Compositio Math. 140 (2004) 333–358
DOI: 10.1112/S0010437X03000071

Representations modulo p of the p-adic group $GL(2, F)$

Marie-France Vignéras

Abstract

Let p be a prime number and let F be a local field with finite residual field of characteristic p. The Langlands local correspondence modulo $\ell \neq p$ for $GL(n, F)$ is known for all integers $n \geqslant 1$ but the case $\ell = p$ is still mysterious even when $n = 2$ (the case $n = 1$ is given by the local class field theory). Any irreducible $\overline{\mathbf{F}}_p$-representation of $GL(n, F)$ has a non-zero vector invariant by the pro-p-Iwahori subgroup $I(1)$ and the pro-p-Iwahori–Hecke $\overline{\mathbf{F}}_p$-algebra $\mathcal{H}_{\overline{\mathbf{F}}_p}(GL(n, F), I(1))$ plays a fundamental role in the theory of $\overline{\mathbf{F}}_p$-representations of G. We get when $n = 2$: (i) A bijection between the irreducible $\overline{\mathbf{F}}_p$-representations of dimension 2 of the Weil group $W(\overline{F}/F)$ and the simple supersingular modules of the pro-p-Iwahori–Hecke $\overline{\mathbf{F}}_p$-algebra $\mathcal{H}_{\overline{\mathbf{F}}_p}(GL(2, F), I(1))$. (ii) A new proof of the Barthel–Livne classification of the irreducible non-supersingular $\overline{\mathbf{F}}_p$-representations of $GL(2, F)$ using the $I(1)$-invariant functor. (iii) A bijection between the irreducible $\overline{\mathbf{F}}_p$-representations of $GL(2, \mathbf{Q}_p)$ and the simple right $\mathcal{H}_{\overline{\mathbf{F}}_p}(GL(2, \mathbf{Q}_p), I(1))$-modules given by the $I(1)$-invariant functor, using the recent results of Breuil.

Introduction

We consider only smooth representations: the stabilizers are open. An algebraic closure of a field k is denoted by $\overline{k}$. The residual field of F is the finite field $\mathbf{F}_q$ with q elements. In 1994, Barthel and Livne classified the irreducible subquotients of the $\overline{\mathbf{F}}_p$-representation of $G := GL(2, F)$ parabolically induced from a $\overline{\mathbf{F}}_p$-character of a maximal split torus and showed the existence of other irreducible representations that they called supersingular. Recently in 2001, in the particular case $F = \mathbf{Q}_p$, Breuil showed that the supersingular $\overline{\mathbf{F}}_p$-representations of G are in bijection with the irreducible $\overline{\mathbf{F}}_p$-representations of dimension 2 of the Weil group of $\overline{\mathbf{Q}}_p/\mathbf{Q}_p$, but the method of Breuil does not work when $F \neq \mathbf{Q}_p$. In this article, there is no restriction on F and we replace the $\overline{\mathbf{F}}_p$-representations of G by the modules of the Hecke $\overline{\mathbf{F}}_p$-algebra $\mathcal{H}_{\overline{\mathbf{F}}_p}(G, I(1))$ of G with respect to the pro-p-Iwahori subgroup $I(1)$; we classify the simple $\mathcal{H}_{\overline{\mathbf{F}}_p}(G, I(1))$-modules. The easy construction of the irreducible $\overline{\mathbf{F}}_p$-representations of the Weil group $W(\overline{F}/F)$ is done in [Vig97]. There is a striking similarity between the two classifications which suggests the existence of a Langlands correspondence. The basic question of a bijection between the irreducible $\overline{\mathbf{F}}_p$-representations of G and the simple right $\mathcal{H}_{\overline{\mathbf{F}}_p}(G, I(1))$-modules given by $I(1)$-invariant functor remains open when $F \neq \mathbf{Q}_p$. We proceed now to a more detailed description of the results and of the techniques in this article.

The finite-dimensional simple $\mathcal{H}_{\overline{\mathbf{F}}_p}(G, I(1))$-modules have dimension $\leqslant 2$ and those of dimension 2 are in bijection with the characters of the center of $\mathcal{H}_{\overline{\mathbf{F}}_p}(G, I(1))$ via their central characters. The proof proceeds in three steps. First, we classify the simple modules of the Hecke algebra

Received 20 September 2001, accepted in final form 25 February 2002.
2000 Mathematics Subject Classification 11S37, 11F70, 20C08, 20G05, 22E50.
Keywords: mod p representations, p-adic group, pro-p-Iwahori–Hecke algebra.

https://doi.org/10.1112/S0010437X03000071 Published online by Cambridge University Press

$\mathcal{H}_{\overline{\mathbf{F}}_p}(G, I)$ with respect to an Iwahori subgroup I. Next we classify the simple modules of another algebra that we call the 'second' Iwahori–Hecke algebra $\mathcal{H}_{\overline{\mathbf{F}}_p}(G, I)_2$. The two Iwahori–Hecke algebras do not depend on F. In the last step, we deduce the classification of the simple $\mathcal{H}_{\overline{\mathbf{F}}_p}(G, I(1))$-modules. For this, we remark that the cyclic group $S_2 = \{1, s\}$ of order 2 acts naturally on the $\overline{\mathbf{F}}_p$-characters χ of I because $I/I(1) \simeq (\mathbf{F}_q^*)^2$ and we prove that the compactly induced representations $\operatorname{ind}_I^G \chi$ have the following property: $\operatorname{ind}_I^G \chi, \operatorname{ind}_I^G \chi'$ are isomorphic when χ' is S_2-conjugate to χ (the result is not true in the finite case), and have no intertwining operators when $\chi' \neq \chi$ are not S_2-conjugate. This implies that the Hecke algebra $\mathcal{H}_{\overline{\mathbf{F}}_p}(G, I(1))$ is a direct sum $\oplus\mathcal{H}_\omega$, parametrized by the S_2-orbits ω of $\overline{\mathbf{F}}_p$-characters χ of I, where $\mathcal{H}_\omega = \operatorname{End} \operatorname{ind}_I^G \chi$ (isomorphic to the usual Iwahori–Hecke algebra) when $\chi = \chi s$ is not regular, and $\mathcal{H}_\omega = \operatorname{End} \operatorname{ind}_I^G \chi \oplus \chi s$ (isomorphic to the second Iwahori–Hecke algebra) when $\chi \neq \chi s$ is regular.

A small miracle allows us to prove the existence of a natural (but not unique) correspondence between the finite-dimensional simple $\mathcal{H}_{\overline{\mathbf{F}}_p}(G, I(1))$-modules and the semi-simple $\overline{\mathbf{F}}_p$-representations of the Weil group $W(\overline{F}/F)$ of dimension $\leqslant 2$, which restricts to a bijection between the supersingular $\mathcal{H}_{\overline{\mathbf{F}}_p}(G, I(1))$-modules and the irreducible $\overline{\mathbf{F}}_p$-representations of the Weil group of dimension 2. The 'miracle' is the coincidence between the number of S_2-orbits of $\overline{\mathbf{F}}_p$-characters of the split torus $\mathbf{F}_q^* \times \mathbf{F}_q^*$ and the number of orbits of regular $\overline{\mathbf{F}}_p$-characters of $\mathbf{F}_{q^2}^*$ for the Frobenius $x \to x^q$.

We classify the non-supersingular irreducible $\overline{\mathbf{F}}_p$-representations of G by describing their $I(1)$-invariant vectors as a $\mathcal{H}_{\overline{\mathbf{F}}_p}(G, I(1))$-module. The classification of the non-supersingular irreducible $\overline{\mathbf{F}}_p$-representations of G was already done by Barthel and Livne, by studying compact induction from $GL(2, O_F)$ where O_F is the ring of integers of F. We work with the pro-p-Iwahori subgroup instead of the maximal compact subgroup.

Any non-zero $\overline{\mathbf{F}}_p$-representation of G has a non-zero $I(1)$-invariant vector; also the functor of $I(1)$-invariants from the $\overline{\mathbf{F}}_p$-representations of G to the right $\mathcal{H}_{\overline{\mathbf{F}}_p}(G, I(1))$-modules is very important. The main question is to know if this functor restricts to a bijection between the irreducible $\overline{\mathbf{F}}_p$-representations of G and the simple $\mathcal{H}_{\overline{\mathbf{F}}_p}(G, I(1))$-modules. If the answer is yes, then we have classified the irreducible $\overline{\mathbf{F}}_p$-representations of G. We prove that the answer is yes for the non-supersingular ones. We can prove that the answer is yes for the supersingular ones only when $F = \mathbf{Q}_p$, using the results of Breuil which are valid only in this case. For any F, we can attach to any finite dimensional supersingular $\mathcal{H}_{\overline{\mathbf{F}}_p}(G, I(1))$-module M, the set of irreducible $\overline{\mathbf{F}}_p$-representations of G which contain M. We prove that this 'packet' contains only supersingular modules.

Let us mention that in the finite case or when the characteristic of the field of coefficients is different from p, there are no supersingular representations and the answer is yes. There is a striking difference between the local and finite cases for the principal representations. In the local case the principal representations of G defined by a regular $\overline{\mathbf{F}}_p$-character of the diagonal torus are irreducible whereas in the finite case the principal representations of $GL(2, \mathbf{F}_q)$ always have length $\geqslant 2$, with length exactly 2 only when $q = p$ (§ A.6).

We can replace the field of coefficients $\overline{\mathbf{F}}_p$ by any algebraically closed field R of characteristic p; when R is uncountable, the simple $\mathcal{H}_R(G, I(1))$-modules are always finite dimensional and the irreducible R-representations of G always have a central character.

For the integral properties of the $\overline{\mathbf{Q}}_p$-representations of G and their reductions modulo p, it is important to consider the Hecke algebra $\mathcal{H}_R(G, I(1))$ over a general commutative ring R. Many results will be given over such a ring. We refrain from changing G by a more general group except in one case: the description following Schneider and Stuhler [SS91] of the kernel of $\operatorname{ind}_I^G \chi \to \operatorname{ind}_B^G \chi_B$ for any $\overline{\mathbf{F}}_p$-character χ_B of a Borel subgroup B compatible with the $\overline{\mathbf{F}}_p$-character χ of the Iwahori subgroup I where we suppose that G is $GL(n, F)$. The description of the simple modules

https://doi.org/10.1112/S0010437X03000071 Published online by Cambridge University Press

for the Hecke $\overline{\mathbf{F}}_p$-algebra of a general reductive p-adic group G with respect to a pro-p-Iwahori subgroup is probably accessible;[1] we preferred to concentrate on $GL(2,F)$ which will serve as a model for other groups. The main obstacle at present seems to be to prove (or disprove) the basic relation between irreducible $\overline{\mathbf{F}}_p$-representations of $GL(2,F)$ and of the pro-p-Iwahori–Hecke algebra.

For the sake of completeness, the Appendix contains the known formula necessary for the computations with the Hecke algebras, some explicit computations, and some facts for groups with an Iwahori decomposition.

1. Simple modules of the Iwahori–Hecke algebra

In all the chapters R is a commutative ring, R^* is the group of units of R, F is a local field, p_F is a generator of the maximal ideal of the ring of integers O_F of F, q is the order of the residual field of F,

$$I = \left\{ \begin{pmatrix} a & b \\ p_F c & d \end{pmatrix},\ a,d \in O_F^*, b,c \in O_F \right\}$$

is the standard Iwahori subgroup of $G = GL(2,F)$ (unless otherwise specified), $t := \left(\begin{smallmatrix} 0 & 1 \\ p_F & 0 \end{smallmatrix}\right)$, $s := \left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)$. Clearly, $ts = \left(\begin{smallmatrix} 1 & 0 \\ 0 & p_F \end{smallmatrix}\right)$, $st = \left(\begin{smallmatrix} p_F & 0 \\ 0 & 1 \end{smallmatrix}\right), t^2 = p_F I_2$ where $I_2 = \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)$. The normalizer of I in G is generated by I and by t, and the normalizer of the diagonal torus T of G is generated by T and by s (or t).

1.1 Iwahori–Hecke algebra

The (affine) Iwahori–Hecke R-algebra of G is the endomorphism algebra:

$$\mathcal{H}_R(G,I) := \operatorname{End}_{RG} \operatorname{ind}_I^G 1$$

isomorphic to the convolution R-algebra of functions on double cosets of G modulo I with values in R and finite support. More details can be found in the § A.1. The algebra can be described by generators and relations [Vig96, I.3.14, p. 25]:[2]

$$\mathcal{H}_R(G,I) \simeq \mathcal{H}_R(q) := R[T^{\pm 1}, S], \quad (S-q)(S+1) = 0, \quad T^2 S = S T^2. \tag{1.1}$$

The isomorphism from $\mathcal{H}_R(G,I)$ to $\mathcal{H}_R(q)$ sends the characteristic functions E_t, E_s of ItI, IsI to T, S. The relation $T^2 S = S T^2$ says that T^2 belongs to the center as it should. One can replace q in (1.1) by any $v \in R$ and define an algebra $\mathcal{H}_R(v)$. The algebras $\mathcal{H}_R(v)$ are isomorphic for $v \neq -1$ at least if R is a field, because the quadratic relation is $U^2 = -U$ after the change of variables $U = (S-v)(v+1)^{-1}$. When $v = -1$, the quadratic relation becomes $U^2 = 0$ after the change of variables $U = S+1$.

We will classify the simple finite dimensional right $\mathcal{H}_R(0)$-modules when R is a field. When the characteristic of R is p, the (affine) Iwahori–Hecke R-algebra of G is isomorphic to $\mathcal{H}_R(0)$. We could use the isomorphism $\mathcal{H}_R(0) \simeq \mathcal{H}_R(v)$ for $v \neq -1$ and the classification in the case $v = q \neq 0$ in R given in [Vig97] when R is an algebraically closed field. For a possible application to the reduction modulo p or for a possible extension to the case $n > 2$, we give a direct proof of the classification valid for any $v \neq -1$. The interesting case is obtained by passage to the limit $v = 0$.

The center $\mathcal{Z}_R(v)$ of $\mathcal{H}_R(v)$ acts by a scalar on a simple finite dimensional $\mathcal{H}_R(v)$-module, and we start by the description of the center.

