RESTRICTION OF PRO-$p$-IWAHORI-HECKE MODULES

KAROL KOZIOL

ABSTRACT. Let $p$ be a prime number, and $F$ a nonarchimedean local field of residual characteristic $p$. We explore the interaction between the pro-$p$-Iwahori-Hecke algebras of the group $\text{GL}_n(F)$ and its derived subgroup $\text{SL}_n(F)$. Using the interplay between these two algebras, we deduce two main results. The first is an equivalence of categories between Hecke modules in characteristic $p$ over the pro-$p$-Iwahori-Hecke algebra of $\text{SL}_2(\mathbb{Q}_p)$ and smooth mod-$p$ representations of $\text{SL}_2(\mathbb{Q}_p)$ generated by their pro-$p$-Iwahori-invariants. The second is a “numerical correspondence” between packets of supersingular Hecke modules in characteristic $p$ over the pro-$p$-Iwahori-Hecke algebra of $\text{SL}_n(F)$, and irreducible, $n$-dimensional projective Galois representations.

CONTENTS

1. Introduction ........................................ 1
2. Notation ........................................... 5
   2.1. Root Data .................................. 5
   2.2. Weyl Groups ................................ 6
3. Pro-$p$-Iwahori-Hecke Algebras .................. 8
   3.1. Bruhat Decompositions ....................... 8
   3.2. The Algebras ................................ 9
4. Equivalence of Categories between $G_S$-Representations and $\mathcal{H}_S$-modules .... 12
   4.1. Mod-$p$ Representations .................... 12
   4.2. Generalizations ............................. 17
5. $L$-Packets of $\mathcal{H}_S$-modules ............. 20
   5.1. Supersingular Hecke Modules ............... 21
   5.2. $L$-packets ................................ 22
6. Galois Groups and Projective Galois Representations .... 27
   6.1. Galois Groups .............................. 27
   6.2. Galois Representations .................... 28
   6.3. Comparison with Große-Klönne’s Functor .... 33
Appendix A. Proof of Proposition 6.12 ........... 37
References .............................................. 41

1. INTRODUCTION

In recent years, there has been a great deal of interest and activity surrounding the (still nebulous) mod-$p$ version of the Local Langlands Program. This situation is best understood for the group $\text{GL}_2(\mathbb{Q}_p)$: there exists a correspondence between isomorphism classes of semisimple mod-$p$ representations of $\text{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$ of dimension 2 and (certain) smooth, finite
length, semisimple mod-$p$ representations of $GL_2(\mathbb{Q}_p)$, due to Breuil ([7]). Moreover, this correspondence is compatible with a $p$-adic version of the Local Langlands Correspondence (cf. [8]; see also [9], [13], [15], [19], [20], [29]).

Serious difficulties arise when one considers groups other than $GL_2(\mathbb{Q}_p)$, however. For example, Breuil and Paskúnas have shown in [12] that, for $F$ a nontrivial unramified extension of $\mathbb{Q}_p$, there is an infinite family of representations of $GL_2(F)$ associated to a “generic” Galois representation. Therefore, it is not clear what the “shape” of a mod-$p$ correspondence should be for a general reductive group. Nevertheless, Breuil and Herzig have given a construction of the “ordinary part” of such a correspondence, and shown that it appears in certain spaces of mod-$p$ automorphic forms ([11]).

An alternative viewpoint for examining these difficulties comes through the study of Hecke modules. In order to define these objects, we require some notation. From this point onwards, we let $F$ be a nonarchimedean local field with residue field of size $q$ and characteristic $p$. Let $G$ denote the group $GL_n(F)$ and $G_S$ its derived subgroup $SL_n(F)$. We also let $I(1)$ denote the pro-$p$-Iwahori subgroup of $G$, and set $I_S(1) := I(1) \cap G_S$. Letting $\bullet$ represent either the empty symbol or “$S$,” we define the pro-$p$-Iwahori-Hecke algebra $H_\bullet$ as the convolution algebra of compactly supported, $\overline{F}_p$-valued functions on the double coset space $I_\bullet(1) \backslash G/I_\bullet(1)$. Since the groups $G$ and $G_S$ are split over $F$, the structure of these Hecke algebras is well-understood (cf. [34]).

The reason for considering modules of the algebra $H_\bullet$ comes from the following key fact. Given a smooth, mod-$p$ representation $\pi$ of $G_\bullet$, its space of $I_\bullet(1)$-invariants $\pi^{I_\bullet(1)}$ is a nonzero vector space over $\overline{F}_p$. Hence, we obtain a functor

$$\mathcal{I}_\bullet : \mathcal{Rep}_p(G_\bullet) \longrightarrow \mathcal{Mod} - H_\bullet$$

from the category of smooth, mod-$p$ representations of $G_\bullet$ to the category of right $H_\bullet$-modules. The results contained in [25], [34], and [17] suggest that perhaps there is some weak formulation of the Local Langlands Correspondence with representations of $G_\bullet$ replaced by modules over $H_\bullet$. Moreover, one hopes that the functor $\mathcal{I}_\bullet$ will provide the necessary link between the two categories above, and yield information about the category of smooth representations (though one doesn’t expect an equivalence of categories in general: see [24]).

The questions that emerge when one considers such a Local Langlands Correspondence for Hecke modules have been investigated most extensively for the group $GL_n(F)$. Results of Vignéras and Ollivier (cf. [34] and [25]) provide a classification of simple, supersingular right $H$-modules (see [34] for the precise definitions). These are the modules that should act as a substitute for supercuspidal representations of $G$. Additionally, the two aforementioned articles show that we have an equality

$$\# \left\{ \text{simple, supersingular} \right. $$

$$\left. \text{$H$-modules of dimension } n \text{ with fixed action of a uniformizer} \right\} = \# \left\{ \text{irreducible, mod-$p$ Galois representations of dimension } n \text{ with fixed determinant of Frobenius} \right\},$$

where we consider all objects up to isomorphism. One may see this as a “numerical Langlands Correspondence” for Hecke modules. By recent work of Große-Klöhnne ([17]), we now know that this numerical bijection is induced by a functor, at least in the case where $F = \mathbb{Q}_p$.

In the present article, we explore the analogous situation for the group $SL_n(F)$. The algebra $H_S$ has been considered in the context of a potential Local Langlands Correspondence for Hecke modules only for $n = 2$ (cf. [1]). Here, we define the notion of $L$-packets of
supersingular $\mathcal{H}_S$-modules (for arbitrary $n$), which come by restriction from supersingular $\mathcal{H}$-modules. Among these, it is natural (in light of (1)) to single out a certain subset which we call “regular.” We then obtain the following equality, analogous to (1) above:

\[
\text{(2) } \# \left\{ \text{regular, supersingular } L\text{-packets of } \mathcal{H}_S\text{-modules} \right\} = \# \left\{ \text{irreducible, mod-} p \text{ projective Galois representations of dimension } n \right\}
\]

In fact, we prove a more precise version of the above statement (see Corollary 6.11). Additionally, when $F = \mathbb{Q}_p$, we define a map between the two sets above which realizes this equality (analogous to the functor constructed in [17]), and is moreover compatible with Große-Klönn’s functor (Corollary 6.16).

We now describe the contents of this article in more detail. After recalling the necessary notation in Section 2 to define extended and affine Weyl groups, we recall in Section 3 the presentations of the algebras $\mathcal{H}$ and $\mathcal{H}_S$, due to Vignéras. Proposition 3.3 then shows that we have an injection $\mathcal{H}_S \hookrightarrow \mathcal{H}$, making $\mathcal{H}$ into a free $\mathcal{H}_S$-module. Note that the results of Section 3 apply with little change to the case where $G$ is (the group of $F$-rational points of) an arbitrary split, connected, reductive group, and $G_S$ is its simply connected derived subgroup. See Subsection 4.2 for the precise statements and further generalizations to Iwahori-Hecke algebras.

In Section 4, we examine more closely the functor $I_\bullet$. In order to accurately speak of an equivalence of categories, we must slightly alter the category $\text{Rep}_{\mathbb{F}_p}(G_\bullet)$. We let $\text{Rep}^{I_{S(1)} \mathbb{F}_p}(G_\bullet)$ denote the full subcategory consisting of representations generated by their space of $I_{\bullet(1)}$-invariant vectors, and continue to denote by $I_\bullet$ the functor of invariants restricted to this subcategory. Our main result in this direction is the following:

**Theorem (Theorem 4.6).** Assume $(n, p) = 1$. Then the functor $I$ induces an equivalence of categories between $\text{Rep}_{\mathbb{F}_p}^{I_{1(1)} \mathbb{F}_p}(G)$ and $\text{Mod} - \mathcal{H}$ if and only if the functor $I_S$ induces an equivalence of categories between $\text{Rep}_{\mathbb{F}_p}^{I_{S(1)} \mathbb{F}_p}(G_S)$ and $\text{Mod} - \mathcal{H}_S$.

Using results of Ollivier ([24]) on the functor of $I(1)$-invariants for $\text{GL}_2(F)$ (and a slight extension of Theorem 4.6), we obtain the following corollary.

**Corollary (Corollary 4.7).** The functor $I_S$ induces an equivalence of categories between $\text{Rep}_{\mathbb{F}_p}^{I_{S(1)} \mathbb{F}_p}(\text{SL}_2(\mathbb{Q}_p))$ and $\text{Mod} - \mathcal{H}_S$ when $p > 2$.

In the course of proving the above theorem, we also obtain information about the adjoint functor to $I_\bullet$. In order to describe it, we need some more notation. We let $1$ denote the trivial character of $I_{\bullet(1)}$, and define the pro-$p$ universal module by

$$C_\bullet = \text{c-ind}_{I_{\bullet(1)}}^{I_\bullet}(1).$$

As $C_\bullet^{I_{\bullet(1)}}$ identifies with $\mathcal{H}_\bullet$, the pro-$p$ universal module is naturally a (left) module over $\mathcal{H}_\bullet$. Hence, the functor sending a right $\mathcal{H}_\bullet$-module $m$ to $m \otimes_{\mathcal{H}_\bullet} C_\bullet$ gives an adjoint functor to $I_\bullet$. In the context of a potential equivalence of categories, the flatness properties of the module $C_\bullet$ are extremely important. As a byproduct of the proof of the above theorem, we obtain the following result.

**Proposition (Corollary 4.3).** The module $C$ is flat over $\mathcal{H}$ if and only if the module $C_S$ is flat over $\mathcal{H}_S$. 
Using [28], we obtain the following:

**Corollary (Corollary 4.4).** Assume $n = 2$. Then $C_S$ is flat if and only if $q = p$.

As a second application of the interaction between the algebras $H$ and $H_S$, we investigate the supersingular modules for $H_S$ in Section 5. The precise notion of supersingularity may be found in [34]; roughly, a simple $H_S$-module $m$ is supersingular if every element of the center of $H_S$ which is “of positive length” acts by 0. We will not need the exact definition of supersingularity here, as we have a complete description of such modules ([26]):

**Theorem (Theorems 5.2 and 5.4).** Let $m$ be a simple, right $H_S$-module. Then $m$ is supersingular if and only if $m$ is a character of $H_S$, unequal to the trivial or sign character.

There is a natural conjugation action on $H$ by the multiplicative subgroup of elements of length 0, which preserves the subspace $H_S$. Therefore, given any supersingular character $\chi$ of $H_S$ and an element $T_w$ of length 0, we may define a new character $T_w \cdot \chi$, given on $H_S$ by first conjugating the argument by $T_w$ and then applying $\chi$. Mimicking the classical case of complex representations of $G_S$, we make the following definition:

**Definition.** An $L$-packet of supersingular $H_S$-modules is an orbit of the subgroup of $H$ of length 0 elements on the set of supersingular characters of $H_S$.

In order to proceed further, we must impose an additional “regularity” condition on $L$-packets, defined more precisely in Definition 5.6. Given this, we are able to count the number of regular, supersingular $L$-packets of size $d$, for $d$ a divisor of $n$ (Corollary 5.10).

Our next goal is to relate the $L$-packets thus constructed to projective, mod-$p$ Galois representations, which we take up in Section 6. After recalling the structure of Galois groups attached to local fields and their representations, we define projective Galois representations. An extremely useful result of Tate (Theorem 6.4) states that

$$H^2(\text{Gal} (\overline{F}/F), \mathbb{F}_p^\times) = 0,$$

which implies that every projective representation of the absolute Galois group lifts to a genuine representation. In order to work with these objects combinatorially, we isolate those lifts for which the action of a Frobenius element of $\text{Gal}(\overline{F}/F)$ has a fixed determinant. Once this choice is made, we arrive at our main theorem:

**Theorem (Corollaries 6.10 and 6.11).** Let $d$ be a divisor of $n$. The number of regular supersingular $L$-packets of $H_S$-modules of size $d$ is equal to the number of irreducible projective Galois representations of dimension $n$ having exactly $d^{\frac{n-1}{n}}$ isomorphism classes of lifts. This number is equal to

$$h(d) = \frac{1}{d} \sum_{e|d} \mu \left( \frac{d}{e} \right) g(e),$$

where $\mu$ denotes the Möbius function, and

$$g(e) = \sum_{f|n} \mu \left( \frac{n}{f} \right) \left( \frac{f}{(e,f)} \cdot q - 1 \right) q^{(e,f)} - 1.$$

In particular, the number of regular supersingular $L$-packets of $H_S$-modules is equal to the number of irreducible projective Galois representations of dimension $n$. 
Some remarks are in order. Firstly, we note the function \( g(e) \) can be computed quite explicitly in terms of Euler’s phi function. With some work, one can show that \( h(d) \not= 0 \) if and only if \( \frac{d^{q-1}}{n} \in \mathbb{Z} \) (Lemma 5.11), so that the statement of the above theorem is consistent. Secondly, when \( n = 2 \) and \( F = \mathbb{Q}_p \), we recover the bijection contained in work of Abdellatif ([1]).

Thirdly, this numerical correspondence is slightly more precise than the numerical correspondence for supersingular \( \mathcal{H} \)-modules, due to Vignéras and Ollivier (cf. (1)). Our correspondence establishes a numerical bijection between subsets on both sides of (2), which should give clues as to how a (potential) functorial correspondence should behave in general.

Finally, let us remark that the work of [17] shows how to construct a functor from the category of finite length modules over the pro-\( p \)-Iwahori-Hecke algebra of a general connected reductive group \( G \), defined and split over \( \mathbb{Q}_p \), to the category of \( \phi \)-modules. When \( G = \text{GL}_n(\mathbb{Q}_p) \), this functor (along with Fontaine’s equivalence of categories) induces the numerical correspondence (1). We compute this functor for supersingular \( L \)-packets of \( \mathcal{H}_S \)-modules in Subsection 6.3, and show how to define a map from the set of regular supersingular \( L \)-packets to the set of irreducible, projective mod-\( p \) Galois representations. Moreover, we show in Corollary 6.15 that this map realizes the numerical correspondence of Corollary 6.11.

Acknowledgements. I would like to thank my advisor Professor Rachel Ollivier for her support and guidance throughout the course of working on this article, and for many extremely useful comments. Several parts of this paper were written during the conference “Modular Representation Theory of Finite and \( p \)-adic Groups” at the Institute for Mathematical Sciences, National University of Singapore, and I would like to thank the institution for its support. During the preparation of this article, support was also provided by NSF Grant DMS-0739400.

2. Notation

Fix a prime number \( p \), and let \( F \) be a nonarchimedean local field of residual characteristic \( p \). Denote by \( \mathfrak{o} \) its ring of integers, and by \( \mathfrak{p} \) the unique maximal ideal of \( \mathfrak{o} \). Fix a uniformizer \( \varpi \) and let \( k = \mathfrak{o}/\mathfrak{p} \) denote the (finite) residue field. The field \( k \) is a finite extension of \( \mathbb{F}_p \) of size \( q = p^f \). We fix also a separable closure \( \overline{F} \) of \( F \), and let \( k_{\overline{F}} \) denote its residue field. Let \( \iota : k_{\overline{F}} \longrightarrow \overline{F} \) denote a fixed isomorphism, and assume that every \( \overline{F}_p \)-valued character factors through \( \iota \).

Let \( n \geq 2 \), and denote by \( G \) the \( F \)-rational points of the algebraic group \( \text{GL}_n \). We denote by \( G_S \) the derived subgroup of \( G \), equal to the group \( \text{SL}_n(F) \). For any subgroup \( J \) of \( G \), we will denote by \( J_S = J \cap G_S \) its intersection with \( G_S \). The maximal torus of diagonal matrices in \( G \) will be denoted by \( T \).

We begin by discussing the various Weyl groups associated to \( G \) and \( G_S \).

2.1. Root Data. For an algebraic subgroup \( J \) of \( G \), we let \( X^*(J) \) (resp. \( X_*(J) \)) denote the group of algebraic characters (resp. cocharacters) of \( J \). In particular, the groups \( X^*(T) \) and \( X_*(T) \) are both \( \mathbb{Z} \)-modules of rank \( n \), in duality by a perfect pairing

\[ \langle -, - \rangle : X^*(T) \times X_*(T) \longrightarrow \mathbb{Z}, \]

defined by $\chi(\xi(a)) = a^{\langle \chi, \xi \rangle}$, for $\chi \in X^*(T), \xi \in X_*(T)$ and $a \in F^\times$. We have a similar statement for $T_S$, with $X^*(T_S)$ and $X_*(T_S)$ being $\mathbb{Z}$-free of rank $n - 1$.

We let $\Phi \subset X^*(T)$ denote the set of roots of $T$ acting on $\text{Lie}(G)$ by conjugation; it is a root system of type $A_{n-1}$. We partition $\Phi$ into two disjoint sets

$$\Phi = \Phi^+ \sqcup \Phi^-,$$

where $\Phi^+$ consists of all characters of the form

$$\alpha_{i,j} \left( \begin{array}{cccc} t_1 & t_2 & & \\ & t_2 & \ddots & \\\\ & & \ddots & t_j \\ & & & t_n \end{array} \right) = t_i t_j^{-1},$$

for $1 \leq i < j \leq n$, and $\Phi^- = -\Phi^+$. The Borel subgroup $B$ corresponding to this choice of positive roots is the subgroup of $G$ of upper triangular matrices. We denote by $U$ its unipotent radical.

For $1 \leq i \leq n - 1$, we let $\alpha_i := \alpha_{i,i+1} \in \Phi^+$. The elements $\alpha_i$ are the simple roots, and constitute a basis for $\Phi$. We let $s_i$ denote the reflection of $X^*(T)$ and associated to $\alpha_i$. The reflections $s_i$ generate a Coxeter group isomorphic to $S_n$, the symmetric group on $n$ letters. We describe this action explicitly. For $\alpha \in \Phi$, let

$$\varphi_\alpha : \text{SL}_2 \longrightarrow \text{GL}_n$$

denote the standard morphism of algebraic groups defined by the root $\alpha$. If $1 \leq i \leq n - 1$ and $\chi \in X^*(T)$, we define $\chi^{s_i}$ by

$$\chi^{s_i}(t) := \chi^{n_i}(t) = \chi(t n_i t_i^{-1}),$$

where $t \in T$ and

$$n_i := \varphi_{\alpha_i} \left( \begin{array}{cc} 0 & 1 \\ -1 & 0 \end{array} \right) = \left( \begin{array}{cccc} 1 \\ & \ddots \\ & & 0 & 1 \\ & & -1 & 0 \\ & & & \ddots \\ & & & & 1 \end{array} \right)^{i-th \text{ row}} \left( \begin{array}{cccc} \right)^{(i + 1)-th \text{ row}}.$$

2.2. Weyl Groups. In order to ease notation in the following discussion (and throughout the remainder of the article), we let $\bullet$ denote either the empty symbol or $S$.

Since the group $G_\bullet$ is split over $F$, the torus $T_\bullet$ extends to a smooth closed $\mathfrak{o}$-subgroup scheme of $G_\bullet$ (see [32], Sections 3.4, 3.5, and 3.8). We may therefore define the subgroup $T_\bullet(\mathfrak{o})$ of $\mathfrak{o}$-valued points of $T_\bullet$ (that is, elements with entries in $\mathfrak{o}^\times$), and denote its maximal pro-$p$ subgroup by $T_\bullet(1 + p)$. By Teichmüller lifting, we will identify $T_\bullet(k)$, the group of $k$-valued points of $T_\bullet$, with a finite subgroup of $T_\bullet(\mathfrak{o})$.

