LEVEL 1 HECKE ALGEBRAS OF MODULAR FORMS
MODULO $p$

JOËL BELLAÏCHE AND CHANDRASHEKHAR KHARE

Abstract. In this paper, we study the structure of the local components of the
(shallow, i.e. without $U_p$) Hecke algebras acting on the space of modular forms
modulo $p$ of level 1, and relate them to pseudo-deformation rings. In many
cases, we prove that those local components are regular complete local algebras
of dimension 2, generalizing a recent result of Nicolas and Serre for the case
$p = 2$.

Contents

1. Introduction 2
   1.1. General notations 2
   1.2. Definition of the Hecke algebras modulo $p$ 2
   1.3. Aim of the paper 4
   1.4. Deformations rings of pseudo-representations 4
   1.5. Statement of the main results 6
2. The divided congruences modules of Katz 8
3. Hecke operators on divided congruences 9
4. Divided congruences of level $\Gamma_0(p)$ 11
5. Full Hecke algebras 12
6. Local components of normal and full Hecke algebras 13
7. Proof of Theorem III 14
8. Proof of Theorem I 14
9. Proof of Theorem II 15
10. When are the reducible modular representations unobstructed? 16
Appendix: the case $p = 3$ 19
   A.1. Results 19
   A.2. Proof of the theorem assuming Propositions 27 and 31 21
   A.3. Proof of Proposition 27 22
   A.4. Sketch of the proof of Proposition 31 23
References 24

2000 Mathematics Subject Classification. 11R.
Joël Bellaïche was supported by NSF grant DMS 1101615.
1.1. General notations. In all this paper we fix a prime number \( p \). We shall denote by \( K \) a finite extension of \( \mathbb{Q}_p \), by \( \mathcal{O} \) the ring of integers of \( K \), by \( \mathfrak{p} \) the maximal ideal of \( \mathcal{O} \), by \( \pi \) a uniformizer of \( \mathcal{O} \) and by \( \mathbb{F} \) the finite residue field \( \mathcal{O}/\pi \).

We call \( G_{\mathbb{Q},p} \) the Galois group of a maximal algebraic extension of \( \mathbb{Q} \) unramified outside \( p \) and \( \infty \). For \( \ell \) a prime \( \neq p \), we denote by \( \text{Frob} \ell \in G_{\mathbb{Q},p} \) a Frobenius element at \( \ell \). We denote by \( c \) a complex conjugation in \( G_{\mathbb{Q},p} \). We write \( G_{\mathbb{Q},p} \) for \( \text{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p) \). There is a natural map \( G_{\mathbb{Q},p} \to G_{\mathbb{Q},p}^1 \), well defined up to conjugacy. For \( \rho \) a representation of \( G_{\mathbb{Q},p} \), we shall denote by \( \rho|_{G_{\mathbb{Q},p}} \) the composition of that map with \( \rho \): this is a representation of \( G_{\mathbb{Q},p}^1 \), well-defined up to isomorphism. We denote by \( \omega_p : G_{\mathbb{Q},p} \to \mathbb{F}^* \) the cyclotomic character modulo \( p \).

1.2. Definition of the Hecke algebras modulo \( p \). We shall denote by \( S_k(\mathcal{O}) \) the module of cuspidal modular forms of weight \( k \) and level 1 with coefficients in \( \mathcal{O} \), that we see by the \( q \)-expansion map as a sub-module of \( \mathcal{O}[[q]] \). For \( f \in S_k(\mathcal{O}) \), we shall denote by \( \sum_{n \geq 1} a_n(f) q^n \) its image in \( \mathcal{O}[[q]] \). We denote by \( S_{\leq k}(\mathcal{O}) \) the submodule \( \sum_{i=0}^k S_i(\mathcal{O}) \) (the sum is direct\(^1\)) of \( \mathcal{O}[[q]] \). We denote by \( S_k(\mathbb{F}) \) the space of cuspidal modular forms of weight \( k \) and level 1 over \( \mathbb{F} \) in the sense of Swinnerton-Dyer and Serre, that is the image of \( S_k(\mathcal{O}) \) by the reduction map \( \mathcal{O}[[q]] \to \mathbb{F}[[q]] \), \( f \mapsto \tilde{f} \) which reduces each coefficient modulo \( p \). It is clear that the natural map \( S_k(\mathcal{O})/\mathfrak{p} S_k(\mathcal{O}) \to S_k(\mathbb{F}) \) is an isomorphism. Similarly, we denote by \( S_{\leq k}(\mathbb{F}) \) the image of \( S_{\leq k}(\mathcal{O}) \) by the reduction map \( f \mapsto \tilde{f} \). The reader should be aware that the natural map \( S_{\leq k}(\mathcal{O})/\mathfrak{p} S_{\leq k}(\mathcal{O}) \to S_{\leq k}(\mathbb{F}) \) is surjective but not an isomorphism in general, or in other words, that \( S_{\leq k}(\mathbb{F}) = \sum_{i=0}^k S_i(\mathbb{F}) \) but that the sum is not direct in general.

All the modules considered above have a natural action of the Hecke operators \( T_n \) for \( p \nmid n \). We call \( T_k \) the \( \mathcal{O} \)-subalgebra of \( \text{End}_\mathcal{O}(S_{\leq k}(\mathcal{O})) \) generated by the \( T_n \)'s, \( p \nmid n \), and similarly \( A_k \) the \( \mathbb{F} \)-subalgebra of \( \text{End}_\mathbb{F}(S_{\leq k}(\mathbb{F})) \) generated by the \( T_n \)'s, \( p \nmid n \). Note that it would amount to the same to define \( T_k \) or \( A_k \) as generated by the Hecke operators \( T_\ell \) and \( S_\ell \) for \( \ell \neq p \) instead, where \( S_\ell \) is the operator acting on

\(^1\)It is indeed a well-known fact that that over \( \mathbb{C} \) (hence over any ring of characteristic 0) the sum of the spaces of modular forms of different weights, seen as subspaces of \( \mathbb{C}[[q]] \), is direct. However we have not been able to find a reference in the literature, so we give a simple argument. If the sum was not direct, there would be a non-zero form \( f \) of some weight \( k \) with the same \( q \)-expansion \( \sum a_n q^n \) as a sum of forms \( g_i \) of weights \( k_i \leq k - 2 \). By the Hecke estimates for the \( g_i \) (see e.g. [24, Chapter 7, theorem 5]), one would have \( a_n = O(n^{k/2 - 1}) \), hence \( \sum|a_n|^2 = O(n^{k - 2}) \). Hence the Dirichlet series defining the Rankin \( L \)-function, \( L(f \otimes \tilde{f}, s) = \sum |a_n|^2/n^s \) would converge absolutely on the half-plane \( \text{Re } s > k - 1 \), contradicting a famous theorem of Rankin (cf. [21]) saying that \( L(f \otimes \tilde{f}, s) \) has a simple pole at \( s = k \).
forms of weight $k$ as the multiplication by $\ell^{k-2}$: this equivalence is clear from the relations

\begin{align}
T_{mn} &= T_m T_n \text{ when } (m,n) = 1 \\
T_{\ell^n+1} &= T_\ell T_{\ell^n} - \ell S_\ell T_{\ell^{n-1}} \text{ for } n \geq 1.
\end{align}

Recall that on $q$-expansions, for a form $f \in S_k(O)$, one has for every $n \geq 1$,

\begin{align}
a_n(T_\ell f) &= a_\ell n(f) \text{ if } \ell \nmid n \\
a_n(T_\ell f) &= a_\ell n(f) + \ell^{k-1} a_{n/\ell}(f) \text{ if } \ell \mid n \\
a_n(S_\ell f) &= \ell^{k-2} a_n(f).
\end{align}

Since the actions of the operators $T_\ell$ on the various modules considered above are compatible in an obvious sense, one has a natural morphism of $\mathbb{F}$-algebras $T_k/pT_k \to A_k$ which is obviously surjective, but in general not an isomorphism as will be clear from the sequel. One also has surjective morphisms $T_{k+1} \to T_k$ and $A_{k+1} \to A_k$ given by restriction, and we can consider the projective limit:

$$T = \lim_{\leftarrow} T_k, \quad A = \lim_{\leftarrow} A_k.$$  

By passage to the limit we obtain a surjective map $T/pT \to A$.

A well-known important fact is that $T$ and $A$ are complete semi-local rings. More precisely, if $\mathbb{F}$ is large enough, the maximal ideals, hence the local components, of both $T$ and $A$ are in bijection with $\mathbb{F}$-valued systems of eigenvalues for all the operators $T_\ell$ and $\ell S_\ell$ (for $\ell$ prime not dividing $p$) which have a non-trivial eigenspace in $S_{\leq k}(\mathbb{F})$ for $k$ large enough, and those systems are finitely many. By Deligne's theorem on the existence of Galois representations attached to eigenforms and by the Deligne-Serre lemma, those systems of eigenvalues are in bijection with the set of isomorphism classes of modular Galois representations $\bar{\rho} : G_{\mathbb{Q},p} \to \text{GL}_2(\mathbb{F})$ (the bijection being: eigenvalue of $T_\ell \leftrightarrow \text{tr}(\bar{\rho}(\text{Frob}_\ell))$, eigenvalue of $\ell S_\ell \leftrightarrow \text{det}(\bar{\rho}(\text{Frob}_\ell))$).

Here and below, modular means that $\bar{\rho}$ is the semi-simplified reduction of a stable lattice for the Galois representation $\rho : G_{\mathbb{Q},p} \to \text{GL}_2(K)$ attached by Deligne's construction to an eigenform in $M_k(O)$ for some integer $k$. We stress that by definition, our modular representations are semi-simple. By enlarging $\mathbb{F}$ if needed we can and shall assume that if $\bar{\rho}$ is irreducible, then it is absolutely irreducible. We call $T_{\bar{\rho}}$ and $A_{\bar{\rho}}$ the local components of $T$ and $A$ corresponding to a modular representation $\bar{\rho}$. These rings are complete local rings. By definitions, the image of $T_\ell \in T$ in the residue field $\mathbb{F}$ of $T_{\bar{\rho}}$ or $A_{\bar{\rho}}$ is $\bar{\rho}(\text{Frob}_\ell)$. The surjective map $T/pT \to A$ sends $T_{\bar{\rho}}/pT_{\bar{\rho}}$ onto $A_{\bar{\rho}}.$
1.3. **Aim of the paper.** The aim of this paper is to study the local components $A_{\bar{\rho}}$ of the Hecke algebra $A$ modulo $p$, and their relation with deformation rings defined below. The study of the local components $A_{\bar{\rho}}$ was initiated by Jochnowitz ([14]) who proved that $A_{\bar{\rho}}$ is infinite-dimensional as a vector space over $F$, and continued by Khare ([16]), who proved, under the hypothesis that $\bar{\rho}$ is absolutely irreducible, that $A_{\bar{\rho}}$ is noetherian and has Krull’s dimension at least 1. Recently, the structure of $A$ in the case $p = 2$ has been determined by Nicolas and Serre. Let us explain their result, which is the direct motivation for this work. When $p = 2$, we can take $O = \mathbb{Z}_2$ and there is only one modular representation $\bar{\rho} : G_{Q,p} \rightarrow GL_2(F_2)$, which is $\bar{\rho} = 1 \oplus 1$. In other words, the ring $A = A_{\bar{\rho}}$ is local. Nicolas and Serre show that $A$ is isomorphic to a power series ring in two variables: $A \simeq F_2[[x, y]]$. Their proof of this result is long and difficult, but elementary. The result was extended to $p = 3$ by the first-named author of this article, who proved that $A = A_{\bar{\rho}} = F_3[[x, y]]$ for the unique modular representation $\bar{\rho} = 1 + \omega_3$ in this case (a sketch of the proof is reproduced in the appendix of this paper). In this paper we shall give a generalization of these results for an arbitrary prime $p > 3$, using results of Böckle, Katz, Hida, Gouvea-Mazur, Wiles, Taylor-Wiles.

