main results. The reader should assume that all fields discussed are finite extensions of $\mathbb{Q}_p$ where p is an odd prime. All field extensions will be finite and tamely ramified. If E/F is such an extension and if L is the maximal unramified extension of F contained in E then we use the standard notations $e(E/F) = [E : L]$ and $f(E/F) = [L : F]$. Tameness means that $e(E/F)$ is not divisible by p .

Lemma 3.1. *If E/F is a totally ramified, tamely ramified extension of finite degree n then:*

- $1 + \mathfrak{P}_F = (1 + \mathfrak{P}_F)^n = (1 + \mathfrak{P}_E)^n \cap \mathfrak{O}_F^\times$.
- $(\mathfrak{O}_E^\times)^n \cap \mathfrak{O}_F^\times = (\mathfrak{O}_F^\times)^n$.
- *There exist prime elements ϖ_E and ϖ_F of E and F , respectively, such that $\varpi_E^n = \varpi_F$. Given one such ϖ_F the coset $\varpi_F(\mathfrak{O}_F^\times)^n$ is the set of all such prime elements of F .*

Proof. Let p be the characteristic of the residue field of F . Then since E/F is totally ramified and tamely ramified, its degree n is not divisible by p . Let ϖ be a prime element of F . If $a \in \mathfrak{O}_F$ then applying Hensel's Lemma to the polynomial

$$f(x) = \varpi^{-1}((1 + \varpi x)^n - (1 + \varpi a))$$

allows one to find $b \in \mathfrak{O}_F$ such that $(1 + \varpi b)^n = 1 + \varpi a$. It follows that $(1 + \mathfrak{P}_F)^n = 1 + \mathfrak{P}_F$ and

$$1 + \mathfrak{P}_F = (1 + \mathfrak{P}_F)^n \subset (1 + \mathfrak{P}_E)^n \cap \mathfrak{O}_F^\times \subset 1 + \mathfrak{P}_F.$$

This proves the first claim.

To prove the second claim, it suffices to show that

$$(\mathfrak{O}_E^\times)^n \cap \mathfrak{O}_F^\times \subset (\mathfrak{O}_F^\times)^n.$$

Let μ be the set of roots of unity in E whose order is relatively prime to p . Then μ is also the set of roots of unity in F whose order is relatively prime to p . We have $\mathfrak{O}_E^\times = \mu \cdot (1 + \mathfrak{P}_E)$ and $\mathfrak{O}_F^\times = \mu \cdot (1 + \mathfrak{P}_F)$. Suppose $u \in (\mathfrak{O}_E^\times)^n \cap \mathfrak{O}_F^\times$. Then there exists $\zeta \in \mu$ and $v \in 1 + \mathfrak{P}_E$ such that $u = (\zeta v)^n$. We have $\zeta^{-n}u = v^n \in (1 + \mathfrak{P}_E) \cap \mathfrak{O}_F^\times = 1 + \mathfrak{P}_F$. Since $1 + \mathfrak{P}_F = (1 + \mathfrak{P}_F)^n$, we can assume $v \in 1 + \mathfrak{P}_F$. Thus $u = (\zeta v)^n \in (\mathfrak{O}_F^\times)^n$. The second claim follows.

The fact that there exist prime elements ϖ_E and ϖ_F of E and F such that $\varpi_E^n = \varpi_F$ is well known. Suppose we have two such pairs (ϖ_E, ϖ_F) and (ϖ'_E, ϖ'_F) . Let $w = \varpi'_E \varpi_E^{-1}$. Then $w^n = \varpi'_F \varpi_F^{-1} \in (\mathfrak{O}_E^\times)^n \cap \mathfrak{O}_F^\times = (\mathfrak{O}_F^\times)^n$. So $\varpi'_F \in \varpi_F(\mathfrak{O}_F^\times)^n$. Conversely, given $\varpi'_F = \varpi_F t^n$, with $t \in \mathfrak{O}_F^\times$, then $(t\varpi_E, \varpi'_F)$ is another pair of the same type as (ϖ_E, ϖ_F) . This completes the proof. $\square$

Lemma 3.2. *Let L be a finite totally ramified, tamely ramified extension of F of degree m and let E be a ramified quadratic extension of L . Let $n = 2m$ and let ϖ_F be a representative of the coset $\varpi_F(\mathfrak{O}_F^\times)^n$ of all prime elements of F that have an n -th root ϖ_E in E . Then ϖ_F has an m -th root ϖ_L in L .*

Proof. First, we show that there exists a triple $(\varpi_F, \varpi_L, \varpi_E)$ of prime elements for F , L and E , respectively, such that $\varpi_L^m = \varpi_F$ and $\varpi_E^2 = \varpi_L$.

Choose a prime element ϖ_F in F that has an m -th root ϖ_L in E . If ϖ_L has a square root ϖ_E in E then $(\varpi_F, \varpi_L, \varpi_E)$ is a triple of the desired type.

On the other hand, if ϖ_L does not have a square root in E then we may choose a root of unity u in L of order prime to p such that $u\varpi_L$ has a square root in E . But since L/F is totally ramified, it must be the case that u lies in F . We now rename $u\varpi_L$ and $u^m\varpi_F$ as ϖ_L and ϖ_F , respectively, and take ϖ_E to be a square root of the new element ϖ_L . This proves the existence of the desired triple.

Given such a triple $(\varpi_F, \varpi_L, \varpi_E)$, Lemma 3.1 implies that the coset $\varpi_F(\mathfrak{O}_F^\times)^n$ is the set of all prime elements of F that have an n -th root in E . But since we have chosen ϖ_F so that it has an m -th root in L , it follows that every element of the latter coset has an m -th root in L . $\square$

For general field extensions of even degree, it is not necessarily the case that the extension field must contain a quadratic extension of the base field. For example, there are quartic extensions of $\mathbb{Q}$, called primitive quartic fields, that do not contain any quadratic extensions of $\mathbb{Q}$.

On the other hand, for finite fields it is obviously true that an even degree extension $\mathbb{F}_{q^n}/\mathbb{F}_q$ contains the quadratic extension $\mathbb{F}_{q^2}$ of $\mathbb{F}_q$. For the field extensions that we are considering in this section, we also have a positive result:

Lemma 3.3. *If E is a finite, tamely ramified extension of F of even degree then E contains a quadratic extension of F .*

Proof. Consider first the special case in which E/F is a totally ramified, tamely ramified extension of even degree $n = 2m$. Then $E = F[\varpi_E]$, where ϖ_E is a prime element in E that is an n -th root of a prime element in F . Then E contains the ramified quadratic extension $F[\varpi_E^m]$ of F .

Now assume E/F is tamely ramified and $f(E/F)$ is even. Let L be the maximal unramified extension of F contained in E . This is the unique unramified extension of F of degree $f(E/F)$ and it contains the unique unramified quadratic extension of F . So our claim holds in this case.

Now suppose E/F is tamely ramified, $f(E/F)$ is odd, and $e(E/F)$ is even. Let L be the maximal unramified extension of F contained in E . We know that E contains a totally ramified quadratic extension K of L . It suffices to show that K contains a ramified quadratic extension of F . We may as well replace E by K or, equivalently, assume $e(E/F) = 2$. Then $E = L[\varpi_E]$, where ϖ_E is the square root of a prime element ϖ_L in L . Let ε be a nonsquare root of unity in F . In other words, $\varepsilon^{(q_F-1)/2} = -1$, where q_F be the order of the residue field of F . Since $f(E/F)$ is odd, $\varepsilon^{(q_F^{f(E/F)}-1)/2} = -1$ and thus ε is also a nonsquare root of unity in L . Therefore, given a prime element ϖ_F in F , the element ϖ_L must either lie in $\varpi_F(\mathfrak{O}_L^\times)^2$ or $\varepsilon\varpi_F(\mathfrak{O}_L^\times)^2$. It follows that either $F[\sqrt{\varpi_F}]$ or $F[\sqrt{\varepsilon\varpi_F}]$ is a ramified quadratic extension of F contained in E . $\square$

Given a finite extension E/F , let $y_{E/F}$ be defined by letting $y_{E/F} - 1$ be the number of quadratic extensions of F contained in E . Thus, in the present setting, $y_{E/F}$ must be 1, 2 or 4. The relevance of $y_{E/F}$ to the study of distinguished tame supercuspidal representations is discussed in §5.1.

Lemma 3.4. *Let E be a tamely ramified degree n extension of F such that $e = e(E/F)$ and $f = f(E/F)$ are even. Let L be the maximal unramified extension of F contained in E . Then $y_{E/F} = 4$ if and only if $(\mathfrak{O}_L^\times)^2 F^\times$ contains a prime element ϖ_L in L that has an e -th root in E .*

Proof. When $\varpi_E \in E$ is an e -th root of a prime element ϖ_L in L , we let $\sqrt{\varpi_L} = \varpi_E^{e/2}$. The element ϖ_L lies in $(\mathfrak{O}_L^\times)^2 F^\times$ precisely when it has the form $\varpi_L = u^2 \varpi_F$, where $u \in \mathfrak{O}_L^\times$ and ϖ_F is a prime element of F . In the latter situation, $u^{-1} \sqrt{\varpi_L}$ is a square root $\sqrt{\varpi_F}$ of ϖ_F that lies in E . Thus $F[\sqrt{\varpi_F}]$ is a ramified quadratic extension of F that is contained in E . Since f is even, E must also contain an unramified quadratic extension of F and thus $y_{E/F} = 4$.

Now suppose $y_{E/F} = 4$. Then, since E contains ramified quadratic extensions of F , there exists a prime element ϖ_F in F with a square root $\sqrt{\varpi_F}$ in E . There also exists a prime element ϖ_L in L with an e -th root ϖ_E in E . Let $\sqrt{\varpi_L} = \varpi_E^{e/2}$ and let $u = \sqrt{\varpi_L}(\sqrt{\varpi_F})^{-1} \in \mathfrak{O}_E^\times$. The element $\varpi_L \varpi_F^{-1} = u^2$ is an element

of $\mathfrak{D}_L^\times \cap (\mathfrak{D}_E^\times)^2$. The element u must lie in $\mathfrak{D}_L^\times$, since otherwise $L[u]$ would be an unramified quadratic extension of L contained in E . It follows that $\varpi_L \in (\mathfrak{D}_L^\times)^2 F^\times$, which completes the proof. $\square$

Lemma 3.5. *Let L be a tamely ramified extension of F with even ramification degree $e(L/F)$. Let E be an unramified quadratic extension of L . Then $y_{E/F} = 4$.*

Proof. Let $e = e(E/F) = e(L/F)$. Let K be the maximal unramified extension of F contained in L . Choose a prime element ϖ_K in K that has an e -th root $\varpi_L \in L$. Let $\sqrt{\varpi_K} = \varpi_L^{e/2}$. Then $K[\sqrt{\varpi_K}]$ is a ramified quadratic extension of K contained in L . The unique unramified quadratic extension of $K[\sqrt{\varpi_K}]$ is contained in E . It suffices to solve our problem with E replaced by the latter quadratic extension of $K[\sqrt{\varpi_K}]$.

Consequently, we now assume $e = 2$ and $L = K[\sqrt{\varpi_K}]$. Since $f(E/F)$ is even, it must be the case that E contains an unramified quadratic extension of F . Therefore it suffices to show that E contains a ramified quadratic extension of F .

Fix a prime element ϖ_F in F . Since E/L is an unramified quadratic extension, it is possible to choose a square root $v \in E$ of the unit $\varpi_F \varpi_K^{-1}$. Then $v \sqrt{\varpi_K}$ is a square root of ϖ_F in E . It follows that E contains a ramified quadratic extension of F and thus the proof is complete. $\square$

Lemma 3.6. *Suppose Q_1 is a quadratic extension of F and Q_2 is a quadratic extension of Q_1 . Then one of the following holds:*

- (1) $y_{Q_2/F} = 2$ and $(N_{Q_2/F}(Q_2^\times))(F^\times)^2 = N_{Q_1/F}(Q_1^\times)$.
- (2) $y_{Q_2/F} = 4$ and $(N_{Q_2/F}(Q_2^\times))(F^\times)^2 = (F^\times)^2$.

Proof. Clearly, $y_{Q_2/F} = 2$ or 4 . Suppose $y_{Q_2/F} = 4$. Then there must exist a quadratic extension Q_0 of F that is contained in Q_2 and is distinct from Q_1 . By transitivity of norms, $N_{Q_2/F}(Q_2^\times)$ must be contained in both $N_{Q_0/F}(Q_0^\times)$ and $N_{Q_1/F}(Q_1^\times)$. Since

$$N_{Q_0/F}(Q_0^\times) \cap N_{Q_1/F}(Q_1^\times) = (F^\times)^2,$$

we see that $y_{Q_2/F} = 4$ implies that $(N_{Q_2/F}(Q_2^\times))(F^\times)^2 = (F^\times)^2$.

It now suffices to show that if $y_{Q_2/F} = 2$ then $(N_{Q_2/F}(Q_2^\times))(F^\times)^2 = N_{Q_1/F}(Q_1^\times)$. So let us assume $y_{Q_2/F} = 2$ and thus Q_1/F is the unique quadratic extension of F contained in Q_2 . We observe that the image of $N_{Q_1/F}(Q_1^\times)$ in $F^\times/(F^\times)^2$ is a subgroup of order two that contains the image of $N_{Q_2/F}(Q_2^\times)$ in $F^\times/(F^\times)^2$. It suffices therefore to show that the image of $N_{Q_2/F}(Q_2^\times)$ in $F^\times/(F^\times)^2$ is nontrivial.

There are several cases to consider. First, suppose both Q_1/F and Q_2/Q_1 are ramified. If ϖ_{Q_2} is any prime element in Q_2 then $N_{Q_2/F}(\varpi_{Q_2})$ is a prime element in F . This gives an element of $N_{Q_2/F}(Q_2^\times)$ whose image in $F^\times/(F^\times)^2$ is nontrivial.

Now, suppose both Q_1/F and Q_2/Q_1 are unramified. Then $N_{Q_2/F}(\mathfrak{D}_{Q_2}^\times) = \mathfrak{D}_F^\times$. Thus we can choose an element of $N_{Q_2/F}(\mathfrak{D}_{Q_2}^\times)$ that is a nonsquare unit in F .

Next, suppose Q_1/F is unramified and Q_2/Q_1 is ramified. There exists a prime element ϖ_{Q_1} in Q_1 that has a square root ϖ_{Q_2} in Q_2 . It must be the case that $\varpi_{Q_1} \notin (\mathfrak{D}_{Q_1}^\times)^2 F^\times$, since otherwise we would have $y_{Q_2/F} = 4$. We can choose a prime element ϖ_F in F and a nonsquare unit u in Q_1 such that $\varpi_{Q_1} = u\varpi_F$. Now, $N_{Q_2/F}(\varpi_{Q_2}) = N_{Q_1/F}(-\varpi_{Q_1}) = N_{Q_1/F}(u) \cdot \varpi_F^2$. But the latter element has nontrivial image in $F^\times/(F^\times)^2$ since $N_{Q_1/F}$ determines an isomorphism

$$\mathfrak{D}_{Q_1}^\times/(\mathfrak{D}_{Q_1}^\times)^2 \rightarrow \mathfrak{D}_F^\times/(\mathfrak{D}_F^\times)^2$$

of groups of order two.

Finally, we are left with the case in which Q_1/F is ramified and Q_2/Q_1 is unramified. But this case is impossible since $y_{Q_2/Q_1} = 2$. $\square$

Lemma 3.7. *Suppose L is a finite tamely ramified extension of F and suppose E is a finite tamely ramified extension of L of even degree. If $y_{E/F} = 2$ then $y_{E/L} = 2$.*

Proof. Assume $y_{E/F} = 2$. Since $[E : L]$ is even, Lemma 3.3 implies that $y_{E/L} = 2$ or 4. Suppose $y_{E/L} = 4$. Then E contains square roots of all elements of L . In particular, it contains square roots of all elements of F . This implies $y_{E/F} = 4$ which is a contradiction. $\square$

Lemma 3.8. *If E is a finite, tamely ramified extension of F of degree n then the image of $N_{E/F}(E^\times)$ in $F^\times/(F^\times)^2$ is:*

- $F^\times/(F^\times)^2$, if $y_{E/F} = 1$,
- $N_{L/F}(L^\times)/(F^\times)^2$, if $y_{E/F} = 2$ and L is the unique quadratic extension of F contained in E ,
- trivial, if $y_{E/F} = 4$.

Consequently, the index of $N_{E/F}(E^\times) \cdot (F^\times)^2$ in $F^\times$ is $y_{E/F}$.

Proof. Suppose L is a quadratic extension of F that is contained in E . Then $L^\times/((L^\times)^2 F^\times)$ has order two. (See Lemma 5.6 in [HL1], for example.) Therefore, the norm $N_{L/F}$ must induce an isomorphism

$$L^\times/((L^\times)^2 F^\times) \cong N_{L/F}(L^\times)/(F^\times)^2.$$

If L_1 and L_2 are distinct quadratic extensions of F contained in E then the images of $N_{L_1/F}(L_1^\times)$ and $N_{L_2/F}(L_2^\times)$ in $F^\times/(F^\times)^2$ have trivial intersection. Consequently, the image of $N_{E/F}(E^\times)$ in $F^\times/(F^\times)^2$ must be trivial. So if $y_{E/F} = 4$ then $N_{E/F}(E^\times)$ must have trivial image in $F^\times/(F^\times)^2$.

Now suppose $y_{E/F} = 2$ and L is the unique quadratic extension of F contained in E . Then, according to Lemma 3.3, there exists a tower

$$F = Q_0 \subset Q_1 \subset \cdots \subset Q_r \subset E,$$

where $Q_1 = L$ and each extension of successive terms is quadratic, except for for E/Q_r which is an extension of odd degree. The homomorphism

$$E^\times/(E^\times)^2 \rightarrow Q_r^\times/(Q_r^\times)^2$$

induced by N_{E/Q_r} is an isomorphism (since $N_{E/Q_r}(Q_r^\times)(Q_r^\times)^2 = Q_r^\times$). It follows that the image of $N_{E/Q_{r-1}}(E^\times)$ in $Q_{r-1}^\times/(Q_{r-1}^\times)^2$ has order two. If $r = 1$, we are done. Otherwise, we apply Lemmas 3.6 and 3.7 to deduce that the image of $N_{E/Q_{r-2}}(E^\times)$ in $Q_{r-2}^\times/(Q_{r-2}^\times)^2$ has order two. Repeatedly applying Lemmas 3.6 and 3.7 in this way, we deduce that the image of $N_{E/F}(E^\times)$ in $F^\times/(F^\times)^2$ has order two. But by transitivity of norms, the latter image is contained in $N_{L/F}(L^\times)$. Therefore, the image of $N_{E/F}(E^\times)$ in $F^\times/(F^\times)^2$ is $N_{L/F}(L^\times)$.

Finally, if E/F contains no quadratic extensions of F then n must be odd. In this case, as we have just argued for E/L , we can show that $N_{E/F}$ maps $E^\times$ onto $F^\times/(F^\times)^2$. $\square$

4. J -SYMMETRIC EMBEDDINGS

In this section, we develop a geometric algebraic theory to study variants of the question:

When does a degree n extension E of a field F have an F -linear embedding in the set of symmetric matrices in $M_n(F)$?

The latter question has been studied especially for its applications to the theory of symmetric bilinear forms, but, since we are interested in rather different applications, we need to refine various aspects of the theory. The basic results regarding existence of embeddings are mostly known and we refer to [B] for more details and references to the literature.

The trace form $(x, y) \mapsto \text{tr}_{E/F}(xy)$ on E has tended to play a central role in the theory of embeddings of the type just mentioned. However, we downplay the use of trace forms and pursue a different approach than that which was used in [HL1] in the case of odd n . The two approaches are contrasted somewhat in §6.1. For our purposes, the approach we use is simpler, more illuminating, and leads to more canonical constructions.

Though the results in this section are rather simple, the reader may be surprised to see how frequently these results are used throughout the paper in seemingly different contexts.

We assume throughout this section that our fields do not have characteristic two. Though we often consider general fields (whose characteristic is not two), we really are only interested in finite extensions of a field $\mathbb{F}_p$ or $\mathbb{Q}_p$, where p is an odd prime.

4.1. Preliminaries. Let E/F be a field extension of (finite) degree n . Let $G = GL_n(F)$ and let $\mathfrak{g} = M_n(F)$ (viewed as an associative algebra, not a Lie algebra). Fix an F -basis $e_1, \dots, e_n$ of E . Then, for each $y \in E$, there is a column vector

$$\underline{y} = \begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix} \in F^n$$

such that

$$y = \sum_{i=1}^n y_i e_i.$$

We use $y \mapsto \underline{y}$ to identify E with F^n and then, given $x \in E$, we let $\underline{x}$ denote the matrix of the F -linear transformation $y \mapsto xy$ on E . We then have

$$\underline{x}\underline{y} = \underline{xy},$$

for all $x, y \in E$, and

$$xe_j = \sum_{i=1}^n x_{ij} e_i$$

for all j .

Every F -embedding of E in $\mathfrak{g}$ has the form $x \mapsto \underline{x}$ for a suitable choice of F -basis of E .

Let

$$J = J_n = \begin{pmatrix} & & 1 \\ & \ddots & \\ 1 & & \end{pmatrix} \in G.$$

Definition 4.1. A matrix $X \in \mathfrak{g}$ is *J -symmetric* if $J \cdot {}^t X \cdot J = X$ or, equivalently, if it is symmetric about its anti-diagonal (consisting of the matrix entries X_{ij} with $i + j = n + 1$). An F -embedding of E in $\mathfrak{g}$ is *J -symmetric* if its image consists only of J -symmetric matrices.

The notion of a J -symmetric embedding may be generalized by replacing transpose by the order two anti-automorphism σ_ν of $\mathfrak{g}$ given by

$$\sigma_\nu(X) = \nu^{-1} {}^t X \nu,$$

where ν is any fixed symmetric matrix in G .

Definition 4.2. If $\nu \in G$ is symmetric then a matrix $X \in \mathfrak{g}$ is *ν -symmetric* if $\sigma_\nu(X) = X$. An F -embedding of E in $\mathfrak{g}$ is *ν -symmetric* if its image consists of ν -symmetric matrices.

We will see that, for the field extensions E/F of interest to us, J -symmetric embeddings of E always exist, whereas ν -symmetric embeddings do not exist for arbitrary symmetric matrices ν . Moreover, once one fixes a J -symmetric embedding of E , it is easy to describe the ν -symmetric embeddings for arbitrary ν according to the following:

Proposition 4.3. *Suppose $x \mapsto \underline{\underline{x}}$ is a J -symmetric embedding of E in $\mathfrak{g}$. Then the set of symmetric matrices ν in G such that $x \mapsto \underline{\underline{x}}$ is ν -symmetric is identical to $J\underline{\underline{E}}^\times$. If $x \in E^\times$ and $\nu = J\underline{\underline{x}}$ then $\det(\nu) = (-1)^{n(n-1)/2} N_{E/F}(x)$.*

Proof. Assume $\nu \in G$ is symmetric and $x \mapsto \underline{\underline{x}}$ is a J -symmetric embedding of E in $\mathfrak{g}$. If $x \in E$ then ${}^t(J\underline{\underline{x}}) = {}^t\underline{\underline{x}}J = J\underline{\underline{x}}$. So the elements of $J\underline{\underline{E}}$ are all symmetric matrices. The given embedding is ν -symmetric precisely when every $x \in E$ satisfies $\underline{\underline{x}} = \nu^{-1}({}^t\underline{\underline{x}})\nu = \nu^{-1}J\underline{\underline{x}}J\nu$. In other words, the embedding is ν -symmetric exactly when $J\nu$ centralizes $\underline{\underline{E}}$. Since $\underline{\underline{E}}$ is its own centralizer, our first assertion follows. The second assertion reduces to the well-known fact that if E is embedded as an F -subalgebra of $\mathfrak{g}$ then the restriction of the determinant to the image of E agrees with the norm map $N_{E/F}$. $\square$

For us, one of the most important properties of J -symmetric embeddings is their transitivity with respect to towers of fields:

Lemma 4.4. *Let L be an intermediate field of E/F with $r = [L : F]$ and $s = n/r = [E : L]$. Suppose L is embedded in $M_r(F)$ via a J_r -symmetric embedding and suppose E is embedded in $M_s(L)$ via a J_s -symmetric embedding. Then the composite embedding of E in $\mathfrak{g} = M_n(F) = M_s(M_r(F))$ is J_n -symmetric.*

Proof. Embed L in $M_r(F)$ in a J_r -symmetric way. Thus,

$$J_r {}^t x J_r = x,$$

for all $x \in L$. (For simplicity, we are suppressing the double underline notation.)