We let $N_{G_\bullet}(T_\bullet)$ denote the normalizer of $T_\bullet$ in $G_\bullet$, and define the following groups:

$$W_{\bullet,0} := N_{G_\bullet}(T_\bullet)/T_\bullet,$$

$$W_\bullet := N_{G_\bullet}(T_\bullet)/T_\bullet(\mathfrak{o}),$$

$$W_\bullet^{(1)} := N_{G_\bullet}(T_\bullet)/T_\bullet(1 + p).$$
The elements $n_i$ for $1 \leq i \leq n - 1$ defined above normalize the torus $T_\bullet$, and along with $T_\bullet$ generate $N_{G_\bullet}(T_\bullet)$. Hence, the group $W_{\bullet,0}$ is a finite Coxeter group isomorphic to $S_n$, generated by (the classes of) the elements $n_i$. Notice that we have an injection $N_{G_\bullet}(T_S) \hookrightarrow N_G(T)$, which induces an isomorphism
\[ W_{S,0} = N_{G_\bullet}(T_S)/T_S \cong N_G(T)/T = W_0. \]

Let $\alpha_0 := \alpha_1 + \alpha_2 + \ldots + \alpha_{n-1}$ denote the highest root of the root system $\Phi$ with respect to $\Phi^+$, and set
\[ n_0 := \varphi_{\alpha_0} \begin{pmatrix} 0 & -\omega^{-1} \\ \omega & 0 \end{pmatrix} = \begin{pmatrix} 1 & -\omega^{-1} \\ & \ddots \\ & & 1 \end{pmatrix}. \]

We let $W_{aff}$ denote the subgroup of $W$ generated by (the images of) the elements $n_i$ for $0 \leq i \leq n - 1$. The group $W_{aff}$ is an affine Coxeter group of type $\tilde{A}_{n-1}$ with generating set
\[ S := \{n_1, \ldots, n_{n-1}, n_0\} \]
and braid relations
\[
(n_i n_j) = 1 \quad \text{if} \quad |i - j| = 0, \\
(n_i n_j)^3 = 1 \quad \text{if} \quad |i - j| = 1, \\
(n_i n_j)^2 = 1 \quad \text{if} \quad |i - j| > 1,
\]
where we consider the indices $i, j$ modulo $n$, and where the products are computed in $W$. We let $t : W_{aff} \rightarrow \mathbb{N}$ denote the length function on the Coxeter group $(W_{aff}, S)$.

The following results are straightforward.

**Proposition 2.1.** We have an isomorphism of Coxeter groups $W_S \cong W_{aff}$.

**Proof.** The elements $n_i$ all lie in $N_{G_\bullet}(T_S)$, and it is clear that any element of $N_{G_\bullet}(T_S)$ may be written as a product of the $n_i$ and an element of $T_S(\mathfrak{o})$. Hence, we have a surjection $N_{G_\bullet}(T_S) \rightarrow W_{aff}$, whose kernel is exactly $N_{G_\bullet}(T_S) \cap T(\mathfrak{o}) = T_S(\mathfrak{o})$. \qed

**Proposition 2.2.** The group $W_S^{(1)}$ is isomorphic to the subgroup of $W^{(1)}$ generated by (the images of) the elements $n_i$ for $0 \leq i \leq n - 1$ and $t \in T_S(k)$.

**Proof.** It is clear that we have a surjection from $N_{G_\bullet}(T_S)$ onto the group described, whose kernel is exactly $N_{G_\bullet}(T_S) \cap T(1 + \mathfrak{p}) = T_S(1 + \mathfrak{p})$. \qed

Consider now the exact sequence
\[ 1 \rightarrow T_S \rightarrow T \rightarrow T/T_S \rightarrow 1, \]
where $T/T_S$ is a torus of rank 1. Taking the cocharacter group of this exact sequence, we obtain
\[ 1 \rightarrow X_*(T_S) \rightarrow X_*(T) \rightarrow X_*(T/T_S) \rightarrow 1. \]
We fix a splitting of the surjection $X_*(T) \rightarrow X_*(T/T_S)$, and denote by $h' \in X_*(T)$ a cocharacter generating the image of this splitting.

We let $W_{aff}^{(1)}$ denote the preimage in $W^{(1)}$ of $W_{aff}$ under the natural projection map $W^{(1)} \rightarrow W$. Proposition 2.2 shows that $W_{aff}^{(1)}$ is generated by the image of $W_S^{(1)}$ in $W^{(1)}$ and the images of the elements $h'(a)$ for $a \in k^\times$. 
Let $\omega$ denote the element of $G$ given by

$$\omega := \begin{pmatrix} 0 & 1 & \cdots & \cdots \\ \vdots & \ddots & \ddots & \vdots \\ \vdots & \cdots & 0 \\ \varpi & \cdots & 1 & 0 \end{pmatrix};$$

it satisfies

$$\omega^{-1} n_i \omega = n_{i+1},$$

where the index is considered modulo $n$. One easily verifies that $W$ is generated by (the images of) the elements $n_i$ for $0 \leq i \leq n - 1$ and $\omega$, and moreover, we have a decomposition

$$W = \omega^\mathbb{Z} \rtimes W_{\text{aff}}$$

(cf. [34], Section 1.2). Consequently, $W^{(1)}$ is generated by (the images of) the elements $n_i$ for $0 \leq i \leq n - 1$, $\omega$, and $t$ for $t \in T(k)$. By Proposition 1 of [34], the length function $\ell$ on $W_{\text{aff}} \cong W_S$ inflates to $W^{(1)}$ and $W_{S}^{(1)}$ in such a way that $\ell(\omega) = \ell(t) = 0$ for every $t \in T(k)$. For convenience, we shall further inflate the length function from $W^{(1)}$ to $N_G(T)$. Since the isomorphism of Proposition 2.2 preserves length, we deduce the following.

**Proposition 2.3.** The elements $\{\omega^j h'(a)\}_{j \in \mathbb{Z}, a \in k^\times}$ form a set of coset representatives for the coset spaces $W_S^{(1)} \backslash W^{(1)}$ and $W^{(1)}/W_{S}^{(1)}$. In particular, the coset spaces admit representatives of length 0.

### 3. Pro-$p$-Iwahori-Hecke Algebras

#### 3.1. Bruhat Decompositions.

Let $\bullet$ denote either the empty symbol or $S$. By Sections 3.4.1 and 3.4.2 of [32], the groups $G_\bullet$, $B_\bullet$, $U_\bullet$ and $T_\bullet$ all have integral models over $\mathfrak{o}$. We let $I_\bullet$ denote the Iwahori subgroup of $G_\bullet$, which we take to be the preimage of $B_\bullet(k)$ under the quotient map $G_\bullet(\mathfrak{o}) \rightarrow G_\bullet(k)$. We let $I_\bullet(1)$ denote its pro-$p$ radical, which may be defined as the preimage of the group $U_\bullet(k)$ under the quotient map. This yields the decomposition $I_\bullet = T_\bullet(k) \ltimes I_\bullet(1)$. See also Section 3.7 of [32].

Using the Iwahori subgroup $I_\bullet$, we obtain an associated Bruhat decomposition (cf. [32], Section 3.3):

$$G_\bullet = \bigsqcup_{w \in W_\bullet} I_\bullet w I_\bullet.$$

Here $I_\bullet w I_\bullet$ denotes the double coset $I_\bullet \hat{w} I_\bullet$ for any lift $\hat{w}$ in $N_{G_\bullet}(T_\bullet)$ of $w$. Using this, one easily obtains the following double coset decomposition (cf. [34], Theorem 6):

$$G_\bullet = \bigsqcup_{w \in W_\bullet^{(1)}} I_\bullet(1) w I_\bullet(1).$$
3.2. The Algebras. We consider the free \( \mathbb{Z} \)-module \( \mathcal{C}_* \) defined by
\[
\mathcal{C}_* := \left\{ f : G_* \to \mathbb{Z} : \begin{array}{l}
\diamond f(ig) = f(g) \text{ for } i \in I_*(1), g \in G_* \\
\diamond \text{supp}(f) \text{ is compact}
\end{array} \right\}.
\]
The space \( \mathcal{C}_* \) is naturally equipped with a left action of \( G_* \) given by right translation. For any element \( g \in G_* \), we denote by \( 1_{I_*(1)}g \in \mathcal{C}_* \) the characteristic function of the coset \( I_*(1)g \).

We define the pro-\( p \)-Iwahori-Hecke algebra as
\[
\mathcal{H}_* := \text{End}_{G_*}(\mathcal{C}_*)
\]
with product given by composition. By Frobenius Reciprocity we have
\[
\mathcal{H}_* \cong \text{End}_{G_*}(\mathcal{C}_*) \cong \text{Hom}_{I_*(1)}(1, \mathcal{C}_*/I_*(1)) \cong \mathcal{C}^{I_*(1)}_*;
\]
we therefore identify \( \mathcal{H}_* \) with the free \( \mathbb{Z} \)-module \( \mathbb{Z}[I_*(1)/G_*/I_*(1)] \), with the product given by convolution. For an element \( g \in G_* \), we let \( T_g^* \) denote the characteristic function of the coset \( I_*(1)gI_*(1) \). By abuse of notation, we shall often speak of elements \( T_w^* \), where \( w \in W^{(1)}_* \), by the Bruhat decomposition (equation (3)), this is independent of the choice of lift of \( w \) to \( N_{G_*}(T^*) \).

We will need one more algebra, defined as follows. Let \( Z \) be the center of \( G \), and denote by \( Z(\varpi^Z) \) the subgroup of \( Z \) consisting of elements whose entries are a power of \( \varpi \). We define the free \( \mathbb{Z} \)-module \( \mathcal{C}_Z^\varpi \) by
\[
\mathcal{C}_Z^\varpi := \left\{ f : G \to \mathbb{Z} : \begin{array}{l}
\diamond f(ig) = f(g) \text{ for } i \in Z(\varpi^Z)I(1), g \in G \\
\diamond \text{supp}(f) \text{ is compact}
\end{array} \right\}.
\]
Once again, this space has a natural action of \( G \). We set
\[
\mathcal{H}_Z := \text{End}_G(\mathcal{C}_Z^\varpi);
\]
by Frobenius Reciprocity, the algebra \( \mathcal{H}_Z \) identifies with \( \mathcal{C}_Z^{Z(\varpi^Z)I(1)} = \mathcal{C}_Z^{I(1)} \), with the product given by convolution of functions.

For \( 0 \leq i \leq n-1 \), we let \( T_i \) denote the rank 1 subtorus of \( T^\varpi_S \) defined by the embedding \( \varphi_{\alpha_i} \), above; that is, we have
\[
T_i = \left\{ \varphi_{\alpha_i} \begin{pmatrix} a & 0 \\ 0 & a^{-1} \end{pmatrix} : a \in F^\times \right\}.
\]
We also set
\[
\tau_i^* := \sum_{t \in T_i(k)} T^*_{t^i}.
\]

The structures of \( \mathcal{H}_* \) and \( \mathcal{H}_Z \) are summarized in the following theorem.

**Theorem 3.1** ([34], Theorem 1 and [28], Section 5.1.3). Let \( \bullet \) denote either the empty symbol or \( S \).

1. As a \( \mathbb{Z} \)-module, the ring \( \mathcal{H}_* \) is free with basis \( \{ T_{w}^{*} \}_{w \in W^{(1)}_*} \).
2. (Braid relations) We have
\[
T_{w}^{*} T_{w'}^{*} = T_{ww'}^{*},
\]
for any \( w, w' \in W^{(1)}_* \) satisfying \( \ell(ww') = \ell(w) + \ell(w') \).
3. (Quadratic relations) For \( 0 \leq i \leq n-1 \), we have
\[
(T_{n_i}^{*})^2 = q T_{n_i}^{*} + T_{n_i}^{*} \tau_{i}^{*}.
\]
4. The ring \( \mathcal{H}_{S,Z} \) is generated by the elements \( T_{n_i}^{S} \) and \( T_{t}^{S} \) for \( 0 \leq i \leq n-1 \), \( t \in T_{S}(k) \).
(5) The ring $\mathcal{H}_Z$ is generated by the elements $T_{n_i}, T_\omega$ and $T_t$ for $0 \leq i \leq n - 1$, $t \in T(k)$.

(6) We have an isomorphism of $\mathbb{Z}$-algebras

$$\mathcal{H}_Z \cong \mathcal{H}_Z/(T_\omega^n - 1).$$

For future applications, we will also need the affine subalgebra of $\mathcal{H}_{\bullet,Z}$.

**Definition 3.2.**

(1) We denote by $\mathcal{H}_{\text{aff},Z}$ the free $\mathbb{Z}$-submodule of $\mathcal{H}_Z$ generated by $T_w$ for $w \in W^{(1)}$. By Corollary 3 of [34], $\mathcal{H}_{\text{aff},Z}$ is a subalgebra of $\mathcal{H}_Z$, called the affine pro-$p$-Iwahori-Hecke algebra.

(2) We define $\mathcal{H}_{S,\text{aff},Z}$ to be equal to $\mathcal{H}_{S,Z}$.

**Remarks.**

(1) By Theorem 3.1 and the remarks following Proposition 2.2, we see that $\mathcal{H}_{\text{aff},Z}$ is generated by the elements $T_{n_i}$ and $T_t$ for $0 \leq i \leq n - 1$ and $t \in T(k)$.

(2) Since the subgroup of $W_S$ generated by the elements $n_i$, with $0 \leq i \leq n - 1$, is $W_S$ itself (cf. Proposition 2.1), the second part of Definition 3.2 is consistent with Corollary 3 of [34].

We may now relate the various Hecke algebras.

**Proposition 3.3.**

(1) The linear map defined by

$$\mathfrak{f} : \mathcal{H}_{S,Z} \rightarrow \mathcal{H}_Z$$

$$T_g^S \mapsto T_g$$

where $g \in G_S$, is an injective $\mathbb{Z}$-algebra homomorphism.

(2) Let $\mathfrak{T}_g$ denote the image of $T_g$ in $\mathcal{H}_Z/(T_\omega^n - 1) \cong \mathcal{H}_Z$. Then the linear map defined by

$$\mathfrak{T} : \mathcal{H}_{S,Z} \rightarrow \mathcal{H}_Z$$

$$T_g^S \mapsto \mathfrak{T}_g$$

where $g \in G_S$, is an injective $\mathbb{Z}$-algebra homomorphism.

**Proof.** The proofs for both parts are similar; we prove the first assertion.

One can easily show that the $G_S$-linear map defined by

$$\mathfrak{f} : \mathcal{C}_{S,Z} \rightarrow \mathcal{C}_{Z|G_S}$$

$$1_{I_S(1)} \mapsto 1_{I(1)}$$

is injective. Taking $I_S(1)$-invariants gives the injection

$$\mathcal{H}_{S,Z} \cong \mathcal{C}_{S,Z}^{I_S(1)} \xrightarrow{\mathfrak{f}} \mathcal{C}_{Z}^{I(1)} \cong \mathcal{H}_Z,$$

which is easily seen to send $T_g^S$ to $T_g$ for $g \in G_S$.

It remains to check compatibility of $\mathfrak{f}$ with the algebra structures. The injection $W_S^{(1)} \hookrightarrow W^{(1)}$ is compatible with the length function $\ell$; hence, if $n, n' \in N_{G_S}(T_S)$ are two elements satisfying $\ell(nn') = \ell(n) + \ell(n')$, we get

$$\mathfrak{f}(T_n^S)T_{n'}^S = T_nT_{n'} = T_{nn'} = \mathfrak{f}(T_{nn'}) = \mathfrak{f}(T_n^S T_{n'}^S).$$

In addition,

$$\mathfrak{f}(\tau_i^S) = \tau_i$$
for $0 \leq i \leq n - 1$. Since $\ell(t) = 0$ for $t \in T_S(k)$, we obtain
\[
(f(T^S)_{n_i})^2 = T^2_{n_i} \\
= qT^2_{n_i} + T^S_{n_i}\tau_i \\
= q(f(T^S)_{n_i^2}) + f(T^S)_{n_i}\tau_i^S \\
= f(qT^S_{n_i^2} + T^S_{n_i}\tau_i^S) \\
= f((T^S)_{n_i^2}).
\]

Using the proposition above, we shall henceforth identify $H_{S,Z}$ with its images in $H_Z$ and $H_{Z}$. Thus, we have the following chain of inclusions:

$$H_{S,aff,Z} = H_{S,Z} \subset H_{aff,Z} \subset H_Z.$$

**Proposition 3.4.** Let $h' \in X_*(T)$ denote the fixed cocharacter lifting a generator of $X_*(T/T_S)$.

1. As a left (resp. right) $H_{S,Z}$-module, $H_Z$ is free with basis $\{T^S_{\omega h'(a)}\}_{j \in \mathbb{Z}, a \in k^\times}$.
2. As a left (resp. right) $H_{S,Z}$-module, $H_Z$ is free with basis $\{T^S_{\omega h'(a)}\}_{0 \leq j < n, a \in k^\times}$.

**Proof.** This follows immediately from Proposition 2.3 and the braid relations of Theorem 3.1. □

**Corollary 3.5.**

1. The subspace

$$H'_Z := \bigoplus_{j \leq j, a \in k^\times \atop (j,a) \neq (0,1)} H_{S,Z}T^S_{\omega h'(a)}$$

is stable by the action of left and right multiplication by $H_{S,Z}$. Moreover, we have

$$H_Z \cong H_{S,Z} \oplus H'_Z$$

as both left and right $H_{S,Z}$-modules.

2. The subspace

$$H'_Z := \bigoplus_{0 \leq j < n, a \in k^\times \atop (j,a) \neq (0,1)} H_{S,Z}T^S_{\omega h'(a)}$$

is stable by the action of left and right multiplication by $H_{S,Z}$. Moreover, we have

$$H_Z \cong H_{S,Z} \oplus H'_Z$$

as both left and right $H_{S,Z}$-modules.

**Proof.** It is clear that $H'_Z$ is stable by left multiplication by $H_{S,Z}$. To show it is stable by right multiplication, let $w \in W^1_S$. One easily sees that $\omega^j h'(a)$ normalizes $N_{G_S}(T_S)$ and $T_S(1 + p)$, so that (by abuse of notation) we have $\omega^j h'(a)wh'(a)^{-1}\omega^{-j} \in W^1_S$. Since $\ell(\omega^j h'(a)) = 0$, we obtain

$$T^S_{\omega h'(a)}T_w = T^S_{\omega^j h'(a)wh'(a)^{-1}\omega^{-j} \omega^j h'(a)} \in H_{S,Z}T^S_{\omega h'(a)}.$$

□

Over the next several sections, we present some consequences of the interactions between these algebras.
4. Equivalence of Categories between $G_S$-Representations and $H_S$-modules

4.1. Mod-$p$ Representations. Let $\bullet$ denote either the empty symbol or $S$. From this point onwards, we denote by

$$C_\bullet := C_{\bullet, \mathbb{Z} \otimes \mathbb{F}_p}, \quad H_\bullet := H_{\bullet, \mathbb{Z} \otimes \mathbb{F}_p}, \quad H_{\bullet, \text{aff}} := H_{\bullet, \text{aff}, \mathbb{Z} \otimes \mathbb{F}_p},$$

$$C := C_{\mathbb{Z} \otimes \mathbb{F}_p}, \quad H := H_{\mathbb{Z} \otimes \mathbb{F}_p}$$

the base change of each object of $\mathbb{F}_p$.

We shall now be concerned with the category $\text{Rep}_{\mathbb{F}_p}(G_{\bullet})$ of smooth representations of $G_{\bullet}$ over $\mathbb{F}_p$. Let $\pi$ be a smooth $\mathbb{F}_p$-representation of the group $G_{\bullet}$; Frobenius Reciprocity for compact induction gives

$$\pi I_{\bullet, (1)} \cong \text{Hom}_{I_{\bullet, (1)}}(1, \pi |_{I_{\bullet, (1)}}) \cong \text{Hom}_{C_{\bullet}}(\text{c-ind}^{I_{\bullet, (1)}}(1), \pi) \cong \text{Hom}_{G_{\bullet}}(C_{\bullet}, \pi),$$

where $1$ denotes the trivial character of $I_{\bullet, (1)}$. The algebra $H_\bullet$ has a natural right action on $\text{Hom}_{G_{\bullet}}(C_{\bullet}, \pi)$, which induces a right action on $\pi I_{\bullet, (1)}$. In this way, we obtain the functor of $I_{\bullet, (1)}$-invariants

$$I_{\bullet} : \text{Rep}_{\mathbb{F}_p}(G_{\bullet}) \longrightarrow \text{Mod} - H_\bullet \quad \pi \mapsto \pi I_{\bullet, (1)}$$

from the category of smooth $\mathbb{F}_p$-representations of $G_{\bullet}$ to the category of right $H_\bullet$-modules.

