On a numerical Langlands correspondence modulo p with the pro-p-Iwahori Hecke ring

Marie-France Vignéras

Abstract. We show that the pro-p-Iwahori Hecke ring $\mathcal{H}^{(1)}$ of a split reductive p-adic group G admits an Iwahori-Matsumoto presentation and a Bernstein basis, and we determine its centre. The proof consists of a direct extension of methods already developped for the Iwahori Hecke ring. When $G = GL(n)$, we conjecture that the number $M_n(q)$ of the irreducible $\overline{\mathbf{F}}_p$-representations of $\mathcal{H}^{(1)}$ with a null central character (called supersingular representations) of dimension n, and with a fixed action of an uniformizer, is equal to the number $N_n(q)$ of the irreducible $\overline{\mathbf{F}}_p$-representations of dimension n of the local Weil group with a fixed value of the determinant on a Frobenius. Here, q is the cardinal of the residual field $\mathbf{F}_q$ of F and $N_n(q)$ is nothing else than the number of irreducible unitary polynomials of degree n in $\mathbf{F}_q[X]$. We show the inequality $M_n(q) \geq N_n(q)$ and that the equality is equivalent to: any irreducible supersingular irreducible $\overline{\mathbf{F}}_p$-representation of $\mathcal{H}^{(1)}$ contains a character of the affine subring $\mathcal{H}^{(1)}_{aff}$.

We present the results, then we give the proofs. See the conjecture (§7, §38), the Iwahori-Matsumoto presentation (§11), the Bernstein basis (§31), the centre (§33), the supersingular representations (§34), the inequality $M_n(q) \geq N_n(q)$ (§37). The proofs start in §39.

1 Notation. All representations will be smooth representations. In a semidirect product HK of groups, the normal subgroup K will be on the right side. A ring is a $\mathbf{Z}$-algebra. The multiplicative group of a ring R is denoted R^* and the algebraic closure of a field R is denoted $\overline{R}$. We fix:

- F a local non archimedean field (a finite extension of $\mathbf{Q}_p$ or a field of Laurent series $\mathbf{F}_q((t))$ on a finite field $\mathbf{F}_q$ with q elements), of residual field $\mathbf{F}_q$ of characteristic p, O_F the ring of integers, P_F the maximal ideal, p_F an uniformizer, Fr a geometric Frobenius in the Weil group $W(\overline{F}/F)$,

- C an algebraically closed field. We will abbreviate: when the characteristic of C is (...), by: in characteristic (...).

- D a division algebra of dimension n^2 over its centre F, with ring of integers O_D and maximal ideal P_D.

More notations will be given in §9, §39.

Let $z \in C^*$ and n a positive integer. By the local Langlands (and Jacquet-Langlands) correspondence in characteristic different from p, we have bijections betwen the isomorphism classes of

a) the irreducible C-representations of $W(\overline{F}/F)$ of dimension n, with determinant equal to z on Fr,

b) the irreducible C-representations of D^* of dimension n, with central character equal to z on p_F,*

c) the irreducible supercuspidal C-representations of $GL(n,F)$, with central character equal to z on p_F.

* Warning: the bijection with b) has not been proved in the non banal case (positive characteristic $\neq p$ dividing the order of $GL(n,\mathbf{F}_q)$); this should be accessible with the help of the theory of types done by Zink and Broussous.

2 Our purpose is to explore the possibility of the existence of a local Langlands (and Jacquet-Langlands) correspondence *in characteristic p.*

When $n=1$, there is no problem because the local Langlands correspondence arises by Fourier transform from the isomorphism of F^* with the topological abelianized group $W(\overline{F}/F)^{ab}$ given by local class field theory. By definition, any character of F^* is supercuspidal.

We suppose from now on that $n \geq 2$.

3 *In characteristic p, the local Langlands correspondence over $\overline{\mathbf{Q}}_p$ gives by reduction modulo p, a local Langlands correspondence between $W(\overline{F}/F)$ and D^*.*

The (trivial) reason is that *the representations of $W(\overline{F}/F)$ and of D^* are tame in characteristic p* (trivial on the wildly ramification group or on $1+P_D$). The local Langlands correspondence over $\overline{\mathbf{Q}}_p$ respects tameness and gives a bijection between irreducible tame representations of dimension n in characteristic p, compatible with the reduction modulo p. (See Vigneras M.-F. "A propos d'une conjecture de Langlands modulaire" Luminy 1994. In "Finite Reductive Groups: Related Structures and Representations. Marc Cabanes, Editor. Birkhauser PM 141, 1997, 415-452. "Représentations modulaires galois-quaternions pour un corps p-adique". Journées Arithmétiques d'Ulm, Progress in Mathematics, Birkauser (1987)).

4 Let $z \in C^*$ fixed. In **any** characteristic, there is a bijection between:

a)$_t$ the irreducible tame C-representations of $W(\overline{F}/F)$ of dimension n, with determinant equal to z on Fr,

b)$_t$ the irreducible tame C-representations of D^* of dimension n, with p_F acting by z,

d)' the irreducible C-representations of dimension n of the semidirect product $\mathbf{F}_{q^n}^*(\mathbf{Z}/n\mathbf{Z})$ where a generator of $\mathbf{Z}/n\mathbf{Z}$ acts on $\mathbf{F}_{q^n}^*$ by $x \mapsto x^q$,

d) the irreducible unitary polynomials $P \in \mathbf{F}_q[X]$ of degree n.

One knows that the number $N_n(q)$ of polynomials in d) is positive and given by the formula

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

where μ is the Moebius function, equivalent to $q^n = \sum_{d|n} dN_d(q)$ (proof as in Ireland K. Rosen M. A classical introduction to modern number theory page 84, GTM 84 Springer (1990)]). Interesting properties of $N_n(q)$ are given in §21.

5 There is no $GL(n,F)$ in §3 and in §4. In characteristic $\neq p$, the local Langlands correspondence is a bijection between the tame representations a)$_t$, b)$_t$ and

c)$_t$ the supercuspidal irreducible C-representations of $GL(n,F)$ which are tame: having a *non zero vector invariant by the first congruence subgroup* $1 + p_F M(n, O_F)$ of $GL(n, O_F)$ (level 0 in the theory of types), with p_F acting by z.

The supercuspidal $\overline{\mathbf{Q}}_p$-representations of $GL(n,F)$ do **not** have a non zero vector invariant by the pro-p-Sylow $Iw^{(1)}$ of an Iwahori subgroup Iw, but the irreducible $\overline{\mathbf{F}}_p$-representations of $GL(n,F)$ have always a *non zero vector invariant by $Iw^{(1)}$*.

Another striking point is that the supercuspidal $\overline{\mathbf{Q}}_p$-representations of $GL(n,F)$ have *non commensurable $\overline{\mathbf{Z}}_p$-structures*, the classification of the $\overline{\mathbf{Z}}_p$-structures, up to commensurability, seems to be part of the p-adic local Langlands correspondence, according to Christophe Breuil. It is not known if one can find an integral structure with finite length reduction, but one can show that there is one with admissible reduction using that any irreducible integral supercuspidal $\overline{\mathbf{Q}}_p$-representation of $GL(n,F)$ appears in a $\overline{\mathbf{Q}}_p$-representation of $GL(n,F)$ with a natural integral structure of admissible reduction (see Vigneras M.-F. Formal degrees and existence of stable arithmetic lattices of cuspidal representations of p-adic reductive groups, Invent. math. 98, 549-563 (1989)).

The classification of irreducible $\overline{\mathbf{F}}_p$-representations of $GL(n,F)$ is unknown, even for the group $GL(2,F)$ when $F \neq \mathbf{Q}_p$.

6 As $GL(n,F)$ is hard, we will replace it by the Hecke ring of $Iw^{(1)}$:

$$\mathcal{H}^{(1)} = \mathcal{H}(GL(n,F), Iw^{(1)}),$$

that we call the pro-p-Iwahori Hecke ring.

The reason is that we hope that the functor of $Iw^{(1)}$-invariants induces a bijection between the irreducible $\overline{\mathbf{F}}_p$-representations of $GL(n,F)$ and the irreducible $\overline{\mathbf{F}}_p$-representations of $\mathcal{H}^{(1)}$.

This is true for the finite group $GL(n,\mathbf{F}_q)$ (see the forthcoming book of Cabanes and Enguehard for a complete bibliography), for the group $GL(2,\mathbf{Q}_p)$ [V2], and for the C-representations of $GL(n,F)$ with a non zero $Iw^{(1)}$-invariant vector when the characteristic of C is different from p [V4 I.6.3].

7 Denote $M_n(q)$ the number of irreducible *supersingular* (§8) $\overline{\mathbf{F}}_p$-representations of dimension n of the pro-p-Iwahori Hecke ring $\mathcal{H}^{(1)}$ of $GL(n,F)$ where p_F acts by $z \in \overline{\mathbf{F}}_p^*$ fixed.

Conjecture (numerical Langlands correspondence modulo p for $\mathcal{H}^{(1)}$)

There is an equality $N_n(q) = M_n(q)$.

When $n = 1$,

$$\mathcal{H}^{(1)} = \mathbf{Z}[F^*/(1+P_F)],$$

any $\overline{\mathbf{F}}_p$-character of $\mathcal{H}^{(1)}$ will be supersingular, and it is evident that $N_1(q) = M_1(q) = q-1$.

The representations of $\mathcal{H}^{(1)}$ are more tractable than the representations of $GL(n,F)$, and we expect that the classification of the supersingular irreducible $\overline{\mathbf{F}}_p$-representations of $\mathcal{H}^{(1)}$ of dimension n is simple (§38), as the classification of the irreducible $\overline{\mathbf{F}}_p$-representations of the Weil group $W(\overline{F}/F)$ of dimension n.

8 We need to give a representation theoretic definition of the supersingular representations of $\mathcal{H}^{(1)}$, analogues of the supercuspidal representations of $GL(n,F)$.

Definition *A supersingular irreducible representation of $\mathcal{H}^{(1)}$ is an irreducible representation with a* **null** *central character in characteristic p.*

A similar definition is given in [V3] for the classical Iwahori Hecke ring $\mathcal{H}$.

We will explain in §34 what is a null central character of $\mathcal{H}^{(1)}$.

By the Harish-Chandra philosophy of cusp forms, an irreducible representation of $GL(n,F)$ is attached to the conjugacy class of a Levi subgroup of $GL(n,F)$ via parabolic induction. The irreducible representations attached to the group $GL(n,F)$ are called supercuspidal. We propose to call *supersingular* a supercuspidal irreducible representation of $GL(n,F)$ in characteristic p.

When $n=2$, Barthel and Livne (Modular representations of GL_2 of a local field: the ordinary, unramified case. J. of Number Theory 55, 1-27, Irreducible modular representations of a local field. Duke Math. J. 75, 1994, 261-292.) classified the irreducible $\overline{\mathbf{F}}_p$-representations attached to the maximal split torus of $GL(2,F)$ (unique proper Levi subgroup of $GL(2,F)$ modulo conjugaison). They called *supersingular*, instead of supercuspidal, the other ones by analogy with the supersingular elliptic curves and show that they are quotients of explicit cyclic non zero representations V of $GL(2,F)$ constructed using compact induction. Later Breuil (Sur quelques représentations modulaires et p-adiques de $GL_2(\mathbf{Q}_p)$ I, preprint 2001) proved that the V are irreducible when $F=\mathbf{Q}_p$.

The definitions of supersingularity for $GL(n,F)$ and $\mathcal{H}^{(1)}$ should be compatible with the $Iw^{(1)}$-invariant functor. This is known only for $GL(2,\mathbf{Q}_p)$ [V2].

9 The structure of the pro-p-Iwahori Hecke ring $\mathcal{H}^{(1)}$, similar to the description by Iwahori and Matsumoto [IM] of the classical Iwahori Hecke ring $\mathcal{H}$, is given in §11. We replace $GL(n,F)$ by the group G of F-rational points of a split connected reductive group defined over F.

Notation and preliminaries. Notations as in §1, and

- T is a maximal split F-torus of G, $m \geq 1$ the rank of T, $B=TU$ a F-Borel subgroup of G containing T of unipotent radical U; the split connected reductive group G is defined over O_F (Bruhat-Tits, Groupes algébriques sur un corps local, Proc. Driebergen Conference on local fields, Springer-Verlag 1972, page 31), Iw is the inverse image of $B(\mathbf{F}_q)$ by the (surjective)

reduction $G(O_F) \to G(\mathbf{F}_q)$, and $Iw^{(1)}$ is the inverse image of $U(\mathbf{F}_q)$. We have $T(O_F) = T(F) \cap Iw$, $T(1+P_F) = T(F) \cap Iw^{(1)}$. The Teichmüller isomorphism $\mathbf{F}_q^* \to \mu_{q-1}(O_F)$ with image the roots of unity of order prime to p, gives a splitting $T(\mathbf{F}_q) \to T(O_F)$ and we identify $T(\mathbf{F}_q)$ with its image in $T(O_F)$. The Iwahori subgroup Iw is the semidirect product

$$Iw \simeq T(\mathbf{F}_q) Iw^{(1)}.$$

- N is the normalizer of T in G. The three Weyl groups $W_o, W, W^{(1)}$ are the quotients of $N(F)$ by the three subgroups $T(F)$, $T(O_F)$, $T(1+P_F)$, which are in bijection with the double classes of $G(O_F)$ modulo Iw, of $G(F)$ modulo Iw, of $G(F)$ modulo $Iw^{(1)}$ (§42).

- $W_o = N(F)/T(F)$ is the (finite) Weyl group, a Coxeter group generated the set $S_o = \{s_1, \dots, s_{n-1}\}$ of reflexions associated to the simple roots $\{\alpha_1, \dots, \alpha_{n-1}\}$ of T in $\mathrm{Lie}\, U$.

- $W = N(F)/(T(F) \cap Iw)$ is the (infinite) generalised affine Weyl group,

$$W \simeq W_o X \quad \text{(semidirect product)}, \quad X = T(F)/T(O_F),$$

$s_o^{(1)}, \dots, s_o^{(r)}$, the reflexions associated to the highest positive roots $\alpha_o^{(1)}, \dots, \alpha_o^{(r)}$, of the r irreducible components of the root system [IM proposition 1.1 page 10], $S = S_o \cup \{s_o^{(1)}, \dots, s_o^{(r)}\}$ (disjoint union), ℓ the length on W associated to S, Ω the commutative subgroup of elements of length 0 which normalizes S, W_{aff} the Coxeter group generated by the elements of S, is the affine Weyl group. We have

$$W = \Omega W_{aff}, \quad W_{aff} \simeq W_o X_{aff}, \quad X_{aff} = W_{aff} \cap X, \quad \Omega \simeq X/X_{aff}, \quad \text{(semidirect products)},$$

and $(\Omega \cap X) X_{aff}$ is a subgroup of finite index in X.

- $W^{(1)} = N(F)/(T(F) \cap Iw^{(1)})$ and $W_{aff}^{(1)} = W_{aff} T(\mathbf{F}_q)$ (semidirect product) are the analogue of W, W_{aff},

$$W^{(1)} \simeq W_o X^{(1)} \simeq W T(\mathbf{F}_q) \simeq \Omega W_{aff}^{(1)} \quad \text{(semidirect products)}, \quad \mathrm{X}^{(1)} = \mathrm{T(F)/T}(1+\mathrm{P_F}) \simeq \mathrm{X} \times \mathrm{T}(\mathbf{F}_\mathrm{q}).$$

10 Definition *There exists a unique extension of the length ℓ and of the Bruhat order $<$ on W* [V3] *to $W^{(1)} = WT(\mathbf{F}_q)$ such that*

(i) $\ell(twt') = \ell(w)$ for $t, t' \in T(\mathbf{F}_q), w \in W$,

(ii) $w < w'$ for $w, w' \in W^{(1)}$ if and only if there exists $t, t' \in T(\mathbf{F}_q)$ with $wt, w't' \in W$ and $wt < w't'$.

(i) implies that the braid group of $W^{(1)}$ [L2, 2.1 page 603] is isomorphic to the twisted tensor product of the braid group of W by the normal subgroup $T(\mathbf{F}_q)$.

For $g \in N(F)$ of image $w \in W^{(1)}$, we denote by T_w the double class $Iw^{(1)}gIw^{(1)}$ viewed as an element in $\mathcal{H}^{(1)}$. For $s \in S$, we denote by $T_s(\mathbf{F}_q)$ the group of $\mathbf{F}_q$-rational points of the image of the cocharacter $h_s : G_m \to T$ associated to s. The group $T_s(\mathbf{F}_q)$ is isomorphic to $\mathbf{F}_q^*$.