Embed E in $M_s(L)$ in J_s -symmetric way. Then

$$J_s {}^T x J_s = x,$$

for all $x \in E$, where $x \mapsto {}^T x$ is the transpose in $M_s(L)$.

Since

$$M_s(L) \subset M_s(M_r(F)) = \mathfrak{g},$$

if $x \in M_s(L)$ then one needs to distinguish between the transpose $^T x$ in $M_s(L)$ and the transpose $^t x$ in $\mathfrak{g}$.

The relation between these two transposes can be precisely expressed as follows. Let $x \in M_s(L)$. Then $x = (x_{ij})$, where $x_{ij} \in L$ and $1 \leq i, j \leq s$. We have

$$^T x = {}^T(x_{ij}) = (x_{ji})$$

and

$$^t x = {}^t(x_{ij}) = ({}^t x_{ji}) = (J_r x_{ji} J_r) = J_r^s {}^T x J_r^s,$$

where J_r^s is the block diagonal matrix

$$J_r^s = J_r \oplus \cdots \oplus J_r$$

in G whose diagonal blocks are all J_r . We observe that

$$J_n = J_s J_r^s = J_r^s J_s.$$

(Here, we are using the embedding of $M_s(L)$ in $M_s(M_r(F)) = \mathfrak{g}$ to view J_s as an element of $\mathfrak{g}$.) Therefore, if $x \in E$ then we have

$$J_n {}^t x J_n = J_n J_r^s {}^T x J_r^s J_n = J_s {}^T x J_s = x.$$

This proves our claim. $\square$

The computations in the latter proof (and the notations J_r^s and $^T x$) are used implicitly and explicitly in what follows.

4.2. Existence and construction of J -symmetric integral embeddings. For a given symmetric matrix $\nu \in G$, we observe that if $X_1, \dots, X_s \in \mathfrak{g}$ are ν -symmetric matrices that commute with each other then their product $X_1 \cdots X_s$ is also ν -symmetric. In particular, powers of ν -symmetric matrices are ν -symmetric. When $\nu = J$, this yields the following basic construction of J -symmetric embeddings:

Lemma 4.5. *Suppose $n > 1$ is an integer and suppose τ is an element of F such that $x^n - \tau$ is irreducible over F . Let $E = F[\omega]$, where ω is an n -th root of τ . Then the embedding of E in $\mathfrak{g}$ associated to the basis $1, \omega, \omega^2, \dots, \omega^{n-1}$ is J -symmetric.*

Proof. The matrix that corresponds to the image of ω in $\mathfrak{g}$ is

$$\omega = \begin{pmatrix} 0 & 0 & \cdots & 0 & \tau \\ 1 & 0 & \cdots & 0 & 0 \\ 0 & 1 & \ddots & & \vdots \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ 0 & \cdots & 0 & 1 & 0 \end{pmatrix}.$$

The latter matrix is clearly symmetric about its anti-diagonal. Thus it is J -symmetric and so are its powers, as are all F -linear combinations of these powers. Therefore, the given embedding is J -symmetric. $\square$

Example 4.6. If E/F is quadratic and $E = F[\sqrt{\tau}]$ then

$$x + y\sqrt{\tau} = \begin{pmatrix} x & y\tau \\ y & x \end{pmatrix}$$

is a J -symmetric embedding of E in $M_2(F)$.

For finite fields, Lemma 4.5 does not construct all J -symmetric embeddings. For example, if $E = \mathbb{F}_{27}$ and $F = \mathbb{F}_3$, there is no polynomial $x^3 - \tau$ that is irreducible over $\mathbb{F}_3$.

We now describe another method for obtaining J -symmetric embeddings that begins with the choice of an arbitrary F -basis of E and determines whether, after some change of basis, one can obtain a basis such that the associated embedding of E in $\mathfrak{g}$ is J -symmetric.

Let us say that $e_1, \dots, e_n$ is our initial choice of an F -basis of E . For the present approach, we need to assume E/F is separable. For each $a \in E$, one obtains a symmetric F -bilinear form on E by

$$\langle x, y \rangle_a = \text{tr}_{E/F}(axy).$$

In matrix terms, we have

$$\langle x, y \rangle_a = {}^t \underline{x} \nu^a \underline{y},$$

where $\nu^a \in G$ is the symmetric matrix whose ij -th entry is

$$\nu_{ij}^a = \text{tr}_{E/F}(ae_i e_j).$$

(Invertibility of ν^a follows from our separability assumption.) For $b \in E$, we have

$${}^t \underline{b} \nu^a = \nu^{ab} = \nu^a \underline{b}.$$

Consequently, if a can be chosen so that $\nu^a = J$ then the chosen embedding is J -symmetric. On the other hand, if one can choose $a \in E$ and $g \in G$ so that ${}^t g \nu^a g = J$ then replacing $\{e_i\}$ by $\{\sum_j g_{ji} e_j\}$ gives a basis that yields a J -symmetric embedding.

Lemma 4.7. *Let $F = \mathbb{F}_q$ and $E = \mathbb{F}_{q^n}$, where q is a power of an odd prime. Then there exists a J_n -symmetric embedding of E in $\mathfrak{g}$.*

Proof. We adapt the proof of Lemma 5.13 of [HL1] to finite fields. Let β be a primitive $(q^n - 1)$ -root of 1 in E . Let f be the minimal polynomial of β over F . Let $e_i = \beta^{i-1}$ for $i \in \{1, \dots, n\}$. This gives an F -basis of E . Let $a = f'(\beta)^{-1}$ and define a symmetric matrix ν^a in $\mathfrak{g}$ by

$$(\nu^a)_{ij} = \text{tr}_{E/F}(ae_i e_j) = \sum_{k=1}^n \sigma_k(a) \sigma_k(e_i) \sigma_k(e_j),$$

where $\sigma_1, \dots, \sigma_n$ are the distinct Galois automorphisms of E/F . The matrix identity

$$\nu^a = (\sigma_j(e_i)) (\sigma_i(a) \delta_{ij}) (\sigma_i(e_j))$$

implies

$$\det(\nu^a) = N_{E/F}(a f'(\beta)) (-1)^{n(n-1)/2} = (-1)^{n(n-1)/2} = \det J_n.$$

So ν^a and J_n must be similar symmetric matrices in $\text{GL}_n(F)$. Therefore, we can choose $g \in \text{GL}_n(F)$ such that ${}^t g \nu^a g = J_n$. We use g to change our basis: $e'_i = \sum_j g_{ji} e_j$. The embedding associated to the latter basis is then J -symmetric. $\square$

For the rest of this section, we take E/F to be a tamely ramified degree n extension of fields that are finite extensions of $\mathbb{Q}_p$ with p odd. The existence of a J -symmetric embedding of E in $\mathfrak{g}$ in this case follows from Lemma 5.14 in [HL1], however, we will establish some more refined results.

Definition 4.8. A J -symmetric integral embedding of E in $\mathfrak{g}$ is a J -symmetric F -embedding of E in $\mathfrak{g}$ associated to an $\mathfrak{O}_F$ -basis of $\mathfrak{O}_E$. In this case, the basis is called a J -symmetric integral basis of E/F .

The next result proves the existence of a J -symmetric integral embedding of E in $\mathfrak{g}$ of a very special type that is convenient for block matrix calculations:

Lemma 4.9. *Let L be the maximal unramified extension of F contained in E and take $e = [E : L]$ and $f = [L : F]$.*

- (1) *There exists a prime element ϖ_E of E such that ϖ_E^e lies in L . For such a ϖ_E , taking $\alpha_j = \varpi_E^{j-1}$ yields a J -symmetric integral basis $\alpha_1, \dots, \alpha_e$ of E/L .*
- (2) *There exists a J -symmetric integral basis $\beta_1, \dots, \beta_f$ of L/F .*
- (3) *Let $e_1, \dots, e_n$ be the tensor product*

$$\alpha_1\beta_1, \alpha_1\beta_2, \dots, \alpha_2\beta_1, \alpha_2\beta_2, \dots$$

of bases $\{\alpha_j\}$ and $\{\beta_k\}$ of the types just described. Then $e_1, \dots, e_n$ is a J -symmetric integral basis of E/F .

Proof. For Assertion (1), the existence of ϖ_E follows from Lemma 3.1, while the remaining claim follows from Lemma 4.5.

For Assertion (2), we start by imitating the proof of Lemma 4.7, replacing the extension $\mathbb{F}_{q^n}/\mathbb{F}_q$ by L/F . We take β to be a primitive $(q^f - 1)$ -root of 1 in L . Associated to this choice is a matrix ν^a in $K = \mathrm{GL}_f(\mathfrak{O}_F)$ defined as in the proof of Lemma 4.7. Reducing mod $\mathfrak{P}_F$, the matrices ν^a and J_f are similar, and both are similar to a diagonal matrix $\delta \in \mathrm{GL}_f(\mathfrak{O}_F)$. Therefore, there exist $k, \ell \in K$ such that the entries of ${}^t k \nu^a k$, ${}^t \ell J_f \ell$, and δ are all congruent modulo $\mathfrak{P}_F$. According to Lemma 4 in [HMa], there exist upper triangular matrices $u, v \in \mathrm{GL}_f(\mathfrak{O}_F)$ that reduce to the identity matrix mod $\mathfrak{P}_F$ and satisfy ${}^t u \delta u = {}^t k \nu^a k$ and ${}^t v \delta v = {}^t \ell J_f \ell$. Take $h = ku^{-1}v\ell^{-1} \in K$. Then ${}^t h \nu^a h = J_f$. Taking $\beta_i = \sum_j h_{ji} \beta^{j-1}$ yields a J -symmetric integral basis $\beta_1, \dots, \beta_f$ of L/F .

Assertion (3) follows from Lemma 4.4 and the fact that tensor products of integral bases are again integral bases. $\square$

Lemma 4.10. *Given a tower of intermediate fields*

$$F = E_d \subset E_{d-1} \subset \dots \subset E_0 \subset E_{-1} = E,$$

such that each E_i with $i \in \{-1, \dots, d-1\}$ is embedded in $M_{[E_i: E_{i+1}]}(E_{i+1})$ via a J -symmetric integral embedding, the composite embedding of E in $\mathfrak{g}$ is a J -symmetric integral embedding.

Proof. Our claim follows from Lemma 4.4 and the fact that if L is an intermediate field of E/F , then the tensor product of an integral basis of L/F with an integral basis of E/L is an integral basis of E/F . $\square$

4.3. Embeddings of degree n extensions of F stable under an outer automorphism. Let F be a field and let $x \mapsto \bar{x}$ be an automorphism of F whose square is trivial. Let F' be the fixed field of $x \mapsto \bar{x}$. There are two cases:

- (1) $F = F'$ and $\bar{x} = x$ for all $x \in F$.
- (2) F/F' is quadratic and $\mathrm{Gal}(F/F') = \{1, x \mapsto \bar{x}\}$.

If X is a matrix with entries in F , we denote by $\overline{X}$ the matrix whose ij -th entry is $\overline{X_{ij}}$. We also let $X^* = {}^t\overline{X}$. If X is a square matrix and $X^* = X$ then we say X is **hermitian**. As before, we let $G = \mathrm{GL}_n(F)$ and $\mathfrak{g} = \mathrm{M}_n(F)$ and we fix a degree n extension E of F .

Fix a matrix $\nu \in G$ that is a scalar multiple of a hermitian matrix. Define an anti-automorphism σ_ν^* of $\mathfrak{g}$ of order two by

$$\sigma_\nu^*(X) = \nu^{-1} X^* \nu.$$

Definition 4.11. A ν -**embedding** of E in $\mathfrak{g}$ is an F' -embedding whose image is stable under σ_ν^* .

The relevance of ν -embeddings to the main problems addressed in this paper is as follows. We are considering tame supercuspidal representations of a group $G = \mathrm{GL}_n(F)$. These representations are associated to G -data that involve various subgroups $G^i = \mathrm{GL}_{n_i}(E_i)$ of G . If θ is an orthogonal involution of G that stabilizes G^i then the restriction of θ to G^i may not be an orthogonal involution but, rather, a unitary involution (in the obvious sense). (See Proposition 4.15.) So when we consider $G = \mathrm{GL}_n(F)$ in this section, we really have a twisted Levi subgroup G^i in mind.

Fix a ν -embedding of E in $\mathfrak{g}$ and identify E with its image in $\mathfrak{g}$. For every intermediate field L of E/F the restriction of σ_ν^* to L is an F' -automorphism whose square is trivial. We let L^ν denote the fixed field of $\sigma_\nu^*|L$. If $F \neq F'$ then $\sigma_\nu^*|L$ must have order two and L/L^ν must be quadratic. But if $F = F'$, we either have $L = L^\nu$ or L/L^ν is quadratic.

In the present setting, the notion of a ν -symmetric embedding of E in $\mathfrak{g}$ is identical to the notion of a ν -embedding of E in $\mathfrak{g}$ such that $E = E^\nu$. Since we have dealt with such embeddings in the previous section, we will now assume that our given embedding of E in $\mathfrak{g}$ is a “strict ν -embedding” in the following sense:

Definition 4.12. A **strict ν -embedding** of E in $\mathfrak{g}$ is a ν -embedding such that E/E^ν is quadratic.

It turns out that J -symmetric embeddings are just as useful in studying strict ν -embeddings as they are in studying ν -symmetric embeddings. Note that $\mathrm{Gal}(E/E^\nu) = \{1, \sigma_\nu^*|E\}$.

We first treat the case in which $F = F'$:

Proposition 4.13. *Let L be an intermediate field of E/F such that E/L is quadratic and let $r = [L : F] = n/2$. Choose $\tau \in L$ so that $E = L[\sqrt{\tau}]$ and embed E in $\mathrm{M}_2(L)$ via*

$$x + y\sqrt{\tau} = \begin{pmatrix} x & y\tau \\ y & x \end{pmatrix}$$

and embed L in $\mathrm{M}_r(F)$ via a J_r -symmetric embedding. Then the symmetric matrices ν in $G = \mathrm{GL}_n(F)$ such that $\sigma_\nu|E$ is the nontrivial Galois automorphism of E/L are precisely the matrices of the form

$$\nu = \begin{pmatrix} 1_r & 0 \\ 0 & -1_r \end{pmatrix} J_n x,$$

where $x \in E^\times$ and $\mathrm{tr}_{E/L}(x) = 0$. The determinant of ν is then given by $\det_G(\nu) = N_{E/F}(x) = \det(J_n)N_{L/F}(x)^2$.

Proof. Suppose x lies in E . Then $x = \begin{pmatrix} a & b\tau \\ b & a \end{pmatrix}$ for some $a, b \in L$. The Galois conjugate of x is identical to $\mu x \mu$, where $\mu = 1_r \oplus (-1_r)$. We need to compute the set of symmetric matrices ν in G such that

$$x = \sigma_\nu(\mu x \mu) = \nu^{-1} \mu {}^t x \mu \nu = (J_n \mu \nu)^{-1} x (J_n \mu \nu)$$

for all $x \in E$. The latter condition simply says that $J_n \mu \nu$ centralizes E or, equivalently, $J_n \mu \nu \in E^\times$. Thus the symmetric matrices in question are those symmetric matrices that lie in $\mu J_n E^\times$.

Now suppose $x \in E^\times$ and let $\nu = \mu J_n x$. Then ν is symmetric exactly when $\mu J_n x = \nu = {}^t \nu = {}^t x J_n \mu = J_n (J_n {}^t x J_n) \mu = J_n x \mu$. But, since $\mu J_n = -J_n \mu$, we deduce that ν is symmetric precisely when $-\mu x = x \mu$ or, equivalently, $-x = \mu x \mu$. The latter condition is the same as $\mathrm{tr}_{E/L}(x) = 0$.

The determinant identity reduces to showing that $\det(\mu J_n) = 1$, which is easily verified. $\square$

The analogous result when F/F' is quadratic is:

Proposition 4.14. *Assume F/F' is quadratic and choose $\tau \in F'$ so that $F = F'[\sqrt{\tau}]$. Assume L is a degree n extension of F' that is embedded in $M_n(F')$ via a J_n -symmetric embedding. Assume $L \cap F = F'$ and let E be the degree n extension of F given by $E = LF = L[\sqrt{\tau}]$. Embed E in $\mathfrak{g} = M_n(F)$ by extending scalars from F' to F . (In other words, given $x, y \in L$, identify the element $x + y\sqrt{\tau} \in E$ with an element of $M_n(F)$ by viewing x and y as elements of $M_n(F')$ and $\sqrt{\tau}$ as a scalar matrix in $M_n(F)$.)*

Then the set $J_n L^\times F^\times$ is identical to the set of matrices in $J_n E^\times$ that are scalar multiples of hermitian matrices. It is also identical to the set of $\nu \in G = \mathrm{GL}_n(F)$ that are scalar multiples of hermitian matrices and satisfy $\sigma_\nu^|E \in \mathrm{Gal}(E/L)$. If $x \in E^\times$ and $\nu = J_n x$ then*

$$\det_G(\nu) = (-1)^{n(n-1)/2} N_{E/F}(x).$$

Proof. Suppose ν is a scalar multiple of a hermitian matrix and $\sigma_\nu^*|E \in \mathrm{Gal}(E/L)$. If $x \in L$ then

$$x = \sigma_\nu^*(x) = \nu^{-1} {}^t x \nu = \nu^{-1} J_n x J_n \nu = (J_n \nu)^{-1} x (J_n \nu).$$

So $J_n \nu$ centralizes L . Since $J_n \nu$ also commutes with $\sqrt{\tau}$, it follows that $J_n \nu$ centralizes E . Hence $J_n \nu \in E^\times$ or, in other words, $\nu \in J_n E^\times$.

Now suppose $x \in E^\times$ and let $\nu = J_n x$. Then ν is a scalar multiple of a hermitian matrix if and only if there exists $z \in F^\times$ such that $z\nu$ is hermitian. But $z\nu = zJx$ and $(z\nu)^* = \bar{z}\nu^* = \bar{z}x^*J = \bar{z}J\bar{x}$. Hence, ν is a scalar multiple of a hermitian matrix exactly when there exists $z \in F^\times$ such that $zx = \bar{z}\bar{x}$ or, in other words, $zx \in L$. So ν is a scalar multiple of a hermitian matrix precisely when $x \in L^\times F^\times$.

Assume $x \in L^\times F^\times$ and let $\nu = J_n x$. If $u \in L$ then $\sigma_\nu^*(u) = \nu^{-1} \cdot {}^t u \cdot \nu = \nu^{-1} J_n u J_n \nu = x^{-1} u x = u$. In addition, $\sigma_\nu^*(\sqrt{\tau}) = -\sqrt{\tau}$. Hence, σ_ν^* is the nontrivial element of $\mathrm{Gal}(E/L)$. $\square$

4.4. Restriction and extension of involutions. Our definition of “orthogonal involution of G ” may be rephrased as follows: an F -automorphism of $\mathbf{G} = \mathrm{GL}_n$ is an orthogonal involution of $G = \mathrm{GL}_n(F)$ if it has the form $\theta_\nu(g) = \sigma_\nu(g^{-1})$ for

some symmetric matrix $\nu \in G$. Similarly, if F/F' is quadratic, we say that an F' -automorphism of $\mathbf{G}$ is a “unitary involution of G ” if it has the form $\theta_\nu(g) = \sigma_\nu^*(g^{-1})$ for some $\nu \in G$ that is a scalar multiple of a hermitian matrix.

Suppose L is an extension of F of degree $r < n$ and suppose G' is a suitable subgroup of G isomorphic to $\mathrm{GL}_r(L)$. We now consider the problem of restricting orthogonal and unitary involutions of G to orthogonal and unitary involutions of G' . We start with restrictions of orthogonal involutions:

Proposition 4.15. *Let L be an intermediate field of E/F with $r = [L : F]$ and $s = n/r = [E : L]$. Suppose L is embedded in $\mathrm{M}_r(F)$ via a J_r -symmetric embedding and suppose E is embedded in $\mathrm{M}_s(L)$ via a J_s -symmetric embedding. Let $G = \mathrm{GL}_n(F)$ and $G' = \mathrm{GL}_s(L)$.*

- (1) *For $\nu \in G$, the following conditions are equivalent:*
 (a) *${}^t\nu = \nu$ and $\sigma_\nu(x) = x$ for all $x \in L$.*
 (b) *The matrix $\nu' = J_r^s \nu$ lies in G' and, viewed as an element of G' , it is symmetric.*

If (a) and (b) hold then $\sigma_\nu|_{\mathrm{M}_s(L)} = \sigma_{\nu'}$ and

$$\det_G(\nu) = (-1)^{n(r-1)/2} N_{L/F}(\det_{G'}(\nu')).$$

- (2) *Assume L is a quadratic extension $L'[\sqrt{\tau}]$ of an intermediate field L' of L/F . Embed L in $\mathrm{M}_2(L')$ using the J_2 -symmetric embedding*

$$x + y\sqrt{\tau} = \begin{pmatrix} x & y\tau \\ y & x \end{pmatrix},$$

for all $x, y \in L' \subset \mathrm{M}_{r/2}(F)$, with L' embedded in $\mathrm{M}_{r/2}(F)$ using a $J_{r/2}$ -symmetric embedding. Let $\beta = \begin{pmatrix} -\tau J_{r/2} & 0 \\ 0 & J_{r/2} \end{pmatrix}$ and $\gamma = \beta \oplus \cdots \oplus \beta \in G$.

Let $z \mapsto \bar{z}$ be the nontrivial Galois automorphism of L/L' . Then for $\nu \in G$ the following conditions are equivalent:

- (a) *${}^t\nu = \nu$ and $\sigma_\nu(x) = \bar{x}$ for all $x \in L$.*
 (b) *The matrix $\nu' = \gamma \nu$ lies in G' and, viewed as an element of G' , it is hermitian with respect to L/L' .*

If (a) and (b) hold then $\sigma_\nu|_{\mathrm{M}_s(L)} = \sigma_{\nu'}^$ and*

$$\det_G(\nu) = (-1)^{n/2} N_{L'/F}(\tau)^s N_{L/F}(\det_{G'}(\nu')).$$

Proof. Our proof builds on the proof of Lemma 4.4 and we use some of the same identities. As in the proof of Lemma 4.4, if x is a matrix with entries in F , we let ${}^t x$ denote the transpose of x . If x is a matrix with entries in L , we let ${}^T x$ denote the transpose. Since L is embedded in $\mathrm{M}_r(F)$, a matrix with entries in L will have both types of transpose and if $x \in \mathrm{M}_s(L)$ then these transposes are related by

$${}^t x = J_r^s {}^T x J_r^s.$$

Assume $\nu \in G$ and write ν as an s -by- s block matrix in which the ij -th block ν_{ij} lies in $\mathrm{M}_r(F)$. Condition 1(a) is equivalent to saying that whenever $1 \leq i, j \leq s$, we have ${}^t \nu_{ji} = \nu_{ij}$ and ${}^t x \nu_{ij} = \nu_{ij} x$, for all $x \in L$. But for $x \in L$, we have ${}^t x = J_r {}^T x J_r$. It is now easy to see that the following conditions are equivalent:

- ${}^t x \nu_{ij} = \nu_{ij} x$, for all $x \in L$,
- $J_r x J_r \nu_{ij} = \nu_{ij} x$, for all $x \in L$,
- $J_r \nu_{ij}$ centralizes L ,
- $J_r \nu_{ij} \in L$.