1.4. **Deformations rings of pseudo-representations.** To state our results, we need to recall Chenevier’s notion of pseudo-representations\(^2\) – restricted to dimension 2 for simplicity: if $S$ is a commutative ring, and $G$ is a group, a pseudo-representation (cf. [5, Lemma 1.9]) of $G$ on $S$ is an ordered pair of functions $(t, d)$ from $G$ to $S$, such that:

(a) $d$ is a morphism of groups $G \rightarrow S^*$;
(b) $t(1) = 2$;
(c) for all $g$ and $h$ in $G$, $t(gh) = t(hg)$;
(d) for all $g$ and $h$ in $G$, $d(g)t(g^{-1}h) + t(gh) = t(g)t(h)$

When $G$ and $S$ have a topology, we say that $(t, d)$ is continuous if both $t$ and $d$ are.

If $\rho : G \rightarrow GL_2(S)$ is a representation (i.e. a morphism of groups), then $(t_{\rho} := \text{tr} \rho, d_{\rho} := \text{det} \rho)$ is a pseudo-representation of $G$ to $S$, called the pseudo-representation attached to $\rho$. Conversely, a pseudo-representation $(t, d)$ of $G$ to $K$, where $K$ is an algebraically closed field, is attached to a unique semi-simple representation $\rho : G \rightarrow GL_2(K)$ (see [5, Theorem A]). When 2 is invertible in $S$, $(t, d)$ is determined by $t$, which is a pseudo-character of dimension 2 in the sense

\(^2\)Cf. [5], where this notion has the not very convenient name determinant.
of Rouquier ([22]), and the theory of pseudo-representations reduces to the more classical theory of pseudo-characters.

Let $S$ be a henselian local ring, with residue field $K = S/m$ algebraically closed, and $(t, d) : G \to S$ is a pseudo-representation, whose residual pseudo-representation $(t \mod m, d \mod m)$ of $G$ to $K$ is attached to a representation $\bar{\rho} : G \to \text{GL}_2(K)$ which is absolutely irreducible. Then a theorem of Chenevier ([5]) asserts that $(t, d)$ is attached to a unique representation $\rho : G \to \text{GL}_2(S)$.

Let $C$ be the category of local complete $\mathcal{O}$-algebras $S$ with maximal ideal $m_S$ such that $S/m_S = \mathbb{F}$, the morphisms being the local morphisms of $\mathcal{O}$-algebras, and let $\tilde{C}$ be the full subcategory of $C$ whose objects are the local complete $\mathbb{F}$-algebras $S$. Let us fix an odd continuous representation $\bar{\rho} : G_{\mathbb{Q}, p} \to \text{GL}_2(\mathbb{F})$. We define a functor $D_{\bar{\rho}}$ from $C$ to $\text{SETS}$ by sending $S$ to the set of continuous pseudo-representations $(t, d)$ of $G_{\mathbb{Q}, p}$ to $S$ such that $t \mod m_S = \text{tr} \bar{\rho}$, $d \mod m = \det \bar{\rho}$, and $t(c) = 0$.

We denote by $\tilde{D}_{\bar{\rho}}$ the restriction of $D_{\bar{\rho}}$ to the subcategory $\tilde{C}$, and by $\tilde{D}_{\bar{\rho}}^0$ the sub-functor of $\tilde{D}_{\bar{\rho}}$ of deformations $(t, d)$ with constant determinant, that is such that $d = \bar{d}$. Those three functors $D_{\bar{\rho}}, \tilde{D}_{\bar{\rho}}, \tilde{D}_{\bar{\rho}}^0$ are representable by local algebras $R_{\bar{\rho}}, \tilde{R}_{\bar{\rho}}, \tilde{R}_{\bar{\rho}}^0$, and one has clearly a natural isomorphism $R_{\bar{\rho}}/pR_{\bar{\rho}} = \tilde{R}_{\bar{\rho}}$ and a natural surjective map $\tilde{R}_{\bar{\rho}} \to \tilde{R}_{\bar{\rho}}^0$.

**Definition 1.** Let $\bar{\rho}$ be a modular representation $G_{\mathbb{Q}, p} \to \text{GL}_2(\mathbb{F})$. We shall say that $\bar{\rho}$ is **unobstructed** if the tangent space $\text{Tan} \tilde{D}_{\bar{\rho}}^0$ to the functor $\tilde{D}_{\bar{\rho}}^0$ has dimension 2.

One can prove that this tangent space always have dimension at least 2. When $\bar{\rho}$ is irreducible, by the result of Chenevier mentioned above, the functor $\tilde{D}_{\bar{\rho}}^0$ is just the usual functor of deformations of $\bar{\rho}$, as representation and with constant determinant on the category $\tilde{C}$. Hence we see that $\bar{\rho}$ is unobstructed in our sense if and only if it is in the sense of Mazur (cf. [18, §1.6]), that is if and only if $H^1(G_{\mathbb{Q}, p}, \text{ad}^0 \bar{\rho})$ has dimension 2. For examples of irreducible $\bar{\rho}$ which are unobstructed, or obstructed, see [4] and other works of the same author. By contrast, reducible representations are often, or, admitting the Vandiver conjecture, always unobstructed: when $p = 2$, then $\bar{\rho} = 1 \oplus 1$ is unobstructed by [5, Lemma 5.3] (see also [1, Prop. 3]), and when $p > 2$ see Theorem 22.

It is easy to glue all the pseudo-representations attached to the representations associated to modular eigenforms of level 1 and all weights, in order to prove:

---

3When $p > 2$, this condition is automatic and can be forgotten. Indeed, since $d(c) \mod m_S = \det \bar{\rho}(c) = -1$, and $d(c)^2 = 1$ it follows from Hensel’s lemma that $d(c) = -1$. Then $(d)$ applied to $g = c, h = 1$, implies that $0 = 2t(c)$, hence $t(c) = 0$. 
Proposition 2. Fix a modular representation $\rho$. There exists a unique continuous pseudo-representation $(\tau, \delta) : G_{\mathbb{Q},p} \rightarrow \mathbb{T}_\rho$ such that $\tau(\text{Frob}_\ell) = T_\ell$ for all $\ell \neq p$.

It satisfies also $\delta(\text{Frob}_\ell) = \ell S_\ell$ for all primes $\ell \neq p$, $\tau(e) = 0$, and we have $\tau \pmod{m_{\mathbb{T}_\rho}} = \text{tr} \bar{\rho}$, $\delta \pmod{m_{\mathbb{T}_\rho}} = \text{det} \bar{\rho}$.

Let $(\tilde{\tau}, \tilde{\delta})$ the pseudo-representation obtained by composing $(\tau, \delta)$ with the natural morphisms $\mathbb{T}_\rho \rightarrow A_{\bar{\rho}}$. Thus $\tilde{\tau} \pmod{m_{A_{\bar{\rho}}}} = \text{tr} \bar{\rho}$, $\tilde{\delta} \pmod{m_{A_{\bar{\rho}}}} = \text{det} \bar{\rho}$. Moreover, the determinant $\tilde{\delta} : G_{\mathbb{Q},p} \rightarrow A_{\bar{\rho}}^*$ is constant (more precisely equal to $\omega_k p$ where $k$ is the weight of a modular form associated to $\bar{\rho}$.)

We omit the proof of that proposition, which is simple and exactly similar as its case $p = 2$ which can be found in [1, Step 1 of the proof of Theorem 1].

The pseudo-representation $(\tau, \delta)$ (resp. $(\tilde{\tau}, \tilde{\delta})$) of the proposition is an element of $D_{\bar{\rho}}(\mathbb{T}_\rho)$ (resp. of $D_{\bar{\rho}}(A_{\bar{\rho}})$) hence defines a morphism $R_\rho \rightarrow \mathbb{T}_\rho$ in the category $\mathcal{C}$ (resp. a morphism $\tilde{R}_\rho^0 \rightarrow A_{\bar{\rho}}$ in the category $\tilde{\mathcal{C}}$). These morphisms are surjective, because their images contain $T_\ell$ and $\ell S_\ell$, as the image of the trace and determinant of Frob $\ell$ for the universal pseudo-representation, respectively, for all $\ell \neq p$.

1.5. Statement of the main results. We shall prove the following three results concerning the Hecke algebra $A_{\bar{\rho}}$ and its relation with the deformation ring $\tilde{R}_\rho^0$.

Theorem I. Assume that $\bar{\rho}$ is unobstructed. Then the morphism $\tilde{R}_\rho^0 \rightarrow A_{\bar{\rho}}$ is an isomorphism, and $A_{\bar{\rho}}$ is isomorphic to a power series ring in two variables $\mathbb{F}[[x,y]]$

Theorem II. Assume that $\bar{\rho}$ is absolutely irreducible after restriction to the Galois group of $\mathbb{Q}(\zeta_p)$. If $\bar{\rho}|_{G_{\mathbb{Q},p}}$ is reducible, assume in addition that $\bar{\rho}|_{G_{\mathbb{Q},p}}$ is not isomorphic to $\chi \otimes \begin{pmatrix} 1 & 0 \\ \ast & 1 \end{pmatrix}$ nor to $\chi \otimes \begin{pmatrix} 1 & \ast \\ 0 & \omega_p \end{pmatrix}$, where $\chi$ is any character $G_{\mathbb{Q},p} \rightarrow \mathbb{F}^*$ and $\ast$ may be trivial or not. Then $\tilde{R}_\rho^0 \rightarrow A_{\bar{\rho}}$ is an isomorphism and both rings have dimension 2.

Theorem III. In any case, $\tilde{R}_\rho^0$ and $A_{\bar{\rho}}$ have dimension at least 2.