11 Theorem Iwahori-Matsumoto presentation of the pro-p-Iwahori Hecke ring
The ring $\mathcal{H}^{(1)}$ is a $\mathbf{Z}$-free module of basis $(T_w)_{w\in W^{(1)}}$ with product satisfying
(i) the braid relations $T_{ww'} = T_wT_{w'}$ for all $w, w' \in W^{(1)}$ such that $\ell(ww') = \ell(w) + \ell(w')$,
(ii) the quadratic relations $T_s^2 = q + T_s(\sum_{t\in T_s(\mathbf{F}_q)} T_t)$ for all $s \in S$.

The element $\sum_{t\in T_s(\mathbf{F}_q)} T_t$ commutes with T_s and T_x for $x \in X$, but is not central (§33).

The proof, given from §39 until §45, is an easy extension of the proof of Iwahori and Matsumoto [IM].

One may replace the integer q by an indeterminate $\mathbf{q}$ in the quadratic relation (ii), keeping the finite group $T_s(\mathbf{F}_q)$ inchanged. One gets a $\mathbf{Z}[\mathbf{q}]$-algebra $\mathbf{H}^{(1)}$ with specialisation the ring $\mathcal{H}^{(1)}$ when $\mathbf{q} \to q$. The theorem 11 has many applications, as we know from the theory of the classical Iwahori Hecke ring.

12 Corollary *1) The map $T_w \to q_w = q^{\ell(w)}$ for all $w \in W^{(1)}$, extends by linearity to a ring morphism* ind $: \mathcal{H}^{(1)} \to \mathbf{Z}$.
2) T_w is invertible in $\mathcal{H}^{(1)}[q^{-1}]$ for any $w \in W^{(1)}$ and

$$T_w^* := q^{\ell(w)}T_w^{-1} = T_w + \sum_{w'<w} a_{w'}T_{w'}, \quad a_{w'} \in \mathbf{Z},$$

belongs to $\mathcal{H}^{(1)}$.

In fact, the first property is used in the proof of the quadratic relations in §45. Note that the quadratic relation implies that for $s \in S$:

$$T_s^* := qT_s^{-1} = T_s - \sum_{t\in T_s(\mathbf{F}_q)} T_t.$$

The Iwahori-Matsumoto basis $(T_w)_{w\in W^{(1)}}$ reflects the decomposition $W^{(1)} \simeq \Omega W^{(1)}_{aff}$.

13 Corollary The affine pro-p-Iwahori Hecke ring $\mathcal{H}^{(1)}_{aff}$

1) The free $\mathbf{Z}$*-module of basis* $(T_w)_{w\in W^{(1)}_{aff}}$ *is a subring* $\mathcal{H}^{(1)}_{aff}$ *of* $\mathcal{H}^{(1)}$.

2) The free $\mathbf{Z}$*-module of basis* $(T_u)_{u\in\Omega}$ *is a subring of* $\mathcal{H}^{(1)}$ *isomorphic to* $\mathbf{Z}[\Omega]$.

3) $\mathcal{H}^{(1)}$ *is isomorphic to the twisted tensor product* $\mathbf{Z}[\Omega]\hat{\otimes}\mathcal{H}^{(1)}_{aff}$.

These properties be proved directly. By definition of a twisted tensor product, $(T_u \otimes T_w)_{(u,w)\in\Omega\times W^{(1)}_{aff}}$ is a $\mathbf{Z}$-basis of $\mathbf{Z}[\Omega]\hat{\otimes}\mathcal{H}^{(1)}_{aff}$ and the product satisfies $(T_u \otimes T_w)(T_{u'} \otimes T_{w'}) = T_{uu'} \otimes T_{u'^{-1}wu'}T_{w'}$.

The finite group $T(\mathbf{F}_q)$ embeds in the group of the units of $\mathcal{H}^{(1)}$ by the map $t \mapsto T_t$. There is a good Fourier theory for $T(\mathbf{F}_q) \simeq (\mathbf{F}^*_q)^m$ over a commutative ring R which contains a root of 1 of order $q-1$ and where $q-1$ is invertible.

One writes $R \supset \{\mu_{q-1}, (q-1)^{-1}\}$ for such a ring R; one identifies the group of R-characters of $T(\mathbf{F}_q)$ with the group $\hat{T}(\mathbf{F}_q)$ of $\mathbf{F}_q$-characters of $T(\mathbf{F}_q)$, by the evident W_o-equivariant bijection.

In a direct product $A \oplus B$ of subrings A, B the multiplication of an element of A by an element of B is always 0.

14 Corollary *Let* $R \supset \{\mu_{q-1}, (q-1)^{-1}\}$ *be a commutative ring which contains a root of* 1 *of order* $q-1$ *and where* $q-1$ *is invertible. Any* W_o*-orbit* γ *in* $\hat{T}(\mathbf{F}_q)$ *defines a central idempotent* $\varepsilon_\gamma \in \mathcal{H}^{(1)}_R$,

$$\varepsilon_\gamma = \sum_{\lambda\in\gamma} \varepsilon_\lambda, \quad \varepsilon_\lambda = (q-1)^{-m} \sum_{t\in T(\mathbf{F}_q)} \lambda^{-1}(t)T_t,$$

and the R*-algebra* $\mathcal{H}^{(1)}_R$ *is a direct product of the sub-*R*-algebras* $\mathcal{H}^{(1)}_R\varepsilon_\gamma$,

$$\mathcal{H}^{(1)}_R = \oplus_{\gamma\in W_o\backslash\hat{T}(\mathbf{F}_q)}\ \mathcal{H}^{(1)}_R\varepsilon_\gamma.$$

For any $\lambda \in \hat{T}(\mathbf{F}_q)$ denote

$$S_\lambda = \{s \in S,\ \lambda \text{ trivial on } T_s(\mathbf{F}_q)\}.$$

Each R-algebra $\mathcal{H}_R^{(1)}\varepsilon_\gamma$ has an Iwahori-Matsumoto presentation: $\mathcal{H}_R^{(1)}\varepsilon_\gamma \simeq \mathcal{H}(\gamma)_R = \mathcal{H}(\gamma) \otimes_{\mathbf{Z}} R$ for the following ring $\mathcal{H}(\gamma)$:

15 Definition *The ring $\mathcal{H}(\gamma)$ is the $\mathbf{Z}$-free module of basis $(T_w\varepsilon_\lambda)_{(w,\lambda)\in W\times\gamma}$, of product satisfying*

(i) The unit is $\varepsilon_\gamma = \sum_{\lambda\in\gamma} \varepsilon_\lambda$.

(ii) The idempotent relations: for all $w, w' \in W$ and for all $\lambda, \lambda' \in \gamma$,

$(T_w\varepsilon_\lambda)(T_{w'}\varepsilon_{\lambda'}) = T_wT_{w'}\varepsilon_{\lambda'}$ if $\lambda = w'(\lambda')$, and $(T_w\varepsilon_\lambda)(T_{w'}\varepsilon_{\lambda'}) = 0$ if $\lambda \neq w'(\lambda')$.

(iii) The braid relation: for all $w, w' \in W$ with $\ell(ww') = \ell(w) + \ell(w')$, and $\lambda \in \gamma$,

$T_wT_{w'}\varepsilon_\lambda = T_{ww'}\varepsilon_\lambda$.

(iv) The quadratic relations: let $(s, \lambda) \in S \times \gamma$, then:

$T_s^2\varepsilon_\lambda = q\varepsilon_\lambda + (q-1)T_s\varepsilon_\lambda$, if $s \in S_\lambda$,

$= q\varepsilon_\lambda$, if $s \notin S_\lambda$.

By Fourier theory, the R-module generated by $(T_t\varepsilon_\gamma)_{t\in T(\mathbf{F}_q)}$ is equal to the free R-module of basis $(\varepsilon_\lambda)_{\lambda\in\gamma}$. From the Iwahori-Matsumoto presentation, a basis of $\mathcal{H}_R^{(1)}$ is $(T_wT_t)_{(w,t)\in W\times T(\mathbf{F}_q)}$ hence $\mathcal{H}_R^{(1)}\varepsilon_\gamma$ is equal to the R-free module of basis $(T_w\varepsilon_\lambda)_{(w,\lambda)\in W\times\gamma}$. We have $T_w\varepsilon_\lambda = \varepsilon_{w_o(\lambda)}T_w$ for $w \in W$ with image $w_o \in W_o$ where $w_o(\lambda)(t) = \lambda(w_o^{-1}(t))$ for $t \in T(\mathbf{F}_q)$. Using $T_t\varepsilon_\lambda = \lambda(t)\varepsilon_\lambda$ one sees that $T_s^2\varepsilon_\lambda = q\varepsilon_\lambda + (\sum_{t\in T_s(\mathbf{F}_q)} \lambda(t))T_s\varepsilon_\lambda$.

16 The free $\mathbf{Z}$-module generated by $(\varepsilon_\lambda)_{\lambda\in\gamma}$ in $\mathcal{H}(\gamma)$, denoted by $\mathbf{Z}[\gamma]_{deg}$, is a direct product of rings isomorphic to $\mathbf{Z}$,

$$\mathbf{Z}[\gamma]_{deg} \simeq \oplus^{|\gamma|}\mathbf{Z}.$$

One may replace the integer q by an indeterminate $\mathbf{q}$ in the definition of $\mathcal{H}(\gamma)$. One gets a $\mathbf{Z}[\mathbf{q}]$-algebra $\mathbf{H}(\gamma)$. By the specialization $\mathbf{q} \to 1$, it is isomorphic to the twisted product $\mathbf{Z}[W]\tilde{\otimes}\mathbf{Z}[\gamma]_{deg}$.

Lemma *The ring $\mathcal{H}(\gamma)$ is a deformation of $\mathbf{Z}[W]\tilde{\otimes}\mathbf{Z}[\gamma]_{deg}$.*

17 The stabilizer $C_{W_o}(\gamma)$ in W_o of a W_o-orbit γ in $\hat{T}(\mathbf{F}_q)$, is defined as the *conjugacy class* of the stabilizer in W_o of any element of γ.

Lemma *Suppose that the image of the morphism* $t \mapsto s(t)t^{-1} : T(\mathbf{F}_q) \to T(\mathbf{F}_q)$ *is equal to* $T_s(\mathbf{F}_q)$ *for all* $s \in S$. *Then the rings* $\mathcal{H}(\gamma)$ *and* $\mathcal{H}(\gamma')$ *are isomorphic when the* W_o*-orbits* γ, γ' *in* $\hat{T}(\mathbf{F}_q)$ *have the same stabilizer in* W_o.

Then S_λ defined in §15, is the set of $s \in S$ which fix λ. The hypothesis is satisfied for $G = GL(n, F)$ but not in general ($G = SL(2, F), q$ odd).

If $\phi : \gamma \to \gamma'$ is a W_o-equivariant bijection between two W_o-orbits in $\hat{T}(\mathbf{F}_q)$, the linear map

$$\mathcal{H}(\gamma) \to \mathcal{H}(\gamma'), \quad T_w \varepsilon_\lambda \mapsto T_w \varepsilon_{\phi(\lambda)}, \quad (w, \lambda) \in W \times \gamma$$

is an algebra isomorphism.

Examples

18 The classical Iwahori Hecke ring $\mathcal{H}$ is the free $\mathbf{Z}$-module of basis $(T_w)_{w \in W}$ with product satisfying the braid relations (§11) and the quadratic relation

$T_s^2 = q + (q-1)T_s$ for all $s \in S$.

Under the hypothesis in §17, $\mathcal{H} \simeq \mathcal{H}(\gamma)$ if $|\gamma| = 1$.

19 Define the ring $\mathcal{H}_{reg}$ as the the free $\mathbf{Z}$-module of basis $(T_w)_{w \in W}$ with product satisfying the braid relations (§11) and the quadratic relation

$T_s^2 = q$ for all $s \in S$.

Under the hypothesis in §17, if $|\gamma| = |W_o|$, then $\mathcal{H}(\gamma) \simeq \mathcal{H}_{reg} \tilde{\otimes}_{\mathbf{Z}} \mathbf{Z}[\gamma]_{deg}$, called the regular Iwahori ring.

It is not always possible to find such an orbit γ (think of $GL(2), q = 2$).

One defines also a subregular Iwahori ring associated to γ of stabilizer in W_o equal to $\{1, s\}$ for some $s \in S$.

A general principle is that every property of the classical Iwahori Hecke ring extends to the pro-p-Iwahori Hecke ring, and that the regular Iwahori ring is the easier than the classical Iwahori Hecke ring.

20 We suppose $G = GL(n, F)$. A W_o-orbit in $\hat{T}(\mathbf{F}_q)$ is identified with a S_n-orbit γ in $(\mathbf{F}_q^*)^n$. The centralizer in S_n of γ is the conjugacy class of a subgroup of S_n of the form

$$S_{p(n)} = S_{n_1} \times \ldots \times S_{n_k},$$

for a unique partition $p(n) \sim (n_1 \geq \ldots \geq n_k > 0)$ of length $k \leq q-1$.

We denote $\mathcal{H}_{p(n)}, \mathcal{H}_{R,p(n)}$ the isomorphism classes of $\mathcal{H}(\gamma), \mathcal{H}(\gamma)_R$ (see §15, §16).

One can represent γ by an element $\lambda = (\lambda_1^{n_1}, \ldots, \lambda_k^{n_k}) \in (\mathbf{F}_q^*)^n$ where $\lambda_1, \ldots, \lambda_k$ of $\mathbf{F}_q^*$ are distinct, hence $k \leq q-1$, and $p(n) \sim (n_1 \geq \ldots \geq n_k > 0)$ is a (unique) partition of n. The length k of the partition $p(n)$ is the sum $k = k_1 + \ldots + k_r$ of the multiplicities $k_i > 0$ defined by

$$p(n) \sim (m_1^{k_1}, \ldots, m_r^{k_r}),\ m_1 > m_2 > \ldots > m_r > 0.$$

The number of S_n-orbits γ in $\hat{T}(\mathbf{F}_q)$ giving the same partition $p(n)$ is $\frac{(q-1)\ldots(q-k)}{(k_1)!\ldots(k_r)!}$.

Proposition Pro-p-Iwahori Hecke R-algebra of $GL(n, F)$ for R as in §14.

$$\mathcal{H}_R^{(1)} \simeq \oplus_{p(n)} \oplus^{\frac{(q-1)\ldots(q-k)}{(k_1)!\ldots(k_r)!}} \mathcal{H}_{R,p(n)}$$

where the sum is over the partitions $p(n)$ of n of length $k \leq q-1$, and $k_1, \ldots k_r$ are the multiplicities of $p(n)$.

The Iwahori Hecke ring $\mathcal{H}$ corresponds to $p(n) = (n)$, the regular Iwahori ring $\mathcal{H}_{reg} \tilde{\otimes}_{\mathbf{Z}} \mathbf{Z}[S_n]_{deg}$ corresponds to $p(n) = (1^n)$ (§19) and appears only if $q < n$. The subregular Iwahori ring corresponds to $p(n) = (2, 1^{n-1})$ and appears only if $q < n+1$.

21 To any function $c : p(n) \to c_{p(n)}$ with values in $\mathbf{Z}$ defined on the set of partitions $p(n)$ of n, we associate the function $f_c : \{1, \ldots, n\} \to \mathbf{Q}$ such that

$$f_c(k) = \sum_{p(n)} \frac{c_{p(n)}}{(k_1)! \ldots (k_r)!},$$

sum over the partitions $p(n)$ of n of length k, where (k_i) are the multiplicities of $p(n)$. For the lengths $k = 1, n-1, n$ there is a unique partition of length k, and

$$f_c(1) = c_{(n)}, \quad f_c(n) = \frac{c_{(1^n)}}{n!}, \quad f_c(n-1) = \frac{c_{(2,1^{n-2})}}{(n-2)!}.$$

For other lengths k there is more than one partition of length k.
To any function $f : \{1, \ldots, n\} \to \mathbf{Q}$, one associates the polynomial

$$M_{f,n}(X) = \sum_{1 \leq k \leq n} f(k)(X-1)\ldots(X-k).$$

The number $N_n(q)$ of irreducible unitary polynomials $P \in \mathbf{F}_q[X]$ of dimension n, is also equal to

$$N_n(q) = M_{\phi,n}(q),$$

for a function $\phi : \{1, \ldots, n\} \to (1/n)\mathbf{Z}$ given by two different expressions:

- The Moebius expression (deduced from §4) of $\phi(k)$ for $1 \leq k \leq n$,

$$k!\phi(k) = (-1)^{k+1}[C_k^1 N_n(2) - C_k^2 N_n(3) + C_k^3 N_n(4) - \ldots + (-1)^{k+1} N_n(k+1)].$$

- The Newton expression (deduced from the Newton interpolation formula that I learned from Alain Lascoux),

$$n\phi(k) = \sum_{d|n} \mu(n/d) S_{d-k}(1, \ldots, k+1),$$

where $S_k(x_1, \ldots, x_n)$ is the sum of all the monomials in $x_1, \ldots, x_n$ of total degree k if $k > 0$, $S_o(x_1, \ldots, x_n) = 1$ and $S_k(x_1, \ldots, x_n) = 0$ if $k < 0$. For a prime number n, the Newton expression implies that $\phi(1), \ldots, \phi(p-1)$ are positive integers. We compute the values of $\phi : \{1, \ldots, n\} \to (1/n)\mathbf{Z}$ in some cases:

$$\phi(1) = N_n(2), \quad \phi(n-1) = (n+1)/2, \quad \phi(n) = 1/n.$$

We construct in §25 a function $p(n) \mapsto c_{p(n)}$ on the set of partitions of n with positive values $c_{p(n)} > 0$ such that $N_n(q) = M_{f_c}(q)$.