[1] Note added in the revised form. Rachel Ollivier classified the simple modules of the Iwahori–Hecke $\overline{\mathbf{F}}_p$-algebra of $GL(3,F)$ in her DEA (Université de Paris 7 – Denis Diderot, June 2002).

[2] The referee mentioned the following description of the Hecke–Iwahori algebra which is more natural in number theory: $\mathcal{H}_R(G,I) \simeq R[Z^{\pm 1}, U, w]$ with the relations $ZU = UZ, w^2 = Z, UwU = Z(qw + (q-1)U)$; with our notations $w = T, U = TS$ and $Z = T^2$.

https://doi.org/10.1112/S0010437X03000071 Published online by Cambridge University Press

1.2 Center

Suppose $R = \mathbf{Z}[v^{\pm 1/2}]$. Then S is invertible in $\mathcal{H}_{\mathbf{Z}[v^{\pm 1/2}]}(v)$ with

$$vS^{-1} = S - v + 1. \tag{1.2}$$

By the theory of Bernstein, the subalgebra $\mathbf{Z}[v^{\pm 1/2}][X_1^{\pm 1}, X_2^{\pm 1}]$ of $\mathcal{H}_{\mathbf{Z}[v^{\pm 1/2}]}(v)$ is commutative, where

$$v^{1/2}X_1 := ST, \quad v^{1/2}X_2 := T(S - v + 1); \tag{1.3}$$

as a left or right $\mathbf{Z}[v^{\pm 1/2}][X_1^{\pm 1}, X_2^{\pm 1}]$-module, $\mathcal{H}_{\mathbf{Z}[v^{\pm 1/2}]}(v)$ is free of basis $\{1, S\}$; the symmetric Laurent polynomials in $\mathbf{Z}[v^{\pm 1/2}][X_1^{\pm 1}, X_2^{\pm 1}]$ are the center $\mathcal{Z}_{\mathbf{Z}[v^{\pm 1/2}]}(v)$ of $\mathcal{H}_{\mathbf{Z}[v^{\pm 1/2}]}(v)$ [Vig96, I.3.15, p. 26].

Suppose that R is any commutative ring. The subalgebra $R[T^{\pm 2}, ST, T(S - v + 1)]$ of $\mathcal{H}_R(v)$ is commutative and one checks by a direct computation that the center $\mathcal{Z}_R(v)$ of $\mathcal{H}_R(v)$ is $R[T^{\pm 2}, Z(v)]$ where

$$Z(v) = (S + 1)T + T(S - v), \tag{1.4}$$

using the formulas $vX_1X_2 = T^2,\ v^{1/2}(X_1 + X_2) = Z(v)$.

1.3 Characters

The characters of $\mathcal{H}_R(v)$ are

$$M_1(\tau, \varepsilon) : T \mapsto \tau,\ S \to \varepsilon$$

for $(\tau, \varepsilon) \in R^* \times \{v, -1\}$. The character is called ‘trivial’ when $\varepsilon = v$ and ‘sign’ when $\varepsilon = -1$. The central elements $Z(v), T^2$ act on $M_1(\tau, \varepsilon)$ by multiplication by $\tau(2\varepsilon + 1 - v), \tau^2$. The element $Z(v)$ acts by $\tau(1 + v)$ on a trivial character and by $-\tau(1 + v)$ on a sign character. The action of the center on the trivial character $M_1(\tau, v)$ and on the sign character $M_1(-\tau, -1)$ is the same.

1.4 Standard modules

Let R be any commutative ring and let $v \in R$. For any $a \in R, z \in R^*$, one defines a *standard right $\mathcal{H}_R(v)$-module* of dimension 2

$$M_2(a, z) := Rm \oplus RmT, \quad m(S + 1) = 0, \quad mT(S - v) = am, \quad mT^2 = zm.$$

The matrices of T, S, ST on the basis $\{m, mT\}$ are (the columns are the images of the basis)

$$\begin{pmatrix} 0 & z \\ 1 & 0 \end{pmatrix}, \quad \begin{pmatrix} -1 & a \\ 0 & v \end{pmatrix}, \quad \begin{pmatrix} 0 & vz \\ -1 & a \end{pmatrix},$$

and one checks $T^2S = ST^2, (S + 1)(S - v) = 0$. The central elements $Z(v), T^2$ acts by a, z, and *the modules $M_2(a, z)$ have different central characters*. The trace of ST is a.

Proposition 1.1. *Assume that R is a field. The standard $\mathcal{H}_R(v)$-module $M_2(a, z)$ is reducible if and only if $a^2 = z(v + 1)^2$ and z is a square in R.*

When $a = v + 1 = 0$ and $\tau^2 = z$ with $\tau \in R$, the standard module is the direct sum $M(\tau, -1) \oplus M(-\tau, -1)$ if the characteristic of R is different from 2, and indecomposable of length 2 if the characteristic of R is 2.

When $a = \tau(v+1) \neq 0$ and $\tau^2 = z$ with $\tau \in R$, the standard module $M_2(a, z)$ is indecomposable, with submodule a trivial character $M_1(\tau, v)$ and with quotient a sign character $M_1(-\tau, -1)$.

Proof. A reducible standard $M_2(a, z)$ module contains a character $M_1(\tau, \varepsilon)$ with the same action of the center,

$$a = \pm\tau(1 + v), \quad z = \tau^2.$$

Conversely, suppose that $z = \tau^2$ and $\tau(v + 1) = a$ for some $\tau \in R$ such that $z = \tau^2$.

https://doi.org/10.1112/S0010437X03000071 Published online by Cambridge University Press

If $a = 0$ then $v + 1 = 0$, $(S + 1)^2 = 0$ in $M_2(0, z)$. When the characteristic of R is different from 2, the standard module is the direct sum $M(\tau, -1) \oplus M(-\tau, -1)$. When the characteristic of R is 2, the standard module is indecomposable of length 2, because T does not act by multiplication by τ.

If $a \neq 0$, the standard module $M_2(a, z)$ contains a unique proper submodule $M_1(\tau, v)$. Indeed $T^2 = \tau^2$ and T does not act by multiplication by a scalar, hence the image of $T + \tau$ is $Rm(T + \tau)$ for m as in § 1.4. We see that $(T + \tau)(S - v) = 0$, hence $m(T + \tau)$ is an $\mathcal{H}_R(v)$-eigenvector with eigenvalue $M_1(\tau, v)$ and the multiplicity of $M_1(\tau, v)$ is 1. There is another character $M_1(\tau, -1)$ with the same action of the center. We see that $(T - \tau)(S + 1) \neq 0$, hence $M_1(-\tau, -1)$ is not contained in $M_2(a, z)$. Modulo the unique stable line $Rm(T + \tau)$, we have $mT \equiv -\tau m$ and $mS \equiv -m$, hence the quotient character is $M_1(-\tau, -1)$. □

THEOREM 1.2. *When R is an algebraically closed field, any finite dimensional simple right $\mathcal{H}_R(v)$-module is a character or a standard module.*

Proof. Let M be a finite dimensional simple right $\mathcal{H}_R(v)$-module which is not a character. The center acts on M by a character, because R is algebraically closed. Suppose that the action of $(Z(v), T^2)$ is given by $(a, z) \in R \times R^*$. The elements T or S cannot act by a scalar because M is not a character. The kernel of $S + 1$ in M is non-zero, different from M, and stable by $T(S - v)$. We choose an eigenvector m of $T(S - v)$ in $\mathrm{Ker}(S + 1)$. By (1.4), we have $mT(S - v) = am$. The R-vector space $Rm + RmT$ is stable by S, T. As M is not a character, we deduce that its dimension is 2 and $M = M(a, z)$. □

1.5 Reduction modulo p

We call (E, R, k) a *p-modular setting* when R is the ring of integers of a finite extension E of $\mathbf{Q}_p$ and $k \subset \overline{\mathbf{F}}_p$ is the residual field of R. We denote $r_p : R \to k$ the reduction modulo p. We consider q in R and we have $r_p(q) = 0$.

Given an R-module X, we call $X_E = E \otimes_R X$ its E-extension and $r_p(X) := k \otimes_{R,r_p} X$ its reduction modulo p.

The E-extension of the R-algebra $\mathcal{H}_R(q)$ is $\mathcal{H}_E(q)$ and its reduction modulo p is $\mathcal{H}_k(0)$.

The E-extension M_E of an $\mathcal{H}_R(q)$-module M is an $\mathcal{H}_E(q)$-module and its reduction modulo p is an $\mathcal{H}_k(0)$-module $r_p(M)$. A finite dimensional $\mathcal{H}_E(q)$-module M_E is called R-integral when it is isomorphic to the E-extension of an $\mathcal{H}_R(q)$-module M, free as an R-module. One calls M an R-integral structure of M_E. Modulo isomorphism, the semi-simplification of the $\mathcal{H}_k(0)$-module $r_p(M)$ depends only on the semi-simplification of the $\mathcal{H}_E(q)$-module M and not on the choice of the R-integral structure M, by the usual proof [Vig96, I.9.6].

A character $M_1(\tau, \varepsilon)$ of $\mathcal{H}_E(q)$ is R-integral when $\tau \in R^*$, and conversely. A standard module $M_2(a, z)$ of $\mathcal{H}_E(q)$ is R-integral when $a \in R, z \in R^*$, i.e. when its central character is integral, and conversely; the standard module $M_2(a, z)$ of $\mathcal{H}_R(q)$ is an R-integral structure of the corresponding standard module of $\mathcal{H}_E(q)$. The reduction modulo p of a character or of a standard module of $\mathcal{H}_R(q)$ is a character or a standard module of $\mathcal{H}_k(q)$, and any character or standard module of $\mathcal{H}_k(q)$ is the reduction modulo p of a character or standard module of $\mathcal{H}_R(q)$, because the map $r_p : R \to k$ is surjective.

1.6 Action of R^*

The multiplicative group R^* acts on the left $\mathcal{H}_R(v)$-modules M by 'twist': in the twist $M\nu_{z_o}$ of M by $z_o \in R^*$, the action of T is multiplied by z_o, the action of S remains unchanged. There exists $z_o \neq 1$ such that the standard module $M_2(a, z)$ is isomorphic to its twist $M_2(a, z)\nu_{z_o} = M_2(az_o, zz_o^2)$ iff $a = 0, z_o = -1$ and the characteristic of R is different from 2.

https://doi.org/10.1112/S0010437X03000071 Published online by Cambridge University Press

2. Simple modules of the second Iwahori–Hecke algebra

The standard pro-p-Iwahori subgroup $I(1)$

$$I(1) = \left\{ \begin{pmatrix} 1+p_F a & b \\ p_F c & 1+p_F d \end{pmatrix},\ a,b,c,d \in O_F \right\}$$

is the pro-p-Sylow subgroup of the Iwahori subgroup I defined § 1. The quotient $I/I(1)$ is isomorphic to the diagonal torus $T(q) := T(\mathbf{F}_q)$ of the finite group $G(q) := GL(2, \mathbf{F}_q)$. We will identify the R-characters χ of I trivial on $I(1)$, the characters of $I/I(1)$, and the R-characters of $T(q)$. When the characteristic of R is p, any R-character of I is trivial on $I(1)$. The Weyl group $S_2 = \{1, s\}$ acts on $T(q)$ hence on the R-characters χ of $T(q)$. The element t (defined at the beginning of § 1) acts as s on $I/I_1 \simeq T(q)$ and normalizes I (but s does not normalize I).

The compactly induced R-representations $\operatorname{ind}_I^G \chi$ of $G = GL(2,F)$ are important: when R is a field of characteristic p which contains a root of 1 of order $q-1$, any irreducible R-representation of G is a quotient of some $\operatorname{ind}_I^G \chi$.

Let $f_{Ig,\chi} \in \operatorname{ind}_I^G \chi$ of support Ig and value 1 at $g \in G$. The functions $f_{Ig,\chi}$ for all $g \in I\backslash G$ form an R-basis of $\operatorname{ind}_I^G \chi$ and any $f_{Ig,\chi}$ generates $\operatorname{ind}_I^G \chi$ as an RG-module. Let χ, χ' be two R-characters of I trivial on $I(1)$.

Proposition 2.1.

a) $\operatorname{Hom}_{RG}(\operatorname{ind}_I^G \chi', \operatorname{ind}_I^G \chi) = 0$ *if* χ', χ *are not* S_2*-conjugate.*

b) *There is an RG-isomorphism*

$$\tau : \operatorname{ind}_I^G \chi \simeq \operatorname{ind}_I^G \chi s.$$

defined by $\tau f_{I,\chi} = f_{It,\chi s}$.

Note that, in the finite case, part b is false (Proposition A.2).

Proof. The restriction to I of $\operatorname{ind}_I^G \chi$ is isomorphic to a direct sum

$$\oplus_{w \in S_2.(T/T_o)} \operatorname{ind}_I^{IwI} \chi \simeq \oplus_{w \in S_2.(T/T_o)} \operatorname{ind}_{I_w}^I \chi w$$

where:

- $T = T(F)$ is the diagonal subgroup of G and $T_o = T(O_F)$;
- $s \in S_2$ is identified with $\left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)$;
- $\chi w := \chi$ if $w \in T/T_o$ and $\chi w := \chi s$ if $w \in s.(T/T_o)$;
- $\operatorname{ind}_I^{IwI} \chi$ is the subspace of functions in $\operatorname{ind}_I^G \chi$ with support contained in IwI;
- $I_w = I \cap w^{-1} I w$.

