p-adic integral structures of some representations of $GL(2,F)$

Marie-France Vignéras

Abstract. Let F be a local non archimedean field of residue field $\mathbf{F}_q$. We show that if V is a smooth $\overline{\mathbf{Q}}_p$-representation of $G = GL(2,F)/p_F^{\mathbf{Z}}$ generated by the space $V^{I(1)}$ of its pro-p-Iwahori invariant vectors, then a p-adic integral structure of the $\mathcal{H}(G, I(1))$-module $V^{I(1)}$ generates a p-adic integral structure of the representation V of G, under a certain condition on the Gauss sums of the non trivial characters μ of $\mathbf{F}_q^*$ (embedded in $I/I(1)$ via $x \to \mathrm{diag}(x, x^{-1})$) appearing in $V^{I(1)}$. When $q = p$, the condition is equivalent to μ not quadratic if $p \equiv 1 (\mathrm{mod}\, 4)$.

1. Introduction

1.1. Let p be a prime number, F a local non archimedean field with a finite residual field $\mathbf{F}_q$ of characteristic p. The complex smooth representations of the group G of F-points of a connected reductive F-group are reasonably well understood, but the p-adic integral structures are not. One constructs easily a p-adic integral structure for a principal series induced from a p-adic integral character, or for a Steinberg, or for a supercuspidal irreducible representation of G. There are two basic open problems. The first one is that supercuspidal representations may have p-adic integral structures which are not commensurable, but we will not consider this problem here. The second problem concerns the principal series not induced by p-adic integral characters, which are locally p-adic integral (the non zero space of invariants by some open compact subgroup K has a p-adic integral structure stable by the Hecke $\mathbf{Z}$-algebra of K): do they admit a p-adic integral structure ? Even when $G = GL(2,F)$, the answer is not known. The absence of a p-integral Haar measure on G is the main difficulty.

For some irreducible locally algebraic representations of $GL(2,\mathbf{Q}_p)$, Breuil, Berger-Breuil, Colmez constructed a p-adic integral structure, from the (ϕ,Γ)-module associated by Fontaine to the associated p-adic Galois representation.

This method is very deep but one should not need Galois (ϕ, Γ)-modules to construct p-adic integral structures for G ! There should exist a theory of p-adic integral structures in the framework of representations of reductive p-adic groups. When $\ell \neq p$, the equivalence of categories between the complex representations generated by their vectors invariant by the pro-p-Iwahori group $I(1)$ and the right complex modules of the pro-p-Iwahori Hecke complex algebra $H_{\mathbf{C}}^{(1)}$, can be used to transfer ℓ-integral $H^{(1)}$-structures (which poses no problem even for $\ell = p$) to ℓ-integral G-structures. Can one replace ℓ by p ? We concentrate here only on the simplest case $GL(2, F)$ which can be easily reduced to $G := GL(2, F)/p_F^{\mathbf{Z}}$, when p_F is a generator of the maximal ideal of the integer ring O_F. We will show that there is a transfer of p-integral structure from a "part" of $H_{\mathbf{C}}^{(1)}$ to G.

Let (E, O_E, k_E) be a a finite extension of $\mathbf{Q}_p$ which contains $\mu_{p(q-1)}$ and $\sqrt{q}$, its ring of integers, its residue field.

For any commutative ring R, the pro-p-Iwahori R-algebra is the scalar extension $H_R^{(1)} = R \otimes_{\mathbf{Z}} H^{(1)}$ where $H^{(1)} = \mathrm{End}_{\mathbf{Z}G}\, \mathbf{Z}[G/I(1)]$.

We say that a commutative ring R contains μ_m when m is an integer ≥ 1 and $X^m - 1$ has m distinct roots in R.

Let V be a smooth E-representation of G. An O_E-integral structure L of V is a G-stable free O_E-submodule which contains a E-basis of V.

Let W be a right $H_E^{(1)}$-module. An O_E-integral structure M of W is a $H^{(1)}$-stable free O_E-submodule which contains a E-basis of W.

If L is an O_E-integral structure of V, then $L^{I(1)}$ is an O_E-integral stucture of the right $H_E^{(1)}$-module $V^{I(1)}$.

The group $\mathbf{F}_q^*$ embeds diagonally in the Iwahori group I via the Teichmüller morphism $\mathbf{F}_q^* \to O_F^*$ and $x \to \mathrm{diag}(x, x^{-1})$.

We consider for $y \in \mathbf{F}_q$, and for a complex character $\mu : \mathbf{F}_q^* \to E^*$, the Gauss sum

$$G_q(y, \mu) := \sum_{x \in \mathbf{F}_q^*} \mu(x) e(xy), \quad e(x) := e^{2i\pi tr(x)/p}. \tag{1}$$

where $tr : \mathbf{F}_q \to \mathbf{F}_p$ is the trace. $G_q(0, \mu) = 0$ if $\mu \neq \mathrm{id}$ is not trivial and $G(0, \mathrm{id}) = q - 1, G(y, \mathrm{id}) = -1$ if $y \neq 0$.

Definition 1.1. *Let $\mathcal{F}$ be the set of characters μ of $\mathbf{F}_q^*$ of such that*

$$G_q(y, \mu) \pm \sqrt{q} \neq 0$$

for all $y \in \mathbf{F}_q^*$ if $p \neq 2$. If $q = 4$ we replace $\pm$ by $+$. If $p = 2, q \neq 4$ we fix any sign ε and we replace $\pm$ by ε.

When $p = q$, the set $\mathcal{F}$ is equal to the set of all characters of $\mathbf{F}_p^*$ when $p = 2$ or $p \equiv 3 \pmod 4$. When $q = p \equiv 1 \pmod 4$ only the non trivial quadratic character is missing.

The set $\mathcal{F}$ is stable by $\mu \to \mu^{-1}$ and not empty because it contains the trivial character and the characters of order $q-1$. There is a central idempotent $e_{\mathcal{F}}$ in the abelian category of E-representations V of G generated by their $I(1)$-invariant vectors, such that $V = e_{\mathcal{F}}V$ if and only if the eigenvalues of $\mathbf{F}_q^*$ acting on $V^{I(1)}$ belong to $\mathcal{F}$. The group $\mathbf{F}_q^*$ acts trivially if and only if $V^{I(1)} = V^I$.

Theorem 1.2. *Let V be a smooth E-representation of G generated by its $I(1)$-invariant vectors, such that $e_{\mathcal{F}}V = V$. If M is an O_E-integral stucture of $V^{I(1)}$, then the $O_E G$-submodule L of V generated by M is O_E-free, isomorphic to the quotient of $M \otimes_{H^{(1)}_{O_E}} O_E[I(1)\backslash G]$ by its torsion.*

The only difficulty is the O_E-freeness of L. The theorem is easier when V is generated by its vectors invariant by the Iwahori group I. In this case, the O_E-module $M \otimes_{H_{O_E}} O_E[I\backslash G]$ has no torsion. As we do not treat a general open compact subgroup, why do we worry for a pro-p-Iwahori group? The reason is that a pro-p-Iwahori group $I(1)$ is the analogue of a pro-p-Sylow of $GL(2,F)$.

1.2. The O_E-freeness of L is deduced from the structure of the Iwahori universal module $R[I(1)\backslash G]$ over a commutative ring R as a $H^{(1)}_R$-module. This information can be found with the tree of $SL(2,F)$. The tree is perfectly adapted to the Iwahori group because the oriented edges are in bijection with the classes $I\backslash G$. The Iwahori Hecke R-algebra H_R is generated by two elements T, S satisfying $T^2 = 1, (S+1)(S-q) = 0$ where q is the order of the residual field of F [**9**].

Theorem 1.3. *Let R be a commutative ring where $q+1$ is invertible. There exists a subset X in $I\backslash G$ containing the trivial class e_o such that the map $(h_x)_{x\in X} \to \sum h_x x$ is an isomorphism*

$$H_R(S+1) \oplus_{x\in X - e_o} H_R(S-q) \simeq R[I\backslash G].$$

When R is also principal, this implies that the functor

$$? \to ? \otimes_{H_R} R[I\backslash G]$$

from right H_R-modules to RG-modules, respects R-freeness.

The pro-p-Iwahori universal module $R[I(1)\backslash G]$ as a $H^{(1)}_R$-module is not so simple. We suppose that q is a nonzerodivisor in R, which is not a problem when R is a p-adic ring but forbids R to be a characteristic p field. The Iwahori group is the semi-direct product of the pro-p-Iwahori subgroup and of a finite two dimensional torus μ^2_{q-1}. When $q = 2$ we have $I = I(1)$, hence we suppose now $q \geq 3$.

Definition 1.4. *Let $\mathcal{F}^{reg}$ be the set of non trivial complex characters of $\mathbf{F}_q^*$. Let d be the smallest positive integer such that*

$$d \prod_{y\in\mathbf{F}_q,\mu\in\mathcal{F}^{reg}} (G_q(y,\mu)\pm\sqrt{q})^{-1}$$

is algebraically integral, if $p\neq 2$. If $p=2$ we replace $\pm$ by $+$ if $q=4$ and by any fixed sign ε.

d is divisible by q because $G_q(0,\mu)=0$ when μ is not trivial.

We say that a $\mathbf{Z}$-module M is annihilated by $2d^\infty$ if for any non zero $m\in M$ we have $2d^{n+1}m=0$ for some integer $n\geq 0$.