By §20, the number $M_n(q)$ of irreducible supersingular $\overline{\mathbf{F}}_p$-representations of the pro-p-Iwahori Hecke ring of $GL(n, F)$, of dimension n, where p_F acts by $z \in \overline{\mathbf{F}}_p^*$ fixed, is equal to

$$M_n(q) = M_{f_a,n}(q)$$

where $a_{p(n)}$ is the number of irreducible supersingular $\overline{\mathbf{F}}_p$-representations of $\mathcal{H}_{p(n)}$, of dimension n where p_F acts by z, for any partition $p(n)$ of n. The conjecture (§7) is equivalent to:

22 Conjecture *We have an equality $f_a = \phi$.*

The numerical Langlands correspondence modulo p for the Iwahori, subregular Iwahori, subregular Iwahori rings associated to the partitions $(n), (2, 1^{n-2}), (1^n)$ of n is equivalent to the equalities

$$f_a(1) = N_n(2),\ f_a(n-1) = (n+1)/2,\ f_a(n) = 1/n.$$

$f_a(1) = N_n(2)$ means that the number of irreducible polynomials of dimension n in $\mathbf{F}_2[X]$ is equal to the number of irreducible supersingular $\overline{\mathbf{F}}_p$-representations of the Iwahori Hecke ring of dimension n where p_F acts by z. There is a similar formulation with the regular Iwahori ring and the subregular Iwahori ring.

Suppose G general (§9) until the end of §34 (except for §25). Denote $W_I = \{1\}$ if $I = \emptyset$, and $W_I =$ the group generated by the elements of I. The group W_I is finite if $I \neq S$.

23 Proposition *The $\overline{\mathbf{F}}_p$-characters of $\mathcal{H}^{(1)}_{aff}$ are in bijection with the pairs (λ, I) where $\lambda \in \hat{T}(\mathbf{F}_q)$ and $I \subset S_\lambda$ (defined in §15), called parameters. The character $\chi_{\lambda,I}$ of $\mathcal{H}^{(1)}_{aff,\mathbf{F}_q}$ associated to the parameter (λ, I) is defined by*

$\chi_{\lambda,I}(T_{wt}) = 0$, *if $w \in W_{aff} - W_I$ and $t \in T(\mathbf{F}_q)$,*
$\chi_{\lambda,I}(T_{wt}) = \lambda(t)(-1)^{\ell(w)}$, *if $w \in W_I$ and $t \in T(\mathbf{F}_q)$.*

The proof is given in §47. For any W_o-orbit γ in $\hat{T}(\mathbf{F}_q)$, $\chi_{\lambda,I}$ does not vanish on $\mathcal{H}^{(1)}_{aff,\mathbf{F}_q}\varepsilon_\gamma$ if and only if $\lambda \in \gamma$.

Iwahori case: $\mathcal{H}_{aff,\mathbf{F}_q}$ has 2^n characters χ_I, parametrized by the subsets I of S, $\chi_S(T_{wt}) = (-1)^{\ell(w)}$ is the sign character and $\chi_\emptyset(T_{wt}) = 0$ if $w \neq 1$, and $\chi_\emptyset(T_t) = 1$, is the "trivial" character.
Regular case: $\mathcal{H}^{(1)}_{aff,\mathbf{F}_q}\varepsilon_\gamma$ has $|W_o|$ characters $\chi_\lambda(T_{wt}) = \lambda(t)$, parametrized by $\lambda \in \gamma$.

24 The irreducible $\overline{\mathbf{F}}_p$-representations of $\mathcal{H}^{(1)}$ containing a character of $\mathcal{H}^{(1)}_{aff}$ are described using Clifford theory and §13 3). The action of Ω on

$W_{aff}^{(1)}$ factorizes through its projection Ω_o in W_o. This action induces an action of Ω_o on the parameters (λ, I). The stabilizer of a Ω_o-orbit of (λ, I) is defined as the conjugacy class of the stabilizer $C_{\Omega_o}(\lambda, I))$ of (λ, I) in Ω_o. The group Ω_o is a subgroup of the automorphism group of the affine Dynkin diagram and is commutative when the root system of G is irreducible. The commutative group $\Omega \cap X$ is free of finite rank and embeds in the group of units of the center of $\mathcal{H}^{(1)}$ by $x \mapsto T_x$.

When the root system of G is irreducible, the automorphism group of the affine Dynkin diagram is [IM §1.8]:

$\mathbf{Z}/n\mathbf{Z}$ type A_{n-1},
$\mathbf{Z}/4\mathbf{Z}$ type D_{1+2n},
$\mathbf{Z}/2 \times \mathbf{Z}/2\mathbf{Z}$ type D_{2n},
$\mathbf{Z}/2\mathbf{Z}$ type B_n, C_n, E_7,
$\mathbf{Z}/3\mathbf{Z}$ type E_6,
$\{1\}$ type E_8, F_4, G_2.

Denote b the l.c.m. of the orders of the elements in Ω_o. For a $\overline{\mathbf{F}}_p$-character ω_X of $\Omega \cap X$, denote by $\mathbf{F}_q(\omega_X, \mu_b)/\mathbf{F}_q$ the finite extension generated by μ_b and by the values of ω_X in $\overline{\mathbf{F}}_p$.

Proposition *Suppose that the root system of G is irreducible. Let ω_X be a $\overline{\mathbf{F}}_p$-character of $\Omega \cap X$. There is a bijection between*

- the Ω_o-orbits of parameters (λ, I) of cardinal d,

- the irreducible $\overline{\mathbf{F}}_p$-representations V of $\mathcal{H}^{(1)}$ of dimension d containing a character of $\mathcal{H}^{(1)}_{aff,\overline{\mathbf{F}}_p}$, where $\Omega \cap X$ acts by ω_X.

The bijection has the properties:

1) V contains $\chi_{\lambda,I}$ if and only if the restriction of V to $\mathcal{H}^{(1)}_{aff}$ is equal to the direct sum of the Ω_o-conjugates of $\chi_{\lambda,I}$.

2) If V contains $\chi_{\lambda,I}$, then V factorizes through $\mathcal{H}(\gamma)_{\overline{\mathbf{F}}_p}$ (§14) where γ is the W_o-orbit of λ.

3) The number of V containing $\chi_{\lambda,I}$ is equal to the prime to p part of the order of $C_{\Omega_o}(\lambda, I)$.

4) V is defined over $\mathbf{F}_q(\omega_X, \mu_b)$.

The sign and trivial $\overline{\mathbf{F}}_p$-characters of $\mathcal{H}_{aff}$ extend to characters of $\mathcal{H}^{(1)}$.

All the $\overline{\mathbf{F}}_p$-characters of $\mathcal{H}^{(1)}_{aff}$ extend to a character of $\mathcal{H}^{(1)}$ for the types E_8, F_4, G_2.

25 Proposition *Suppose $G = GL(n, F)$. The number of $\overline{\mathbf{F}}_p$-representations of $\mathcal{H}^{(1)}$ of dimension n containing a character of $\mathcal{H}^{(1)}_{aff,\overline{\mathbf{F}}_p}$, where p_F acts by $z \in \overline{\mathbf{F}}_p^*$ fixed, is equal to $N_n(q)$.*

Equivalently, the number of parameters (λ, I) is equal to q^n, i.e. the number of pairs (x, e) of maps $x : \mathbf{Z}/n\mathbf{Z} \to \mathbf{F}_q^*$, $e : \mathbf{Z}/n\mathbf{Z} \to \{0, 1\}$ such that $e(i) \neq 0$ implies $x(i) = x(i+1)$ for $i \in \mathbf{Z}/n\mathbf{Z}$, is equal to q^n (§59).

Denote $c_{p(n)}$ the number of irreducible $\overline{\mathbf{F}}_p$-representations of dimension n of the algebra $\mathcal{H}_{p(n)}$, containing a character of $\mathcal{H}_{aff}^{(1)}$ and where p_F acts by a fixed $z \in \overline{\mathbf{F}}_p^*$, for any partition $p(n)$ of n. We check in §49 that $c_{p(n)}$ is positive. By (§21)

$$N_n(q) = M_{f_c}(q).$$

The conjecture (§22) is equivalent to:

Conjecture *We have an equality $a_{p(n)} = c_{p(n)}$ for any partition $p(n)$ of n of length $\leq q - 1$.*

26 The definition of a supersingular $\overline{\mathbf{F}}_p$-representation of the pro-p-Iwahori Hecke ring $\mathcal{H}^{(1)}$ uses the existence of another $\mathbf{Z}$-basis reflecting the decomposition $W^{(1)} \simeq W_o X^{(1)}$, that we call the *Bernstein* $\mathbf{Z}$*-basis*.

As for the classical Iwahori Hecke ring, the proof starts by showing the existence of a big commutative subalgebra in the $\mathbf{Z}[q^{-1}]$-algebra $\mathcal{H}^{(1)}[q^{-1}]$. This follows from a general argument [V1, §II.10.1] using:

a) The pro-p-Iwahori group $Iw^{(1)}$ is decomposed with respect to the Borel subgroup $B = TU$ and its opposite $B^- = TU^-$ (§39),

$$Iw^{(1)} = (Iw^{(1)} \cap U(F))(Iw^{(1)} \cap T(F))(Iw^{(1)} \cap U^-(F)).$$

b) T_{y_o} is invertible in $\mathcal{H}^{(1)}[q^{-1}]$, for some $y_o \in X$ image of an element of $T(F)$ which *strictly dilates* $U(F)$ (§12).

The image in X or in $X^{(1)}$ of an element of $T(F)$ which dilates $U(F)$ is called antidominant; it is called dominant if its contracts $U(F)$.

27 Commutative subalgebra *For any commutative ring R where q is invertible, there exists a unique R-algebra injective morphism*

$$\theta = \theta^- : R[X^{(1)}] \to \mathcal{H}_R^{(1)}$$

such that $\theta_x = T_x$ *if* $x \in X^{(1)}$ *is antidominant.*

Any $x \in X^{(1)}$ can be written as $x = y_1 y_2^{-1}$ for $y_1, y_2 \in X^{(1)}$ antidominant, and we have $\theta_x = T_{y_1} T_{y_2}^{-1}$. For x dominant, $\theta_x = T_{x^{-1}}^{-1}$. There a similar morphism θ^+ equal to T_x on the dominant elements as in [L2] [V3], but the morphism θ^- is more natural for the parabolic restriction (the Jacquet functor) and also from the geometric point of view [HP]. When one accepts a square root $q^{1/2}$ in R, it is better to consider the normalized elements (§12):

$$\tilde{T}_w = q_w^{-1/2} T_w, \quad \tilde{\theta}_x = \mathrm{ind}(\theta_x)^{-1/2} \theta_x = \tilde{T}_{y_1} \tilde{T}_{y_2}^{-1}.$$

We have $T_w = \tilde{T}_w = \theta_w = \tilde{\theta}_w$ for an element $w \in (\Omega \cap X) T(\mathbf{F}_q)$ (i.e. of length 0). We denote $\mathcal{A}_R^{(1)} = \mathcal{A}_R^{-,(1)}$ the image of θ (and $\mathcal{A}_R^{+,(1)}$ the image of θ^+). The action of W_o on $X^{(1)}$ gives a linear action on $\mathcal{A}_R^{(1)}$: $w_o(\theta_x) = \theta_{w_o(x)}$ for $(w_o, x) \in W_o \times X^{(1)}$.

One gives now a formula for $T_s \tilde{\theta}_x - \tilde{\theta}_{s(x)} T_s$ for $(s, x) \in S_o \times X^{(1)}$, used in the proof of the second basic property §29 proved in §52. The proof which follows [L2, proposition 3.6] in given in §51.

We give the formula using the usual notations of affine Hecke algebras, where the law on $X = T(F)/T(O_F) \simeq \mathbf{Z}^m$ is written additively. The group $\hat{T}(F)$ of rational characters of $T(F)$ identifies with $\hat{X} \simeq \mathrm{Hom}(T(F)/T(O_F), \mathbf{Z})$. When $G = SL(2, F)$, the unique simple root α generates to $2\hat{X}$. When $G = GL(2, F)$, the unique simple root α does not belong to $2\hat{X}$, because there is a $\mathbf{Z}$-basis (y_1, y_2) of $\hat{X}$ with $\alpha = y_1 - y_2$. Let $s \in S_o$ corresponding to a simple root α and $\tilde{s} \in S$ defined as in [L2, 2.4]. If $s(x) = x + p h_s$ with $p \in \mathbf{Z}$ where $h_s \in X$ is the associated coroot, we have $\tilde{\theta}_{s(x)} = \tilde{\theta}_x \tilde{\theta}_{h_s}^p$ and $\tilde{\theta}_x - \tilde{\theta}_{s(x)} = \tilde{\theta}_x (1 - \tilde{\theta}_{h_s}^p)$

28 Proposition *Let* R *be a commutative ring which contains an invertible square root of* q. *Let* $s \in S_o$ *corresponding to a simple root* α_s *and a coroot* h_s, *and let* $t \in T(\mathbf{F}_q)$, $x \in X$. *Then,*

$$T_s \tilde{\theta}_t - \tilde{\theta}_{s(t)} T_s = 0.$$

If $s(x) = x$, *then* T_s *and* $\tilde{\theta}_x$ *commute. Otherwise,*

$$T_s\tilde{\theta}_x - \tilde{\theta}_{s(x)}T_s = \frac{\tilde{\theta}_x - \tilde{\theta}_{s(x)}}{1-\tilde{\theta}_{h_s}} \sum_{t\in T_s(\mathbf{F}_q)} T_t, \quad \text{if} \quad \alpha_s \notin 2\hat{X},$$

$$T_s\tilde{\theta}_x - \tilde{\theta}_{s(x)}T_s = \frac{\tilde{\theta}_x - \tilde{\theta}_{s(x)}}{1-\tilde{\theta}_{2h_s}} \left[\sum_{t\in T_s(\mathbf{F}_q)} T_t + \tilde{\theta}_{h_s} \sum_{t\in T_{\tilde{s}}(\mathbf{F}_q)} T_t \right], \quad \text{if} \quad \alpha_s \in 2\hat{X}.$$

As well known for the classical Iwahori Hecke algebra, one deduces from §27 and §28 the existence of two Bernstein $\mathbf{Z}[q^{-1}]$-basis of $\mathcal{H}^{(1)}[q^{-1}]$:

29 Bernstein basis *Let R be a commutative ring where q is invertible. Then $(\theta_x T_{w_o})_{(w_o,x)\in W_o\times X^{(1)}}$ and $(T_{w_o}\theta_x)_{(w_o,x)\in W_o\times X^{(1)}}$ are two R-basis of the pro-p-Iwhahori Hecke R-algebra $\mathcal{H}_R^{(1)}$.*

The existence of a Bernstein $\mathbf{Z}$-basis of $\mathcal{H}^{(1)}$ will be proved without using §28, but will be deduced from §27 and from the following result:

30 Integrality *For any $(w_o, x) \in W_o \times X^{(1)}, w = xw_o \in W^{(1)}$, set*

$$E_w = q_w^{1/2}\tilde{\theta}_x\tilde{T}_{w_o}.$$

Then

$$E_w = T_w + \sum_{w'<w} a_{w'}T_{w'}, \quad a_{w'} \in \mathbf{Z}.$$

Same properties are true for $E_w^+ = q_w^{1/2}\tilde{T}_{w_o}\tilde{\theta}_x^+,\ w = w_o x \in W_o X^{(1)}$.