It is fundamental that the sequence

$$1 \to I(1) \cap I_w \to I_w \to T(\mathbf{F}_q) \to 1$$

is exact. This property implies $I = I(1) I_w$ and the restrictions of $\chi', \chi w$ to I_w are equal if and only if $\chi' = \chi w$. By the Frobenius reciprocity, the compact induction from an open compact subgroup is left adjoint to the restriction and the induction from a closed subgroup is right adjoint to the restriction [Vig96, I.5.7]. Thus we have

$$\operatorname{Hom}_{RG}(\operatorname{ind}_I^G \chi', \operatorname{ind}_I^G \chi) \simeq \operatorname{Hom}_{RI}(\chi', \operatorname{ind}_I^G \chi) \simeq \oplus_{w \in S_2.(T/T_o)}\ \operatorname{Hom}_{RI}(\chi', \operatorname{ind}_{I_w}^I \chi w),$$
$$\operatorname{Hom}_{RI}(\chi', \operatorname{ind}_{I_w}^I \chi w) \simeq \operatorname{Hom}_{RI_w}(\chi', \chi w) \simeq \operatorname{Hom}_{RI}(\chi', \chi w).$$

We deduce from this the first part of the proposition. The properties of t imply that $f_{It,\chi s} \in \operatorname{ind}_I^G \chi s$ is an eigenvector with eigenvalue χ for the action of I. Hence there is a (unique) RG homomorphism

τ sending $f_{I,\chi}$ to $f_{It,\chi s}$. As $Ig \to Itg$ is a bijection between the cosets of $I\backslash G$, τ is an isomorphism and the second part of the proposition is proved. □

2.1 The Hecke algebra of χ

We consider now the Hecke algebra of χ (see § A.1):

$$\mathcal{H}_R(G,\chi) := \operatorname{End}_{RG} \operatorname{ind}_I^G \chi.$$

The R-module of (I,χ)-invariants of $\operatorname{ind}_I^G \chi$ identifies canonically with the R-module $\mathcal{H}_R(G,\chi)$, and is a free R-module with basis the elements $E_g = E_{g,\chi}$ of support IgI and value 1 at g, for all the double classes modulo I of the set of $g \in G$ such that $\chi(gxg^{-1}) = \chi(x)$ for any $x \in I \cap g^{-1}Ig$. There are two cases:

- $\chi = \chi s$ is fixed S_2, called the *Iwahori or non-regular case*;
- $\chi \neq \chi s$ is not fixed S_2, called the *regular case*.

2.1.1 *The Iwahori case.* In the Iwahori case, the character χ extends to a character $\chi_1 \det$ of G where $\det : G \to F^*$ is the determinant, and χ_1 is an R-character of G; this implies

$$\operatorname{ind}_I^G \chi \simeq \chi_1 \det \otimes \operatorname{ind}_I^G 1,$$

and the elements $\chi_1(-1)E_{t,\chi},\ \chi_1(-1)E_{s,\chi}$ of $\mathcal{H}_R(G,\chi)$ satisfy the relations in § A.3). The algebras

$$\mathcal{H}_R(G,I) \simeq \mathcal{H}_R(G,\chi)$$

are isomorphic by the linear map such that $T \to \chi_1(-1)E_{t,\chi},\ S \to \chi_1(-1)E_{s,\chi}$.

2.1.2 *The regular case.* Until the end of § 2, we suppose that we are in the regular case. As an R-module, $\mathcal{H}_R(G,\chi)$ has a basis formed by the functions $E_{g,\chi}$ of support IgI and value 1 at g, for all $g \in T$ modulo $T_o = T \cap I$, by § 2.1. The images of $p_F I_2, ts$ in $T/T_o \simeq \mathbf{Z}^2$ form a $\mathbf{Z}$-basis and $st = p_F(ts)^{-1}$ (see the introduction of § 1).

PROPOSITION 2.2. *In the regular case, the Hecke R-algebra $\mathcal{H}_R(G,\chi)$ is commutative, generated by $E^{\pm 1}_{p_F I_2,\chi}, E_{ts,\chi}, E_{st,\chi}$ with the relation $E_{ts,\chi}E_{st,\chi} = qE_{p_F I_2,\chi}$.*

This is obtained by reduction modulo p from the integral versions of classical results on Hecke algebras in the theory of types (a direct proof is given in § A.2, see also [BL94, Proposition 13]).

The isomorphism $\tau : \operatorname{ind}_I^G \chi \to \operatorname{ind}_I^G \chi s$ sending $f_{I,\chi}$ to $f_{It,\chi s}$ (see Proposition 2.1) permutes $E_{st,\chi}, E_{ts,\chi s}$. One sees using $tI = It,\ t(st)t^{-1} = ts$ that

$$\tau E_{p_F I_2,\chi} = E_{p_F I_2,\chi s}\tau, \quad \tau E_{st,\chi} = E_{ts,\chi s}\tau, \quad \tau E_{ts,\chi} = E_{st,\chi s}\tau.$$

Consider the commutative algebra $R[Z^{\pm 1}, X, Y]$ and its quotient

$$\mathcal{Z}_R(q)_2 := R[Z^{\pm 1}, X, Y]/(XY - qZ),$$

canonically isomorphic to

- $\mathcal{H}_R(G,\chi)$ by $E_{p_F I_2,\chi} \mapsto Z,\ E_{ts,\chi} \mapsto X,\ E_{st,\chi} \mapsto Y$;
- $\mathcal{H}_R(G,\chi s)$ by $E_{p_F I_2,\chi s} \mapsto Z,\ E_{ts,\chi s} \mapsto Y,\ E_{st,\chi s} \mapsto X$.

Via the natural injective maps $\chi \to \chi \oplus \chi s, \chi s \to \chi \oplus \chi s$ the algebra $\mathcal{H}_R(G,\chi) \oplus \mathcal{H}_R(G,\chi s)$ identifies with the 'diagonal' subalgebra of $\mathcal{H}_R(G,\chi \oplus \chi s)$. Set $E_{g,\chi\oplus\chi s} = E_{g,\chi} + E_{g,\chi s}$ for any $g \in T$. From Proposition 2.1 we deduce the following corollary.

COROLLARY 2.3. *In the regular case, there is an R-algebra isomorphism*

$$\mathcal{H}_R(G,\chi \oplus \chi s) \simeq M(2, \mathcal{Z}_R(q)_2)$$

https://doi.org/10.1112/S0010437X03000071 Published online by Cambridge University Press

such that

$$E_{p_F I_2,\chi\oplus\chi s} \to \begin{pmatrix} Z & 0 \\ 0 & Z \end{pmatrix}, \quad E_{ts,\chi\oplus\chi s} \mapsto \begin{pmatrix} X & 0 \\ 0 & Y \end{pmatrix}, \quad E_{st,\chi\oplus\chi s} \mapsto \begin{pmatrix} Y & 0 \\ 0 & X \end{pmatrix}.$$

The isomorphism depends on the *ordered couple* $(\chi, \chi s)$. We denote by $T, S \in \mathcal{H}_R(G, \chi \oplus \chi s)$ the elements with support ItI, IsI and value $\left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)$ at t, s defined as in the § 1. They satisfy (see (A.3) and (A.5)):

$$S^2 = q, \quad ST = E_{st,\chi\oplus\chi s}, \quad T^2 = E_{p_F I_2,\chi\oplus\chi s}.$$

The center of $\mathcal{H}_R(G, \chi \oplus \chi s)$ is generated by

$$E_{ts,\chi} + E_{st,\chi s}, \quad E_{st,\chi} + E_{ts,\chi s}, \quad T^2$$

corresponding respectively to the scalar matrices X, Y, Z in $M(2, \mathcal{Z}_R(q)_2)$ via the isomorphism.

2.2 The second Iwahori–Hecke algebra

We will call

$$\mathcal{H}_R(q)_2 := M(2, \mathcal{Z}_R(q)_2)$$

the *second Iwahori–Hecke R-algebra of G*. We can define algebras $\mathcal{H}_R(v)_2 := M(2, \mathcal{Z}_R(v)_2)$ for any $v \in R$. The characters of the center $\mathcal{Z}_R(v)_2$ are

$$\omega(x, y, z) : X \mapsto x, \quad Y \mapsto y, \quad Z \mapsto z,$$

for any $(x, y, z) \in R^2 \times R^*,\ xy = vz$.

2.3 Standard module

The natural right $\mathcal{H}_R(v)_2$-module $M_2(x, y, z)$ of dimension 2 with central character $\omega(x, y, z)$ is called a standard $\mathcal{H}_R(v)_2$-module.

The module which corresponds to $M_2(x, y, z)$ via the isomorphism of Corollary 2.3 is denoted

$$M_2(x, y, z, \chi) = M_2(y, x, z, \chi s), \tag{2.1}$$

and called a standard right $\mathcal{H}_R(G, \chi \oplus \chi s)$-module.

The unique non-zero eigenvalue of $\mathcal{H}_R(G, \chi)$ in $M_2(x, y, z, \chi)$ is

$$E_{p_F I_2,\chi} \mapsto z, \quad E_{ts,\chi} \mapsto x, \quad E_{st,\chi} \mapsto y.$$

The trace of ST in $M_2(x, y, z, \chi)$ is $a := x + y$.

The image of (2.1) by the automorphism τ is

$$M_2(y, x, z, \chi) = M_2(x, y, z, \chi s).$$

When R is a field, the standard $\mathcal{H}_R(G, \chi\oplus\chi s)$-modules are simple, and any simple $\mathcal{H}_R(G, \chi\oplus\chi s)$-module is of the form (2.1).

2.4 Reduction modulo p

We assume that (E, R, k) is a p-modular setting and $r_p : R \to k$ the reduction modulo p as in § 1.5. We consider q in R.

Assertion 2.4. A simple $\mathcal{H}_E(q)_2$-module is R-integral iff its central character is R-integral; the reduction modulo p of a simple R-integral $\mathcal{H}_E(q)_2$-module is simple. A simple $\mathcal{H}_k(q)_2$-module

$$M_2(x, y, z), \quad (x, y, z) \in k^2 \times k^*, \quad xy = 0,$$

https://doi.org/10.1112/S0010437X03000071 Published online by Cambridge University Press

is the reduction modulo p of an R-integral $\mathcal{H}_E(q)_2$-module

$$M_2(x',y',z'), \quad (x',y',z') \in R^2 \times R^*, x'y' = qz', \quad r_p(x',y',z') = (x,y,z)$$

with one exception: $M_2(0,0,z), z \in k^*$ when q is a uniformizing parameter of R, is not the reduction of an R-integral $\mathcal{H}_E(q)_2$-module.

These assertions are immediate, except maybe the last one. A simple $\mathcal{H}_k(q)_2$-module, i.e. $M(x, y, z)$ with $(x,y,z) \in k^2 \times k^*,\ xy = 0$, is the reduction modulo p of an R-integral $\mathcal{H}_E(q)_2$-module if the parameters (x,y,z) are the reduction modulo p of parameters $(x',y',z') \in R^* \times R^2,\ x'y' = qz'$. If x (or y) is not 0, there is no problem: one lifts x, z to units $x', z' \in R^*$ and one sets $y' = qz'x'^{-1}$. If $x = y = 0$, any lift x' of x and any lift y' of y in R is divisible by a uniformizing parameter p_R of R. As any lift of z is a unit $z' \in R^*$, the equation $x'y' = qz'$ implies that q is divisible by p_R^2.

2.5 Action of R^*

As in § 1.6, the multiplicative group R^* acts on the right $\mathcal{H}_R(q)_2$-modules M by 'twist'. For $z_o \in R^*$, the action of X, Y, Z on the twist $M\nu_{z_o}$ of M by z_o are multiplied respectively by z_o, z_o, z_o^2.

There exists $z_o \neq 1$ such that the standard module $M_2(x,y,z)$ is isomorphic to its twist $M_2(x,y,z)\nu_{z_o} = M_2(xz_o, yz_o, zz_o^2)$ iff $x = y = 0, z_o = -1$ and the characteristic of R is different from 2.

3. Simple modules of the Hecke algebra of the pro-p-Iwahori

The Hecke R-algebra of $G = GL(2,F)$ with respect to the pro-p-Iwahori $I(1)$ is

$$\mathcal{H}_R(G, I(1)) := \operatorname{End}_{RG} \operatorname{ind}_{I(1)}^G 1.$$

This algebra is the central object of this article. We will restrict ourselves now and in the next sections to a commutative ring R such that the regular representation $R[\mathbf{F}_q^*]$ of $\mathbf{F}_q^*$ is a sum of characters. The main example in characteristic 0 is $R = \mathbf{Z}[1/(q-1), \zeta_{q-1}]$ where ζ is a complex root of 1 of order $q-1$, and the main example in characteristic p is $R = \mathbf{F}_q$.

We describe the structure of the algebra $\mathcal{H}_R(G, I(1))$.

Proposition 3.1. *We have a canonical algebra isomorphism*

$$\mathcal{H}_R(G, I(1)) \simeq \oplus_{\chi = \chi s} \mathcal{H}_R(G, \chi) \oplus_{\chi \neq \chi s} \mathcal{H}_R(G, \chi \oplus \chi s),$$

for all S_2-orbits of the R-characters χ of $I/I(1)$.

Proof. The R-representation $\operatorname{ind}_{I(1)}^I 1$ decomposes as a direct sum

$$\operatorname{ind}_{I(1)}^I 1 \simeq \oplus_\omega \sigma_\omega,$$

where ω are the S_2-orbits of the R-characters χ of $I/I(1)$, and $\omega = \sigma_\omega = \chi = \chi s$ in the Iwahori case and $\sigma_\omega = \chi \oplus \chi s$ in the regular case $\omega = \{\chi \neq \chi s\}$. From the transitivity of the compact induction

$$\operatorname{ind}_{I(1)}^G 1 = \operatorname{ind}_I^G(\operatorname{ind}_{I(1)}^I 1)$$

and the commutativity

$$\operatorname{ind}_I^G(\oplus_\omega \sigma_\omega) = \oplus_\omega \operatorname{ind}_I^G \sigma_\omega,$$

one obtains a linear R-isomorphism

$$\mathcal{H}_R(G, I(1)) \simeq \oplus_\omega \mathcal{H}_R(G, \sigma_\omega).$$

The isomorphism respects the product because *there are no non-zero intertwining operators between* $\operatorname{ind}_I^G \sigma_\omega$ *and* $\operatorname{ind}_I^G \sigma_{\omega'}$ *for two distinct S_2-orbits $\omega \neq \omega'$* by Proposition 2.1. The projections

https://doi.org/10.1112/S0010437X03000071 Published online by Cambridge University Press

$e_\omega : \operatorname{ind}_{I(1)}^G 1 \to \operatorname{ind}_I^G \sigma_\omega$ for all S_2-orbits ω form a set of central orthogonal idempotents of $\operatorname{End}_{RG} \operatorname{ind}_{I(1)}^G 1$, with sum 1.