When R is a commutative ring R which contains μ_{q-1}, the central idempotent $e_{\mathcal{F}}$ identifies naturally to an element of $R[I/I(1)]$ central in $H_R^{(1)}$.

In the next theorem, X is the same set of outward edges than in the theorem 1.3.

Theorem 1.5. *Let R be a commutative ring which contains $\mu_{p(q-1)}$ and a square root of q, where q^2-1 is invertible and $2d$ is a nonzerodivisor. Then, there is an injective map $X\to I(1)\backslash G$ and two elements $a,b\in R[I/I(1)]$ central in $H_R^{(1)}$, such that such that the map $(h_x)_{x\in X}\to\sum h_x x$*

$$e_{\mathcal{F}}H_R^{(1)}(S+a)\oplus_{x\in X-e_o} e_{\mathcal{F}}H_R^{(1)}(S-b)\to e_{\mathcal{F}}R[I(1)\backslash G]$$

is injective and of cokernel annihilated by $2d^\infty$.

When R is also local principal complete, this implies that the functor

$$?\to(?\otimes_{H_R} R[I(1)\backslash G])/\text{torsion}$$

from right $e_{\mathcal{F}}H_R^{(1)}$-modules to RG-modules, respects R-freeness.

1.3. These results where found and written while the author was a fellow at the Radcliffe Institute of Advanced Study at Harvard University in the fall of 2005, benefiting of excellent conditions and of enriching contacts with fellows working in a broad range of academic disciplines or creative arts. The key theorems 1.3, 1.5 are inspired by the results of Rachel Ollivier on the flatness of the pro-p-Iwahori universal $\overline{\mathbf{F}}_p$-module over the pro-p-Iwahori Hecke algebra. The author is very grateful to Vytautas Paskunas for preventing an embarassing mistake, to Alberto Arabia, Jean-Pierre Serre, Don Zagier for amical advice, to William Stein for his help with magma, to Dick Gross, Barry Mazur, and Richard Taylor for their invitation to the Harvard mathematical department, to the mathematicians of M.I.T., Boston University, and Brandeis for inviting the author to give talks on this subject.

2. Preliminaries

2.1. Let G be the group of F-points of a connected reductive group. If K is an open compact subgroup of G, the Hecke ring of K in G is $H(G,K) := \mathrm{End}_{\mathbf{Z}G}\,\mathbf{Z}[G/K)]$, the Hecke R-algebra of K in G is $H_R(G,K) := R\otimes_{\mathbf{Z}} H(G,K)$, for any commutative ring R.

Proposition 2.1. *Let E be a field of characteristic different from p and K an open compact subgroup of G, of pro-order prime to the characteristic of E. Then the functor of K-invariants is an equivalence from the category of smooth E-representations of G generated by their vectors K-invariants to the category of right $H_E(G,K)$-modules, if the equivalence is true on some extension L of E.*

Proof. When the characteristic of E is different from p, there is an E-Haar measure on G, and a convolution Hecke algebra $H_E(G)$ of functions for an E-Haar measure. The Hecke algebra $H_E(G)$ acts on a smooth E-representation of G. The category of smooth E-representations of G is equivalent to the category of $H_E(G)$-modules V such that $H_E(G)V = V$; when the pro-order of K is prime to the characteristic of E, there is an idempotent $e \in H_E(G)$ such that $V^K = eV$ ([**9**] I.4.4); the algebra $eH_E(G)e$ is isomorphic to its opposite and to the Hecke algebra $H_E(G,K)$ of K in G ([**9**] I.3.2, I.3.4); the functor $V \to eV$ is an equivalence between the category of smooth E-representations V of G generated by eV and the category of left modules $eH_E(G)e$-modules M if any subrepresentation W of V is generated by eW for any V generated by eV; the inverse functor is $M \to H_E(G)e\otimes_{eH_E(G)e} M$ ([**9**] I.6.6); one can replace "if" by "if and only if" because an equivalence of category implies $\mathrm{Hom}_{EG}(W,V) \simeq \mathrm{Hom}_{eH_E(G)e}(eW, eV)$. When $E \subset L$ is an extension of fields and V is a smooth E-representation of G, then $V_L = L \otimes_E V$ is a smooth L-representation of G, one identifies $V, H_E(G)$ with their natural images in $V_L, H_L(G)$; one has $eV_L = (eV)_L$. If W is a subrepresentation of V, then W_L is a subrepresentation of V_L. Hence if the functor of K-invariants is an equivalence for L-representations, it is an equivalence for E-representations. □

Corollary 2.2. *The equivalence is true when $E \subset \mathbf{C}$ and K is an Iwahori subgroup I or a pro-p-Iwahori subgroup $I(1)$.*

In particular, the corollary applies when E is a finite extension of $\mathbf{Q}_p$.

Proof. The equivalence is true when E is isomorphic to a subfield of $\mathbf{C}$ by [**1**] corollary 3.9 because an Iwahori subgroup I and its pro-p-unipotent radical $I(1)$ are "bons" [**1**] 2.1 relatively to a maximal split torus of G by the theory of Bruhat-Tits [**11**] prop.1.25. □

More generally, The equivalence is true when the characteristic of E is *banal* (over an algebraic closure of E the only problem to extend the proof of [BD corollary 3.9] is the generic irreducibility of representations induced from an irreducible supercuspidal representation of a Levi subgroup; the generic irreducibility has been proved by Dat **[5]** prop.3.3). In the theory of types, one consider equivalence of categories induced by the functor $V \to V^{K,\sigma} := \mathrm{Hom}_K(\sigma, V)$ where σ is an irreducible representations of K; when σ is the trivial representation, $V^{K,\sigma} = V^K$; there is an analogue of the proposition 2.1 for (K, σ) when σ is not trivial.

2.2. The proof of the theorems 1.3 and 1.5 uses the following elementary lemma.

Lemma 2.3. *Let A be a commutative ring, M an A-module which is a direct sum of free A-modules M_j of finite rank n_j, and J the union of subsets J_j of $M(\leq j) := \sum_{k\leq j} M_k$ with n_j elements, for all $j \in \mathbf{N}$. If for all $j \in \mathbf{N}$,*

$$aM_j \subset \ M(\leq j-1) + \sum_{?\in J_j} A?$$

for some nonzerodivisor a in A, then the sum $N := \sum_{?\in J} A?$ is direct and the A-module quotient M/N is annihilated by a^∞.

An equivalent version is:

Lemma 2.4. *Let A be a commutative ring, M a free A-module of finite rank n, which is a direct factor of an A-module $P \oplus M$.*

1) n elements $(f_i)_{1\leq i\leq n}$ in M are linearly A-independent if and only if $aM \subset \sum_{i=1}^n Af_i$ for some nonzerodivisor $a \in A$.

2) Let $(\phi_i)_{1\leq i\leq n}$ be n elements in $P \oplus M$. Then the sum (with $n+1$ terms) $P + \sum_{1\leq i\leq n} A\phi_i$ is direct if and only if $aM \subset P + \sum_{i=1}^n A\phi_i$ for some nonzerodivisor $a \in A$.

Proof. 1) Let c be the determinant of the matrix $C \in M(n, A)$ giving the coefficients of $(f_i)_{1\leq i\leq n}$ on an A-basis $(e_i)_{1\leq i\leq n}$ of M. By the Cramer formula, $cM \subset \sum_{i=1}^n Af_i$.

If $aM \subset \sum_{i=1}^n Af_i$ for $a \in A$, there exist a matrix $D \in M(n, A)$ such that the determinant of CD is a^n. Hence c divises a^n If a is a nonzerodivisor, c is a nonzerodivisor.

$(f_i)_{1\leq i\leq n}$ are linearly independent if and only if c is a nonzerodivisor in A (**[3]** A III.95 Cor. 2).

2) One applies 1) to the components $(f_i)_{1\leq i\leq n}$ of $(\phi_i)_{1\leq i\leq n}$ in M. If the $(f_i)_{1\leq i\leq n}$ are linearly independent, then the $(\phi_i)_{1\leq i\leq n}$ are linearly indepen-

dent. The sum $P + \sum_{1\leq i\leq n} A\phi_i$ is direct if and only if the $(f_i)_{1\leq i\leq n}$ are linearly independent. □

2.3. Another elementary lemma will be also used.

Lemma 2.5. *Let $R[X]$ be the commutative R-algebra generated by X and the relation $(X+a)(X-b)=0$ where $a,b\in R$. Let M be a left $R[X]$-module. When $a+b$ is a nonzerovisisor on M, the natural map*

$$(X+a)M\oplus(X-b)M\to M$$

is injective of image containing $(a+b)M$. When $a+b$ is invertible on M, it is an isomorphism.