Let $\text{Rep}^{I_{\bullet, (1)}}_{\mathbb{F}_p}(G_{\bullet})$ denote the full subcategory of $\text{Rep}_{\mathbb{F}_p}(G_{\bullet})$ of objects generated by their space of $I_{\bullet, (1)}$-invariants. We continue to denote by $I_{\bullet}$ the functor above restricted to the subcategory $\text{Rep}^{I_{\bullet, (1)}}_{\mathbb{F}_p}(G_{\bullet})$. Lemma 3 Part (1) of [4] implies that this functor is faithful.

Given a right $H_\bullet$-module $m$, we may consider the $G_{\bullet}$-representation $m \otimes H_\bullet C_{\bullet}$, with the action of $G_{\bullet}$ given on the right tensor factor. We thus obtain a functor

$$T_{\bullet} : \text{Mod} - H_\bullet \longrightarrow \text{Rep}^{I_{\bullet, (1)}}_{\mathbb{F}_p}(G_{\bullet})$$

$$m \mapsto m \otimes H_\bullet C_{\bullet}.$$
It is natural to ask whether the functors defined above induce equivalences of categories. This shall be the main goal of this section. We begin with some simple lemmas.

**Lemma 4.1.**

1. There exists an isomorphism
   \[ \mathcal{H} \otimes_{\mathcal{H}_S} C_S \cong C|_{G_S} \]
   which is both \( G_S \)-equivariant and \( \mathcal{H} \)-equivariant.

2. There exists an isomorphism
   \[ \mathcal{H} \otimes_{\mathcal{H}_S} C_S \cong C|_{G_S} \]
   which is both \( G_S \)-equivariant and \( \mathcal{H} \)-equivariant.

**Proof.** We prove the first assertion. Recall the map \( f \) defined in the proof of Proposition 3.3:

\[
\begin{align*}
\mathcal{C}_S & \rightarrow \mathcal{C}|_{G_S} \\
1_{I_5(1)} & \rightarrow 1_{I(1)}
\end{align*}
\]

It is obviously \( G_S \)- and \( \mathcal{H}_S \)-equivariant. By Frobenius Reciprocity, we obtain a map \( \tilde{f} \), defined by

\[
\begin{align*}
\tilde{f}: \mathcal{H} \otimes_{\mathcal{H}_S} C_S & \rightarrow \mathcal{C}|_{G_S} \\
T_w \otimes g.1_{I_5(1)} & \mapsto T_w(f(g.1_{I_5(1)})) = g.T_w(1_{I(1)})
\end{align*}
\]

for \( g \in G_S \). The map \( \tilde{f} \) is \( G_S \)- and \( \mathcal{H} \)-equivariant. Therefore it remains to show that it is an isomorphism.

We note that \( \{ \omega^j h'(a) \}_{j \in \mathbb{Z}, a \in k^\times} \) is a set of coset representatives for the double coset space \( I(1) \backslash G/G_S \). Using the Mackey decomposition, we obtain

\[
\mathcal{C}|_{G_S} \cong \bigoplus_{j \in \mathbb{Z}, a \in k^\times} \text{c-ind}^{I(1)}_{I(1)} \omega^j h'(a)G_S(1),
\]

where \( \text{c-ind}^{I(1)}_{I(1)} \omega^j h'(a)G_S(1) \) denotes the subspace of \( \mathcal{C} \) with support contained in \( I(1) \omega^j h'(a)G_S \). Analogously, \( \{ T_{\omega^j h'(a)} \}_{j \in \mathbb{Z}, a \in k^\times} \) is a basis for \( \mathcal{H} \) over \( \mathcal{H}_S \), and we obtain

\[
\mathcal{H} \otimes_{\mathcal{H}_S} C_S \cong \bigoplus_{j \in \mathbb{Z}, a \in k^\times} T_{\omega^j h'(a)} \otimes_{\mathcal{H}_S} \mathcal{C}_S.
\]

It is clear that \( \tilde{f} \) defines an isomorphism between \( T_{\omega^j h'(a)} \otimes_{\mathcal{H}_S} \mathcal{C}_S \) and \( \text{c-ind}^{I(1)}_{I(1)} \omega^j h'(a)G_S(1) \), which finishes the proof. \( \square \)

**Corollary 4.2.**

1. Let \( \mathcal{M} \) be a right \( \mathcal{H} \)-module. We then have an isomorphism
   \[ \mathcal{M}|_{\mathcal{H}_S} \otimes_{\mathcal{H}_S} C_S \cong \mathcal{M} \otimes_{\mathcal{H}} \mathcal{C}|_{G_S} \]
   as \( G_S \)-representations.

2. Let \( \overline{\mathcal{M}} \) be a right \( \mathcal{H} \)-module. We then have an isomorphism
   \[ \overline{\mathcal{M}}|_{\mathcal{H}_S} \otimes_{\mathcal{H}_S} C_S \cong \overline{\mathcal{M}} \otimes_{\mathcal{H}} \mathcal{C}|_{G_S} \]
   as \( G_S \)-representations.
Proof. We have
\[
\mathcal{M}|_{\mathcal{H}_S} \otimes \mathcal{H}_S \mathcal{C}_S \cong \mathcal{M} \otimes \mathcal{H} \otimes \mathcal{H}_S \mathcal{C}_S \\
\cong \mathcal{M} \otimes \mathcal{H} \mathcal{C}|_{\mathcal{H}_S},
\]
where the last line follows from the preceding lemma. The second claim follows similarly. □

Corollary 4.3. The module \( \mathcal{C} \) is flat over \( \mathcal{H} \) if and only if \( \mathcal{C}_S \) is flat over \( \mathcal{H}_S \), if and only if \( \mathcal{C} \) is flat over \( \mathcal{H} \).

Proof. This is a simple exercise in (non)commutative algebra, which we recall.

Assume first that \( \mathcal{C}_S \) is flat over \( \mathcal{H}_S \), and let
\[
0 \rightarrow \mathcal{M}' \rightarrow \mathcal{M} \rightarrow \mathcal{M}'' \rightarrow 0
\]
be a short exact sequence of right \( \mathcal{H} \)-modules. Restricting to \( \mathcal{H}_S \) and tensoring by \( \mathcal{C}_S \), we obtain a short exact sequence
\[
0 \rightarrow \mathcal{M}'|_{\mathcal{H}_S} \otimes \mathcal{H}_S \mathcal{C}_S \rightarrow \mathcal{M}|_{\mathcal{H}_S} \otimes \mathcal{H}_S \mathcal{C}_S \rightarrow \mathcal{M}''|_{\mathcal{H}_S} \otimes \mathcal{H}_S \mathcal{C}_S \rightarrow 0
\]
of \( \mathcal{C}_S \)-representations. By Corollary 4.2, this exact sequence is equal to
\[
0 \rightarrow \mathcal{M}' \otimes \mathcal{H} \mathcal{C}|_{\mathcal{H}_S} \rightarrow \mathcal{M} \otimes \mathcal{H} \mathcal{C}|_{\mathcal{H}_S} \rightarrow \mathcal{M}'' \otimes \mathcal{H} \mathcal{C}|_{\mathcal{H}_S} \rightarrow 0.
\]
This implies that the sequence remains exact upon considering the action of \( G \), and therefore \( \mathcal{C} \) is flat over \( \mathcal{H} \).

Assume conversely that \( \mathcal{C} \) is flat over \( \mathcal{H} \), and let
\[
0 \rightarrow \mathcal{M}' \rightarrow \mathcal{M} \rightarrow \mathcal{M}'' \rightarrow 0
\]
be a short exact sequence of right \( \mathcal{H}_S \)-modules. Let \( \tilde{\mathcal{M}} = \mathcal{M} \otimes \mathcal{H}_S \mathcal{H} \) denote the induced module (with similar notation for \( \mathcal{M}' \) and \( \mathcal{M}'' \)). Since \( \mathcal{H} \) is free over \( \mathcal{H}_S \), it is flat in particular, and therefore we obtain an exact sequence of \( G \)-representations
\[
0 \rightarrow \tilde{\mathcal{M}}' \otimes \mathcal{H} \mathcal{C} \rightarrow \tilde{\mathcal{M}} \otimes \mathcal{H} \mathcal{C} \rightarrow \tilde{\mathcal{M}}'' \otimes \mathcal{H} \mathcal{C} \rightarrow 0.
\]
Restricting to \( \mathcal{H}_S \) and once again applying Corollary 4.2, we obtain an exact sequence of \( \mathcal{H}_S \)-representations
\[
0 \rightarrow \tilde{\mathcal{M}}'|_{\mathcal{H}_S} \otimes \mathcal{H}_S \mathcal{C}_S \rightarrow \tilde{\mathcal{M}}|_{\mathcal{H}_S} \otimes \mathcal{H}_S \mathcal{C}_S \rightarrow \tilde{\mathcal{M}}''|_{\mathcal{H}_S} \otimes \mathcal{H}_S \mathcal{C}_S \rightarrow 0.
\]
Since \( \mathcal{H}_S \) is a direct factor of \( \mathcal{H} \) as an \( \mathcal{H}_S \)-module (cf. Corollary 3.5), we know that \( \mathcal{M} \otimes \mathcal{H}_S \mathcal{C}_S \) is a direct factor of \( \tilde{\mathcal{M}}|_{\mathcal{H}_S} \otimes \mathcal{H}_S \mathcal{C}_S \) (and likewise for \( \mathcal{M}' \) and \( \mathcal{M}'' \)). Hence, we obtain a diagram
\[
\begin{array}{ccc}
\mathcal{M}' \otimes \mathcal{H}_S \mathcal{C}_S & \longrightarrow & \mathcal{M} \otimes \mathcal{H}_S \mathcal{C}_S & \longrightarrow & \mathcal{M}'' \otimes \mathcal{H}_S \mathcal{C}_S & \longrightarrow & 0 \\
\downarrow & & \downarrow & & \downarrow & & \\
\tilde{\mathcal{M}}'|_{\mathcal{H}_S} \otimes \mathcal{H}_S \mathcal{C}_S & \longrightarrow & \tilde{\mathcal{M}}|_{\mathcal{H}_S} \otimes \mathcal{H}_S \mathcal{C}_S & \longrightarrow & \tilde{\mathcal{M}}''|_{\mathcal{H}_S} \otimes \mathcal{H}_S \mathcal{C}_S & \longrightarrow & 0
\end{array}
\]
where both rows are exact and all squares commute. This implies that the leftmost arrow in the top row is injective, which implies \( \mathcal{C}_S \) is flat over \( \mathcal{H}_S \). The proof of the second equivalence is similar. □

Corollary 4.4.

(1) Let \( n = 2 \). Then \( \mathcal{C}_S \) is flat if and only if \( q = p \).

(2) Let \( n = 3 \) and assume \( q = p \). Then \( \mathcal{C}_S \) is flat if and only if \( p = 2 \).

Proof. Using the previous corollary, part (1) follows from [23], Théorème 1, while part (2) follows from [28], Théorème 7.15. □
Lemma 4.5. Assume that \((n, q) = 1\) and let \(\pi \in \text{Rep}_{F_p}^{I(1)}(G)\). We then have an equality of vector spaces \(\pi^{I_1(1)} = \pi^{I(1)}\).

Proof. It is clear that \(\pi^{I(1)} \subset \pi^{I_1(1)}\). We prove the opposite inclusion.

Consider the short exact sequence
\[
1 \longrightarrow I_1(1) \longrightarrow I(1) \overset{\text{det}}{\longrightarrow} 1 + p \longrightarrow 1.
\]
By Proposition 6(b) of Chapitre IV and Lemme 2 of Chapitre V of [30], the map \(x \mapsto x^{1/n}\) is an automorphism of \(1 + p\) (since \(p\) and \(n\) are relatively prime). Hence, if \(Z\) denotes the center of \(G\), the map
\[
x \mapsto \begin{pmatrix} x^{1/n} \\ \vdots \\ x^{1/n} \end{pmatrix}
\]
gives an isomorphism \(1 + p \cong Z(1 + p)\), and a section to the surjection \(I(1) \overset{\text{det}}{\longrightarrow} 1 + p\). Thus, we have a decomposition
\[
I(1) \cong I_1(1) \times Z(1 + p).
\]
Now, since \(Z(1 + p)\) is contained in \(I(1)\), it acts trivially on \(\pi^{I(1)}\). As \(\pi\) is generated by its space of \(I(1)\)-invariants, \(Z(1 + p)\) acts trivially on the whole of \(\pi\). Hence, by the above decomposition, we get \(\pi^{I_1(1)} \subset \pi^{I(1)}\).

\(\square\)

Remark. By considering the action of \(H\) on \(\pi^{I(1)}\) and restricting to \(H_1\), the above lemma actually yields an isomorphism of \(H_1\)-modules
\[
\pi^{I_1(1)} \cong \pi^{I(1)}|_{H_1}.
\]

Theorem 4.6. Assume that \((n, q) = 1\). The functors \(\mathcal{I}\) and \(\mathcal{T}\) induce an equivalence of categories between \(\text{Rep}_{F_p}^{I(1)}(G)\) and \(\text{Mod} - \mathcal{H}\) if and only if \(\mathcal{I}_1\) and \(\mathcal{T}_1\) induce an equivalence of categories between \(\text{Rep}_{F_p}^{I_1(1)}(G_1)\) and \(\text{Mod} - \mathcal{H}_1\), if and only if \(\mathcal{T}\) and \(\mathcal{T}_1\) induce an equivalence of categories between \(\text{Rep}_{F_p}^{I(1)}(G_{\pi=1})\) and \(\text{Mod} - \mathcal{H}\).

Proof. Once again, the proofs of both equivalences are similar. We prove the first statement.

\((\Longrightarrow)\) Assume first that \(\mathcal{I}\) and \(\mathcal{T}\) induce an equivalence of categories, and let \(m\) be a right \(\mathcal{H}\)-module. We will show that the natural map
\[
m \longrightarrow I_1 \circ T_1(m) = (m \otimes \mathcal{H}_1 \mathcal{C}_1)^{I_1(1)}
\]
is an isomorphism.

Let \(\tilde{m}\) denote the induced \(\mathcal{H}\)-module \(m \otimes \mathcal{H}_1 \mathcal{H}\), and let \(m'\) denote the right \(\mathcal{H}_1\)-module \(m \otimes \mathcal{H}_1 \mathcal{H}_1'(\otimes \mathcal{H}_1' \mathcal{F}_p)\) (where \(\mathcal{H}_1'\) is as in Corollary 3.5). Since \(\mathcal{H}_1\) is a direct summand of \(\mathcal{H}\), we have an injection
\[
m \longrightarrow \tilde{m}|_{\mathcal{H}_1} \cong m \oplus m'.
\]
By Corollary 4.2, we have (in the category of \(G_1\)-representations)
\[
\tilde{m}|_{\mathcal{H}_1} \cong \tilde{m} \otimes \mathcal{H}_1 \mathcal{C}_{1|G_1}.\]
Taking $I_S(1)$-invariants of both sides and applying equation (4) gives

$$\left(\tilde{m}\right|_{H_S \otimes H_S C_S})^{I_S(1)} \cong \left(\tilde{m} \otimes H S\right)^{I(1)}|_{H_S} \cong \left(\tilde{m} \otimes H C\right)^{I(1)}|_{H_S}. $$

Since $I$ and $T$ induce an equivalence, we have that the homomorphism

$$\tilde{m} \rightarrow I \circ T(\tilde{m}) = (\tilde{m} \otimes H C)^{I(1)}$$

is bijective. Thus we get

$$\tilde{m}|_{H_S} \cong \left(\tilde{m} \otimes H C\right)^{I(1)}|_{H_S} \cong \left(\tilde{m}|_{H_S \otimes H_S C_S}\right)^{I_S(1)},$$

and in particular

$$m \oplus m' \cong \left(m \otimes H_S C_S\right)^{I_S(1)} \oplus \left(m' \otimes H_S C_S\right)^{I_S(1)}.$$ 

Since the image of $m$ (resp. $m'$) under the natural map $\tilde{m} \rightarrow (\tilde{m} \otimes H C)^{I(1)}$ must lie in the space $\left(m \otimes H_S C_S\right)^{I_S(1)}$ (resp. $\left(m' \otimes H_S C_S\right)^{I_S(1)}$), we conclude that

$$m \cong \left(m \otimes H_S C_S\right)^{I_S(1)} = I \circ T_S(m).$$

Now let $\pi \in \text{Rep}_{I_S(1)}^L(G_S)$, and consider the natural map

$$T_S \circ \mathcal{I}_S(\pi) = \pi^{I_S(1)} \otimes H_S C_S \rightarrow \pi$$

$$v \otimes 1_{I_S(1)} \rightarrow g \cdot v,$$

where $v \in \pi^{I_S(1)}$ and $g \in G_S$. Since $\pi$ is generated by its space of $I_S(1)$-invariant vectors, this map is surjective. Letting $\pi'$ denote its kernel, we obtain a short exact sequence

$$0 \rightarrow \pi' \rightarrow \pi^{I_S(1)} \otimes H_S C_S \rightarrow \pi \rightarrow 0.$$ 

Taking $I_S(1)$-invariants of this short exact sequence yields

$$0 \rightarrow (\pi')^{I_S(1)} \rightarrow \left(\pi^{I_S(1)} \otimes H_S C_S\right)^{I_S(1)} \rightarrow \pi^{I_S(1)},$$

and the statement just proved shows that the third arrow is an isomorphism. Hence $(\pi')^{I_S(1)} = 0$, and faithfulness of the functor $\mathcal{I}_S$ shows $\pi' = 0$. We conclude that

$$T_S \circ \mathcal{I}_S(\pi) = \pi^{I_S(1)} \otimes H_S C_S \cong \pi.$$ 

($\Longleftrightarrow$) Assume now that $\mathcal{I}_S$ and $T_S$ induce an equivalence of categories, and let $M \in \text{Mod}_{-H}$. Consider the natural map

$$M \rightarrow \mathcal{I} \circ T(M) = (M \otimes H C)^{I(1)}$$

$$m \rightarrow m \otimes 1_{I(1)}.$$ 

We claim that this map is an isomorphism. Indeed, if we restrict this morphism to $H_S$ and use Corollary 4.2 and equation (4), we obtain

$$M|_{H_S} \rightarrow (M \otimes H C)^{I(1)}|_{H_S} \cong (M \otimes H C|_{G_S})^{I_S(1)} \cong (M|_{H_S \otimes H_S C_S})^{I_S(1)}.$$
Since $\mathcal{I}_S$ and $\mathcal{T}_S$ induce an equivalence of categories, this map is an isomorphism, and we obtain

$$\mathcal{M} \cong (\mathcal{M} \otimes_{\mathcal{H}} \mathcal{C})^{(1)} = \mathcal{I} \circ \mathcal{T}(\mathcal{M}).$$

Now let $\Pi \in \operatorname{Rep}^{F(1)}_{\mathbb{F}_p}(G)$. In order to show that $\mathcal{T} \circ \mathcal{I}$ is naturally isomorphic to $\operatorname{id}_{\operatorname{Rep}^{I(1)}_{\mathbb{F}_p}(G)}$, we proceed exactly as in the proof of $\mathcal{T}_S \circ \mathcal{I}_S \simeq \operatorname{id}_{\operatorname{Rep}^{I_S(1)}_{\mathbb{F}_p}(G_S)}$ above. Hence, we conclude

$$\mathcal{T} \circ \mathcal{I}(\Pi) = \Pi^{(1)} \otimes_{\mathcal{H}} \mathcal{C} \cong \Pi.$$

\[\square\]

**Corollary 4.7.** Let $\mathcal{I} : \operatorname{Rep}^{F(1)}_{\mathbb{F}_p}(G) \longrightarrow \operatorname{Mod} - \mathcal{H}$ denote the functor of $I(1)$ invariants.

(1) The functor $\mathcal{I}$ induces an equivalence of categories for $n = 2$ and $F = \mathbb{Q}_p$ with $p > 2$.

Let $\mathcal{I}_S : \operatorname{Rep}^{I_S(1)}_{\mathbb{F}_p}(G_S) \longrightarrow \operatorname{Mod} - \mathcal{H}_S$ denote the functor of $I_S(1)$ invariants.

(2) The functor $\mathcal{I}_S$ induces an equivalence of categories for $n = 2$ and $F = \mathbb{Q}_p$ with $p > 2$.

(3) The functor $\mathcal{I}_S$ does not induce an equivalence of categories when $n = 2$ and $q > p > 2$.

(4) The functor $\mathcal{I}_S$ does not induce an equivalence of categories when $n = 2$ and $F = \mathbb{F}_p((T))$ with $p > 2$.