The basic components $\mathcal{H}_R(G, \sigma_\omega)$ of $\mathcal{H}_R(G, I(1))$ have been studied in §§ 1 and 2. The algebra $\mathcal{H}_R(G, \sigma_\omega)$ is canonically isomorphic to the Iwahori–Hecke algebra $\mathcal{H}_R(q)$ in the Iwahori or non-regular case, and is (non-canonically) isomorphic to the second Iwahori–Hecke algebra $\mathcal{H}_R(q)_2$ in the regular case. □

3.1 Modules

Let ω be an S_2-orbit of an R-character χ of $I/I(1)$ and let M be a right $\mathcal{H}_R(G, \sigma_\omega)$-module. We denote by (M, ω) the corresponding $\mathcal{H}_R(G, I(1))$-module; if M is standard, we say that (M, ω) is standard. In fact only χ will appear when M is irreducible: if χ is not regular then $\omega = \chi$, and if ω is not regular either χ or χs appears already in the notation for M and we suppress ω. We deduce with the notations of §§ 1 and 2 the classification of all finite-dimensional simple right $\mathcal{H}_R(G, I(1))$-modules.

Proposition 3.2. *Let R be any algebraically closed field of any characteristic. The finite dimensional simple right $\mathcal{H}_R(G, I(1))$-modules are*

i) *the characters (§ 1.3)*
$$M_1(t, \varepsilon, \chi)$$
for all non-regular R-characters $\chi = \chi s$ of $T(q)$, $t \in R^*, \varepsilon \in \{-1, q\}$;

ii) *the standard modules of dimension 2 (§ 1.4)*
$$M(a, z, \chi)$$
for all non-regular R-characters $\chi = \chi s$ of $T(q), a \in R, z \in R^*$, $a^2 \neq z(q+1)^2$;

iii) *the standard modules of dimension 2 (§ 2.3),*
$$M(x, y, z, \chi)$$
for all regular R-characters $\chi \neq \chi s$ of $T(q), x, y \in R, z \in R^*$, $xy = qz$.

The only isomorphisms are $M(x, y, z, \chi) \simeq M(y, x, z, \chi s)$ when $\chi \neq \chi s$.

3.2 Supersingular modules

For reasons which will be clear later, when the characteristic of R is p, for each S_2-orbit ω of R-characters of I/I_1, the unique simple standard right $\mathcal{H}(G, \sigma_\omega)$-module $M_2(0, z, \omega)$ where p_F acts by multiplication by z and the trace of ST is 0, is called supersingular. The number of supersingular simple right $\mathcal{H}_R(G, I(1))$-modules with a given action of p_F is $(q^2 - q)/2$, i.e. the number of S_2-orbits ω of R-characters of the group $I/I(1) \simeq \mathbf{F}_q^* \times \mathbf{F}_q^*$.

4. Irreducible representations of $GL(2, F)$

Over any commutative ring R, the category $\operatorname{Mod}_R G$ of R-representations of $G := GL(2, F)$ and the category $\operatorname{Mod} \mathcal{H}_R(G, I(1))$ of right $\mathcal{H}_R(G, I(1))$-modules are related by the functor of invariant vectors by the pro-p-Iwahori subgroup $I(1)$
$$V \mapsto V^{I(1)} : \operatorname{Mod}_R G \to \operatorname{Mod} \mathcal{H}_R(G, I(1)).$$

Conjecture 4.1 (Main conjecture). When R is an algebraically closed field of characteristic p, the functor of $I(1)$-invariant vectors induces a bijection between the irreducible representations of G with a non-zero $I(1)$-invariant vector and a central character, and the simple finite-dimensional right $\mathcal{H}_R(G, I(1))$-modules (modulo isomorphism).

https://doi.org/10.1112/S0010437X03000071 Published online by Cambridge University Press

When the characteristic of R is $\neq p$, the result is known and the proof is not even difficult [Vig96, I.6.3].

When the characteristic of R is p, any non-zero R-representation V of G has a non-zero $I(1)$-invariant vector, because any $v \in V$ generates a finite dimensional $R[I(1)]$-module. When the main conjecture is true, we get from the preceding sections the classification of the irreducible R-representations of G with a central character. The main conjecture will be proved when $F = \mathbf{Q}_p, R = \overline{\mathbf{F}}_p$ in Theorem 5.4.

Note. In [BL95], [BL94] and [Bre01], the functor of $I(1)$-invariant vectors plays an important but hidden role. Instead of the Hecke algebra of the trivial $\overline{\mathbf{F}}_p$-representation of the pro-p-Iwahori, they use the Hecke algebra of an irreducible $\overline{\mathbf{F}}_p$-representation of $GL(2, O_F)F^*$ which is always a commutative algebra isomorphic to $\overline{\mathbf{F}}_p[T]$.

4.1 Principal representations

Let R be a commutative ring. We change the notation for χ. Now χ is an R-character of the diagonal subgroup $T = T(F)$ of G, and $\chi(q)$ is the restriction of χ to $T(O_F)$. We suppose that $\chi(q)$ is trivial on the pro-p-Sylow of $T(O_F)$, hence $\chi(q)$ identifies to an R-character of $I/I(1)$. The *principal representation*

$$\operatorname{ind}_B^G \chi$$

is the representation of G induced from the character of the upper triangular subgroup B inflated from χ.

The representation $\operatorname{ind}_B^G \chi$ is generated by $f_{BI,\chi}$ (see § 4.3) and has a central character. We describe now the right $\mathcal{H}_R(G, I(1))$-module $(\operatorname{ind}_B^G \chi)^{I(1)}$. The well known disjoint union

$$G = BI \cup BsI = BI(1) \cup BsI(1) = BI(1) \cup BtI(1),$$

since $st \in B$, implies that

$$(\operatorname{ind}_B^G \chi)^{I(1)} = Rf_{BI,\chi} \oplus Rf_{BtI,\chi}$$

where $f_{BI,\chi}, f_{BtI,\chi}$ are the unique functions in $(\operatorname{ind}_B^G \chi)^{I(1)}$ of support BI, BtI and value 1 at $1, t$. The functions $f_{BI,\chi}, f_{BtI,\chi}$ are eigenvectors for the action of I of eigenvalues $\chi(q)$ and $\chi(q)s$. The right $\mathcal{H}_R(G, I(1))$-module $(\operatorname{ind}_B^G \chi)^{I(1)}$ identifies with an $\mathcal{H}_R(G, \omega)$-module where $\omega = \chi(q)$ if $\chi(q) = \chi(q)s$ and $\omega = \chi(q) \oplus \chi(q)s$ if $\chi(q) \neq \chi(q)s$. With the notation of the preceding sections for the standard modules and for s, t, we have the following theorem.

THEOREM 4.2. *The right $\mathcal{H}_R(G, I(1))$-module $(\operatorname{ind}_B^G \chi)^{I(1)}$ is equal to the standard module*

$$M_2(q\chi(ts)^{-1}, \chi(st)^{-1}, \chi(p_F I_2)^{-1}, \chi(q)) \quad \text{when } \chi(q) \neq \chi(q)s,$$
$$M_2(q\chi(ts)^{-1} + \chi(st)^{-1}, \chi(p_F I_2)^{-1}, \chi(q)) \quad \text{when } \chi(q) = \chi(q)s.$$

Proof. Appendix (§ A.5). □

COROLLARY 4.3. *Suppose that R is a field of characteristic p.*

1) *The $\mathcal{H}_R(G, I(1))$-module $(\operatorname{ind}_B^G \chi)^{I(1)}$ is*
   - *cyclic, indecomposable,*
   - *simple if and only if $\chi \neq \chi s$.*
2) *Two $\mathcal{H}_R(G, I(1))$-modules $(\operatorname{ind}_B^G \chi)^{I(1)}$ and $(\operatorname{ind}_B^G \chi')^{I(1)}$ are isomorphic if and only if $\chi = \chi'$.*

Proof.

1) The standard modules are cyclic. When $\chi(q) \neq \chi(q)s$, the standard $\mathcal{H}_R(G, \omega)$-modules are simple and $\chi \neq \chi s$ is regular. We consider now the Iwahori case $\chi(q) = \chi(q)s$. Then the character

https://doi.org/10.1112/S0010437X03000071 Published online by Cambridge University Press

χ is regular if and only if $\chi(st) \neq \chi(ts)$ and by Proposition 1.1, a standard $\mathcal{H}(G, I)$-module $M_2(a, z)$ is always indecomposable, and it is reducible if and only if $a^2 = z$ when the characteristic of R is p. Using that $\chi(st)\chi(ts) = \chi(p_F I_2)$, we see that $\chi(st) = \chi(ts)$ if and only if $M_2(\chi(st)^{-1}, \chi(p_F I_2)^{-1})$ is reducible.

2) Two standard $\mathcal{H}_R(G, I(1))$-modules are isomorphic if and only if they have the same central character.

  i) Regular case: the S_2-orbit of $\chi(q)$ has two elements. From § 2.3, the modules $M_2(0, \chi(st)^{-1}, \chi(p_F I_2)^{-1}, \chi(q)), M_2(0, \chi'(st)^{-1}, \chi'(p_F I_2)^{-1}, \chi'(q))$
  - are isomorphic if and only if their values on st and on $p_F I_2$ are the same, i.e. $\chi = \chi'$, when $\chi(q) = \chi'(q)$;
  - are never isomorphic when $\chi'(q) = \chi(q)s$, because $M_2(0, \chi'(st)^{-1}, \chi'(p_F I_2)^{-1}, \chi'(q)) = M_2(\chi'(st)^{-1}, 0, \chi'(p_F I_2)^{-1}, \chi(q))$ and $\chi(st) \neq 0$.

  ii) Iwahori case: $\chi(q) = \chi(q)s = \chi'(q)$. By Proposition 1.1, the modules $M_2(\chi(st)^{-1}, \chi(p_F I_2)^{-1})$ and $M_2(\chi'(st)^{-1}, \chi'(p_F I_2)^{-1})$ are isomorphic if and only if their values on st and on $p_F I_2$ are the same, i.e. $\chi = \chi'$. □

4.2 Integral structure

Let (E, R, k) be a p-modular setting as in § 1.5. The principal representation induced from an R-integral E-character has an evident R-integral structure with reduction the principal representation parabolically induced from the reduction of χ. We will soon prove that the converse is not true. There are R-integral representations which are not induced from an R-integral E-character. The $I(1)$-invariants of an R-integral principal representation are clearly an R-integral $\mathcal{H}_E(G, I(1))$-module. The converse is probably true, but has not been proved without restrictions on χ, F.

Proposition 4.4.

i) *The* $\mathcal{H}_E(G, I(1))$*-module* $(\operatorname{ind}_B^G \chi)^{I(1)}$ *is* R*-integral iff*

$$\chi(p_F I_2) \in R^*, \quad \chi(st)^{-1} + q\chi(ts)^{-1} \in R.$$

ii) *When* $F = \mathbf{Q}_p$ *and* χ *unramified, the principal representation* $\operatorname{ind}_B^G \chi$ *of* G *is* R*-integral iff the* $\mathcal{H}_E(G, I(1))$*-module* $(\operatorname{ind}_B^G \chi)^{I(1)}$ *is* R*-integral.*

One deduces part i from Theorem 4.2 and from §§ 1.6 and 2.4; then property ii results from Breuil [Bre01, 3.2.1].

The condition of R-integrality is equivalent to condition a or to condition b below:

a) $\chi(st)\chi(ts) \in R^*, \chi(st)^{-1}, q\chi(ts)^{-1} \in R$;

b) $0 \leqslant \operatorname{val} \chi(ts) = -\operatorname{val} \chi(st) \leqslant \operatorname{val}(q)$ where val is the valuation in E.

4.3 Irreducibility and indecomposability criteria

The simple following criteria of irreducibility or of indecomposability are very useful to study a principal representation when R is a field of characteristic p.

Criterium 4.5 (Irreducibility). *Let* R *be any field of characteristic* p *and let* $V \in \operatorname{Mod}_R G$ *non-zero generated by* $V^{I(1)}$*. If* $V^{I(1)}$ *is simple as a right* $\mathcal{H}_R(G, I(1))$*-module, then* V *is irreducible.*

Proof. Let W be a non-zero subrepresentation of V. Then $W^{I(1)}$ is a non-zero $\mathcal{H}_R(G, I(1))$-submodule of $V^{I(1)}$, hence $W^{I(1)} = V^{I(1)}$ because $V^{I(1)}$ is simple. As $V^{I(1)}$ generates V as a representation of G we deduce $W = V$. Hence V is irreducible. □

Criterium 4.6 (Indecomposability). *Let* R *be any field of characteristic* p *and let* $V \in \operatorname{Mod}_R G$ *non-zero. If* $V^{I(1)}$ *is indecomposable as a right* $\mathcal{H}_R(G, I(1))$*-module, then* V *is indecomposable.*

Proof. Let W_1, W_2 be two non-zero subrepresentations of V such that $V = W_1 \oplus W_2$. Then $W_1^{I(1)}, W_2^{I(1)}$ are non-zero and $V^{I(1)} = W_1^{I(1)} \oplus W_2^{I(1)}$. □

We give now a simple proof of the decomposition of a principal representation $\operatorname{ind}_B^G \chi$, using Corollary 4.3, when R is a field of characteristic p (see [BL94, BL95]).

4.4 Decomposition of a principal representation

Theorem 4.7. *When R is a field of characteristic p, the principal representation $\operatorname{ind}_B^G \chi$ is irreducible when $\chi \neq \chi s$ is regular, and for two different regular characters χ, χ', the representations $\operatorname{ind}_B^G \chi, \operatorname{ind}_B^G \chi'$ are not isomorphic. The representation $\operatorname{ind}_B^G 1$ is indecomposable of length 2, with submodule the trivial representation and quotient the Steinberg representation.*

This is false for the finite case or in characteristic $\neq p$. In the finite case, $\operatorname{ind}_B^G \chi$ is always reducible; in characteristic $\neq p$ the Jordan–Holder sequences of $\operatorname{ind}_B^G \chi, \operatorname{ind}_B^G \chi s$ are always the same.