When $p = 2$, Theorem I is proved (hence Theorem III as well, and Theorem II is empty) in [19], [20] (for the part concerning the structure of $A$) and [1] (for the relation with $\tilde{R}_\rho^0$). For $p = 3$, we sketch a proof in the appendix of this paper.

Let us give an idea of the proof of Theorem III and Theorem II in the case $p > 3$ (as Theorem I follows easily from Theorem III and the definition of unobstructed, see 8). For Theorem III, we start with results of Gouvêa-Mazur obtained with the "infinite fern" method (hence using the deep results of Coleman on the existence of $p$-adic families of finite slope modular forms), which proves that dim $\mathbb{T}_\rho \geq 4$. We
need to relate the characteristic 0 Hecke-algebra $\mathbb{T}_\rho$ with the characteristic $p$ Hecke algebra $A_\rho$. There are various obstacles to a direct comparison. First $\mathbb{T}_\rho$ is obtained by the action of the Hecke operators on $S(\mathcal{O})$ while $A_\rho$ is obtained by the action of the same operators on $S(\mathbb{F})$, and $S(\mathbb{F})$ is not equal to $S(\mathcal{O}) \otimes_\mathcal{O} \mathbb{F}$. To circumvent this problem, we work with the larger rings of divided congruences in the sense of Katz, $D(\mathcal{O})$ and $D(\mathbb{F})$, for which we do have, by construction, $D(\mathcal{O}) \otimes_\mathcal{O} \mathbb{F} = D(\mathbb{F})$.

We then need to control the changes introduced in our Hecke algebras by the change of modules of modular forms. By definition, the Hecke algebra that acts on $D(\mathcal{O})$ is the same as the one, $\mathbb{T}$, constructed on $S(\mathcal{O})$. Moreover a result of Katz allows us to compare $D(\mathbb{F})$ and $S(\mathbb{F})$, and from this the Hecke algebras on $D(\mathbb{F})$ with the Hecke algebra $A$ constructed on $S(\mathbb{F})$. It therefore remains to compare the Hecke algebra $\mathcal{T}$ on $D(\mathcal{O})$ with the Hecke algebra on $D(\mathbb{F}) = D(\mathcal{O}) \otimes \mathbb{F}$. The main difficulty here is that the formation of Hecke algebras needs not commute with non-flat base changes. To solve the difficulty, we need to change again the Hecke algebras and replace them by their full counterpart, defined by the action of the $T_\ell$, $\ell S_\ell$ for $\ell \neq p$ and $U_p$. As the full Hecke algebras are in duality with $D(\mathcal{O})$, those do commute with non-flat base change.

Then it remains to control how the addition of the $U_p$ operator changes our Hecke algebras, both in characteristic $p$ and 0, which we do by using (resp. generalizing) a result of Jochnowitz. At the end of these comparisons of many Hecke algebras, we conclude that $A_\rho = \mathbb{T}_\rho/(p, T)$ where $T$ is in the maximal ideal of $\mathbb{T}$. It follows that $\dim A_\rho \geq 2$, since as we have said $\dim \mathbb{T}_\rho \geq 4$.

To prove Theorem II, we need to use, in addition of what have already been said, a result of Böckle, according to which $\mathbb{T}_\rho$ is of dimension exactly 4 under the hypotheses of Theorem II. To conclude, we prove that $\mathbb{T}_\rho$ is also flat over the Iwasawa algebra $\mathbb{Z}_p[[T]]$, which implies that $\dim \mathbb{T}_\rho/(p, T)$ is of dimension 2.

The authors thank Bas Edixhoven, Matthew Emerton, Mark Kisin, Barry Mazur and Jean-Pierre Serre, for their interest in this project and several useful conversations about it. They are also thankful to the referees of this paper for a careful reading and helpful suggestions.

In the sections §2 to §9 we assume $p > 3$. 
2. The divided congruences modules of Katz

This § and the next one intend to be a short exposition, without the proofs of the main results, of the theory of divided congruences of Katz, while introducing some objects and notations important for this article.

The divided congruences module of cuspidal forms of weight at most \( k \) and level 1, that we shall denote by \( D_{\leq k}(\mathcal{O}) \) is defined as the \( \mathcal{O} \)-submodule of \( S_{\leq k}(K) = \bigoplus_{i=0}^{k} S_i(K) \subset K[[q]] \) of forms whose \( q \)-expansion lies in \( \mathcal{O}[[q]] \). Thus, \( D_{\leq k}(\mathcal{O}) \) is a free of finite rank \( \mathcal{O} \)-module, which contains \( S_{\leq k}(\mathcal{O}) \) as a co-torsion sub-module.

We define the divided congruence module of cuspidal forms of level 1, denoted by \( D(\mathcal{O}) \) as \( \bigcup_{k=0}^{\infty} D_{\leq k}(\mathcal{O}) \) (the union being taken in \( \mathcal{O}[[q]] \)). The module \( D(\mathcal{O}) \) contains \( S(\mathcal{O}) \) as a co-torsion submodule.

Remark 3. Let us recall that the name divided congruences is justified by the following elementary fact: let \( f_i \in S_{k_i}(\mathcal{O}) \) a finite set of forms of distinct weights \( k_i \). Assume that these forms satisfy a congruence:

\[
\sum_{i} f_i \equiv 0 \pmod{p^n}
\]

for some integer \( n \). Then \( (\sum_{i} f_i)/\pi^n \) belongs to \( D(\mathcal{O}) \). And it is clear that every element of \( D(\mathcal{O}) \) is of this form.

Observe that the algebra \( D(\mathcal{O}) \) is not a graded sub-algebra of the graded (by the weight) algebra \( S(K) = \sum_{i=0}^{\infty} S_i(K) \). In the example above, \( (\sum_{i} f_i)/\pi^n \) belongs to \( D(\mathcal{O}) \) but the individual terms \( f_i/\pi^n \) in general do not.

A fundamental result on divided congruences is the following.

Theorem 4 (Katz). There exists a unique action of \( \mathbb{Z}_p^* \) on \( D(\mathcal{O}) \) denoted by \( (x,f) \mapsto x \cdot f \), such that for \( x \in \mathbb{Z}_p^* \), and \( f \in S_{k}(\mathcal{O}) \subset D(\mathcal{O}) \), \( x \cdot f = x^k f \)

Note that the uniqueness is easy, as knowing the action of \( x \) on each \( S_k(\mathcal{O}) \) implies knowing it on \( S(\mathcal{O}) \), which is a co-torsion sub-module of the torsion-free module \( D(\mathcal{O}) \). Concretely, if the \( f_i \) are as in (6), and \( f = (\sum_{i} f_i)/\pi^n \in D(\mathcal{O}) \), then \( x \cdot f \) has to be equal to \( (\sum_{i} x^{k_i} f_i)/\pi^n \). But the existence of the action is much more difficult, because, as noted by Katz and Hida, it is not clear that the \( q \)-expansion of \( (\sum_{i} x^{k_i} f_i)/\pi^n \) is in \( \mathcal{O}[[q]] \). Instead the construction of this action by Katz uses the geometric interpretation of divided congruences and the tower of Igusa. See [15, Corollary 1.7] for the proof.

We define \( D_{\leq k}(\mathbb{F}) \) as the image of \( D_{\leq k}(\mathcal{O}) \) by the reduction map \( f \mapsto \tilde{f}, \mathcal{O}[[q]] \rightarrow \mathbb{F}[[q]] \). This is similar to the definition of \( S_{\leq k}(\mathbb{F}) \) (which is a sub-module of \( D_{\leq k}(\mathbb{F}) \)),
but the following lemma provides an alternative definition of $D_{\leq k}(\mathcal{F})$ which does not hold for $S_{\leq k}(\mathcal{F})$.

**Lemma 5.** The natural map $D_{\leq k}(\mathcal{O}) \otimes_\mathcal{O} \mathbb{F} \to D_{\leq k}(\mathcal{F})$ is an isomorphism.

**Proof —** This is because $\mathcal{O}[[q]]/D_{\leq k}(\mathcal{O})$ is without torsion, which follows from the definition of $D_{\leq k}(\mathcal{O})$.  

We define $D(\mathbb{F})$ as the union of the $D_{\leq k}(\mathcal{F})$ for $k = 1, 2, 3, \ldots$. By definitions, $S(\mathbb{F}) \subset D(\mathbb{F})$. By the lemma, $\mathbb{Z}_p^*$ acts on $D(\mathbb{F})$. It is clear that this action preserves $S(\mathbb{F})$, since any $\tilde{f}$ in $S(\mathbb{F})$ is a sum $\sum_{i \in (\mathbb{Z}/p\mathbb{Z})^*} \tilde{f}_i$, where $\tilde{f}_i$ is the action of an $f_i \in \bigoplus_{k \equiv i \pmod{p-1}} S_k(\mathcal{O})$, and $x \in \mathbb{Z}_p^*$ acts on $\tilde{f}_i$ by $x \cdot \tilde{f}_i = \bar{x}^* \tilde{f}_i$, where $\bar{x}$ is the reduction mod $x$ in $\mathbb{F}_p^*$. In particular, $1 + p\mathbb{Z}_p$ acts trivially on $S(\mathbb{F})$.

**Theorem 6** (Katz). The space $S(\mathbb{F})$ is the space of invariants of $1 + p\mathbb{Z}_p$ acting on $D(\mathbb{F})$.

This is proved in [15, §4]; see also [13, Theorem 1.1].

We observe that the two results of Katz recalled in this section are proved only there for $p > 3$. We don’t know whether they also hold for $p = 2, 3$.

### 3. Hecke Operators on Divided Congruences

An important consequence of the existence of the action of $\mathbb{Z}_p^*$ on $D(\mathcal{O})$ (Theorem 4) is the possibility of defining Hecke operators on that module.

**Corollary and Definition 7** (Hida, cf. [13], page 243). For $\ell$ a prime $\neq p$, and $f = \sum_{n \geq 0} a_n q^n \in D(\mathcal{O})$, define $S_\ell(f) = \ell^{-2} (\ell \cdot f) \in D(\mathcal{O})$, and define an element $T_\ell f = \sum_{n \geq 1} a_n (T_\ell f) q^n \in \mathcal{O}[[q]]$ with

\begin{align*}
(7) \quad a_n(T_\ell f) & = a_{n\ell}(f) \text{ if } \ell \nmid n \\
(8) \quad a_n(T_\ell f) & = a_{n\ell}(f) + \ell^{-1} a_{n/\ell}(\ell \cdot f) \text{ if } \ell \mid n.
\end{align*}

Then $T_\ell f \in D(\mathcal{O})$. The operators $T_\ell$ and $S_\ell$ of $D(\mathcal{O})$ for every $\ell \neq p$ commute and act on the stable submodule $S(\mathcal{O})$ as the usual $T_\ell$’s and $S_\ell$’s.