Proof. Let $m\in M$. The formula $(a+b)m=(X+a)m-\ (X-b)m$ shows that $(a+b)M$ is contained in the image. If $(X+a)m\in(X-b)M$ then $(a+b)m\in(X-b)M$ by the formula and $(a+b)(X+a)m=0$ because $(X+a)(X-b)=0$. If $a+b$ is a nonzerodivisor in R then $(X+a)m=0$, hence the map is injective. □

2.4. Notations.

Let $O_F, p_F, \mathbf{F}_q, \mu_{q-1}$ be the ring of integers of F, an uniformizer, the residual field of order q, the roots of unity of order prime to p in O_F, $K:=GL(2,O_F)$, I the Iwahori group, $G=GL(2,F)/p^{\mathbf{Z}}$.

$$I:=\{\begin{pmatrix}a&b\\p_Fc&d\end{pmatrix},\quad a,d\in O_F^*,\ b,c\in O_F\},\tag{2}$$

$I(1)$ the pro-p-Iwahori,

$$I(1):=\{\begin{pmatrix}a&b\\p_Fc&d\end{pmatrix}\in I,\ \ a-1,d-1\in p_FO_F\},\tag{3}$$

$$s:=\begin{pmatrix}0&1\\1&0\end{pmatrix},\ \ t:=\begin{pmatrix}0&1\\p_F&0\end{pmatrix},\ \ st=\begin{pmatrix}p_F&0\\0&1\end{pmatrix},\quad ts=\begin{pmatrix}1&0\\0&p_F\end{pmatrix}.\tag{4}$$

One identifies $\mathbf{F}_q$ with $0\cup\mu_{q-1}\subset O_F$, and for all $n\geq 1$, $\mathbf{F}_q^n$ with a system of representatives of $O_F/p_F^nO_F$ by the map

$$x=(x_n,\dots,x_1)\to a(x):=x_1+p_Fx_2+\dots p_F^{n-1}x_n.$$

One identifies O_F with subgroups of the pro-p-Iwahori via

$$u_x:=\begin{pmatrix}1&x\\0&1\end{pmatrix},\quad v_x:=\begin{pmatrix}1&0\\p_Fx&1\end{pmatrix}.\tag{5}$$

Any element of the Iwahori is equal to $v_x \operatorname{diag}(y, y') u_{x'}$ with unique $x, x' \in O_F$ $y, y' \in O_F^*$. One sets for $x = (x_n, \dots, x_1) \in \mathbf{F}_q^n$,

$$(6) \quad g_x^o := stv_{x_n} \dots stv_{x_2} su_{x_1} = g_{a(x);n} := \begin{pmatrix} 0 & p_F^{n-1} \\ 1 & a(x) \end{pmatrix}, \quad tg_x^o = \begin{pmatrix} 1 & a(x) \\ 0 & p_F^n \end{pmatrix},$$

$$(7) \quad g_x^1 := stv_{x_n} \dots stv_{x_1} = g_{a(x);n} := \begin{pmatrix} p_F^n & 0 \\ p_F a(x) & 1 \end{pmatrix}, \quad tg_x^1 = \begin{pmatrix} p_F a(x) & 1 \\ p_F^{n+1} & 0 \end{pmatrix}.$$

The element t normalizes I and $tv_x = u_x t,\ sv_x = u_{p_F x} s$, $su_{1/x} s = u_x \lambda_{-1} h_x s u_x$ if $x \neq 0$, where

$$(8) \qquad \lambda_x := \begin{pmatrix} x & 0 \\ 0 & 1 \end{pmatrix}, \quad h_x := \begin{pmatrix} x & 0 \\ 0 & 1/x \end{pmatrix}.$$

One has the disjoint decompositions

$$(9) \qquad IsI = \cup_{x \in \mathbf{F}_q} Isu_x, \quad IstI = \cup_{x \in \mathbf{F}_q} Istv_x, \quad ItsI = \cup_{x \in \mathbf{F}_q} Itsu_x.$$

One has the same decomposition for $I(1)$ [**9**].

2.5. The oriented edges of the tree of $SL(2, F)$ will appear often, because they are in canonical bijection with the classes $I\backslash G$ (read this as $Ip_F^{\mathbf{Z}}\backslash GL(2, F)$); the vertices are in canonical bijection with the classes $K\backslash G$ [**7**]. For any commutative ring R, the Iwahori universal R-module $R[I\backslash G]$ identifies with the free R-module generated by the oriented edges e of the tree

$$R[I\backslash G] = \oplus_e Re.$$

The commuting right action of G and left action of the Hecke Iwahori ring

$$H := \operatorname{End}_{\mathbf{Z}G} \mathbf{Z}[I\backslash G]$$

on $\mathbf{Z}[I\backslash G]$ on the Iwahori universal module $\mathbf{Z}[I\backslash G]$, translate to a right action of $g \in G$ on $\oplus_e \mathbf{Z}e,\ e \to eg$ permuting the oriented edges e, and of two linear operators T, S where T reverses the orientation, and S sends an oriented edge e to the sum of the q oriented edges different from e but with the same origin.

We denote by $e_o = (v^o, v^1)$ the oriented edge corresponding to I, with origin the vertex v^o corresponding to $K = GL(2, O_F)$ and end the vertex v^1 corresponding to Kt. The image of e_o by T is the opposite edge

$$(10) \qquad Te_o = (v^1, v^o) = e_o t.$$

The image of e_o by S is the sum σ_o of the outward q oriented edges $e_x^o = (v^o, v_x^o)$ different from e_o with origin v^o,

$$(11) \qquad Se_o = \sigma_o := \sum_{x \in \mathbf{F}_q} e_x^o, \quad e_x^o = e_o g_x^o, \quad g_x^o = su_x = \begin{pmatrix} 0 & 1 \\ 1 & x \end{pmatrix}.$$

The Iwahori Hecke ring H is identified with the convolution ring of double classes modulo I, and T, S correspond to ItI, IsI. Using that the action of S commutes with G, one sees that

$$S\sigma_o = qe_o + (q-1)\sigma_o. \tag{12}$$

One deduces immmediately the keys relations:

$$(S+1)(S-q)e_o = 0, \quad (q+1)e_o = (S+1)e_o + (q-1)\sigma_o. \tag{13}$$

The ring H is $\mathbf{Z}$-free of basis $(ST)^k, (ST)^k S, (TS)^k, (TS)^k T$ for $k \geq 0$ (this is well known, can be deduced from (15) given later), generated by S, T satisfying the relations

$$T^2 = 1,\ (S+1)(S-q) = 0. \tag{14}$$

2.6. Our arguments will use induction on the distance on the tree. The $q+1$ vertices v^1, v^o_x for $x \in \mathbf{F}_q$, adjacent to v^o, form the sphere $S(1)$ of vertices centered in v^o of radius 1, and

$$E(0) := \{e_o, e^o_x, \quad x \in \mathbf{F}_q\}$$

is the set of outward edges relating v^o to $S(1)$. The image of $e_o = (v^o, v^1)$ by ST is the sum of the q outward edges $e^1_x = (v^1, v^1_x)$ of origin v^1

$$STe_o = \sum_{x\in\mathbf{F}_q} e^1_x, \quad e^1_x = e_o g^1_x, \quad g^1_x = stv_x = \begin{pmatrix} p_F & 0 \\ p_F x & 1 \end{pmatrix}. \tag{15}$$

because $IsItI = IstI = \cup_{x\in\mathbf{F}_q} Istv_x$ by the equation (9). By transitivity of the action of G, the image of $e_o g$ by ST is the sum $\sum_{?\in\mathbf{F}_q} e_o stv_? g$ of the q outward edges of origin $v^1 g$. In particular for $g = su_x,\ x \in \mathbf{F}_q$,

$$STe^o_x = \sum_{y\in\mathbf{F}_q} e^o_{y,x}, \quad e^o_{y,x} := (v^o_x, v^o_{y,x}) = Ig^o_{y,x}, \quad g^o_{y,x} = stv_y su_x, \quad v^o_x = Ktsu_x.$$

By induction for $n \geq 1$, the sphere $S(n+1)$ centered in v^o of radius n is $S(n+1) = \{v^o_{x_{n+1},\dots,x_1}, \quad v^1_{x_n,\dots,x_1}, \quad x_n, \dots, x_1 \in \mathbf{F}_q\}$, i.e.

$$S(n+1) = \{v^\varepsilon_x = v^1 g^\varepsilon_x,\ \varepsilon \in \{0,1\},\ x \in \mathbf{F}_q^{n+1-\varepsilon}\}, \tag{16}$$

and $E(n) = \{e^o_{x_{n+1},\dots,x_1}, \quad e^1_{x_n,\dots,x_1}, \quad x_{n+1}, \dots, x_1 \in \mathbf{F}_q\}$ where

$$e^o_{x_{n+1},\dots,x_1} = (v^o_{x_n,\dots,x_1}, v^o_{x_{n+1},\dots,x_1}), \quad e^1_{x_n,\dots,x_1} := (v^1_{x_{n-1},\dots,x_1}, v^1_{x_n,\dots,x_1}),$$

is the set of oriented edges relating the vertices of $S(n)$ with the adjacent vertices of $S(n+1)$, i.e.

$$E(n) = \{e^\varepsilon_x = e_o g^\varepsilon_x,\ \varepsilon \in \{0,1\},\ x \in \mathbf{F}_q^{n+1-\varepsilon}\}. \tag{17}$$

We will use the notations $?(\leq n) := ?(0) \cup \ldots \cup ?(n)$, and $? = \cup_{n\geq 0} ?(n)$. The set of outward edges is $E := \cup_{n\geq 0} E(n)$.

2.7. A system of representatives of the classes $I\backslash G$ will be used to have a section of the natural surjective map $I(1)\backslash G \to I\backslash G$.

Lemma 2.6. *A system of representatives of the classes $I\backslash G$ is*

$$\mathcal{E} := \{1, g_x^\varepsilon, t, tg_x^\varepsilon, \quad \text{for } \varepsilon \in \{0,1\}, x \in \mathbf{F}_q^n, n \in \mathbf{N} - \{0\}\}. \tag{18}$$

They correspond to the outward edges e_o, e_x^ε and the inward edges Te_o, Te_x^ε.