The coefficients of $(E_w)_{w\in W^{(1)}}$ on the Iwahori-Matsumoto basis $(T_w)_{w\in W^{(1)}}$ are *integers* and form a triangular matrix for the Bruhat order $<$ on $W^{(1)}$ (§10). The proof given in §53, relies on the "fundamental lemma" giving the coefficients of $T_{v^{-1}}^{-1}T_w$ on the Iwahori-Matsumoto basis for $v, w \in W^{(1)}$, as in [V3]. From §27, §29, §30, one obtains the important structure results §31, §32, §33; see (§54, §55) for the proofs.

31 Bernstein Z-basis
(i) $(E_w)_{w\in W^{(1)}}$ is a $\mathbf{Z}$-basis of $\mathcal{H}^{(1)}$ (the Bernstein $\mathbf{Z}$-basis).

(ii) $(E_x)_{x\in X^{(1)}}$ *is a* $\mathbf{Z}$*-basis of the commutative ring*

$$\mathcal{A}^{(1)} = \mathcal{A}^{(1)}_{\mathbf{Z}[q^{-1}]} \cap \mathcal{H}^{(1)}.$$

When $G = GL(n, F)$, a presentation of the ring $\mathcal{A}^{(1)}$ is given in §35.

Same properties are true for E^+_w and $\mathcal{A}^{+,(1)}$.

32 Finiteness

(i) $\mathcal{A}^{(1)}$ *is a finitely generated commutative ring.*
(ii) $\mathcal{H}^{(1)}$ *is a finitely generated left* $\mathcal{A}^{(1)}$*-module.*

$\mathcal{A}^{+,(1)}$ satisfies (i) and $\mathcal{H}^{(1)}$ is a finitely generated right $\mathcal{A}^{+,(1)}$-module.

The group W_o acts on $\mathcal{A}^{(1)}$ (it acts on $\mathcal{A}^{(1)}_{\mathbf{Z}[q^{-1}]}$ as in (§27) and $w_o(E_x) = E_{w_o(x)}$ for $x \in X^{(1)}$ because $x \mapsto q_x$ is W_o-invariant [V3, appendice 1]). Denote by $(\mathcal{A}^{(1)})^{W_o}$ the subring of W_o-invariants of $\mathcal{A}^{(1)}$, by $\{x\}$ the W_o-orbit of $x \in X^{(1)}$ and by $z_{\{x\}}$ the sum of the W_o-conjugates of E_x.

33 Centre

(i) $\mathcal{A}^{(1)}$ *is a finitely generated* $(\mathcal{A}^{(1)})^{W_o}$*-module, and* $(\mathcal{A}^{(1)})^{W_o}$ *is a finitely generated commutative ring, of* $\mathbf{Z}$*-basis* $(z_{\{x\}})_{\{x\}\in W_o\backslash X^{(1)}}$.
(ii) The center of $\mathcal{H}^{(1)}$ *is equal to* $(\mathcal{A}^{(1)})^{W_o}$.
(iii) $\mathcal{H}$ *is a finitely generated module over its center.*

The proof of (ii) uses the decomposition §14, because $\tilde{\theta}_x + \tilde{\theta}_{s(x)}$ does not commute in general with T_s when $s \in S_o$ and $x \in X^{(1)}$ (§28).

A similar theory is valid for the affine pro-p-Iwahori Hecke ring $\mathcal{H}^{(1)}_{aff}$. The action of W_o on the commutative subring $\mathcal{A}^{(1)}_{aff}$ of $\mathbf{Z}$-basis $(E_{xt})_{(x,t)\in X_{aff}\times T(\mathbf{F}_q)}$ (§27) and the action of Ω on $\mathcal{H}^{(1)}_{aff}$ (§24) are not compatible.

In characteristic p, we define a "null" character of the center of $\mathcal{H}^{(1)}$ needed in §8 to define a supersingular representation. It is a character as null as possible (it cannot vanish on invertible elements). The group

$(\Omega \cap X)T(\mathbf{F}_q)$ of elements of length 0 in $X^{(1)}$, embeds in the group of units of $\mathcal{A}^{(1)}$ by the map $x \to E_x = T_x$.

34 Definitions *(characteristic p).*

A null character of $\mathcal{A}^{(1)}$ is a character χ of $\mathcal{A}^{(1)}$ such that $x \in X$ and $\chi(E_x) \neq 0$, implies $x \in \Omega \cap X$.

A null character of the center of $\mathcal{H}^{(1)}$ is the restriction of a null character of $\mathcal{A}^{(1)}$.

An irreducible representation of $\mathcal{H}^{(1)}$ where the center acts by a null character is called supersingular.

An irreducible $\overline{\mathbf{F}}_p$-representation of $\mathcal{H}^{(1)}$ is supersingular if and only if it is finite dimensional and contains a null character of $\mathcal{A}^{(1)}$.

Similar definitions can be given for $\mathcal{H}^{(1)}_{aff}$. A null character of $\mathcal{A}^{(1)}_{aff}$ is a character χ of $\mathcal{A}^{(1)}_{aff}$ such that $x \in X_{aff}$ and $\chi(E_x) \neq 0$, implies $x = 1$.

We suppose until the proofs that $G = GL(n, F), n \geq 2$. Among the irreducible $\overline{\mathbf{F}}_p$-representations of $\mathcal{H}^{(1)}$ constructed in §25, we will determine the supersingular ones.

They are those associated to any character ω_X of $\Omega \cap X$ and to the Ω_o-orbit of any supersingular character $\chi_{\lambda,I}$ of $\mathcal{H}^{(1)}_{aff}$. The actions of Ω_o on $\mathcal{A}^{(1)}_{aff}$ and on the Ω_o-orbit of $\chi_{\lambda,I}$ being not compatible, the Ω_o-orbit of a singular character $\chi_{\lambda,I}$ may contain non supersingular characters.

35 There is an explicit description of the commutative algebra $\mathcal{A}^{(1)}$ in $\mathcal{H}^{(1)}$, similar to the explicit descrition of the commutative subalgebra $\mathcal{A}$ in the Iwahori Hecke algebra $\mathcal{H}$ given in [V3].

Notation The notation are not quite those of [V3,3.1] because we consider here θ^- instead of θ^+ (§27). Let B is the upper triangular group, $T(F)$ is the diagonal isomorphic to $(F^*)^n$, the simple roots are $\alpha_i(t) = t_i t_{i+1}^{-1}$ for $t = (t_1, \ldots, t_n) \in T(F)$ for $1 \leq i \leq n-1$, the coweights $X \simeq \mathbf{Z}^n$ identify with the diagonal matrices with coefficients in $p_F^{\mathbf{Z}}$, the antidominant coweights $\omega_t = (0^{n-t}, 1^t)$ have length $(n-t)t$, their conjugates $S_n(\omega_t)$ are the coweights $y_I = (y_i)$ where $y_i = 1$ if $i \in I$ and $y_i = 0$ in $\{1, \ldots, n\} - I$, for any subset I of $\{1, \ldots, n\}$ of cardinal $0 \leq t \leq n$. We denote E_I for E_{y_I} and $Z = E_{\{1,\ldots,n\}}$.

The elements E_I are product of elements $T_{w_i}, T^*_{w_i}$ (§12) for all antidominant coweights. We have [V3 3.1]:

$$E_\emptyset = 1, \quad E_i = q^{n-i} T_{w_{i-1}} T^{-1}_{w_i}, \quad 1 \leq i \leq n.$$

Proposition $G = GL(n, F)$

The ring $\mathcal{A}^{(1)}$ is the commutative $\mathbf{Z}$-algebra generated by $(E_I)_{I \subset \{1,\ldots,n\}}$ and Z^{-1}, with the relations

$$E_\emptyset = 1, \quad Z = E_{\{1,\ldots,n\}}, \quad q^{t(t-1)/2} E_I = \prod_{i \in I} E_i, \quad I \subset \{1, \ldots, n\}, \ t = |I|.$$

A *minimal expression* of E_x for $x \in X^{(1)}$ is an expression of the form :

$$E_x = T_u T^{\varepsilon_1}_{\sigma_1} \ldots T^{\varepsilon_m}_{\sigma_m}, \quad m = \ell(x)$$

where $u \in \Omega T(\mathbf{F}_q)$ has length 0, $\sigma_i \in S$ and $T^{\varepsilon_i}_{\sigma_i} \in \{T_{\sigma_i}, T^*_{\sigma_i}\}$ (§12). The existence of minimal expressions, terminology introduced in [HP §5], is proved as in the classical case [H2 proposition 3.4]. The proof of Haines gives a simple and useful way to obtain a minimal expression, from which one deduces properties of the minimal expressions of E_I for $I \subset \{1, \ldots, n\}$.

36 Proposition $G = GL(n, F)$

i. Any E_x for $x \in X^{(1)}$ has a minimal expression.

ii. For any $1 \leq t \leq n-1$, E_{ω_t} has a minimal expression which contains T_s for all $s \in S_o$.

iii. For any $1 \leq t \leq n-1$ and for any $y \in S_n(\omega_t)$, E_y has a minimal expression which contains $T^*_{s_o}$.

One deduces from §35 and §36 the supersingular representations containing a character of $\mathcal{H}^{(1)}_{aff}$ (§13), see (§57).

37 Theorem $G = GL(n, F)$

Any irreducible $\overline{\mathbf{F}}_p$-representation of $\mathcal{H}^{(1)}$ containing a character of $\mathcal{H}^{(1)}_{aff}$ different from the trivial and the sign characters, is supersingular.

By §25, the theorem implies:

$$N_n(q) \leq M_n(q).$$

The conjecture (§7) is equivalent to:

38 Conjecture $G = GL(n, F)$
Any supersingular irreducible $\overline{\mathbf{F}}_p$*-representation of* $\mathcal{H}^{(1)}$ *of dimension* n *contains a character of* $\mathcal{H}^{(1)}_{aff}$.

Many thanks to Rachel Ollivier and to Christophe Breuil whose work motivated this paper, and to Ulrich Goertze and Alain Lascoux for their interest. Most of these results were presented at the conference on p-adic representations of p-adic groups hold at Luminy in June 2003.

Proofs

Iwahori-Matsumoto presentation of the pro-p-Iwahori Hecke ring
(proof of the theorem §11)

We will prove the theorem 11 for a Chevalley group G over F associated to an irreducible root system as in [IM]. The proof extends naturally to a reducible root system as explained in [IM], and to a connected reductive split group over F.

39 Notations We use the notations of §9. The opposite of B is the Borel subgroup $B^- = TU^- = U^-T$. One chooses a Chevalley system (Bruhat-Tits Groupes réductifs sur un corps local, I.H.E.S. 60, page 53). For any root α of T in $\mathrm{Lie}\, G$, there is a morphism $\Phi_\alpha : SL(2,F) \to G(F)$ such that $T(F)$ contains the $h_\alpha(F^*)$, $N(F)$ is generated by $T(F)$ and the w_α, denoting

$$w_\alpha = \Phi_\alpha \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \quad h_\alpha(t) = \Phi_\alpha \begin{pmatrix} t & 0 \\ 0 & t^{-1} \end{pmatrix}, \quad u_\alpha(a) = \Phi_\alpha \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix}, \ (t,a) \in F^* \times F,$$

and

$$U(*) = \prod_{\alpha>0} U_\alpha(*), \quad U^-(*) = \prod_{\alpha>0} U_{-\alpha}(*)$$

for any order on the positive roots, denoting $U_\alpha(*)$ the group generated by $u_\alpha(a)$ for $a \in *$ where $* \in \{F, O_F, P_F\}$. When α is a simple root $\alpha_i, 1 \leq i \leq n-1$, we replace in the index, α_i by i (so that $w_i = \Phi_i(..)$, etc.). Denote

$$w_o = \Phi_{\alpha_o} \begin{pmatrix} 0 & p_F \\ -p_F^{-1} & 0 \end{pmatrix} = h_{\alpha_o}(p_F) w_{\alpha_o}, \quad h_o = h_{\alpha_o},$$

where α_o is the highest root. Denote $\zeta : N(F) \to W$ the projection, $s_\alpha = \zeta w_\alpha$ for all roots α, and $s_i = \zeta w_i$ for $0 \leq i \leq n-1$.

To follow the notation of Iwahori-Matsumoto, instead of $Iw, Iw^{(1)}$ associated to B as in §9, we will consider the Iwahori subgroup I and the pro-p-Iwahori $I^{(1)}$ associated to B^-,

$$I = U(P_F)B^-(O_F) = B^-(O_F)U(P_F), \quad I^{(1)} = U(p_F)T(1+P_F)U^-(O_F) = U^-(O_F)T(1+P_F)U^+(p_F),$$

(as Iwahori subgroups are conjugate in $G(F)$, theorem 11 can be proved for $I^{(1)}$ instead of $Iw^{(1)}$). We have the decompositions

$$\begin{array}{lllllll} I^{(1)} & = & (I^{(1)})^{(i)} U_{-\alpha_i}(O_F), & (I^{(1)})^{(i)} & = & U(P_F)T(1+P_F)\prod_{\alpha>0,\alpha\neq\alpha_i} U_{-\alpha}(O_F), & 1 \leq i \leq n-1, \\ I^{(1)} & = & (I^{(1)})^{(o)} U_{\alpha_o}(P_F), & (I^{(1)})^{(o)} & = & U^-(O_F)T(1+P_F)\prod_{\alpha>0,\alpha\neq\alpha_o} U_{\alpha}(P_F), \end{array}$$

for a certain order, and $I \cap w_i^{-1} I w_i = \Gamma_i T(\mathbf{F}_q)$ for $0 \leq i \leq n-1$, where $\Gamma_i = I^{(1)} \cap w_i^{-1} I^{(1)} w_i$.

From [IM proposition 2.6 page 31, and its proof], one obtains the following lemma.

40 Lemma *We have*

$$\begin{array}{rcl} \Gamma_i & = & (I^{(1)})^{(i)} U_{-\alpha_i}(P_F), \quad 1 \leq i \leq n-1, \\ \Gamma_o & = & (I^{(1)})^{(o)} U_{\alpha_o}(P_F^2). \end{array}$$

In other terms, using the isomorphism $O_F \simeq \mathbf{F}_q \times P_F$, we have disjoint unions

$$\begin{array}{rcllll} I^{(1)} & = & \cup_{a \in \mathbf{F}_q} & \Gamma_i & u_{-\alpha_i}(a), & 1 \leq i \leq n-1, \\ I^{(1)} & = & \cup_{a \in \mathbf{F}_q} & \Gamma_o & u_{\alpha_o}(p_F a)..... & \end{array}$$

$$\begin{array}{rcll} I^{(1)} w_i I^{(1)} & = & \cup_{a \in \mathbf{F}_q} & I^{(1)} w_i u_{-\alpha_i}(a), \quad 1 \leq i \leq n-1, \\ I^{(1)} w_o I^{(1)} & = & \cup_{a \in \mathbf{F}_q} & I^{(1)} w_o u_{\alpha_o}(p_F a). \end{array}$$

The group $T(\mathbf{F}_q) \simeq T(O_F)/T(1+P_F) \subset W$ is embedded in $T(O_F) \subset N(F)$ by the Teichmüller morphism. One chooses a section σ of the projection $\zeta^{(1)} : N(F) \to W^{(1)}$ such that $\sigma(w_i x t) = s_i \sigma(x) t$ with $\sigma(x) \in T(F)$ for $0 \leq i \leq n-1, x \in X, t \in T(\mathbf{F}_q)$. The kernel of the morphism $\zeta^{(1)}$ is the group $T(1+P_F)$ contained in the pro-p-Iwahori $I^{(1)}$. Hence $I^{(1)}\sigma(w), \sigma(w)I^{(1)}, I^{(1)}\sigma(w)I^{(1)}$ are independent of the choice of the map σ and depends only on $w \in W^{(1)}$.

41 Lemma *Let $w \in W^{(1)}$ and let i be an integer $0 \leq i \leq n-1$. Then*

(i) if $\ell(s_i w) > \ell(w)$, we have $I^{(1)} w_i I^{(1)} \sigma(w) I^{(1)} = I^{(1)} \sigma(s_i w) I^{(1)}$,

(ii) if $\ell(s_i w) < \ell(w)$, we have $I^{(1)} w_i I^{(1)} \sigma(w) I^{(1)} = I^{(1)} \sigma(s_i w) I^{(1)} \cup_{t \in \mathbf{F}_q^*} I^{(1)} h_i(t) \sigma(w) I^{(1)}$ (disjoint union).