(5) The functor $\mathcal{I}_S$ does not induce an equivalence of categories when $n = 3$ and $q = p > 3$.

**Proof.** Using Theorem 4.6 above, parts (1) - (4) follow from Théorème 1.3 of [24], and part (5) follows from Corollary 4.4. \[\square\]

### 4.2. Generalizations

We now provide some generalizations of the above results. As the proofs are virtually the same as the ones given above for $\operatorname{GL}_n$, we will omit them (for the most part), and only indicate where they differ.

#### 4.2.1. Other Reductive Groups

Let $G$ denote the group of $F$-rational points of a split, connected, reductive group, with simply connected derived subgroup. We denote by $G_S$ the group of $F$-rational points of the derived subgroup, by $T$ a maximal split torus of $G$, and set $T_S := T \cap G_S$. The set of roots of $T$ acting on $\operatorname{Lie}(G)$ is denoted by $\Phi$, and we fix a set of simple roots $\Pi \subset \Phi$; restriction to $T_S$ gives a bijection between $\Phi$ and the set of roots of $T_S$ acting on $\operatorname{Lie}(G_S)$ ([6], Section 21.1).

Let $\bullet$ denote either the empty symbol or $S$. Each of the groups defined above have integral models defined over $\mathfrak{o}$ (cf. [32], Sections 3.4, 3.5, and 3.8), and therefore we can speak of the subgroup $T_{\bullet}(\mathfrak{o})$, its maximal pro-$p$ subgroup $T_{\bullet}(1 + p)$, and the group $T_{\bullet}(k)$. We define the following Weyl groups:

$$W_{\bullet,0} := T_{G_{\bullet}}(T_{\bullet}) / T_{\bullet},$$

$$W_{\bullet} := T_{G_{\bullet}}(T_{\bullet}) / T_{\bullet}(\mathfrak{o}),$$

$$W_{\bullet}^{(1)} := T_{G_{\bullet}}(T_{\bullet}) / T_{\bullet}(1 + p).$$

The choice of simple roots $\Pi$ provides us with a set of simple affine reflections in $W_{\bullet}$; we let $W_{\bullet, \text{aff}}$ denote the subgroup these reflections generate. See [22], Section 1.5 for more details.

The injection $N_{G}(T_S) \hookrightarrow N_{G}(T)$ induces an injection

$$W_{S} = N_{G_S}(T_S) / T_S(\mathfrak{o}) \hookrightarrow N_{G}(T) / T(\mathfrak{o}) = W,$$
which fits into a diagram

\[
\begin{array}{cccccc}
1 & \longrightarrow & X_*(\mathbb{T}_S) & \longrightarrow & \mathbb{W}_S & \longrightarrow & \mathbb{W}_{S,0} & \longrightarrow & 1 \\
& & \downarrow & & \downarrow & & \downarrow & \downarrow & \\
1 & \longrightarrow & X_*(\mathbb{T}) & \longrightarrow & \mathbb{W} & \longrightarrow & \mathbb{W}_0 & \longrightarrow & 1
\end{array}
\]

(5)

with exact rows and commuting squares. Here we have used the isomorphism \(X_*(\mathbb{T}_\bullet) \cong \mathbb{T}_\bullet \setminus \mathbb{T}_\bullet(\mathfrak{o})\), given by sending a cocharacter \(\xi\) to the class of \(\xi(\varpi^{-1})\).

We have the following results regarding the above Weyl groups.

**Proposition 4.8.** The map \(\iota\) induces an isomorphism \(\mathbb{W}_{S,0} \cong \mathbb{W}_0\).

*Proof.* This follows from Section 21.1 and Theorem 21.2 of [6]. □

**Proposition 4.9.** The map \(\iota\) induces an isomorphism \(\mathbb{W}_S \cong \mathbb{W}_{aff}\).

*Proof.* We note firstly that \(\iota\) restricts to a bijection between the coroots of \(\mathbb{T}_S\) and the coroots of \(\mathbb{T}\). By fixing compatible splittings in diagram (5), the discussion contained in Section 1.5 of [22] and the previous proposition imply that the map \(\iota\) induces an isomorphism between \(\mathbb{W}_{S,aff}\) and \(\mathbb{W}_{aff}\). The assumption that \(G_S\) is simply connected implies that the submodule of \(X_*(\mathbb{T}_S)\) generated by the coroots of \(G_S\) is the whole of \(X_*(\mathbb{T}_S)\), and therefore \(\mathbb{W}_{S,aff} = \mathbb{W}_S\). □

Now, Section 1.5 of [22] implies that \(\mathbb{W}\) admits a decomposition

\[\mathbb{W} \cong \Omega \times \mathbb{W}_{aff} \cong \Omega \times \mathbb{W}_S,\]

where \(\Omega\) denotes the subgroup of elements of length 0 in \(\mathbb{W}\) (the length on \(\mathbb{W}\) is defined in Section 1.4 of *loc. cit.*). Furthermore, the groups \(\mathbb{W}^{(1)}_S\) and \(\mathbb{W}_S\) fit into a diagram

\[
\begin{array}{cccccc}
1 & \longrightarrow & \mathbb{T}_S(k) & \longrightarrow & \mathbb{W}^{(1)}_S & \longrightarrow & \mathbb{W}_S & \longrightarrow & 1 \\
& & \downarrow & & \downarrow & & \downarrow & \downarrow & \\
1 & \longrightarrow & \mathbb{T}(k) & \longrightarrow & \mathbb{W}^{(1)} & \longrightarrow & \mathbb{W} & \longrightarrow & 1
\end{array}
\]

with exact rows and commuting squares. The length function on \(\mathbb{W}^{(1)}_S\) is given by inflation from \(\mathbb{W}_S\), and after a quick diagram chase, we conclude the following.

**Proposition 4.10.** The coset spaces \(\mathbb{W}^{(1)}_S \setminus \mathbb{W}^{(1)}\) and \(\mathbb{W}^{(1)} / \mathbb{W}^{(1)}_S\) admit representatives of length 0.

We may now define the Hecke algebras. In the standard apartment (corresponding to \(\mathbb{T}\)) of the semisimple Bruhat-Tits building of \(G\) we fix a chamber, and let \(I\) denote the associated Iwahori subgroup. We let \(I(1)\) denote its pro-p radical, and set \(I_S := G_S \cap I, I_S(1) := G_S \cap I(1)\).

We consider the free \(\mathbb{Z}\)-module \(C_{\bullet,\mathbb{Z}}\) defined by

\[C_{\bullet,\mathbb{Z}} := \left\{ f : G_\bullet \longrightarrow \mathbb{Z} : \begin{array}{ll}
\diamond f(ig) = f(g) & \text{for } i \in I_\bullet(1), g \in G_\bullet \\
\diamond \text{supp}(f) \text{ is compact}
\end{array} \right\}.\]

This is naturally a \(G_\bullet\)-representation, with action given by right translation. We define the pro-p-Iwahori-Hecke algebra as

\[H_{\bullet,\mathbb{Z}} := \operatorname{End}_{G_\bullet}(C_{\bullet,\mathbb{Z}});\]

by Frobenius Reciprocity, we have an identification \(H_{\bullet,\mathbb{Z}} \cong C_{\bullet,\mathbb{Z}}^{I_\bullet(1)}\), with the \(\mathbb{Z}\)-algebra structure given by convolution of functions. Using a slight generalization of the Bruhat decomposition
(see Section 3.3.1 of [32] and Theorem 6 of [34]), we see that a basis for $H_{\bullet,Z}$ is given by the characteristic functions of the double cosets $I_\bullet(1)\dot{w}I_\bullet(1)$, where $\dot{w}$ is any lift of an element of $W_\bullet$. Theorem 1 of [34] once again gives us the structure of the algebra $H_{\bullet,Z}$, and we deduce the following results.

**Proposition 4.11.** There exists an injection of $\mathbb{Z}$-algebras

$$H_{S,Z} \hookrightarrow H_{Z},$$

which makes $H_{Z}$ into a free module over $H_{S,Z}$. Moreover, $H_{S,Z}$ is a direct summand of $H_{Z}$, both as a left and right $H_{S,Z}$-module.

We denote by

$$H_{\bullet} := H_{\bullet,Z} \otimes_{\mathbb{Z}} \overline{\mathbb{F}}_p \quad \text{and} \quad C_{\bullet} := C_{\bullet,Z} \otimes_{\mathbb{Z}} \overline{\mathbb{F}}_p$$

the base changes of $H_{\bullet,Z}$ and $C_{\bullet,Z}$ to $\overline{\mathbb{F}}_p$, respectively.

**Proposition 4.12.** There exists an isomorphism

$$H \otimes_{H_{S}} C_{S} \cong C|_{G_{S}},$$

which is both $G_{S}$-equivariant and $H$-equivariant.

**Corollary 4.13.** The module $C$ is flat over $H$ if and only if $C_{S}$ is flat over $H_{S}$.

4.2.2. *Iwahori-Hecke Algebras.* We now briefly recall Iwahori-Hecke algebras for the groups $GL_n(F)$ and $SL_n(F)$. The comparison of these algebras has been initiated by Abdellatif in [1], Section 6.2.

Let $\bullet$ denote either the empty symbol or $S$. We set

$$C_{\bullet,Z} := \left\{ f : G_{\bullet} \rightarrow \mathbb{Z} : \begin{array}{l} \diamond f(ig) = f(g) \text{ for } i \in I_{\bullet}, g \in G_{\bullet} \\ \diamond \text{supp}(f) \text{ is compact} \end{array} \right\},$$

equipped with a $G_{\bullet}$-action given by right translation. The *Iwahori-Hecke algebra* is defined as

$$H_{\bullet,Z} := \text{End}_{G_{\bullet}}(C_{\bullet,Z});$$

once again, we have $H_{\bullet,Z} \cong C_{\bullet,Z}^*$, with the $\mathbb{Z}$-algebra structure given by convolution of functions. Section 3.3.1 of [32] shows that a basis for $H_{\bullet,Z}$ is given by characteristic functions of the double cosets $I_{\bullet,w}I_{\bullet}$, where $\dot{w}$ is any lift of an element of $W_{\bullet}$. The structure of $H_{\bullet,Z}$ is given by [18], Theorem 3.3 and Proposition 3.4, and we again deduce the following results.

**Proposition 4.14.** There exists an injection of $\mathbb{Z}$-algebras

$$H_{S,Z} \hookrightarrow H_{\bullet},$$

which makes $H_{\bullet}$ into a free module over $H_{S,Z}$. Moreover, $H_{S,Z}$ is a direct summand of $H_{\bullet}$, both as a left and right $H_{S,Z}$-module.

**Proof.** The first claim is Théorème 6.2.1, part 2, of [1]. The statements about freeness and the direct sum decomposition follow exactly as in the proofs of Proposition 3.4 and Corollary 3.5, respectively.

We now let

$$H_{\bullet} := H_{\bullet,Z} \otimes_{\mathbb{Z}} \overline{\mathbb{F}}_p \quad \text{and} \quad C_{\bullet} := C_{\bullet,Z} \otimes_{\mathbb{Z}} \overline{\mathbb{F}}_p$$

denote the base changes of $H_{\bullet,Z}$ and $C_{\bullet,Z}$ to $\overline{\mathbb{F}}_p$, respectively.
Proposition 4.15. There exists an isomorphism
\[ \mathcal{H} \otimes_{\mathcal{H}_S} \mathcal{C}_S \cong \mathcal{C}|_{\mathcal{G}_S}, \]
which is both \( \mathcal{G}_S \)-equivariant and \( \mathcal{H} \)-equivariant.

Corollary 4.16. The module \( \mathcal{C} \) is flat over \( \mathcal{H} \) if and only if \( \mathcal{C}_S \) is flat over \( \mathcal{H}_S \).

4.2.3. The group \( U(1,1)(E/F) \). Consider now the group \( U(1,1)(E/F) \), where \( E \) is the unramified quadratic extension of \( F \) contained in \( \overline{\mathbb{F}}_p \). We assume here that \( F \) has odd residual characteristic. The mod-\( p \) representation theory of the group \( U(1,1)(E/F) \) has been investigated in [2] and [21], and we now record how this group interacts with its Hecke algebra.

Let \( Iw(1) \) denote the pro-\( p \)-Iwahori subgroup of \( U(1,1)(E/F) \), and let
\[ \mathcal{H}(U(1,1)(E/F), Iw(1)) := \text{End}_{U(1,1)(E/F)}(\text{c-ind}_{Iw(1)}^{U(1,1)(E/F)}(1)) \]
denote the pro-\( p \)-Iwahori-Hecke algebra of \( U(1,1)(E/F) \) (over \( \overline{\mathbb{F}}_p \)). One can show using the methods of [34] (cf. proof of Theorem 1) that the structure of \( \mathcal{H}(U(1,1)(E/F), Iw(1)) \) is similar to that of the pro-\( p \)-Iwahori-Hecke algebra of the derived group \( SU(1,1)(E/F) \cong SL_2(F) \). Letting \( n = 2 \), we deduce the following.

Proposition 4.17. There exists an injection of algebras
\[ \mathcal{H}_S \hookrightarrow \mathcal{H}(U(1,1)(E/F), Iw(1)) \]
which makes \( \mathcal{H}(U(1,1)(E/F), Iw(1)) \) into a free module of finite rank over \( \mathcal{H}_S \). Moreover, \( \mathcal{H}_S \) is a direct summand of \( \mathcal{H}(U(1,1)(E/F), Iw(1)) \), both as a left and right \( \mathcal{H}_S \)-module.

Proposition 4.18. There exists an isomorphism
\[ \mathcal{H}(U(1,1)(E/F), Iw(1)) \otimes_{\mathcal{H}_S} \mathcal{C}_S \cong \text{c-ind}_{Iw(1)}^{U(1,1)(E/F)}(1)|_{SU(1,1)(E/F)}, \]
which is both \( SU(1,1)(E/F) \)-equivariant and \( \mathcal{H}(U(1,1)(E/F), Iw(1)) \)-equivariant.

Using these facts, Theorem 4.6 and its corollary carry over with little change, and we obtain the following consequence.

Theorem 4.19. The functor of \( Iw(1) \)-invariants induces an equivalence of categories between
\[ \mathcal{H}_{\mathcal{H}(U(1,1)(Q_p^2/Q_p))} \text{ and } \mathcal{H}(U(1,1)(Q_p^2/Q_p), Iw(1)). \]

5. \( L \)-packets of \( \mathcal{H}_S \)-modules

Once again, we let \( \bullet \) denote either the empty symbol or \( S \) throughout.
5.1. Supersingular Hecke Modules. We recall the following definition of supersingular modules.

**Definition 5.1** ([34], Definition 3). Let \( m \) be a nonzero right \( H_\bullet \)-module. Then \( m \) is said to be supersingular if the center of \( H_\bullet \) acts by a character which is null.

For a more precise definition of a null character of the center of \( H_\bullet \), we refer to Definition 2 (loc. cit.). We have the following theorems on the structure of supersingular modules.

**Theorem 5.2.** Let \( m \) be a simple supersingular right \( H_\bullet \)-module. Then \( m \) contains a character for the affine pro-p-Iwahori-Hecke algebra \( H_{\bullet, \text{aff}} \).

*Proof.* When \( G_\bullet = G = \text{GL}_n(F) \), this is the exactly the content of Section 7 of [25]. In fact, the same proofs apply to the group \( G_S \). One only needs to verify that the proof of Proposition 7.2 (loc. cit.) goes through. By Gordan’s Lemma, the monoid of dominant elements in \( T_S/T_S(\mathfrak{o}) \) is finitely generated. We simply replace the condition “\( n_j \) is at least 2” by “\( n_j \) is at least \( N + 1 \),” where \( N = \max(\langle \alpha, \mu \rangle) \) with \( \alpha \) ranging over \( \Phi^+ \) and \( \mu \) ranging over the generators of the dominant elements of \( T_S/T_S(\mathfrak{o}) \) (using the inverse of the isomorphism \( X_*(T_S) \cong T_S/T_S(\mathfrak{o}) \) sending \( \xi \) to the class of \( \xi(\varnothing) \)). See also Proposition 5.10 of [26]. \( \square \)

The characters of the algebra \( H_{\bullet, \text{aff}} \) are described explicitly by the following construction. Let \( \lambda: T_\bullet(k) \rightarrow \overline{\mathbb{F}}_p^\times \) be a character, and set

\[
S_\lambda := \{ n_i \in S : \lambda|_{T_i(k)} \text{ is the trivial character of } T_i(k) \}.
\]

We remark that the set \( S_\lambda \) can never have size \( n - 1 \); if the character \( \lambda \) is trivial on \( n - 1 \) of the tori \( T_i(k) \), then it must be trivial on the remaining one.

**Proposition 5.3** (Proposition 2 in [34]). The characters of \( H_{\bullet, \text{aff}} \) are parametrized by pairs \((\lambda, J)\), where \( \lambda: T_\bullet(k) \rightarrow \overline{\mathbb{F}}_p^\times \) is a character and \( J \subset S_\lambda \). We denote the character associated to the pair \((\lambda, J)\) by \( \chi^\bullet_{\lambda, J} \). This character is defined by

\[
\begin{align*}
(1) & \quad \chi^\bullet_{\lambda, J}(T_t) = \lambda(t) \text{ for } t \in T_\bullet(k), \\
(2) & \quad \chi^\bullet_{\lambda, J}(T_{n_i}) = 0 \text{ if } n_i \notin J, \\
(3) & \quad \chi^\bullet_{\lambda, J}(T_{n_i}) = -1 \text{ if } n_i \in J.
\end{align*}
\]

Let 1 denote the trivial character of \( T_\bullet(k) \). The proposition above shows in particular, that the algebra \( H_{\bullet, \text{aff}} \) possesses two distinguished characters: the trivial character \( \chi^\bullet_{1, \emptyset} \), sending all \( T_{n_i} \) to 0, and the sign character \( \chi^\bullet_{1, S} \), sending all \( T_{n_i} \) to \(-1\).

Since the algebras \( H_{S, \text{aff}} \) and \( H_S \) coincide, Theorem 5.2 implies that every simple supersingular module of \( H_S \) is a character. We have the following converse. This result is due to Rachel Ollivier, and I would like to thank her for allowing me to include it here.

**Theorem 5.4.** Let \( \chi^S_{\lambda, J}: H_S \rightarrow \overline{\mathbb{F}}_p \) be a character, which is not the trivial or sign character. Then \( \chi^S_{\lambda, J} \) is supersingular.

*Proof.* The case \( n = 2 \) is easily verified by hand, so we assume \( n > 2 \).

Recall from [34], Corollary 2, that we have an involutive automorphism \( \iota \) of \( H_S \) defined by

\[
\iota(T_{n_i}) = -T_{n_i} + \tau_i, \quad \iota(T_t) = T_t
\]

for \( t \in T_S(k) \). By Proposition 3.2 of [26], \( \chi^S_{\lambda, J} \) is supersingular if and only if \( \chi^S_{\lambda, J} \circ \iota = \chi^S_{\lambda, S \setminus J} \) is supersingular, so we may assume \( \chi^S_{\lambda, J}(T_{n_0}) = 0 \).
Let $\Pi'_\lambda$ denote the subset of $\{n_1, \ldots, n_{n-1}\} = S \setminus \{n_0\}$ such that $\lambda^{n_i} = \lambda$ for every $n_i \in \Pi'_\lambda$, and set $\Pi_\lambda = \Pi'_\lambda \setminus J$. Let $X_s(T_S) \otimes_{\mathbb{Z}} \mathbb{R}$ denote the standard apartment of the Bruhat-Tits building of $G_S$, $\sigma_0$ the vertex corresponding to $G_S(o)$, and $C$ the chamber corresponding to $I_S$. We let $F$ denote the facet of $C$ containing $\sigma_0$ satisfying
\[ \{n_i \in S \setminus \{n_0\} : \langle \alpha_i, \xi \rangle = 0 \text{ for all } \xi \in F \} = \Pi_\lambda. \]
If $F$ was equal to $\sigma_0$, we would have $\Pi_\lambda = \Pi'_\lambda = S \setminus \{n_0\}$, which implies $J = \emptyset$. Since $n > 2$, this gives $\lambda = 1$, implying that $\chi^S_{\lambda,J}$ is the trivial character. Hence, we must have $F \neq \sigma_0$.