We also define operators $T_n$ for $(n, p) = 1$ by the formulas (1) and (2).

**Proof —** Let $f \in D(\mathcal{O})$. Since $\ell \cdot f \in D(\mathcal{O})$, and $\ell$ is invertible in $\mathcal{O}$, $S_\ell f \in D(\mathcal{O})$. Also $T_\ell$ coincides with the usual operator $T_\ell$ for any form in $S_k(\mathcal{O})$. Hence if $f = (\sum_i f_i)/\pi^n$ with $f_i \in S_k(\mathcal{O})$, then $\pi^n T_\ell f = \sum_i T_\ell f_i$ by linearity hence $T_\ell f$ lies in $S_{\leq k}(K)$ for $k = \max(k_i)$. On the other hand, the coefficients of the $q$-expansion of $T_\ell f$ are in $\mathcal{O}$ by definition, so $T_\ell f \in D_{\leq k}(\mathcal{O}) \subset D(\mathcal{O})$. The other assertions are clear.  

\[ \square \]
We define the operators $T_\ell$ and $S_\ell$, and $T_n$ for $n$ coprime to $p$, on $D(\mathbb{F})$ by reducing the operators with the same name on $D(O)$ modulo $p$.

**Lemma 8.** The sub-algebra of $\text{End}_O(D_{\leq k}(O))$ generated by the Hecke operators $T_n$ for $p \nmid n$ is naturally isomorphic to $\mathbb{T}_k$ (defined in §1.2).

**Proof** — Denote temporarily by $\mathbb{T}'_k$ the sub-algebra of $\text{End}_O(D_{\leq k}(O))$ generated by the Hecke operators $T_n$ for $p \nmid n$. The restriction from $D_{\leq k}(O)$ to $S_{\leq k}(O)$ defines a morphism of $O$-algebras $\mathbb{T}'_k \to \mathbb{T}_k$, which is surjective because its image contains all the $T_n$ for $p \nmid n$. Let $u \in \mathbb{T}'_k$ be an element of the kernel of that map. Then by definition $u$ acts trivially on $S_{\leq k}(O)$. Therefore, $u$ factors as a map $D_{\leq k}(O)/S_{\leq k}(O) \to D_{\leq k}(O)$. Since the source of this map is torsion while the target is torsion free, $u = 0$, and the map $\mathbb{T}'_k \to \mathbb{T}_k$ is an isomorphism $\square$

In particular the algebra $\mathbb{T}$ (see 1.2) acts faithfully on $D(O)$, and we can see it as a sub-algebra of $\text{End}_O(D(O))$.

**Lemma 9.** The homomorphism $\phi: \mathbb{Z}_p^* \to \text{End}_O(D(O))$, defined by $\phi(x)f = x \cdot f$, $f \in D(O)$ takes values in the sub-algebra $\mathbb{T}$.

**Proof** — Let us provide $D(O)$ with the sup norm $|\sum a_nq^n| = \sup_n |a_n|$, and $\text{End}_O(D(O))$ with the weak topology, so that a sequence of operators $u_n \in \text{End}_O(D(O))$ converges to $u$ if and only if for every $f \in D(O)$, $|u_n f - uf|$ converges to 0. We claim that $\mathbb{T}$ is closed in $\text{End}_O(D(O))$. Indeed, if $u_n \in \mathbb{T}$, and $(u_n)$ converges to $u \in \text{End}_O(D(O))$, then for every $k \geq 0$, the restriction of $u$ to $D_{\leq k}(O)$ is the limit of the restriction of $u_n$ to $D_{\leq k}(O)$, hence is in $\mathbb{T}_k$ since $\mathbb{T}_k$ is closed (even compact) in the finite-type $O$-module $\text{End}_O(D_{\leq k}(O))$. This shows that $u$ is in $\lim_{\leftarrow} \mathbb{T}_k = \mathbb{T}$, hence the claim.

For the weak topology, the map $\phi: \mathbb{Z}_p^* \to \text{End}_O(D(O))$ is continuous, since for any given $f \in D(O)$, we can write $f = (\sum_i f_i)/\pi^n \in D(O)$ with $f_i \in S_i(O)$, and $x \cdot f = (\sum_i x^i f_i)/\pi^n$ which makes clear that if $x_n$ converges to $x$ in $\mathbb{Z}_p^*$, then $|x_n f - xf|$ converges to 0.

For $\ell \neq p$ a prime number, one has $\phi(\ell) = \ell^2 S_\ell \in \mathbb{T}$. If $x \in \mathbb{Z}_p^*$, there exists by Dirichlet’s theorem on primes in arithmetic sequences a sequence of primes $\ell_n$ (different from $p$) converging to $x$ $p$-adically. Therefore $\phi(\ell_n)$ converges to $\phi(x)$ in $\text{End}_O(D(O))$. Hence $\phi(x) \in \mathbb{T}$. $\square$
Remark 10. The proof of the lemma shows that the two natural topologies one can consider on $\mathcal{T}$ are the same: the topology of the projective limit $\varprojlim T_k$, each $T_k$ having its natural topology of finite rank $\mathcal{O}$-modules; and the topology obtained by restriction of the weak topology on $\text{End}_\mathcal{O}(D(\mathcal{O}))$. Hence an equivalent definition of $\mathcal{T}$ would be as the closed subalgebra of $\text{End}_\mathcal{O}(D(\mathcal{O}))$ (for its weak topology) generated by the $T_\ell$ and $S_\ell$.

Let us define the Iwasawa algebra $\Lambda = \mathcal{O}[[1 + p\mathbb{Z}_p]]$. By choosing a topological generator (say $1 + p$) of $1 + p\mathbb{Z}_p$ one determines an isomorphism $\Lambda \cong \mathcal{O}[[T]]$ under which the maximal ideal $m_\Lambda$ of $\Lambda$ becomes $\langle \pi, T \rangle$. The morphism $\phi : 1 + p\mathbb{Z}_p \to \mathcal{T}^*$ defines a morphism $\psi : \Lambda \to \mathcal{T}$. Using that morphism, one regards $\mathcal{T}$ as a $\Lambda$-algebra.

4. Divided congruences of level $\Gamma_0(p)$

We shall also need a variant with level $\Gamma_0(p)$: $S_k(\Gamma_0(p), K)$ denotes the space of cusp forms of weight $k$ and level $\Gamma_0(p)$ with coefficients in $K$. The divided congruence module of cuspidal forms of weight at most $k$ and level $\Gamma_0(p)$, that we shall denote by $D_{\leq k}(\Gamma_0(p), \mathcal{O})$ is defined as the $\mathcal{O}$-submodule of $S_{\leq k}(\Gamma_0(p), K) = \bigoplus_{i=0}^k S_i(\Gamma_0(p), K)$ of forms whose $q$-expansion lies in $\mathcal{O}[[q]]$. Similarly, the divided congruence module of cuspidal forms of level $\Gamma_0(p)$ is defined as $D(\Gamma_0(p), \mathcal{O}) = \bigcup_{k=0}^\infty D_{\leq k}(\Gamma_0(p), \mathcal{O})$. The theorems and corollary above also hold (with the same references) for $D(\Gamma_0(p), \mathcal{O})$ instead of $D(\mathcal{O})$.

Proposition 11. The closure of $D(\mathcal{O})$ and $D(\Gamma_0(p), \mathcal{O})$ in $\mathcal{O}[[q]]$ (provided with the topology of uniform convergence) are equal.

Proof — Their common closure is the space of $p$-adic modular functions of tame level 1, denoted $V_{par}(\mathcal{O}, 1)$ in [11], see loc. cit., Proposition I.3.9. □

Corollary 12. There is an isomorphism preserving $q$-expansions $D(\Gamma_0(p), \mathcal{O}) \otimes_\mathcal{O} \mathbb{F} \simeq D(\mathbb{F})$.

We call $\mathcal{T}_k(\Gamma_0(p))$ the sub-algebra of $\text{End}_\mathcal{O}(\Gamma_0(p), D_{\leq k}(\mathcal{O}))$ generated by the Hecke operators $T_n$ for $p \nmid n$, and we define $\mathcal{T}(\Gamma_0(p))$ as $\varprojlim_k \mathcal{T}_k(\Gamma_0(p))$

Corollary 13. The algebras $\mathcal{T}(\Gamma_0(p))$ and $\mathcal{T}$ are naturally isomorphic.

Proof — The natural morphism $r : \mathcal{T}(\Gamma_0(p)) \to \mathcal{T}$ is obtained by the projective limit of the surjective restriction maps $\mathcal{T}_k(\Gamma_0(p)) \to \mathcal{T}_k$. Hence $r$ is surjective. The algebra $\mathcal{T}(\Gamma_0(p))$ acts faithfully on $D(\Gamma_0(p), \mathcal{O})$. By continuity of the Hecke
Let us recall that the operator $U_p$ is defined on $q$-expansions by $U_p(\sum a_n q^n) = \sum a_{pn} q^n$. This operator leaves stable the subspace of modular forms $S_{\leq k}(\Gamma_0(p), K)$ of $K[[q]]$, and since it also preserves the integrality of coefficients, it leaves stable $D_{\leq k}(\Gamma_0(p), \mathcal{O})$ and $D(\Gamma_0(p), \mathcal{O})$. By reduction, the subspace $D_{\leq k}(\Gamma_0(p), \mathbb{F})$ of $\mathbb{F}[[q]]$ is also stable by $U_p$, and so is the subspace $D(\Gamma_0(p), \mathbb{F}) = D(\mathbb{F})$ (cf. Corollary 12) of $\mathbb{F}[[q]]$. Note that the subspaces $S_{\leq k}(\mathbb{F}) \subset D_{\leq k}(\mathbb{F})$ of $\mathbb{F}[[q]]$ are also stable by $U_p$, since they are stable by $T_p$ and in characteristic $p$, the operators $T_p$ and $U_p$ coincide.

We define the full Hecke algebras $\mathcal{T}_k^{\text{full}}$ as the subalgebra of $\text{End}_{\mathcal{O}}(D_{\leq k}(\Gamma_0(p), \mathcal{O}))$ generated by the Hecke operators $T_\ell$ and $S_\ell$ for $\ell$ prime different form $p$, and by $U_p$. We let $\mathcal{T}_k^{\text{full}} = \varprojlim \mathcal{T}_k^{\text{full}}$. We define the following full Hecke algebras in characteristic $p$: $DA_k^{\text{full}}$ (resp. $A_k^{\text{full}}$) is the sub-algebra of $\text{End}_\mathbb{F}(D_{\leq k}(\mathbb{F}))$ (resp. of $\text{End}_\mathbb{F}(S_{\leq k}(\mathbb{F}))$) generated by the the Hecke operators $T_\ell$ and $S_\ell$ for $\ell$ prime different form $p$, and by $U_p$. We let $DA_k^{\text{full}} = \varprojlim DA_k^{\text{full}}$ and $A_k^{\text{full}} = \varprojlim A_k^{\text{full}}$.