This is the analogue of [IM 2.8 page 33]: for $w \in W$ and an integer $0 \leq i \leq n-1$:
- if $\ell(s_i w) > \ell(w)$, we have $I w_i I \sigma(w) I = I \sigma(s_i w) I$,
- if $\ell(s_i w) < \ell(w)$, we have $I w_i I \sigma(w) = I \sigma(s_i w) I \cup I \sigma(w) I$.

We multiply the expression of $I^{(1)}w_iI^{(1)}$ in (§40) by $\sigma(w)I^{(1)}$ on the right side to obtain using the equality $I^{(1)}w_i = I^{(1)}\sigma(s_iw)\sigma(w)^{-1}$:

$$\begin{array}{lcll} I^{(1)}w_iI^{(1)}\sigma(w)I^{(1)} & = & I^{(1)}\sigma(s_iw)\ \sigma(w)^{-1}U_{-\alpha_i}(O_F)\sigma(w)\ I^{(1)} & 1 \le i \le n-1, \\ I^{(1)}w_oI^{(1)}\sigma(w)I^{(1)} & = & I^{(1)}\sigma(s_ow)\ \sigma(w)^{-1}U_{\alpha_o}(P_F)\sigma(w)\ I^{(1)}. & \end{array}$$

a) Suppose $\ell(s_iw) > \ell(w)$. The pro-p-groups $\sigma(w)^{-1}U_{-\alpha_i}(O_F)\sigma(w)$ if $1 \le i \le n-1$, and $\sigma(w)^{-1}U_{\alpha_o}(P_F)\sigma(w)$ are contained in I hence in $I^{(1)}$, by [IM proof of 2.8 page 33]. We deduce (i).

b) Suppose $\ell(s_iw) < \ell(w)$. Then we use the detailed expression for $I^{(1)}w_iI^{(1)}$ in (§40) to obtain

$I^{(1)}w_iI^{(1)}\sigma(w)I^{(1)} = \cup_{a\in\mathbf{F}_q}I^{(1)}\sigma(s_iw)\sigma(w)^{-1}u_{-\alpha_i}(a)\sigma(w)I^{(1)}$

$= I^{(1)}\sigma(s_iw)I^{(1)} \cup_{t\in\mathbf{F}_q^*} I^{(1)}w_iu_{-\alpha_i}(t)\sigma(w)I^{(1)}$ for $1 \le i \le n$,

$I^{(1)}w_oI^{(1)}\sigma(w)I^{(1)} = \cup_{a\in\mathbf{F}_q}I^{(1)}\sigma(s_ow)\sigma(w)^{-1}u_{\alpha_o}(p_Fa)\sigma(w)I^{(1)}$

$= I^{(1)}\sigma(s_ow)I^{(1)} \cup_{t\in\mathbf{F}_q^*} I^{(1)}w_ou_{\alpha_o}(p_Ft)\sigma(w)I^{(1)}$.

The terms in $t \in \mathbf{F}_q^*$ are written

$I^{(1)}w_iu_{-\alpha_i}(t)\sigma(w)I^{(1)} = I^{(1)}\ w_iu_{-\alpha_i}(t)w_i^{-1}\ w_i\sigma(w)I^{(1)}$,

$I^{(1)}w_ou_{\alpha_o}(p_Ft)\sigma(w)I^{(1)} = I^{(1)}\ w_ou_{\alpha_o}(p_Ft)w_o^{-1}\ w_o\sigma(w)I^{(1)}$.

The elementary formulas in $SL(2,F)$

$$\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ t & 1 \end{pmatrix}\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & -t \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ -t^{-1} & 1 \end{pmatrix}\begin{pmatrix} -t & 0 \\ 0 & -t^{-1} \end{pmatrix}\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ -t^{-1} & 1 \end{pmatrix}$$

$$\begin{pmatrix} 0 & p_F \\ -p_F^{-1} & 0 \end{pmatrix}\begin{pmatrix} 1 & p_Fa \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 0 & -p_F \\ p_F^{-1} & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ -p_F^{-1}a & 1 \end{pmatrix},$$

$$\begin{pmatrix} 1 & 0 \\ -p_F^{-1}t & 1 \end{pmatrix} = \begin{pmatrix} 1 & -p_Ft^{-1} \\ 0 & 1 \end{pmatrix}\begin{pmatrix} t^{-1} & 0 \\ 0 & t \end{pmatrix}\begin{pmatrix} 0 & p_F \\ -p_F^{-1} & 0 \end{pmatrix}\begin{pmatrix} 1 & -p_Ft^{-1} \\ 0 & 1 \end{pmatrix},$$

and the homomorphism $\Phi_{\alpha_i} : SL(2,F) \to G$, imply that

$$\begin{array}{lcll} w_iu_{-\alpha_i}(t)w_i^{-1} & \subset & I^{(1)}h_i(-t)w_iI^{(1)}, & 1 \le i \le n-1, \\ w_ou_{\alpha_o}(p_Ft)w_o^{-1} & \subset & I^{(1)}h_o(t^{-1})w_oI^{(1)} & \end{array}$$

(recall $w_o = h_o(p_F)w_{\alpha_o} = w_{\alpha_o}h_o(p_F^{-1})$ and $h_o(p_Ft)w_{\alpha_o} = h_o(t)w_o$). Hence

$I^{(1)}\ w_iu_{-\alpha_i}(t)w_i^{-1}\ w_i\sigma(w)I^{(1)} \subset I^{(1)}h_{\alpha_i}(-t)w_iI^{(1)}\sigma(s_iw)I^{(1)}$ for $1 \le i \le n-1$,

$I^{(1)}\ w_ou_{\alpha_o}(p_Ft)w_o^{-1}\ w_o\sigma(w)I^{(1)} \subset I^{(1)}h_o(t^{-1})w_oI^{(1)}w_o\sigma(w)I^{(1)}$.

Using (i) with $\ell(s_i w) < \ell(s_i s_i w)$ and $s_i^2 = -1$, we have for $0 \leq i \leq n$, and $a = -t$ or t^{-1},

$I^{(1)} w_i I^{(1)} \sigma(s_i w) I^{(1)} = I^{(1)} \sigma(s_i s_i w) I^{(1)} = I^{(1)} h_i(-1) \sigma(w) I^{(1)}$.

For $t \in O_F^*$, $I^{(1)} h_i(t) = h_i(t) I^{(1)}$ depends only on the image of t in $\mathbf{F}_q^*$ and $I^{(1)} h_i(t) w_i I^{(1)} \sigma(s_i w) I^{(1)}$ is contained in $I^{(1)} h_i(t) I^{(1)} h_{\alpha_i}(-1) \sigma(w) I^{(1)}$ $= I^{(1)} h_{\alpha_i}(-t) \sigma(w) I^{(1)}$. The maps $t \to -t$ or $t \to -t^{-1}$ are bijections on $\mathbf{F}_q^*$ and one obtains (ii).

Remark By the property (ii) of the proposition, $(G(F), I^{(1)}, N(F))$ is not a generalized BN-pair in the sense of [M] The properties of 3.2 (loc. cit.) are satisfied except (iii) (a). The property (ii) is the essential difference with the Iwahori case. The only reason not to give the Iwahori-Matsumoto description of the pro-p-Iwahori Hecke algebra for a *general* reductive connected group over F, comes from the fact that the property (ii) is more complicated when the group is not split. (The reader interested in describing $\mathcal{H}^{(1)}$ for G general, may find useful to know the notion of split BN-pair in characteristic p defined by Cabanes and Enguehard in their forthcoming book on representations of reductive finite groups (definition 2.20), and that references for a complete proof of the Iwahori-Matsumoto description of the Iwahori Hecke algebra for G exist, by combining [M], Masumoto H. Générateurs et relations des groupes de Weyl généralisés. C.R.A.S. Paris 258 (1964), 3419-3422, and Iwahori N. Generalized Tits system (Bruhat decomposition) on p-adic semisimple groups, Proc. of Symp. in pure math. IX, page 79, AMS 1966).

42 Theorem *$G(F) = \cup_{w \in W^{(1)}} I^{(1)} \sigma(w) I^{(1)}$ (disjoint union).*

This is a corollary of the decomposition $G(F) = \cup_{w \in W} I \sigma(w) I$ ([IM theorem 2.16 page 36] and for G general [M 3.3 (b)]).

Use the semidirect products $W^{(1)} = WT(\mathbf{F}_q)$, $I = T(\mathbf{F}_q) I^{(1)}$. For $t \in T(\mathbf{F}_q)$ non trivial and $w \in W$, we have $\sigma(wt) = \sigma(w)t$ and the double classes $I^{(1)} \sigma(w) t I^{(1)}$ and $I^{(1)} \sigma(w) I^{(1)}$ are disjoint because $tx = \sigma(w)^{-1} y \sigma(w)$ with $x, y \in I^{(1)}$ is impossible as the closed subgroup of I generated by tx is not a pro-p-group.

43 Lemma *The normalizer of $I^{(1)}$ in $G(F)$ is equal to the normalizer of I in $G(F)$.*

Proof. An element of $G(F)$ which normalizes I normalizes its pro-p-radical $I^{(1)}$. The converse is true because $\sigma(w)$, $(w = w_o x t \in W_o X T(\mathbf{F}_q))$, normalizes $T(O_F)$ and sends $u_\alpha(t)$

on $u_{w_o(\alpha)}(\pm p_F^{(x,w_o(\alpha))}t)$ for all roots α. One deduces that if $\sigma(w)$ normalizes $I^{(1)}$, it will normalize I.

By [IM 2.4 page 34], the normalizer of I in $G(F)$ is $I\Omega I$.

44 Proposition *$[I : I \cap g^{-1}Ig] = [I^{(1)} : I^{(1)} \cap g^{-1}I^{(1)}g]$ for any $g \in G(F)$.*

Proof. As a function on $G(F)$, the index $[I^{(1)} : I^{(1)} \cap g^{-1}I^{(1)}g]$ is left and right invariant by $I^{(1)}$. We may suppose that $g = n \in N(F)$ because $G(F) = I^{(1)}N(F)I^{(1)}$. Then $I \cap n^{-1}In = T(\mathbf{F}_q)(I^{(1)} \cap n^{-1}I^{(1)}n)$ as in §39, and $[I : I \cap n^{-1}In] = [I^{(1)} : I^{(1)} \cap n^{-1}I^{(1)}n]$ because the order of $T(\mathbf{F}_q)$ is prime to the pro-order of $I^{(1)}$.

45 The proof of the theorem §11 uses §41 , §42, §44.

a) The pro-p-Iwahori-Hecke ring $\mathcal{H}(G, I^{(1)})$ is defined as the endomorphism algebra $\mathrm{End}_{\mathbf{Z}G(F)}\, \mathbf{Z}[I^{(1)}\backslash G(F)]$, the group $G(F)$ acting on $\mathbf{Z}[I^{(1)}\backslash G(F)]$ by the regular representation [Bki GAL IV §2 ex.22]. By §42, the value at $I^{(1)}$ identifies $\mathcal{H}(G, I^{(1)})$ with the free $\mathbf{Z}$-module generated by the double cosets $I^{(1)}\sigma(w)I^{(1)}$, $w \in W^{(1)}$. The double coset $I^{(1)}\sigma(w)I^{(1)}$ seen as an element in $\mathcal{H}(G, I^{(1)})$, is denoted by T_w and called a **basic** element of the **Iwahori-Matsumoto basis** $(T_w)_{w\in W^{(1)}}$ of $\mathcal{H}(G, I^{(1)})$.

b) The multiplication is defined by

$$T_xT_y = \sum_z m_{x,y}^z T_z,$$

for $x, y, z \in W^{(1)}$, where the structure constants are defined as the number of cosets of the form $I^{(1)}x$ in the set $(I^{(1)}\sigma(x)^{-1}I^{(1)}\sigma(z)) \cap (I^{(1)}\sigma(y)I^{(1)})$,

$$m_{x,y}^z = |I^{(1)}\backslash(I^{(1)}\sigma(x)^{-1}I^{(1)}\sigma(z) \cap I^{(1)}\sigma(y)I^{(1)})|.$$

The support of T_xT_y is the set of T_z such that $m_{x,y}^z \neq 0$. We have $m_{x,y}^z \neq 0$ if and only if $I^{(1)}\sigma(z)I^{(1)} \subset I^{(1)}\sigma(x)I^{(1)}\sigma(y)I^{(1)}$. The map

$$\mathrm{ind} : \mathcal{H}(G, I^{(1)}) \to \mathbf{Z}, \quad \sum_{w\in W^{(1)}} a_w T_w \to \sum_{w\in W^{(1)}} a_w [I^{(1)} : I^{(1)} \cap \sigma(w)I^{(1)}\sigma(w)^{-1}],$$

where $a_w \in \mathbf{Z}$, is a ring morphism [V4 I.3.5]. One deduces from §44 and [IM 3.2 page 44] that $\mathrm{ind}(T_w) = q^{\ell(w)}$. This proves the first property of §12.

c) The braid relations in §11 result from the part (i) of the lemma §41, and the quadratic relations from the part (ii) of §41 : for $0 \leq i \leq n-1$,

$$T_{s_i}^2 = a_{i,o} + \sum_{t \in \mathbf{F}_q^*} a_{i,t} T_{h_i(t)} T_{s_i}$$

for positive integers $a_{i,o}, a_{i,t}$ given by explicit formulas

$$a_{i,o} = |I^{(1)} \backslash (I^{(1)} w_i^{-1} I^{(1)} \cap I^{(1)} w_i I^{(1)})| = |I^{(1)} \backslash I^{(1)} w_i I^{(1)}| = q,$$

$$a_{i,t} = |I^{(1)} \backslash (I^{(1)} w_i^{-1} I^{(1)} h_i(t) w_i \cap I^{(1)} w_i I^{(1)})|.$$

Applying the ring morphism ind : $\mathcal{H}(G, I^{(1)}) \to \mathbf{Z}$ to the formula of $T_{s_i}^2$, we get $q^2 = a_{i,o} + q \sum_{t \in \mathbf{F}_q^*} a_{i,t}$. Since $a_{i,o} = q$, we obtain $\sum_{t \in \mathbf{F}_q^*} a_{i,t} = q - 1$. As each $a_{i,t}$ is an integer ≥ 1, the only possibility is $a_{i,t} = 1$ for any $t \in \mathbf{F}_q^*$.

47 Proof of proposition §23

It is clear that $\chi_{\lambda,I}$ is a character of $\mathcal{H}^{(1)}_{aff,\mathbf{F}_q}$.

Let χ be a character of $\mathcal{H}^{(1)}_{aff,\mathbf{F}_q}$. The restriction of χ to $T(\mathbf{F}_q)$, naturally embedded in $\mathcal{H}^{(1)}_{aff,\mathbf{F}_q}$ by $t \mapsto T_t$, is a character $\lambda : T(\mathbf{F}_q) \to \mathbf{F}_q^*$. The quadratic relations (§11) imply $\chi(T_s)^2 = \chi(T_s) \sum_{t \in T_s(\mathbf{F}_q)} \lambda(t)$ for all $s \in S$.

- If λ is not trivial on $T_s(\mathbf{F}_q)$ then $\sum_{t \in T_s(\mathbf{F}_q)} \lambda(t) = 0$ hence $\chi(T_s) = 0$ if s does not belong to S_λ.

- If λ is trivial on $T_s(\mathbf{F}_q)$, i.e. $s \in S_\lambda$, then $\sum_{t \in T_s(\mathbf{F}_q)} \lambda(t) = -1$ because the order of $T_s(\mathbf{F}_q) \simeq \mathbf{F}_q^*$ is equal to -1 in a ring of characteristic p, hence $\chi(T_s)^2 = -\chi(T_s)$.

The subset of S_λ such that $\chi(T_s) = -1$ is I. Using the braid relations (§11) we see that $\chi = \chi_{\lambda,I}$.

The character $\chi_{\lambda,I}$ does not vanish on $\varepsilon_\gamma \mathcal{H}^{(1)}_{aff,\mathbf{F}_q}$ if and only if $\chi_{\lambda,I}(\varepsilon_\gamma) \neq 0$. This is equivalent to $\lambda \in \gamma$.

48 Proof of §25

Let $k \subset \overline{\mathbf{F}}_p$ be a field containing $\mathbf{F}_q(\omega_X, \mu_a)$. For $\chi = \chi_{\lambda,I}$, denote Ω^χ the group of $u \in \Omega$ such that $\chi^u = \chi$ and Ω_o^χ the projection of Ω^χ in W_o. The characters χ^{u_o}, $u_o \in \Omega_o / \Omega_o^\chi$, are the distinct conjugates of χ by Ω and Ω^χ is the inverse image of Ω_o^χ in Ω.