Fix $\xi \in X_s(T_S)$ such that $\langle \alpha_i, \xi \rangle \geq 0$ for $1 \leq i \leq n - 1$, and such that $\ell(\xi) > 0$ (we define the length of a cocharacter using the isomorphism $X_s(T_S) \cong T_S/T_S(o) \subset W_S$ sending $\xi$ to the class of $\xi(\varnothing)$). Let $z_\xi$ denote the central element defined by $\xi$ (cf. [26], Section 2.2.1). By Proposition 4.1 and equation (4.1) (loc. cit.), we have
\[ \chi^S_{\lambda,J}(z_\xi) = \chi^S_{\lambda,J}(B^+_F(\xi)), \]
where $B^+_F(\xi)$ denotes the generalized Bernstein function defined in [27]. One can show, using the existence of a unique highest root, that the condition $F \neq \sigma_0$ implies $B^+_F(\xi) \in T_{n_0}H_S$.

This gives the desired result, since $\chi^S_{\lambda,J}(T_{n_0}) = 0$. See also Theorem 5.13 of [26].

5.2. $L$-packets. Consider now a simple supersingular module $\mathcal{M}$ for $\mathcal{H}$. By Theorem 5.2, $\mathcal{M}|_{H_S}$ contains a character. Restricting to $H_S$, we obtain a character $\chi$ of $H_S$, which furthermore must be supersingular. By the construction of the character $\chi$, the underlying vector space is stable by elements of the form $T_{h(a)}$ for $a \in k^\times$, and we obtain
\[ \mathcal{M}|_{H_S} = \sum_{j=0}^{n-1} \chi \cdot T_{\omega^j} \]
by simplicity of $\mathcal{M}$.

The element $\omega$ acts on the set $S$ by conjugation, and we see that
\[ \chi^S_{\lambda,J} \cdot T_{\omega^j} \cong \chi^{\lambda^\omega \cdot J \omega^j}, \]
where $\lambda^\omega$ is defined by $\lambda^\omega(t) = \lambda(\omega t \omega^{-1})$ for $t \in T_\omega(k) \cong I_\omega/I_\omega(1)$. This leads to the following definition.

**Definition 5.5.** Let $\lambda : T_S(k) \rightarrow \mathbb{F}_p^S$ be a character, and $J \subset S_\lambda \subset S$. We define an action of $\omega^J$ on the characters of $H_S$ by
\[ \omega^J \chi^S_{\lambda,J} := \chi^S_{\lambda^\omega \cdot J \omega^j} \cong \chi^S_{\lambda,J} \cdot T_{\omega^j}. \]
We define an $L$-packet of $H_S$-modules to be an orbit of $\omega^J$ acting on characters of $H_S$. We say an $L$-packet is supersingular if it consists entirely of supersingular characters, or, equivalently, if it contains a supersingular character.

In particular, we see that the size of an $L$-packet must divide $n$.

**Definition 5.6.** We say a supersingular character $\chi^S_{\lambda,J}$ is regular if there exists a simple supersingular $H$-module $\mathcal{M}$ of dimension $n$ such that $\chi^S_{\lambda,J}$ is a Jordan-Hölder factor of $\mathcal{M}|_{H_S}$. We say an $L$-packet is regular every character contained in the packet is regular, or, equivalently, if it contains a regular character.
It is an easy exercise to see that if $\mathfrak{M}$ is a simple $n$-dimensional supersingular $\mathcal{H}$-module, the restriction $\mathfrak{M}|_{\mathcal{H}_{\text{aff}}}$ is a direct sum of $n$ distinct characters. This implies that $\chi_{\lambda,J}^S$ is regular if and only if, for any character $\tilde{\lambda} : T(k) \to \mathbb{F}_p^\times$ satisfying $\tilde{\lambda}|_{T_S(k)} = \lambda$, the orbit of the character $\chi_{\tilde{\lambda},J}$ of $\mathcal{H}_{\text{aff}}$ has size $n$ under the action of $\omega^Z$ (where the action of $\omega^Z$ on $\chi_{\tilde{\lambda},J}$ is defined by equation (6)).

**Lemma 5.7.**

1. The number of supersingular characters of $\mathcal{H}_S$ is $q + q^2 + \ldots + q^{n-1}$.
2. The number of regular supersingular characters of $\mathcal{H}_S$ is

$$\frac{1}{q-1} \sum_{d|n} \mu \left( \frac{n}{d} \right) q^d,$$

where $\mu : \mathbb{N} \to \{-1, 0, 1\}$ denotes the Möbius function.

**Proof.** (1) We identify characters $\lambda$ of $T_S(k)$ with elements of $(\mathbb{Z}/(q-1)\mathbb{Z})^n/\langle(1, 1, \ldots, 1)\rangle$, that is, equivalence classes of $n$-tuples $((a_1, a_2, \ldots, a_n))$. Let $\chi_{\lambda,J}^S$ be a character of $\mathcal{H}_S$, where $J$ is a subset of $S$, and $\lambda$ is identified with $((a_1, a_2, \ldots, a_n))$. The condition $n_i \in J$ implies that $a_i - a_{i+1} \equiv 0 \pmod{q-1}$, with the indices taken modulo $n$. Thus, given $J \subseteq S$, there are exactly $(q-1)^{n-1-|J|}$ characters $\lambda$ such that $\chi_{\lambda,J}^S$ is a character of $\mathcal{H}_S$, and exactly one character $\lambda$ such that $\chi_{\lambda,J}^S$ is a character of $\mathcal{H}_S$. Therefore, the total number of characters of $\mathcal{H}_S$ is

$$1 + \sum_{J \subseteq S} (q-1)^{n-1-|J|} = 1 + (q-1)^{-1} \left( \sum_{j=0}^{n \choose j} (q-1)^{n-j} - 1 \right) = 1 + (q-1)^{-1}(q^n - 1) = 2 + q + q^2 + \ldots + q^{n-1}.$$

Since the only characters which are not supersingular are the trivial and sign characters, the result follows.

(2) By the remark following Definition 5.6, a character $\chi_{\tilde{\lambda},J}^S$ is regular if and only if we can find $\chi_{\tilde{\lambda},J}^S$ “lifting $\chi_{\lambda,J}^S$” whose orbit under $\omega^Z$ has size $n$. The result then follows from [34], Lemma 15 Part (3).}

In what follows, we let $(e_1, \ldots, e_j)$ denote the greatest common divisor of the integers $e_1, \ldots, e_j \in \mathbb{Z}$, with $(e_1) = e_1$. In addition, for any integer $a \in \mathbb{Z}$, we shall denote by

$$[a] = \frac{q^a - 1}{q - 1}$$

the $q$-analog of $a$.

To proceed further, we need a combinatorial lemma.

**Lemma 5.8.** Let $f : \mathbb{N} \to \mathbb{C}$ be an arbitrary arithmetic function, let $\mu : \mathbb{N} \to \{-1, 0, 1\}$ denote the Möbius function, and let $\sigma_0(m)$ denote the number of divisors of $m$. We then have

$$f(m) - \sum_{j=1}^{\sigma_0(m)-1} (-1)^{j+1} \sum_{1 \leq e_1 < \ldots < e_j < m \atop e_i | m} f((e_1, \ldots, e_j)) = \sum_{e|m} \mu \left( \frac{m}{e} \right) f(e).$$
Proof. Rewriting the left-hand side above, we obtain
\[
f(m) - \sum_{j=1}^{\sigma_0(m)-1} (-1)^j \sum_{1 \leq e_1 < \ldots < e_j < m} f((e_1, \ldots, e_j)) = f(m) + \sum_{e|m} f(e) \sum_{1 \leq e_1 < \ldots < e_j < m} (-1)^j.
\]
Therefore, it suffices to prove
\[
\mu \left( \frac{m}{e} \right) = \sum_{j=1}^{\sigma_0(m/e)-1} (-1)^j \{1 \leq e_1 < \ldots < e_j < m : e_i|m, (e_1, \ldots, e_j) = e\};
\]
setting \(m' = \frac{m}{e} \) and \(e'_i = \frac{e_i}{e}\), this is equivalent to showing
\[
\mu(m') = \sum_{j=1}^{\sigma_0(m')-1} (-1)^j \{1 \leq e'_1 < \ldots < e'_j < m' : e'_i|m', (e'_1, \ldots, e'_j) = 1\}.
\]
The claim now follows from (the example following) Proposition 4.29 in [3]; one takes \(P\) to be the distributive lattice of divisors of \(m'\), with partial order given by \(x \preceq y\) if and only if \(y\) divides \(x\).

Proposition 5.9. Let \(d\) be a divisor of \(n\), and let \(g(d)\) denote the number regular supersingular characters of \(\mathcal{H}_S\) whose orbit under \(\omega^Z\) has size dividing \(d\). We then have
\[
g(d) = \sum_{e|n} \mu \left( \frac{n}{e} \right) \left\lfloor \frac{e}{(d,e)} \right\rfloor, q - 1 \right).
\]
Proof. Let \(\chi_{\lambda,J}^S\) be a supersingular character whose orbit under \(\omega^Z\) has size dividing \(d\). This means that \(\omega^{-d}J\omega^d = J\), that is, the set \(J\) is stable under the map \(n_i \mapsto n_i + d\). Hence, the subsets \(J\) of \(S\) satisfying \(\omega^{-d}J\omega^d = J\) correspond bijectively to subsets \(J'\) of \(\{n_1, \ldots, n_d\}\) in the obvious way.

Let \(\lambda\) correspond to the equivalence class
\[
((a_1, a_2, \ldots, a_n)) \in (\mathbb{Z}/(q-1)\mathbb{Z})^n/(1,1,\ldots,1)).
\]
The condition \(\lambda^{\omega^d} = \lambda\) implies that there exists \(z \in \mathbb{Z}/(q-1)\mathbb{Z}\) such that
\[
a_{i+d} \equiv a_i + z \pmod{q-1}
\]
for every \(0 < i \leq n\) (where we consider the indices modulo \(n\)). Summing these equations gives
\[
\sum_{j=0}^{n/d-1} a_{i+jd} \equiv n d z + \sum_{j=0}^{n/d-1} a_{i+jd} \pmod{q-1},
\]
so that
\[
z \equiv 0 \pmod{\left(\frac{n}{d}, q - 1\right)}.
\]
The element corresponding to \(\lambda\) takes the form
\[
\left( (a_1, \ldots, a_d, a_1 + z, \ldots, a_d + z), a_1 + (\frac{n}{d} - 1) z, \ldots, a_d + (\frac{n}{d} - 1) z \right).
\]
Now, let \(J \subset S\) satisfy \(\omega^{-d}J\omega = J\), and let \(J'\) be the subset of \(\{n_1, \ldots, n_d\}\) to which it corresponds. Note that \(J'\) must be a proper subset, else we would have \(J = S\) and \(\lambda\) would
be the trivial character. The number of characters $\chi_{\lambda,J}^S$ which satisfy $\omega^d \chi_{\lambda,J}^S = \chi_{\lambda,J}^S$ and for which $J$ corresponds to a fixed $J'$ is therefore equal to

$$(q - 1)^{d - 1 - |J'|} \left( \frac{n}{d}, q - 1 \right).$$

Hence, the total number of supersingular characters satisfying $\omega^d \chi_{\lambda,J}^S = \chi_{\lambda,J}^S$ is equal to

$$-1 + \sum_{J' \leq \{n_1, \ldots, n_d\}} (q - 1)^{d - 1 - |J'|} \left( \frac{n}{d}, q - 1 \right) = -1 + (q - 1)^{-1} \left( \sum_{j=0}^{d} \binom{d}{j} (q - 1)^{d - j} - 1 \right) \times \left( \frac{n}{d}, q - 1 \right)$$

$$= -1 + (q - 1)^{-1}(q^d - 1) \left( \frac{n}{d}, q - 1 \right)$$

$$= -1 + [d] \left( \frac{n}{d}, q - 1 \right)$$

(the $-1$ accounts for the contribution of the trivial character $\chi_{1, \emptyset}^S$).

It remains to verify how many of these characters are regular. Let $\tilde{\lambda} : T(k) \rightarrow \mathbb{F}_p^\times$ be a character whose restriction to $T_3(k)$ is equal to $\lambda$, and let $e$ be a proper divisor of $n$. Denote by $\chi_{\tilde{\lambda},J}^S : \mathcal{H}_\text{aff} \rightarrow \mathbb{F}_p^\times$ a character of the affine Hecke algebra $\mathcal{H}_\text{aff}$ “lifting $\chi_{\lambda,J}^S$,” and assume $\omega^e \chi_{\tilde{\lambda},J}^S = \chi_{\tilde{\lambda},J}^S$. This implies in particular that $\omega^{-e}J \omega^e = J$; hence, we obtain $\omega^{-d,e}J \omega^{d,e} = J$, and the set of such $J$ correspond bijectively to subsets $J'$ of $\{n_1, \ldots, n_{(d,e)}\}$.

We let $\tilde{\lambda}$ correspond to

$$(a_1, a_2, \ldots, a_n) \in (\mathbb{Z}/(q - 1)\mathbb{Z})^n$$

(lifting the class $((a_1, a_2, \ldots, a_n)) \in (\mathbb{Z}/(q - 1)\mathbb{Z})^n/((1, 1, \ldots, 1))$ above). By the above computation, the $n$-tuple corresponding to $\tilde{\lambda}$ is of the form

$$\left( a_1, a_d, a_1 + z, \ldots, a_d + z, \ldots, a_1 + \left( \frac{n}{d} - 1 \right) z, \ldots, a_d + \left( \frac{n}{d} - 1 \right) z \right).$$

For an integer $i \in \mathbb{Z}$, we let $\overline{i} \in \mathbb{Z}$ denote the unique integer satisfying $0 < i \leq d$ and $i \equiv \overline{i} \pmod{d}$. The $n$-tuple corresponding to $\tilde{\lambda}$ then satisfies

$$(7) \quad a_i \equiv a_{\overline{i}} + \left\lfloor \frac{i - 1}{d} \right\rfloor z \pmod{q - 1}$$

for every $0 < i \leq n$. The condition $\tilde{\lambda}^{e} = \tilde{\lambda}$ implies, for example, that

$$a_1 \equiv a_{1 + je} \equiv a_{1 + \overline{je}} + \left\lfloor \frac{je}{d} \right\rfloor z \pmod{q - 1}$$

for every $0 \leq j < \frac{n}{e}$. Now, we have $je \equiv 0 \pmod{d}$ if and only if $j \equiv 0 \left( \mod \frac{d}{(d,e)} \right)$; setting $j = \frac{d}{(d,e)}$ above yields

$$\frac{e}{(d,e)}z \equiv 0 \pmod{q - 1},$$

which gives

$$z \equiv 0 \left( \mod \frac{q - 1}{\frac{e}{(d,e)}, q - 1} \right).$$
Equation (7) above also has the following consequence. Fix $0 < i \leq (d, e)$. For any integer $0 \leq m < \frac{n}{(d, e)}$, there exists a unique integer $0 \leq j < \frac{d}{(d, e)}$ such that $je \equiv m(d, e) \pmod{d}$. This gives

\[
a_{i+m(d,e)} \equiv a_{i+je} + \left\lfloor \frac{i + m(d,e) - 1}{d} \right\rfloor z
\]

This implies that the character $\tilde{\lambda}$ is determined by the integers $a_1, \ldots, a_{(d,e)}$ and the element $z$. Proceeding as above, given a proper subset $J'$ of $\{n_1, \ldots, n_{(d,e)}\}$, we obtain

\[
(q-1)^{(d,e)-1-|J'|} \left( \frac{e}{(d, e)}, q-1 \right)
\]

characters $\chi_{\lambda,J}$ such that the lift $\chi_{\tilde{\lambda},J}$ has an orbit of size dividing $e$, with $J$ corresponding to a fixed $J'$. Hence, the total number of supersingular characters $\chi_{\tilde{\lambda},J}$ such that the lift $\chi_{\tilde{\lambda},J}$ has an orbit of size dividing $e$ is

\[
-1 + [(d, e)] \left( \frac{e}{(d, e)}, q-1 \right).
\]

By the inclusion-exclusion principle, the number of regular supersingular characters of $H_S$ is

\[
-1 + [d] \left( \frac{n}{d}, q-1 \right) - \sum_{j=1}^{\sigma_0(n)-1} (-1)^{j+1} \sum_{\substack{1 \leq e_1 < \ldots < e_j < n \\ e_i \mid n}} -1 + [(d, e_1, \ldots, e_j)] \left( \frac{(e_1, \ldots, e_j)}{(d, e_1, \ldots, e_j)}, q-1 \right).
\]

Applying Lemma 5.8 with $f(e) = -1 + [(d, e)] \left( \frac{e}{(d, e)}, q-1 \right)$ and using the fact that $\sum_{e \mid n} \mu \left( \frac{n}{e} \right) = 0$ gives the result.

Remark. Evaluating the function $g(d)$ at 1, we obtain

\[
g(1) = \sum_{e \mid n} \mu \left( \frac{n}{e} \right) (e, q-1).
\]

As a function of $n$, $g(1)$ is multiplicative; this property implies that

\[
g(1) = \begin{cases} 
\varphi(n) & \text{if } (n, q-1) = n, \\
0 & \text{if } (n, q-1) \neq n,
\end{cases}
\]

where $\varphi$ denotes Euler’s phi function.
Corollary 5.10. Let \( d \) be a divisor of \( n \), and let \( h(d) \) denote the number of regular supersingular \( L \)-packets of \( H_S \)-modules of size \( d \). We then have
\[
h(d) = \frac{1}{d} \sum_{e \mid d} \mu \left( \frac{d}{e} \right) g(e).
\]

Proof. By the inclusion-exclusion principle and Lemma 5.8, the total number of regular supersingular characters with orbit of exact order \( d \) is
\[
g(d) - \sum_{j=1}^{\sigma_0(d)-1} (-1)^{j+1} \sum_{1 \leq e_1 < \ldots < e_j < d, e_i \mid d} g((e_1, \ldots, e_j)) = \sum_{e \mid d} \mu \left( \frac{d}{e} \right) g(e).
\]

Lemma 5.11. Let \( d \) be a divisor of \( n \).

1. We have \( g(d) \neq 0 \) if and only if \( \left( \frac{n}{d}, q-1 \right) = \frac{n}{d} \).
2. We have \( h(d) \neq 0 \) if and only if \( \left( \frac{n}{d}, q-1 \right) = \frac{n}{d} \).

Proof. By Corollary 5.10, it suffices to prove the first claim. The proof is a tedious (but straightforward) exercise in elementary number theory, and is left to the reader. \( \square \)

6. Galois Groups and Projective Galois Representations

We now recall the necessary objects in order to define projective Galois representations.

6.1. Galois Groups. Let \( G_F := \text{Gal}(\overline{F}/F) \) denote the absolute Galois group of \( F \), and let \( I_F \) denote the inertia subgroup of elements which act trivially on the residue field \( k_F \). For any extension \( L \) of \( F \), contained in \( \overline{F} \), we define \( G_L := \text{Gal}(\overline{F}/L) \). Let \( F^{ur} \) denote the maximal unramified extension of \( F \); we may then realize the subgroup \( I_F \) as
\[
I_F = \text{Gal}(F^{ur}/F).
\]
This gives \( G_F/I_F \cong \text{Gal}(F^{ur}/F) \cong \text{Gal}(\overline{k}/k) \cong \hat{\mathbb{Z}} \), where the last isomorphism is given by sending the geometric Frobenius to 1. We denote by \( \text{Fr}_q \) a fixed element of \( G_F \) whose image in \( \text{Gal}(F^{ur}/F) \) is equal to a geometric Frobenius element. Finally, for \( m \geq 1 \), we let \( F_m \) denote the unique unramified extension of \( F \) of degree \( m \) contained in \( \overline{F} \).

We fix a compatible system \( \{ q^m \sqrt[1]{\overline{x}} \}_{m \geq 1} \) of \( (q^m - 1) \)th roots of \( \overline{x} \), and let \( \omega_m : I_F \rightarrow \mathbb{F}^\times_p \) denote the character given by
\[
\omega_m : h \mapsto \iota \circ \sigma_F \left( \frac{h, \sqrt[q^m-1]{\overline{x}}}{q^m \sqrt[q^m-1]{\overline{x}}} \right),
\]
where \( h \in I_F \) and \( \sigma_F : \sigma_F \rightarrow k_F \) denotes the reduction modulo the maximal ideal. Lemma 2.5 of [10] shows that the character \( \omega_m \) extends to a character of \( G_{F_m} \); we continue to denote by \( \omega_m \) the extension which sends the element \( \text{Fr}_q^m \) to 1. Moreover, for \( \lambda \in \mathbb{F}^\times_p \), we let \( \mu_{m,\lambda} : G_{F_m} \rightarrow \mathbb{F}^\times_p \) denote the unramified character which sends \( \text{Fr}_q^m \) to \( \lambda \). The properties of these characters relevant to this discussion are summarized in the following lemma.
Lemma 6.1. Let $m$ be a positive integer.