So condition 1(a) is equivalent to saying ${}^t\nu_{ji} = \nu_{ij}$ for all i, j and $J_r^s \nu \in G'$. But if $J_r^s \nu \in G'$ then ${}^t\nu_{ji} = ({}^t\nu_{ji} J_r) J_r = {}^t(J_r \nu_{ji}) J_r = J_r(J_r \nu_{ji}) = \nu_{ji}$. It follows that condition 1(a) is equivalent to condition 1(b).

Now assume conditions 1(a) and 1(b) are satisfied and $x \in M_s(L)$. Then we have

$$\sigma_\nu(x) = \nu^{-1} {}^t x \nu = \nu'^{-1} J_r^s {}^t x J_r^s \nu' = \nu'^{-1} {}^T x \nu' = \sigma_{\nu'}(x).$$

Therefore, $\sigma_\nu|_{M_s(L)} = \sigma_{\nu'}$. The determinant identity follows from the transitivity of norms formula in §7.4 of [J1]. More specifically, we have

$$\begin{aligned} N_{L/F}(\det_{G'}(\nu')) &= \det_G(\nu') = \det_G(J_r^s) \det_G(\nu) \\ &= ((-1)^{r(r-1)/2})^s \det_G(\nu) \\ &= (-1)^{n(r-1)/2} \det_G(\nu). \end{aligned}$$

We next consider the proof of assertion 2. Let

$$\varepsilon = \begin{pmatrix} 1_{r/2} & 0 \\ 0 & -1_{r/2} \end{pmatrix}$$

and observe that $\bar{z} = \varepsilon z \varepsilon$ for all $z \in L$.

Assume $\nu \in G$ and write ν as an s -by- s block matrix (ν_{ij}) with $\nu_{ij} \in M_r(F)$. Condition 2(a) says ${}^t\nu_{ji} = \nu_{ij}$ and ${}^t x \nu_{ij} = \nu_{ij} \varepsilon x \varepsilon$, for all $x \in L$ and all i, j . The following conditions are easily seen to be equivalent:

- ${}^t x \nu_{ij} = \nu_{ij} \varepsilon x \varepsilon$, for all $x \in L$,
- $x J_r \nu_{ij} \varepsilon = J_r \nu_{ij} \varepsilon x$, for all $x \in L$,
- $J_r \nu_{ij} \varepsilon$ centralizes L ,
- $J_r \nu_{ij} \varepsilon \in L$,
- $\varepsilon J_r \nu_{ij} \in L$,
- $\sqrt{\tau} \varepsilon J_r \nu_{ij} \in L$.

Since

$$\sqrt{\tau} \varepsilon J_r = \begin{pmatrix} 0 & \tau \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1_{r/2} & 0 \\ 0 & -1_{r/2} \end{pmatrix} \begin{pmatrix} 0 & J_{r/2} \\ J_{r/2} & 0 \end{pmatrix} = \beta,$$

condition 2(a) is equivalent to saying ν is symmetric and $\nu' = \gamma \nu \in G'$. But if ν is symmetric and $\nu' \in G'$ then

$$\begin{aligned} \overline{\nu'_{ij}} &= \varepsilon \nu'_{ij} \varepsilon = \varepsilon \beta \nu_{ij} \varepsilon = \varepsilon \beta {}^t \nu_{ji} \varepsilon = \varepsilon \beta ({}^t \nu_{ji} {}^t \beta) {}^t \beta^{-1} \varepsilon \\ &= \varepsilon \beta {}^t \nu'_{ji} {}^t \beta^{-1} \varepsilon = \varepsilon \beta J_r \nu'_{ji} J_r {}^t \beta^{-1} \varepsilon = -\sqrt{\tau} \nu'_{ji} J_r {}^t \beta^{-1} \varepsilon \\ &= -\nu'_{ji} \sqrt{\tau} J_r {}^t \beta^{-1} \varepsilon = -\nu'_{ji} \sqrt{\tau} J_r {}^t \sqrt{\tau}^{-1} \varepsilon J_r \varepsilon \\ &= \nu'_{ji} \sqrt{\tau} J_r {}^t \sqrt{\tau}^{-1} J_r = \nu'_{ji} \sqrt{\tau} \sqrt{\tau}^{-1} = \nu'_{ji} \end{aligned}$$

for all i, j . It follows that condition 2(a) is equivalent to condition 2(b).

Now suppose $x \in M_s(L)$. Using block matrices in $GL_s(M_r(F)) = G$, define matrices $\xi = \varepsilon \oplus \cdots \oplus \varepsilon$ and $\zeta = \sqrt{\tau} \oplus \cdots \oplus \sqrt{\tau}$ in G . Then

$$\begin{aligned} \sigma_\nu(x) &= \nu^{-1} {}^t x \nu = \nu^{-1} J_r^s {}^T x J_r^s \nu = \nu^{-1} J_r^s \xi {}^T \bar{x} \xi J_r^s \nu \\ &= \nu^{-1} J_r^s \xi \zeta^{-1} {}^T \bar{x} \zeta \xi J_r^s \nu = \nu'^{-1} {}^T \bar{x} \nu' = \sigma_{\nu'}(x). \end{aligned}$$

The verification of the determinant formula is similar to the previous determinant formula, except that the determinant of J_r^s is replaced by

$$\begin{aligned}
 \det_G(\gamma) &= \det_{\mathrm{GL}_r(F)}(\beta)^s \\
 &= \det_{\mathrm{GL}_{r/2}(F)}(J_{r/2})^{2s} \det_{\mathrm{GL}_{r/2}(F)}(-\tau)^s \\
 &= (-1)^{(r/2)((r/2)-1)s} N_{L'/F}(-\tau)^s \\
 &= (-1)^{(n/2)((r/2)-1)} (-1)^{n/2} N_{L'/F}(\tau)^s \\
 &= (-1)^{(nr)/4} N_{L'/F}(\tau)^s \\
 &= (-1)^{s(r/2)^2} N_{L'/F}(\tau)^s \\
 &= (-1)^{sr/2} N_{L'/F}(\tau)^s \\
 &= (-1)^{n/2} N_{L'/F}(\tau)^s. \quad \square
 \end{aligned}$$

We now consider restrictions of unitary involutions:

Proposition 4.16. *Assume F/F' is quadratic and choose $\tau \in F'$ so that $F = F'[\sqrt{\tau}]$. Assume L' is a degree r extension of F' that is embedded in $M_r(F')$ via a J_r -symmetric embedding. Assume E' is a degree s extension of L' that is embedded in $M_s(L')$ via a J_s -symmetric embedding. Let $n = rs$.*

Assume $E' \cap F = F'$ and let E be the degree n extension of F given by $E = E'F = E'[\sqrt{\tau}]$. Embed E in $\mathfrak{g} = M_n(F)$ by extending scalars from F' to F . (In other words, given $x, y \in E'$, identify the element $x + y\sqrt{\tau} \in E$ with an element of $M_n(F)$ by viewing x and y as elements of $M_s(L') \subset M_s(M_r(F')) = M_n(F')$ and $\sqrt{\tau}$ as a scalar matrix in $M_n(F)$.)

Let $L = L'[\sqrt{\tau}]$. Let $G = \mathrm{GL}_n(F)$ and $G' = \mathrm{GL}_s(L)$. Then for $\nu \in G$ the following conditions are equivalent:

- (a) ν is a hermitian matrix and $\sigma_\nu^*|L \in \mathrm{Gal}(L/L')$.
- (b) The matrix $\nu' = J_r^s \nu$ lies in G' and, viewed as an element of G' , it is hermitian.

If (a) and (b) hold then $\sigma_\nu^*|M_s(L) = \sigma_{\nu'}^*$ and

$$\det_G(\nu) = (-1)^{n(r-1)/2} N_{L/F}(\det_{G'}(\nu')).$$

Proof. Assume $\nu \in G$ and write ν as an s -by- s block matrix in which the ij -th block ν_{ij} lies in $M_r(F)$. Then ν is hermitian precisely when $\nu_{ji}^* = \nu_{ij}$ whenever $1 \leq i, j \leq s$. On the other hand, if ν is hermitian then $\sigma_\nu^*|L'$ is trivial precisely when $J_r \nu_{ij}$ centralizes L' for all i, j . But since $J_r \nu_{ij}$ automatically commutes with $\sqrt{\tau}$, to say that $J_r \nu_{ij}$ centralizes L' is the same as saying it centralizes L which, in turn, is the same as saying $J_r \nu_{ij} \in L$.

So condition (a) is equivalent to saying $\nu_{ji}^* = \nu_{ij}$ for all i, j and $J_r^s \nu \in G'$. But if $J_r^s \nu \in G'$ then $\nu_{ji}^* = (\nu_{ji}^* J_r) J_r = (J_r \nu_{ji})^* J_r = J_r (J_r \overline{\nu_{ji}}) = \overline{\nu_{ji}}$. It follows that condition (a) is equivalent to condition (b).

Now assume conditions (a) and (b) are satisfied and $x \in M_s(L)$. Then we have

$$\sigma_\nu^*(x) = \nu^{-1} x^* \nu = \nu'^{-1} J_r^s x^* J_r^s \nu' = \nu'^{-1} x^\bullet \nu' = \sigma_{\nu'}(x),$$

where x^* is the conjugate transpose of x in $\mathfrak{g}$ and $x^\bullet$ is the conjugate transpose of x in $M_s(L)$. Therefore, $\sigma_\nu|M_s(L) = \sigma_{\nu'}$. The determinant identity is proved in a similar fashion to the proof to the corresponding identity in Proposition 4.15. $\square$

5. ORTHOGONAL SIMILITUDES

5.1. Generalities. In this section, G will denote a general linear group $\mathrm{GL}_n(F)$, with $n > 1$, where F is a field whose characteristic is not 2. As in §2, we really only need to study the case in which F is either a finite field or a finite extension of some p -adic field $\mathbb{Q}_p$, but our initial results hold for arbitrary F .

We are interested in special cases of a very general and basic problem involving orthogonal similitude groups. Fix a symmetric matrix $\nu \in G$ and define an orthogonal involution θ by $\theta(g) = \nu^{-1} {}^t g^{-1} \nu$. As usual, G^θ will denote the orthogonal group comprised of the fixed points of θ in G and, in addition, G_θ will denote the orthogonal similitude group. Thus G_θ consists of the elements $g \in G$ such that $g\theta(g)^{-1}$ lies in the center Z of G . The similitude ratio defines a homomorphism $\mu : G_\theta \rightarrow Z : g \mapsto g\theta(g)^{-1}$ and yields exact sequences

$$1 \rightarrow G^\theta \rightarrow G_\theta \rightarrow \mu(G_\theta) \rightarrow 1$$

and

$$1 \rightarrow G^\theta/Z^\theta \rightarrow G_\theta/Z \rightarrow \mu(G_\theta)/\mu(Z) \rightarrow 1$$

and isomorphisms

$$\begin{aligned} G_\theta/G^\theta &\cong \mu(G_\theta), \\ G_\theta/(ZG^\theta) &\cong \mu(G_\theta)/\mu(Z). \end{aligned}$$

We are interested in special cases of the following:

Problem 5.1. Given a subgroup H of G , compute the abelian group

$$G_\theta/((H \cap G_\theta)ZG^\theta).$$

We actually only need to know the order of the latter groups or, in other words, the constants

$$m_H(\theta) := [G_\theta : (H \cap G_\theta)ZG^\theta].$$

Since the similitude ratio gives an isomorphism

$$G_\theta/((H \cap G_\theta)ZG^\theta) \cong \mu(G_\theta)/\mu((H \cap G_\theta)Z),$$

we have

$$m_H(\theta) = [\mu(G_\theta) : \mu((H \cap G_\theta)Z)].$$

There is one special class of examples of particular interest. Suppose E is a degree n extension of F that is embedded in $M_n(F)$ via an F -linear embedding. Let T be the torus $E^\times$ in G and assume that T is θ -split in the sense that $\theta(t) = t^{-1}$, for all $t \in T$. In this situation, we are interested in computing $m_T(\theta)$. It will turn out that $m_T(\theta)$ depends on the number of quadratic extensions of F that are contained in E .

Definition 5.2. The involution θ is a **distinguishing involution** if there exists a degree n field extension E of F that is embedded in $M_n(F)$ via an F -embedding such that the torus $T = E^\times$ is θ -split.

Roughly speaking, the involutions that are not distinguishing involutions do not contribute to the theory of distinguished representations of G (at least in the setting we consider). Thus we assume that our involution θ is a distinguishing involution and we assume that we have fixed E and T as just described.

If F' is any extension of F , then as in §3, we let

$$y_{F'/F} = 1 + \#\{\text{quadratic extensions of } F \text{ contained in } F'\}.$$

In particular, taking $\overline{F}$ to be an algebraic closure of F , we have

$$y_{\overline{F}/F} = [F^\times : (F^\times)^2],$$

since a nontrivial square class $x(F^\times)^2$ corresponds to the quadratic extension $F[\sqrt{x}]$. Similarly, for arbitrary F' we have

$$y_{F'/F} = [(F'^\times)^2 \cap F^\times : (F^\times)^2].$$

We now enumerate some elementary facts that apply to general F :

- Lemma 5.3.** (1) $\mu(Z) = Z^2 = (F^\times)^2$.
 (2) $\mu(T \cap G_\theta) = (E^\times)^2 \cap F^\times$.
 (3) $m_H(\theta)$ is a divisor of $y_{\overline{F}/F}$, for all H .
 (4) If $H_1 \subset H_2$ then $m_{H_2}(\theta)$ is a divisor of $m_{H_1}(\theta)$.
 (5) $m_Z(\theta) = y_{E/F} \cdot m_T(\theta)$.

The proofs of these facts are obvious. The next result is standard, but we include a proof for completeness.

Lemma 5.4. If n is odd then $\mu((H \cap G_\theta)Z) = Z^2 = (F^\times)^2$ and $m_H(\theta) = 1$ for all H .

Proof. If $z \in Z$ then $\det z = z^n \equiv z \pmod{Z^2}$. In particular, if $g \in G_\theta$, we may take $z = \mu(g)$. Since $\det \mu(g) \in Z^2$, we deduce that $\mu(g) \in Z^2$. Thus, for all H , we have

$$Z^2 \subseteq \mu((H \cap G_\theta)Z) \subseteq \mu(G_\theta) \subseteq Z^2$$

which implies $\mu((H \cap G_\theta)Z) = Z^2$ and $m_H(\theta) = 1$. □

Lemma 5.5. If n even and $\theta = \theta_J$ is associated to

$$J = \begin{pmatrix} & & 1 \\ & \ddots & \\ 1 & & \end{pmatrix}$$

then $\mu(G_\theta) = Z = F^\times$. Therefore, $m_Z(\theta) = y_{\overline{F}/F}$ and $m_T(\theta) = y_{\overline{F}/F}/y_{E/F}$.

Proof. Our claim follows from the fact that if $z \in F^\times$ and

$$g_z = \text{diag}(z, \dots, z, 1, \dots, 1),$$

where the first $n/2$ diagonal entries equal z , then $\mu(g_z) = z$. □

5.2. Finite fields. When F is a finite field of odd characteristic, we have the following consequence of Lemma 5.3:

Lemma 5.6. Suppose q is a power of an odd prime. If $F = \mathbb{F}_q$ and $E = \mathbb{F}_{q^2}$ then $y_{\overline{F}/F} = 2$ and

- (1) $m_Z(\theta) = y_{E/F} = \begin{cases} 1, & \text{if } n \text{ is odd,} \\ 2, & \text{if } n \text{ is even.} \end{cases}$
 (2) $m_T(\theta) = 1$.
 (3) $\mu(T \cap G_\theta) = (\mathbb{F}_{q^n}^\times)^2 \cap \mathbb{F}_q^\times = \begin{cases} (\mathbb{F}_q^\times)^2, & \text{if } n \text{ is odd,} \\ \mathbb{F}_q^\times, & \text{if } n \text{ is even.} \end{cases}$

Proof. We observe that $y_{\overline{F}/F} = 2$, since $(\mathbb{F}_q^\times)^2$ has index 2 in $\mathbb{F}_q^\times$. Statement (3) follows from this together with Lemma 5.3 (2) and it implies

$$y_{E/F} = [(\mathbb{F}_{q^2}^\times)^2 \cap \mathbb{F}_q^\times : (\mathbb{F}_q^\times)^2] = \begin{cases} 1, & \text{if } n \text{ is odd,} \\ 2, & \text{if } n \text{ is even.} \end{cases}$$

Statements (1) and (2) follow from Lemma 5.4 when n is odd and they follow from parts (3) and (5) of Lemma 5.3 when n is even. $\square$

5.3. p -adic fields.

Proposition 5.7. *If F is a finite extension of $\mathbb{Q}_p$ with $p \neq 2$ then $y_{\overline{F}/F} = 4$ and:*

- (1) *If $y_{E/F} = 1$ then n is odd and $m_H(\theta) = 1$ for all H .*
- (2) *If $y_{E/F} = 2$ and L is the unique quadratic extension of F in E then $\mu(T \cap G_\theta) = (E^\times)^2 \cap F^\times = (L^\times)^2 \cap F^\times$ and*
 - (a) *If θ is in the G -orbit of θ_J then $\mu(G_\theta) = Z = F^\times$ and $m_Z(\theta) = 4$ and $m_T(\theta) = 2$.*
 - (b) *Let $\theta = \theta_\nu$ be an orthogonal involution of G associated to a symmetric matrix $\nu \in G$ such that $(-1)^{n/2} \det \nu \in N_{L/F}(L^\times) - (F^\times)^2$. Then $\mu(G_\theta) = \mu(T \cap G_\theta)$ and $m_Z(\theta) = 2$ and $m_T(\theta) = 1$.*
- (3) *If $y_{E/F} = 4$ then $m_Z(\theta) = 4$ and $m_T(\theta) = 1$.*

Proof. Since p is odd, $[F^\times : (F^\times)^2] = 4$ and hence $y_{\overline{F}/F} = 4$. This implies that $y_{E/F}$ is a divisor of 4. Lemma 3.3 implies that $y_{E/F} = 1$ precisely when n is odd. Thus statement (1) follows from Lemma 5.4. Statement (3) follows from part (4) of Lemma 5.3.

Now assume $y_{E/F} = 2$. We have $\mu(T \cap G_\theta) = (E^\times)^2 \cap F^\times$, according to part (2) of Lemma 5.3. Suppose $\alpha \in (E^\times)^2 \cap F^\times$ and $\alpha \notin (F^\times)^2$. Choose $\beta \in E^\times$ such that $\alpha = \beta^2$. The field $F[\beta]$ is a quadratic extension of F contained in E and hence it equals L . This implies $\alpha \in (L^\times)^2 \cap F^\times$ and hence $(E^\times)^2 \cap F^\times = (L^\times)^2 \cap F^\times$.

Statement 2(a) is a special case of Lemma 5.5. Assume now we are in the setting of statement 2(b). Because ν and J have different discriminants, the G -orbit of θ is determined by the discriminant of ν (see Proposition 2.6). Since we are free to replace θ by another element of its G -orbit, we may assume that ν is a diagonal matrix of the form

$$\nu = \text{diag}(1, \dots, 1, \tau),$$

with $\tau \in F^\times$.

We wish to determine the image of the similitude homomorphism $\mu : G_\theta \rightarrow F^\times$. This is equivalent to determining the set of all $z \in F^\times$ such that the equation

$$g \nu^{-1} {}^t g \nu = z$$

is solvable for $g \in G$. Let us rewrite the latter equation as

$$g(z\nu)^{-1} {}^t g = \nu^{-1}.$$

Let $e_1, \dots, e_n$ be the rows of g . View these rows as vectors in the quadratic space $V = F^n$ with inner product associated to the diagonal matrix $(z\nu)^{-1}$.

Let us consider the Hasse invariant of V (as defined in Definition 2.2). To compute the Hasse invariant, one needs to diagonalize the quadratic form on V or, in other words, one needs to choose an orthogonal basis. If one uses the basis

$e_1, \dots, e_n$ just specified then one obtains $\text{Hasse}(V) = 1$. On the other hand, if one uses the standard basis of F^n one gets

$$\begin{aligned} \text{Hasse}(V) &= (z, z)^{(n-1)(n-2)/2} (z, z\tau)^{n-1} \\ &= (z, z)^{(n-2)/2} (z, z\tau) \\ &= (z, z)^{n/2} (z, \tau) \\ &= (z, -1)^{n/2} (z, \tau) \\ &= (z, (-1)^{n/2} \tau) \\ &= (z, (-1)^{n/2} \det \nu). \end{aligned}$$

Therefore if $z \in \mu(G_\theta)$ then $(z, (-1)^{n/2} \det \nu) = 1$ or, in other words, $z \in N_{K/F}(K^\times)$, where $K = F[\sqrt{\beta}]$ and $\beta = (-1)^{n/2} \det \nu$. Note that since we assumed ν and J have distinct discriminants, we know that β cannot be a square in $F^\times$.

We observe that the sets $((K^\times)^2 \cap F^\times) - (F^\times)^2$ and $N_{L/F}(L^\times) - (F^\times)^2$ each comprise a single square class in $F^\times / (F^\times)^2$. Since these square classes both contain β , they must be identical. So we have $(K^\times)^2 \cap F^\times = N_{L/F}(L^\times)$. But the latter condition is equivalent to the condition $\text{Hilbert}(\alpha, \beta) = 1$, where $L = F[\sqrt{\alpha}]$ for some square root $\sqrt{\alpha}$ of some nonsquare α in $F^\times$. By symmetry of the Hilbert symbol, we deduce $(L^\times)^2 \cap F^\times = N_{K/F}(K^\times)$. Thus $z \in (L^\times)^2 \cap F^\times = \mu(T \cap G_\theta)$. Since we have shown $\mu(T \cap G_\theta) \subseteq \mu(G_\theta) \subseteq \mu(T \cap G_\theta)$, we deduce that $\mu(G_\theta) = \mu(T \cap G_\theta)$. Consequently, $m_T(\theta) = 1$ and, according to part (5) of Lemma 5.3, $m_Z(\theta) = 2$. This completes the proof of statement 2(b). $\square$

Lemma 5.8. *Assume F is a finite extension of $\mathbb{Q}_p$ with $p \neq 2$. Let E be a tamely ramified degree n extension of F that contains a unique quadratic extension L of F . Let E_0 be an intermediate field of E/F such that E/E_0 is unramified. Embed E in $M_{n_0}(E_0)$, with $n_0 = [E : E_0]$, via a J -symmetric embedding and embed E_0 in $M_{m_0}(F)$, with $m_0 = [E_0 : F]$, via a J -symmetric embedding. Let $H = E_0^\times \text{GL}_{n_0}(\mathfrak{O}_{E_0})$ and assume θ is the orthogonal involution θ_J of $G = \text{GL}_n(F)$. Then $m_H(\theta) = m_T(\theta) = 2$.*

Proof. Assume the hypotheses in the statement of the lemma. In particular, we assume that $\theta = \theta_{J_n}$. According to part 1(a) of Proposition 4.15, the restriction of θ to $G^0 = \text{GL}_{n_0}(E_0)$ is the orthogonal involution $\theta_0 = \theta_{J_{n_0}}$ of G^0 associated to J_{n_0} . Let $\mu_0 : G_{\theta_0}^0 \rightarrow E_0^\times$ be the similitude homomorphism associated to θ_0 .

