Abstract. The motivation of this paper is the search for a Langlands correspondence modulo $p$. We show that the pro-$p$-Iwahori Hecke ring $\mathcal{H}_1^{(1)}$ of a split reductive $p$-adic group $G$ over a local field $F$ of finite residue field $\mathbb{F}_q$ with $q$ elements, admits an Iwahori-Matsumoto presentation and a Bernstein $\mathbb{Z}$-basis, and we determine its centre. We prove that the ring $\mathcal{H}_1^{(1)}$ is finitely generated as a module over its centre. These results are proved in [11] only for the Iwahori Hecke ring. Let $p$ be the prime number dividing $q$ and let $k$ be an algebraically closed field of characteristic $p$. A character from the centre of $\mathcal{H}_1^{(1)}$ to $k$ which is "as null as possible" will be called null. The simple $\mathcal{H}_1^{(1)}$-modules with a null central character are called supersingular. When $G = GL(n)$, we show that each simple $\mathcal{H}_1^{(1)}$-module of dimension $n$ containing a character of the affine subring $\mathcal{H}_1^{aff}$ of dimension $n$ is supersingular, using the minimal expressions of Haines generalized to $\mathcal{H}_1^{(1)}$, and that the number of such modules is equal to the number of irreducible $k$-representations of the Weil group $W_F$ of dimension $n$ (when the action of an uniformizer $p_F$ in the Hecke algebra side and of the determinant of a Frobenius $\text{Fr}_F$ in the Galois side are fixed), i.e. the number $N_n(q)$ of unitary irreducible polynomials in $\mathbb{F}_q[X]$ of degree $n$. One knows that the converse is true by explicit computations when $n = 2$ [10], and when $n = 3$ (Rachel Ollivier).

Introduction

The results are presented before the proofs. The main results are: the conjectures 1, 2, the Iwahori-Matsumoto presentation (Theorem 1), the Bernstein basis (Theorem 2), the centre (Theorem 4), the definition 4 of supersingular, when $G = GL(n)$ the construction of $N_n(q)$ supersingular irreducible representations of $\mathcal{H}_1^{(1)}$ of dimension $n$ with a fixed action of $p_F$ (Proposition 3, Theorem 5), and the elementary formula for $N_n(q)$ in the appendix, reflecting the decomposition of the algebra $\mathcal{H}_1^{(1)}$ (Proposition 4).

Many thanks to Rachel Ollivier and to Christophe Breuil whose work motivated this paper, and to Ulrich Goertze for his amical help. Most of these results were presented at the conference on $p$-adic/mod $p$ representations of $p$-adic groups and non abelian Iwasawa theory, hold at Luminy in June 2003.

M.-F. Vigneras
Institut de Mathématiques de Jussieu, Université de Paris 7-Denis Diderot, 2 place Jussieu, 75251 Paris Cedex 05, France
1. Results

We fix a local non archimedean field $F$ (a finite extension of $\mathbb{Q}_p$ or a field of Laurent series $\mathbb{F}_q((t))$ on a finite field $\mathbb{F}_q$ with $q$ elements), of residual field $\mathbb{F}_q$ of characteristic $p$, $O_F$ the ring of integers, $P_F$ the maximal ideal, $p_F$ an uniformizer, $W_F = W(\overline{F}/F)$ a Weil group, $Fr_F \in W(\overline{F}/F)$ a geometric Frobenius. \footnote{The multiplicative group of a ring $R$ is denoted by $R^*$ and the separable algebraic closure of a field $R$ is denoted by $\overline{R}$. The field $\mathbb{F}_p$ can be replaced by any algebraically closed field $k$ of characteristic $p$. All representations of $p$-adic reductive groups will be smooth representations, and modules of Hecke algebra will be right modules.}

The classification of irreducible $\mathbb{F}_p$-representations of $GL(n, F)$ is unknown, even for the group $GL(2, F)$ when $F \neq \mathbb{Q}_p$. We replace $GL(n, F)$ by the Hecke ring $H^{(1)}(GL(n, F), I_w)$ of the pro-$p$-radical $I_w$ of an Iwahori subgroup $I_w$ of $GL(n, F)$, that we call the pro-$p$-Iwahori Hecke ring. The algebra $H^{(1)}(GL(n, F), I_w)$ depends only on $(n, q)$. The same is true for the scalar extension $H^{(1)}(\mathbb{F}_p) = H^{(1)}(GL(n, F), I_w) \otimes \mathbb{Z}$. We will sometimes denote $H^{(1)}(GL(n, F), I_w) = H^{(1)}(n, q)$ and $H^{(1)}(\mathbb{F}_p) = H^{(1)}(n, q)$.

Any non zero $\mathbb{F}_p$-representation of $GL(n, F)$ has a non zero $I_w$-invariant vector. We hope that the functor of $I_w$-invariants induces a bijection between the irreducible $\mathbb{F}_p$-representations of $GL(n, F)$ and the simple $H^{(1)}(\mathbb{F}_p)$-modules.

This is trivially true for $n = 1$. The supersingular $H^{(1)}(\mathbb{F}_p)$-modules should be the analogues of the supercuspidal $\mathbb{F}_p$-representations of $GL(n, F)$. When $n = 1$, any $\mathbb{F}_p$-character of $H^{(1)}(\mathbb{F}_p)$ is supersingular.

**Definition 1.** When $n \geq 2$, a simple $H^{(1)}(\mathbb{F}_p)$-module with a null central character is called supersingular.

See the precise definition 4. When $n = 2$, the functor of $I_w$-invariants gives a bijection \cite{10} – from the irreducible NON supercuspidal smooth $\mathbb{F}_p$-representations of $GL(2, F)$ (subquotients of parabolic induced representations), to the NON supersingular irreducible $H^{(1)}(2, q)$-modules, – when $F = \mathbb{Q}_p$, from the irreducible supercuspidal smooth $\mathbb{F}_p$-representations of $GL(2, \mathbb{Q}_p)$, to the supersingular irreducible $H^{(1)}(2, p)$-modules.

1.1. **Numerical local Langlands correspondence modulo $p$ between $W_F$ and the pro-$p$-Iwahori Hecke ring of $GL_F$**

For an integer $n \geq 2$ and for $z \in \mathbb{F}_p^*$, we denote by

- $W(n, q)_z$: the set of isomorphism classes of the irreducible $\mathbb{F}_p$-representations $\rho$ of $W_F$ of dimension $n$ with $\det \rho(Fr_F) = z$,