(1) For $d$ dividing $m$, we have
$$\omega_{m}^{(q^{m}-1)/(q^{d}-1)} = \omega_{d}.$$ 

(2) For $h \in I_F$, we have
$$\omega_{m}(Fr_{q}^{h}Fr_{q}^{-1}) = \omega_{m}(h)^q.$$ 

(3) Any smooth $F_p$-character of $G_{F_{m}}$ is of the form $\mu_{m,\lambda}\omega_{r}$ with $\lambda \in \mathbb{F}_p^\times$ and $0 \leq r < q^m - 1$.

Proof. Part (1) is clear from the definition. Part (2) follows from the proof of Lemma 2.5 in [10], while part (3) is Lemma 2.2. □

6.2. Galois Representations. We begin by recalling the classification of irreducible $n$-dimensional mod-$p$ representations of the group $G_{F}$. Throughout, we assume that $GL_n(\mathbb{F}_p)$ and $PGL_n(\mathbb{F}_p)$ are given the discrete topology. We take [33], Sections 1.13 and 1.14, and [5], Section 2, as our references.

An element $r$ of $\mathbb{Z}/(q^n - 1)\mathbb{Z}$ is said to be primitive if we have
$$r \not\equiv 0 \pmod{\frac{n}{\gcd(n, d)}}$$
for every proper divisor $d$ of $n$. The necessary results are summarized in the following proposition.

Proposition 6.2.

(1) Any continuous irreducible $n$-dimensional mod-$p$ representation of $G_{F}$ is isomorphic to
$$\text{ind}_{G_{F_{n}}}^{G_{F}}(\mu_{n,\lambda}\omega_{r}),$$
where $\lambda \in \mathbb{F}_p^\times$, and $r \in \mathbb{Z}/(q^n - 1)\mathbb{Z}$ is primitive.

(2) We have an isomorphism
$$\text{ind}_{G_{F_{n}}}^{G_{F}}(\mu_{n,\lambda}\omega_{r}) \cong \text{ind}_{G_{F_{n}}}^{G_{F}}(\mu_{n,\lambda'}\omega_{r'})$$
if and only if $\lambda' = \lambda$ and $r' = q^a r$ for some $a \in \mathbb{Z}$.

(3) Restricting to $G_{F_{n}}$, we obtain
$$\text{ind}_{G_{F_{n}}}^{G_{F}}(\mu_{n,\lambda}\omega_{r})|_{G_{F_{n}}} \cong \mu_{n,\lambda}\omega_{r} \oplus \mu_{n,\lambda}\omega_{qr} \oplus \ldots \oplus \mu_{n,\lambda}\omega_{q^{n-1}r}.$$

(4) The representation $\text{ind}_{G_{F_{n}}}^{G_{F}}(\mu_{n,\lambda}\omega_{r})$ satisfies
$$\det(\text{ind}_{G_{F_{n}}}^{G_{F}}(\mu_{n,\lambda}\omega_{r})) = \mu_{1,(-1)^{n}+1} \otimes (\mu_{n,\lambda}\omega_{r}) \circ \text{ver} = \mu_{1,(-1)^{n}+1}\lambda\omega_{1},$$
where $\text{ver} : G_{F_{n}}^{ab} \to G_{F_{n}}^{ab}$ is the transfer map.

Proof. Parts (1) and (2) follow from Section 1.14 of [33], part (3) follows from Mackey theory, and part (4) may be deduced from Proposition 13.15 of [14]. See also Lemma 2.1.4 and the subsequent remarks in [5]. □

We now consider projective representations.
Definition 6.3. By an \( n \)-dimensional mod-\( p \) projective Galois representation we mean a continuous homomorphism from \( \mathcal{G}_F \) to \( \text{PGL}_n(\mathbb{F}_p) \). We say a projective Galois representation is irreducible if it does not factor through a proper parabolic subgroup of \( \text{PGL}_n(\mathbb{F}_p) \). Moreover, we say two projective representations \( \sigma \) and \( \sigma' \) are equivalent if there exists an element \( m \in \text{PGL}_n(\mathbb{F}_p) \) such that \( \sigma(g) = m\sigma'(g)m^{-1} \) for all \( g \in \mathcal{G}_F \). This equivalence relation will be denoted \( \sigma \sim \sigma' \).

Given any continuous \( n \)-dimensional Galois representation \( \rho \), we denote by

\[
[\rho] : \mathcal{G}_F \to \text{GL}_n(\mathbb{F}_p) \to \text{PGL}_n(\mathbb{F}_p)
\]

the projective representation obtained as the composition of \( \rho \) with the natural quotient map. The extent to which these representations constitute all projective Galois representations is given by the following theorem.

Theorem 6.4. We have

\[
H^2(\mathcal{G}_F, \mathbb{F}_p^\times) = 0,
\]

where we consider continuous cohomology. Consequently, every irreducible \( n \)-dimensional projective Galois representation lifts to a genuine Galois representation, i.e., is of the form \( [\rho] \), where \( \rho \) is a continuous irreducible \( n \)-dimensional Galois representation.

Proof. This follows from (the proof of) Theorem 4 (and its corollary) in [31]; one simply uses the decomposition \( \mathbb{F}_p^\times \cong \bigoplus_{\ell \neq p} \mathbb{Q}_\ell / \mathbb{Z}_\ell \).

Lemma 6.5. We have an equivalence

\[
\left[ \text{ind}_{\mathcal{G}_F}^{\mathcal{G}_F} (\mu_n, \lambda, \omega_n^r) \right] \sim \left[ \text{ind}_{\mathcal{G}_F}^{\mathcal{G}_F} (\omega_n^r) \right].
\]

Proof. Let \( \sqrt[n]{\lambda} \) denote an \( n \)th root of \( \lambda \). We then have

\[
\left[ \text{ind}_{\mathcal{G}_F}^{\mathcal{G}_F} (\mu_n, \lambda, \omega_n^r) \right] \sim \left[ \text{ind}_{\mathcal{G}_F}^{\mathcal{G}_F} (\omega_n^r) \otimes \mu_1, \sqrt[n]{\lambda} \right] \sim \left[ \text{ind}_{\mathcal{G}_F}^{\mathcal{G}_F} (\omega_n^{rq}) \right].
\]

Since we are interested in irreducible projective Galois representations, the above results imply we only need to consider representations of the form \( \left[ \text{ind}_{\mathcal{G}_F}^{\mathcal{G}_F} (\omega_n^r) \right] \) with \( r \) primitive.

Definition 6.6. Let \( \sigma \) be an irreducible projective Galois representation of dimension \( n \). We will say a Galois representation \( \rho \) is a lift of \( \sigma \) if \( \rho \) is of the form

\[
\rho = \text{ind}_{\mathcal{G}_F}^{\mathcal{G}_F} (\omega_n^r)
\]

and \( [\rho] \sim \sigma \).

Note that by Theorem 6.4 and Lemma 6.5, such a lift always exists. Moreover, any lift of \( \left[ \text{ind}_{\mathcal{G}_F}^{\mathcal{G}_F} (\omega_n^r) \right] \) is of the form

\[
\text{ind}_{\mathcal{G}_F}^{\mathcal{G}_F} (\omega_n^{q^m}) \otimes \omega_1^m \cong \text{ind}_{\mathcal{G}_F}^{\mathcal{G}_F} (\omega_n^{q^{m+n}}) \cong \text{ind}_{\mathcal{G}_F}^{\mathcal{G}_F} (\omega_n^{q^{(r+m)n}}).
\]

Hence, any irreducible projective Galois representation has at most \( q - 1 \) isomorphism classes of lifts. This also shows we may always choose a lift satisfying \( 0 \leq r < [n] \).
Proposition 6.7. Let $d$ be a divisor of $n$ and let $r \in \mathbb{Z}/(q^n - 1)\mathbb{Z}$ with $0 \leq r < [n]$. The number of such $r$ which are primitive and satisfy $q^dr \equiv r \pmod{[n]}$ is equal to

$$g(d) = \sum_{e \mid n} \mu\left(\frac{n}{e}\right) [(d,e)] \left(\frac{e}{(d,e)}, q - 1\right).$$

Proof. Firstly, note that for $a, b \in \mathbb{N}$, we have the equation

$$(9) \quad ([a], q^b - 1) = [(a, b)] \left(\frac{a}{(a,b)}, q - 1\right)$$

(see, for example, equation (13) under the entry “Greatest Common Divisor” in [35]). Assume we have

$$(q^d - 1)r \equiv 0 \pmod{[n]}.$$  

By the above equation, this is equivalent to

$$r \equiv 0 \pmod{\frac{[n]}{[d](\frac{n}{d}, q - 1)}}.$$  

Hence, we have $r \equiv s\frac{[n]}{[d](\frac{n}{d}, q - 1)}$ with $0 \leq s < [d](\frac{n}{d}, q - 1)$. It remains to determine which of these elements are primitive. Let $e$ be a proper divisor of $n$, and assume

$$r \equiv s\frac{[n]}{[d](\frac{n}{d}, q - 1)} \equiv 0 \pmod{\frac{[n]}{[e]}}.$$  

Applying equation (9) twice, we have

$$\left(\frac{[n]}{[d](\frac{n}{d}, q - 1)}, \frac{[n]}{[e]}\right) = \frac{\left([n], \frac{[n]}{[e]}\right)([n], q^d - 1)}{[d](\frac{n}{d}, q - 1)}$$  

$$\left(\frac{[n], \frac{[n]}{[e]}(\frac{n}{e}, q^d - 1)}{[d](\frac{n}{d}, q - 1)}ight) = \left([n], \frac{[n]}{[e]}\right)(q^d - 1)$$  

$$= \left([n], \frac{[n]}{[e]}(\frac{n}{e}, q^d - 1)\right)$$  

$$= \left([n], \frac{[n]}{[e]}\right)(q^d - 1)$$  

$$= \left([n], \frac{[n]}{[e]}(\frac{n}{e}, q^d - 1)\right)$$  

$$\left(\frac{[n], \frac{[n]}{[e]}(\frac{n}{e}, q^d - 1)}{[d][e](\frac{n}{d}, q - 1)}\right)$$  

$$\left([n], \frac{[n]}{[e]}\right)(\frac{e}{(d,e)}, q - 1).$$  

Therefore, the equation

$$s\frac{[n]}{[d](\frac{n}{d}, q - 1)} \equiv 0 \pmod{\frac{[n]}{[e]}}.$$
is equivalent to

\[ s \equiv 0 \left( \text{mod } \frac{[d] \left( \frac{n}{d}, q - 1 \right)}{[(d, e)] \left( \frac{e}{(d, e)}, q - 1 \right)} \right). \]

Hence, the number of \( 0 \leq r < [n] \) satisfying \( q^d r \equiv r \pmod{[n]} \) and \( r \equiv 0 \pmod{[n]/[e]} \) is

\[ [(d, e)] \left( \frac{e}{(d, e)}, q - 1 \right). \]

Using the inclusion-exclusion principle, the number of \( 0 \leq r < [n] \) which are primitive and satisfy \( q^d r \equiv r \pmod{[n]} \) is

\[ [d] \left( \frac{n}{d}, q - 1 \right) - \sum_{j=1}^{\sigma(n) - 1} (-1)^{j+1} \sum_{1 \leq e_1 < \ldots < e_j < n} \left[ \left( \frac{e}{(d, e)}, q - 1 \right) \right] \left( \frac{e_1, \ldots, e_j}{(d, e_1, \ldots, e_j)}, q - 1 \right); \]

applying Lemma 5.8 with \( f(e) = [(d, e)] \left( \frac{e}{(d, e)}, q - 1 \right) \) yields the result. □

**Corollary 6.8.** Let \( d \) be a divisor of \( n \), and let \( r \in \mathbb{Z}/(q^n - 1)\mathbb{Z} \) with \( 0 \leq r < [n] \). The number of such \( r \) which are primitive and such that \( d \) is the minimal integer satisfying \( q^d r \equiv r \pmod{[n]} \) is

\[ \sum_{e|d} \mu \left( \frac{d}{e} \right) g(e). \]

**Proof.** This follows from the previous proposition, the inclusion-exclusion principle, and Lemma 5.8 (cf. the proof of Corollary 5.10). □

**Lemma 6.9.** Assume \( \sigma \) is an irreducible projective Galois representation of dimension \( n \), and let \( \text{ind}_{gF_{\omega_n}}^{G_{\omega_n}} (\omega_n^r) \) be a fixed lift of \( \sigma \) with \( 0 \leq r < [n] \). Then the number of isomorphism classes of lifts of \( \sigma \) is of the form \( \frac{d-1}{n} q^n \), where \( d \) is a divisor of \( n \). Moreover, \( \sigma \) has exactly \( d-1 \) isomorphism classes of lifts if and only if \( d \) is the minimal divisor of \( n \) satisfying \( q^d r \equiv r \pmod{[n]} \).

**Proof.** There is nothing to prove if \( \sigma \) has \( q-1 \) lifts, so assume that \( \sigma \) has fewer than \( q-1 \) isomorphism classes of lifts. This means exactly that there exists some integer \( 1 \leq d < n \) and some \( 0 \leq m < q-1 \) such that

\[ r + m[n] \equiv q^d r \pmod{q^n - 1}. \]

One easily verifies that we may take \( d \) to be a proper divisor of \( n \), and we may further take \( d \) to be the smallest such divisor. Proceeding as in the proof of Proposition 6.7, we get that

\[ r \equiv s \left[ \frac{n}{d} \left( \frac{n}{d}, q - 1 \right) \right] \pmod{q^n - 1}, \]

with \( 0 \leq s < \left[ \frac{n}{d} \left( \frac{n}{d}, q - 1 \right) \right] \). Substituting into equation (10) above, we obtain

\[ m \equiv \bar{s} \left( \frac{q-1}{\left( \frac{n}{d}, q - 1 \right)} \right) \pmod{q - 1}, \]

where \( 0 \leq \bar{s} < \left( \frac{n}{d}, q - 1 \right) \) is the unique integer satisfying \( s \equiv \bar{s} \pmod{\left( \frac{n}{d}, q - 1 \right)} \).
Now, the assumption that \( q^dr \equiv r \pmod{[n]} \) implies \( g(d) \neq 0 \), so that \( \left( \frac{n}{d}, q - 1 \right) = \frac{n}{d} \) by Lemma 5.11. This fact, along with the primitivity of \( r \), implies \( \sigma \) is an invertible element of \( \mathbb{Z}/ \left( \frac{n}{d}, q - 1 \right) \mathbb{Z} = \mathbb{Z}/ \frac{n}{d} \mathbb{Z} \). Hence, we obtain

\[
 r + d\frac{q-1}{n}[n] \equiv r + \frac{q-1}{\left( \frac{n}{d}, q - 1 \right)}[n] \equiv q^dr \pmod{q^n - 1}
\]

for some integer \( 1 \leq d' < n \) (not necessarily dividing \( n \)). Therefore, we have

\[
 \text{ind}_{F^{\text{rep}}} (\omega_n) \otimes \omega_1^{d(q-1)/n} \cong \text{ind}_{F^{\text{rep}}} (\omega_n^r).
\]

Moreover, the minimality of \( d \) implies that the representations

\[
 \text{ind}_{F^{\text{rep}}} (\omega_n), \text{ind}_{F^{\text{rep}}} (\omega_n^r) \otimes \omega_1, \ldots, \text{ind}_{F^{\text{rep}}} (\omega_n) \otimes \omega_1^{(d(q-1)/n)-1}
\]

are pairwise nonisomorphic. This shows that \( \sigma \) has exactly \( d \frac{q-1}{n} \) isomorphism classes of lifts.

We again suppose that \( d \) is a proper divisor of \( n \). Assume now that \( \sigma \) has exactly \( d \frac{q-1}{n} \) isomorphism classes of lifts, so that \( \left( \frac{n}{d}, q - 1 \right) = \frac{n}{d} \). This ensures that the representations

\[
 \text{ind}_{F^{\text{rep}}} (\omega_n^r), \text{ind}_{F^{\text{rep}}} (\omega_n^r) \otimes \omega_1, \ldots, \text{ind}_{F^{\text{rep}}} (\omega_n^r) \otimes \omega_1^{(d(q-1)/n)-1}
\]

are pairwise nonisomorphic. In light of this, we must have

\[
 r + d\frac{q-1}{n}[n] \equiv q^e r \pmod{q^n - 1}
\]

for some \( 1 \leq e < n \). Adding \( (\frac{n}{d} - 1)d\frac{q-1}{n}[n] \) to both sides and applying this equation recursively, we obtain

\[
 r \equiv r + \frac{n}{d}d\frac{q-1}{n}[n] \equiv q^{ne/d}r \pmod{q^n - 1}.
\]

The primitivity of \( r \) shows that \( d \) divides \( e \). We have now

\[
 r + d\frac{q-1}{n}[n] \equiv q^d r \pmod{q^n - 1},
\]

where \( u \) is some invertible element of \( \mathbb{Z}/\frac{n}{d} \mathbb{Z} \); adding an appropriate multiple of \( d \frac{q-1}{n} \) to both sides, we get

\[
 r + sd\frac{q-1}{n}[n] \equiv q^d r \pmod{q^n - 1}
\]

for some \( s \). Thus, \( d \) satisfies \( q^d r \equiv r \pmod{[n]} \). If \( d \) was not the minimal such divisor, then the first part of the proof shows that we would obtain fewer than \( d \frac{q-1}{n} \) isomorphism classes of lifts, a contradiction.

\[
\square
\]

**Corollary 6.10.** Let \( d \) be a divisor of \( n \). The number of irreducible projective Galois representations \( \sigma \) of dimension \( n \) which have exactly \( d \frac{q-1}{n} \) isomorphism classes of lifts is equal to

\[
 h(d) = \frac{1}{d} \sum_{e \mid d} \mu \left( \frac{d}{e} \right) g(e).
\]

**Proof.** By the preceding lemma, the number of such representations is equal to the number of primitive \( 0 \leq r < [n] \) such that \( d \) is the minimal integer satisfying \( q^d r \equiv r \pmod{[n]} \), subject to the equivalence relation \( r \equiv r' \) if \( r' \equiv q^a r \pmod{[n]} \) for some \( a \in \mathbb{Z} \). Corollary 6.8 implies that this number is exactly \( h(d) \).

\[
\square
\]

**Remark.** The statement of the corollary should be understood in the following sense: we have \( d \frac{q-1}{n} \in \mathbb{Z} \) if and only if \( \left( \frac{n}{d}, q - 1 \right) = \frac{n}{d} \), if and only if \( h(d) \neq 0 \) by Lemma 5.11.
Corollary 6.11. Let $d$ be a divisor of $n$. The number of regular supersingular $L$-packets of $H_S$-modules of size $d$ is equal to the number of irreducible projective Galois representations of dimension $n$ having exactly $d\frac{n-1}{n}$ isomorphism classes of lifts. In particular, the number of regular supersingular $L$-packets of $H_S$-modules is equal to the number of irreducible projective Galois representations of dimension $n$.

Proof. This follows from Corollaries 5.10 and 6.10, and Lemma 6.9. \hfill \Box

6.3. Comparison with Große-Klönne’s Functor. Große-Klönne has recently constructed a functor from the category of right $H_S$-modules to the category of étale $(\varphi^\sigma, \Gamma_0)$-modules ([17]). When applied to the group $GL_n(\mathbb{Q}_p)$, his construction, composed with Fontaine’s equivalence of categories, yields a bijection between isomorphism classes of (absolutely) simple, supersingular right $H$-modules of dimension $n$ and isomorphism classes of (absolutely) irreducible $n$-dimensional mod-$p$ representations of $\text{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$. We now analyze these $(\varphi^\sigma, \Gamma_0)$-modules for $SL_n(\mathbb{Q}_p)$. For this subsection only, we adhere to the notation of loc. cit.; the reader should consult that article for precise statements and definitions.