A system of representatives of the classes $K\backslash G$ is

$$1, t, tg_x^\varepsilon, \quad \text{for } \varepsilon \in \{0,1\}, x \in \mathbf{F}_q^n, n \in \mathbf{N} - \{0\}. \tag{19}$$

They correspond to the vertices $v^o, v^1, v_x^\varepsilon$.

The unique oriented edge e^v ending by the vertex $v = v_x^\varepsilon$ is the outward edge e_x^ε, and the set of outward edges of origin v is

$$E_v := \{e_{y,x}^\varepsilon, y \in \mathbf{F}_q\}.$$

By (15), ST sends an outward edge e to the sum of the q outward edges starting from the end of e,

$$STe^v = \sigma_v := \sum_{e\in E_v} e. \tag{20}$$

2.8. We choose a set D of distinguished outward half lines in the tree having the property: no oriented edge starting from the origin v^o belongs to a distinguished line, for any vertex $v \neq v^o$ there is a unique outward edge z_v with origin v belonging to a distinguished line.

Definition of D. A vertex v is the origin of a distinguished half line $D_v \in D$ if and only if $v \in S(1)$, or $v = v_x^\varepsilon$ and $x = (x_n, \ldots, x_1)$ has the property that $x_n \neq 0$. The vertex v_1 on the distinguished line D_v adjacent to v is v_o^1 if $v = v^1$ and $v_{o,x}^\varepsilon$ if $v = v_x^\varepsilon$. By induction for $k \geq 1$, the vertex $v_{k+1} \in D_v$ adjacent to $v_k = v_?^\varepsilon$ is $v_{k+1} = v_{o,?}^\varepsilon$.

Let X be the complementary set of D in E. We extend to X the notations given for E, for example $X_{v^o} = X(0) = E_{v^o} = E(0)$, $X_v = E_v - z_v$, $X(n) = E(n) \cap X$.

By (20), we have:

Lemma 2.7. *When v is not the origin, a basis of the $\mathbf{Z}$-module $\mathbf{Z}E_v$ generated by the outward edges starting from v is (STe^v, X_v).*

3. Iwahori universal module

We prove the theorems on the Iwahori universal module and their applications to the integral structures of representations generated by their Iwahori invariant vectors.

We give a basis of the Iwahori universal module, compatible with the orientation, the distance to the origin and stable by T.

Proposition 3.1. *1) A basis of* $\oplus_{e\in E(\leq n)} \mathbf{Z}e$ *is* $(ST)^k x$ *for all* $x \in X(r), k \geq 0, r+k \leq n$.

2) A basis of $\oplus_{e\in TE(\leq n)} \mathbf{Z}e$ *is* $(TS)^k Tx$ *for all* $x \in X(r), k \geq 0, k+r \leq n$

3) A basis of the Iwahori universal $\mathbf{Z}$*-module* $\mathbf{Z}[I\backslash G]$ *is* $(ST)^k x, T(ST)^k x$ *for all* $x \in X, k \geq 0$.

Proof. 1) For $Y \subset \mathbf{Z}[I\backslash G]$ we set $\mathbf{Z}Y := \sum_{?\in Y} \mathbf{Z}?$. We prove 1) by induction on n. By definition $X(0) = E(0)$ is a basis of $\mathbf{Z}E(0)$. We suppose 1) true for $n-1$. We have $STE(?) \subset \mathbf{Z}E(?+1)$ for any integer $? \in \mathbf{N}$. The set $E(n)$ is contained in $STE(\leq n-1) + \sum \mathbf{Z}(n)$, because STe^v, X_v is a basis of $\mathbf{Z}E_v$ for any $v \in S(n)$ and $e^v \in E(n-1)$, by the lemma (2.7). This implies 1) for n (a particular case of the lemma 2.3).

2) and 3) are immediate consequences of 1).

□

We give now a second basis of the Iwahori universal R-module, stable by S, T, compatible with the the distance, but not with the orientation (the stability by S is incompatible with the comaptibility with the orientation).

Let $J(0) := \{(S+1)e_o, (S-q)e \text{ for } e \in E(0) - e_o\}$, for any integer $n \geq 1$ let $J(n) := \{(S-q)e \text{ for } e \in X(n)\}$. Set J for the union of $J(n)$ for $n \geq 0$ and $\mathbf{Z}E(\leq -1) := \{0\}$.

Lemma 3.2. *We have* $(q+1)E(n) \subset \mathbf{Z}[T]E(\leq n-1) + \mathbf{Z}J(n)$ *for any integer* $n \geq 0$.

Proof. We have the system of $q+1$ equations:

$$(S+1)e_o = e_o + \sigma_o, \tag{21}$$

$$(S-q)e = -(q+1)e + e_o + \sigma_o \tag{22}$$

for $e \in E(0) - e_o$. When n is an integer $n \geq 1$ and v is a vertex in $S(n)$, we have the system of q equations:

$$STe^v = \sigma_v \tag{23}$$

$$(S-q)x - Te^v = -(q+1)x + \sigma_v. \tag{24}$$

for $x \in X_v = E_v - z_v$. These two systems can be inverted:

$$(q+1)e_o = (S+1)e_o + (S-q)\sigma_o, \tag{25}$$

$$(q+1)e = (S+1)e_o - (S-q)e, \tag{26}$$

$$(q+1)z_v = 2STe^v + \sum_{x \in X_v} [(S-q)x - Te^v], \tag{27}$$

$$(q+1)x = STe^v + Te^v - (S-q)x \tag{28}$$

for any $e \in E(0) - e_o,\ x \in E_v - z_v, v \neq v^o$. Note that $e^v \in E(n-1)$

□

We apply the lemma 2.3 to deduce:

Lemma 3.3. *Let R be a commutative ring where $q+1$ is invertible. Then $T^\varepsilon (ST)^k ?$ for all $k \geq 0,\ \varepsilon \in \{0,1\},\ ? \in J$, is an R-basis of $R[I\backslash G]$.*

The importance of this second basis is the description of the Iwahori universal R-module $R[I\backslash G]$ as a left module on the Iwahori Hecke R-algebra H_R. Since $H_R = R[T, ST]$ we deduce

Proposition 3.4. *Let R be a commutative ring where $q+1$ is invertible.*
Then $R[I\backslash G] = H_R(S+1)e_o \oplus_{x \in X - e_o} H_R(S-q)x$.

From the lemma 2.5, when $q+1$ is invertible in R, the R-module H_R is a direct sum

$$H_R = H_R(S+1) \oplus H_R(S-q); \tag{29}$$

the H_R-modules $H_R(S+1), H_R(S-q)$ are projective. The maps $h \to he : H \to He$ are bijective for any oriented edge e; hence by the proposition, the H_R-module $R[I\backslash G]$ is projective **[6]**.

Corollary 3.5. *Let R be a commutative ring where $q+1$ is invertible and let M be a right H_R-module. Set $M_{e_o} := M(S+1),\ M_x := M(S-q)$ for $x \in X - e_o$.*
Then the map $(m_x)_{x \in X} \to \sum_{x \in X} m_x \otimes x$ is an isomorphism

$$M(S+1) \oplus_{x \in X - e_o} M(S-q) \simeq M \otimes_{H_R} R[I\backslash G].$$

The next corollary gives the freeness necessary for integral structures.

Corollary 3.6. *Let R be a commutative principal ring where $q+1$ is invertible and let M be an R-free right H_R-module. Then $M \otimes_{H_R} R[I\backslash G]$ is R-free.*

Proof. A submodule of a free module on a principal ring is free. □

Let E be a finite extension of $\mathbf{Q}_p$ which contains $\mu_{p(q-1)}$, O_E its ring of integers, k_E its residue field.

Theorem 3.7. *Let V be a smooth E-representation of G generated by its I-invariant vectors. If M is an O_E-integral stucture of V^I, then the O_EG-submodule L of V generated by M is an O_E-integral structure of V, isomorphic to $M \otimes_{H_{O_E}} O_E[I\backslash G]$.*

Proof. L is the image of the composite of the two natural G-morphisms

$$M \otimes_{H_{O_E}} O_E[I\backslash G] \to V^I \otimes_{H_E} E[I\backslash G] \to V.$$

By the corollary [**?**], the second morphism is an isomorphism. The natural morphism $? \to ? \otimes_{O_E} E$ is injective when ? is an O_E-free module. Hence the first morphism is injective by the corollary 3.6. □

4. Pro-p-Iwahori universal module

We prove the theorems on the pro-p-Iwahori universal module and their applications to the integral structures of representations generated by their pro-p-wahori invariant vectors.