The $\mathbf{Z}$-module $(\mathcal{H}^{(1)})^\chi$ of basis T_{uw}, $(u,w) \in \Omega^\chi \times W_{aff}$ is a subalgebra of $\mathcal{H}^{(1)}$ isomorphic to $\mathbf{Z}[\Omega^\chi] \hat{\otimes} \mathcal{H}^{(1)}_{aff}$ by §13. The set of characters χ_o of Ω^χ which extend the k-character w_X of

$\Omega \cap X$ is not empty and in bijection with the set of k-characters χ' of $(\mathcal{H}^{(1)})^\chi$ which extend χ and where $\Omega \cap e^X$ act by ω_X. If χ' is one of them, the other ones are $\chi'\xi$ for the k-characters ξ of Ω_o^χ inflated to Ω^χ. The induced representation

$$V = \mathcal{H}^{(1)} \otimes_{(\mathcal{H}^{(1)})^\chi} \chi'$$

is absolutely irreducible of dimension the index $[\Omega_o : \Omega_o^\chi]$, its restriction to $\mathcal{H}^{(1)}_{aff}$ is $\oplus \chi^{u_o}$ the sum above $u_o \in \Omega_o/\Omega_o^\chi$. This process gives a bijection between

- the isomorphism classes of the irreducible k-representations V of $\mathcal{H}^{(1)}$ containing χ, where $\Omega \cap X$ acts by ω_X,
- the k-characters χ' of $(\mathcal{H}^{(1)})^\chi$ extending χ, with restriction ω_X on $\Omega \cap X$,
- the k-characters ξ of Ω_o^χ.

The number of ξ is equal to the cardinal of Ω_o^χ if and only if $(p, \Omega_o^\chi) = 1$.

49 Proof of : $c_{p(n)}$ is positive (§25).

Let $p(n) = (n_1 \geq n_2 \geq \ldots \geq n_k > 0)$ be a partition of n. We want to find a parameter (λ, I) with trivial stabilizer in Ω_o (called a Ω_o-regular parameter) and λ of partition $p(n)$ (§20).

- Choose λ with $\lambda_1 = \ldots = \lambda_{n_1}, \lambda_{n_1+1} = \ldots = \lambda_{n_1+n_2}$, etc. with $\lambda_1, \lambda_{n_1+1}, \ldots, \lambda_{n_{k-1}+1}$ all distinct. The partition of λ is $p(n)$.

- If the stabilizer of λ in Ω_o is trivial, then the Ω_o-orbit of (λ, I) for any $I \subset S_\lambda$, by instance $I = \emptyset$, has n elements, hence $c_{p(n)} > 0$.

- If the stabilizer of λ in Ω_o is not trivial, then λ is fixed by Ω_o, $p(n) = n$ and $S_\lambda = S$ because a generator τ of $\Omega_o \simeq \mathbf{Z}/n\mathbf{Z}$ acts on $S = \{s_i = (i, i+1),\ i \in \mathbf{Z}/n\mathbf{Z}\}$ by $s_i \mapsto s_{i+1}$. The Ω_o-orbit of (λ, I) for any $I \subset S$ with one element, has n elements, hence $c_{p(n)} > 0$.

50 Computations of f_c (§37)

Iwahori case. The number of subsets I of $\{1, \ldots, n\}$ such that the w_o-orbit of I has d elements is equal to $dc_{(n),d}$. The number of subsets of $\{1, \ldots, n\}$ is equal to the number of elements of a finite field $\mathbf{F}_{2^n}$. Hence

$$2^n = \sum_{d|n} d\, c_{(n),d} = \sum_{d|n} dN_d(2).$$

We deduce that $c_{(n)} = N_n(2)$. By §22, $f_c(1) = c_{(n)}$.

Subregular case. When $n = 2$, the subregular case is the Iwahori case. Suppose $n \geq 3$ and $n - 1 \geq q - 1$. Choose $n-1$ distinct elements $a, b_1, \ldots, b_{n-2}$ in $\mathbf{F}_q^*$. The S_n-orbit of $(a, a, b_1, \ldots, b_{n-2}) \in (\mathbf{F}_q^*)^n$ has $n!/2$ elements which form $n!/2n$ regular Ω_o-orbits. The set S_λ

has one element when λ is the Ω_o-orbit of $(a, a, *, \dots, *)$. Such λ give $2(n-2)!$ parameters. The set S_λ is empty when λ is the Ω_o-orbit of $(a, *, \dots, a, *, \dots, *)$ where S_λ is empty. Hence $c_{(2,1^{n-2})} = 2(n-2)! + (n!/2n) - (n-2)! = (n-2)!(n+1)/2$. By §22, $f_c(1) = c_{(2,1^{n-2})}/(n-2)!$.

Regular case. Suppose $n \leq q-1$ and choose n distinct elements $a_1, \dots, a_n$ in $\mathbf{F}_q^*$. The S_n-orbit of $(a_1, \dots, a_n) \in (\mathbf{F}_q^*)^n$ has $n!$ elements which form $(n-1)!$ regular Ω_o-orbits with S_λ empty. Hence $c_{(1^n)} = (n-1)!$. By §22, $f_c(1) = c_{(1^n)}/n!$.

$n = 4$. Besides the Iwahori, the subregular and the regular partitions, there are two partitions $(3,1), (2,2)$ of 4 of length 2, and $f_c(2) = c_{(3,1)} + c_{(2,2)}/2$ by §22. Suppose $q \neq 2$ and choose two distinct elements a, b in $\mathbf{F}_q^*$.

The S_4-orbit of $\lambda = (a, a, a, b) \in (\mathbf{F}_q^*)^4$ is a regular Ω_o-orbit. The set S_λ has two elements. Hence $c_{(3,1)} = 4$.

The S_4-orbit of $(a, a, b, b) \in (\mathbf{F}_q^*)^4$ has six elements $(a, a, b, b), (b, a, a, b), (b, b, a, a), (a, b, b, a)$ and is the union of two Ω_o-orbits, one regular and $(a, b, a, b), (b, a, b, a)$. For λ in the regular w_o-orbit, S_λ has two elements. Hence $c_{(2,2)} = 4$.

$n = 5$. Besides the Iwahori, the subregular and the regular partitions, there are two partitions $(4,1), (3,2)$ of 4 of length 2, without multiplicities, and two partitions $(3,1,1), (2,2,1)$ of length 3, with multiplicities. We have $f_c(2) = c_{(4,1)} + c_{(3,2)}$ and $f_c(3) = (c_{(3,1,1)} + c_{(2,2,1)})/2$ by §22.

Suppose $q \neq 2$ and choose two distinct elements a, b in $\mathbf{F}_q^*$.

The S_5-orbit of $\lambda = (a, a, a, a, b) \in (\mathbf{F}_q^*)^5$ is a regular Ω_o-orbit and S_λ has three elements. Hence $c_{(4,1)} = 8$.

The S_5-orbit of $(a, a, a, b, b) \in (\mathbf{F}_q^*)^5$ has ten elements, union of the regular w_o-orbits of (a, a, a, b, b) and of (a, a, b, a, b) where S_λ has respectively three and one elements. Hence $c_{(3,2)} = 10$.

Suppose $q \neq 2, 3$ and choose three distinct elements a, b, c in $\mathbf{F}_q^*$.

The S_5-orbit of $(a, a, a, b, c) \in (\mathbf{F}_q^*)^5$ has twenty elements which form four regular w_o-orbits represented by (a, a, a, b, c) and (a, a, a, c, b) where S_λ has two elements, by (a, b, a, a, c) and by (a, b, a, c, a) where S_λ has one element. Hence $c_{(3,1,1)} = 12$.

The S_5-orbit of $(a, a, b, b, c) \in (\mathbf{F}_q^*)^5$ has thirty elements which form six regular w_o-orbits represented by (a, a, b, b, c) or (b, b, a, a, c) where S_λ has two elements, by (a, b, b, a, c) or (b, a, a, b, c) where S_λ has one element, and by (a, b, a, c, b) and (a, b, a, b, c) where S_λ is empty. Hence $c_{(2,2,1)} = 14$.

51 Proof of §28 (additive notation)

- When $t \in T(\mathbf{F}_q)$, we have $\tilde{\theta}_t = T_t$ and $T_s T_t = T_{s(t)} T_s$ by the braid relation because $\ell(st) = \ell(s) + \ell(t)$.

- When $s \in S_o, x \in X, s(x) = x$, the length formula [IM] implies $\ell(sx) = \ell(xs) = \ell(x) + \ell(s)$ and T_s and T_x commute by the braid relation.

One can write $x = y_1 - y_2$ with y_1, y_2 antidominant fixed by s. Hence θ_x and T_s commute.

If the relation

$$T_s\tilde{\theta}_x - \tilde{\theta}_{s(x)}T_s = \frac{\tilde{\theta}_x - \tilde{\theta}_{s(x)}}{1-\tilde{\theta}_h} \sum_{t\in T_s(\mathbf{F}_q)} T_t,$$

is true for x and for x', then the relation is true for xx' and x^{-1}. Indeed, for $x + x'$ multiply by $\tilde{\theta}_{x'}$ on the left the relation for x, and multiply by $\tilde{\theta}_{s(x')}$ on the right the relation for x', then substract. For x^{-1} multiply by $\tilde{\theta}_x^{-1}$ on the left and by $\tilde{\theta}_{s(x)}^{-1}$ and on the right the relation for x.

If the relation

$$T_s\tilde{\theta}_x - \tilde{\theta}_{s(x)}T_s = \frac{\tilde{\theta}_x - \tilde{\theta}_{s(x)}}{1-\tilde{\theta}_{2h}} \left[\sum_{t\in T_s(\mathbf{F}_q)} T_t + \tilde{\theta}_h \sum_{t\in T_{\tilde{s}}(\mathbf{F}_q)} T_t\right]$$

is true for x, x' it is true for $x + x'$ and $-x$, by similar arguments.

Let $s \in S_o, x \in X, s(x)\neq x$. When x is antidominant then $s(x) = x+ph_s$ with $p > 1$, the braid relation implies [L2 2.3 page 603]:

a) $\ell(sx) = \ell(x) - 1$

b) $\ell(xsx) = 2\ell(x) - 2p + 1$

c) $x + s(x) = ph_s + 2x$ is antidominant, and $\ell(x + s(x)) = 2\ell(x) - 2p$,

- Suppose that $\alpha_s \notin 2\hat{X}$. Then any $x \in X$ can be written as $nx + x'$ with $n \in \mathbf{Z}$, x antidominant and $s(x) = x + h_s$, $s(x') = x'$. It is enough to prove §28 is for x, i.e.

$\tilde{\theta}_{s(x)}T_s = T_s^*\tilde{\theta}_x$.

By a), b), c), we have: $T_{x+s(x)}T_s = T_{xsx}$, $T_x = T_sT_{sx}$, $T_{xsx} = T_xT_{sx}$ hence $\theta_xT_s^{-1}\theta_xT_s^{-1} = T_xT_s^{-1}T_xT_s^{-1} = T_{x+s(x)} = \theta_{2x+h_s} = \theta_x\theta_{s(x)}$. Now multiply on the left by $T_s\theta_x^{-1}$ and on the right by T_s to obtain $T_s\theta_{s(x)}T_s = \theta_x$. We deduce (§12): $\mathrm{ind}(\theta_x) = q_s^2\ \mathrm{ind}(\theta_{s(x)})$ and $T_s\tilde{\theta}_{s(x)}T_s = q_s\tilde{\theta}_x$. Multiply on the left by T_s^{-1} and replace $q_sT_s^{-1}$ by T_s^*.

- Suppose that $\alpha_s \in 2\hat{X}$. Then X contains a unique antidominant element x with $s(x) = x + 2h_s$ and $s'(x) = x$ for all $s' \in S - \{s\}$ (compare

with [L2 2.5 page 604]). Any element of X can be written as $nx + x'$ with $n \in \mathbf{Z}$ and $s(x') = x'$. It is enough to prove §28 for x, i.e.

$T_s^* \tilde{\theta}_x = \tilde{\theta}_{s(x)} T_s + \tilde{\theta}_{x+h_s} (\sum_{t \in T_{\tilde{s}}(\mathbf{F}_q)} T_t)$.

Following Lusztig (loc. cit.), using only the braid relations, one finds two elements $w', w'' \in W$ such that $T_{xsx} = T_{w''w'} = T_{w''} T_{w'}$, $T_{2x+h_s} = T_{w''} T_{\tilde{s}} T_{w'}$, $T_x T_{sx} = T_{w''} T_{\tilde{s}}^2 T_{w'}$ (same proof than loc.cit.). With the braid relations, one deduces:

$T_x^{-1} T_{w''} T_{w'} = T_x^{-1} T_{xsx} = T_x^{-1} T_{x+s(x)} T_s$ by b) and c) $= T_x^{-1} T_{2x+2h_s} T_s = \theta_{s(x)} T_s$, because $w = 2x + 2h_s$ is antidominant by c).

$T_x^{-1} T_{w''} T_{\tilde{s}} T_{w'} = T_x^{-1} T_{w''} T_{\tilde{s}} T_{w'} = T_x^{-1} T_{2x+h_s} = \theta_{x+h_s}$, because $x + h_s$ is antidominant hence $2x + h_s$ is antidominant.

$T_x^{-1} T_{w''} T_{\tilde{s}}^2 T_{w'} = T_x^{-1} T_x T_{sx} = T_{sx} = T_s^{-1} T_x = T_s^{-1} \theta_x$.

We set $\gamma = T_{w'}, \gamma' = T_x^{-1} T_{w''}$ and we have $\theta_{s(x)} T_s = \gamma' \gamma$, $\theta_{x+h_s} = \gamma' T_{\tilde{s}} \gamma$, $T_s^{-1} \theta_x = \gamma' T_{\tilde{s}}^2 \gamma$. These relations were proved using only the braid relations. We deduce from §12, $q_s^{-1/2} \tilde{\theta}_{s(x)} T_s = \gamma' \gamma \ \mathrm{ind}(\gamma\gamma')^{-1/2}$, $q_{\tilde{s}}^{1/2} \tilde{\theta}_{x+h_s} = \gamma' T_{\tilde{s}} \gamma \ \mathrm{ind}(\gamma\gamma')^{-1/2}$, $q_{\tilde{s}} q_s^{1/2} T_s^{-1} \tilde{\theta}_x = \gamma' T_{\tilde{s}}^2 \gamma \ \mathrm{ind}(\gamma\gamma')^{-1/2}$. Then the quadratic relation of $T_{\tilde{s}}$ (§11) gives

$q T_s^{-1} \tilde{\theta}_x = \tilde{\theta}_{s(x)} T_s + \tilde{\theta}_{x+h_s} (\sum_{t \in T_{\tilde{s}}(\mathbf{F}_q)} T_t)$

Replace $q T_s^{-1}$ by T_s^*.

52 Proof of §29.

a) By §28, the R-module generated by $(\theta_x T_{w_o})_{(w_o,x) \in W_o \times X^{(1)}}$ and the R-module generated by $(T_{w_o} \theta_x)_{(w_o,x) \in W_o \times X^{(1)}}$ are equal to $\mathcal{H}_R^{(1)}$. The argument is as in [L2 proof of 3.7 page 609].

b) $(\theta_x T_{w_o})_{(w_o,x) \in W_o \times X^{(1)}}$ are linearly independent over R. The proof is as in [L2 3.4 page 607], using that for $y \in X$ antidominant and $w_o \in W_o$ one has $\ell(y w_o) = \ell(y) + \ell(w_o)$ hence $\theta_y T_{w_o} = T_y T_{w_o} = T_{y w_o}$, and that for a finite set Y in $X^{(1)}$, there exists $y \in X$ such that all the elemts of yY are antidominant. Multipliying on the left by θ_y a linear dependence relation between the $\theta_x T_{w_o}$ for $(x, w_o) \in Y \times W_o$ one gets a linear independence relation between the $(T_w)_{w \in W^{(1)}}$ which is absurd.

c) $(T_{w_o} \theta_x)_{(w_o,x) \in W_o \times X^{(1)}}$ are linearly independent over R. This is deduced from b) using that for $w_o \in W_o, b \in \mathcal{A}_R$, $T_{w_o} b \in w_o(b) T_{w_o} + \sum_{u_o \in W_o, u_o < w_o} \mathcal{A}_R T_{u_o}$, by §28. If there is a non zero relation $\sum_{w_o \in W_o} T_{w_o} b_{w_o} = 0$ with $b_{w_o} \in \mathcal{A}_R$, let m the maximum length of the w_o such that $b_{w_o} \neq 0$. Then $\sum_{w_o \in W_o, \ell(w_o) = m} w_o(b_{w_o}) T_{w_o} \in \sum_{u_o \in W_o, l(u_o) < m} \mathcal{A}_R T_{u_o}$. By b), $(T_{w_o})_{w_o \in W_o}$ is a basis of $\mathcal{H}_R^{(1)}$ as a left $\mathcal{A}_R$-module, hence $w_o(b_{w_o}) = 0$ for all w_o of length m. This is absurd.