We take $F = \mathbb{Q}_p$, $\mathfrak{o} = \mathbb{Z}_p$, with residue field $\mathbb{F}_p$, and uniformizer $\varpi = p$. We let $k$ denote the residue field in a fixed (sufficiently large) finite extension of $\mathbb{Q}_p$. Let $X$ denote the Bruhat-Tits building of $G_S$, and $A = X_{\omega}(T_S) \otimes_{\mathbb{Z}} \mathbb{R}$ the standard apartment corresponding to $T_S$. We let $C$ be the chamber corresponding to the Iwahori subgroup $I_S$, and choose a seminfinite chamber gallery as follows: the building $X$ is naturally isomorphic to the semisimple building of $G$, and therefore $G$ acts on $X$. For $i \geq 0$, we set

$$C^{(i)} := (n_{n-1}^{-1} \omega)^i C,$$

and note that the action on $A$ of

$$(n_{n-1}^{-1} \omega)^n = n_{n-1}^{-1} \omega \cdot \cdots \cdot n_2^{-1} \omega = \omega n_{n-1} n_{n-2} \cdots n_1^{-1} n_0^{-1}$$

is the same as the action of

$$\phi := n_{n-1}^{-1} n_{n-2}^{-1} \cdots n_1^{-1} n_0^{-1} \in G_S.$$

We have $\phi.C^{(i)} = C^{(i+n)}$ by definition. The choice of a chamber gallery and such an element $\phi$ provides us with a half tree $Y \subset X$ and a simplicial isomorphism between $Y$ and “the half tree of $\text{PGL}_2(\mathbb{Q}_p)$” (cf. loc. cit., Section 3).

To every simple supersingular $H_S$-module $\chi^{S}_{\lambda, j}$, we associate an $n$-tuple of integers

$$(k_1, \ldots, k_{n-1}, k_n)$$

as follows (cf. loc. cit., Section 8). For $1 \leq i \leq n - 1$, we let $0 \leq k_{i+1} \leq p - 1$ satisfy

$$\lambda \left( \varphi_{i\alpha_i} \begin{pmatrix} x & 0 \\ 0 & x^{-1} \end{pmatrix} \right) = x^{k_{i+1}}.$$

If $\lambda|_{T_i(\mathbb{F}_p)}$ is not the trivial character of $T_i(\mathbb{F}_p)$, then $k_{i+1}$ is uniquely determined. The condition of $\lambda|_{T_i(\mathbb{F}_p)}$ being equal to the trivial character of $T_i(\mathbb{F}_p)$ is equivalent to $n_i \in S_\lambda$; in this case, we set $k_{i+1} = p - 1$ if $n_i \in J$ and $k_{i+1} = 0$ otherwise. Likewise, we define $0 \leq k_1 \leq p - 1$ as the integer satisfying

$$\lambda \left( \varphi_{00} \begin{pmatrix} x^{-1} & 0 \\ 0 & x \end{pmatrix} \right) = x^{k_1}.$$
subject to the same restrictions as above if \( \lambda | T_0(\mathbb{F}_p) \) is trivial.

Tracing through the construction of \([17]\), we arrive at the following proposition.

**Proposition 6.12.** The \((\varphi^n, \Gamma_0)\)-module \( D_{\lambda,J} \) associated to \( \chi^S_{\lambda,J} \) is one-dimensional over \( k_{\mathcal{E}} = k((t)) \), spanned by a vector \( e \), with actions given by

\[
\varphi^n(e) = (-1)^n \left( \prod_{j=1}^{n} k_j! \right)^{-1} t^{-\sum_{j=0}^{n-1} (p-1-k_{n-j})p^j} e,
\]

\[
\gamma(e) = \frac{t}{(1+t)^{\chi_{\text{cyc}}(\gamma)}-1} \left( \prod_{j=1}^{n} k_j! \right)^{-1} t^{-\sum_{j=0}^{n-1} (p-1-k_{n-j})p^j} e,
\]

where \( \gamma \in \Gamma_0 \) and \( \chi_{\text{cyc}} : \Gamma \xrightarrow{\sim} \mathbb{Z}_p^* \) denotes the cyclotomic character. In particular, we see that distinct supersingular characters \( \chi^S_{\lambda,J} \) give rise to distinct \((\varphi^n, \Gamma_0)\)-modules.

**Proof.** See Appendix. \( \Box \)

**Remark.** The construction of \( D_{\lambda,J} \) depends on the choice of chamber gallery \( C^{(0)}, C^{(1)}, C^{(2)}, \ldots \) and the element \( \phi \).

Let \( \chi^S_{\lambda,J} \) be as before, and let \( (k_1, \ldots, k_{n-1}, k_n) \) denote the associated \( n \)-tuple. We define the rational number \( r \) (depending on \( \lambda \) and \( J \)) as

\[
(11) \quad r := \frac{1}{p-1} \sum_{j=0}^{n-1} (p-1-k_{n-j})p^j.
\]

By Theorem 8.5 of \( \text{loc. cit.} \), \( r \) is in fact an integer. The condition of regularity on \( \chi^S_{\lambda,J} \) is equivalent to the condition that the pair \((\tilde{\lambda}, J)\) satisfies Hypothesis (70) of \( \text{loc. cit.} \) for any lift \( \tilde{\lambda} \) of \( \lambda \) to \( T(\mathbb{F}_p) \), the finite torus of \( \text{GL}_n(\mathbb{Q}_p) \). By Theorems 8.6(c) and 8.7, \((\tilde{\lambda}, J)\) satisfying Hypothesis (70) is equivalent to the integer \( r \) being primitive (note that the proof of Theorem 8.7 shows how to construct a pair \((\tilde{\lambda}, J)\) from such an \( r \)). Combining everything, we obtain the following.

**Proposition 6.13.** Let \( \chi^S_{\lambda,J} \) be a simple supersingular \( \mathcal{H}_S \)-module, and let \( r \) be the integer given by equation (11). Then \( \chi^S_{\lambda,J} \) is regular if and only if \( r \) is primitive.

We can push the construction of Proposition 6.12 a bit further. Given a one-dimensional \((\varphi^n, \Gamma_0)\)-module \( D_{\lambda,J} \) as above, we construct an \( n \)-dimensional \((\varphi, \Gamma_0)\)-module as follows. Let \( D_{\lambda,J} \) denote the \( k_{\mathcal{E}} \) vector space spanned by \( \{e_0, \ldots, e_{n-1}\} \), with actions given by

\[
\varphi(e_i) = \begin{cases} 
 e_{i+1} & \text{if } 0 \leq i < n-1, \\
 (-1)^n \left( \prod_{j=1}^{n} k_j! \right)^{-1} t^{-\sum_{j=0}^{n-1} (p-1-k_{n-j})p^j} e_0 & \text{if } i = n-1,
\end{cases}
\]

\[
\gamma(e_i) = \left( \frac{t}{(1+t)^{\chi_{\text{cyc}}(\gamma)}-1} \right) \left( \prod_{j=1}^{n} k_j! \right)^{-1} t^{-\sum_{j=0}^{n-1} (p-1-k_{n-j})p^j} e_i,
\]

where \( \gamma \in \Gamma_0 \). If we let \( k_{\mathcal{E}}[\varphi, \Gamma_0] \) and \( k_{\mathcal{E}}[\varphi^n, \Gamma_0] \) denote the “twisted group rings” over \( k_{\mathcal{E}} \) considered in Section 6.1 of \( \text{loc. cit.} \), then \( D_{\lambda,J} \) is just the induced module

\[
k_{\mathcal{E}}[\varphi, \Gamma_0] \otimes k_{\mathcal{E}}[\varphi^n, \Gamma_0] D_{\lambda,J}.
\]
From the explicit construction, it is clear that $\widetilde{D}_{\lambda,J}$ is isomorphic to $D_{\lambda^{\omega^{-1}},\omega^{1}J\omega^{-1}}$. Moreover, we have

$$\widetilde{D}_{\lambda,J} \cong \bigoplus_{i=0}^{n-1} D_{\lambda^{\omega^{-i}},\omega^{i}J\omega^{-i}}$$

as $(\varphi^n, \Gamma_0)$-modules, the isomorphism given by sending $k_\xi, \bar{e}_i$ to $D_{\lambda^{\omega^{-i}},\omega^{i}J\omega^{-i}}$. The discussion of Section 2.2 of [5] shows that we may (nonuniquely) extend the action of $\Gamma_0$ to $\Gamma$, so that we obtain a bona fide $(\varphi, \Gamma)$-module. By abuse of notation, we shall also denote this module by $\widetilde{D}_{\lambda,J}$.

We may now relate simple supersingular $H_S$-modules and projective Galois representations more precisely. We denote by

$$D \mapsto W(D)$$

Fontaine’s equivalence of categories, from the category of $(\varphi, \Gamma)$-modules over $k_\xi$ to the category of finite-dimensional representations of $G_{\mathbb{Q}_p}$ over $k$ (see [16] for more details). Applying this functor to the $(\varphi, \Gamma)$-module $\widetilde{D}_{\lambda,J}$ and using the computations contained in Section 2.2 of [5], we obtain

$$W(\widetilde{D}_{\lambda,J}) = \text{ind}_{G_{\mathbb{Q}_p^n}^{G_{\mathbb{Q}_p^n}}}^{G_{\mathbb{Q}_p^n}} (\omega_n^{s}) \otimes \mu_{1, \beta} \omega_1^{s}$$

for some $0 \leq s < p - 1, \beta \in \mathbb{F}_p^\times$, and $r$ as in equation (11). Here $\mathbb{Q}_p^n$ denotes the unique unramified extension of $\mathbb{Q}_p$ of degree $n$ contained in a fixed algebraic closure $\overline{\mathbb{Q}}_p$. Precomposing this with Große-Klönne’s functor (and the lifting map $D_{\lambda,J} \mapsto \widetilde{D}_{\lambda,J}$) and postcomposing with the projectivization functor, we get a map $\mathcal{W}$ from the set of simple supersingular $H_S$-modules to the category of projective Galois representations. Explicitly, it is given by

$$\mathcal{W}(\chi_{\lambda,J}^S) = \left[ W(\widetilde{D}_{\lambda,J}) \right] \sim \left[ \text{ind}_{G_{\mathbb{Q}_p^n}^{G_{\mathbb{Q}_p^n}}}^{G_{\mathbb{Q}_p^n}} (\omega_n^{s}) \right],$$

where $r$ is given by equation (11).

There are several immediate consequences of this definition. Firstly, we see that the isomorphism class of $\mathcal{W}(\chi_{\lambda,J}^S)$ is independent of the choice of action of $\Gamma$ on the $(\varphi, \Gamma_0)$-module $\widetilde{D}_{\lambda,J}$, so that the map $\mathcal{W}$ is well-defined. Secondly, Propositions 6.2 and 6.13 and Theorem 6.4 show that $\chi_{\lambda,J}^S$ is regular if and only if $\mathcal{W}(\chi_{\lambda,J}^S)$ is irreducible. Finally, it is clear that two simple supersingular $H_S$-modules in the same orbit under $\omega^Z$ will yield isomorphic projective Galois representations under $\mathcal{W}$, so we may view $\mathcal{W}$ as a map defined on supersingular $L$-packets of $H_S$-modules.

**Proposition 6.14.** Let $\chi_{\lambda,J}^S$ be a simple, regular supersingular $H_S$-module, and let $d$ be a divisor of $n$. Then the orbit of $\chi_{\lambda,J}^S$ under $\omega^Z$ has size $d$ if and only if $\mathcal{W}(\chi_{\lambda,J}^S)$ has exactly $d^{\frac{n-1}{n}}$ isomorphism classes of lifts.

**Proof.** Let $(k_1, \ldots, k_{n-1}, k_n)$ denote the $n$-tuple of integers associated to $\chi_{\lambda,J}^S$, and $d$ a divisor of $n$. The group $\omega^Z$ acts on the set of such $n$-tuples by

$$\omega.(k_1, \ldots, k_{n-1}, k_n) := (k_n, k_1, \ldots, k_{n-1}),$$

and we claim $\omega^d \chi_{\lambda,J}^S = \chi_{\lambda,J}^S$ if and only if $\omega^d.(k_1, \ldots, k_{n-1}, k_n) = (k_1, \ldots, k_{n-1}, k_n)$. In the notation of Proposition 5.9, we see that the integers $k_i$ satisfy

$$k_i \equiv a_i - a_i \pmod{p-1},$$

where
where the indices are considered modulo $n$. Hence, if $\lambda^d = \lambda$, then we obtain

$$k_i \equiv k_{i+d} \pmod{p-1}.$$ 

If $k_i \not\equiv 0 \pmod{p-1}$, then the definition of the $n$-tuple shows that $k_i = k_{i+d}$, so we obtain the desired periodicity. On the other hand, the condition $k_i \equiv 0 \pmod{p-1}$ is equivalent to $n_{i-1} \in S_{\lambda}$. Since $\lambda^d J \lambda^{-d} = J$, we have $k_i = p-1$ if and only if $n_{i-1} \in J = \lambda^d J \lambda^{-d}$, if and only $n_{i+d-1} = \lambda^{-d} n_{i-1} \lambda^d \in J$, if and only if $k_{i+d} = p-1$. This gives the desired periodicity on the $n$-tuple $(k_1, \ldots, k_{n-1}, k_n)$. Tracing through these arguments in reverse gives the converse.

Now let $r$ be given by equation (11). We claim that $\lambda^d(k_1, \ldots, k_{n-1}, k_n) = (k_1, \ldots, k_{n-1}, k_n)$ if and only if $p^d r \equiv r \pmod{n}$. Indeed, the condition $\lambda^d(k_1, \ldots, k_{n-1}, k_n) = (k_1, \ldots, k_{n-1}, k_n)$ implies that $r$ takes the form

$$r = \frac{1}{p-1} \frac{p^n - 1}{p^d - 1} \sum_{j=0}^{d-1} (p-1-k_{n-j})p^j,$$

so that

$$p^d r = \frac{1 + p^d - 1}{p-1} \frac{p^n - 1}{p^d - 1} \sum_{j=0}^{d-1} (p-1-k_{n-j})p^j$$

$$= r + \left\lfloor \frac{n}{p} \right\rfloor \sum_{j=0}^{d-1} (p-1-k_{n-j})p^j.$$ 

The converse statement follows similarly.

Combining everything, we get that $\lambda^d \chi^S_{\lambda,J} = \chi^S_{\lambda,J}$ if and only if $p^d r \equiv r \pmod{n}$. Using Lemma 6.9, we see that the orbit of $\chi^S_{\lambda,J}$ has size $d$ if and only if $d$ is the minimal divisor of $n$ satisfying $p^d r \equiv r \pmod{n}$, if and only if $W(\chi^S_{\lambda,J})$ has exactly $d\frac{n}{p-1}$ isomorphism classes of lifts.

**Remark.** Since $W$ factors through the formation of $L$-packets, the above proposition shows in particular that we obtain an induced map from the set of regular supersingular $L$-packets of $H$-modules of size $d$ to the set of irreducible projective representations of $G_{Q_p}$ of dimension $n$ having exactly $d\frac{n}{p-1}$ isomorphism classes of lifts.

**Corollary 6.15.** The map $W$ realizes the numerical bijection of Corollary 6.11. More precisely, $W$ induces a bijection between regular supersingular $L$-packets of $H$-modules of size $d$ and irreducible projective representations of $G_{Q_p}$ of dimension $n$ having exactly $d\frac{n}{p-1}$ isomorphism classes of lifts.

**Proof.** Given an irreducible projective representation $\left[\text{ind}_{G_{Q_p}}^G (\omega^n)\right]$, Theorem 8.7 of [17] shows how to construct a simple, regular supersingular $H$-module $\chi^S_{\lambda,J}$ such that $W(\chi^S_{\lambda,J}) \sim \left[\text{ind}_{G_{Q_p}}^G (\omega^n)\right]$. Hence, the map $W$ from regular supersingular $L$-packets of size $d$ to irreducible projective Galois representations having $d\frac{n}{p-1}$ isomorphism classes of lifts is surjective. By Corollary 6.11, these two sets have the same size, and $W$ must be injective as well.

**Corollary 6.16.** Let $M$ be an $H$-module. We let $\mathcal{M} \mapsto \mathcal{G}(\mathcal{M})$ denote the functor from the category of finite-dimensional $H$-modules over $k$ to the category of continuous $G_{Q_p}$-representations over $k$ constructed in Section 8 of [17], and let $\mathcal{M} \mapsto \mathcal{J}(\mathcal{M}|_{H_S})$ denote the functor obtained by taking the Jordan-Hölder constituents of the $H_S$-module $\mathcal{M}|_{H_S}$ (without
restriction of multiplicity). The following diagram of sets is commutative (where we consider all objects up to isomorphism and over $k$):

$$
\begin{align*}
\{ \text{absolutely simple,} & \quad \text{supersingular} \\
\text{n-dimensional $H$-modules} & \} \\
\xrightarrow{g_{K(-)}} & \{ \text{absolutely irreducible} \\
\text{n-dimensional} & \} \\
\text{$G_K$-representations} & \}
\end{align*}
$$

$$
\begin{align*}
\{ \text{regular, supersingular} & \quad \text{L-packets of} \\
\text{$HS$-modules} & \} \\
\xrightarrow{W(-)} & \{ \text{absolutely irreducible} \\
\text{n-dimensional projective} & \} \\
\text{$G_{Q_p}$-representations} & \}
\end{align*}
$$

$J_H(-|_{HS}) \downarrow \downarrow J_H(-|_{HS})$

Proof. This follows from the explicit calculation of Theorem 8.5 in [17], and the comments preceding Proposition 6.14.

Appendix A. Proof of Proposition 6.12

We now carry out the computations for the proof of Proposition 6.12, which have been relegated to the appendix due to an excess of notation. We maintain the notation of Subsection 6.3, so that $F = \mathbb{Q}_p$, $o = \mathbb{Z}_p$, etc..

We let $X_+$ denote the “half tree of $PGL_2(\mathbb{Q}_p)$” described in Section 3 of [17], and let $X_+$ denote the half tree $X_+$ with the (unique) extremal edge removed. The choice of the chamber gallery $C^{(0)}, C^{(1)}, C^{(2)}, \ldots$ and the element $\phi$ provides us with a half tree $Y \subset X$ and isomorphism of simplicial complexes

$$
\Theta : Y \xrightarrow{\sim} X_+.
$$

The isomorphism $\Theta$ is defined by certain elements $\nu_j$ of $G_S$, which we take to be the following. We set

$$
\nu_j := \varphi_{a_{n-1-j,n}} \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & \cdots & 1 & \cdots & 1 \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ 1 & \cdots & 1 & \cdots & 1 \end{pmatrix} \begin{pmatrix} \text{$(n-1-j)^{\text{th}}$ row} \end{pmatrix}
$$

for $0 \leq j < n - 1$, and take $\nu_{n-1} := \nu_0^{-1}$. For $j \geq n$, the element $\nu_j$ is determined by equation (24) of loc. cit.. If we let

$$
\mathfrak{N}_0 := \left\{ \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix} : a \in \mathbb{Z}_p \right\}
$$

and

$$
\varphi := \begin{pmatrix} p & 0 \\ 0 & 1 \end{pmatrix} \in GL_2(\mathbb{Q}_p),
$$

then the isomorphism $\Theta$ is “equivariant” for the action of $U \cap IS$ on $Y$ and $\mathfrak{N}_0$ on $X_+$ (resp. the action of $\phi$ on $Y$ and $\varphi^n$ on $X_+$). See loc. cit., Theorem 3.1 for more details.

We make the isomorphism $\Theta$ explicit for future reference. Recall from loc. cit. that for $i \geq -1$ we define $v_i := \varphi^i.[\mathbb{Z}_p \oplus \mathbb{Z}_p] \in X_+$. For $0 \leq i \leq n - 1$, we also define

$$
F_i := C \cap n_i^{-1}.C = C^{(0)} \cap n_i^{-1}.C^{(0)}.
$$

We then have the following identifications under the map $\Theta$, for $0 \leq i \leq n - 1$ and $m \geq 0$:
\begin{align}
(12) \quad \Theta^{-1}(\{v_{mn+i}, v_{mn+i-1}\}) &= \Theta^{-1}(\varphi^m(\{v_i, v_{i-1}\})) \\
&= \varphi^m \Theta^{-1}(\{v_i, v_{i-1}\}) \\
&= \varphi^m C(i) \\
&= \varphi^m n_{n-1} n_{n-2} \cdots n_{n-i} C
\end{align}

$\Theta^{-1}(v_{mn+i}) = \Theta^{-1}(\varphi^m(v_i))$

\begin{align}
&= \varphi^m, \Theta^{-1}(v_i) \\
&= \varphi^m n_{n-1} n_{n-2} \cdots n_{n-i} F_{n-i-1} \\
&= \varphi^m n_{n-1} n_{n-2} \cdots n_{n-i} n_{n-i-1} F_{n-i-1}
\end{align}

Now let $\chi^S_{\lambda,J}$ be a supersingular character of $\mathcal{H}_S$ (which we consider as being valued in $k$), let $(k_1, \ldots, k_{n-1}, k_n)$ the associated $n$-tuple, and let $\mathcal{V}_{\lambda,J}$ denote the partial coefficient system on $X$ constructed in Section 5 of loc. cit.. Any chamber of $X$ has the form $g.C$ for some $g \in G_S$; we then have

$$\mathcal{V}_{\lambda,J}(g.C) = \{ f \in \text{c-ind}^I_{S, S}(\lambda) : \text{supp}(f) \subset I_S g^{-1} \}.$$ 

We let $f_1$ denote the function in $\mathcal{V}_{\lambda,J}(C)$ satisfying

$$\text{supp}(f_1) = I_S, \quad f_1(h) = \lambda(h)$$

for $h \in I_S$. Note that $f_1$ spans $\mathcal{V}_{\lambda,J}(C)$ (and therefore, $g.f_1$ spans $\mathcal{V}_{\lambda,J}(g.C)$).