4.1. We suppose from now on $q \geq 3$. The Iwahori group I is the semi-direct product of the pro-p-Iwahori $I(1)$ and of $I/I(1) \simeq (\mathbf{F}_q^*)^2 \simeq \mu_{q-1}^2$ diagonally embedded. For $g, g' \in GL(2,F)$ and $\lambda, \lambda' \in \mu_{q-1}^2$, the equality $I(1)\lambda g = I(1)\lambda' g'$ implies $Ig = Ig'$ and if $g = g'$ then $\lambda = \lambda'$. The geometric space underlying the pro-p-Iwahori universal $\mathbf{Z}$-module is a fibered space by the finite torus μ_{q-1}^2 above the tree. An element of the fiber Γ_e over the oriented edge e of the tree, is an oriented edge e with a "spin" in μ_{q-1}^2. One cannot pick canonically in Γ_e, the oriented edge e with trivial spin. We decide that $I(1)g$ with g in the chosen system of representatives $\mathcal{E}$ of $I\backslash G$ (18) will be the oriented edge $e = Ig$ with trivial spin and $I(1)\gamma g$ for $\gamma \in \mu_{q-1}^2$, will be the oriented edge e with spin γ. We identify $e = Ig$ with $(e,1) = I(1)g$ for $g \in \mathcal{E}$. The pro-p-universal module is

$$\mathbf{Z}[I(1)\backslash G] = \oplus_e \mathbf{Z}\Gamma_e,$$

where $\mathbf{Z}\Gamma_e$ is the free $\mathbf{Z}$-module generated by the the elements in Γ_e. The pro-p-Iwahori Hecke ring $H^{(1)}$ isomorphic to the convolution ring of double classes modulo $I(1)$ and is generated by the classes of $\gamma \in \mu_{q-1}^2$, t, s (4). The

action of $G \times H^{(1)}$ on $\mathbf{Z}[I(1)\backslash G]$ commutes with the projection $\mathbf{Z}[I(1)\backslash G] \to \mathbf{Z}[I\backslash G]$. This is clear for $g \in G$. For $H^{(1)}$ this results from the fact that the double classes modulo $I(1)$ of γ, t, s have the same decomposition in $I(1)$-classes $I(1)\gamma I(1) = I(1)\gamma,\ I(1)tI(1) = I(1)t, I(1)sI(1) = \cup_{x\in\mathbf{F}_q} I(1)su_x$, than the double classes modulo I in I-classes (9).

We still denote by $T : I(1)g \to I(1)tg,\ S : I(1)g \to \sum_{x\in\mathbf{F}_q} I(1)su_x g$ their linear extension to the universal pro-p-Iwahori module. The linear operators $T_\gamma : I(1)g \to I(1)\gamma g$ permute the spins. The element s of order 2 acts naturally on $I/I(1) \simeq \mu_{q-1}^2$. We have

$$T^2 = 1,\ \ TT_\lambda = T_{s\lambda}T,\ ST_\lambda = T_{s\lambda}S,\ T_\lambda T_{\lambda'} = T_{\lambda\lambda'}. \tag{30}$$

The spin ring is

$$A := \mathbf{Z}[T_\lambda\ \ (\lambda \in \mu_{q-1}^2)] \simeq \mathbf{Z}[I/I(1)]$$

acts simply transitively on each fiber $\Gamma_e = Ae$. The subring A^s of invariants by s is central in $H^{(1)}$ and contains

$$\tau := \sum_{x\in\mu_{q-1}} T_{h_x}, \quad \tau^2 = (q-1)\tau. \tag{31}$$

with h_x as in (8). We have

$$Se_o = \sum_{x\in\mathbf{F}_q} I(1)su_x = \sigma_o \tag{32}$$

$$Se_y^o = \sum_{x\in\mathbf{F}_q} I(1)su_x su_y = e_o + T_{\lambda_{-1}} \sum_{x\in\mu_{q-1}} T_{h_x} e^o_{x+y}. \tag{33}$$

We deduce

$$S\sigma_o = qe_o + T_{\lambda_{-1}}\tau\sigma_o \tag{34}$$

and using (32),

$$S^2 = q + \tau\ T_{\lambda_{-1}}S. \tag{35}$$

The equations (15) (**??**) for ST are also true in $H^{(1)}$. The ring $H^{(1)}$ is generated by the spin ring A and the elements T, S satisfying the relations (30), (35), and is a free A-module of basis

$$(ST)^k,\ (ST)^kS,\ T(ST)^k,\ T(ST)^kS \qquad (k \geq 0).$$

We give a first basis of the pro-p-Iwahori universal module, compatible with the orientation and the filtration given by the distance to the origin on the tree, trivially deduced from the first basis of the Iwahori universal module (proposition 3.1).

Proposition 4.1. *1) An A-basis of* $\oplus_{e\in E(\leq n)}Ae$ *is* $(ST)^k x$ *for all* $x \in X(r), k \geq 0, r+k \leq n$.

2) A basis of $\oplus_{e\in TE(\leq n)}Ae$ *is* $(TS)^k Tx$ *for all* $x \in X(r), k \geq 0, k+r \leq n$.

3) A basis of pro-p-Iwahori universal A-module $\mathbf{Z}[I(1)\backslash G]$ *is* $(ST)^k x, T(ST)^k x$ *for all* $x \in X, k \geq 0$.

This basis of $\mathbf{Z}[I(1)\backslash G]$ is T-stable but not S-stable. We extend the scalars to a commutative ring R and we try to decompose $R[\mathbf{Z}[I(1)\backslash G]$ as a direct product which is $H^{(1)}$-stable. A central idempotent of $H_R^{(1)}$ will give such a decomposition. The lemma 2.3 is useful to find idempotents. If $(q-1)$ is invertible, $R[\tau] = R[\tau]\tau \oplus R[\tau](\tau+1-q) \simeq R \oplus R$. As $R[\tau]$ is central in $H_R^{(1)}$, the algebra $? = H_R^{(1)}, A_R, A_R^s$ is a direct sum of two R-algebras, the Iwahori component $?^{Iw} :=?\tau$ and the regular component $?^{reg} :=?(\tau+1-q)$.

Lemma 4.2. *When* $q-1$ *is invertible in R, the Iwahori component* $H_R^{(1),Iw}$ *of the pro-p-Iwahori algebra is isomorphic to the Iwahori Hecke* A_R^{Iw}*-algebra* $H_{A_R^{Iw}}$.

Proof. Since $T_{h_x}\tau = 1$ for all $x \in \mu_{q-1}$, the Iwahori component A_R^{Iw} of A_R is central in $H_R^{(1),Iw}$. When $p = 2, T_{\lambda_{-1}} = 1$, one sees on the relations (30), (35) that $H_R^{(1),Iw}$ is $H_{A_R^{Iw}}$. When $p \neq 2$, since 2 is invertible in R, $A_R^{Iw} = \oplus_{\varepsilon=\pm 1} A_R^{Iw}(T_{\lambda_{-1}}+\varepsilon)$. The $A_R^{Iw}(T_{\lambda_{-1}}+\varepsilon)$-algebra $H_{R,\varepsilon}^{(1),Iw} := H_R^{(1),Iw}(T_{\lambda_{-1}}+\varepsilon)$ is generated by T, S satisfying

$$T^2 = 1, \quad S^2 = q + \varepsilon(q-1)S,$$

isomorphic to the Iwahori Hecke algebra $H_{A_R^{Iw}(T_{\lambda_{-1}}+\varepsilon)}$ by $T \to T, S \to \varepsilon S$. □

The R-algebra H_R^{reg} generated by S, T satisfying

$$T^2 = 1, \quad S^2 = q,$$

is called the regular Hecke R-algebra [**8**].

Lemma 4.3. *When* $q-1$ *is invertible in R, the regular component* $H_R^{(1),reg}$ *of the pro-p-Iwahori algebra is isomorphic to the twisted tensor product of the* $A^{s,reg}$ *algebras* A^{reg} *and the regular Hecke* $A_R^{s,reg}$*-algebra.*

Hence $H_R^{(1),reg} = A^{reg} \otimes_{A_R^{s,reg}} H^{reg}_{A_R^{s,reg}}$ as an R-module, the product beeing twisted by the action of $H^{reg}_{A_R^{s,reg}}$ on A, trivial on $A_R^{s,reg}$ and equal to s on S, T.

Proof. In the regular component $H_R^{(1),reg}$, we have $S^2 = q$ because $\tau = 0$. The subalgebra of $H_R^{(1),reg}$ generated by T, S and the central algebra $A_R^{s,reg}$ is

isomorphic to the the regular Hecke $A_R^{s,reg}$-algebra. The R-algebra $H_R^{(1),reg}$ is generated by A^{reg}, T, S. □

4.2. We study now the universal pro-p-Iwahori module $R[I(1)\backslash G]$ as a $H_R^{(1),reg}$-module.

Suppose that $q \geq 3,\ q-1$ is invertible in R. When $q = p^{2r}$ for an integer $r \geq 1$, set $\sqrt{q} = p^r$. When $q = p^{2r+1}$ we suppose that p is a square in R and we set $\sqrt{q} = p^r\sqrt{p}$.

As in the Iwahori case, we consider the A_R^{reg}-module $A_R^{reg}E(0)$ generated by the outward edges starting from the origin. We note S instead of $S(\tau + 1 - q)$ in $H_R^{(1),reg}$ to simplify. The action of $S \in H_R^{(1),reg}$ is given by (32), (33). We have $S(S + \varepsilon\sqrt{q}) = \varepsilon\sqrt{q}(S + \varepsilon\sqrt{q})$ for $\varepsilon = \pm 1$, and S stabilizes $A_R^{reg}E(0)$. We consider the subset

$$J_\varepsilon(0) = \{(S + \varepsilon\sqrt{q})e_o,\ (S - \varepsilon\sqrt{q})e \text{ for all } e \in E(0) - e_o\}$$

of $A_R^{reg}E(0)$ and the key property:

$A_R^{reg}J_\varepsilon(0)$ contains $aE(0)$ for some non zero integer a.

If the key property is true for a nonzerodivisor $a \in R$, then $J_\varepsilon(0)$ is A_R^{reg}-free. This results from the first part of the elementary lemma 2.4 applied to the free A_R^{reg}-module $M = A_R^{reg}E(0)$ and to $J_\varepsilon(0) = (f_i)_{1 \leq i \leq n}$.