Proof.

a) Irreducible principal representations. By Criterium 4.5 of irreducibility, the cyclic representation $\operatorname{ind}_B^G \chi$ (see Theorem 4.10(a)) is irreducible when the $\mathcal{H}_R(G, I(1))$-module $(\operatorname{ind}_B^G \chi)^{I(1)}$ is simple. Then we apply Corollary 4.3.

b) Reducible principal representations. When χ is not regular, $\operatorname{ind}_B^G \chi$ is of the form $\chi_1 \det \otimes \operatorname{ind}_B^G 1$ for a character χ_1 of F^*.

The principal representation $\operatorname{ind}_B^G 1$ is indecomposable because $(\operatorname{ind}_B^G 1)^{I(1)}$ is indecomposable by Corollary 4.3. It is reducible because it contains the trivial representation. The quotient of $\operatorname{ind}_B^G 1$ by the trivial representation is called the Steinberg R-representation St of G. The Steinberg representation is cyclic because $\operatorname{ind}_B^G 1$ is cyclic. The image of the natural map

$$(\operatorname{ind}_B^G 1)^{I(1)} \to (\mathrm{St})^{I(1)}$$

is irreducible (the sign character). By Criterium 4.5 of irreducibility, St is irreducible if this map is surjective. The functor of $I(1)$-invariant is not right exact and this is not evident. We may replace $I(1)$ by I because $(\operatorname{ind}_B^G 1)^{I(1)} = (\operatorname{ind}_B^G 1)^I$ and this implies that the characters of I subquotients of $\operatorname{ind}_B^G 1$ restricted to I are trivial, hence $\mathrm{St}^{I(1)} = \mathrm{St}^I$. We recall the proof of the surjectivity of the natural map

$$(\operatorname{ind}_B^G 1)^I \to (\mathrm{St})^I$$

due to Barthel and Livne [BL95, 3.4]. Let $f \in \operatorname{ind}_B^G 1$ fixed by I modulo the constants. There exists a function $a : I \to \overline{\mathbf{F}}_p$ such that $f(gi) = f(g) + a(i)$ for any $g \in G, i \in I$. We want to prove that $a(i) = 0$ for any $i \in I$. This is certainly the case for any $i \in I$ such that there exists $g \in G$ with $gig^{-1} \in B$. Hence $a(i) = 0$ when $i \in I$ is upper or lower triangular. These matrices generate the group I as

$$\begin{pmatrix} a & b \\ p_F c & d \end{pmatrix} = \begin{pmatrix} a & 0 \\ p_F c & d - p_F cb/a \end{pmatrix} \begin{pmatrix} 1 & b/a \\ 0 & 1 \end{pmatrix},$$

and it is clear that $f(gi) = f(g)$ and $f(gi') = f(g)$ for any $g \in G$ implies that $f(gii') = f(g)$ for any $g \in G$.

Let U be the strictly upper triangular group of G. General arguments [Vig96, II.2.1] imply the following.

Corollary 4.8. *In characteristic p, the trivial representation and the irreducible principal representations of G are the only irreducible representations with non-zero U-coinvariants.*

https://doi.org/10.1112/S0010437X03000071 Published online by Cambridge University Press

This is false in the finite case, or in characteristic $\neq p$ and $q+1 \neq 0$ where the U-coinvariant of the Steinberg representation is never 0.

Corollary 4.9. *In characteristic p, the functor of $I(1)$-invariants gives a bijection between the isomorphism classes of the irreducible subquotients of the principal representations of G and the isomorphism classes of the simple right $\mathcal{H}_R(G, I(1))$-modules which are not supersingular (§ 3.2).*

4.5 Parabolic induction and compact induction

The next theorem describes the principal R-representation $\operatorname{ind}_B^G \chi$ of G as a canonical quotient of the compactly induced $\operatorname{ind}_I^G \chi(q)$, where χ is an R-character of B, with restriction $\chi(q)$ to $T(O_F)$ trivial on the pro-p-Sylow of $T(O_F)$ and identified to an R-character of $I/I(1)$. This is a non-trivial result, essentially due to Schneider and Stuhler who considered the case $G = GL(n,F), R = \mathbf{Z}, \chi = \mathrm{id}$. This theorem was extended by Dat [Dat99] to a much more general setting but only over a field of characteristic $\neq p$. As the hypothesis $n=2$ and $R = \overline{\mathbf{F}}_p$ brings no simplification we suppose in this section $G = GL(n,F)$ and that R is a commutative ring. The notations already introduced for $GL(2,F)$ extend naturally.

Theorem 4.10. *The function $f_{Ig,\chi(q)} \in \operatorname{ind}_I^G \chi(q)$ has support I and value 1 at $g \in G$, and the function $f_{BI,\chi} \in (\operatorname{ind}_B^G \chi)^{I(1)}$ has support $BI = BI(1)$ and value 1 at $1 \in G$. The function $f_{BI,\chi}$ is an eigenvector for the action of I of eigenvalue $\chi(q)$. Also we have a unique RG-homomorphism*

$$\Phi : \operatorname{ind}_I^G \chi(q) \to \operatorname{ind}_B^G \chi$$

sending $f_{I,\chi(q)}$ to $f_{BI,\chi}$. The map Φ is surjective because $\operatorname{ind}_B^G \chi$ is a cyclic RG-module generated by $f_{BI,\chi}$.

This results from [SS91, Proposition 8, p. 78] as follows.

a) *Any open compact subset of $B\backslash G$ can be written as a finite disjoint union of subsets of the form $B\backslash BIg$ with $g \in G$.*

We give a proof of a stronger version of part a in part 3 of § A.7 valid in a more general setting. In part a one can suppose $g \in HK$ where $K := GL(n, O_F)$ and H is the semi-group generated by the diagonal matrices $z^{\pm 1}, y_1, \dots, y_{n-1}$ defined by

$$z := p_F I_n = \operatorname{diag}(p_F, \dots p_F), \quad y_1^{-1} := \operatorname{diag}(1, p_F \dots p_F), \dots, y_{n-1}^{-1} := \operatorname{diag}(1, \dots 1, p_F).$$

The Iwahori subgroup I has an Iwahori decomposition

$$I = (I \cap \overline{U}) T(O_F)(I \cap U)$$

where $B = T(F)U$ and $\overline{B} = T(F)\overline{U}$ is the lower triangular subgroup. The elements in the semi-group H contract $I \cap U$, normalize $T(O_F)$, dilate $I \cap \overline{U}$.

We will determine the kernel of Φ. For any $g \in T(F)$, there exists a function E_g (denoted $E_{g,\chi(q)}$ in § 2) in $\mathcal{H}_R(G, \chi(q))$ with support IgI and with value 1 at g. The basic property of H is that the linear map

$$\tau_{\chi(q)} : \; R[H] \to \mathcal{H}_R(G, \chi(q)), \quad h \mapsto E_h$$

is injective and respects the following product.

b) *For any $h, h' \in H$ we have $E_h * E_{h'} = E_{hh'}$.*

The well known proof is recalled in § A.7. The image of $R[H]$ in $\mathcal{H}_R(G, \chi(q))$ is a commutative subalgebra denoted by $\mathcal{A}$. We prove in a more general setting (§ A.7) the important geometric property [SS91, Proposition 7, p. 77]:

c) *$BIhk \cap BIhk' \neq \emptyset$ implies $Ihk = Ihk'$ for any $(h, k, k') \in H \times K^2$.*

This is the main ingredient of the following relation:

d) $\Phi(E_h) = \chi(h)^{-1} f_{BI,\chi}$ *for any* $h \in H$.

Note that as an R-module, $\mathcal{H}_R(G, \chi(q))$ identifies with the $(I, \chi(q))$-invariants of $\operatorname{ind}_I^G \chi(q)$ and we can define $\Phi(E_h)$. The property d follows from the fact that $\Phi(E_h)$ is $I(1)$-invariant and of support contained in $BIhI = BI$ as h^{-1} contracts $I \cap \overline{B}$. Hence $\Phi(E_h) = \Phi(E_h)(1) f_{BI,\chi}$. To show that $\Phi(E_h)(1) = \chi(h)^{-1}$, one uses that

$$IhI = Ih(I \cap \overline{U}) = \cup_k Ihk$$

finite disjoint union) where $k \in I \cap \overline{U}$, $\chi(q)$ is trivial on $I \cap \overline{U}$,

$$E_h = \sum_k f_{Ihk,\chi(q)}, \quad \Phi(E_h) = \sum_k (hk)^{-1} f_{BI,\chi},$$

and the union $BIhI = \cup_k BIhk$ is disjoint by property c. The identity $1 \in G$ belongs to BIh and we deduce $\Phi(E_h)(1) = h^{-1} f_{BI,\chi}(1) = \chi(h^{-1})$.

The character χ^{-1} of $T(F)$ defines a semi-group homomorphism $H \to R$, and an R-algebra homomorphism $\mathcal{A} \to R$ sending h and E_h on $\chi^{-1}(h)$ for all $h \in H$, still denoted by χ^{-1}. We obtain in this way all the characters of H and $\mathcal{A}$ sending y_i, E_{y_i} to an invertible element in R for all $1 \leqslant i \leqslant n-1$. The subrepresentation of $\operatorname{ind}_I^G \chi(q)$ generated by $(\alpha - \chi^{-1}(\alpha)) f_{I,\chi(q)}$ for all $\alpha \in \mathcal{A}$ is contained in the kernel of Φ by relation d. This means that the kernel of the projection

$$p : \operatorname{ind}_I^G \chi(q) \to R \otimes_{\mathcal{A},\chi^{-1}} \operatorname{ind}_I^G \chi(q)$$

is contained in the kernel of Φ, and therefore there exists an RG-homomorphism

$$\overline{\Phi} : R \otimes_{\mathcal{A},\chi^{-1}} \operatorname{ind}_I^G \chi(q) \to \operatorname{ind}_B^G \chi$$

such that $\Phi = \overline{\Phi} \circ p$. The map $\overline{\Phi}$ is surjective as Φ. We will prove that $\overline{\Phi}$ is injective.

THEOREM 4.11. $\overline{\Phi} : R \otimes_{\mathcal{A},\chi^{-1}} \operatorname{ind}_I^G \chi(q) \to \operatorname{ind}_B^G \chi$ *is an isomorphism.*

The proof which follows [SS91] consists in finding a subspace X of $\operatorname{ind}_I^G \chi(q)$ such that the restriction of p to X remains surjective, and the restriction of Φ to X is injective. The first try is the subspace X' of functions with support contained in IHK. From [SS91, Lemma 12, p. 80] we obtain the following:

e) *For any* $g \in G$, *there exists* $h \in H$ *such that* $IhIg \subset IHK$.

The restriction of p to X' remains surjective. Indeed for any $g \in G$, the image by p of $f_{Ig,\chi(q)}$ and of $\chi(h) E_h * f_{Ig,\chi(q)}$ of support contained in $IhIg$ are equal. This results from relation d and from the formula $f_{Ig,\chi(q)} + \chi(h)((E_h - \chi(h)^{-1}) * f_{Ig,\chi(q)}) = \chi(h) E_h * f_{Ig,\chi(q)}$.

The element $h_o \in H$ defined by

$$h_o^{-1} := \operatorname{diag}(1, p_F, \ldots, p_F^{n-1})$$

has the following property:

f) *Given* $h \in H$ *and a big enough integer* $n > 0$, *there exists* $h' \in H$ *with* $h'h = h_o^n$.

This implies, using $Ih'Ihk \subset Ih'hK$ for $h, h' \in H, k \in K$ and the argument above, that the restriction of p to the union

$$X := \bigcup_{n \geqslant 0} \operatorname{ind}_I^{Ih_o^n K} \chi(q)$$

remains surjective. The property c implies that the restriction of Φ to X is injective. The theorem is proved. □

https://doi.org/10.1112/S0010437X03000071 Published online by Cambridge University Press

5. Supersingular modules and Galois $\overline{\mathbf{F}}_p$-representations of dimension 2

Let R be an algebraically closed field of characteristic p and let $G := GL(2, F)$. Any irreducible R-representation σ of $W(\overline{F}/F)$ of dimension 2 is trivial on the wild ramification subgroup and any irreducible R-representation of G has a non-zero $I(1)$-invariant vector. If there is a local Langlands R-correspondence for $GL(2, F)$, and if the main Conjecture 4.1 is true, there will be a 'local Langlands correspondence' between the irreducible R-representations of $W(\overline{F}/F)$ of dimension 2 and the supersingular simple right $\mathcal{H}_R(G, I(1))$-modules of § 3.2.

Definition 5.1 (Supersingular modules). An irreducible R-representation of G is called supersingular if it is not a subquotient of $\operatorname{ind}_B^G \chi$ for some R-character χ of B.

A simple right $\mathcal{H}_R(G, I(1))$-module is called supersingular, if it is not isomorphic to a subquotient of $(\operatorname{ind}_B^G \chi)^{I(1)}$, for some R-character χ of B.

Remark. The number of supersingular simple right $\mathcal{H}_R(G, I(1))$-modules with a given action of p_F is $(q^2 - q)/2$.

This is coherent with § 3.2 and Theorem 4.2. The terminology 'supersingular' instead of 'supercuspidal' was introduced by Barthel and Livne and is natural in the context of elliptic curves.

An R-character of F^* is determined by its value z_o on p_F and by its restriction to the subgroup of roots of 1 of order dividing $q - 1$ in F^*, identified with a non-regular character $\chi_o = \chi_o s$ of $I/I(1)$. The twist of the simple supersingular $\mathcal{H}_R(G, I(1))$-module $M(0, z, \omega)$ by the character of F^* associated to (z_o, χ_o) is defined as $M(0, zz_o, \omega\chi_o)$.