Likewise, any facet of codimension 1 is of the form $g.F_i$ for some $g \in G_S$ and a unique $0 \leq i \leq n - 1$; we then have

$$\mathcal{V}_{\lambda,J}(g.F_i) = \{ f \in \text{c-ind}^I_{S, S}(\lambda) \otimes \mathcal{H}_i \text{ ind}^{\text{stab}G_S(F_i)}_{I_S(1)}(1) : \text{supp}(f) \subset \text{stab}G_S(F_i) g^{-1} \}.$$ 

Here $\text{stab}G_S(F_i)$ is the (parahoric) subgroup generated by $I_S$ and $n_i$, and $\mathcal{H}_i$ is the subalgebra of $\mathcal{H}_S$ generated by $T_t$ for $t \in T_i(\mathbb{F}_p)$ and the element $T_{n_i}$. The space $\mathcal{V}_{\lambda,J}(F_i)$ is naturally a representation of $\text{stab}G_S(F_i)$. The group $\text{stab}G_S(F_i)$ contains a subgroup which maps surjectively onto $SL_2(\mathbb{F}_p)$; the restriction of the representation $\mathcal{V}_{\lambda,J}(F_i)$ to this subgroup is isomorphic to $\text{Sym}^{k_{i+1}}(k^2)$. We let $f^i_0$ denote the function in $\mathcal{V}_{\lambda,J}(F_i)$ satisfying

$$\text{supp}(f^i_0) = \text{stab}G_S(F_i), \quad f^i_0(h) = h.t_{F_i,F_i}(1)$$

for $h \in \text{stab}G_S(F_i)$, and where $t_{F_i,F_i}$ is the map constructed in loc. cit., Section 5. The restriction maps of the coefficient system $\mathcal{V}_{\lambda,J}$ are the unique $k$-linear maps which are “$G$-equivariant” and which satisfy

$$r^C_{F_i}(f_1) = f^i_0;$$

more explicitly, for $g \in G_S$, we have

$$r^g.C_{F_i}(g.f_1) = g.f^i_0.$$

By restriction, we may view $\mathcal{V}_{\lambda,J}$ as a coefficient system on $Y$. Pushing forward by $\Theta$, we obtain a coefficient system $\Theta_* \mathcal{V}_{\lambda,J}$ on $\bar{x}_+$, and we consider the space

$$H_0(\bar{x}_+, \Theta_* \mathcal{V}_{\lambda,J}).$$
defined by the short exact sequence

\[ 0 \longrightarrow \bigoplus_{\text{edges } e \text{ of } \mathcal{F}_+} \Theta_e \mathcal{V}_{\lambda, J}(e) \xrightarrow{\partial} \bigoplus_{\text{vertices } v \text{ of } \mathcal{F}_+} \Theta_e \mathcal{V}_{\lambda, J}(v) \longrightarrow H_0(\mathcal{F}_+, \Theta_e \mathcal{V}_{\lambda, J}) \longrightarrow 0. \]

Here \( \partial \) is the map sending an element \( f \in \Theta_e \mathcal{V}_{\lambda, J}(\{v, v'\}) \) to

\[ r^{\Theta^{-1}(\{v, v'\})}(f) + r^{\Theta^{-1}(\{v, v'\})}(f). \]

In particular, using the equations (12) and (13), we have the following equalities:

\[ \partial(n_{n-1}^{-1}n_{n-2}^{-1} \cdots n_{n-i}^{-1} : f_1) = n_{n-1}^{-1}n_{n-2}^{-1} \cdots n_{n-i-1}^{-1} f_0^{-n} + n_{n-1}^{-1}n_{n-2}^{-1} \cdots n_{n-i-1}^{-1} f_0^{-n-1}, \]

for \( 1 \leq i \leq n - 1 \), and

\[ \partial(\phi : f_1) = \phi : f_0^n + \phi : f_0^{n-1}. \]

The space \( H_0(\mathcal{F}_+, \Theta_e \mathcal{V}_{\lambda, J}) \) has an action of the submonoid of \( \text{GL}_2(\mathbb{Q}_p) \) generated by \( \varphi^n \) and \( \mathfrak{N}_0 \), and therefore is naturally a module over the twisted polynomial ring \( k_\mathcal{F}^+[\varphi^n] \), where \( k_\mathcal{F}^+ \) is the completed group ring of \( \mathfrak{N}_0 \) over \( k \). In the terminology of loc. cit., \( H_0(\mathcal{F}_+, \Theta_e \mathcal{V}_{\lambda, J}) \) is a standard cyclic \( k_\mathcal{F}^+[\varphi^n] \)-module of perimeter 1. Additionally, by Theorem 4.3 (loc. cit.), we have

\[ H_0(\mathcal{F}_+, \Theta_e \mathcal{V}_{\lambda, J})^{\mathfrak{N}_0} \cong \Theta_e \mathcal{V}_{\lambda, J}(\{v_0, v_{-1}\}) = \mathcal{V}_{\lambda, J}(C), \]

where we identify \( \mathcal{V}_{\lambda, J}(C) \) with a subspace of \( H_0(\mathcal{F}_+, \Theta_e \mathcal{V}_{\lambda, J}) \) by the map \( f_1 \mapsto f_0^{-n-1} \).

In what follows, we denote the natural actions of \( U \cap I_S \) and \( \phi \) on \( \mathcal{V}_{\lambda, J} \) by a period, and denote the actions of \( \mathfrak{N}_0 \) and \( \varphi^n \) (induced by \( \Theta \)) by \( * \). In addition, for \( 1 \leq i, j \leq n \) satisfying \( i \neq j \), we set

\[ \nu_{i,j} := \varphi_{a_{i,j}} \left( \begin{array}{cc} 1 & 1 \\ 0 & 1 \end{array} \right) \in G_S \quad \text{and} \quad t_{i,j} := \nu_{i,j} - 1 \in k[G_S], \]

and set

\[ \nu := \left( \begin{array}{cc} 1 & 1 \\ 0 & 1 \end{array} \right) \in \mathfrak{N}_0 \quad \text{and} \quad t := \nu - 1 \in k[[\mathfrak{N}_0]] = k_\mathcal{F}^+. \]

We then obtain

\[ \varphi^n \ast f_0^{-n-1} = \phi \overline{f_0^{-n-1}} \]

Using the explicit action of \( \mathfrak{N}_0 \) on \( \Theta_e \mathcal{V}_{\lambda, J} \) described in loc. cit., Theorem 4.2, we get (for \( m \geq 0 \))

\[ \nu_{n-1}^{m-1} \varphi^n \ast f_0^{-n-1} = -\nu_{n-1}^{m-1} \ast \phi \overline{f_0^0} = -\nu_{n-1}^{m-1} \overline{\nu_{n-1}^{m-1} f_0^0} = -n_{n-1}^{-1} n_{n-2}^{-1} \cdots n_{1}^{-1} \nu_{n-1}^{m-1} n_{n-1}^{-1} \cdot \overline{f_0^0}. \]

Since

\[ t_{n,1}^{k_1} n_0^{-1} \cdot \overline{f_0^0} = k_1 ! \overline{f_0^0}, \]
(cf. loc. cit., Lemma 2.5), we get
\[
\begin{align*}
\tau^{n-1} k_1 \varphi^n * f_0^{n-1} &= -\tau^{n-1} k_1 \varphi_j f_0^n \\
&= -(\nu_{n-1} - 1) k_1 \varphi_j f_0^n \\
&= -k_1 \nu_{n-1} n_{n-2} \cdots n_{n-1} f_0^n \\
&= k_1 \nu_{n-1} n_{n-2} \cdots n_{n-1} f_0^n.
\end{align*}
\]

Now let \(1 \leq i \leq n - 1\). We have
\[
\begin{align*}
\tau^{\nu_{i-1}} n_{n-1} n_{n-2} \cdots n_{n-i} f_0^{n-i} &= \nu_{i-1} n_{n-1} n_{n-2} \cdots n_{n-i} f_0^{n-i} \\
&= n_{n-1} n_{n-2} \cdots n_{n-i} f_0^{n-i}.
\end{align*}
\]

As before, we have
\[
\begin{align*}
t^{k_{n-i+1}} n_{n-i} f_0^{n-i} &= k_{n-i+1} f_0^{n-i},
\end{align*}
\]
so we obtain
\[
\begin{align*}
t^{k_{n-i+1}} n_{n-i} f_0^{n-i} &= (\nu_{i-1} - 1) k_{n-i+1} n_{n-2} \cdots n_{n-i} f_0^{n-i} \\
&= -k_{n-i+1} n_{n-2} \cdots n_{n-i+1} f_0^{n-i}.
\end{align*}
\]

Note that the last line is only valid if \(i \geq 2\).

Combining everything, we obtain
\[
\begin{align*}
t^{\sum_{j=0}^{n-1} k_{n-j} \nu_j} \varphi^n * f_0^{n-1} &= (-1)^n \left( \prod_{j=1}^n k_j ! \right) f_0^{n-1}.
\end{align*}
\]

The results contained in Section 6.2 of loc. cit. show that the \(\varphi^n\)-module \(D_{\lambda,J}\) associated to \(\chi_{\lambda,J}^S\) is one-dimensional over \(k_{\bar{c}} = \text{Frac}(k_{\bar{c}}) = k((t))\), spanned by a vector \(\bar{c}\), with relation
\[
\varphi^n(\bar{c}) = (-1)^n \left( \prod_{j=1}^n k_j ! \right)^{-1} t^{\sum_{j=0}^{n-1} (p-1-k_{n-j}) \nu_j} \bar{c}
\]
(note that the proofs of loc. cit. necessary to deduce this do not rely on the action of \(\Gamma\)).

Now, Corollary 7.3 of loc. cit. shows that we may extend \(D_{\lambda,J}\) to a \((\varphi^n, \Gamma_0)\)-module, and therefore it suffices to compute the \(\Gamma_0\)-action. Let \(\gamma \in \Gamma_0\) act on \(\bar{c}\) by a Laurent series \(P_\gamma(t) \in k_{\bar{c}}^\times = k((t))^\times\). The commuting actions of \(\varphi^n\) and \(\Gamma_0\) give the relation
\[
\begin{align*}
\zeta \cdot t^{\sum_{j=0}^{n-1} (p-1-k_{n-j}) \nu_j} P_\gamma(t^{\nu_j}) \bar{c} &= \varphi^n(P_\gamma(t) \bar{c}) \\
&= \varphi^n(\gamma(\bar{c})) \\
&= \gamma(\varphi^n(\bar{c})) \\
&= \zeta \cdot (1 + t)^{\chi_{\text{cyic}}(\gamma)} - 1 - \sum_{j=0}^{n-1} (p-1-k_{n-j}) \nu_j P_\gamma(t) \bar{c},
\end{align*}
\]
where we denote \(\zeta := (-1)^n \left( \prod_{j=1}^n k_j ! \right)^{-1}\) for brevity. Therefore, we get
\[
\begin{align*}
t^{\sum_{j=0}^{n-1} (p-1-k_{n-j}) \nu_j} P_\gamma(t^{\nu_j}) &= ((1 + t)^{\chi_{\text{cyic}}(\gamma)} - 1 - \sum_{j=0}^{n-1} (p-1-k_{n-j}) \nu_j P_\gamma(t)) \bar{c}.
\end{align*}
\]
Comparing degrees shows that \( P_\gamma(t) \in k[[t]]^\times \). Let us write \( P_\gamma(t) = a_\gamma \widetilde{P}_\gamma(t) \), with \( a_\gamma \in k^\times \) and \( \widetilde{P}_\gamma(t) \in 1 + tk[[t]] \); then

\[
\widetilde{P}_\gamma(t^{p^n}) \widetilde{P}_\gamma(t)^{-1} = P_\gamma(t^{p^n}) P_\gamma(t)^{-1} = \left( \frac{(1 + t)^{\chi_{cyc}(\gamma)} - 1}{t} \right)^{-\sum_{j=0}^{n-1} (p-1-k_{n-j})p^j} \in 1 + tF_p[[t]].
\]

Expanding the left-hand side shows that we actually have \( \widetilde{P}_\gamma(t) \in 1 + tF_p[[t]] \). By Proposition 6(b) of Chapitre IV and Lemme 2 of Chapitre V of [30], \( x \mapsto x^{p^n-1} \) is an automorphism of \( 1 + tk[[t]] \), and we see that the equation

\[
\widetilde{P}_\gamma(t)^{p^n-1} = \widetilde{P}_\gamma(t^{p^n}) \widetilde{P}_\gamma(t)^{-1} = \left( \frac{(1 + t)^{\chi_{cyc}(\gamma)} - 1}{t} \right)^{-\sum_{j=0}^{n-1} (p-1-k_{n-j})p^j}
\]

is equivalent to

\[
\widetilde{P}_\gamma(t) = \left( \frac{(1 + t)^{\chi_{cyc}(\gamma)} - 1}{t} \right)^{-\sum_{j=0}^{n-1} (p-1-k_{n-j})p^j}.
\]

One easily checks that the assignment \( \gamma \mapsto a_\gamma \) is a homomorphism from \( \Gamma_0 \) to \( k^\times \), so that \( a_\gamma|_{k^1} = a_\gamma|_{k^1} = 1 \). However, using the same argument as above, the map \( \gamma \mapsto \gamma|_{k^1} \) is an automorphism of \( \Gamma_0 \cong 1 + p\mathbb{Z}_p \), so that \( a_\gamma = 1 \) for all \( \gamma \in \Gamma_0 \).

**References**

[1] Abdellatif, R., “Autour des représentations modulo \( p \) des groupes réductifs \( p \)-adiques de rang 1.” Thesis, Université Paris-Sud XI, (2011).
[2] Abdellatif, R., “Induction parabolique modulo \( p \) pour les groupes \( p \)-adiques quasi-déployés de rang 1.” Preprint (2013); available at http://perso.ens-lyon.fr/ramla.abbeldnif/Articles/rang1.pdf.
[3] Aigner, M., “Combinatorial Theory.” Grundlehren der mathematischen Wissenschaften, vol. 234, Springer, Berlin, (1997).
[4] Barthel, L. and Livné, R., “Irreducible Modular Representations of \( GL_2 \) of a Local Field.” Duke Math J., Vol. 75, (1994), 261-292.
[5] Berger, L., “On some modular representations of the Borel subgroup of \( GL_2(Q_p) \).” Compos. Math., 146, No. 1, (2010), 58-80.
[6] Borel, A., “Linear Algebraic Groups.” Graduate Texts in Mathematics, Vol. 126, Springer, 1991.
[7] Breuil, C., “Sur quelques représentations modulaires et \( p \)-adiques de \( GL_2(Q_p) \).” Compositio Math., 138, (2003) http://arxiv.org/abs/1206.4413, 165-188.
[8] Breuil, C., “Sur quelques représentations modulaires et \( p \)-adiques de \( GL_2(Q_p) \) II.” J. Inst. Math. Jussieu, 2, (2003), 1-36.
[9] Breuil, C., “Invariant \( L \) et série spéciale \( p \)-adique.” Ann. Scient. E.N.S. 37, (2004), 559-610.
[10] Breuil, C., “Representations of Galois and \( GL_2 \) in characteristic \( p \).” Course given at Columbia University, available at http://www.math.columbia.edu/~breuil/PUBLICATIONS/New-York.pdf.
[11] Breuil, C. and Herzig, F., “Ordinary representations of \( G(Q_p) \) and fundamental algebraic representations.” Preprint (2012); arXiv:1206.4413.
[12] Breuil, C. and Paskūnas, V., “Toward a modulo \( p \) Langlands correspondence for \( GL_2 \).” Memoirs of the AMS 216, (2012).
[13] Colmez, P., “Représentations de \( GL_2(Q_p) \) et \( (\varphi, \Gamma) \)-modules.” Astérisque 330, (2010), 281-509.
[14] Curtis, C. and Reiner, I., “Methods of Representation Theory, Volume I.” John Wiley & Sons, (1981).
[15] Emerton, M., “Local-global compatibility in the \( p \)-adic Langlands programme for \( GL_2/Q \).” Preprint (2010); available at http://www.math.uchicago.edu/~emerton/pdffiles/lg.pdf.
[16] Fontaine, J.-M., “Représentations \( p \)-adiques des corps locaux (1ère partie).” The Grothendieck Festschrift, Volume II. Birkhäuser Progress in Math. 87, (1990), 249-309.
[17] Große-Kröner, E., “From pro-\( p \) Iwahori-Hecke modules to \( (\varphi, \Gamma) \)-modules I.” Preprint (2013); available at http://www.math.hu-berlin.de/~zsksa/Grosse-Kroenner/1waheycal.pdf.
[18] Iwahori, N., and Matsumoto, H., “On some Bruhat decomposition and the structure of the Hecke rings of $p$-adic Chevalley groups.” *Publ. Math. de l’IHEs*, tome 25, (1965), 5-48.

[19] Kisin, M., “The Fontaine-Mazur conjecture for $GL_2$.” *J. Amer. Math. Soc.* 22, (2009), 641-690.

[20] Kisin, M., “Deformations of $G_{\mathbb{Q}_p}$ and $GL_2(\mathbb{Q}_p)$ representations.” *Astérisque* 330, (2010), 511-528.

[21] Kozioł, K., “A classification of the irreducible mod-$p$ representations of $U(1,1)(\mathbb{Q}_p^2/\mathbb{Q}_p)$.” Preprint (2012); arXiv:1210.0646.

[22] Lusztig, G., “Affine Hecke algebras and their graded version.” *J. Amer. Math. Soc.*, vol. 2:3, (1989), 599-635.

[23] Ollivier, R., “Platitude du pro-$p$-module universel de $GL_2(F)$ en caractéristique $p$.” *Compositio Math.*, 143, No. 3, (2007), 703-720.

[24] Ollivier, R., “Le foncteur des invariants sous l’action du pro-$p$-Iwahori de $GL_2(F)$.” *J. für die reine und angewandte Mathematik.*, 635, (2009), 149-185.

[25] Ollivier, R., “Parabolic induction and Hecke modules in characteristic $p$ for $p$-adic $GL_n$.” *ANT*, Vol. 4, No. 6, (2010), 701-742.

[26] Ollivier, R., “Compatibility between Satake and Bernstein-type isomorphisms in characteristic $p$.” Preprint (2012); arXiv:1211.5366. Preprint also available at http://www.math.columbia.edu/~ollivier/Compatibility.pdf

[27] Ollivier, R., “An inverse Satake isomorphism in characteristic $p$.” Preprint (2012); arXiv:1207.5557.

[28] Ollivier, R. and Sécherre, V., “Modules universels de $GL_3$ sur un corps $p$-adique en caractéristique $p$.” Preprint (2011); arXiv:1105.2957.

[29] Paškūnas, V., “The image of Colmez’s Montreal functor.” Preprint (2010); arXiv:1005.2008.

[30] Serre, J.-P., “Corps Locaux.” Hermann, Paris, (1968).

[31] Serre, J.-P., “Modular forms of weight one and Galois representations.” *Algebraic Number Fields (L-functions and Galois properties)* A. Fröhlich, ed., Academic Press, London, (1977), 193-268.

[32] Tits, J., “Reductive Groups over Local Fields.” *Automorphic Forms, Representations and L-function, Proc. Symp. Pure Math. XXXIII*, (1979), 29-69.

[33] Vigneras, M.-F., “A propos d’une conjecture de Langlands modulaire.” *Finite Reductive Groups: Related Structures and Representations*. M. Cabanes, ed. Birkhauser Progress in Math. 141, (1997), 415-452.

[34] Vigneras, M.-F., “Pro-$p$-Iwahori Hecke algebra and supersingular $\overline{\mathbb{F}}_p$-representations.” *Math. Ann.*, 331, (2005), 523-556.

[35] Weisstein, E., “CRC Concise Encyclopedia of Mathematics.” Second Edition. Chapman and Hall/CRC, (2002).