Suppose $h \in \text{GL}_{n_0}(\mathfrak{O}_{E_0})$, $z \in E_0^\times$ and $g = hz$. Then $g \in G_{\theta_0}^0$ if and only if $h \in G_{\theta_0}^0$. If $h \in \text{GL}_{n_0}(\mathfrak{O}_{E_0}) \cap G_{\theta_0}^0$ then, taking determinants, we see that $\mu_0(h) \in \mathfrak{O}_{E_0}^\times$.

Arguing as in the proof of Lemma 5.4, we see that when n_0 is odd we have $\mu_0(\text{GL}_{n_0}(\mathfrak{O}_{E_0}) \cap G_{\theta_0}^0) = (\mathfrak{O}_{E_0}^\times)^2$. Arguing as in the proof of Lemma 5.5, we see that when n_0 is even we have $\mu_0(\text{GL}_{n_0}(\mathfrak{O}_{E_0}) \cap G_{\theta_0}^0) = \mathfrak{O}_{E_0}^\times$. It follows that

$$\mu_0(H \cap G_{\theta_0}^0) = \begin{cases} (E_0^\times)^2, & \text{if } n_0 \text{ is odd,} \\ \mathfrak{O}_{E_0}^\times (E_0^\times)^2, & \text{if } n_0 \text{ is even.} \end{cases}$$

Thus

$$\mu(H \cap G_\theta) = \mu_0(H \cap G_{\theta_0}^0) \cap F^\times = \begin{cases} (E_0^\times)^2 \cap F^\times, & \text{if } n_0 \text{ is odd,} \\ \mathfrak{O}_{E_0}^\times (E_0^\times)^2 \cap F^\times, & \text{if } n_0 \text{ is even.} \end{cases}$$

On the other hand, $m_H(\theta) = [\mu(G_\theta) : \mu(H \cap G_\theta)]$ and, according to Lemma 5.5, we have $\mu(G_\theta) = F^\times$.

If n_0 is odd then $y_{E_0/F}$ must be 2, according to Lemma 3.3, and thus

$$m_H(\theta) = [F^\times : (E_0^\times)^2 \cap F^\times] = \frac{4}{y_{E_0/F}} = 2.$$

Now suppose n_0 is even. Then

$$m_H(\theta) = [F^\times : \mathfrak{D}_{E_0}^\times (E_0^\times)^2 \cap F^\times].$$

We observe that E must contain an unramified quadratic extension of F and thus L/F is unramified. Since L is the unique quadratic extension of F in E , we have $(E^\times)^2 \cap F^\times = (L^\times)^2 \cap F^\times$. Since E contains the unique unramified quadratic extension of E_0 , it follows that $\mathfrak{D}_{E_0}^\times \subset (E^\times)^2$. Since L is an unramified quadratic extension of F , it must be the case that $(L^\times)^2 \cap F^\times = \mathfrak{D}_F^\times (F^\times)^2$. Therefore,

$$(L^\times)^2 \cap F^\times = \mathfrak{D}_F^\times (F^\times)^2 \subseteq \mathfrak{D}_{E_0}^\times (E_0^\times)^2 \cap F^\times \subseteq (E^\times)^2 \cap F^\times = (L^\times)^2 \cap F^\times.$$

We now have

$$m_H(\theta) = [F^\times : (L^\times)^2 \cap F^\times] = 2.$$

Our assertion now follows from part 2(a) of Proposition 5.7. $\square$

6. SPLIT T -ORBITS OF ORTHOGONAL INVOLUTIONS

6.1. Generalities. Let E/F be a (finite) degree n field extension. Embed E in $M_n(F)$ via a J -symmetric embedding. Let $G = \mathrm{GL}_n(F)$ and $T = E^\times$.

Definition 6.1. A **split T -orbit** is a T -orbit of orthogonal involutions of G such that T is θ -split.

The main objective of this section is to study the split T -orbits in G , especially in the following two cases:

- F is a finite extension of $\mathbb{Q}_p$ for some odd prime p and E/F is tamely ramified.
- E and F are finite fields of odd order.

In particular, we would like to determine the number of split T -orbits that lie within a given G -orbit of orthogonal involutions.

Let

$$Y_{E/F} = E^\times / ((E^\times)^2 F^\times).$$

Then the cardinality of $Y_{E/F}$ is just the number $y_{E/F}$ defined in §3. Let $\mathcal{O}^T$ denote the set of split T -orbits of orthogonal involutions of G .

The following generalizes the statement of Lemma 5.6 of [HL1], but the proof is identical:

Lemma 6.2. *If $[F^\times : (F^\times)^2] = [E^\times : (E^\times)^2] < \infty$ then $y_{E/F} - 1$ is the number of quadratic extensions of F contained in E .*

Let us recall the statement of Corollary 5.5 in [HL1]:

Lemma 6.3. *If E/F is separable then the map*

$$\mu_{E/F} : Y_{E/F} \rightarrow \mathcal{O}^T$$

that sends the coset of $x \in E^\times$ to the orbit of the involution θ_ν with $\nu_{ij} = \mathrm{tr}_{E/F}(x e_i e_j)$ is a bijection.

We will not actually need to use Lemma 6.3 in this paper, but, instead, we use a more convenient variant that uses the theory of J -symmetric embeddings:

Lemma 6.4. *The map*

$$\mu'_{E/F} : Y_{E/F} \rightarrow \mathcal{O}^T$$

that sends the coset of $x \in E^\times$ maps to the orbit of θ_{Jx} is a bijection. The involution θ_J lies in a split T -orbit.

Proof. According to Proposition 4.3, the set of symmetric matrices ν in G such that T is θ_ν -split is identical to $J_n T$. If $x_1, x_2 \in T$ then $\theta_{Jx_1} = \theta_{Jx_2}$, precisely when $Jx_2x_1^{-1}J \in F^\times$ or, equivalently, $x_2x_1^{-1} \in F^\times$. This shows that $xF^\times \mapsto \theta_{Jx}$ determines a bijection between $E^\times/F^\times$ and the set of orthogonal involutions θ of G such that T is θ -split.

Now suppose $x, y \in T$. Then $(y \cdot \theta_{Jx})(g) = yx^{-1}J^t y^t g^{-1} t y^{-1} J x y^{-1} = x^{-1}y^2 J^t g^{-1} J x y^{-2} = \theta_{Jxy^{-2}}(g)$, for all $g \in G$. Interpreting the identity $y \cdot \theta_{Jx} = \theta_{Jxy^{-2}}$ as a T -equivariance property of the aforementioned bijection, we deduce that $\mu'_{E/F}$ is a well-defined bijection. $\square$

Lemma 6.4 may appear to apply to any finite extension, however, we stress that we are assuming throughout this section that E has a J -symmetric embedding in $M_n(F)$.

6.2. Finite fields. Assume E/F is an extension of finite fields. From Lemma 2.5, Lemma 6.2, and Lemma 6.3 (or Lemma 6.4), we see that

$$\begin{aligned} \#\mathcal{O}^T &= y_{E/F} = \begin{cases} 1, & \text{if } n \text{ is odd,} \\ 2, & \text{if } n \text{ is even,} \end{cases} \\ &= \#\{G\text{-orbits of orthogonal involutions}\}. \end{aligned}$$

Lemma 6.5. *Each G -orbit of orthogonal involutions contains a unique split T -orbit.*

Proof. When n is odd, the unique split T -orbit is obviously contained in the unique G -orbit.

Now suppose n is even. If $\nu \in G$ is symmetric then the G -orbit of θ_ν is characterized by the discriminant of ν , Lemma 2.5. On the other hand, according to Proposition 4.3, θ_ν lies in a split T -orbit precisely when $\nu \in JT$. Suppose this is the case, that is, $\nu = Jx$ for some $x \in T$. The determinant of x is $N_{E/F}(x)$. But since $N_{E/F}(E^\times) = F^\times$, we see that there must be a single split T -orbit in each of the two G -orbits. $\square$

6.3. p -adic fields. In this section, we assume that E/F is a tamely ramified degree n extension of fields that are finite extensions of $\mathbb{Q}_p$, with $p \neq 2$.

According to Lemma 6.3 (or Lemma 6.4) and Lemma 6.2, we have

$$\#\mathcal{O}^T = y_{E/F} = 1 + \#\{\text{quadratic extensions of } F \text{ contained in } E\}.$$

Recall from §1.3 the inventory of G -orbits of orthogonal involutions of G :

- Θ_J is the G -orbit of θ_J ,
- if n is odd then Θ_{nqs} is only other G -orbit besides Θ_J ,
- if n is even and greater than two, Θ_{nqs} denotes the G -orbit consisting of orthogonal involutions θ_ν where ν not similar to J but has the same discriminant,

- if n is even there are three additional G -orbits of orthogonal involutions and they correspond to the three possible discriminants other than the discriminant of J .

Having described the G -orbits and enumerated the split T -orbits, we now describe the split T -orbits in more detail and determine in which G -orbits they lie. The main result is:

Proposition 6.6. *The elements of $\mathcal{O}^T$ are described as follows:*

- $y_{E/F} = 1$ (equivalently, n is odd): The T -orbit of θ_J is the only element of $\mathcal{O}^T$.
- $y_{E/F} = 2$: The set $\mathcal{O}^T$ consists of the T -orbit of θ_J and the T -orbit of involutions θ_{Jx} where $x \in E^\times - ((E^\times)^2 F^\times)$. The two T -orbits lie in distinct G -orbits. The discriminants of these orbits are distinct since $\det x = N_{E/F}(x) \in N_{L/F}(L^\times) - (F^\times)^2$, where L is the unique quadratic extension of F contained in E .
- $y_{E/F} = 4$ (equivalently, $Y_{E/F} = E^\times / (E^\times)^2$): Three of the four T -orbits in $\mathcal{O}^T$ lie in Θ_J . Let ϖ_E be a prime element of E such that $\varpi_E^{e(E/F)}$ lies in the maximal unramified extension of F contained in E . Let u be a nonsquare unit in E and let $\nu = Ju\varpi_E$. Then the T -orbit of θ_ν lies in Θ_{nqs} .

Proof. When $y_{E/F} = 1$ or 2 , our assertions follow directly from Lemma 6.4. Therefore, we assume $y_{E/F} = 4$. A set of coset representatives for

$$Y_{E/F} = E^\times / ((E^\times)^2 F^\times) = E^\times / (E^\times)^2$$

is given by $\{1, u, \varpi_E, u\varpi_E\}$, where u is a nonsquare unit in E and ϖ_E is a prime element of E .

We will choose u and ϖ_E as follows: u will be a nonsquare root of unity in E and ϖ_E will be chosen as in Lemma 4.9. Without loss of generality, we may assume we have an embedding as in Lemma 4.9 and we will adopt the notations of this lemma. Note that u and $\varpi_L = \varpi_E^e$ must lie in the maximal unramified extension L of F contained in E , where $e = [E : L]$ and $f = [L : F]$.

Recall from Lemma 3.8 that $N_{E/F}(E^\times) \subset (F^\times)^2$. It follows that all matrices of the form Jx , with $x \in E^\times$, have the same discriminant as J . This means that each split T -orbit must lie in either Θ_J or Θ_{nqs} . The G -orbit of a given split T -orbit is therefore determined by its Hasse invariant.

Obviously, the T -orbit of θ_J lies in Θ_J . According to Lemma 5.9 in [HL1], the Hasse invariant of Ju is trivial and hence θ_{Ju} also lies in Θ_J . It remains to determine the G -orbits containing $\theta_{J\varpi_E}$ and $\theta_{Ju\varpi_E}$. It suffices to compute the Hasse invariants of $J\varpi_E$ and $Ju\varpi_E$. To give a uniform computation of both of these Hasse invariants, we suppose w is either 1 or u and we compute the Hasse invariant of $Jw\varpi_E$.

Let ϖ_F be any prime element in F . Since $y_{E/F} = 4$, we may choose a square root $\sqrt{\varpi_F}$ in E . Then there exists a unit v in E such that $\varpi_E^{e/2} = v\sqrt{\varpi_F}$. Since $\varpi_L = v^2\varpi_F$, we see that $v^2 \in \mathfrak{D}_L^\times$. In fact, $v^2 \in (\mathfrak{D}_L^\times)^2$, since otherwise $L[v]$ would be an unramified quadratic extension of L contained in the totally ramified extension E/L . It follows that $v \in \mathfrak{D}_L^\times$.

Using the explicit form of ϖ_E in Lemma 4.9 and the proof of Lemma 4.5, we see that

$$J_n \varpi_E = J_{(e-1)f} \oplus J_f \varpi_L.$$

Note that since w lies in L it may be viewed as an element of $M_f(F)$ and we have

$$J_n w \varpi_E = J_{(e-1)f} w \oplus J_f \varpi_L w.$$

The matrix $J_f \varpi_L w \varpi_F^{-1} = J_f w v^2$ has the same discriminant and Hasse invariant as $J_f w$. Since $J_f \varpi_L w \varpi_F^{-1}$ must be similar to $J_f w$ and since ϖ_F is a scalar matrix, we deduce that $J_f \varpi_L w$ is similar to $J_f \varpi_F w$.

Comparing discriminants and Hasse invariants, we see that $J_{(e-1)f} w$ is similar to $J_{(e-2)f} w \oplus J_f w$. Likewise, $J_{(e-2)f} w$ and $I_{(e-2)f}$ are similar. It follows that $J w \varpi_E$ has the same Hasse invariant (and discriminant) as $J_f w \oplus J_f w \varpi_F$. Since we are only interested in computing Hasse invariants, we may as well replace $J w \varpi_E$ by $J_f w \oplus J_f w \varpi_F$. Since we have essentially just reduced to the case in which $e = 2$, we will, for simplicity, assume $e = 2$.

There exist units $u_1, \dots, u_f$ in F such that $J_f w$ is similar to the diagonal matrix with diagonal $(u_1, \dots, u_f)$. Thus $J w \varpi_E$ is similar to the diagonal matrix with diagonal

$$(u_1, \dots, u_f, u_1 \varpi_F, \dots, u_f \varpi_F).$$

The Hasse invariant of $J w \varpi_E$ can now be computed using standard properties of the Hilbert symbol, such as the fact that $(a, b) = 1$ when $a, b \in \mathfrak{D}_F^\times$ and $(ab, c) = (a, c)(b, c)$, when $a, b, c \in F^\times$. Using the latter properties, we see that the Hasse invariant is

$$\prod_{i,j} (u_i, u_j \varpi_F) \prod_{i < j} (u_i \varpi_F, u_j \varpi_F).$$

The first product is

$$\prod_{i,j} (u_i, u_j \varpi_F) = \prod_{i,j} (u_i, \varpi_F) = \left(\prod_i (u_i, \varpi_F) \right)^f = 1.$$

Thus the Hasse invariant reduces to:

$$\begin{aligned} \prod_{i < j} (u_i \varpi_F, u_j \varpi_F) &= \prod_{i < j} (u_i, \varpi_F)(u_j, \varpi_F)(\varpi_F, \varpi_F) \\ &= \left(\prod_i (u_i, \varpi_F) \right)^{f-1} (\varpi_F, \varpi_F)^{(f/2)(f-1)} \\ &= (\det(J_f w), \varpi_F)(\varpi_F, \varpi_F)^{f/2} \\ &= ((-1)^{f/2} N_{L/F}(w), \varpi_F)(\varpi_F, \varpi_F)^{f/2} \\ &= ((-\varpi_F)^{f/2} N_{L/F}(w), \varpi_F). \end{aligned}$$

We observe that $N_{L/F}$ determines an isomorphism $\mathfrak{D}_L^\times / (\mathfrak{D}_L^\times)^2 \cong \mathfrak{D}_F^\times / (\mathfrak{D}_F^\times)^2$. Thus $N_{L/F}(u)$ represents the nontrivial coset in $\mathfrak{D}_F^\times / (\mathfrak{D}_F^\times)^2$.

Suppose $f/2$ is even. Then the Hasse invariant reduces to the Hilbert symbol $(N_{L/F}(w), \varpi_F)$. If $w = 1$ this is trivial. Suppose $w = u$. The Hilbert symbol involves solutions to

$$N_{L/F}(u)x^2 + \varpi_F y^2 = z^2.$$

It suffices to consider solutions with $x, y, z \in \mathfrak{D}_F$ such that x, y and z do not all lie in $\mathfrak{P}_F$. Reducing modulo $\mathfrak{P}_F$ yields

$$N_{L/F}(u)x^2 \equiv z^2,$$

where x and z do not both lie in $\mathfrak{P}_F$. Since $N_{L/F}(u)$ is a nonsquare, we deduce that the Hasse invariant is -1 when $f/2$ is even and $w = u$.

Suppose $f/2$ is odd. The Hasse invariant equals the Hilbert symbol $(-\varpi_F N_{L/F}(w), \varpi_F)$. Again, when $w = 1$ the Hilbert symbol is trivial and so we assume $w = u$. The Hilbert symbol involves solutions to

$$-\varpi_F N_{L/F}(u)x^2 + \varpi_F y^2 = z^2.$$

The latter equation has solutions precisely when

$$-N_{L/F}(u)x^2 + y^2 = \varpi_F z^2.$$

Reducing modulo $\mathfrak{P}_F$ as before, we deduce that the Hasse invariant is -1 . Our assertions now follow. $\square$

7. TAME SUPERCUSPIDAL REPRESENTATIONS

7.1. Buildings of general linear groups. We give a streamlined exposition of the theory of the lattice function model for the Bruhat-Tits building of a general linear group over a nonarchimedean local field F . Our primary reference is [BL].

Fix a vector space V of finite dimension n over F and, in this section, let $G = GL(V)$. To develop the desired explicit model for the building of G , we need to fix a valuation $\omega : F \rightarrow \mathbb{R} \cup \{+\infty\}$. We will let γ denote $\omega(\varpi)$, where ϖ is any prime element of F .

Definition 7.1. An **(additive) norm on V (with respect to ω)** is a map $x : V \rightarrow \mathbb{R} \cup \{+\infty\}$ that satisfies:

- $x(v + w) \geq \inf\{x(v), x(w)\}$, for all $v, w \in V$,
- $x(\alpha v) = \omega(\alpha) + x(v)$, for all $\alpha \in F, v \in V$,
- $x(v) = +\infty$ if and only if $v = 0$.

The set $\mathcal{B} = \mathcal{B}(G)$ of all norms on V provides an explicit model for the (extended) Bruhat-Tits building of G . (See Theorem 2.11, Corollary 2.11 in [BT] or Proposition 1.4 in [BL] and the discussion that precedes it.) But there is another model for the building, namely, the lattice function model in [BL], that is more useful for us. Rather than dwell on the norm model, we recall how norms parametrize lattice functions and then we discuss the tools we need in lattice function terms.

Definition 7.2. A **lattice function on V (with respect to ω)** is a map L that assigns to each real number r a lattice L_r in V such that

- if $r \leq s$ then $L_r \supseteq L_s$,
- $\mathfrak{P}_F L_r = L_{r+\gamma}$, for all $r \in \mathbb{R}$,
- $L_r = \bigcap_{t < r} L_t$, for all $r \in \mathbb{R}$.

If $x \in \mathcal{B}$ then there is an associated lattice function $L_x : r \mapsto L_{x,r}$ defined by

$$L_{x,r} = \{v \in V : x(v) \geq r\},$$

for $r \in \mathbb{R}$. This defines a canonical bijection from $\mathcal{B}$ onto the set of lattice functions on V . The inverse map send the lattice function $L : r \mapsto L_r$ to the norm $x_L \in \mathcal{B}$ defined by

$$x_L(v) = \max\{r : v \in L_r\}.$$

(See Proposition 2.4 in [BL].)

The natural action of G on V gives rise to an action of G on the set of lattices in V . This yields an action of G on lattice functions, given by

$$(g \cdot L)_r = gL_r,$$

and this corresponds to the following standard action of G on norms:

$$(g \cdot x)(v) = x(g^{-1}v).$$

We define an equivalence relation on $\mathcal{B}$ by declaring that $x \sim y$ precisely when $x - y$ is a constant. The set $\mathcal{B}_{\text{red}} = \mathcal{B}_{\text{red}}(G)$ of equivalence classes is a model for the reduced Bruhat-Tits building of G . If $x \in \mathcal{B}$, we will let $[x]$ denote the corresponding point in $\mathcal{B}_{\text{red}}$. In the lattice function model, two lattice functions L and L' are equivalent exactly when there is a constant c such that $L'_r = L_{r+c}$, for all $r \in \mathbb{R}$.

In the lattice chain model, the facets in the reduced building are readily apparent, as we now explain. Given a lattice function L , let $L_\bullet$ denote the associated chain of distinct lattices that occur in the image of L . Then $L_\bullet$ is a lattice chain in the following sense:

Definition 7.3. A **lattice chain** on V is a totally ordered (nonempty) chain of lattices in V that is stable under homotheties. Such a lattice chain is determined by a segment:

$$L_0 \supsetneq L_1 \supsetneq \cdots \supsetneq L_{m-1} \supsetneq \mathfrak{P}_F L_0.$$

The number m is called the **period of the lattice chain**.

(Note that in this definition, we do not mean to suggest that a lattice chain comes equipped with a grading by integers or, in particular, a base point L_0 .)

Given $x \in \mathcal{B}$, the lattice chain $L_{x,\bullet}$ is what determines the facet of the image of x in the reduced building $\mathcal{B}_{\text{red}}$. If m is the period of $L_{x,\bullet}$, then $m - 1$ is the dimension of the facet. In particular, to give a vertex in $\mathcal{B}_{\text{red}}$ is equivalent to giving a lattice chain of the form $L_\bullet = \{\mathfrak{P}_F^i L : i \in \mathbb{Z}\}$, where L is some fixed lattice in V . Equivalently, vertices in $\mathcal{B}_{\text{red}}$ correspond to homothety classes of lattices.

We now consider the apartments in $\mathcal{B}$. When we write $c \in \mathbb{R}^n$, we mean c is the element of $\mathbb{R}^n$ which in component form is $(c_1, \dots, c_n)$. Similarly, when we say “let e be a basis of V ,” we mean that e is ordered F -basis $e_1, \dots, e_n$ of V . Given $c \in \mathbb{R}^n$, define $x_e^c \in \mathcal{B}$ by

$$x_e^c \left(\sum_{i=1}^n \alpha_i e_i \right) = \inf_i \{ \omega(\alpha_i) + c_i \},$$

where the α_i ’s lie in F . It turns out that every element $x \in \mathcal{B}$ has the form x_e^c , but the choice of (c, e) is not uniquely determined by x .

Apartments in the building of G are parametrized by the maximal split tori of G . Such a torus has n eigenspaces of dimension one and they completely characterize the torus. Suppose e is a basis of V . Then there is an associated maximal split torus

$$T_e = \{t \in G : te_i \in F^\times e_i \text{ for all } i\}.$$

Permuting the basis vectors or multiplying them by scalars does not affect the resulting torus.