53 Proof of §30.

For any $w = xw_o \in W^{(1)}$, with $w_o \in W_o, x \in X^{(1)}$, we choose x_1, x_2 antidominant with $x = x_2^{-1}x_1$. By definition,

$$E_w = q_{x_2^{-1}x_1w_o}^{1/2} q_{x_2}^{1/2} q_{x_1}^{-1/2} q_{w_o}^{-1/2} T_{x_2}^{-1} T_{x_1} T_{w_o} = (q_{x_2^{-1}x_1w_o} q_{x_2^{-1}} q_{x_1w_o}^{-1})^{1/2}\, T_{x_2}^{-1} T_{y_1w_o}$$

because $\ell(x_1w_o) = \ell(x_1) + \ell(w_o)$ when x_1 is antidominant and $q_{x_2} = q_{x_2^{-1}}$. Then we use the fundamental lemma 53.1 on the expansion of $(q_{vw}q_vq_w^{-1})^{1/2}T_{v^{-1}}^{-1}T_w$ for $v, w \in W^{(1)}$ in the Iwahori-Matsumoto basis, as in [V3 lemma 1.2].

Let $v' = s_1 \dots s_m \in W_{aff}$ (reduced expression, $s_i \in S$) and let $w \in W^{(1)}$. A sequence $(s_{i_1}, \dots, s_{i_r})$ extracted from the sequence $(s_1, \dots, s_m)$ is called
- left w-distinguished if $ws_1 \dots s_{i_1-1} < ws_1 \dots s_{i_1}$,
$ws_1 \dots \hat{s}_{i_1} \dots s_{i_2-1} < ws_1 \dots \hat{s}_{i_1} \dots s_{i_2}, \ \dots, \quad ws_1 \dots \hat{s}_{i_1} \dots \hat{s}_{i_r-1} < ws_1 \dots \hat{s}_{i_1} \dots \hat{s}_{i_r}$.
- right w-distinguished if $s_{i_r+1} \dots s_m w < s_{i_r} \dots s_m w, \ \dots,$
$s_{i_1+1} \dots \hat{s}_{i_2} \dots \hat{s}_{i_r} \dots s_m w < s_{i_1} \dots \hat{s}_{i_2} \dots \hat{s}_{i_r} \dots s_m w$.

53.1 Fundamental lemma *Let $v, w \in W^{(1)}$.*

1) $q_{vw}q_vq_w^{-1} = c_{v,w,-}^2$ where $c_{v,w,-} \in q^{\mathbf{N}}$.

2) Let $s_1, \dots, s_m \in S$ and $v_o \in W^{(1)}$ of length 0 such that $v = v_os_1 \dots s_m$ is a reduced decomposition. Let $\tau = (s_{i_1}, \dots, s_{i_r})$ be a right w-distinguished sequence of length $r \geq 1$ extracted from the sequence $(s_1, \dots, s_m)$. Then $q_{vw} = q_{s_1 \dots \hat{s}_{i_1} \dots \hat{s}_{i_r} \dots s_m w} q^r d_{v,w,-}(\tau)^2$ where $d_{w,v,-}(\tau) \in q^{\mathbf{N}}$.

3) We have

(R_-)

$$c_{v,w,-}\ T_{v^{-1}}^{-1} T_w = T_{vw} + \sum_{\tau=(s_{i_1},\dots,s_{i_r})} d_{v,w,-}(\tau)\lambda_{v,\tau,-}\ T_{v_os_1 \dots \hat{s}_{i_1} \dots \hat{s}_{i_r} \dots s_m w},$$

where the sum is taken over the left w-distinguished sequences $\tau = (s_{i_1}, \dots, s_{i_1})$ of length $r \geq 1$ extracted from $(s_1, \dots, s_m)$ and

$$\lambda_{v,\tau,-} = \prod_{k=1}^{r} (- \sum_{t \in T_{s_{i_k}}(\mathbf{F}_q)} T_{v_os_1 \dots s_{i_k-1}(t)}).$$

The sum corresponding to $i_1 = 1$ the sum is $\sum_{t \in T_{s_1}(\mathbf{F}_q)} T_{v_o(t)}$.

The relation (R_-) for (v,w) is written in the ring $\mathcal{H}^{(1)}$. It looks simpler in $\mathcal{H}^{(1)}[q^{-1/2}]$ with the normalized elements $\tilde{T}_w = q_w^{-1/2} T_w$ for $w \in W^{(1)}$, using (1) and (2). Note that for $s \in S$,

$$\tilde{T}_s^{-1} = \tilde{T}_s + \tilde{\lambda}_s, \quad \tilde{\lambda}_s = q^{-1/2}\lambda_s, \ \lambda_s = -\sum_{t \in T_s(\mathbf{F}_q)} T_t.$$

The fundamental lemma is equivalent to (1), (2) and (3) with the relation (R_-) replaced by

$$(\tilde{R}_-) \qquad \tilde{T}_{v^{-1}}^{-1}\tilde{T}_w = \tilde{T}_{vw} + \sum_{\tau=(s_{i_1},\dots,s_{i_r})} \tilde{\lambda}_{v,\tau,-}\ \tilde{T}_{s_1\dots\hat{s}_{i_1}\dots\hat{s}_{i_r}\dots s_m v_o w},$$

where $\tilde{\lambda}_{v,\tau,-} = q^{r/2}\lambda_{v,\tau,-}$.

Proof of the fundamental lemma.

As $q_w = q^{\ell(w)}$ the property 1) results from a well known property of the length $\ell(vw) - \ell(w) - \ell(v) \in 2\mathbf{N}$. The relation $(\tilde{R}_-)$ for (v,w) is equivalent to the relation $(\tilde{R}_-)$ for $(s_1 \dots s_m, w)$, and is proved by induction on the length m. When $s \in S$, the relation $(\tilde{R}_-)$ for (s,w) results from the braid relation:

$\tilde{T}_s^{-1}\tilde{T}_w = \tilde{T}_{sw}$ if $\ell(sw) < \ell(w)$ and $\tilde{T}_s^{-1}\tilde{T}_w = \tilde{T}_{sw} + \tilde{\lambda}_s\tilde{T}_w$ if $\ell(w) < \ell(sw)$.

When $v = s_1 s_2$ has length 2, the relation $(\tilde{R}_-)$ for $(s_1 s_2, w)$ is obtained by multiplying by $\tilde{T}_{s_1}^{-1}$ on the left the relation $(\tilde{R}_-)$ for (w, s_2) and by commuting (see §11) $\tilde{T}_{s_1}^{-1}\tilde{\lambda}_{s_2} = s_1(\tilde{\lambda}_{s_2})\tilde{T}_{s_1}^{-1}$ if $w < ws_1$. We obtain that $\tilde{T}_w\tilde{T}_{s_1}^{-1}\tilde{T}_{s_2}^{-1}$ is equal to:

$\tilde{T}_{s_1}^{-1}\tilde{T}_{s_2 w}$ if $s_2 w < w$, and we apply the relation $(\tilde{R}_-)$ for $(s_1, s_2 w)$,

$\tilde{T}_{s_1}^{-1}\tilde{T}_{s_2 w} + s_1(\tilde{\lambda}_{s_2})\tilde{T}_{s_1}^{-1}\tilde{T}_w$ if $w < s_2 w$, and we apply the relation $(\tilde{R}_-)$ for $(s_1, s_2 w)$ and for (s_1, w).

Repeating this process, one obtains the relation $(\tilde{R}_-)$ for any (v,w).

The property 2) is proved by recurrence on m as in [V3 1.2]. The crucial case is when $i_r = m$ which is deduced from the lemma 53.2, variant of [V3 1.3].

53.2 Lemma *let $w \in W^{(1)}$ and $s_1, \dots, s_m \in S$ such that $w < s_m w$ and $s_1 \dots s_m$ is a reduced decomposition. Then*

a) $s_1 \dots s_{m-1} w < s_1 \dots s_m w$
b) $q_{s_1 \dots s_m w} = q_{s_1 \dots s_{m-1} w} q^{1+2c}$ *for an integer* $0 \leq c \leq m-1$.

The proof is as in [V3 1.3].

a) Notice that $w < s_m w$ is equivalent to $w^{-1} < w^{-1} s_m$ and $s_1 \dots s_{m-1} w < s_1 \dots s_m w$ is equivalent to $w^{-1} s_{m-1} \dots s_1 < w^{-1} s_m \dots s_1$, and apply [H1 lemma 5.6].

b) Recurrence on m. The case $m = 1$ is evident. By recurrence hypothesis, $q_{s_2 \dots s_m w} = q_{s_2 \dots s_{m-1} w} q^{1+2c}$ for some $0 \leq c \leq m-2$. Writing $q_{s_1 \dots s_m w} = q_{s_2 \dots s_m w} q^x, q_{s_1 \dots s_{m-1} w} = q_{s_2 \dots s_{m-1} w} q^y$ with $x, y \in \{\pm 1\}$, we obtain $q_{s_1 \dots s_m w} = q_{s_1 \dots s_{m-1} w} q^{1+2c+x-y}$. We have $x - y \in \{-2, 0, 2\}$. We deduce b) because the case $x - y = -2$ and $c = 0$ is impossible. Otherwise $q q_{s_1 \dots s_m w} = q_{s_1 \dots s_{m-1} w}$ implying $\ell(s_1 \dots s_m w) + 1 = \ell(s_1 \dots s_{m-1} w)$ because $q_w = q^{\ell(w)}$, which contradicts a).

There an analogue for the expansion of $(q_{wv} q_w^{-1} q_v)^{1/2} T_w T_{v^{-1}}^{-1}$ in the Iwahori-Matsumoto basis, analogue of §30 for E_w^+.

53.3 Variant *Let* $w, v \in W^{(1)}$.

1) $q_{wv} q_w^{-1} q_v = c_{w,v,+}^2$ *is the square of* $c_{w,v,+} \in q^{\mathbf{N}}$.

2) Let $s_1, \dots, s_m \in S$ *and* $v_o \in W^{(1)}$ *of length* 0 *such that* $v = s_1 \dots s_m v_o$ *is a reduced decomposition. Let* $\sigma = (s_{i_1}, \dots, s_{i_r})$ *be a left* w*-distinguished sequence of length* $r \geq 1$ *extracted from the sequence* $(s_1, \dots, s_m)$. *Then* $q_{wv} = q_{w s_1 \dots \hat{s}_{i_1} \dots \hat{s}_{i_r} \dots s_m} q^r d_{w,v,+}(\sigma)^2$ *where* $d_{w,v,+}(\sigma) \in q^{\mathbf{N}}$.

3) We have

(R_+)

$$c_{w,v,+} T_w T_{v^{-1}}^{-1} = T_{wv} + \sum_{\sigma = (s_{i_1}, \dots, s_{i_r})} d_{w,v,+}(\sigma) T_{w s_1 \dots \hat{s}_{i_1} \dots \hat{s}_{i_r} \dots s_m v_o} \lambda_{v,\sigma,+}$$

where the sum is taken over the left w*-distinguished sequences* $\sigma = (s_{i_1}, \dots, s_{i_r})$ *of length* $r \geq 1$ *extracted from the sequence* $(s_1, \dots, s_m)$, *and*

$$\lambda_{v,\sigma,+} = \prod_{k=1}^{r} (- \sum_{t \in T_{s_{i_k}}(\mathbf{F}_q)} T_{v_o s_m \dots s_{i_k+1}(t)}).$$

Proof. 1) as before.

2) [V3 1.2].

3) The relation (R_+) my be replaced by

$$(\tilde{R}_+) \qquad \tilde{T}_w \tilde{T}_{v^{-1}}^{-1} = \tilde{T}_{wv} + \sum_{\sigma=(s_{i_1},\ldots,s_{i_r})} \tilde{T}_{ws_1\ldots\hat{s}_{i_1}\ldots\hat{s}_{i_r}\ldots s_m v_o} \tilde{\lambda}_{v,\sigma,+}$$

where $\tilde{\lambda}_{v,\sigma,+} = q^{r/2}\lambda_{v,\sigma,+}$. The relation $(\tilde{R}_+)$ for (w,v) is equivalent to the relation $(\tilde{R}_+)$ for $(w, s_1 \ldots s_m)$, and is proved by induction on the length m. When $v = s \in S$, the relation $(\tilde{R}_+)$ results from the braid relation:

$\tilde{T}_w \tilde{T}_s^{-1} = \tilde{T}_{ws}$ if $\ell(ws) < \ell(w)$ and $\tilde{T}_w \tilde{T}_s^{-1} = \tilde{T}_{ws} + \tilde{T}_w \tilde{\lambda}_s$ if $\ell(w) < \ell(ws)$.

When $v = s_1 s_2$ has length 2, the relation $(\tilde{R}_+)$ for $(w, s_1 s_2)$ is obtained by multiplying by $\tilde{T}_{s_2}^{-1}$ on the right the relation $(\tilde{R}_+)$ for (w, s_1) and by commuting (see §11, and denote $s(T_t) = T_{s(t)}$) $\tilde{\lambda}_{s_1} \tilde{T}_{s_2}^{-1} = \tilde{T}_{s_2}^{-1} s_2(\tilde{\lambda}_{s_1})$ if $w < ws_1$. We obtain that $\tilde{T}_w \tilde{T}_{s_1}^{-1} \tilde{T}_{s_2}^{-1}$ is equal to:

$\tilde{T}_{ws_1} \tilde{T}_{s_2}^{-1}$ if $ws_1 < w$, and we apply the relation $(\tilde{R}_+)$ for (ws_1, s_2)

$\tilde{T}_{ws_1} \tilde{T}_{s_2}^{-1} + \tilde{T}_w \tilde{T}_{s_2}^{-1} s_2(\tilde{\lambda}_{s_1})$ if $w < ws_1$, and we apply the relation $(\tilde{R}_+)$ for (ws_1, s_2) and for (w, s_2).

Repeating this process, one obtains the relation $(\tilde{R}_+)$ for (w,v).

54 Proof of §32. The proof is as in [V3 (1.6.3), (1.6.5)] and relies on the formula:

$$E_{x'xw_o} = q_{x'xw_o}^{1/2} \tilde{\theta}_{xx'} \tilde{T}_{w_o} = q_{x'xw_o}^{1/2} \tilde{\theta}_x \tilde{\theta}_{x'} \tilde{T}_{w_o} = q_{x'xw_o}^{1/2} q_{x'}^{-1/2} q_{xw_o}^{-1/2} E_{x'} E_{xw_o}$$

for $(w_o, x, x') \in W_o \times X^{(1)} \times X^{(1)}$. If $\ell(x'xw_o) = \ell(x') + \ell(xw_o)$, then the formula implies $E_{x'xw_o} = E_{x'} E_{xw_o}$. For any $w_o \in W_o$, there exists a finite set $X(w_o) = \{x_1, \ldots, x_r\}$ in X such that pour tout $x \in X$ there is $x_i \in X(w_o)$ with $\ell(xw_o) = \ell(xx_i^{-1}) + \ell(x_i w_o)$ [V3 (1.6.3)]. The same is true for $X^{(1)} = XT(\mathbf{F}_q)$. One deduces that the $\mathbf{Z}$-module $\mathcal{H}^{(1)}(w_o)$ of basis $(E_{xw_o})_{x \in X^{(1)}}$ is a $\mathcal{A}^{(1)}$-left module generated by $(E_{xw_o})_{x \in X(w_o)}$.

As in [V3 (1.6.5)], $\mathcal{A}^{(1)}$ is a ring generated by $(E_x)_{x \in W_o(M_-)}$ where M_- is finite system of generators of the monoid of antidominant elements in $X^{(1)}$.

55 Proof of §33

(i) follows from §32 i) by a general argument [Bki AC V 1.9 th. 2 page 29].

(iii) results from (ii), (i) and §32 (ii).

Proof of (ii).

Note that $\tilde{\theta}_x\varepsilon_\lambda + \tilde{\theta}_{s(x)}\varepsilon_{s(\lambda)}$ commutes with T_s when $(x,\lambda) \in X \times \hat{T}(\mathbf{F}_q)$. Let γ a W_o-orbit in $\hat{T}(\mathbf{F}_q)$. The centre of the ring $\mathcal{H}(\gamma)$ (§15) is determined first, then the centre of $\mathcal{H}^{(1)}$ is obtained using §14. In order to do that, we use the analogues of §30, §31, §32 for $\mathcal{H}(\gamma)$.