We have natural surjective morphisms of algebras (sending Hecke operators to Hecke operators with the same name) $\mathcal{T}_k^{\text{full}} \otimes_{\mathcal{O}} \mathbb{F} \to DA_k^{\text{full}}$ (induced by the reduction map $D_{\leq k}(\Gamma_0(p), \mathcal{O}) \to D_{\leq k}(\Gamma_0(p), \mathbb{F})$) and $DA_k^{\text{full}} \to A_k^{\text{full}}$ (induced by the inclusion $S_{\leq k}(\mathbb{F}) \subset D_{\leq k}(\mathbb{F}) \subset D_{\leq k}(\Gamma_0(p), \mathbb{F}))$, hence by passage to the limit, surjective maps $\mathcal{T}_k^{\text{full}} \to DA_k^{\text{full}} \to A_k^{\text{full}}$.

**Proposition 14.** The pairings $\mathcal{T}_k^{\text{full}} \times D_{\leq k}(\mathcal{O}) \to \mathcal{O}$, $DA_k^{\text{full}} \times D_{\leq k}(\mathbb{F}) \to \mathbb{F}$ and $A_k \times S_{\leq k}(\mathbb{F})$ given by $(t, f) \mapsto a_1(tf)$ are perfect.

**Proof —** This is elementary and well-known. \qed

**Corollary 15.** The map $\mathcal{T}_k^{\text{full}} \to DA_k^{\text{full}}$ induces an isomorphism $\mathcal{T}_k^{\text{full}} \otimes_{\mathcal{O}} \mathbb{F} \simeq DA_k^{\text{full}}$. Hence an isomorphism $\mathcal{T}_k^{\text{full}} \otimes_{\mathcal{O}} \mathbb{F} \simeq DA_k^{\text{full}}$. 


Proof — It is clear that the map $\mathcal{T}_k^{\text{full}} \otimes \mathcal{O} \mathcal{F} \to DA_k^{\text{full}}$ is surjective. The preceding proposition assures that its source has dimension the rank of $D_{\leq k}(\mathcal{O})$ and that its image has dimension $\dim D_{\leq k}(\mathcal{F})$. These two numbers are equal since $D_k(\mathcal{O})$ is torsion-free. This proves the corollary.

The composition $\Lambda \to \mathcal{T} \to \mathcal{T}^{\text{full}}$ defines a structure of $\Lambda$-algebra on $\mathcal{T}^{\text{full}}$. Those results combined with the main results of Katz yield:

**Proposition 16.** One has $\mathcal{T}^{\text{full}}/m_\Lambda \mathcal{T}^{\text{full}} \simeq A^{\text{full}}$

**Proof —** Set $\tilde{\Lambda} = \Lambda / \pi \Lambda$ and $m_{\tilde{\Lambda}}$ its maximal ideal (which is principal). By the above corollary, $\mathcal{T}^{\text{full}}/\pi \mathcal{T}^{\text{full}} \simeq DA^{\text{full}}$ as $\tilde{\Lambda}$-module. By Theorem 6, $S(\mathcal{F}) = D(\mathcal{F})[m_{\tilde{\Lambda}}]$. By Prop. 14, this implies $A = DA/m_{\tilde{\Lambda}} DA = \mathcal{T}/m_{\tilde{\Lambda}} \mathcal{T}$. □

6. Local components of normal and full Hecke algebras

The Hecke algebras $\mathcal{T}^{\text{full}}$ and $A^{\text{full}}$ are semi-local, and for both of them, their local components are in bijection with the set of $\mathcal{F}$-valued systems of eigenvalues of all the Hecke operators $T_n$ that appear in $S(\mathcal{F})$, or what amounts to the same, the pairs $(\rho, \lambda)$, where $\rho : G_{\mathbb{Q}, p} \to \text{GL}_2(\mathcal{F})$ is a modular representation attached to some eigenform $f \in S(\mathcal{F})$, and $\lambda$ is the eigenvalue of $U_p$ on $f$. We shall denote by $\mathcal{T}^{\text{full}}_{\rho, \lambda}$ and $A^{\text{full}}_{\rho, \lambda}$ the corresponding local algebras.

**Proposition 17.** One has a natural isomorphism of $A_{\rho}$-algebras $A_{\rho}[[U_p]] \simeq A^{\text{full}}_{\rho, 0}$, and a natural isomorphism of $\mathcal{T}_{\rho}$-algebras $\mathcal{T}_{\rho}[[U_p]] \simeq \mathcal{T}^{\text{full}}_{\rho, 0}$.

**Proof —** The first isomorphism is due to Jochnowitz, see [14]. For the second we mimic her proof with some adaptations.

We have a natural surjective map $\mathcal{T}_k[U_p] \to \mathcal{T}_k^{\text{full}}$. Since $U_p$ is topologically nilpotent in $\mathcal{T}_k^{\text{full}}$, this map induces by passage to the limit and localization a surjective map $\mathcal{T}_{\rho, 0}[[U_p]] \to \mathcal{T}_{\rho, 0}^{\text{full}}$. By corollary 13, the algebra $\mathcal{T}$ (resp. $\mathcal{T}^{\text{full}}$) acts faithfully on $D(\Gamma_0(p), \mathcal{O})$, and the quotient $\mathcal{T}_{\rho}$ of $\mathcal{T}$ (resp. $\mathcal{T}^{\text{full}}_{\rho, 0}$) is the largest quotient that acts faithfully on $D(\Gamma_0(p), \mathcal{O})_{\rho}$ (resp. $D(\Gamma_0(p), \mathcal{O})_{\tilde{\rho}}$) where $D(\Gamma_0(p), \mathcal{O})_{\rho}$ (resp. $D(\Gamma_0(p), \mathcal{O})_{\tilde{\rho}}$) is the (direct) sum of the generalized eigenspaces for all the $T_\ell$ and $S_\ell$ for $\ell \neq p$ (resp. and for $U_p$) with system of eigenvalues in $\mathcal{O}$ that lift the $\mathcal{F}$-valued system attached to $\tilde{\rho}$ (resp. to $(\tilde{\rho}, 0)$). Therefore, to prove that $\mathcal{T}_{\rho, 0}[[U_p]] \to \mathcal{T}_{\rho, 0}^{\text{full}}$ is an isomorphism it is sufficient to prove that $\mathcal{T}_{\tilde{\rho}, 0}[[U_p]]$ acts faithfully on $D(\Gamma_0(p), \mathcal{O})_{\tilde{\rho}, 0}$. 
Recall that on $D(\Gamma_0(p), \mathcal{O})_{p,0}$ we have an operator $V$ which acts on $q$-expansions as $\sum a_n q^n \mapsto \sum a_n q^{pn}$ (cf. e.g. [11, §II.2]). One sees immediately on $q$-expansion that $U_p V = \text{Id}$ and that $VU_p$ is a projector. Thus $V$ is injective on $D(\Gamma_0(p), \mathcal{O})_{p,0}$, $U_p$ is surjective, and $VU_p$ is the projector of kernel $\text{Ker} U_p$ and image $\text{Im} V$.

We claim that for every $t \in T_\bar{p}$, $t \neq 0$, there exists $g \in D(\Gamma_0(p), \mathcal{O})_{p,0}$ such that $U_p g = 0$ but $tg \neq 0$. Indeed there exists an $f$ in $D(\Gamma_0(p), \mathcal{O})_{\bar{p}}$, such that $tf \neq 0$. Let $i$ be the smallest integer such that $tf$ has a coefficient $a_n \neq 0$ with $p^i \mid n$. Then $U_p^i tf$ has a coefficient $a_n \neq 0$ with $n$ relatively prime to $p$. Therefore $U_p^i tf$ is not in the image of $V$, hence is not in the image of the projector $VU_p$, hence is not in the kernel of the projector $1 - VU_p$. That is, $(1 - VU_p)U_p^i tf \neq 0$. Define $g = (1 - VU_p)U_p^i f$. Then clearly $U_p g = 0$ (so $g \in D(\Gamma_0(p), \mathcal{O})_{\bar{p},0}$) and because $t$ commutes with $U_p$ and $V$, $tg \neq 0$, and the claim is proved.

Now let us prove that $T_\bar{p}(U_p)$ acts faithfully on $D(\Gamma_0(p), \mathcal{O})_{p,0}$. Let $\sum_{j=n}^{\infty} t_j U_p^j \in T_\bar{p}(U_p)$ with $t_j \in T_\bar{p}$ and $t_n \neq 0$. Then by the claim, there is $g \in D(\Gamma_0(p), \mathcal{O})_{p,0}$ such that $t_n g \neq 0$ but $U_p g = 0$. Let $h = V^n g$, so that $U_p^n h = g$. Then $t_n(U_p^n h) = t_n g \neq 0$, but $U_p^{n+1} h = U_p g = 0$, and so $U_p^i h = 0$ for all $i > n$, and $(\sum_{j=n}^{\infty} t_j U_p^j)h \neq 0$. On the other hand, since $U_p^{n+1} h = 0$, $h$ is the generalized eigenspace of $U_p$-eigenvalue 0, hence $h \in D(\Gamma_0(p), \mathcal{O})_{p,0}$, which proves the faithfulness.

7. Proof of Theorem III

We need to prove that $\dim A_{\bar{p}} \geq 2$. It is equivalent to prove $\dim A_{\bar{p}}[[U_p]] \geq 3$, that is by Prop. 17, $\dim A_{\bar{p},0}^{\text{full}} \geq 3$. By Proposition 16, $A_{\bar{p},0}^{\text{full}}$ is isomorphic to $T_{\bar{p},0}^{\text{full}}/m_\Lambda T_{\bar{p},0}^{\text{full}}$. Since the ideal $m_\Lambda$ is generated by two elements, one has by the hauptidealsatz that $\dim A_{\bar{p},0}^{\text{full}} \geq \dim T_{\bar{p},0}^{\text{full}} - 2$ so it suffices to prove that $\dim T_{\bar{p},0}^{\text{full}} \geq 5$. But by Prop. 17, that’s $\dim T_{\bar{p}}[[U_p]] = \dim T_{\bar{p}} + 1$. It therefore suffices to prove that $\dim T_{\bar{p}} \geq 4$. But that is precisely the result given by Gouvêa-Mazur’s infinite fern argument, cf. [12] and [9].