Lemma 4.4. *The sum $\sum_{?\in J_\varepsilon(0)} H_R^{(1),reg}?$ is direct when $A_R^{reg}J_\varepsilon(0)$ contains $aE(0)$ for a nonzerodivisor $a \in R$.*

Proof. $H_R^{(1)} = A_R[ST, S]$. Since $S? \in R?$ for any $? \in J_\varepsilon(0)$ and $J_\varepsilon(0)$ is A_R^{reg}-free, the sum $\sum_{?\in J_\varepsilon(0)} A_R^{reg}[S]? = \sum_{?\in J_\varepsilon(0)} A_R^{reg}?$ is direct. By the proposition 4.1, $\sum_{?\in J_\varepsilon(0)} A_R^{reg}[ST]?$ is a direct sum because $J_\varepsilon(0) \subset A_R E(0)$.

□

In general, the key property is false but we will find an idempotent $e \in A_R^{s,reg}$ such that $A_R^{reg}J_\varepsilon(0)$ contains $aeE(0)$ for some nonzero integer a (with an exception $\varepsilon = 1, q = 4$). The idempotent e is central in $H_R^{(1),reg}$ and $e? = e?^{reg}$ for $? = H_R^{(1)}, A_R, A_R^s$. The same proof than in the lemma 4.4 shows that the sum $\sum_{?\in J_\varepsilon(0)} eH_R^{(1)}?$ is direct if a is a nonzerodivisor R.

4.3. Suppose that $q \geq 3,\ q-1$ is invertible in R and $\sqrt{q} \in R$. The equations $Se_o = \sigma_o = \sum_{e\in E(0)-e_o} e,\ S\sigma_o = qe_o$, imply that

$$2qe_o = \sqrt{q}(S + \varepsilon\sqrt{q})e_o + (S - \varepsilon\sqrt{q})\sigma_o \tag{36}$$

belongs to $RJ_\varepsilon(0)$. We have to suppose that $2q$ is a non zerodivisor in R, which is infortunate. The q equations

$$v_o^o := T_{\lambda_{-1}} S e_o = T_{\lambda_{-1}} \sum_{x\in\mathbf{F}_q} e_x^o \tag{37}$$

$$v_y^o := T_{\lambda_{-1}}((S-\varepsilon\sqrt{q})e_y^o - e_o) = -\varepsilon\sqrt{q}T_{\lambda_{-1}}e_y^o + \sum_{x\in\mathbf{F}_q^*} T_{h_x} e_{x+y}^o, \tag{38}$$

for $y \in \mathbf{F}_q^*$ will be studied with an additive Fourier transform.

We suppose that R contains μ_p, i.e. there is an injective morphism $x \to \zeta_p^x : \mathbf{F}_p \to R^*$ ($\zeta_p = e^{2i\pi}/p$ when $R = \mathbf{C}$), and we take an additive Fourier transform:

$$\sigma_x := \sum_{?\in\mathbf{F}_q} e(x?)e_?^o, \quad v_x := \sum_{?\in\mathbf{F}_q} e(x?)v_?^o$$

for $x \in \mathbf{F}_q$ where $e(x) := \zeta_p^{tr(x)}$ and

$$tr(?) = \sum_{i=0}^{r-1} ?^{p^i} \quad \text{when } q = p^r$$

is the trace $\mathbf{F}_q \to \mathbf{F}_p$. The additive characters $e_x(?) = e(x?) : \mathbf{F}_q \to R^*$ for all $x \in \mathbf{F}_q^*$ are distinct and not trivial because the trace is not degenerate and $\zeta_p^?$ is injective. We compute the coefficients of $(v_x)_{x\in\mathbf{F}_q}$ on $(\sigma_x)_{x\in\mathbf{F}_q}$. The Gauss sum

$$G_q(x) := \sum_{y\in\mathbf{F}_q^*} e(xy)T_{h_y} \qquad (x \in \mathbf{F}_q)$$

will appear naturally. We have $G_q(0) = 0$. We have

$$v_o - v_o^o = \sum_{y\in\mathbf{F}_q^*} v_y^o = -\varepsilon\sqrt{q}T_{\lambda_{-1}}\sigma_o + \varepsilon\sqrt{q}T_{\lambda_{-1}}e_o^o + \sum_{x,y\in\mathbf{F}_q^*} T_{h_x}e_{x+y}^o$$

$$\sum_{x,y\in\mathbf{F}_q^*} T_{h_x}e_{x+y}^o = \sum_{t\in\mathbf{F}_q} e_t^o \sum_{x\neq t} T_{h_x} = -\sum_{t\in\mathbf{F}_q^*} T_{h_t}e_t^o.$$

$$v_o = -\varepsilon\sqrt{q}T_{\lambda_{-1}}\sigma_o + v_o^o + \varepsilon\sqrt{q}T_{\lambda_{-1}}e_o^o - \sum_{t\in\mathbf{F}_q^*} T_{h_t}e_t^o.$$

For $u \in \mathbf{F}_q^*$,

$$v_u - v_o^o = \sum_{y\in\mathbf{F}_q^*} e(uy)v_y^o = -\varepsilon\sqrt{q}T_{\lambda_{-1}}\sigma_u + \varepsilon\sqrt{q}T_{\lambda_{-1}}e_o^o + \sum_{x,y\in\mathbf{F}_q^*} e(yu)T_{h_x}e_{x+y}^o$$

$$\sum_{x,y\in\mathbf{F}_q^*} e(yu)T_{h_x}e^o_{x+y} = \sum_{t\in\mathbf{F}_q} e(tu)e^o_t \sum_{x\neq t} e(-xu)T_{h_x} =$$

$$G_q(-u)\sigma_u - \sum_{t\in\mathbf{F}_q^*} T_{h(t)}e^o_t.$$

$$v_u = (G_q(-u) - \varepsilon\sqrt{q}T_{\lambda_{-1}})\sigma_u + v^o_o + \varepsilon\sqrt{q}T_{\lambda_{-1}}e^o_o - \sum_{t\in\mathbf{F}_q^*} T_{h(t)}e^o_t.$$

We obtain:

Lemma 4.5. *$w := v_y - (G_q(-y) - \varepsilon\sqrt{q}T_{\lambda_{-1}})\sigma_y$ does not depend on $y \in \mathbf{F}_q$.*

We will not use the value of

$$w := v^o_o + \varepsilon\sqrt{q}T_{\lambda_{-1}}e^o_o - \sum_{t\in\mathbf{F}_q^*} T_{h(t)}e^o_t$$

but we mention that

$$qw = qv^o_o + \varepsilon\sqrt{q}T_{\lambda_{-1}}(\sum_{x\in\mathbf{F}_q}\sigma_x) - \sum_{t\in\mathbf{F}_q^*, x\in\mathbf{F}_q} T_{h(t)}e(-tx)\sigma_x =$$

$$qv^o_o + \varepsilon\sqrt{q}T_{\lambda_{-1}}(\sum_{x\in\mathbf{F}_q}\sigma_x) - \sum_{x\in\mathbf{F}_q^*} G_q(-x)\sigma_x = qv^o_o - \sum_{x\in\mathbf{F}_q}(G_q(-x) - \varepsilon\sqrt{q}T_{\lambda_{-1}})\sigma_x.$$

Lemma 4.6. *$2qe_o$ and $2q^2\prod_{x\in\mathbf{F}_q}(G_q(x) - \varepsilon\sqrt{q}T_{\lambda_{-1}})e^o_y$ for all $y \in \mathbf{F}_q$, belong to $A_R^{reg}J_\varepsilon(0)$.*

Proof. By (4.3) $2qe_o$ and $2\varepsilon\sqrt{q}\sigma_o = \varepsilon\sqrt{q}(S + \varepsilon\sqrt{q})e_o - (S - \varepsilon\sqrt{q})\sigma_o$ belong to $RJ_\varepsilon(0)$, by (38) $(2qv^o_x)_{x\in\mathbf{F}_q}$ is contained in $R[T_{\lambda_1}]J_\varepsilon(0)$. By Fourier transform $(2qv_x)_{x\in\mathbf{F}_q}$ belong to $A_R^{reg}J_\varepsilon(0)$, hence $2qw = 2qv_o + \varepsilon\sqrt{q}T_{\lambda_1}2q\sigma_o$ and $2q(G_q(-x) - \varepsilon\sqrt{q}T_{\lambda_{-1}})\sigma_x = 2qv_x - 2qw$ for all $x \in \mathbf{F}_q$, belong to $A_R^{reg}J_\varepsilon(0)$. By inverse Fourier transform $(qe^o_x)_{x\in\mathbf{F}_q}$ belongs to the A_R^{reg}-module generated by $(\sigma_x)_{x\in\mathbf{F}_q}$. □

We suppose that R contains μ_{q-1} in order to replace $G_q(x) - \varepsilon\sqrt{q}T_{\lambda_{-1}}$ in A_R^{reg} by the elements $G_q(x,\mu) - \varepsilon\sqrt{q}\eta$ in R obtained by specialisation $T_{h_x} \to \mu(x)$, $T_{\lambda_{-1}} \to \eta$ for $\eta = 1$ if $p = 2$ and $\eta \in \{\pm 1\}$ if $p \neq 2$, and for $\mu : \mathbf{F}_q^* \to R^*$ a non trivial character. By definition

$$G_q(x,\mu) := \sum_{y\in\mathbf{F}_q^*} e(xy)\mu(y).$$

One associate to μ an idempotent $e_\mu = \sum_{x\in\mathbf{F}_q^*}\mu(x)^{-1}T_{h_x}$ in A_R (even when μ is trivial), and an idempotent $e_{\mu^{\pm 1}} \in A_R^{\mathrm{s}}$ equal to $e_\mu + e_{\mu^{-1}}$ if $\mu \neq \mu^{-1}$ and e_μ if e_μ if $\mu = \mu^{-1}$.