Properties of $\mathcal{H}(\gamma)$

(i) The matrix of the coefficients of $(E_w\varepsilon_\lambda)_{(w,\lambda)\in W\times\gamma}$ on the Iwahori-Matsumoto basis $(T_w\varepsilon_\lambda)_{(w,\lambda)\in W\times\gamma}$ of $\mathcal{H}(\gamma)$ is integral and triangular with 1 on the diagonal.

It is enough to prove that $[\sum_{t\in T_s(\mathbf{F}_q)} T_{w_o(t)}]\varepsilon_\lambda \in \mathbf{Z}\varepsilon_\lambda$ for any $(s,w_o) \in S \times W_o$ (§30, §54.1). It is clear that $[\sum_{t\in T_s(\mathbf{F}_q)} T_{w_o(t)}]\varepsilon_\lambda = 0$ if λ is not trivial on the subgroup $w_o(T_s(\mathbf{F}_q))$ and $[\sum_{t\in T_s(\mathbf{F}_q)} T_{w_o(t)}]\varepsilon_\lambda = (q-1)\varepsilon_\lambda$ if λ is trivial on $w_o(T_s(\mathbf{F}_q))$, because $T_t\varepsilon_\lambda = \lambda(t)\varepsilon_\lambda$ for any $t \in T(\mathbf{F}_q)$.

(ii) $(E_w\varepsilon_\lambda)_{(w,\lambda)\in W\times\gamma}$ is a $\mathbf{Z}$-basis of $\mathcal{H}(\gamma)$, and the $\mathbf{Z}$-submodule $\mathcal{A}(\gamma)$ of basis $(E_x\varepsilon_\lambda)_{(x,\lambda)\in X\times\gamma}$ is a commutative subring of $\mathcal{H}(\gamma)$.

(iii) $\mathcal{A}(\gamma)$ is a finitely generated commutative ring, and $\mathcal{H}(\gamma)$ is a finitely generated left $\mathcal{A}(\gamma)$-module.

Let R be a commutative ring which contains $\{\mu_{q-1}, 1/q(q-1)\}$. The group W_o acts on $\mathcal{A}(\gamma)$ by $w_o(E_x\varepsilon_\lambda) = E_{w_o(x)}\varepsilon_{w_o(\lambda)}$ for $(w_o,x,\lambda) \in W_o \times X \times \gamma$. Denote $\mathcal{A}(\gamma)^{W_o}$ the subring of W_o-fixed elements of $\mathcal{A}(\gamma)$ and $z_{\{x,\lambda\}}$ the sum of the W_o-conjugates of $E_x\varepsilon_\lambda$.

(iv) $\mathcal{A}(\gamma)$ is a finitely generated $\mathcal{A}(\gamma)^{W_o}$-module, and $\mathcal{A}(\gamma)^{W_o}$ is a finitely generated commutative ring, of $\mathbf{Z}$-basis $(z_{\{x,\lambda\}})_{\{x,\lambda\}\in W_o\backslash(X\times\gamma)}$.

Use [Bki AC V 1.9 th. 2 page 29].

One shows that $\mathcal{A}(\gamma)^{W_o}$ is the center of $\mathcal{H}(\gamma)$. By §28 and §29, $z_{\{x,\lambda\}}$ is central (this can be done over $\mathbf{C}$). By §16, $\mathcal{A}(\gamma)^{W_o}$ exhausts the center of $\mathcal{H}(\gamma)$.

For any $\lambda \in \hat{T}(\mathbf{F}_q)$ we have $\sum_{t\in T_s(\mathbf{F}_q)} T_t\varepsilon_\lambda = \sum_{t\in T_s(\mathbf{F}_q)} \lambda(t) = \sum_{t\in T_s(\mathbf{F}_q)} \lambda(s(t)) = \sum_{t\in T_s(\mathbf{F}_q)} T_t\varepsilon_{s(\lambda)}$ because $s(t) = t^{-1}$ on $T_s(\mathbf{F}_q)$. By §28, T_s commutes with $\tilde{\theta}_x\varepsilon_\lambda + \tilde{\theta}_{s(x)}\varepsilon_{s(\lambda)}$. The sum $\tilde{\theta}_{\{x,\lambda\}}$ of

the W_o-conjugates of $\tilde{\theta}_x\varepsilon_\lambda$ is an element of the commutative algebra $\mathcal{A}_{\mathbf{C}}$ which commutes with T_{w_o} for any $w_o \in W_o$. Such an element is a central element of $\mathcal{H}(\gamma)_{\mathbf{C}}$ by §29. As $q_{xt} = q_x$ is W_o-invariant as a function of $XT(\mathbf{F}_q)$, $z_{\{x,\lambda\}} = q_x^{1/2}\tilde{\theta}_{\{x,\lambda\}}$ is central in $\mathcal{H}(\gamma)$.

By §16, the ring $\mathcal{H}(\gamma)$ is a deformation of $\mathbf{Z}[W]\tilde{\otimes}\mathbf{Z}[\gamma]_{deg}$. The group W acts by conjugation on W and (via its quotient W_o) on γ, and linearly on $\mathbf{Z}[W]\tilde{\otimes}\mathbf{Z}[\gamma]_{deg}$ via its action on the canonical basis $(e_w \otimes e_\lambda)$. The set of $(w,\lambda) \in W \times \gamma$ such that $e_w \otimes e_\lambda$ has a finite number of conjugates by W, is $X \times \gamma$. For $(x,\lambda) \in X \times \gamma$, denote $e_{\{x,\lambda\}}$ the sum of the W_o-conjugates of $e_x \otimes e_\lambda$. These elements are clearly linearly independent and the center of $\mathbf{Z}[W]\tilde{\otimes}\mathbf{Z}[\gamma]_{deg}$ is the free $\mathbf{Z}$-module of basis $(e_{\{x,\lambda\}})_{\{x,\lambda\}\in W_o\backslash X\times\gamma}$. One finishes the proof that the center of $\mathcal{H}(\gamma)$ is the free $\mathbf{Z}$-module of basis $(z_{\{x,\lambda\}})_{\{x,\lambda\}\in W_o\backslash X\times\gamma}$ as in [Lusztig asterisque 101-102 proof of theorem 8.1 page 222].

By §14, the center of $\mathcal{H}^{(1)}_{\mathbf{C}}$ is $(\mathcal{A}^{(1)}_{\mathbf{C}})^{W_o} = \oplus\mathcal{A}(\gamma)^{W_o}_{\mathbf{C}}$. Clearly $(z_{\{x\}})_{\{x\}\in W_o\backslash X^{(1)}}$ is a $\mathbf{C}$-basis of $(\mathcal{A}^{(1)}_{\mathbf{C}})^{W_o}$ contained in $\mathcal{H}^{(1)}$. By §31, it is also a $\mathbf{Z}$-basis of $\mathcal{A}(\gamma)^{W_o}$, and $\mathcal{A}^{W_o}_{\mathbf{C}} \cap \mathcal{H} = \mathcal{A}^{W_o}$. Hence the center of $\mathcal{H}^{(1)}$ is equal to $(\mathcal{A}^{(1)})^{W_o}$.

56 (i) Any character of $(\Omega \cap X)T(\mathbf{F}_q)$ extends to a null character of $\mathcal{A}^{(1)}$.

Let R be a commutative ring of characteristic p and let ξ be a R-character of $(\Omega\cap X)T(\mathbf{F}_q)$. Consider the linear form χ on $\mathcal{A}^{(1)}_R$ such that $\chi(E_x) = \xi(x)$ for $x \in (\Omega\cap X)T(\mathbf{F}_q)$ and $\chi(E_x) = 0$ for $x \in X^{(1)}$ not in $(\Omega \cap X)T(\mathbf{F}_q)$. Claim: χ is an R-character of $\mathcal{A}^{(1)}$, i.e. (§54):

$$q_{x'x}^{1/2}\chi(E_{x'})\chi(E_x) = q_{x'}^{1/2}q_x^{1/2}\chi(E_{x'x}), \quad (x, x' \in X^{(1)}).$$

If xx' has length > 0, then x or x' has length > 0, this is clear because both sides are 0.
If xx' has length 0, the formula for the length [V3 Appendice 1] shows that x, x' have the same length; if their length is 0, the formula is $\xi(xx') = \xi(x)\xi(x')$ which is true, if their length is > 0 the formula is $0 = q_x\xi(x'x)$ which is true because $q_x = 0$ in R.

(ii) A character of $\mathcal{A}^{(1)}$ is null if and only if its restriction to $\mathcal{A}^{(1)}_{aff}$ is null.

Suppose that: $\chi(E_y)\neq 0$ for $y \in X_{aff}$ implies $y = 1$. Let $x \in X$ such that $\chi(E_x)\neq 0$. There exists a positive integer n such that $x^n = uy$ with $(u,y) \in (\Omega \cap X) \times X_{aff}$ because $(\Omega\cap X) \times X_{aff}$ has finite index in X. We have $(E_x)^n = E_{x^n} = E_uE_y$ and $\chi(E_x)^n = \xi(u)\chi(E_y)$. As $\chi(E_x)\neq 0$ we have $y = 1$. This means that x^n has length 0, which is equivalent to x of length 0.

57 Proof of 36.

Note that $\mu_1 = us_1 \dots s_{n-1}$ where

$$\mu_1 = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ \dots & \dots & \dots & \dots \\ 0 & 0 & 0 & p \end{pmatrix}, \quad u := \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ \dots & \dots & \dots & \dots \\ p_F & 0 & 0 & 0 \end{pmatrix}.$$

Denote $\tau = E_u$. The following expressions were computed by Lusztig [L1 page 643-644]:

$E_{\mu_1} = \tau T_1 \dots T_{n-1}$
$E_{\mu_2} = \tau^2 (T_2 T_1) \dots (T_{n-1} T_{n-2})$
.....
$E_{\mu_t} = \tau^t (T_t \dots T_2 T_1) \dots (T_{n-1} T_{n-2} \dots T_{n-t})$
.....
$E_{\mu_{n-1}} = \tau^{n-1} T_{n-1} T_{n-2} \dots T_1$.

The length of μ_t is $t(n-t)$ hence these are minimal expressions; one sees that T_s appears in these minimal expressions for all $s \in S$.

Let $y \in S_n(\mu_t)$ different from μ_t of minimal expression

$$E_y = \tau^t T^*_{u^{-t} s(a) u^t} \dots T^*_{u^{-t} s(1) u^t} T_{s'(1)} \dots T_{s'(t(n-t)-a)}$$

for two maps $s : \{1, \dots, a\} \to S_o$, $s' : \{1, \dots, t(n-t)-a\} \to S$ and $1 \leq a \leq t(n-t)$. Note that $u^{-1} s_i u = s_{i+1}$ for $s_i = (i, i+1)$ for $1 \leq i \leq n$ modulo n. In the simple recipe given by Haines in [H2 proposition 3.4] to construct a minimal expression, $s(1) = s_{n-t}$. Hence $T^*_{s_o}$ appears in any minimal expression of E_y.

58 Proof of §37.

For G general, we have (§23):

a) $\chi_{\lambda,I}(T_s) = 0$, $\chi_{\lambda,I}(T^*_s) = 0$ if $s \in S - S_\lambda$,
b) $\chi_{\lambda,I}(T_s) = 0$, $\chi_{\lambda,I}(T^*_s) = -1$ if $s \in S_\lambda - I$,
c) $\chi_{\lambda,I}(T_s) = -1$, $\chi_{\lambda,I}(T^*_s) = 0$ if $s \in I$.

Let $x \in X$ antidominant, of reduced decomposition $x = u\sigma_1 \dots \sigma_m$ with $u \in \Omega T(\mathbf{F}_q), \sigma_i \in S, m = \ell(x)$. The set S is normalized by u hence $u\sigma_i u^{-1} \in S$. We have

$$E_x = T_u T_{\sigma_1} \dots T_{\sigma_m}, \quad E_{x^{-1}} = T_u^{-1} T^*_{u\sigma_m u^{-1}} \dots T^*_{u\sigma_1 u^{-1}}.$$

The value of a sign character ($I = S$) on E_x is not zero, the value of a trivial character ($I = \emptyset$) on $E_{x^{-1}}$ is not zero. These characters are never supersingular.

Suppose that $I \neq \emptyset, S$. If the root system is irreducible $S = S_o \cup \{s_o\}$. We choose $\chi_{\lambda,I}$ in its Ω_o-orbit such that $s_o \in I$. There exists some $s \in S_o$ which does not belong to I.

An irreducible $\overline{\mathbf{F}}_p$-representation V of $\mathcal{H}^{(1)}$ which contains $\chi_{\lambda,I}$ and where $\Omega \cap X$ acts by a fixed character, is generated by the Ω_o-conjugates of an eigenvector v of $\mathcal{H}^{(1)}_{aff}$ with eigenvalue $\chi_{\lambda,I}$.

Suppose $G = GL(n, F)$. By §36, we have $E_y v = 0$ for all $y \in S_n(\mu_t)$, all $1 \leq t \leq n-1$. By §35, V is supersingular.

59 Proof of §25 : *The number of pairs* (x, e) *of maps* $x : \mathbf{Z}/n\mathbf{Z} \to \mathbf{F}_q^*$, $e : \mathbf{Z}/n\mathbf{Z} \to \{0, 1\}$ *such that* $e(i) \neq 0$ *implies* $x(i) = x(i+1)$ *for* $i \in \mathbf{Z}/n\mathbf{Z}$, *is equal to* q^n.

We have $q-1$ choices for $x(1)$. Once $x(1)$ has been chosen, we choose $x(2)$. There are $q-2$ choices for $x(1) \neq x(2)$ and one choice for $x(1) = x(2)$. When $x(1) = x(2)$ there are two choices for $e(1)$. The number of choices for $(x(2), e(1))$ is $q - 2 + 2 = q$. For a given choice of $x(1), x(2), e(1)$, there are q choices for $x(3), e(2)$. By induction we choose finally $x(n), e(n-1)$. It remains to choose $e(n)$. We can always choose $e(n) = 0$, hence there are $q^n - q^{n-1}$ possibilities with $e(n) = 0$. We may choose $e(n) = 1$ if and only if $x(n) = x(1)$. For each value of $x(1)$, there are q^{n-2} possiblities for $(x(2), e(1), \ldots, x(n-1), e(n-2))$. If $x(n-1) = x(n) = x(1)$, there are 2 possibilities for $e(n-1)$. If $x(n-1) \neq x(n) = x(1)$ there is only one. Hence there are $q^{n-2}(q-2+2) = q^{n-1}$ possiblities with $e(n) = 1$. The total number of pairs (x, e) is $q^n - q^{n-1} + q^{n-1} = q^n$.

References

[Bki AC] BOURBAKI Nicolas, Algèbre commutative. Chapitre 5 à 7. Masson 1985.

[IM] IWAHORI N. and MATSUMOTO H., On some Bruhat decomposition and the structure of the Hecke rings of p-adic Chevalley groups. Inst. Hautes Etudes Sci. Publ. Math. No. 25 1965 5–48.

[H1] HAINES Thomas J., The combinatorics of Bernstein functions. Trans. Am. Math. Soc. 353, No 3 (2001), 1251-1278.

[H2] HAINES Thomas J., Test functions for Shimura varieties. The Shimura case. Duke Math. Journal 106 (2001), 19-40.

[HP] HAINES Thomas J.; PETTET Alexandra, Formulae relating the Bernstein and Iwahori-Matsumoto presentations of an affine Hecke algebra. J. Algebra 252 (2002), no. 1, 127–149.

[L1] LUSZTIG Georges, Some examples of square integrable representations of semisimple p-adic groups. Transactions of the A.M.S. 277 no2 (1983) 623-653.

[L2] LUSZTIG Georges, Affine Hecke algebras and their graded version. Journal of the American Mathematical Society 2 no3 (1989) 599-635.

[M] MORRIS L. Tamely ramified intertwining algebras, Inventiones 114, 1-54 (1993).

[V1] VIGNERAS Marie-France, Induced representations of reductive p-adic groups in characteristic $l \neq p$. Selecta Mathematica New Series 4 (1998) 549-623.

[V2] Representations modulo p of the p-adic group $GL(2, F)$. Preprint 2001. Compositio Mathematica, to appear.

[V3] Algèbres de Hecke affines génériques. Preprint 2002. math.RT/0301058.

[V4] Représentations l-modulaires d'un groupes réductif p-adique avec $l \neq p$. Birkhauser Progress in Math.137 (1996).