8. Proof of Theorem I

Assuming that $\bar{p}$ is unobstructed, we need to prove that the surjective map $\tilde{R}_{\bar{p}}^0 \to A_{\bar{p}}$ is an isomorphism of local regular rings of dimension 2. But by assumption, the cotangent space of $\tilde{R}_{\bar{p}}^0$ has dimension 2, while the Krull dimension of $A_{\bar{p}}$ is at least 2 by Theorem III. The result follows.
9. Proof of Theorem II

**Theorem 18** (Böckle, Diamond-Flach-Guo, Gouvêa-Mazur, Kisin). *Under the hypotheses of Theorem II, the natural map \( \bar{R}_\rho \to \bar{T}_\rho \) is an isomorphism between local rings of dimension 4.*

*Proof —* (compare [9]). Under more restrictive assumptions than Theorem II, namely under the assumption that \( \bar{\rho}_{|G_{\mathbb{Q}_p}} \), if irreducible, is flat up to torsion by a character (cf. [3, Assumption (2.1)]), the fact that \( \bar{R}_\rho \to \bar{T}_\rho \) is an isomorphism is proved in [3, Theorems 3.1 and 3.9]. In [3], this assertion is used only to ensure the validity of Theorem 2.8 *loc. cit.*, due to Diamond ([6, Theorem 1.1]). However, Diamond, with Flach and Guo, later generalized [3, Theorem 2.8], proving it under the hypotheses (ii) of our theorem II: cf. [7, Theorem 3.6]. Therefore, Böckle’s results ([3, Theorems 3.1 and 3.9]) are true, with the same proof, under the hypotheses of Theorem II.

Once we know that \( \bar{R}_\rho \to \bar{T}_\rho \) is an isomorphism, we conclude by recalling that \( \bar{T}_\rho \) has dimension at least 4 by the infinite fern argument of Gouvêa-Mazur (cf. [12]), and that (the tangent space of) \( \bar{R}_\rho \) has dimension at most 4 by a theorem of Kisin (under weaker assumptions than ours), cf. [17, Main Theorem]. □

**Lemma 19.** *The algebra \( \bar{T}_\rho \) is flat over \( \Lambda \) (for the structure of \( \Lambda \)-algebra on \( \bar{T}_\rho \) defined at the end of §3).*

*Proof —* We first observe that \( \bar{T}_\rho \) is flat over \( \mathcal{O} \), because it is torsion-free as a sub-module of \( \bar{T} \), which is itself torsion-free as projective limit of the \( \bar{T}_k \), which are sub-modules of the torsion-free modules \( \text{End}_\mathcal{O}(S_{\leq k}(\mathcal{O})) \). Hence \( \bar{R}_\rho \) is flat over \( \mathcal{O} \).

Second, let \( \chi : G \to \mathcal{O}^* \) be the Teichmüller lift of the character \( \det \rho \). Let us call \( D^0_\rho \) the functor which parametrizes the deformation of \( \bar{\rho} \) with constant determinant \( \chi \). Let \( R^0_\rho \) be the ring representing \( D^0_\rho \). Let us call \( D_{\det \rho} \) the functor of deformation of the character \( \det \bar{\rho} \) which as we have seen is represented by the Iwasawa algebra \( \Lambda \). Consider the morphism of functors \( D_\rho \to D_{\det \rho} \times D^0_\rho \), which to a deformation \( \rho : G_{\mathbb{Q}_p} \to \text{GL}_2(S) \), attaches the pair \( (\det \rho, \rho \otimes ((\det \rho)^{-1} \chi)^{1/2}) \). Here, note that \( (\det \rho)^{-1} \chi \equiv 1 \pmod{m_S} \) by definition of \( \chi \), hence since \( p > 2 \) the character \( (\det \rho)^{-1} \chi \) has a unique square root by Hensel’s lemma. One checks easily that this morphism of functor is an isomorphism. Hence we get a natural isomorphism

\[
\Lambda \otimes_{\mathcal{O}} R^0_\rho \to R_\rho.
\]
Note that the map $\Lambda \to R_\rho$ induced by this isomorphism is by definition the same as the one introduced in §3.

From that isomorphism follows the fact that $R^0_\rho$ is flat over $\mathcal{O}$ (for if it had torsion, so would have $R^0_\rho \otimes \mathcal{O} \Lambda$ since $\Lambda$ is flat over $\mathcal{O}$, contradicting the fact that $T_\rho$ has no $\mathcal{O}$-torsion.) Therefore, $R_\rho = R^0_\rho \otimes \mathcal{O} \Lambda$ is flat over $\Lambda$ by universality of flatness.

To conclude, we observe that the natural diagram

$$
\begin{array}{ccc}
R_\rho & \longrightarrow & T_\rho \\
\downarrow & & \downarrow \\
\Lambda & \rightarrow & T_\rho \\
\end{array}
$$

is commutative. Indeed, the determinant $\delta : G_{\mathbb{Q},p} \to T^*_\rho$ (see Prop. 2) is a deformation of det $\rho$, hence defines a morphism $\psi' : \Lambda \to T_\rho$ since $\Lambda$ is the universal deformation ring of det $\rho$. Moreover, it is clear from the definition of the map $R_\rho \to T_\rho$ that the diagram above commutes if the map $\Lambda \to T_\rho$ is replaced by $\lambda$. Hence we are reduce to showing that $\psi'$ is the same map as the map $\psi$ defined in §3, and to do so, in is enough to do so after composition my any map $\lambda_f : T_\rho \to \overline{K}$ attached to a modular eigenform $f \in S_k(\Gamma)$ for some integer $k$. But $(\lambda_f \circ \psi)(x) = x^{k-1}$ for $x \in \mathbb{Z}_p^*$ by definition of $\psi$ and since $f$ is of weight $k$, while $(\lambda_f \circ \psi')(\ell) = \det \rho_f(\text{Frob}_\ell) = \ell^{k-1}$ for any prime $\ell \neq p$. By continuity, it follows that $\psi = \psi'$.

Since the upper horizontal map of (9) is an isomorphism, it follows that $T_\rho$ is flat over $\Lambda$.□

It follows from the lemma that $T^{\text{full}}_{\rho,0} = T_{\rho}[U_p]$ is also flat over $\Lambda$. Thus the dimension of $T^{\text{full}}_{\rho,0}/m_\Lambda T^{\text{full}}_{\rho,0}$ is equal by [8, Theorem 10.10] to $\dim T^{\text{full}}_{\rho,0} - 2 = 5 - 2 = 3$, hence $A^{\text{full}}_{\rho,0} = A_{\rho}[U_p]$ has dimension 3 and $A_{\rho}$ has dimension 2. This concludes the proof.

10. When are the reducible modular representations unobstructed?

In this §, we discuss the condition, for a modular representation $\rho$, of being unobstructed (definition 1). As noted just after the definition, when $\rho$ is absolutely irreducible, this notion coincide Mazur’s notion of being unobstructed, and has thus been extensively discussed in the literature. This is why we restrict ourselves in this section to a $\rho$ which is reducible. We shall see that in this case, many (conjecturally all) representations are unobstructed.
In the case $p = 2$, we have already noted that the only modular representation $\bar{\rho} = 1 \oplus 1$ was unobstructed. Let us assume that $p > 2$ for the rest of this section.

Since our modular representation $\bar{\rho}$ is reducible, and by definition semi-simple, it is the direct sum of two characters $G_{\mathbb{Q},p} \to \mathbb{F}^*$. By class field theory, any character $G_{\mathbb{Q},p} \to \mathbb{F}^*$ is of the form $\omega_p^a$, where $\omega_p$ is the cyclotomic character modulo $p$ and $a$ is an integer in $\{0, 1, \ldots, p - 2\}$. Hence $\bar{\rho}$ is, up to a twist, of the form $1 \oplus \omega_p^a$, with $a$ odd since $\bar{\rho}$ is, and one has $\text{tr} \bar{\rho} = 1 + \omega_p^a$, det $\bar{\rho} = \omega_p^a$.

The functor $\tilde{D}_0^0$ is the functor of deformations of $(\bar{t}, \bar{d})$ as pseudo-representations $(t, d)$ in the sense of Chenevier, with the condition $d = 1$. (Since $p > 2$, it is by [5] the same functor as the functor which attaches to $S$ a pseudo-character $t : G \to S$ of dimension 2, deforming $\bar{t}$ and satisfying the condition $d(g) := (t^2(g) - t(g^2)) / 2 = 1$ for all $g \in G_{\mathbb{Q},p}$.) Let $\text{Tan}(\tilde{D}_0^0)$ be the tangent space of that functor.

**Proposition 20.** The dimension of $\text{Tan}(\tilde{D}_0^0)$ is $1 + \dim H^1(G_{\mathbb{Q},p}, \omega^a) \dim H^1(G_{\mathbb{Q},p}, \omega^{-a})$

**Proof —** By the main theorem of [2], that tangent space lies in an exact sequence:

$$0 \to \text{Tan} \left( (\tilde{D}_{\omega_p^a} \oplus \tilde{D}_{\omega_p^{-a}})^0 \right) \to \text{Tan}(\tilde{D}_0^0) \to H^1(G_{\mathbb{Q},p}, \omega^a) \otimes H^1(G_{\mathbb{Q},p}, \omega^{-a}) \to H^2(G_{\mathbb{Q},p}, 1)$$

Here, $\tilde{D}_{\omega_p^{\pm a}}$ is the functor of deformations of $\omega_p^{\pm a}$ as character of $G_{\mathbb{Q},p}$, which is the same as for any character and has a tangent space of dimension 1, and the functor $(\tilde{D}_{\omega_p^a} \oplus \tilde{D}_{\omega_p^{-a}})^0$ parametrizes pair of deformations of $\omega_p^a$ and $\omega_p^{-a}$ whose product stays equal to 1. It is then clear that the dimension of the tangent space of this functor is 1. On the other hand, $H^2(G_{\mathbb{Q},p}, 1) = 0$ as is well known (e.g. as a consequence of Tate’s global Euler-Poincaré’s formula). The proposition follows. □

We shall use the following rather standard notation: for $\chi$ a character of $\text{Gal}(\mathbb{Q}(\mu_p)/\mathbb{Q})$, we denote by $A(\chi)$ the part of the $p$-torsion subgroup of the class group $\text{Cl}(\mathbb{Q}(\mu_p))$ on which $\text{Gal}(\mathbb{Q}(\mu_p)/\mathbb{Q})$ acts by $\chi$.

**Lemma 21.** For every odd $a$, one has $\dim H^1(G_{\mathbb{Q},p}, \omega_p^a) = 1 + \dim A(\omega_p^{p-a})$ and $\dim H^1(G_{\mathbb{Q},p}, \omega_p^{-a}) = 1 + \dim A(\omega_p^{a+1})$.

**Proof —** The second equality is the same as the first since $\omega_p^{-a} = \omega_p^{p-1-a}$. We shall therefore only prove the first equality.