Having fixed a basis e , the apartment $\mathcal{A}(T_e)$ associated to T_e is given by

$$\mathcal{A}(T_e) = \{x_e^c : c \in \mathbb{R}^n\}.$$

Implicit in this definition is the fact that $T_e = T_{e'}$ implies $\mathcal{A}(T_e) = \mathcal{A}(T_{e'})$.

When $x = x_e^c$, the corresponding lattice function is

$$L_{x,r} = F_{r-c_1}e_1 + \cdots + F_{r-c_n}e_n,$$

where $F_t = \omega^{-1}([t, +\infty])$.

Suppose $y \in \mathcal{B}$. Then the parahoric subgroup $G_{y,0}$ associated to y is the stabilizer in G of y . Since this means $G_{y,0}$ must also be the stabilizer of L_y , we have

$$G_{y,0} = \{g \in G : gL_{y,r} = L_{y,r}, \text{ for all } r \in \mathbb{R}\}.$$

It is therefore evident that $G_{y,0}$ only depends on the lattice chain $L_{y,\bullet}$ or, in other words, it only depends on the facet of $[y]$ in $\mathcal{B}_{\mathrm{red}}$.

Now suppose we have a degree n extension E of F that is embedded in $M_n(F)$ in an F -linear way. Then, according to Lemma 4.6 in [HL1], the given embedding may be realized as the regular representation of E associated to an F -basis of E . More precisely, given an F -basis $e_1, \dots, e_n$ of E and $x \in E$, define a vector

$$\underline{x} = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} \in V,$$

where $x = x_1e_1 + \cdots + x_ne_n$ and $x_1, \dots, x_n \in F$. Multiplication by x is an F -linear transformation of E and hence defines a matrix $\underline{x} \in M_n(F)$. Given $x, y \in E$, we have the relations $\underline{x} \underline{y} = \underline{xy}$ and $\underline{x} \underline{\underline{y}} = \underline{\underline{xy}}$. We may assume that our basis is chosen so that $x \mapsto \underline{x}$ coincides with the given embedding of E in $M_n(F)$.

The embedded field E now defines a lattice function

$$L_r = \underline{\mathfrak{P}_E^{[re]}}$$

in F^n , where e is the ramification degree $e(E/F)$. The associated lattice chain

$$L_\bullet = \{\underline{\mathfrak{P}_E^k} : k \in \mathbb{Z}\}$$

has period e . In particular, it corresponds to a vertex in $\mathcal{B}_{\mathrm{red}}$ precisely when E/F is unramified. We observe that if our basis is an $\mathfrak{O}_F$ -basis of $\mathfrak{O}_E$ then

$$\underline{\mathfrak{P}_E^k} = \underline{\mathfrak{P}_E^k} \underline{\mathfrak{O}_E} = \underline{\mathfrak{P}_E^k} \mathfrak{O}_F^n.$$

Assume we have fixed our embedding of E and let y be the associated point in $\mathcal{B}$. The Moy-Prasad filtration of $\mathfrak{g} = M_n(F)$ associated to y is given by

$$\mathfrak{g}_{y,r} = \left\{ X \in \mathfrak{g} : X \underline{\mathfrak{P}_E^k} \subset \underline{\mathfrak{P}_E^{k+[er]}} \right\} = \underline{\underline{\varpi_E^{[er]}}} \mathfrak{g}_{y,0}.$$

(See Appendix A in [BL].) If we use integral bases then

$$\mathfrak{g}_{y,0} = \bigcap_{k \in \mathbb{Z}} \underline{\underline{\varpi_E^k}} \mathfrak{gl}_n(\mathfrak{O}_F) \underline{\underline{\varpi_E^{-k}}}.$$

We define Moy-Prasad filtration groups $G_{y,r}$ for $r \geq 0$ by taking $G_{y,0}$ to be the group of units in $\mathfrak{g}_{y,0}$ and $G_{y,r} = 1 + \mathfrak{g}_{y,r}$, for $r > 0$.

In the special case in which E/F is unramified and we use an integral basis then we have

$$\begin{aligned} G_{y,0} &= \mathrm{GL}_n(\mathfrak{O}_F), & G_{y,0+} &= 1 + M_n(\mathfrak{P}_F), \\ G_y(\mathfrak{f}) &:= G_{y,0}/G_{y,0+} \cong \mathrm{GL}_n(\mathfrak{f}), & K &:= G_{[y]} = F^\times \mathrm{GL}_n(\mathfrak{O}_F). \end{aligned}$$

As is recalled in the next section, the construction of tame supercuspidal representations involves towers of field extensions. These towers yield chains of subgroups of the group G on which our representations are defined. We need to have embeddings of the Bruhat-Tits buildings of the various subgroups. This is particularly easy to do using lattice functions. Suppose we are given a tower of fields

$$F \subset E' \subset E,$$

with $n' = [E : E']$, $n'' = [E' : F]$ and $n = n'n'' < \infty$, and given embeddings

$$E' \subset M_{n''}(E'), \quad E \subset M_{n'}(E') \subset M_{n'}(M_{n''}(F)) = M_n(F),$$

and identifications

$$E' = F^{n''}, \quad E = (E')^{n'} = (F^{n''})^{n'} = F^n,$$

as above. To (canonically) embed the extended building of $GL_{n'}(E')$ in the extended building of $GL_n(F)$, we simply view every lattice function on $(E')^{n'}$ as a lattice function on F^n . We obtain a similar embedding of reduced buildings using lattice chains. Note that the period of a lattice chain on $(E')^{n'}$ gets multiplied by the ramification degree $e(E'/F)$ when it is viewed as a lattice chain on F^n . Thus vertices map to vertices precisely when E'/F is unramified.

7.2. Inducing data. This section discusses basic terminology and notations related to the inducing data for the construction of tame supercuspidal representations. In order to be brief, we refer to [HMu] and [HL1] for some basic definitions, though it should be understood that most of these definitions are based on the work of Howe [Ho] and Yu [Y].

Definition 7.4. If E is a tamely ramified extension of F of degree n and φ is a quasicharacter of $E^\times$ then φ is **F -admissible** if

- there does not exist a proper subfield L of E containing F such that φ factors through the norm map $N_{E/L} : E^\times \rightarrow L^\times$;
- if L is a subfield of E containing F and $\varphi \mid (1 + \mathfrak{P}_E)$ factors through $N_{E/L}$, then E is unramified over L .

If φ and φ' are F -admissible quasicharacters of $E^\times$ and $E'^\times$, respectively, then φ and φ' are **F -conjugate** if there exists an F -isomorphism of E with E' that takes φ to φ' .

Suppose E is a finite tamely ramified extension of F and φ is a quasicharacter of $E^\times$. Then the conductor exponent $f(\varphi)$ of φ is the smallest positive integer such that $\varphi \mid 1 + \mathfrak{P}_E^{f(\varphi)} = 1$. Let C_E denote the subgroup of $E^\times$ generated by the roots of unity in $\mathfrak{O}_E^\times$ of order relatively prime to p and by a prime element ϖ_E in E such that ϖ_E^e belongs to F , where e is the ramification index of E over F . If ψ is a character of E that is trivial on $\mathfrak{P}_E$ and nontrivial on $\mathfrak{O}_E$ and if $f(\varphi) > 1$, then there exists a unique

$$\gamma_\varphi \in C_E \cap (\mathfrak{P}_E^{1-f(\varphi)} - \mathfrak{P}_E^{2-f(\varphi)})$$

such that $\varphi(1+t) = \psi(\gamma_\varphi t)$, $t \in \mathfrak{P}_E^{f(\varphi)-1}$.

Definition 7.5. Let E be a tamely ramified extension of F and let φ be a quasicharacter of $E^\times$. If $f(\varphi) > 1$, we say that φ is **generic** over F if $F[\gamma_\varphi] = E$. If $f(\varphi) = 1$, then we say that φ is **generic** over F if φ is F -admissible.

Definition 7.6. If E is a tamely ramified extension of F of degree n , and φ is an F -admissible quasicharacter of $E^\times$ then a **Howe factorization** of φ consists of a tower of fields

$$F = E_d \subsetneq E_{d-1} \subsetneq \cdots \subsetneq E_0 \subseteq E_{-1} = E,$$

with $d \geq 0$, and a collection of quasicharacters $\varphi_i : E_i^\times \rightarrow \mathbb{C}^\times$, for $i = -1, \dots, d$, such that:

- $1 < f(\varphi_0 \circ N_{E/E_0}) < \cdots < f(\varphi_{d-1} \circ N_{E/E_{d-1}})$.
- If φ_d is nontrivial, then $f(\varphi_{d-1} \circ N_{E/E_{d-1}}) < f(\varphi_d \circ N_{E/F})$.
- **(toral case)** If $E_0 = E$ then $\varphi_{-1} = 1$.
- **(nontoral case)** If $E_0 \subsetneq E$ then $f(\varphi_{-1}) = 1$ and φ_{-1} is generic over E_0 .
- φ_i is generic over E_{i+1} , except in the toral case when $i = -1$.
- $\varphi = \varphi_{-1} \prod_{i=0}^d \varphi_i \circ N_{E/E_i}$.

Howe's construction associates an irreducible tame supercuspidal representation π to the following data:

- a degree n tamely ramified extension E of F ,
- an F -admissible quasicharacter $\varphi : E^\times \rightarrow \mathbb{C}^\times$,
- a Howe factorization of φ ,
- an F -linear embedding of E in $M_n(F)$.

Such a collection of data is called a *Howe datum (for G)* in [HL1]. The equivalence class $\pi(\varphi)$ of π only depends on the F -conjugacy class of φ , not on the Howe factorization or the embedding of E .

Assume we have fixed a Howe datum. Then we obtain some auxiliary objects that are used in Yu's construction [Y]:

- A sequence $\vec{\mathbf{G}} = (\mathbf{G}^0, \dots, \mathbf{G}^d)$ of F -groups, where $\mathbf{G}^i$ is the centralizer of E_i in $\mathbf{G} = GL_n$ (and E_i is embedded in $M_n(F)$ by restricting the given embedding of E). Then $G^i \cong GL_{n_i}(E_i)$ with $n_i = [E : E_i]$.
- A maximal F -torus $\mathbf{T}$ in $\mathbf{G}^0$ such that T is the image of $E^\times$ in G .
- A point y in the extended building of G^0 associated to the lattice function in $E_0^{n_0}$ coming from the embedding of E in $M_{n_0}(E_0)$ as in §7.1. The corresponding point $[y]$ in the reduced building of G^0 is a vertex.
- A representation ρ of the isotropy group $K^0 = G_{[y]}^0$ of $[y]$ in G^0 defined as follows. In the toral case, ρ is simply the trivial representation of T . Now assume we are in the nontoral case. Let $G_{y,0}^0$ be the parahoric subgroup of G^0 associated to $[y]$ and $G_{y,0+}^0$ its pro-unipotent radical. The quotient $G_{y,0+}^0 = G_{y,0}^0 / G_{y,0+}^0$ is isomorphic to the group of $\mathfrak{f}$ -rational points of a connected reductive group $\mathbf{G}_y^0$ defined over the residue field $\mathfrak{f}$ of F . The group $\mathbf{G}_y^0(\mathfrak{f})$ is isomorphic to $GL_{n_0}(\mathfrak{f}_{E_0})$, where $\mathfrak{f}_{E_0}$ is the residue field of E_0 and $n_0 = [E : E_0]$. The restriction of φ_{-1} to the multiplicative group of the ring of integers of E yields a nonsingular character λ of an elliptic torus $\mathbf{T}(\mathfrak{f})$ of $\mathbf{G}_y^0(\mathfrak{f})$. The character λ then gives an irreducible cuspidal representation $\pm R_{\mathbf{T}(\mathfrak{f})}^\lambda$ of $\mathbf{G}_y^0(\mathfrak{f})$ via the construction of Green/Deligne/Lusztig [DL]. The inflation of this representation to $G_{y,0}^0$ is the restriction of ρ to $G_{y,0}^0$. To complete the definition of ρ , we use the fact that K^0 is generated by $G_{y,0}^0$ and any prime element ϖ_{E_0} of E_0 and we declare that $\rho(\varpi_{E_0})$ is the scalar operator corresponding to the scalar $\varphi_{-1}(\varpi_{E_0})$.

- A sequence $\vec{\phi} = (\phi_0, \dots, \phi_d)$ of quasicharacters $\phi_i : G^i \rightarrow \mathbb{C}^\times$, where $\phi_i = \varphi_i \circ \det_i$ with $\det_i$ being the function on G^i corresponding to the determinant on $\mathrm{GL}_{n_i}(E_i)$.
- A sequence $\vec{r} = (r_0, \dots, r_d)$ of real numbers, where r_i is the depth of ϕ_i (in the sense of Definition 2.46 in [HMu]) except when $i = d$ and ϕ_d is trivial in which case $r_d = r_{d-1}$.

The 5-tuple $(\vec{G}, y, \vec{r}, \rho, \vec{\phi})$ is a *cuspidal G -datum* in the sense of [HMu, HL1].

For much of the rest of this paper, we would like assume that we have fixed a Howe datum, but, for compatibility with [Y, HMu, HL1], we would like to use all of the above auxiliary objects and notations without explicitly recalling them. With this in mind, we define:

Definition 7.7. A G -datum Ψ consists of a Howe datum together with the auxiliary objects $(\vec{G}, \mathbf{T}, y, \vec{r}, \rho, \vec{\phi})$ associated to the Howe datum.

For a given Howe datum, it is possible to find another Howe datum that has the same embedded field E , the same quasicharacter $\varphi : E^\times \rightarrow \mathbb{C}^\times$, but a different Howe factorization. This yields an equivalence relation on the set of Howe data and hence on the set of G -data. The equivalence class of a given G -datum will be called its **refactorization class**. (This notion is generalized in Definition 4.19 of [HMu].)

Suppose we are given a G -datum. For each $i \in \{0, \dots, d-1\}$, choose an E_{i+1} -basis of E_i and use it to embed E_i in $M_{[E_i:E_{i+1}]}(E_{i+1})$ as in §7.1. Taking $\mathfrak{g}^i = M_{n_i}(E_i)$, we have

$$\mathfrak{g}^i \subset M_{n_i}(M_{[E_i:E_{i+1}]}(E_{i+1})) = \mathfrak{g}^{i+1}.$$

Then for each i the group G^i is just the multiplicative group of $\mathfrak{g}^i$ (viewed as an associative algebra). In particular, we have identities $G^i = \mathrm{GL}_{n_i}(E_i)$, not merely isomorphisms.

Suppose θ is an orthogonal involution of G . The following definition is essentially in Definition 3.13 of [HMu]:

Definition 7.8. A G -datum Ψ is θ -**symmetric** if the data $(\vec{G}, [y], \vec{\phi})$ in Ψ satisfy:

- $\theta(G^i) = G^i$, for all i ,
- $\theta([y]) = [y]$,
- $\phi_i \circ \theta = \phi_i^{-1}$, for all i .

Definition 7.9. Let ϑ be a K^0 -orbit of orthogonal involutions of G and let ξ be a refactorization class of G -data. We write $\vartheta \sim \xi$ if there exists $\Psi \in \xi$ such that Ψ is θ -symmetric for some (hence all, according to Proposition 3.9 in [HL1]) $\theta \in \vartheta$.

According to Proposition 3.9 in [HL1], our definition of the relation $\xi \sim \vartheta$ is equivalent to the definition given in [HL1].

If Θ is a G -orbit of orthogonal involutions of G then the methods of [HMu] reduce the computation of the dimension of $\mathrm{Hom}_{G^\theta}(\pi, 1)$, for $\theta \in \Theta$ and $\pi \in \pi(\varphi)$, to the computation of the dimension of certain Hom-spaces associated to certain θ' -symmetric G -data $\dot{\Psi}$, where θ' is an involution in Θ and $\dot{\Psi}$ is a refactorization of a G -datum associated to φ . More simply put, we ultimately only need to study those G -data $\dot{\Psi}$ and involutions θ' such that $\dot{\Psi}$ is θ' -symmetric. In this paper, we take things further. We show that we may reduce to the case of studying (Ψ, θ) such that Ψ is θ -symmetric and $\mathbf{T}$ is θ -split.

7.3. Parahoric subalgebras and Moy-Prasad filtrations. Suppose we are given a G -datum. The Moy-Prasad filtration objects of relevance to us take the simplest shape when we embed E in $\mathfrak{g}$ as in Lemma 4.9.

For example, using notations as in Lemma 4.9 and letting $\varpi_L = \varpi_E^e$, the parahoric algebra at y is

$$\mathfrak{g}_{y,0} = \begin{pmatrix} M_f(\mathfrak{O}_F) & M_f(\mathfrak{P}_F) & \cdots & M_f(\mathfrak{P}_F) \\ \vdots & \ddots & & \vdots \\ \vdots & & \ddots & M_f(\mathfrak{P}_F) \\ M_f(\mathfrak{O}_F) & \cdots & \cdots & M_f(\mathfrak{O}_F) \end{pmatrix},$$

and the filtration of $\mathfrak{g}_{y,0}$ is given by

$$\mathfrak{g}_{y,r} = \varpi_E^{[er]} \mathfrak{g}_{y,0},$$

where

$$\varpi_E = \begin{pmatrix} 0 & 0 & \cdots & 0 & \varpi_L \\ 1_f & 0 & \cdots & 0 & 0 \\ 0 & 1_f & \ddots & & \vdots \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ 0 & \cdots & 0 & 1_f & 0 \end{pmatrix}.$$

Thus a filtration jump occurs at r precisely when r lies in $\frac{1}{e}\mathbb{Z}$. Consequently, if $\mathfrak{f}$ is the residue field of F then

$$\mathfrak{g}_{y,0}/\mathfrak{g}_{y,0+} \cong \begin{pmatrix} M_f(\mathfrak{f}) & & \\ & \ddots & \\ & & M_f(\mathfrak{f}) \end{pmatrix}$$

and $\mathfrak{g}_{y,r}/\mathfrak{g}_{y,r+} \cong \varpi_E^{[er]} \mathfrak{g}_{y,0}/\mathfrak{g}_{y,0+}$ if $r \in \frac{1}{e}\mathbb{Z}$. If $r \notin \frac{1}{e}\mathbb{Z}$ then $\mathfrak{g}_{y,r}/\mathfrak{g}_{y,r+} = 0$. In particular, with a slight abuse of notation, we have

$$\mathfrak{g}_{y,e^{-1}}/\mathfrak{g}_{y,(e^{-1})+} \cong \begin{pmatrix} & \mathfrak{P}_F M_f(\mathfrak{f}) \\ M_f(\mathfrak{f}) & \\ & \ddots & \\ & & M_f(\mathfrak{f}) \end{pmatrix},$$

$$\mathfrak{g}_{y,2e^{-1}}/\mathfrak{g}_{y,(2e^{-1})+} \cong \begin{pmatrix} & \mathfrak{P}_F M_f(\mathfrak{f}) & \\ & & \mathfrak{P}_F M_f(\mathfrak{f}) \\ M_f(\mathfrak{f}) & & \\ & \ddots & \\ & & M_f(\mathfrak{f}) \end{pmatrix},$$

and so forth.

Note that with the above conventions, the family of objects $\mathfrak{g}_{y,r}$ only depends on the triple (F, e, f) .

Instead of applying Lemma 4.9 directly to our given extension E/F , it is more convenient in our constructions to apply this lemma repeatedly to the successive fields in the tower of fields associated to our given G -datum, using the construction described in Lemma 4.10. Doing this complicates the block matrix structure of

the Moy-Prasad filtration objects, however, after conjugating these objects by a suitable permutation matrix they take the form described above.

7.4. The character η'_θ . Suppose ξ is a refactorization class of G -data. Let $K^0 = G^0_{[y]}$ be associated to ξ and suppose ϑ is a K^0 -orbit of orthogonal involutions such that $\vartheta \sim \xi$. A character $\eta'_\theta : K^{0,\theta} \rightarrow \{\pm 1\}$ is defined in [HMu] and slightly reformulated in [HL1]. In this section, we compute the values of η'_θ we need. (The approach used in our proofs would seem to be applicable to a fairly general class of examples.)

Let us introduce the notations required to state the definition of η'_θ . The groups we use are all defined with respect to any $\Psi \in \xi$ and $\theta \in \vartheta$. The choices of θ and Ψ are irrelevant. (Note that the condition $\vartheta \sim \xi$ implies that the relevant filtration objects will be θ -stable.)

In Definition 7.7, there is a $(d+1)$ -tuple $\vec{r} = (r_0, \dots, r_d)$. Given an index $i \in \{0, \dots, d-1\}$, let $s_i = r_i/2$. The space $\mathfrak{g}^{i+1,\theta}_{y,s_i:s_i^+} = \mathfrak{g}^{i+1,\theta}_{y,s_i} / \mathfrak{g}^{i+1,\theta}_{y,s_i^+}$ has a direct sum decomposition

$$\mathfrak{g}^{i+1,\theta}_{y,s_i:s_i^+} = \mathfrak{g}^{i,\theta}_{y,s_i:s_i^+} \oplus \mathfrak{W}_i^+,$$

where the second summand $\mathfrak{W}_i^+$ is the unique complement of the first summand that is contained in the sum of the root spaces attached to roots in $\Phi(\mathbf{G}^{i+1}, \mathbf{T}) - \Phi(\mathbf{G}^i, \mathbf{T})$. (For simplicity, we abbreviate differentials $d\theta$ as θ .)

Let $\mathfrak{f}$ be the residue field of F and let $\mathfrak{f}_* \cong \mathbb{F}_p$ denote the prime subfield of $\mathfrak{f}$. We note that $\mathfrak{W}_i^+$ has the structure of an $\mathfrak{f}$ -vector space. Moreover, $K^{0,\theta}$ acts by conjugation on $\mathfrak{W}_i^+$ and in this way each element $k \in K^{0,\theta}$ defines an $\mathfrak{f}$ -linear transformation $\text{Ad}(k)$ of $\mathfrak{W}_i^+$.

Given $k \in K^{0,\theta}$, we define

$$\eta'_\theta(k) = \prod_{i=0}^{d-1} (N_{\mathfrak{f}/\mathfrak{f}_*}(\det_{\mathfrak{f}}(\text{Ad}(k)|\mathfrak{W}_i^+)))^{(p-1)/2}.$$

Lemma 7.10. *If $k \in K^{0,\theta} = G^{0,\theta}_{y,0}$ has image in $(\mathbf{G}^{0,\theta}_y)^\circ(\mathfrak{f})$ then*

$$\det_{\mathfrak{f}}(\text{Ad}(k)|\mathfrak{W}_i^+) = 1$$

for all $i \in \{0, \dots, d-1\}$ and, consequently, $\eta'_\theta(k) = 1$.

Proof. Given an index j , let $\mathbf{H}^j$ denote the $\mathfrak{f}$ -group $(\mathbf{G}^{j,\theta}_y)^\circ$. We are interested in the action of $\mathbf{H}^0(\mathfrak{f})$ on a subquotient of $\mathfrak{g}^{i+1,\theta}_{y,s_i}$.

Our definition of $\mathfrak{W}_i^+$ is a variant of the definition in [HL1]. We may regard $\mathfrak{W}_i^+$ as an object that has “depth s_i ”. It will be convenient for us to shift $\mathfrak{W}_i^+$ so that it becomes an object of depth 0. Given an index j and a real number s , we have $\mathfrak{g}^j_{y,s} = \varpi_E^{s'} \mathfrak{g}^j_{y,0}$, where $s' = \lceil se(E/F) \rceil$.