The element $G_q(x) - \varepsilon\sqrt{q}T_{\lambda_{-1}}$ is a nonzerodivisor in $e_{\mu^{\pm 1}}A_R$, if and only if the following elements are nonzerodivisor in R:

a) $G_q(x,\mu) - \varepsilon\sqrt{q},\ G_q(x,\mu^{-1}) - \varepsilon\sqrt{q}$ if $p = 2$,

b) $G_q(x,\mu) + \sqrt{q},\ G_q(x,\mu^{-1}) + \sqrt{q}, G_q(x,\mu) - \sqrt{q},\ G_q(x,\mu^{-1}) - \sqrt{q}$ if $p \neq 2$.

These elements in R are the images of their complex analogues by the morphism $\mathbf{Z}[\sqrt{q}, \mu_{p(q-1)}] \to R$.

The set $\mathcal{F}^{reg}$ of complex non trivial characters μ such that the algebraic integers a) or b) are not 0 for all $x \in \mathbf{F}_q^*$, is stable by $\mu \to \mu^{-1}$. The set $\mathcal{F}^{reg}$ depends on the choice of ε when $p = 2$; it is empty when $q = 4, \varepsilon = 1$ because $G_4(\mu) = 2$ for the two non trivial characters of $\mathbf{F}_4^*$.

If $\mathcal{F}^{reg}$ is not empty, then the product of the algebraic integers in a) or b) for all $x \in \mathbf{F}_q^*, \mu \in \mathcal{F}^{reg}$ is a non zero element in $\mathbf{Z}[\sqrt{q}, \mu_{p(q-1)}]$ and its norm in $\mathbf{Q}$ is a non zero integer d, and $e_{\mathcal{F}}^{reg} = \sum_{\mu^{\pm 1} \in \mathcal{F}^{reg}} e_{\mu^{\pm 1}} \in A_R^s$ is a central idempotent in $H_R^{(1)}$.

Proposition 4.7. *Suppose that $q \geq 3$, $q-1$ invertible and $2qd$ is a nonzerodivisor in R, q is a square in R, and R contains $\mu_{p(q-1)}$.*

If the set $\mathcal{F}^{reg}$ is not empty, then $2q^2 d\ e_{\mathcal{F}}^{reg} E(0) \subset A_R^{reg} J_\varepsilon(0)$ and the sum $\sum_{e \in J_\varepsilon(0)} e_{\mathcal{F}}^{reg} H_R^{(1)}$? is direct.

4.4. Gauss sums We prove that $\mathcal{F}^{reg}$ is not empty.

We recall some properties of the complex Gauss sums $G_q(x,\mu)$ for $x \in \mathbf{F}_q^*, \mu : \mathbf{F}_q^* \to \mathbf{C}^*$ non trivial ([**2**] 1.1.3, 1.1.4). Set $q = p^r$.

a) Set $G_q(\mu) := G_q(1,\mu)$. Then

$$G_q(x,\mu) = \mu(x)^{-1} G_q(\mu), \quad G_q(\mu) = \mu(-1)\overline{G}_q(\mu^{-1}) = G_q(\mu^p) = \eta_\mu \sqrt{q}$$

where $|\eta_\mu| = 1$.

b) By a theorem of Chowla ([**2**] 1.6.1), $G_p(\mu)$ does not equal $\sqrt{p}$ times a root of unity when $q = p$ is odd and μ is not a quadratic character.

c) When q is odd and μ quadratic, we have ([**2**] 11.5.4):

$G_q(\mu) = (-1)^{r-1}\sqrt{q}$ if $p \equiv 1 \pmod 4$,

$G_q(\mu) = (-1)^{r-1} i^r \sqrt{q}$ if $p \equiv 3 \pmod 4$.

d) The Gauss sum $G_q(\mu)$ belongs to the ring of integers O_E of the cyclotomic field $E := \mathbf{Q}(e^{2i\pi/p(q-1)})$. The decomposition in prime ideals of the ideal $O_E G_q(\mu)$ is known ([**2**] 11.2.2). For $1 \leq h \leq q-1$, set

$$s(h) := a_o + \ldots + a_{r-1}$$

for $0 \leq a_i \leq p-1$ and $h = a_o + pa_1 + \ldots + a_{r-1}p^{r-1}$. Let T be a set of $\phi(q-1)/r$ integers $1 \leq h \leq q-1$ which represent the quotient of $(\mathbf{Z}/(q-1)\mathbf{Z})^*$ by the cyclic subgroup generated by the image of p. There are distinct $\phi(q-1)/r$

primes ideals $\mathcal{P}_h$ of O_E for $h \in T$ such that

$$O_E p = \prod_{h\in T} \mathcal{P}_h^{p-1}, \quad O_E G_q(\mu^{-1}) = \prod_{h\in T} \mathcal{P}_h^{s(h)}, \quad O_E G_q(\mu) = \prod_{h\in T} \mathcal{P}_h^{r(p-1)-s(h)}$$

when the order of μ is $q-1$.

Lemma 4.8. *When the order of μ is $q-1$, the Gauss sum $G_q(\mu)$ does not equal $\varepsilon\sqrt{q}$ times a root of unity ζ with $\zeta^{q-1} = 1$, with the only exception: $q = 4, \varepsilon = 1$ where $G_4(\mu) = G_4(\mu^{-1}) = 2$.*

Proof. When η_μ is a root of 1, the relation $G_q(\mu) = \eta_\mu\sqrt{q}$ implies $s(?) = r(p-1)/2$ for all $? \in T$. Since $s(1) = 1$, this means $r(p-1) = 2$, i.e. $p = 2, r = 2, q = 4$ or $p = 3, r = 1, q = 3$. Since $G_4(\mu) = 2$, $\quad G_3(\mu) = i\sqrt{3}$ and i is not of order 3 when $q = 3$, we deduce the lemma. □

For $\varepsilon = \pm 1$, let $\mathcal{F}_\varepsilon^{reg}$ be the set of non trivial characters $\mu : \mathbf{F}_q^* \to \mathbf{C}^*$ such that the complex Gauss sum $G_q(x, \mu) - \varepsilon\sqrt{q} \neq 0$ for all $x \in \mathbf{F}_q^*$.

Lemma 4.9. *1) We have $\mathcal{F}^{reg} := \mathcal{F}_1^{reg} \cap \mathcal{F}_{-1}^{reg}$ if $p \neq 2$.*

2) The set $\mathcal{F}^{reg}$ contains the characters μ of order $q-1$ with an exception: $q = 4, \varepsilon = 1$.

3) When $q = p$, $\mathcal{F}^{reg}$ is equal to the set of non trivial characters of $\mathbf{F}_q^*$ $p \equiv 3 \pmod 4$ or $q = p = 2$. When $p \equiv 1 \pmod 4$, only the quadratic character is missing.

Proof. $G_q(x, \mu) = \varepsilon\sqrt{q}$ is equivalent by a) to $G_q(\mu) = \varepsilon\sqrt{q}\mu(x)$. Apply the lemma 4.8 to see that $\mathcal{F}_\varepsilon^{reg}$ contains the characters μ of order $q-1$ with an exception: $q = 4, \varepsilon = 1$.

If $p = 2$, then $G_q(\mu) = \overline{G}_q(\mu^{-1})$ by a). If $G_q(\mu) + \sqrt{q} \neq 0$ then $\overline{G}_q(\mu) + \sqrt{q} \neq 0$.

If $p \neq 2$, then $G_q(\mu) = \pm\overline{G}_q(\mu^{-1})$ by a). If $G_q(\mu) + \sqrt{q} \neq 0$ and $G_q(\mu) - \sqrt{q} \neq 0$ then the same is true for $\overline{G}_q(\mu)$ and for $G_q(\mu^{-1})$.

One deduces 1) and 2). Clearly 3) results from b) and c). □

4.5. We consider now the upper branches of the tree. Notations as in the sections 2.6, 2.8. Let $n \geq 1$ and let $v \neq v^o$ be a vertex of $S(n)^\varepsilon$ where $\varepsilon = 0, 1$, with $z_v = e_{o,w}^\varepsilon$. We have the q equations

$$v_{o,w}^e := T_{\lambda_{-1}} STe^v = T_{\lambda_{-1}} \sum_{x\in\mathbf{F}_q} e_{x,w}^\varepsilon, \tag{39}$$

$$v_{y,w}^e := T_{\lambda_{-1}}((S - \varepsilon\sqrt{q})e_{y,w}^\varepsilon - Te^v) = -\varepsilon\sqrt{q}T_{\lambda_{-1}} e_{y,w}^\varepsilon + \sum_{x\in\mathbf{F}_q^*} T_{h_x} e_{x+y,w}^\varepsilon. \tag{40}$$

for $y \in \mathbf{F}_q^*$, using (8) and (9). There are similar to the q equations (37), (38) and $e^v \in E(n-1)$. We define the set

$$J_\varepsilon(n) := \{(S - \varepsilon\sqrt{q})e \text{ for } e \in X(n)\}.$$

We choose $\varepsilon = -1$ when $q = 4$. In the next proposition, d is as in the proposition 4.7.