When $a = 1$, a class in $H^1(G_{\mathbb{Q},p}, \omega_p)$ is represented by a cocycle of the form $g \mapsto c_\alpha(g) := g(\alpha) / \alpha$, with $\alpha \in \mathbb{Q}$, $\alpha^p \in \mathbb{Q}$ and $v_\ell(\alpha^p) = 0$ for all prime $\ell \neq p$, and the cocycle $c_\alpha$ is a coboundary if and only if $\alpha \in \mathbb{Q}$ (cf. [26] for this simple application of the Kümmer exact sequence). Therefore the dimension of $H^1(G_{\mathbb{Q},p}, \omega_p)$ is 1 and this
space is generated by the cocycle \( c_\alpha \) for \( \alpha = p \). On the other hand, \( A(\omega_p^{p-1}) = A(1) \) is the \( p \)-torsion of the class group of \( \mathbb{Q} \), so has dimension 0, and the equality is proved.

When \( a > 1 \) by Greenberg-Wiles version of Poitou-Tate duality ([26, Theorem 2]), one has \( \dim H^1(G_{\mathbb{Q},p}, \omega_p^a) = \dim H^0(G_{\mathbb{Q},p}, \omega_p^{1-a}) + 1 \) where \( H^1(G_{\mathbb{Q},p}, \omega_p^{1-a}) = \ker (H^1(G_{\mathbb{Q},p}, \omega_p^{1-a}) \to H^1(G_{\mathbb{Q},p}, \omega_p^{1-a})) \). Since \( H^1(G_{\mathbb{Q},p}, \omega_p^{1-a}) = H^1(I_p, \omega_p^{1-a}) \) (cf. loc. cit.) so \( H^1(G_{\mathbb{Q},p}, \omega_p^{1-a}) \) parametrizes extensions of \( G_{\mathbb{Q}} \)-representations \( 0 \to \omega_p^{1-a} \to V \to 1 \to 0 \) that are unramified everywhere (in the sense that applying the functor of \( I_\ell \)-invariants to this short exact sequence yields a sequence which is still exact, including for \( \ell = p \)), and this space, by Hilbert class field theory, cf. [23, Chapter I], is the space \( A(\omega_p^{1-a}) = A(\omega_p^{p-a}) \).

\[\square\]

**Theorem 22.** The residual representation \( \overline{\rho} = 1 \oplus \omega_p^a \) \((1 \leq a \leq p - 2, \ a \ odd) \) is unobstructed if either of the following condition holds:

(i) \( a > 1 \) and \( p \) does not divide \( B_{a+1}B_{p-a} \) where \( B_n \) is the \( n \)-th Bernoulli number;

(ii) \( a = 1 \);

(iii) Vandiver’s conjecture holds for \( p \).

Therefore, in any of those cases, \( A_{\overline{\rho}} \) is a regular local complete algebra of dimension 2 over \( \overline{\mathbb{F}_p} \).

**Proof —** Let us assume (i). By the reflection theorem ([27, Theorem 10.9]) one has \( p \)-rank \( A(\omega_p^{p-a}) \) \( \leq p \)-rank \( A(\omega_p^a) \) and \( p \)-rank \( A(\omega_p^{a+1}) \leq p \)-rank \( A(\omega_p^{1-a}) \). The \( p \)-rank of \( A(\omega_p^a) \) (resp. \( A(\omega_p^{1-a}) \)) is 0 if \( p \nmid B_{p-a} \) and \( p \nmid B_{a+1} \) by Herbrand’s theorem ([27]). Hence by the Lemma, \( \dim H^1(G_{\mathbb{Q},p}, \omega_p^a) \leq 1 \) and \( \dim H^1(G_{\mathbb{Q},p}, \omega_p^{p-a}) \leq 1 \) and \( \overline{\rho} \) is unobstructed by Prop. 20.

In case (ii), that is \( a = 1 \), we have already seen that \( \dim H^1(G_{\mathbb{Q},p}, \omega_p) \leq 1 \) in the course of the proof of the lemma, and by the lemma again, \( \dim H^1(G_{\mathbb{Q},p}, \omega_p^{-1}) \leq 1 + \dim A(\omega_p^2) \leq 1 + \dim A(\omega_p^{p-2}) \) by the reflexion theorem. By Herbrand’s theorem, \( A(\omega_p^{p-2}) \) is 0 (since \( B_2 = 1/6 \) is not divisible by any \( p \)), and the result follows again from the proposition.

Finally, in case (iii), one just needs to recall that Vandiver’s conjecture is the statement that \( A(\omega_p^m) \) is 0 for every even \( n \), so the result follows again from the lemma and the proposition. \[\square\]
This appendix is devoted to the case $p = 3$ of Theorem I. We give a complete
treatment of the Galois-theoretic part of the proof, which allows us to obtain a more
precise result than Theorem I, with explicit determination of systems of generators
of $A$: it is a concrete illustration of certain of the methods used in this article. But
we only skecth the second part of the proof, concerning the order of nilpotence
of modular forms modulo 3, which uses completely different methods than those
of this paper, more akin to Nicolas and Serre’s methods in characteristic 2. The
details of this second part will appear elsewhere.

A.1. Results. If $p = 3$, the only modular Galois representation is $\bar{\rho} = 1 \oplus \omega_3$,
which is unobstructed. We therefore only need to prove Theorem I, that is that
$A = A_{\bar{\rho}}$ is isomorphic to $F_3[[x,y]]$. If $\ell$ is a prime $\not\equiv 3$, $\text{tr} \bar{\rho} (\text{Frob}_\ell) = 1 + \ell \pmod{3}$.
It follows that the operators $T_\ell$ for $\ell \equiv 2 \pmod{3}$, and $1 + T_\ell$ for $\ell \equiv 1 \pmod{3}$
belongs to the maximal ideal $m_A$ of $A$. We shall write $T_\ell'$ for $1 + T_\ell$ when $\ell \equiv 1$
(mod 3) and for $T_\ell$ when $\ell \equiv 2$ (mod 3) so that the Hecke operators $T_\ell'$ are always
locally nilpotent on $S(F_3)$.

Let us also recall that by [25], $S(F_3)$ is the $F_3$-vector space of basis $(\tilde{\Delta}^k)_k=0,1,2,...$
where $\tilde{\Delta}$ is the reduction modulo 3 of the $q$-expansion of the modular form $\Delta$. We
restrict our attention to the subspace $M$ of $S(F_3)$ generated by $\tilde{\Delta}^k$ for $k \geq 1, k \not\equiv 0$
(mod 3).

Lemma 23. (i) The space $M$ is stable by all the $T_\ell, \ell \not\equiv 3$, hence by $A$.
(ii) The action of $A$ on $M$ is faithful.
(iii) For every cofinite ideal $I$ in $A$, the pairing $A/I \times M[I] \rightarrow F_3, (T,f) \mapsto a_1(Tf)$ is perfect.

Proof — Note that if $\tilde{\Delta}^k = \sum a_nq^n \in F_3[[q]]$, and $a_n \neq 0$, then $n \equiv k \pmod{3}$:
this follows from the case $k = 1$, which results from the known congruences about
$\tau(n)$ ([25]). The space $M$ is therefore the subspace of $S(F_3)$ of forms $\sum a_nq^n$
which satisfy $a_{3n} = 0$ for every integer $n$, and (i) follows then from the formula giving
the action of $T_\ell$ on $q$-expansions. Also one has $S(F_3) = \oplus_{n=0}^{\infty} M^{3n}$, and since for
$f \in S(F_3)$, and $\ell \not\equiv 3$ a prime, one has $T_\ell(f^3) = (T_\ell f)^3$, this decomposition is stable
by $A$ and $S(F_3)$ is, as an $A$-module, isomorphic to a countable direct sum of copies
of $M$. Since $A$ acts faithfully on $S(F_3)$ by construction, (ii) follows, and (iii) is then
routine. □
Let $\mathcal{P}_1$ be the set of primes $\ell$ which are congruent to 1 modulo 3 but not split in the splitting field $L$ of $X^3 - 3$. Let $\mathcal{P}_2$ be the set of primes $\ell$ which are congruent to 2 modulo 3 but not to 8 modulo 9. Note that $\mathcal{P}_1$ and $\mathcal{P}_2$ both have density $1/3$ and are disjoint.

We shall prove the following more precise version of Theorem 1:

**Theorem 24.** There is a (unique) isomorphism of algebras $\mathbb{F}_3[[x, y]] \to A$ which sends $x$ to $T'_2 = T_2$ and $y$ to $T'_7 = 1 + T_7$. For $\ell \neq 3$ a prime, one has $T'_\ell \equiv x \pmod{m_2^A}$ if and only if $\ell \in \mathcal{P}_2$, $T'_\ell \equiv y \pmod{m_2^A}$ if and only if $\ell \in \mathcal{P}_1$, and $T'_\ell \equiv 0 \pmod{m_2^A}$ if and only if $\ell \not\in \mathcal{P}_1 \cup \mathcal{P}_2$.

As in [20], one deduces immediately from the theorem, using Lemma 23(iii), that

**Corollary 25.** There exists a unique basis $m(a, b)_{a \in \mathbb{N}, b \in \mathbb{N}}$ of $M$, adapted to $T'_2$ and $T'_7$ in the following sense:

(i) $m(0, 0) = \tilde{\Delta}$

(ii) $T'_2 m(a, b) = m(a - 1, b)$ if $a \geq 1$, and $T'_2 m(0, b) = 0$.

(iii) $T'_7 m(a, b) = m(a, b - 1)$ if $b \geq 1$, and $T'_7 m(a, 0) = 0$.

(iv) The first coefficient $a_1$ of $m(a, b)$ is zero except if $(a, b) = (0, 0)$.

**Example 26.** With simple computations, one checks that

- $m(0, 1) = \tilde{\Delta}^7 + 2\tilde{\Delta}^{10}$
- $m(0, 2) = \tilde{\Delta}^{13} + 2\tilde{\Delta}^{16} + \tilde{\Delta}^{19} + 2\tilde{\Delta}^{28}$
- $m(1, 0) = \tilde{\Delta}^2$
- $m(2, 0) = \tilde{\Delta}^{4} + 2\tilde{\Delta}^{7} + \tilde{\Delta}^{10}$
- $m(3, 0) = \tilde{\Delta}^8 + 2\tilde{\Delta}^{11}$
- $m(4, 0) = 2\tilde{\Delta}^{13} + 2\tilde{\Delta}^{16} + \tilde{\Delta}^{19} + 2\tilde{\Delta}^{28}$
- $m(1, 1) = 2\tilde{\Delta}^{5} + 2\tilde{\Delta}^{8} + \tilde{\Delta}^{11}$

The proof of the theorem rests on two propositions, one concerning deformation theory, and one of elementary nature, similar to some arguments of Nicolas and Serre about the order of nilpotence of modular forms.