Let us consider the fixed points of θ in $\mathfrak{g}^j_{y,s}$. Let σ be the automorphism of E obtained by identifying $E^\times$ with T and letting $\sigma(t) = \theta(t)^{-1}$ for all $t \in T$. Fix a prime element $\varpi_E \in T$ in E . If $X = \varpi_E^{s'} Y$ is an element of $\mathfrak{g}^j_{y,s}$ then

$$\begin{aligned} \theta(X) = X &\Leftrightarrow \varpi_E^{s'} Y = (\theta(Y)) \sigma(\varpi_E^{s'}) \\ &\Leftrightarrow Y = \varpi_E^{-s'} (\theta(Y)) \sigma(\varpi_E^{s'}) \\ &\Leftrightarrow Y = \theta_s(Y), \end{aligned}$$

where

$$\theta_s(Y) = \varpi_E^{-s'} (\theta(Y)) \sigma(\varpi_E^{s'}).$$

So $Y \mapsto \varpi_E^{s'} Y$ determines an abelian group isomorphism from $\mathfrak{g}_{y,0}^{j,\theta_s}$ onto $\mathfrak{g}_{y,s}^{j,\theta}$. This isomorphism restricts to an isomorphism of $\mathfrak{g}_{y,0+}^{j,\theta_s}$ with $\mathfrak{g}_{y,s+}^{j,\theta}$. We also obtain an $\mathfrak{f}$ -linear isomorphism of $\mathfrak{g}_{y,0+}^{j,\theta_s}$ with $\mathfrak{g}_{y,s+}^{j,\theta}$.

Let $\mathfrak{h}^{j,s} = \text{Lie}(\mathbf{G}_y^{j,\theta_s})$. This is defined over $\mathfrak{f}$. We observe that $\mathfrak{g}_{y,0+}^{j,\theta_s} = \mathfrak{h}^{j,s} = \mathfrak{h}^{j,s}(\mathfrak{f})$.

Define an automorphism of $\mathbf{G}$ by $\alpha_s(g) = \varpi_E^{-s'} g \varpi_E^{s'}$. This yields an automorphism $\bar{\alpha}_s$ of $\mathbf{H}^j$. Note that α_s is the identity map on $\mathbf{T}$ and $\bar{\alpha}_s$ is the identity on $\mathbf{T}$.

Define an action of $\mathbf{H}^j$ on $\mathfrak{h}^{j,s}$ by $h \cdot_s X = \alpha_s(h) X h^{-1}$.

Now let $\chi_{j,s}$ be the character $\mathbf{H}^j \rightarrow \text{GL}_1/\mathfrak{f}$ that sends h to the determinant of the linear transformation $X \mapsto h \cdot_s X$ of $\mathfrak{h}^{j,s}$. This character is certainly trivial on the derived group of $\mathbf{H}^j$. It is also trivial on the center (because α_s is the identity on the center). So $\chi_{j,s}$ is trivial.

We now write $\mathfrak{h}^{i+1,s_i}$ as a direct sum of $\mathfrak{h}^{i,s_i}$ and the unique complement $(\mathfrak{h}^{i,s_i})^\perp$ that is contained in the sum of the root spaces associated to roots in $\Phi^{i+1} - \Phi^i$. The decomposition

$$\mathfrak{h}^{i+1,s_i} = \mathfrak{h}^{i,s_i} \oplus (\mathfrak{h}^{i,s_i})^\perp$$

is defined over $\mathfrak{f}$ even though the root spaces are not.

Now suppose $h \in \mathbf{H}^i$. On the one hand, we have $\chi_{i+1,s_i}(h) = 1$. But the action of h preserves $\mathfrak{h}^{i,s_i}$ and $(\mathfrak{h}^{i,s_i})^\perp$. Let $\chi'_{i+1,s_i}(h)$ and $\chi''_{i+1,s_i}(h)$ be the determinants of the linear transformations of the latter summands.

Then $\chi'_{i+1,s_i}(h) = \chi_{i,s_i^+}(h) = 1$ and thus

$$\chi''_{i+1,s_i}(h) = \chi_{i+1,s_i}(h) \chi'_{i+1,s_i}(h)^{-1} = 1.$$

We have now shown that χ''_{i+1,s_i} is trivial. This implies that $(\mathbf{G}_y^{0,\theta})^\circ(\mathfrak{f})$ acts in a unimodular fashion on $\mathfrak{W}_i^+ \cong (\mathfrak{h}^{i,s_i})^\perp(\mathfrak{f})$. $\square$

8. PROOFS OF THE MAIN THEOREMS

We have already explained in §1.4 how to deduce Theorem 1.1 from Theorems 1.2, 1.3, and 1.4. We now consider the proofs of Theorems 1.2, 1.3, and 1.4.

8.1. Proof outlines. Fix a G -orbit Θ of orthogonal involutions of G and a refactoring class ξ of G -data. Define

$$\langle \Theta, \xi \rangle_G = \dim \text{Hom}_{G^\theta}(\pi, 1),$$

for any $\theta \in \Theta$, $\Psi \in \xi$ and π associated to Ψ . (The fact that this is well-defined is explained in [HMu]. The essential ingredient is Proposition 4.24 in [HMu].)

Since π is induced from a certain open, compact-mod-center subgroup K of G , one can use Mackey's theory to express $\text{Hom}_{G^\theta}(\pi, 1)$ as a direct sum of smaller Hom-spaces parametrized by the double cosets in $K \backslash G / G^\theta$.

Each double coset KgG^θ corresponds to a K -orbit of involutions in Θ , namely, the K -orbit of $g \cdot \theta$. Using this correspondence, one can rewrite the Mackey sum as a sum parametrized by K -orbits of involutions. This is done in Proposition 5.20 [HMu] (though there is an error that is corrected in [HL1]). One advantage of the

latter reformulation is that certain repeated terms in the Mackey sum are identified and collected together.

Unfortunately, the group K has a rather complicated structure that would seem to make it impractical to completely describe the structure of the double coset space $K \backslash G / G^\theta$ or the corresponding space of K -orbits of involutions. Theorem 3.10(1) in [HL1] offers a significant simplification by replacing the sum over K -orbits from [HMu] with a certain sum over K^0 -orbits,

$$(8.1) \quad \langle \Theta, \xi \rangle_G = \sum_{\vartheta \sim \xi} m_{K^0}(\vartheta) \langle \vartheta, \xi \rangle_{K^0},$$

that we now explain.

Suppose that $\vartheta \sim \xi$, in the notation of Definition 7.9, and choose $\theta \in \vartheta$ and $\Psi \in \xi$ such that Ψ is θ -symmetric. Then, by definition,

$$\langle \vartheta, \xi \rangle_{K^0} = \dim \operatorname{Hom}_{K^{0,\theta}}(\rho', \eta'_\theta),$$

where $K^{0,\theta} = K^0 \cap G^\theta$, $\rho' = \rho \otimes (\phi|K^0)$ and ϕ is the quasicharacter of G^0 defined by

$$\phi(g) = \prod_{i=0}^d \phi_i(g).$$

The objects in the latter formula are all defined with respect to the G -datum Ψ , but we observe that ρ' and η'_θ do not vary within the refactorization class ξ .

The constant $m_{K^0}(\vartheta)$ is defined by

$$m_{K^0}(\vartheta) = [G_\theta : (K^0 \cap G_\theta)G^\theta],$$

where θ is an arbitrary element of ϑ and G_θ is the similitude group associated to G^θ . It represents the number of double cosets in $K \backslash G / G^\theta$ that correspond to the K -orbit of θ , as indicated above.

In Lemma 8.6, we show that if $\langle \vartheta, \xi \rangle_{K^0}$ is nonzero then there exists $\Psi \in \xi$ and $\theta \in \vartheta$ such that Ψ is θ -symmetric and $\mathbf{T}$ is θ -stable. Then, in Lemma 8.7, we establish that, in the latter case, $\mathbf{T}$ must actually be θ -split. It also uses the theory of “ J -symmetric embeddings” from §4 to precisely describe the restrictions of orthogonal involutions of G to the subgroups G^i .

Lemma 8.7 shows that if $\langle \vartheta, \xi \rangle_{K^0}$ is nonzero then ϑ must contain a split T -orbit ζ , that is, a T -orbit of involutions θ such that $\mathbf{T}$ is θ -split. According to Proposition 8.10, it must be the case that ϑ contains a unique split T -orbit ζ .

In Proposition 8.11, we replace equation (8.1) with the equation

$$\langle \Theta, \xi \rangle_G = \sum_{\zeta \in \mathcal{O}^T(\Theta)} m_T(\zeta) \langle \zeta, \xi \rangle_T,$$

where we are summing over the set $\mathcal{O}^T(\Theta)$ of split T -orbits in Θ and the constant $m_T(\zeta)$ is defined by

$$m_T(\zeta) = [G_\theta : (T \cap G_\theta)G^\theta].$$

If ζ is contained in the K^0 -orbit ϑ then we show $m_T(\zeta) = m_{K^0}(\vartheta)$ using the theory of J -symmetric embeddings.

In Proposition 8.12, we calculate the terms $\langle \zeta, \xi \rangle_T$. It turns out that $\langle \vartheta, \xi \rangle_{K^0} \leq 1$ and, roughly speaking, this is a consequence of the fact that one has multiplicity-free decompositions over the residue fields. More precisely, we show that $\langle \vartheta, \xi \rangle_{K^0} = 1$ exactly when $\varphi(-1) = 1$.

Let us describe the computation of $\langle \zeta, \xi \rangle_T$ in more detail. Suppose $\langle \zeta, \xi \rangle_T$ is nonzero and ξ is nontoral. Choose $\Psi \in \xi$ and $\theta \in \vartheta$ such that Ψ is θ -symmetric and $\mathbf{T}$ is θ -split. Let $\eta_\theta = \eta'_\theta \otimes (\phi|K^{0,\theta})$. Then, with notations as in §7.2, we have

$$\langle \zeta, \xi \rangle_T = \dim \operatorname{Hom}_{\mathbf{G}_y^{0,\theta}(\mathbf{f})}((-1)^{n_0+1} R_{\mathbf{T}(\mathbf{f})}^\lambda, \eta_\theta).$$

Theorem 3.11 in [HL1] gives a formula for the latter dimension that is a routine generalization of Theorem 3.3 in [Lu]. (Lusztig only discusses the case in which η_θ is trivial.) In Proposition 8.2, we further simplify Theorem 3.11 in [HL1] in the case of nonsingular characters λ and thereby generalize Formula 10.6(a) in [Lu]. If one examines Lusztig's work, one finds that the proofs carry through with no essential modification so long as we know that η'_θ is trivial on $(\mathbf{G}_y^{0,\theta})^\circ(\mathbf{f})$. The required property of η'_θ is verified in Lemma 7.10.

Lemma 8.1 says that the tori that enter into Theorem 3.11 in [HL1] in our case are θ -split and this makes it trivial to evaluate the terms in the formula from Theorem 3.11 in [HL1]. Remarkably, the only value of η'_θ that is needed to evaluate the latter formula is $\eta'_\theta(-1)$, which, from the definition of η'_θ , is obviously trivial since -1 is a scalar. So, in fact, we never actually need to compute η'_θ . (We only needed to know that it is trivial on $(\mathbf{G}_y^{0,\theta})^\circ(\mathbf{f})$ and at -1 .)

When ξ is nontoral, we obtain

$$\langle \zeta, \xi \rangle_T = \begin{cases} 1, & \text{if } \varphi(-1) = 1, \\ 0, & \text{otherwise,} \end{cases}$$

but this formula clearly also holds in the toral case.

Using the theory of J -symmetric embeddings, we show, in Lemma 8.8, that the relevant restrictions of θ to the groups G^i and $\mathbf{G}_y^0(\mathbf{f})$ must always be orthogonal involutions. (Some of the restrictions of θ are not orthogonal involutions, however, they can be ignored because they make no contribution to the dimension we are computing.) Knowing that $\mathbf{G}_y^0(\mathbf{f})$ is an orthogonal group simplifies the computation of $\langle \zeta, \xi \rangle_T$.

When $\varphi(-1) = 1$, the result of computing the terms $\langle \zeta, \xi \rangle_T$ is the formula

$$\langle \Theta, \xi \rangle_G = \sum_{\zeta \in \mathcal{O}^T(\Theta)} m_T(\zeta)$$

of Proposition 8.11. To complete the computation of $\langle \Theta, \xi \rangle_G$ uses our description of the structure of $\mathcal{O}^T(\Theta)$ (from Proposition 6.6) and the values of the constants $m_T(\zeta)$ (from Proposition 5.7). This is discussed in §8.11.

8.2. Reduction to θ -split tori over the residue field. Let $\mathbf{G}$ be a connected reductive group over $\mathbb{F}_q$, where q is a power of an odd prime. Let $\mathbf{T}$ be a maximal torus that is defined over $\mathbb{F}_q$. Let F be the Frobenius automorphism that defines the $\mathbb{F}_q$ -structures. Then $\mathbf{G}^F = \mathbf{G}(\mathbb{F}_q)$ and $\mathbf{T}^F = \mathbf{T}(\mathbb{F}_q)$.

Fix an $\mathbb{F}_q$ -automorphism θ of $\mathbf{G}$ of order two and let $\mathbf{G}^\theta$ be the group of fixed points of θ . Let $\mathbf{T}^\theta = \mathbf{T} \cap \mathbf{G}^\theta$ and $\mathbf{T}_+ = (\mathbf{T}^\theta)^\circ$. When $\mathbf{H}$ is an $\mathbb{F}_q$ -subgroup of $\mathbf{G}$, let $\operatorname{rank}_{\mathbb{F}_q}(\mathbf{H})$ be the $\mathbb{F}_q$ -rank of $\mathbf{H}$. Let $\mathbf{M}$ be the centralizer of $\mathbf{T}_+$ in $\mathbf{G}$. If $g \in \mathbf{G}$ let $Z_{\mathbf{G}}^\circ(g)$ denote the identity component of the centralizer of g in $\mathbf{G}$.

As in [Lu], we define a character

$$\epsilon_{\mathbf{T}} : (\mathbf{T}^\theta)^F / \mathbf{T}_+^F \rightarrow \{\pm 1\}$$

by

$$\epsilon_{\mathbf{T}}(t) = (-1)^{\text{rank}_{\mathbb{F}_q}(\mathbf{M}) + \text{rank}_{\mathbb{F}_q}(\mathbf{M} \cap Z_{\mathbf{G}}^{\circ}(t))}.$$

When $\mathbf{T}$ is θ -split this reduces to

$$\epsilon_{\mathbf{T}}(t) = (-1)^{\text{rank}_{\mathbb{F}_q}(\mathbf{G}) + \text{rank}_{\mathbb{F}_q}(Z_{\mathbf{G}}^{\circ}(t))}.$$

A character λ of $\mathbf{T}^F$ is said to be *nonsingular* if it is not orthogonal to any coroot of $\mathbf{T}$. (This is Definition 5.15(i) in [DL].) In other words, if $h : \mathbf{GL}_1 \rightarrow \mathbf{T}$ is a coroot that is defined over $\mathbb{F}_{q^n}$, for some $n \geq 1$, then

$$(\lambda \circ N)|h(\mathbb{F}_{q^n}^{\times}) \neq 1,$$

where

$$N(t) = t \cdot F(t) \cdots F^{n-1}(t),$$

for $t \in \mathbf{T}(\mathbb{F}_{q^n})$. To say that h is defined over $\mathbb{F}_{q^n}$ means

$$h(\mathbb{F}_{q^n}^{\times}) \subset \mathbf{T}(\mathbb{F}_{q^n})$$

or, equivalently, $F^n h(x) = h(x^{q^n})$, for all $x \in \mathbb{F}_{q^n}^{\times}$. (See 10.2(a) in [Lu].)

If λ is a character of $\mathbf{T}^F$ and χ is a character of $(\mathbf{G}^{\theta})^F$, we define $\Xi_{\mathbf{T}, \lambda, \chi}$ be the set of all $\gamma \in \mathbf{G}^F$ such that $(\gamma \cdot \theta)(\mathbf{T}) = \mathbf{T}$ and

$$\lambda(t) = \chi(\gamma^{-1}t\gamma) \epsilon_{\gamma^{-1}\mathbf{T}\gamma}(\gamma^{-1}t\gamma),$$

for all $t \in (\mathbf{T}^{\gamma \cdot \theta})^F$.

Let $\mathcal{J}$ denote the (possibly empty) set of maximal tori $\mathbf{S}$ of $\mathbf{G}$ for which there exists a Borel subgroup $\mathbf{B}$ such that $\mathbf{S} = \mathbf{B} \cap \theta(\mathbf{B})$. These tori were studied by Vust [Vu] and it follows from his results (Proposition 5 in [Vu] and its corollary) that if $\mathcal{J}$ contains a θ -split maximal torus (as will be the case for our examples) then $\mathcal{J}$ is identical to the set of all θ -split maximal tori in $\mathbf{G}$. If $\mathbf{S}$ is a θ -stable maximal torus then (according to 10.1(a) in [Lu]) $\mathbf{S} \in \mathcal{J}$ if and only if θ does not fix any coroots (or, equivalently, roots) of $\mathbf{S}$.

The following generalizes Lemma 10.4 in [Lu]:

Lemma 8.1. *If λ is a nonsingular character of $\mathbf{T}^F$ and χ is a character of $(\mathbf{G}^{\theta})^F$ that is trivial on $((\mathbf{G}^{\theta})^{\circ})^F$ then $\gamma \in \Xi_{\mathbf{T}, \lambda, \chi}$ implies $\gamma^{-1}\mathbf{T}\gamma \in \mathcal{J}$.*

Proof. If $\gamma \in \mathbf{G}^F$ then $\gamma\mathbf{T}\gamma^{-1}$, like $\mathbf{T}$, is a maximal torus in $\mathbf{G}$ that is defined over $\mathbb{F}_q$ and the character $\gamma\lambda$ of $\gamma\mathbf{T}^F\gamma^{-1}$ defined by $(\gamma\lambda)(\gamma t\gamma^{-1}) = \lambda(t)$, for $t \in \mathbf{T}^F$, is nonsingular. Since $\gamma \in \Xi_{\mathbf{T}, \lambda, \chi}$ if and only if $1 \in \Xi_{\gamma^{-1}\mathbf{T}\gamma, \gamma^{-1}\lambda, \chi}$, it suffices to prove our assertion when $\gamma = 1$.

Suppose $1 \in \Xi_{\mathbf{T}, \lambda, \chi}$. This means $\mathbf{T}$ is θ -stable and $\lambda(t) = \chi(t)\epsilon_{\mathbf{T}}(t)$, for all $t \in (\mathbf{T}^{\theta})^F$. We claim that nonsingularity implies $\mathbf{T} \in \mathcal{J}$. Suppose not. Then θ must fix a coroot h of $\mathbf{T}$. The image of h is a connected group contained in $\mathbf{T}^{\theta}$, hence it is contained in $\mathbf{T}_+$. If h is defined over $\mathbb{F}_{q^n}$ then $h(\mathbb{F}_{q^n}^{\times}) \subset \mathbf{T}_+(\mathbb{F}_{q^n})$. Thus $N(h(\mathbb{F}_{q^n}^{\times})) \subset N(\mathbf{T}_+(\mathbb{F}_{q^n})) \subset \mathbf{T}_+^F \subset \ker(\chi\epsilon_{\mathbf{T}}|(\mathbf{T}^{\theta})^F) \subset \ker \lambda$. But this contradicts nonsingularity. $\square$

The following generalizes Formula 10.6(a) in [Lu]:

Proposition 8.2. *Let λ be a nonsingular character of $\mathbf{T}^F$. Let $R_{\mathbf{T}^F}^{\lambda}$ be the associated Deligne-Lusztig virtual representation of $\mathbf{G}^F$ and let*

$$R_{\mathbf{T}^F, \lambda} = (-1)^{\text{rank}_{\mathbb{F}_q}(\mathbf{T}) + \text{rank}_{\mathbb{F}_q}(\mathbf{G})} R_{\mathbf{T}^F}^{\lambda}$$

be the associated representation of G^F . If χ is a character of $(G^\theta)^F$ that is trivial on $((G^\theta)^\circ)^F$ then the dimension of $\text{Hom}_{(G^\theta)^F}(R_{T^F, \lambda}, \chi)$ is equal to the cardinality of the double coset space $T^F \backslash \Xi_{T, \lambda, \chi} / (G^\theta)^F$.

Proof. We note first that Lusztig's Formula 10.6(a) follows immediately from his Theorem 3.3(a) and his Lemmas 10.4 and 10.5. Similarly, our assertion follows in exactly the same way with Theorem 3.3(a) in [Lu] replaced by Theorem 3.11 in [HL1] and Lemma 10.4 in [Lu] replaced by our Lemma 8.1. (There is no need to modify Lemma 10.5 in [Lu].) $\square$

8.3. Lifting finite θ -stable tori to p -adic θ -stable tori. Fix a G -datum Ψ . Associated to Ψ is the reductive group G_y^0 defined over the residue field $\mathfrak{f}$ of F such that $G_y^0(\mathfrak{f}) = G_{y,0}^0 / G_{y,0+}^0$. The role of the group G in §8.2 is played by G_y^0 . The torus T is the $\mathfrak{f}$ -torus T in G_y^0 such that $T(\mathfrak{f})$ is the image of $T(\mathfrak{O}_F)$ in $G_y^0(\mathfrak{f})$.

The main result in this section is:

Proposition 8.3. *If θ is an orthogonal involution and Ψ is a θ -symmetric nontoral G -datum such that T is θ -stable then there exists $k \in G_{y,0+}^0$ such that kTk^{-1} is θ -stable.*

Our proof is an adaptation of a proof suggested to us by Jeffrey Adler and Joshua Lansky. A similar approach is used in Appendix A of [HL1].

Lemma 8.4. *If θ is an orthogonal involution and Ψ is a θ -symmetric nontoral G -datum such that T is θ -stable then there exists $k \in G_{y,0+}^0$ such that $kTk^{-1} = \theta(T)$.*

Proof. Using field embeddings as in Lemma 4.10, we have

$$G_{y,0+}^0 = 1 + M_{n_0}(\mathfrak{P}_{E_0}).$$

Let H be the E_0 -group GL_{n_0} . Then $H(E_0) = G^0$. There exists a unique E_0 -torus in T_1 in H such that $T_1(E_0) = T$. Similarly, there exists a unique E_0 -torus T_2 in H such that $T_2(E_0) = \theta(T)$. There exists a point $x \in \mathcal{B}(H, E_0)$ such that

$$H(E_0)_{x,0+} = 1 + M_{n_0}(\mathfrak{P}_{E_0}).$$

Let H_x be the reductive $\mathfrak{f}_{E_0}$ -group such that $H_x(\mathfrak{f}_{E_0}) = H(E_0)_{x,0;0+}$. We have

$$G_y^0(\mathfrak{f}) = GL_{n_0}(\mathfrak{f}_{E_0}) = H_x(\mathfrak{f}_{E_0}).$$

The tori T_i correspond to tori T_i in H_x such that

$$T_1(\mathfrak{f}_{E_0}) = T(\mathfrak{f}) = \theta(T)(\mathfrak{f}) = T_2(\mathfrak{f}_{E_0}).$$

Lemma 2.2.2 in [D] applies to H , E_0 , x , T_1 and T_2 and implies that there exists $k \in H_{x,0+}$ such that $kT_1k^{-1} = T_2$. But k lies in $G_{y,0+}^0$ and $kTk^{-1} = \theta(T)$, which implies $kTk^{-1} = \theta(T)$. $\square$

Lemma 8.5. *Let $\mathcal{G}_1 \supset \mathcal{G}_2 \supset \dots$ be a sequence of groups such that $\mathcal{G}_{i+1}$ is normal in $\mathcal{G}_i$ and $[\mathcal{G}_i : \mathcal{G}_{i+1}]$ is (finite and) odd for all i . Let $\mathcal{S}$ be a nonempty set on which $\mathcal{G}_1$ acts transitively. Assume that $\cap_i \mathcal{O}_i$ is a singleton for each sequence $\mathcal{O}_1 \supset \mathcal{O}_2 \supset \dots$ in which $\mathcal{O}_i$ is a $\mathcal{G}_i$ -orbit in $\mathcal{S}$ for all i . Let α be a permutation of $\mathcal{S}$ of order two such that $\alpha(\mathcal{G}_i \cdot x) = \mathcal{G}_i \cdot \alpha(x)$, for all i and for all $x \in \mathcal{S}$. Then α must have a fixed point in $\mathcal{S}$.*

Proof. We first describe a recursive process for choosing a sequence $\mathcal{O}_1 \supset \mathcal{O}_2 \supset \dots$ as in the statement of the lemma, but with the added property that each $\mathcal{O}_i$ is α -stable.