5.1 Galois representations

The irreducible R-representations of $W_F = W(\overline{F}/F)$ of any dimension $n \geqslant 1$ are described in [Vig97, 1.14]. They are

$$\operatorname{ind}_{W_{F_n}}^{W_F} \chi,$$

the representations induced by the regular R-characters χ of W_{F_n}, where F_n/F is the unramified extension in $\overline{F}$ of degree n. The distinct $\operatorname{Gal}(F_n/F)$-conjugates of χ induce isomorphic representations and there are no other isomorphisms between the representations. We need only the case $n = 2$ but this brings no simplification.

Via local class field theory sending a geometric Frobenius to p_F, χ identifies with an R-character of F_n^*, determined by its value $z \in R^*$ at p_F and by its restriction ρ to the subgroup of roots of 1 of order dividing $q^n - 1$ in F_n^*. The determinant of $\operatorname{ind}_{W_{F_n}}^{W_F} \chi$ identifies with the character of F^* associated with (z, ρ_o) where ρ_o is the restriction of ρ to the subgroup of roots of 1 of order dividing $q - 1$ in F^*. The $\operatorname{Gal}(F_n/F)$-orbit of χ identifies with the R-characters of F_n^* associated to $(z, \rho^m),\ m \in q^{\mathbf{Z}}$.

Remark. The number of irreducible R-representations of W_F of dimension n with a given value of the determinant at p_F, is equal to the number

$$m_n(q) = n^{-1} \sum_{d|n} \mu(n/d) q^d,$$

of irreducible unitary polynomials in $\mathbf{F}_q[X]$ of degree n. Here μ is the Möbius function (see [IR90, p. 84] when $q = p$). When $n = 2$ we get:

$$m_2(q) = (q^2 - q)/2.$$

A marvellous *numerical* coincidence occurs.

https://doi.org/10.1112/S0010437X03000071 Published online by Cambridge University Press

5.2 Number of supersingular modules

Remark. The number of supersingular simple right $\mathcal{H}_R(G, I(1))$-modules with a given action of p_F is equal to the number of irreducible R-representations of W_F of dimension 2, with a given value of the determinant at p_F.

Using the following Lemma 5.2, one can show that the next remark holds.

Remark. There is a (not unique) bijection between the irreducible R-representations of W_F of dimension 2 and the supersingular simple right $\mathcal{H}_R(G, I(1))$-modules, compatible with the twist by a character of F^* and local class field theory, such that the determinant corresponds to the central character restricted to F^* naturally embedded in $\mathcal{H}_R(G, I(1))$.

Let μ_F be the fundamental character $O_F^* \to R^*$ trivial on $1 + p_F O_F$. The R-characters of I trivial on $I(1)$ are $\mu_F^i \otimes \mu_F^j$ for integers i, j modulo $q - 1$. The non-trivial element of S_2 permutes i, j.

The regular R-characters of $O_{F_2}^*$ trivial on $1 + p_F O_{F_2}^*$ are $\mu_{F_2}^r$ for integers $r \not\equiv qr$ modulo $q^2 - 1$. The non-trivial element of S_2 permutes r, qr.

One wants a bijection ρ between the set of non-ordered pairs (i, j) of integers modulo $q - 1$, and the set of non-ordered pairs $(r, qr), r \neq qr$, of integers modulo $q^2 - 1$, which is equivariant for the action of the group of integers k modulo $(q - 1)$ which sends (i, j) on $(i + k, j + k)$, and (r, qr) on $(r + k(q + 1), qr + k(q + 1))$.

The two sets have $q(q - 1)/2$ elements. Each orbit of $\mathbf{Z}/(\mathbf{q} - \mathbf{1})\mathbf{Z}$ in the (i, j)-set or in the (r, qr)-set has $q - 1$ elements, with the following exception: if q is odd, the $\mathbf{Z}/(\mathbf{q} - \mathbf{1})\mathbf{Z}$-orbit of

- $(0, (q - 1)/2) \bmod q - 1$, in the (i, j)-set,
- $((q + 1)/2, q[(q + 1)/2]) \bmod q^2 - 1$, in the $(r, qr), r \neq qr$, set has $(q - 1)/2$ elements.

Hence many bijections ρ exist.

LEMMA 5.2. *There exists a bijection from the S_2-orbits of R-characters of $I/I(1)$ to the regular S_2-orbits of $O_{F_2}^*/(1 + p_F O_{F_2})$, compatible with the twist by the characters of $O_F^*/(1 + p_F O_F)$.*

Let us give an example for ρ. The number of $\mathbf{Z}/(\mathbf{q} - \mathbf{1})\mathbf{Z}$-orbits of $q - 1$ elements in each set is $[q/2]$, where $[q/2] = q/2$ if q is even and $[q/2] = (q - 1)/2$ if q is odd. One checks that a set of representatives of these orbits is

- in the (i, j)-set: $(0, n) \bmod q - 1$, for $0 \leqslant n \leqslant [q/2] - 1$,
- in the $(r, qr), r \neq qr$, set: $(n + 1, q(n + 1)) \bmod q^2 - 1$ for $0 \leqslant n \leqslant [q/2] - 1$.

One can choose ρ sending $n(0, 1) + k(1, 1) \bmod q - 1$, to $(n + 1)(1, q) + k(q + 1, q + 1) \bmod q^2 - 1$ for $0 \leqslant n \leqslant [q/2]$.

We give now some partial results on supersingular irreducible R-representations of G.

PROPOSITION 5.3.

1) *Any irreducible R-representation V of G such that the $\mathcal{H}_R(G, I(1))$-module $V^{I(1)}$ has a simple supersingular subquotient is supersingular.*
2) *A simple module contained in $V^{I(1)}$ is trivial or supersingular when V is a supersingular irreducible R-representation of G, on which p_F acts by multiplication by $z \in R^*$.*

Proof.

1) This results from the explicit description of the $\mathcal{H}_R(G, I(1))$-module $V^{I(1)}$ when V is a principal R-representation (Theorem 4.2).

https://doi.org/10.1112/S0010437X03000071 Published online by Cambridge University Press

2) Twisting the irreducible representation V by a character, if necessary, we reduce to the Iwahori case where V is a quotient of $\operatorname{ind}_I^G 1$ or to the regular case where V is a quotient of $\operatorname{ind}_I^G \chi(q) \simeq \operatorname{ind}_I^G \chi(q)s$ for a regular R-character $\chi(q) \neq \chi(q)s$ of I. We prove part 2 in the Iwahori case; a similar argument works in the regular case. In the Iwahori case, $V^{I(1)} = V^I$ because the order of the finite quotient $I/I(1)$ is prime to p. Let $\mathcal{A}$ be the subalgebra of $\mathcal{H}_R(G,I)$ generated by $T^{\pm 2}, ST$. The central element T^2 acts on V^I by multiplication by z. If V^I contains a simple $\mathcal{H}_R(G,I)$-submodule M, it contains an ST-eigenvector m with eigenvalue λ. The RG-morphism

$$\phi_V : \operatorname{ind}_I^G 1 \to V$$

sending the characteristic function f_I of I on m is surjective as V is irreducible. The kernel of ϕ_V contains the subrepresentation of $\operatorname{ind}_I^G 1$ generated by $f_I(\alpha - \mu(\alpha)) = \alpha - \mu(\alpha)$ for all $\alpha \in \mathcal{A}$ where μ is the R-character of $\mathcal{A}$ such that $\mu(T^2) = z, \mu(ST) = \lambda$. This means that V is a quotient of $R \otimes_{\mathcal{A},\mu} \operatorname{ind}_I^G 1$. By Theorem 4.11, λ must be zero because V is supersingular. We deduce that the eigenvalues of ST in M are 0. A trivial character or a supersingular module are the only simple right $\mathcal{H}_R(G,I)$-modules with this property (see §§ 1.3 and 1.4). □

Breuil [Bre01] classified the irreducible supersingular representations, building on the work of Barthel and Livne when $(F,R) = (\mathbf{Q}_p, \overline{\mathbf{F}}_p)$, but his proof cannot work when $F \neq \mathbf{Q}_p$. We prove the main Conjecture 4.1 for $(\mathbf{Q}_p, \overline{\mathbf{F}}_p)$.

Theorem 5.4. *The $I(1)$-invariant functor $V \to V^{I(1)}$ induces a bijection between the isomorphism classes of the irreducible $\overline{\mathbf{F}}_p$-representations of $GL(2,\mathbf{Q}_p)$ with a central character and the isomorphism classes of the finite dimensional simple right $\mathcal{H}_{\overline{\mathbf{F}}_p}(G, I(1))$-modules.*

Proof. By Corollary 4.9 we need only to consider the supersingular irreducible representations of G. From the computations of [Bre01, 3.2.4], proofs of [Bre01, corollaire 4.1.1] and of [Bre01, corollaire 4.1.3], one deduces that $V \to V^{I(1)}$ is an injective map from the supersingular irreducible representations of G to the supersingular $\mathcal{H}_R(G, I(1))$-modules. By a counting argument (see [Bre01, 4.2.3] and § 5.2), the map is a bijection. □

Acknowledgements

Part of the proof was done at the MSRI in Berkeley during the fall of 2000 for the workshop organized by P. Schneider and J. Teitelbaum of Münster, whom I thank for their invitation, but most of it was done in Paris at the Institut de Mathématiques de Jussieu and at the University of Paris 7, during the spring of 2001, after Breuil told me about his result. I thank him for stimulating discussions and for correcting a mistake in a preliminary draft. I thank also the CNRS for the delegation and time during this year, for allowing me to work in excellent conditions.

Appendix A

A.1 Computations in Hecke algebras [Vig96, I.8]

Let R be a commutative ring, let G be a locally profinite group, let K be an open subgroup of G and let (σ, V) be a finitely generated R-representation of K. The *Hecke algebra*

$$\operatorname{End}_{RG} \operatorname{ind}_K^G \sigma$$

is isomorphic as an R-module, to the R-module $\mathcal{H}_R(G,\sigma)$ of functions $f : G \to \operatorname{End}_R V$ with compact support satisfying

$$f(k_1 g k_2) = \sigma(k_1) f(g) \sigma(k_2)$$

for all $g \in G, k_1, k_2 \in K$. We describe an isomorphism after some preliminaries.

https://doi.org/10.1112/S0010437X03000071 Published online by Cambridge University Press

For any $g \in G$ and any $v \in V$ we denote by $[Kg, v]$ the function in $\rho = \mathrm{ind}_K^G \sigma$ with support Kg and value v at g. We have the relation

$$[Kg, v] = \rho(g)^{-1}[K, v].$$

The functions $[Kg, v]$ for g fixed and for v in a set of generators of the R-module V span $\rho := \mathrm{ind}_K^G \sigma$ as an RG-module.

We say that $g \in G$ *intertwines* σ, when the R-module $\mathcal{I}_g$ of intertwining operators $F \in \mathrm{End}_R V$,

$$F\sigma(k) = \sigma(gkg^{-1})F \quad \text{for all } k \in K \cap g^{-1}Kg,$$

is non-zero. This definition is not the same as in [Vig96, I.8.2, I.8.10] where g has been replaced by g^{-1}. The intertwining set is the set of $g \in G$ such that $\mathcal{I}_g$ is non-empty. When $\mathcal{I}_g$ is non-empty, for any $F \in \mathcal{I}_g$ we denote by $[KgK, F]$ the function in $\mathcal{H}_R(G, \sigma)$ with support KgK and value F at g.

The most important case is when σ is a character $K \to R^*$. Then $I_g \simeq R$ if g intertwines σ. When $F \in I_g$ is the identity, $[KgK, F]$ is simply denoted by $[KgK]$ or $E_{g,\sigma}$ or E_g. These elements form an R-basis of $\mathcal{H}_R(G, \sigma)$.

The *R-module isomorphism*

$$A \leftrightarrow f : \mathrm{End}_{RG}\, \mathrm{ind}_K^G \sigma \simeq \mathcal{H}_R(G, \sigma)$$

is defined by

$$f(g) : v \mapsto A[K, v](g) \quad \text{for any } g \in G,\ v \in V$$

and conversely,

$$A : \phi \mapsto f * \phi \quad \text{for any } \phi \in \mathrm{ind}_K^G \sigma$$

where

$$f * \phi(x) := \sum_{t \in K\backslash G} f(xt^{-1})\phi(t)$$

is a well defined element of $\mathrm{ind}_K^G \sigma$. The isomorphism respects the product if the product on $\mathcal{H}_R(G, \sigma)$ is the convolution given by the formula:

$$f * f'(x) = \sum_{t \in K\backslash G} f(xt^{-1})f'(t) = \sum_{t \in G/K} f(t)f'(t^{-1}x).$$

Example I. Convolution of a double coset $f = [KgK, F]$ and of a coset $\phi = [Kg', v]$:

$$[KgK, F] * [Kg', v] = \sum_{Kg''} [Kg'', v'']$$

where

$$KgKg' = \cup_{g''} Kg'' \quad \text{(disjoint union)},$$
$$v'' = \sigma(\alpha)F\sigma(\beta)v, \quad g'' = \alpha g \beta g', \quad \alpha, \beta \in K.$$

Example II. Convolution of two double cosets $f = [KgK, F]$, $f' = [Kg'K, F']$:

$$[KgK, F] * [Kg'K, F'] = \sum_{Kg''K} [Kg''K, F'']$$

https://doi.org/10.1112/S0010437X03000071 Published online by Cambridge University Press

where

$$KgKg'K = \cup_{g''} Kg''K \quad \text{(disjoint union)},$$
$$F'' = \sum_t f(t) f'(t^{-1}g''),$$
$$KgK \cap g''Kg'^{-1}K = \cup_t tK \quad \text{(disjoint union with } m(g, g'; g'') \text{ terms)},$$
$$F'' = \sum_\alpha \sigma(\alpha)F\sigma(\beta)F'\sigma(\gamma), \qquad t = \alpha g, \quad g'' = \alpha g\beta g'\gamma, \quad \alpha, \beta, \gamma \in K.$$

When $KgKg'K = Kgg'K$ and $g^{-1}KgK \cap g'Kg'^{-1}K = K$ the formula gives:

$$[KgK, F] * [Kg'K, F'] = [Kg''K, F''], \quad g'' = gg', \quad F'' = FF'.$$

This is the case when g or g' normalizes K, or when K has an Iwahori decomposition and g, g' are in 'good position' as in § A.7.