Proposition 4.10. *$H_R^{(1)}E(\leq n-1) + A_R J_\varepsilon(n)$ contains $qd\, e_{\mathcal{F}}^{reg}E(n)$ for all $n \geq 1$.*

Proof. Set $N := H_R^{(1)}E(\leq n-1) + A_R J_\varepsilon(n)$. Then $v_{x,w}^\varepsilon$ and its Fourier transform $\sum_{?\in\mathbf{F}_q} e(x?)v_{?,w}^\varepsilon$ belongs to N, for all $x \in \mathbf{F}_q$. The Fourier transform of $e_{o,w}^\varepsilon$ times $G_q(0) - \varepsilon\sqrt{q}T_{\lambda_1}$ beeing $-\varepsilon\sqrt{q}v_{o,w}^e$ belongs to N. The Fourier transform of $v_{x,w}^\varepsilon$ minus the Fourier transform $\sum_{?\in\mathbf{F}_q} e(x?)e_{?,w}^\varepsilon$ of $e_{x,w}^\varepsilon$ times $(G_q(-x) - \varepsilon\sqrt{q}T_{\lambda_1})$ is an element which does not depend on the choice of $x \in \mathbf{F}_q$ by the proof of the lemma 4.5. Looking at $x = 0$, this element belongs to N. Hence the Fourier transform of $e_{x,w}^\varepsilon$ times $(G_q(-x) - \varepsilon\sqrt{q}T_{\lambda_1})$ belongs to N for all $x \in \mathbf{F}_q$. Apply the proposition 4.7. By inverse Fourier transform $qde_{\mathcal{F}}^{reg}e_{x,w}^\varepsilon$ belongs to N for all $x \in \mathbf{F}_q$, where d is the same positive integer than in the proposition 4.7. □

Recall that $q|d$. The second part of the lemma 2.4 implies:

Proposition 4.11. *The sum (with q terms)*

$$e_{\mathcal{F}}^{reg}H_R^{(1)}E(\leq n-1) + \sum_{?\in J_\varepsilon(n)} e_{\mathcal{F}}^{reg}H_R^{(1)}?$$

is direct when d is a nonzerodivisor in R.

4.6. Suppose that $q^2 - 1$ is invertible, $2d$ is a nonzerodivisor, q is a square in R, and R contains $\mu_{p(q-1)}$. We put together the Iwahori and the regular case. Set $e_{\mathcal{F}} = e_{\mathrm{id}} + e_{\mathcal{F}}^{reg} \in A_R^s$ for the central idempotent of $H_R^{(1)}$ associated to the set $\mathcal{F} = \mathrm{id} \cup \mathcal{F}^{reg}$ of characters of $\mathbf{F}_q^*$. We fix a sign ε with $\varepsilon = -1$ if $q = 4$. We define two elements $a, b \in e_{\mathcal{F}}A_R^s$,

$$e_{\mathrm{id}}a = 1,\ e_{\mathrm{id}}b = q, \quad e_{\mathcal{F}}^{reg}a = \varepsilon\sqrt{q},\ e_{\mathcal{F}}^{reg}b = -\varepsilon\sqrt{q}.$$

We have $(e_{\mathcal{F}}S + a)(e_{\mathcal{F}}S - b) = 0$. For $n \geq 0$, let

$$J(\leq n) := \{(S + a)e_o,\ \ (S - b)e \text{ for } e \in X(\leq n) - e_o\}$$

the union of $J(i)$ for $0 \leq i \leq n$, and J the union of all $J(i)$ for $i \geq 0$.

Theorem 4.12. *We have* $2q^2d^{n+1}e_{\mathcal{F}}E(\leq n) \subset H_R^{(1)}J(\leq n)$ *for any* $n \geq 0$, *and* $e_{\mathcal{F}}H_R^{(1)}J = \sum_{?\in J} e_{\mathcal{F}}H_R^{(1)}?$ *is a direct sum isomorphic to*

$$e_{\mathcal{F}}H_R^{(1)}(S+a) \oplus_{x\in X-e_o} e_{\mathcal{F}}H_R^{(1)}(S-b).$$

Proof. Corollary 3.4 and Proposition 4.11. The isomorphism uses that $h \to he : H^{(1)} \to H^{(1)}e$ is injective for any oriented edge e. □

Application. Let M be a right $H_R^{(1)}$-module such that $Me_{\mathcal{F}} = M$. For an outward edge $x \in X$ we set

$$M_{e_o} := M(S+a),\ M_x := M(S-b) \text{ if } x \neq e_o.$$

Corollary 4.13. *Let* M *be a right* $H_R^{(1)}$*-module such that* $Me_{\mathcal{F}} = M$ *and* $2d$ *is a nonzerodivisor in* M. *Then the map*

$$(m_x) \to \sum_x m_x \otimes x :\ \oplus_{x\in X} M_x \to M \otimes_{H_R^{(1)}} R[I(1)\backslash G]$$

is injective, of cokernel annilated by $2d^\infty$.

Proof. The natural $H_R^{(1)}$-morphism $\oplus_{x\in X} e_{\mathcal{F}}H_{R,x}^{(1)} \to e_{\mathcal{F}}R[I(1)\backslash G]$ is injective, with cokernel annihilated by $2d^\infty$. This implies that the kernel and the cokernel of the R-morphism $\oplus_{x\in X} M_x \to M \otimes_{H_R^{(1)}} R[I(1)\backslash G]$ is annihilated by d^∞. But $2d$ is a nonzerodivisor in $M_x \subset M$ for all $x \in X$. Hence the kernel is 0. □

We deduce the freeness necessary for integral structures.

Proposition 4.14. *Suppose that* R *is a local principal complete ring which contains* $\mu_{p(q-1)}$, *where* $q^2 - 1$ *is invertible,* $2d$ *is a nonzerodivisor,* q *is a square. Let* M *be a* R*-free right* $H_R^{(1)}$*-module such that* $Me_{\mathcal{F}} = M$. *Then* $M \otimes_{H_R^{(1)}} R[I(1)\backslash G]$ *modulo its torsion is* R*-free.*

Proof. Let K be the fraction field of R and let L be the quotient of the R-module $M \otimes_{H_R^{(1)}} R[I(1)\backslash G]$ by its torsion. The R-modules $R[I(1)\backslash G]$ and M are R-free of countable rank, hence L is contained in a K-vector space of countable dimension. The natural R-linear map $\oplus_{x\in X} M_x \to L$ remains injective because $\oplus_{x\in X} M_x$ is R-free, and its cokernel is annhilated by $2d^\infty$. This implies that L does not contain a one dimensional K-vector space. □

Let E be a finite extension of $\mathbf{Q}_p$ which contains $\mu_{p(q-1)}$, O_E its ring of integers, k_E its residue field.

Theorem 4.15. *Let V be a smooth E-representation of G generated by its $I(1)$-invariant vectors such that $V^{I(1)} = e_{\mathcal{F}}V^{I(1)}$. If M is an O_E-integral stucture of $V^{I(1)}$, then the O_EG-submodule L of V generated by M is an O_E-integral structure of V.*

Proof. L is the image of the composite of the two natural G-morphisms

$$M \otimes_{H^{(1)}_{O_E}} O_E[I(1)\backslash G] \to V^{I(1)} \otimes_{H^{(1)}_E} E[I\backslash G] \to V.$$

By the corollary 2.2, the second morphism is an isomorphism. The kernel of the natural morphism $? \to ? \otimes_{O_E} E$ is the torsion of ? when ? is an O_E-module. By the proposition 4.14 the image of the first morphism is O_E-free. □

References

[1] Bernstein Joseph, Le "centre" de Bernstein, rédigé par P. Deligne, Représentations des groupes réductifs sur un corps local par Bernstein, Deligne, Kazhdan, Vignéras, Hermann (1984).

[2] Berndt Bruce, Evans Ronald J., Williams Kenneth S., Gauss and Jacobi Sums, Canadian Mathematical Society Series of Monographs and Advanced Texts **21,** Wiley-interscience (1998).

[3] Bourbaki Nicolas, Algèbre I. Hermann (1970).

[4] Breuil Christophe, Sur quelques représentations modulaires et p-adiques de $\mathrm{GL}_2(\mathbf{Q}_p)$ I", Compositio Math **138,** (2003) 165-188.

[5] Dat Jean-Francois, Generalized tempered representations of p-adic groups. Preprint 2004.

[6] Ollivier Rachel, Platitude du $H_{\overline{F}_p}(GL_2(F), I(1)Z)$-module $\mathrm{ind}_{I(1)Z}^{GL_2(F)} 1$, Preprint (2004).

[7] Serre Jean-Pierre, Arbres, amalgames, SL_2, Astérisque 46, 3ème édition, Soc. Math. de France, (1983).

[8] Vignéras Marie-France, Representations of the p-adic group GL(2,F) modulo p, Compositio Math. **140,** (2004) 333-358.

[9] Vignéras Marie-France, Pro-p-Iwahori Hecke algebra and supersingular $\overline{\mathbf{F}}_p$-representations, Mathematische Annalen, online first 15 october 2004. Corrected version to appear.

[10] Vignéras Marie-France, Représentations ℓ-modulaires d'un groupe réductif p-adique avec $\ell \neq p$, Progress in Math. **137,** Birkhäuser (1996).

[11] Vignéras Marie-France, Cohomology of sheaves on the building and R-representations. Invent. math. 127, 349-373 (1997).