Let $\mathcal{O}_1 = \mathcal{S}$. To construct our sequence, we must show that once $\mathcal{O}_i$ is defined, we can choose an α -stable element $\mathcal{O}_{i+1}$ in the set

$$\mathcal{S}_i = \{\mathcal{G}_{i+1}\text{-orbits in } \mathcal{O}_i\}.$$

Since $\mathcal{G}_{i+1}$ is normal in $\mathcal{G}_i$, it must be the case that $\mathcal{G}_i$ acts transitively on $\mathcal{S}_i$. Moreover, the cardinality of $\mathcal{S}_i$ must be odd, since it divides $[\mathcal{G}_i : \mathcal{G}_{i+1}]$, and, in addition, α must define a permutation of $\mathcal{S}_i$, since $\alpha(\mathcal{G}_{i+1}x) = \mathcal{G}_{i+1}\alpha(x)$, for all $x \in \mathcal{O}_i$. We now deduce the existence of an α -fixed orbit $\mathcal{O}_{i+1}$ in $\mathcal{S}_i$ from the fact that every involution of a finite set of odd order must have a fixed point.

Having established that a sequence $\mathcal{O}_1 \supset \mathcal{O}_2 \supset \dots$ of the desired type may be chosen, we can consider $\bigcap_i \mathcal{O}_i$. This is a singleton set $\{x\}$, where x must be a fixed point of α in $\mathcal{S}$. $\square$

Proof of Proposition 8.3. Apply Lemma 8.5 as follows. Take $\mathcal{G}_1 = G_{y,0+}^0$. If $\mathcal{G}_i$ is defined and $\mathcal{G}_i = G_{y,a_i}^0 \neq G_{y,a_i+}^0$ then let $\mathcal{G}_{i+1} = G_{y,a_i+}^0$. Take $\mathcal{S}$ to be the $G_{y,0+}^0$ -orbit of $\mathbf{T}$. Since we have shown $\theta(\mathbf{T}) \in \mathcal{S}$, it follows that $\mathcal{S}$ is θ -stable. So we can take α to be the permutation of $\mathcal{S}$ associated to θ . $\square$

8.4. Reduction to θ -stable tori. We now apply Proposition 8.3 to prove a result that essentially says that every relevant K^0 -orbit of orthogonal involutions contains at least one favorable T -orbit.

Lemma 8.6. *Suppose ξ is a refactorization class of G -data and ϑ is a K^0 -orbit of orthogonal involutions of G such that $\langle \vartheta, \xi \rangle_{K^0}$ is nonzero. Then there exists $\theta \in \vartheta$ and $\Psi \in \xi$ such that Ψ is θ -symmetric and $\mathbf{T}$ is θ -stable. Given $\Psi \in \xi$, if $\theta \in \vartheta$ has the property that Ψ is θ -symmetric and $\mathbf{T}$ is θ -stable, then every involution in the T -orbit of θ must have the same property.*

Proof. We have made two assertions. Since the second one is trivial, it suffices to prove the first one.

Consider first the toral case. The condition $\langle \vartheta, \xi \rangle_{K^0} \neq 0$ implies that $\vartheta \sim \xi$. (This follows from Proposition 3.9 in [HL1] and Propositions 5.9 and 5.20 in [HMu].)

Then Proposition 3.9 in [HL1] implies that we may choose $\Psi \in \xi$ such that Ψ is θ -symmetric for some $\theta \in \vartheta$. Since $\mathbf{G}^0 = \mathbf{T}$ in the toral case, this implies that $\mathbf{T}$ is θ -stable.

Now assume we are in the nontoral case. Again, we can choose $\theta \in \vartheta$ and $\Psi \in \xi$ such that Ψ is θ -symmetric. We have

$$\langle \vartheta, \xi \rangle_{K^0} = \dim \operatorname{Hom}_{G_y^{0,\theta}(\mathfrak{f})}((-1)^{n_0+1} R_{\mathbf{T}(\mathfrak{f})}^\lambda, \eta_\theta),$$

where λ and $R_{\mathbf{T}(\mathfrak{f})}^\lambda$ are defined as in §7.2. Applying Proposition 8.2, this becomes

$$\langle \vartheta, \xi \rangle_{K^0} = \#(\mathbf{T}(\mathfrak{f}) \backslash \Xi_{\mathbf{T}, \lambda, \eta_\theta} / G_y^0(\mathfrak{f})^\theta).$$

Choose $\gamma \in \Xi_{\mathbf{T}, \lambda, \eta_\theta}$, using the assumption that $\langle \vartheta, \xi \rangle_{K^0}$ is nonzero and the resulting fact that $\Xi_{\mathbf{T}, \lambda, \eta_\theta}$ is nonempty. Replacing $\gamma \cdot \theta$ by θ causes 1 to lie in $\Xi_{\mathbf{T}, \lambda, \eta_\theta}$, while not destroying our assumptions that $\theta \in \vartheta$ and Ψ is θ -symmetric. Since $1 \in \Xi_{\mathbf{T}, \lambda, \eta_\theta}$, it must be the case that $\mathbf{T}$ is θ -stable.

Proposition 8.3 now implies that there exists a $k \in G_{y,0+}^0$ such that $k\mathbf{T}k^{-1}$ is θ -stable or, equivalently, $\mathbf{T}$ is $(k^{-1} \cdot \theta)$ -stable. Replacing θ by $k^{-1} \cdot \theta$, we obtain $\theta \in \vartheta$ such that $\mathbf{T}$ is θ -stable and Ψ is θ -symmetric. $\square$

8.5. Reduction to θ -split tori. We now establish the following p -adic analogue of Lemma 8.1:

Lemma 8.7. *Suppose ξ is a refactorization class of G -data and ϑ is a K^0 -orbit of orthogonal involutions of G such that $\langle \vartheta, \xi \rangle_{K^0}$ is nonzero. Then there exists $\theta \in \vartheta$ and $\Psi \in \xi$ such that Ψ is θ -symmetric and $\mathbf{T}$ is θ -split. Given $\Psi \in \xi$, if $\theta \in \vartheta$ has the property that Ψ is θ -symmetric and $\mathbf{T}$ is θ -split, then every involution in the T -orbit of θ must have the same property.*

Proof. As with Lemma 8.6, the second assertion is trivial and thus we only need to prove the first assertion.

Fix a G -datum Ψ and $\theta \in \vartheta$ such that Ψ is θ -symmetric and $\mathbf{T}$ is θ -stable. Let σ be the F -automorphism of E such that $\sigma(x) = \theta(x)^{-1}$, for all $x \in E^\times = T$. It suffices to show that σ must be the identity automorphism.

Suppose σ is nontrivial. Then it must have order two or, in other words, E must be a quadratic extension of the fixed field E^σ of σ . Note that E^σ contains F .

Consider our Howe factorization of φ :

$$\varphi = \varphi_{-1} \prod_{i=0}^d (\varphi_i \circ N_{E/E_i}) = \varphi_{-1} \prod_{i=0}^d (\phi_i|E^\times)$$

and let

$$\varphi' = \phi|E^\times = (\varphi_{-1})^{-1} \varphi = \prod_{i=0}^d (\phi_i|E^\times).$$

Since each ϕ_i is θ -symmetric, so is φ' . (Here, as in [HMu], we say that a quasicharacter χ of a group $\mathcal{G}$ is α -symmetric if $\chi \circ \alpha = \chi^{-1}$, where α is an automorphism of $\mathcal{G}$.)

We have:

$$\begin{aligned} \varphi' \text{ is } \theta\text{-symmetric} &\Leftrightarrow \varphi'(x) = \varphi'(\sigma(x)) \text{ for all } x \in E^\times \\ &\Leftrightarrow \varphi'(x\sigma(x)^{-1}) = 1 \text{ for all } x \in E^\times \\ &\Leftrightarrow \varphi'|U_1(E/E^\sigma) = 1 \\ &\Leftrightarrow \varphi' \text{ factors through } N_{E/E^\sigma} \\ &\Rightarrow \varphi' \text{ is not admissible over } F. \end{aligned}$$

If Ψ is toral then $\varphi_{-1} = 1$ and thus $\varphi' = \varphi$. This means we have shown that φ is not admissible over F . This contradiction shows that σ is indeed trivial in the toral case.

Now assume Ψ is nontoral. Then:

$$\begin{aligned} \varphi_{-1}|(1 + \mathfrak{P}_E) = 1 &\Rightarrow \varphi'|(1 + \mathfrak{P}_E) = \varphi|(1 + \mathfrak{P}_E) \\ &\Rightarrow \varphi|(1 + \mathfrak{P}_E) \text{ factors through } N_{E/E^\sigma} \\ &\Rightarrow E/E^\sigma \text{ is unramified (by admissibility of } \varphi). \end{aligned}$$

We therefore have $E = E^\sigma[\sqrt{\epsilon}]$, for some square root $\sqrt{\epsilon}$ of some nonsquare unit ϵ in E^σ .

Let $E_0^\sigma = E_0 \cap E^\sigma$. Suppose $\mathfrak{f}_{E_0} = \mathfrak{f}_{E_0^\sigma}$. We claim that θ must yield an orthogonal involution of $\mathbf{G}_y^0(\mathfrak{f})$. First, we observe that, according to Proposition 4.15, θ must restrict to either an orthogonal or unitary involution of $G^0 = \mathrm{GL}_{n_0}(E_0)$. If $\theta|G^0$ is an orthogonal involution then $E_0 = E_0^\sigma$ and we apply Proposition 4.13. This says that if E is embedded in $M_2(E^\sigma)$ as the set of matrices

$$\begin{pmatrix} a & b\epsilon \\ b & a \end{pmatrix},$$

with $a, b \in E^\sigma$, and, if E^σ is embedded in a J -symmetric way in $M_{n_0/2}(E_0)$, then $\theta|G^0 = \theta_{\nu'}$ for some symmetric matrix

$$\nu' = \begin{pmatrix} Jz & 0 \\ 0 & -Jz\epsilon \end{pmatrix},$$

with $z \in (E^\sigma)^\times$. Since $(E^\sigma)^\times = E_0^\times \mathfrak{D}_{E^\sigma}^\times$ and $E_0^\times$ is the center of G^0 , we may assume z lies in $\mathfrak{D}_{E^\sigma}^\times$. This implies θ determines an orthogonal involution of $\mathbf{G}_y^0(\mathfrak{f}) = \mathrm{GL}_{n_0}(\mathfrak{f}_{E_0})$ in the present case.

On the other hand, if $\theta|G^0$ is a unitary involution then E_0/E_0^σ is a ramified quadratic extension (since we are assuming $\mathfrak{f}_{E_0} = \mathfrak{f}_{E_0^\sigma}$) and we apply Proposition 4.14. Choosing embeddings as in Proposition 4.14 and arguing as in the previous case, we see that $\theta|G^0$ is the unitary involution associated to some $\nu' \in J\mathfrak{D}_{E^\sigma}^\times$. The matrix ν' is a scalar multiple of a hermitian matrix in $G_{y,0}^0$. It therefore reduces to either a symmetric or skew-symmetric matrix in $\mathrm{GL}_{n_0}(\mathfrak{f}_{E_0})$. The skew-symmetric case can be excluded by the results of Klyachko [K]. (One argues exactly as in the proof of Lemma 6 in [HMa2].)

We have now shown that our assumption that $\mathfrak{f}_{E_0} = \mathfrak{f}_{E_0^\sigma}$ implies that θ yields an orthogonal involution of $\mathbf{G}_y^0(\mathfrak{f}) = \mathrm{GL}_{n_0}(\mathfrak{f}_{E_0})$. Thus $\mathbf{G}_y^{0,\theta}(\mathfrak{f})$ is an orthogonal group and, consequently, all of the elements of $\mathcal{J}$ are θ -split. As in the proof of Lemma 8.6, we consider the set $\Xi_{\mathbf{T},\lambda,\eta_\theta}$. This set must be nonempty, since we assume $\langle \vartheta, \xi \rangle_{K^0}$ is nonzero. If we choose γ in this set then Lemma 8.1 implies $\gamma^{-1}\mathbf{T}\gamma \in \mathcal{J}$. After replacing θ by another element of its $G_{y,0}^0$ -orbit, we can arrange that $\gamma = 1$. Then $\mathbf{T}$ is θ -split and hence

$$\sigma(\sqrt{\epsilon}) \equiv \sqrt{\epsilon} \pmod{\mathfrak{P}_E}.$$

(Note that the datum Ψ is still θ -symmetric.) But $\sigma(\sqrt{\epsilon}) = -\sqrt{\epsilon}$ implies $-\sqrt{\epsilon} \equiv \sqrt{\epsilon}$ which is impossible. It follows that $\mathfrak{f}_{E_0}$ is a quadratic extension of $\mathfrak{f}_{E_0^\sigma}$. Equivalently, E_0/E_0^σ must be an unramified quadratic extension.

Since E/E_0 is unramified and E_0/E_0^σ is unramified, we now know that E/E_0^σ is unramified. Let $n_0 = [E : E_0] = [E^\sigma : E_0^\sigma]$. Suppose n_0 is even. Then E^σ contains an unramified quadratic extension of E_0^σ . But since E_0 is the unique unramified quadratic extension of E_0^σ in E , we deduce that E_0 is contained in E_0^σ , which is absurd. This implies that n_0 must be odd.

Above we defined a quasicharacter φ' and showed that φ' factors through N_{E/E^σ} . Since $\varphi = \varphi_{-1}\varphi'$, it suffices now to show that φ_{-1} also factors through N_{E/E^σ} . This would then imply that φ factors through N_{E/E^σ} contradicting the admissibility of φ over F .

Using Hilbert's Theorem 90 on $U_1(\mathfrak{f}_E/\mathfrak{f}_{E^\sigma})$, we see that if the character λ of $\mathbf{T}(\mathfrak{f})$ (coming from $\varphi_{-1}|\mathfrak{D}_E^\times$) is trivial on $U_1(\mathfrak{f}_E/\mathfrak{f}_{E^\sigma})$ then φ_{-1} is trivial on $U_1(E/E^\sigma)$ and thus φ_{-1} factors through N_{E/E^σ} . So it suffices to show that λ is trivial on $U_1(\mathfrak{f}_E/\mathfrak{f}_{E^\sigma})$.

Since $\langle \vartheta, \xi \rangle_{K^0}$ is nonzero, the space $\mathrm{Hom}_{K^0, \theta}(\rho', \eta'_\theta)$ is nonzero. But $\eta'_\theta = 1$, according to Lemma 7.10 and the fact that the groups $G_y^{0, \theta}$ are connected. It follows that $\mathrm{Hom}_{G_y^{0, \theta}(\mathfrak{f})}(R_{\mathbf{T}(\mathfrak{f})}^\lambda, \chi)$ is nonzero, where χ is the character of $G_y^{0, \theta}(\mathfrak{f})$ that comes from that θ -symmetric quasicharacter $\phi(g) = \prod_{i=0}^d \phi_i(g)$ of G^0 . Proposition 8.2 implies $\Xi_{\mathbf{T}, \lambda, \chi}$ must be nonempty and, after replacing θ by another element of its $G_{y,0}^0$ -orbit, we may assume it contains the identity element. We observe that the character χ must be trivial on $\mathbf{T}(\mathfrak{f})^\theta = \mathrm{U}_1(\mathfrak{f}_E/\mathfrak{f}_{E^\sigma})$ since $\phi|_{\mathbf{T}^\theta}$ is θ -symmetric. (Again, we are using Hilbert's Theorem 90.) It now follows from the definition of $\Xi_{\mathbf{T}, \lambda, \chi}$ that λ is trivial on $\mathrm{U}_1(\mathfrak{f}_E/\mathfrak{f}_{E^\sigma})$. (The function $\epsilon_{\mathbf{T}}$ involved in the definition of $\Xi_{\mathbf{T}, \lambda, \chi}$ is trivial since $\mathbf{T}^\theta$ is connected.) This completes the proof. $\square$

8.6. Reduction to orthogonal involutions on Levi subgroups and finite groups. The next result shows that orthogonal involutions restrict to orthogonal involutions in the cases of relevance to our main results. This fortunate circumstance streamlines matters, since it means that we need not perform case-by-case arguments for an array of different possible restrictions.

Lemma 8.8. *Suppose ξ is a refactorization class of G -data and ϑ is a K^0 -orbit of orthogonal involutions of G such that $\langle \vartheta, \xi \rangle_{K^0}$ is nonzero. Then each $\theta \in \vartheta$ restricts to an orthogonal involution of each of the subgroups $G^i \cong \mathrm{GL}_{n_i}(E_i)$ associated to ξ and, in addition, θ yields an orthogonal involution of $G_y^0(\mathfrak{f}) \cong \mathrm{GL}_{n_0}(\mathfrak{f}_{E_0})$.*

Proof. According to Lemma 8.7, it is possible to choose $\theta \in \vartheta$ such that $\mathbf{T}$ is θ -split. Lemma 4.3 then implies that there exists $x \in T$ such that $\theta = \theta_{Jx}$. Since $T = E^\times = E_0^\times \mathfrak{D}_E^\times$, we can choose $z \in E_0^\times$ and $y \in \mathfrak{D}_E^\times$ such that $x = zy$. Proposition 4.15 implies that the restriction of θ_{Jx} to G^0 is $\theta_{J_{n_0}x}$. Since z is in the center of G^0 , we have $\theta_{J_{n_0}x} = \theta_{J_{n_0}y}$. But $J_{n_0}y$ is a symmetric matrix in $\mathrm{GL}_{n_0}(\mathfrak{D}_{E_0})$ and, consequently, θ yields an orthogonal involution of $G_y^0(\mathfrak{f}) = \mathrm{GL}_{n_0}(\mathfrak{f}_{E_0})$. We have therefore established that there exists at least one $\theta \in \vartheta$ with the asserted properties. But then it follows that every element of ϑ has these properties. $\square$

8.7. The number of split T -orbits in a K^0 -orbit. Let F be a finite extension of $\mathbb{Q}_p$, where p is an odd prime. Let E_0 be tamely ramified finite extension of F of degree m_0 and let E be an unramified extension of E_0 of degree $n_0 = n/m_0$. Embed E in $M_{n_0}(E_0)$ in a J_{n_0} -symmetric way and embed E_0 in $M_{n_0}(F)$ in a J_{m_0} -symmetric way. This gives a J_n -symmetric embedding of E in $M_n(F)$. Let $G = \mathrm{GL}_n(F)$ and $T = E^\times$. Let $G^0 = \mathrm{GL}_{n_0}(E_0)$ and $K^0 = E_0^\times \mathrm{GL}_{n_0}(\mathfrak{D}_{E_0})$.

Lemma 8.9. *Every K^0 -orbit of orthogonal involutions of G contains at most one split T -orbit.*

Proof. Suppose ζ and ζ' are two distinct split T -orbits that lie in a common K^0 -orbit. Then ζ and ζ' must lie in a common G -orbit Θ , but, according to Proposition 6.6, this implies $y_{E/F} = 4$ and $\Theta = \Theta_J$.

There are several cases to consider and the arguments we use to handle them are by no means uniform. The G -orbit Θ_J contains three split T -orbits. Representatives for these orbits are:

- θ_J , where $J = J_n$,
- θ_{Ju} , where u is a nonsquare unit in E ,
- $\theta_{J\varpi}$, where ϖ is a prime element of E_0 such that $\varpi^{e(E/F)}$ lies in the maximal unramified extension of F contained in E_0 .

Suppose $v = 1$ or u . We now show that θ_{Jv} and $\theta_{J\varpi}$ lie in distinct K^0 -orbits. Suppose, to the contrary, that there exists $k \in K^0$ such that $k \cdot \theta_{Jv} = \theta_{J\varpi}$. This is equivalent to

$$\theta_{\iota_{k^{-1}Jvk^{-1}}} = \theta_{J\varpi}$$

which is, in turn, equivalent to the condition $J\varpi kv^{-1}J^tk \in F^\times$. Since $y_{E/F} = 4$, it must be the case that $e(E_0/F)$ is even. Therefore, $F^\times \subset (E_0^\times)^2 \mathfrak{D}_E^\times$. Therefore, we can choose $a \in E_0^\times$ and $b \in \mathfrak{D}_E^\times$ such that

$$a^2b = J\varpi kv^{-1}J^tk.$$

Next, we write $k = hy$, with $h \in \mathrm{GL}_{n_0}(\mathfrak{D}_{E_0})$ and $y \in E_0^\times$. This yields

$$a^2b = J\varpi hyv^{-1}J^ty^th = J\varpi hy^2v^{-1}J^th.$$

Taking determinants and absolute values in the latter equations, we see that the elements ϖ , a and y of E_0 are related by the fact that $\varpi y^2 a^{-2}$ is a unit. But this is impossible since the latter element clearly has odd valuation. This contradiction proves that θ_{Jv} and $\theta_{J\varpi}$ lie in distinct K^0 -orbits, if $v \in \{1, u\}$.

It remains to show that θ_J and θ_{Ju} lie in distinct K^0 -orbits. Assume first that n_0 is even. Suppose there exists $k \in K^0$ such that $k \cdot \theta_J = \theta_{Ju}$. We use Proposition 4.15 to describe the restrictions of our involutions to G^0 . We have

$$\theta_{J_{n_0}u} = \theta_{Ju}|G^0 = k \cdot \theta_J|G^0 = \theta_{\iota_{k^{-1}Jk^{-1}}}|G^0 = \theta_{T_{k^{-1}J_{n_0}k^{-1}}},$$

where $h \mapsto {}^T h$ is the transpose on G^0 . This contradicts the fact that the symmetric matrices $J_{n_0}u$ and ${}^T k^{-1}J_{n_0}k^{-1}$ (in G^0) have distinct discriminants (and n_0 is even).

Now assume n_0 is odd. In this case, we can choose u to be a nonsquare unit in E_0 . Suppose $k \in K^0$ and $\theta_{Ju} = k \cdot \theta_J = \theta_{\iota_{k^{-1}Jk^{-1}}}$. Then $JukJ^tk \in F^\times$. Equivalently, $ukJ^tkJ \in F^\times$. Write $k = hy$, with $h \in \mathrm{GL}_{n_0}(\mathfrak{D}_{E_0})$ and $y \in E_0^\times$. Then we have $uhyJ^ty^thJ = uhy^2J^thJ = uy^2h\theta_J(h)^{-1} \in F^\times$. (Note that $\theta_{J_n}(h) = \theta_{J_{n_0}}(h)$.)