A.2 Notations of § 2

We consider the Hecke algebra $\mathcal{H}_R(G, \sigma)$ where $(G, K, \sigma) = (GL(2, F), I, \chi)$, $\chi \neq \chi s$ regular. The intertwining set of χ is T. The elements $E_{(st)^a(ts)^b}$ for all $a, b \in \mathbf{Z}$ form a basis of $\mathcal{H}_R(G, \chi)$, where s, t are defined at the beginning of § 1. Clearly $Z := E_{p_F I_2}$ belongs to the center of the algebra. Set $X := E_{ts}$ and $Y := E_{(ts)^{-1}}$. We have $E_{st} = ZY$ because $stts = p_F I_2$. We have the following relations 1–3:

1) $Z * E_g = E_g * Z = E_{p_F g}$ for all $g \in T$;

2) $XX^n = X^{n+1}$, $YY^n = Y^{n+1}$ for any integer $n > 0$.

   The relation $XX^n = X^{n+1}$ results from parts a and b below:

   a) $ItsI(ts)^n I = I(ts)^{n+1}I$, i.e. the length of $(ts)^n$ in the generalized affine Weyl group is equal to n,

   b) $ItsI \cap (ts)^{n+1}I(ts)^{-n}I = tsI$ for any integer $n > 0$ because we have the disjoint unions

   $$I(ts)^n I = \bigcup_{x \in A_n} \begin{pmatrix} 1 & 0 \\ p_F x & 1 \end{pmatrix} (ts)^n I, \quad I(ts)^{-n} I = \bigcup_{x \in A_n} \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix} (ts)^{-n} I, \tag{A.1}$$

   where A_n is a system of representatives of $O_F/p_F^n O_F$: A_1 is the set of the elements in O_F satisfying $x^q = x$ and $A_n := \{u_o + p_F u_1 + \cdots + p_F^{n-1} u_{n-1},\ u_i \in A_1\}$. The proof of the relation $YY^n = Y^{n+1}$ is similar.

3) $XY = YX = qE_1$.

Proof of $XY = qE_1$. Applying (A.1) to $n = 1$ we compute $ItsI(ts)^{-1}I$ as a disjoint union of (I, I)-cosets

$$ItsI(ts)^{-1}I = I \bigcup_{u \in A_1 - 0} I \begin{pmatrix} 1 & p_F^{-1}u \\ 0 & 1 \end{pmatrix} I.$$

The formula

$$\begin{pmatrix} 1 & 0 \\ x & 1 \end{pmatrix} = \begin{pmatrix} 1 & 1/x \\ 0 & 1 \end{pmatrix} s \begin{pmatrix} x & 1 \\ 0 & -1/x \end{pmatrix} \tag{A.2}$$

when $x \neq 0$, shows that $\left(\begin{smallmatrix} 1 & p^{-1}u \\ 0 & 1 \end{smallmatrix}\right)$ is not contained in the support ITI of the algebra $\mathcal{H}_R(G, \chi)$, the character χ being regular. Hence $XY = XY(1)E_1$. Applying (A.1) to $n = 1$ and $\chi\left(\begin{smallmatrix} 1 & 0 \\ px & 1 \end{smallmatrix}\right) = 1$ for all $x \in A_1$ we have $XY(1) = q$. The proof of the relation $YX = qE_1$ is similar. □

https://doi.org/10.1112/S0010437X03000071 Published online by Cambridge University Press

A.3 Notations of §§ 1 and 2

We consider the Hecke algebra $\mathcal{H}_R(G,\sigma)$ where $\sigma=\chi$ if χ is non-regular which means $\chi=\chi_1 \det$ for some character χ_1 of O_F^*, and $\sigma=\chi\oplus\chi s$ if χ is regular. As t normalizes I, the product by $[It,*]$ in $\mathcal{H}_R(G,\sigma)$ is very simple:

$$[It,F]*[IgI,F']=[ItgI,FF'],\quad [IgI,F']*[It,F]=[IgtI,F'F]$$

for any $F\in\mathcal{I}_t, g\in G, F'\in\mathcal{I}_g$.

Let $F\in\mathcal{I}_s=\mathcal{I}_t$, $S:=[IsI,F]$; we compute the square S^2.

We have $IsIsI=I\cup IsI$ (disjoint union) and $S^2=[I,S^2(1)]+[IsI,S^2(s)]$. We compute $S^2(1)$. We have

$$IsI=\bigcup_{x\in A_1}\begin{pmatrix}1&x\\0&1\end{pmatrix}sI. \tag{A.3}$$

The representation σ is trivial on $\left(\begin{smallmatrix}1&x\\0&1\end{smallmatrix}\right)$ for any $x\in A_1$ (defined as in (A.1)), and we have $\left(\left(\begin{smallmatrix}1&x\\0&1\end{smallmatrix}\right)s\right)^{-1}=s\left(\begin{smallmatrix}1&-x\\0&1\end{smallmatrix}\right)$. Hence

$$S^2(1)=\sum_{x\in A_1}F^2=qF^2.$$

We compute $S^2(s)$. We have

$$IsI\cap sIsI=\bigcup_{u\in A_1-0}\begin{pmatrix}1&u\\0&1\end{pmatrix}sI$$

because $s\left(\begin{smallmatrix}1&x\\0&1\end{smallmatrix}\right)s=\left(\begin{smallmatrix}1&0\\x&1\end{smallmatrix}\right)$ is equal to 1 if $x=0$ and to $\left(\begin{smallmatrix}1&1/u\\0&1\end{smallmatrix}\right)s\left(\begin{smallmatrix}u&1\\0&-1/u\end{smallmatrix}\right)$ when $x=u\neq0$ by (A.2). As before σ is trivial on $\left(\begin{smallmatrix}1&1/u\\0&1\end{smallmatrix}\right)$ and $\left(\left(\begin{smallmatrix}1&u\\0&1\end{smallmatrix}\right)s\right)^{-1}s=\left(\begin{smallmatrix}1&0\\-u&1\end{smallmatrix}\right)=\left(\begin{smallmatrix}1&-1/u\\0&1\end{smallmatrix}\right)s\left(\begin{smallmatrix}-u&1\\0&1/u\end{smallmatrix}\right)$. We have

$$S^2(s)=F^2\sum_{u\in A_1-0}\sigma\begin{pmatrix}u&1\\0&-1/u\end{pmatrix}.$$

In the non-regular case, $\sigma=\chi$ and $\chi\left(\begin{smallmatrix}u&1\\0&-1/u\end{smallmatrix}\right)=\chi_1(-1)$. We have

$$S^2=[I,qF^2]+[IsI,(q-1)\chi_1(-1)F^2]. \tag{A.4}$$

In the regular case $\chi\neq\chi s$, $\sigma=\chi\oplus\chi s$, $S^2(s)=0$ and we have

$$S^2=[I,qF^2]. \tag{A.5}$$

A.4 Functor from representations of G to modules of Hecke algebras

Let (π,W) be any R-representation of G. The R-module $\operatorname{Hom}_{RK}(\sigma,\pi)$ is a right module for the Hecke algebra $H_R(G,\sigma)$ defined in § A.1 via the canonical isomorphism

$$\operatorname{Hom}_{RK}(\sigma,\pi)\simeq\operatorname{Hom}_{RG}(\operatorname{ind}_K^G\sigma,\pi). \tag{A.6}$$

Explicitly, the action of the double coset $[KgK,F]$ on $D\in\operatorname{Hom}_{RK}(\sigma,\pi)$ is given by

$$D*[KgK,F]:v\mapsto\sum_y\pi(y)^{-1}\,DF\sigma(\kappa)(v) \tag{A.7}$$

for $v\in\sigma$, where $KgK=\cup_y Ky$ (disjoint union), and $y=g\kappa$. Two particular cases are specially important. When g normalizes K, we have $KgK=Kg$ and

$$D*[Kg,F]:v\mapsto\pi(g)^{-1}\,DF(v). \tag{A.8}$$

https://doi.org/10.1112/S0010437X03000071 Published online by Cambridge University Press

When σ is the trivial representation, $\mathrm{Hom}_{RK}(\sigma, \pi)$ identifies to the K-invariant vectors W^K of W and for all $w \in W^K$ we have

$$w * [KgK] = \sum_y \pi(y)^{-1} w. \tag{A.9}$$

A.5 Proof of Theorem 4.2

Notations are as in § 4.1 for the principal representations. Set $\omega = \chi(q)$ if $\chi(q) = \chi(q)s$ is not regular and $\omega = \chi(q) \oplus \chi(q)s$ if $\chi(q) \neq \chi(q)s$ is regular.

The space $\mathrm{Hom}_{RI}(\omega, \mathrm{ind}_B^G \chi)$ identifies with $(\mathrm{ind}_B^G \chi)^{I(1)} = Rf_{BI,\chi} \oplus Rf_{BtI,\chi}$.

The space $\mathrm{Hom}_{RI}(\chi(q), \mathrm{ind}_B^G \chi)$ identifies with $M = (\mathrm{ind}_B^G \chi)^{I(1)}$ when $\chi(q) = \chi(q)s$ is not regular, and $M = Rf_{BI,\chi}$ when $\chi(q) \neq \chi(q)s$ is regular

From (A.9) applied to $(G, K, \sigma, \pi) = (GL(2,F), I, \chi(q), \mathrm{ind}_B^G \chi)$, the right action of $f \in \mathcal{H}_R(G, \chi(q))$ on any $f_\chi \in M$ is given by convolution:

$$f_\chi * f(g) = \sum_{y \in I \backslash G} f_\chi(gy^{-1}) f(y). \tag{A.10}$$

With the notations of § A.1, the central element $E_{p_F I_2} \in \mathcal{H}_R(G, \chi(q))$ acts by multiplication by $\chi(p_F I_2)^{-1}$.

A) We suppose that $\chi(q) = \chi_1 \det$ is not regular, where χ_1 is a character of O_F^* trivial on $1 + p_F O_F$. The matrix of the action of $f \in \mathcal{H}_R(G, \chi(q))$ on M is

$$\begin{pmatrix} f_{BI,\chi} * f(1) & f_{BtI,\chi} * f(t) \\ f_{BI,\chi} * f(t) & f_{BtI,\chi} * f(t) \end{pmatrix}$$

on the basis $\{f_{BI,\chi}, f_{BtI,\chi}\}$.

Let $T, S \in \mathcal{H}_R(G, \chi(q))$ of support ItI, IsI and value 1 at t, s.

As t normalizes I and $t^2 = p_F I_2$ we have

$$f_\chi * T(g) = f_\chi(gt^{-1}) = f_\chi(gp_F^{-1}t) = \chi(p_F I_2)^{-1} f_\chi(gt).$$

In particular, $f_\chi * T(1) = \chi(p_F I_2)^{-1} f_\chi(t),\ f_\chi * T(t) = f_\chi(1)$. The matrix of T is

$$\begin{pmatrix} 0 & \chi(p_F I_2)^{-1} \\ 1 & 0 \end{pmatrix}. \tag{A.11}$$

We compute now $f_\chi * S$. Using $t = (ts)s$ we have $f_\chi(t) = \chi(ts) f_\chi(s)$. By (A.3) and (A.10) we have

$$f_\chi * S(g) = \sum_{x \in A_1} f_\chi \left(g \left(s \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix} \right)^{-1} \right) = \sum_{x \in A_1} f_\chi \left(g \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix} s \right),$$

$$f_\chi * S(1) = \sum_{x \in A_1} f_\chi \left(\begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix} s \right) = q f_\chi(s) = q \chi(ts)^{-1} f_\chi(t).$$

Using (A.2) we have

$$\sum_{x \in A_1} f_\chi \begin{pmatrix} 1 & 0 \\ x & 1 \end{pmatrix} = f_\chi(I_2) + f_\chi(s) \sum_{u \in A_1 - 0} \chi(q) \begin{pmatrix} u & 1 \\ 0 & -1/u \end{pmatrix}, \tag{A.12}$$

$$f_\chi * S(s) = \sum_{x \in A_1} f_\chi \begin{pmatrix} 1 & 0 \\ x & 1 \end{pmatrix} = f_\chi(I_2) + (q-1)\chi_1(-1) f_\chi(s),$$

$$f_\chi * S(t) = \chi(ts) f_\chi(I_2) + (q-1)\chi_1(-1) f_\chi(t).$$

https://doi.org/10.1112/S0010437X03000071 Published online by Cambridge University Press

This shows that the matrix of S is

$$\begin{pmatrix} 0 & q\chi(ts)^{-1} \\ \chi(ts) & (q-1)\chi_1(-1) \end{pmatrix}. \tag{A.13}$$

Set $m := q\chi(ts)^{-1}f_{BI,\chi} - \chi_1(-1)f_{BtI,\chi}$. Then

$$\begin{gathered} m * S\chi_1(-1) = -m \\ m * T\chi_1(-1)(S\chi_1(-1) - q) = (\chi(st)^{-1} + q\chi(ts)^{-1})m \\ m * (T\chi_1(-1))^2 = \chi(p_F I_2)^{-1}m. \end{gathered}$$

The $\mathcal{H}_R(G,\chi(q))$-module M is the image of the standard $\mathcal{H}_R(G,I)$-module,

$$M_2(\chi(st)^{-1} + q\chi(ts)^{-1}, \chi(p_F I_2)^{-1})$$

by the canonical isomorphism $\mathcal{H}_R(G,I) \simeq \mathcal{H}_R(G,\chi(q))$ (see § 1.4 and Paragraph 2.1.1).

B) We suppose now $\chi(q) \neq \chi(q)s$ regular . We compute the right action of $E_{ts}, E_{st} \in \mathcal{H}_R(G,\chi(q))$ on $f_{BI,\chi}$.