Let E'_0 be the maximal unramified extension of F contained in E_0 . Then $E_0 = E'_0[\sqrt[e]{\alpha\varpi_F}]$, for some $\alpha \in \mathfrak{D}_{E'_0}^\times$ and some prime element ϖ_F of F . Here, $e = e(E/F) = e(E_0/F)$. Let E' be the maximal unramified extension of F contained in E . Then $E'[\sqrt[e]{\alpha\varpi_F}] = E'E_0 = E$. Since $y_{E/F} = 4$, Lemma 3.4 implies $\alpha \in (\mathfrak{D}_{E'}^\times)^2$. But the fact that n_0 is odd implies, $\alpha \in (\mathfrak{D}_{E'}^\times)^2 \cap \mathfrak{D}_{E'_0}^\times = (\mathfrak{D}_{E'_0}^\times)^2$. Applying Lemma 3.4 again allows us to deduce that $y_{E_0/F} = 4$. This implies $F^\times \subset (\mathfrak{D}_{E_0}^\times)^2$. Therefore, $h\theta_J(h)^{-1} \in (uy^2)^{-1}(\mathfrak{D}_{E_0}^\times)^2 \subset \mathfrak{D}_{E_0}^\times - (\mathfrak{D}_{E_0}^\times)^2$. Let $\bar{h}$ be the image of h in $\mathrm{GL}_{n_0}(\mathfrak{f}_{E_0})$. Then $\bar{h}$ lies in the similitude group $\mathrm{GO}_{J_{n_0}}(\mathfrak{f}_{E_0})$ and the similitude ratio of $\bar{h}$ is a nonsquare in $\mathfrak{f}_{E_0}$. This is impossible, according to Lemma 5.6. Indeed, the latter result implies that

$$\mathrm{GO}_{J_{n_0}}(\mathfrak{f}_{E_0}) = \mathfrak{f}_{E_0}^\times \mathrm{O}_{J_{n_0}}(\mathfrak{f}_{E_0})$$

which implies that the homomorphism

$$\mathrm{GO}_{J_{n_0}}(\mathfrak{f}_{E_0})/\mathfrak{f}_{E_0}^\times \rightarrow \mathfrak{f}_{E_0}^\times/(\mathfrak{f}_{E_0}^\times)^2$$

induced by the similitude ratio must be trivial since its kernel is $\mathrm{O}_{J_{n_0}}/\{\pm 1\}$. This contradiction completes the proof. $\square$

The proof of the previous lemma involved the special case of the G -orbit Θ_J when $y_{E/F} = 4$, because this is the unique case in which multiple split T -orbits lie in a common G -orbit. We remark that, in the notations of the proof, the involutions θ_J and $\theta_{J\varpi}$ have identical restrictions to G^0 , since $\varpi \in E_0^\times$. Moreover, when n_0 is odd the involutions in all three involutions θ_J , θ_{Ju} and $\theta_{J\varpi}$ have identical restrictions to G^0 , since $u, \varpi \in E_0^\times$. Indeed, according to Proposition 4.15, the restriction of $\theta_{J_n x}$ to G^0 is $\theta_{J_{n_0} x}$ when $x \in E^\times$. But when $x \in E_0^\times$, we have $\theta_{J_{n_0} x} = \theta_{J_{n_0}}$.

8.8. Reduction from K^0 -orbits to split T -orbits. Fix a refactorization class ξ of G -data and a K^0 -orbit ϑ of orthogonal involutions such that $\langle \vartheta, \xi \rangle_{K^0} \neq 0$.

For each $\theta \in \vartheta$, there is an associated involution $\bar{\theta}$ of $\mathbf{G}_y^0(\mathbf{f})$. (Elsewhere in this paper, we abbreviate $\bar{\theta}$ as θ .) Let $\bar{\vartheta}$ be the image of ϑ under $\theta \mapsto \bar{\theta}$.

Since $T = E^\times = E_0^\times \mathfrak{O}_E^\times$ and $E_0^\times$ is the center of G^0 , we see that $\theta \mapsto \bar{\theta}$ maps T -orbits in ϑ to $\mathbf{T}(\mathbf{f})$ -orbits in $\bar{\vartheta}$. Since $K^0 = TG_{y,0}^0 = G_{y,0}^0 T$, we see that $\bar{\vartheta}$ must be a single $\mathbf{G}_y^0(\mathbf{f})$ -orbit. Therefore, we see that the map $\theta \mapsto \bar{\theta}$ yields a surjection from the set of T -orbits in the K^0 -orbit ϑ onto the set of $\mathbf{T}(\mathbf{f})$ -orbits in the $\mathbf{G}_y^0(\mathbf{f})$ -orbit $\bar{\vartheta}$.

Proposition 8.10. *If ξ is a refactorization class of G -data and ϑ is a K^0 -orbit of orthogonal involutions such that $\langle \vartheta, \xi \rangle_{K^0} \neq 0$ then*

- ϑ contains a unique split T -orbit ζ ,
- $\bar{\vartheta}$ contains a unique split $\mathbf{T}(\mathbf{f})$ -orbit $\bar{\zeta}$, and
- $\bar{\zeta}$ is the image of ζ under $\theta \mapsto \bar{\theta}$.

Proof. The existence of a split T -orbit ζ in ϑ is a consequence of Lemma 8.7. The uniqueness of ζ follows from Lemma 8.9. Clearly, the image $\bar{\zeta}$ of ζ under $\theta \mapsto \bar{\theta}$ is a split $\mathbf{T}(\mathbf{f})$ -orbit in $\bar{\vartheta}$. But, according to Lemma 6.5, there must be a unique split $\mathbf{T}(\mathbf{f})$ -orbit in $\bar{\vartheta}$. $\square$

8.9. The T -orbit multiplicity formula.

Proposition 8.11.

$$\langle \Theta, \xi \rangle_G = \sum_{\zeta \in \mathcal{O}^T(\Theta)} m_T(\zeta) \langle \zeta, \xi \rangle_T.$$

Proof. We start by recalling the formula

$$\langle \Theta, \xi \rangle_G = \sum_{\vartheta \sim \xi} m_{K^0}(\vartheta) \langle \vartheta, \xi \rangle_{K^0}$$

from Theorem 3.10(1) in [HL1]. If ϑ is any K^0 -orbit in Θ then, according to Proposition 3.9 in [HL1] and Propositions 5.9 and 5.20 in [HMu], the condition $\langle \vartheta, \xi \rangle_{K^0} \neq 0$ implies $\vartheta \sim \xi$. So the previous sum may be regarded as a sum over all K^0 -orbits ϑ in Θ , not just the orbits that satisfy $\vartheta \sim \xi$.

Proposition 8.10 tells us that if ϑ is a K^0 -orbit contained in Θ such that $\langle \vartheta, \xi \rangle_{K^0}$ is nonzero then ϑ contains a unique split T -orbit ζ . This yields the formula

$$\langle \Theta, \xi \rangle_G = \sum_{\zeta \in \mathcal{O}^T(\Theta)} m_{K^0}(\zeta) \langle \zeta, \xi \rangle_T.$$

To complete the proof, we observe that the case-by-case analysis given in Proposition 5.7 and Lemma 5.8 shows that if $\zeta \subset \vartheta$ then $m_{K^0}(\vartheta) = m_T(\zeta)$. $\square$

8.10. Evaluating $\langle \zeta, \xi \rangle_T$. Let ξ be a refactorization class of G -data and let Θ be a G -orbit of orthogonal involutions of G . Proposition 8.11 establishes the formula

$$\langle \Theta, \xi \rangle_G = \sum_{\zeta \in \mathcal{O}^T(\Theta)} m_T(\zeta) \langle \zeta, \xi \rangle_T.$$

We now evaluate this formula.

Assume, with our usual notation, that $\Psi \in \xi$ comes from an F -admissible quasicharacter $\varphi : E^\times \rightarrow \mathbb{C}^\times$.

Proposition 8.12. *If $\varphi(-1) \neq 1$ then $\langle \Theta, \xi \rangle_G = 0$. If $\varphi(-1) = 1$ then*

$$\langle \Theta, \xi \rangle_G = \sum_{\zeta \in \mathcal{O}^T(\Theta)} m_T(\zeta).$$

Proof. As observed in §1.2, if $\varphi(-1) \neq 1$ then $\langle \Theta, \xi \rangle_G = 0$. Therefore we assume $\varphi(-1) = 1$.

For $\theta \in \zeta \in \mathcal{O}^T(\Theta)$, we have

$$\langle \zeta, \xi \rangle_T = \dim \operatorname{Hom}_{K^{0,\theta}}(\rho', \eta'_\theta).$$

In the toral case, $K^{0,\theta} = \{\pm 1\}$ and $\rho'(-1) = \phi(-1) = \varphi(-1) = 1 = \eta'_\theta(-1)$. (Since -1 is in the center of G , conjugation by -1 is trivial and hence $\eta'_\theta(-1) = 1$.) Our claim in the toral case follows.

Now assume ξ is nontoral. From Lemma 8.8, we know that $\mathbf{G}_y^{0,\theta}(\mathbf{f})$ is an orthogonal group in $\mathbf{G}_y^0(\mathbf{f}) = \operatorname{GL}_{n_0}(\mathbf{f}_{E_0})$. We also know that

$$\langle \zeta, \xi \rangle_T = \dim \operatorname{Hom}_{\mathbf{G}_y^{0,\theta}(\mathbf{f})}((-1)^{n_0+1} R_{\mathbf{T}(\mathbf{f})}^\lambda, \eta_\theta).$$

Applying Proposition 8.2, we obtain

$$\langle \zeta, \xi \rangle_T = \# (\mathbf{T}(\mathbf{f}) \backslash \Xi_{\mathbf{T}, \lambda, \eta_\theta} / \mathbf{G}_y^0(\mathbf{f})^\theta).$$

If $\gamma \in \Xi_{\mathbf{T}, \lambda, \eta_\theta}$ then $\mathbf{T}(\mathbf{f})^{\gamma \cdot \theta} = \{\pm 1\}$. Therefore, $\Xi_{\mathbf{T}, \lambda, \eta_\theta}$ is the set of all $\gamma \in \mathbf{G}_y^0(\mathbf{f})$ such that $\mathbf{T}$ is $(\gamma \cdot \theta)$ -split and

$$\varphi(-1) = \lambda(-1) = \eta_\theta(-1) \varepsilon_{\gamma^{-1} \mathbf{T} \gamma}(-1) = 1.$$

Since we are assuming $\varphi(-1) = 1$, we see that $\Xi_{\mathbf{T}, \lambda, \eta_\theta}$ is simply the set of all $\gamma \in \mathbf{G}_y^0(\mathbf{f})$ such that $\mathbf{T}$ is $(\gamma \cdot \theta)$ -split.

We now adopt the notations in Proposition 8.10. Consider the map from $\Xi_{\mathbf{T}, \lambda, \eta_\theta}$ into the set of $\mathbf{T}(\mathbf{f})$ -orbits of involutions in $\bar{\vartheta}$ given by mapping the double coset of γ to the $\mathbf{T}(\mathbf{f})$ -orbit of the involution $\gamma \cdot \bar{\theta}$. According to Proposition 8.10, the image of this map must be the unique split $\mathbf{T}(\mathbf{f})$ -orbit in $\bar{\vartheta}$ or, in other words, the orbit of $\bar{\theta}$.

So if $\gamma \in \Xi_{\mathbf{T}, \lambda, \eta_\theta}$ then there exists $t \in \mathbf{T}(\mathbf{f})$ such that $\gamma \cdot \bar{\theta} = t \cdot \bar{\theta}$. In other words, $t^{-1} \gamma$ lies in the orthogonal similitude group $\mathbf{G}_y^0(\mathbf{f})_{\bar{\theta}}$. Now Lemma 5.6 implies that

$$\mathbf{G}_y^0(\mathbf{f})_{\bar{\theta}} = (\mathbf{T}(\mathbf{f}) \cap \mathbf{G}_y^0(\mathbf{f})_{\bar{\theta}}) \mathbf{G}_y^{0,\theta}.$$

It follows that $\mathbf{T}(\mathbf{f}) \backslash \Xi_{\mathbf{T}, \lambda, \eta_\theta} / \mathbf{G}_y^0(\mathbf{f})^\theta$ has a single element, namely, the double coset of the identity element. Therefore, $\langle \zeta, \xi \rangle_T = 1$ and our assertion follows. $\square$

Note that in the previous proof, we essentially used a generalized version of Theorem 10.3 in [Lu]. Our Lemma 8.1 provided the generalized version of Lusztig's Lemma 10.4 needed to generalize the proof of Lusztig's theorem.

8.11. Proofs of Theorems 1.2, 1.3 and 1.4. We now evaluate the formula in Proposition 8.12 to obtain Theorems 1.2, 1.3 and 1.4. We may as well assume $\varphi(-1) = 1$. Then Proposition 8.12 says

$$\langle \Theta, \xi \rangle_G = \sum_{\zeta \in \mathcal{O}^T(\Theta)} m_T(\zeta).$$

Proposition 5.7 says that if $\zeta \in \mathcal{O}^T(\Theta)$ then $m_T(\zeta) = 1$, except when $y_{E/F} = 2$ and ζ is the T -orbit of θ_J .

So the evaluation of $\langle \Theta, \xi \rangle_G$ rests on the determination of $\mathcal{O}^T(\Theta)$. But the set $\mathcal{O}^T(\Theta)$ is described by Proposition 6.6 which says that we have the following cases:

- $y_{E/F} = 1$ (equivalently, n is odd): There is one element of $\mathcal{O}^T$, namely, the T -orbit of θ_J ,
- $y_{E/F} = 2$: There are two elements of $\mathcal{O}^T$: the T -orbit of θ_J and the T -orbit of involutions θ_{Jx} where $x \in E^\times - ((E^\times)^2 F^\times)$. The two T -orbits lie in distinct G -orbits.
- $y_{E/F} = 4$: There are four elements of $\mathcal{O}^T$: three of them lie in Θ_J and the fourth lies in Θ_{nqs} .

Suppose π is a tame supercuspidal representation associated to a G -datum in ξ . Then, as we are continuing to assume that $\varphi(-1) = 1$, we see that π is G^θ -distinguished with respect to some (hence all) $\theta \in \Theta$ precisely when $\mathcal{O}^T(\Theta)$ is nonempty. Since $\mathcal{O}^T(\Theta_J)$ is always nonempty, Theorem 1.2 follows. Similarly, Theorem 1.3 reduces to the observation that if $\Theta \neq \Theta_J$ then $\mathcal{O}^T(\Theta)$ is nonempty precisely in the two cases listed in the statement of Theorem 1.3.

It remains to verify Theorem 1.4. Assume $\langle \Theta, \xi \rangle_G$ is nonzero. We have the following cases:

- (1) $\Theta = \Theta_J$ and n odd:
 - There is a unique ζ in $\mathcal{O}^T(\Theta)$ and $m_T(\zeta) = 1$. Thus $\langle \Theta_J, \xi \rangle_G = 1$.
- (2) $\Theta = \Theta_J$ and $y_{E/F} = 2$:
 - There is a unique ζ in $\mathcal{O}^T(\Theta)$ and $m_T(\zeta) = 2$. Thus $\langle \Theta_J, \xi \rangle_G = 2$.
- (3) $\Theta \neq \Theta_J$ and $y_{E/F} = 2$:
 - There is a unique ζ in $\mathcal{O}^T(\Theta)$ and $m_T(\zeta) = 1$. Thus $\langle \Theta_J, \xi \rangle_G = 1$.
- (4) $\Theta = \Theta_J$ and $y_{E/F} = 4$:
 - There are three T -orbits ζ in $\mathcal{O}^T(\Theta)$ and we have $m_T(\zeta) = 1$ in each case. Thus $\langle \Theta_J, \xi \rangle_G = 3$.
- (5) $\Theta \neq \Theta_J$ and $y_{E/F} = 4$:
 - There is a unique ζ in $\mathcal{O}^T(\Theta)$ and $m_T(\zeta) = 1$. Thus $\langle \Theta_J, \xi \rangle_G = 1$.

This completes the proof of Theorem 1.4. $\square$

ACKNOWLEDGEMENTS

The author wishes to thank Jeffrey Adams, Stephen DeBacker, Zhengyu Mao, Omer Offen, Dipendra Prasad, Yiannis Sakellaridis and, especially, Jeffrey Adler and Joshua Lansky for conversations that affected the progress and outcome of this paper. In addition, the author thanks the referee for numerous helpful comments and suggestions that have led to a much improved paper.

REFERENCES

- [B] E. A. Bender, “Characteristic polynomials of symmetric matrices II: Local number fields,” *Linear Multilinear Algebra* **2**, no. 1 (1974), 55–63. MR0447282 (56:5597)
- [BL] P. Broussous and B. Lemaire, “Building of $GL(m, D)$ and centralizers,” *Transform. Groups*, 7 (2002), No. 1, 15–50. MR1888474 (2003c:20060)
- [BT] F. Bruhat and J. Tits, “Schémas engroupes et immeubles des groupes classiques sur un corps local,” *Bull. Soc. Math. France* **112**, (1984), 259–301. MR788969 (86i:20064)
- [CO1] G. Chinta and O. Offen, “A metaplectic Casselman-Shalika formula for GL_r ,” *Representation Theory, Complex Analysis and Integral Geometry I*, edited by Bernhard Krötz, Omer Offen and Eitan Sayag, Birkhäuser, *Progress in Mathematics*. MR2867630 (2012h:22001)
- [CO2] G. Chinta and O. Offen, “Orthogonal period of a $GL_3(\mathbb{Z})$ Eisenstein series,” *Representation Theory, Complex analysis, and Integral Geometry*, 41–59, Birkhäuser, Springer, New York, 2012. MR2885075 (2012k:11059)
- [D] S. DeBacker, “Parameterizing conjugacy classes of maximal unramified tori via Bruhat-Tits theory,” *Michigan Math. J.* **54** (2006), no. 1, 157–178. MR2214792 (2007d:22012)
- [DL] P. Deligne and G. Lusztig, “Representations of reductive groups over finite fields,” *Ann. of Math.* (2) **103** (1976), no. 1, 103–161. MR0393266 (52:14076)
- [FK] Y. Flicker and D. Kazhdan, “Metaplectic correspondence,” *Publ. Math. Inst. Hautes Études Sci.*, No. 64 (1986), 53–110. MR876160 (88d:11049)
- [GS] W. T. Gan and G. Savin, “Representations of metaplectic groups I: epsilon dichotomy and local Langlands correspondence,” preprint.
- [GR] B. Gross and M. Reeder, “From Laplace to Langlands via representations of orthogonal groups,” *Bull. Amer. Math. Soc. (N.S.)* **43** (2006), no. 2, 163–205. MR2216109 (2007a:11159)
- [HL1] J. Hakim and J. Lansky, “Distinguished tame supercuspidal representations and odd orthogonal periods,” *Represent. Theory* **16** (2012), 276–316. MR2925798
- [HMa] J. Hakim and Z. Mao, “Cuspidal representations associated to $(GL(n), O(n))$ over finite fields and p -adic fields,” *J. Algebra* **213** (1999), no. 1, 129–143. MR1674664 (99m:22019)
- [HMa2] J. Hakim and Z. Mao, “Supercuspidal representations of $GL(n)$ distinguished by a unitary subgroup,” *Pacific J. Math.* **185**, (1998), no. 1, 149–162. MR1653208 (99j:22023)
- [HMu] J. Hakim and F. Murnaghan, “Distinguished tame supercuspidal representations,” *Int. Math. Res. Pap.*, IMRP 2008, no. 2, Art. ID rpn005, 166 pp. MR2431732 (2010a:22022)
- [HMu2] J. Hakim and F. Murnaghan, “Tame supercuspidal representations of $GL(n)$ distinguished by a unitary group,” *Comp. Math.* **133** (2002), 199–244. MR1923582 (2003g:22019)
- [HW] A. Helminck and S. Wang, “On rationality properties of involutions of reductive groups,” *Adv. Math.*, **99** (1993), 26–97. MR1215304 (94d:20051)
- [Ho] R. Howe, “Tamely ramified supercuspidal representations of GL_n ,” *Pacific J. Math.* **73** (1977), no. 2, 437–460. MR0492087 (58:11241)
- [J1] N. Jacobson, *Basic Algebra I*, Second edition, W. H. Freeman and Company, New York, 1985. MR780184 (86d:00001)
- [J2] N. Jacobson, “A note on Hermitian forms,” *Bull. Am. Math. Soc.*, **46** (1940), 264–268. MR0001957 (1:325d)
- [Ja] H. Jacquet, “Représentations distinguées pour le groupe orthogonal,” *C. R. Acad. Sci. Paris Sér. I Math.* **312** (1991), no. 13, 957–961. MR1113084 (92h:11041)
- [K] A.A. Klyachko, “Models for the complex representations of the group $GL(n, q)$,” *Math. USSR-Sb.*, **48** (1984), 365–379. MR691984 (84j:20014)
- [Lu] G. Lusztig, “Symmetric spaces over a finite field,” *The Grothendieck Festschrift Vol. III* (ed. P. Cartier, et. al.), Birkhäuser, Boston-Basel-Berlin, 1990, 57–81. MR1106911 (92e:20034)
- [Ma] Z. Mao, “A fundamental lemma for metaplectic correspondence,” *J. Reine Angew. Math.*, **496** (1998), 107–129. MR1605813 (99b:22029)
- [Mu1] F. Murnaghan, “Parametrization of tame supercuspidal representations,” *On certain L-functions*, Clay Math. Proc., **13**, Amer. Math. Soc., Providence, RI, 2011, 439–469. MR2767524 (2012e:22024)
- [Mu2] F. Murnaghan, “Regularity and distinction of supercuspidal representations,” *Harmonic analysis on reductive, p -adic groups*, Contemp. Math., **543**, Amer. Math. Soc., Providence, RI, 2011, 155–183. MR2798427 (2012g:22018)

- [O] O. T. O'Meara, *Introduction to Quadratic Forms*, Reprint of the 1973 edition, Classics in Mathematics, Springer-Verlag, Berlin, 2000. MR1754311 (2000m:11032)
- [Of] O. Offen, "Kloosterman-Fourier inversion for symmetric matrices," *Bull. Soc. Math. France*, 133 (2005), no. 3, 331–348. MR2169821 (2006j:11073)
- [SV] Y. Sakellaridis and A. Venkatesh, "Periods and harmonic analysis on spherical varieties," preprint.
- [Se] J.-P. Serre, *Galois cohomology*, Reprint of the 1997 English edition, Springer Monographs in Mathematics, Springer-Verlag, Berlin, 2002. MR1466966 (98g:12007)
- [Sp1] T. A. Springer, *Linear Algebraic Groups*, Second Edition, Progress in Mathematics Vol. 9, Birkhäuser, Boston, Basel, Berlin, 1998. MR1642713 (99h:20075)
- [Sp2] T. A. Springer, "Some results on algebraic groups with involutions," *Algebraic Groups and Related Topics, Advanced Studies in Pure Mathematics* **6** (1985), 525–543. MR803346 (86m:20050)
- [V] C. Valverde, "On induced representations distinguished by orthogonal groups," preprint.
- [Vu] T. Vust, Opération de groupes réductifs dans un type de cônes presque homogènes, *Bull. Soc. Math. France*, 102 (1974), 317–333. MR0366941 (51:3187)
- [W] M. Weissman, "Split metaplectic groups and their L -groups," preprint.
- [Y] J.-K. Yu, "Construction of tame supercuspidal representations," *J. Amer. Math. Soc.* **14** (2001), no. 3, 579–622 (electronic). MR1824988 (2002f:22033)

DEPARTMENT OF MATHEMATICS AND STATISTICS, AMERICAN UNIVERSITY, WASHINGTON, DC 20016

E-mail address: jhakim@american.edu