From (A.1) we deduce

$$\begin{gathered} ItsI = \bigcup_{x\in A_1} Its\begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix}, \\ IstI = \bigcup_{x\in A_1} Ist\begin{pmatrix} 1 & 0 \\ p_F x & 1 \end{pmatrix} = \bigcup_{x\in A_1} I\begin{pmatrix} 1 & 0 \\ x & 1 \end{pmatrix} st. \end{gathered} \tag{A.14}$$

Applying the formula (A.10) we get

$$f_{BI,\chi} * E_{ts}(1) = \sum_{x\in A_1} f_{BI,\chi}\left(\left(ts\begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix}\right)^{-1}\right) = \sum_{x\in A_1} f_{BI,\chi}\left(\begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix}(ts)^{-1}\right) = q\chi(ts)^{-1},$$

$$f_{BI,\chi} * E_{st}(1) = \sum_{x\in A_1} f_{BI,\chi}\left(\left(\begin{pmatrix} 1 & 0 \\ x & 1 \end{pmatrix}st\right)^{-1}\right) = \chi(st)^{-1}\sum_{x\in A_1} f_{BI,\chi}\begin{pmatrix} 1 & 0 \\ x & 1 \end{pmatrix} = \chi(st)^{-1}$$

as (A.12) is valid in general and in the regular case

$$\chi(q)\begin{pmatrix} u & 1 \\ 0 & -1/u \end{pmatrix} = (\chi_1/\chi_2)(u)\chi_2(-1)$$

for two distinct R-characters $\chi_1 \neq \chi_2$ of $\mathbf{F}_q^*$.

The character given by the action of $\mathcal{H}_R(G,\chi(q))$ on $Rf_{BI,\chi}$ sends (T^2, E_{ts}, E_{st}) on

$$(\chi(p_F I_2)^{-1}, q\chi(ts)^{-1}, \chi(st)^{-1}).$$

A.6 Principal representations of $G(q)$

The Frobenius $x \to x^p$ induces an automorphism of $M_2(\mathbf{F}_q)$:

$$\mathrm{Fr}\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} a^p & b^p \\ c^p & d^p \end{pmatrix}$$

for $a,b,c,d \in \mathbf{F}_q$. We denote by $U(q)$ the unipotent radical of the upper triangular subgroup $B(q)$ of $G(q) := GL(2,\mathbf{F}_q)$ and by $\det : G(q) \to \mathbf{F}_q^*$ the determinant. The irreducible $\overline{\mathbf{F}}_p$-representations of $G(q)$ were computed by Brauer and Nesbitt in 1937. They are the scalar extensions of the irreducible rational representations of $G(q)$.

https://doi.org/10.1112/S0010437X03000071 Published online by Cambridge University Press

Assertion A.1 [BL94]. The irreducible rational representations of $G(q)$ are

$$\rho_{x,y} = \det{}^x \otimes Sym_y, \quad Sym_y := \otimes_{k=0}^{f-1} Sym^{y_k} \operatorname{Fr}^k$$

for a unique integer x modulo $q-1$ and a unique integer $0 \leqslant y \leqslant q-1$, where $0 \leqslant y_o, \dots, y_{f-1} \leqslant p-1$ are the integers given by the p-adic expansion

$$y = y_o + y_1 p + \cdots + y_{f-1} p^{f-1}.$$

The representations Sym^n of $G(q)$ for $0 \leqslant n \leqslant p-1$ are realized in the space of polynomials homogeneous of degree n over $\mathbf{F}_q$:

$$Sym^n \begin{pmatrix} a & b \\ c & d \end{pmatrix} (X^{n-r} Y^r) = (aX + cY)^{n-r} (bX + dY)^r$$

for $a, b, c, d \in \mathbf{F}_q, ad - bc \neq 0$ and $0 \leqslant r \leqslant n$.

The $U(q)$-invariants $\rho_{x,y}^{U(q)}$ and the $U(q)$-coinvariants $\rho_{x,y_{U(q)}}$ have dimension equal to 1; the split torus $T(q)$ acts on the $U(q)$-invariants $\rho_{x,y}^{U(q)}$ by the character

$$\chi_{x,y} \begin{pmatrix} a & 0 \\ 0 & d \end{pmatrix} = (ad)^x a^y,$$

and on the $U(q)$-coinvariants $\rho_{x,y_{U(q)}}$ by the character $\chi_{x,y} s$. The character $\chi_{x,y}$ is regular iff $1 \leqslant y \leqslant q-2$, then $\chi_{x,y} s = \chi_{x',y'},\ x' \equiv x + y,\ y' = q - 1 - y$.

We consider now any field R containing $\mathbf{F}_q$ and the principal R-representations $\operatorname{ind}_{B(q)}^{G(q)} \chi$ of $G(q)$ associated to any R-character χ of the torus $T(q)$. The character χ can be written $\chi_{x,y}$ as above. When χ is regular, the pair (x, y) is unique. The following proposition is the finite analogue of the local Proposition 2.1, the Iwahori I and the pro-p-Iwahori $I(1)$ being the local analogues of the finite groups $B(q)$ and $U(q)$.

Proposition A.2.

a) *The dimension* $\dim_R \operatorname{Hom}_{RG(q)}(\operatorname{ind}_{B(q)}^{G(q)} \chi', \operatorname{ind}_{B(q)}^{G(q)} \chi)$ *is equal to*
  - 0 *if* χ', χ *are not* S_2*-conjugate;*
  - 1 *if* χ', χ *are conjugate and* χ *non-regular;*
  - 2 *if* $\chi' = \chi$ *is regular.*

b) $\operatorname{ind}_{B(q)}^{G(q)} 1$ *is the direct sum of the trivial representation and of the Steinberg representation which is irreducible.*

c) *In the regular case* $\chi \neq \chi s$*, the principal representation* $\operatorname{ind}_{B(q)}^{G(q)} \chi$
  - i) *admits a unique irreducible quotient* $V(\chi)$*, and* $V(\chi_{x,y}) \simeq \rho_{x,y}$*;*
  - ii) *admits a unique irreducible subrepresentation isomorphic to* $V(\chi s)$*;*
  - iii) *is of length* $\geqslant 2$*, and of length* 2 *for any* χ *if and only if* $q = p$*.*

Proof. We recall the well known adjunctions: for any $V \in \operatorname{Mod}_R G(q)$

$$\operatorname{Hom}_{RG(q)}(\operatorname{ind}_{B(q)}^{G(q)} \chi, V) = \operatorname{Hom}_{RT(q)}(\chi, V^{U(q)}),$$

$$\operatorname{Hom}_{RG(q)}(V, \operatorname{ind}_{B(q)}^{G(q)} \chi) = \operatorname{Hom}_{RT(q)}(V_{U(q)}, \chi).$$

From the disjoint union

$$G(q) = B(q) \cup B(q) s B(q)$$

we have $(\operatorname{ind}_{B(q)}^{G(q)} \chi)^{U(q)} \simeq \chi \oplus \chi s$ and by adjunction we have

$$\operatorname{Hom}_{RG(q)}(\operatorname{ind}_{B(q)}^{G(q)} \chi', \operatorname{ind}_{B(q)}^{G(q)} \chi) \simeq \operatorname{Hom}_{RT(q)}(\chi', \chi \oplus \chi s),$$

https://doi.org/10.1112/S0010437X03000071 Published online by Cambridge University Press

from which part a follows. The irreducibility of the Steinberg representation is all that we need to get part b, thanks to part a. This is proved as in the local case (§ 4.4).

The properties i and ii of part c result from Assertion A.1 by adjunction. The simple representations $\rho_{x,y} = V(\chi_{x,y})$ and $\rho_{x',y'} = V(\chi_{x,y}s)$ are never isomorphic by the classification of Assertion A.1, and hence the length of $\operatorname{ind}_{B(q)}^{G(q)} \chi_{x,y}$ is at least 2 and is equal to 2 iff $\dim \rho_{x,y} + \dim \rho_{x',y'} = \dim \operatorname{ind}_{B(q)}^{G(q)} \chi_{x,y}$. Writing $q = p^f$ the dimensions are

$$\dim \rho_{x,y} = \prod_{k=0}^{f-1} (y_k + 1), \quad \dim \rho_{x',y'} = \prod_{k=0}^{f-1} (p - y_k), \quad \dim \operatorname{ind}_{B(q)}^{G(q)} \chi_{x,y} = p^f + 1.$$

Clearly when $f = 1$ we have $\dim \rho_{x,y} + \dim \rho_{x',y'} = \dim \operatorname{ind}_{B(q)}^{G(q)} \chi_{x,y} = p + 1$. When $f > 1$ there is always some integer $1 \leqslant y \leqslant q - 2$ such that the sum $\prod_{k=0}^{f-1}(y_k + 1) + \prod_{k=0}^{f-1}(p - y_k)$ is not equal to $p^f + 1$; take for example $y = 1$ then $y_o = 1$ and $y_k = 0$ for all $1 \leqslant k \leqslant f - 1$ and $\dim \rho_{x,y} = 2, \dim \rho_{x',y'} = (p - 1)p^{f-1}$ but $2 + (p - 1)p^{f-1} < p^f + 1$. We have proved property iii of part c. □

A.7 Iwahori decomposition

Notations are as § A.1. We suppose that (K, σ) has an Iwahori decomposition, i.e. there are closed subgroups $M, N, \overline{N}, P = MN, \overline{P} = M\overline{N}$ of G with $N, \overline{N}$ normalized by $M = P \cap \overline{P}$ such that

$$K = K^- K^o K^+ = K^+ K^o K^-, \tag{A.15}$$

where $K^- := K \cap \overline{N}, K^o := K \cap M, K^+ := K \cap N$, and σ is trivial on K^- and on K^+. An element $h \in G$ contracts K^+, normalizes K^o, dilates K^- when

$$hK^+h^{-1} \subset K^+, \quad hK^oh^{-1} = K^o, \quad hK^-h^{-1} \supset K^-. \tag{A.16}$$

The set of such elements is stable by multiplication and forms a semi-group H.

1) In the Hecke algebra $\mathcal{H}_R(G, \sigma)$,

$$[KhK, F] * [Kh'K, F'] = [Khh'K, FF'] \tag{A.17}$$

for $h, h' \in H$ and $F \in \mathcal{I}_h, F' \in \mathcal{I}_{h'}$. This results from Example II of § A.1 and from:

i) $KhKh'K = Khh'K$, indeed $hKh' = h(K^+K^o)h^{-1}hh'h'^{-1}K^-h' \subset Khh'K$;

ii) $h^{-1}KhK \cap h'Kh'^{-1}K = K$, indeed we can write the left hand side as $h^{-1}K^+hK \cap h'K^-h'^{-1}K$ which is clearly contained in

$$NK \cap \overline{N}K = K. \tag{A.18}$$

The next two properties are used in [SS91, § 4] when $G = GL(n, F)$.

2) Let C be a subgroup of G such that $K \subset C,\ P \cap C = P \cap K$.
Then the relation $PKhc \cap PKh \neq \emptyset$ with $(h, c) \in (H \cap P) \times C$ implies $Khc = Kh$.
One shows first that the relation implies $c \in K$.
As $PK = PK^-,\ PKh = Phh^{-1}K^-h = Ph^{-1}K^-h$, the relation is equivalent to $k_1ck_2 \in P$ for some $(k_1, k_2) \in (h^{-1}K^-h)^2$. As $h^{-1}K^-h \subset K^- \subset C$, we deduce that $k_1ck_2 \in P \cap C = K^oK^+$ and $c \in K$.
Write $c = k^+k^ok^-$ in the Iwahori decomposition of K. Then $Khc = Khk^-$ and $PKhc = PKhk^-$. The relation is equivalent to $k_1'k^-k_2' \in P$ for some $(k_1', k_2') \in (h^{-1}K^-h)^2$. As $P \cap K^- = \{1\}$, we get $k^- \in h^{-1}K^-h$ hence $Khc = Kh$.

3) Let C' be a subgroup of G with *the Iwasawa decomposition*: $G = PC'$ and let $h_o \in H \cap P$ with h_o^{-1} *strongly contracting* $\overline{N}$: the groups $h_o^{-n}K^-h_o^n$ for $n \gg 0$ form a fundamental system of

https://doi.org/10.1112/S0010437X03000071 Published online by Cambridge University Press

neighborhoods of 1 in $\overline{N}$. The cosets $P\backslash PKh_o^n = P\backslash P(h_o^{-n}K^-h_o^n)$ form a fundamental system of neighborhoods of the trivial coset. The cosets $P\backslash PKh_o^n g$ form a fundamental system of neighborhoods of the coset $P\backslash Pg$, for any $g \in G$.

Any compact of $P\backslash G$ is a finite disjoint union of $P\backslash PKh_o^n c$ where $n \gg 0$ and $c \in C'$.

References

BL95 L. Barthel and R. Livne, *Modular representations of GL_2 of a local field: the ordinary, unramified case*, J. Number Theory **55** (1995), 1–27.

BL94 L. Barthel and R. Livne, *Irreducible modular representations of GL_2 of a local field*, Duke Math. J. **75** (1994), 261–292.

Bre01 C. Breuil, *Sur quelques représentations modulaires et p-adiques de $GL_2(\mathbf{Q}_p)$*, Prépublication 2001-35, Université de Paris-Sud.

Dat99 J.-F. Dat, *Types et inductions pour les représentations modulaires des groupes p-adiques. With an appendix by Marie-France Vignéras*, Ann. Sci. École Norm. Sup. (4) **32** (1999), 1–38.

IR90 K. Ireland and M. Rosen, *A classical introduction to modern number theory*, 2nd edn, Graduate Texts in Mathematics, vol. 84 (Springer-Verlag, Berlin, 1990).

SS91 P. Schneider and U. Stuhler, *The cohomology of p-adic symmetric spaces*, Invent. Math. **105** (1991), 47–122.

Vig96 M.-F. Vignéras, *Représentations ℓ-modulaires d'un groupe réductif p-adique*, Prog. Math., vol. 137 (Birkhäuser, Basel, 1996).

Vig97 M.-F. Vignéras, *A propos d'une conjecture de Langlands modulaire*, in *Finite reductive groups*, ed M. Cabanes, Prog. Math. vol. 141, (Birkhäuser, Basel, 1997), 415–452.

Marie-France Vignéras vigneras@math.jussieu.fr
Université de Paris 7 – Denis Diderot, Institut de Mathématiques de Jussieu, 175/179 rue du Chevaleret, Paris 75013, France

https://doi.org/10.1112/S0010437X03000071 Published online by Cambridge University Press