**Proposition 27.** The tangent space $\tilde{D}_0^0(\mathbb{F}_3[e])$ to the functor $\tilde{D}_0^0$ has dimension 2. This space has a basis of pseudo-characters $\tau_1, \tau_2 : G \to \mathbb{F}_3[e]$ (deforming $t = 1 + \omega_3 : G \to \mathbb{F}_3$) such that for $i = 1, 2$, and any prime $\ell \neq 3$, $\tau_i(Frob_\ell)$ is non-constant (that is, lies in $\mathbb{F}_3[e] - \mathbb{F}_3$) if and only if $\ell \in \mathcal{P}_i$. 

To state the second proposition, we need two definitions:

**Definition 28.** For every form $f \in S(\mathbb{F}_3)$, the index of nilpotence of $f$, denoted by $g(f)$, is the smallest integer $n$ such that $T_{\ell_1}^r \ldots T_{\ell_n}^r f = 0$ for any choice of $n$ primes $\ell_1, \ldots, \ell_n$ (not necessarily distinct) different form 3.

**Definition 29.** Let $k \geq 1$ be an integer. Write $k$ in base 3, that is $k = \sum_{i=0}^{r} a_{i} 3^i$, with the $a_i \in \{0, 1, 2\}$, $a_r \neq 0$. We define the content of $k$ by $c(k) = \sum_{i=0}^{r} a_{i} 2^i$.

Let us note for later use the following estimate of $c(k)$:

**Lemma 30.** One has $c(k) \leq 2^{2+\lceil \log k / \log 3 \rceil}$, where $\lceil \log k / \log 3 \rceil$ is the integral part of $\log k / \log 3$.

**Proof** — Let $r = \lceil \log k / \log 3 \rceil$, so that $3^r \leq k < 3^{r+1}$, and $k = \sum_{i=0}^{r} a_{i} 3^i$, with the $a_i \in \{0, 1, 2\}$, $a_r \neq 0$. Then $c(k) = \sum_{i=0}^{r} a_{i} 2^i \leq 2 \sum_{i=0}^{r} 2^i = 2^{r+2} - 2 \leq 2^{r+2}$. □

**Proposition 31.** The index of nilpotence of the form $\tilde{\Delta}^k$ is at most its content, that is $g(\tilde{\Delta}^k) \leq c(k)$.

A.2. Proof of the theorem assuming Propositions 27 and 31. Let us denote by $\tau_{univ} : G \to \tilde{R}_p^0$ the universal pseudo-character and by $m$ the maximal ideal of the deformation ring $\tilde{R}_p^0$. For $\ell \neq 3$ a prime, let us denote by $t_\ell \in \tilde{R}_p^0$ the element $\tau_{univ} (\text{Frob}_\ell)$ and by $t_\ell' \in m$ the element $t_\ell - \text{tr} \bar{\rho}(\text{Frob}_\ell)$. By definition of the map $\tilde{R}_p^0 \to A$, one sees that this map sends $t_\ell$ on $T_\ell$ and $t'_\ell$ on $T'_\ell$.

Since $t'_\ell \in m$, one can see $t'_\ell \in m/m^2$ as an element of the cotangent space of $\text{Spec} \tilde{R}_p^0$, that is as a linear form on the tangent space $\tilde{D}_p^0(\mathbb{F}_3[\epsilon])$. The proposition 27 can be translated as $t'_\ell(\tau_1) \neq 0$ if and only if $\ell \in \mathcal{P}_1$, $t'_\ell(\tau_2) \neq 0$ if and only if $\ell \in \mathcal{P}_2$, where $\tau_1, \tau_2$ is the basis of $\tilde{D}_p^0(\mathbb{F}_3[\epsilon])$ introduced in the Proposition. Hence it is clear that $t'_\ell_1, t'_\ell_2$ form a basis of $m/m^2$ if and only if $\ell_1 \in \mathcal{P}_1$, $\ell_2 \in \mathcal{P}_2$ (up to exchanging $\ell_1$ and $\ell_2$). In particular $t'_2$ and $t'_7$ is a basis of $m/m^2$.

Since the map $\tilde{R}_p^0 \to A$ is surjective, it follows that $T'_2$ and $T'_7$ generate $m_A/m_A^2$, hence by Nakayama, generate the topological algebra $A$. Hence to show that the morphism $\mathbb{F}_2[[x, y]] \to A$ that sends $x$ and $T'_2$ and $y$ on $T'_7$ is an isomorphism, it suffices to prove that $A$ has Krull dimension at least 2.

Thus dim $A/m_A^n A = \dim M[m_A^n] = \dim \{ f \in M, g(f) \leq n \}$. By Prop. 31, the latter space contains all the forms $\tilde{\Delta}^k$ for $c(k) \leq n$, hence by Lemma 30 all the forms $\tilde{\Delta}^k$ for $2^{2+\lceil \log k / \log 3 \rceil} \leq n$, in particular for $k \leq \frac{1}{2} n^{\log 3 / \log 2}$, $k \neq 0$ (mod 3). As the forms $\tilde{\Delta}^k$ are linearly independent, one deduces that dim $A/m_A^n A \geq \frac{2}{2^r} n^{\log 3 / \log 2}$. If
A was of Krull’s dimension 1 (resp. 0), then \( \dim A/m_A^n \) would be linear in \( n \) (resp. constant) for \( n \) large enough, which would contradict the above estimate since \( \log 3/\log 2 > 1 \). Therefore \( A \) has Krull dimension at least 2, hence is isomorphic to \( \mathbb{F}_3[[x, y]] \) by the isomorphism described above, hence has dimension 2.

A.3. Proof of Proposition 27. It suffices to construct two pseudo-characters \( \tau_1 \) and \( \tau_2 \) satisfying for \( i = 1, 2 \), \( \tau_i(\text{Frob}_\ell) \) is non-constant if and only if \( \ell \in \mathcal{P}_i \) because two such pseudo-characters are clearly linearly independent, hence a basis of \( D^0_p(\mathbb{F}_3[\epsilon]) \) since this space has dimension 2 by point (ii) of Theorem 22.

A.3.1. Construction of \( \tau_2 \). We define an additive non-trivial character \( \alpha : G \to \text{Gal}(\mathbb{Q}(\mu_9)/\mathbb{Q}) = (\mathbb{Z}/9\mathbb{Z})^* \to \mathbb{F}_3 \), by \( \alpha(1) = \alpha(8) = 0 \), \( \alpha(2) = \alpha(7) = 1 \), and \( \alpha(4) = \alpha(5) = 2 \). (Note that by Class Field Theory, any non-trivial character \( G \to \mathbb{F}_3 \) factors through the quotient \( \text{Gal}(\mathbb{Q}(\mu_9)/\mathbb{Q}) \) of \( G \) which is cyclic of order 6, hence is either \( \alpha \) or \( -\alpha \)). Define \( \tau_2 : G \to \mathbb{F}_3 \) by \( (1 + \epsilon \alpha) + \omega_3(1 - \epsilon \alpha) \). As the sum of two characters \( G \to \mathbb{F}_3[\epsilon]^* \), \( \tau_\alpha \) is a pseudo-character of \( G \) of dimension 2, clearly deforming \( 1 + \omega_3 \). Its determinant is \( (1 + \epsilon \alpha) \times \omega_3(1 - \epsilon \alpha) = \omega_3 \), hence is constant. Thus, \( \tau_2 \) is an element of \( D^0_p(\mathbb{F}_3[\epsilon]) \). One has for \( \ell \neq 3 \) a prime, \( \tau_2(\text{Frob}_\ell) = 1 + \omega_3(\ell) + \epsilon \alpha(\ell)(1 - \omega_3(\ell)) \). So \( \tau_2(\ell) \) is non-constant if and only if \( \alpha(\ell) \neq 0 \) and \( \omega_3(\ell) \neq 1 \) in \( \mathbb{F}_3 \), that is if and only if \( \ell \) (mod 9) is not 1 and 8, and \( \ell \) (mod 3) is 2, which means \( \ell \in \mathcal{P}_2 \).

A.3.2. Construction of \( \tau_1 \). The splitting field of \( X^3 - 3 \) in \( \mathbb{C} \) is \( L = \mathbb{Q}(u, j) \), where \( u = 3^{1/3} \) and \( j \) is the cubic root of unity \( \frac{-1 + i \sqrt{3}}{2} \). The Galois group \( \text{Gal}(L/\mathbb{Q}) \) is isomorphic to the symmetric group \( S_3 \) by sending \( \sigma \in \text{Gal}(L/\mathbb{Q}) \) to its action on \( \{u, ju, j^2 u\} \) which we identify with \( \{1, 2, 3\} \) by sending \( u \) on 1, \( uj \) on 2, and \( uj^2 \) on 3. With this identification, the character \( \omega_3 : \text{Gal}(L/\mathbb{Q}) \to (\mathbb{Z}/3\mathbb{Z})^* = \{1, -1\} \) is identified with the sign character of \( S_3 \).

We also identify the multiplicative subgroup \( \mu_3(L) = \{1, j, j^2\} \) of \( L^* \) with the additive subgroup of \( \mathbb{F}_3 \) by sending 1 on 0, \( j \) on 1, \( j^2 \) on 2. We define a map \( \tau_1 : S_3 \to \mathbb{F}_3[\epsilon] \) as in the third column of the table below:

<table>
<thead>
<tr>
<th>( \sigma )</th>
<th>( \omega_3(\sigma) )</th>
<th>( \tau_1(\sigma) )</th>
<th>( \frac{1}{2}(\tau_1(\sigma)^2 - \tau_1(\sigma^2)) )</th>
</tr>
</thead>
<tbody>
<tr>
<td>( \text{Id} )</td>
<td>1</td>
<td>2</td>
<td>1</td>
</tr>
<tr>
<td>(12)</td>
<td>-1</td>
<td>0</td>
<td>-1</td>
</tr>
<tr>
<td>(13)</td>
<td>-1</td>
<td>0</td>
<td>-1</td>
</tr>
<tr>
<td>(23)</td>
<td>-1</td>
<td>0</td>
<td>-1</td>
</tr>
<tr>
<td>(123)</td>
<td>1</td>
<td>( 2 + \epsilon )</td>
<td>1</td>
</tr>
<tr>
<td>(132)</td>
<td>1</td>
<td>( 2 + 2\epsilon )</td>
<td>1</td>
</tr>
</tbody>
</table>
One checks by straightforward computations that $\tau_1$ is a pseudo-character on $S_3$ of dimension 2. (A more conceptual proof can be obtained by the arguments of the proof of the main theorem in [2].) The determinant of this pseudo-character has been computed in the last column of the above table, and is seen to be equal to $\omega_3$.

Therefore $\tau_1 : G \to \text{Gal}(L/\mathbb{Q}) = S_3 \to \mathbb{F}_3[\varepsilon]$ is in $D_p^0(\mathbb{F}_3[\varepsilon])$, and one sees from the table that $\tau_1(\text{Frob}_\ell)$ is non-constant if and only if $\text{Frob}_\ell$ in $S_3$ is a 3-cycle, that is if and only if $\text{Frob}_\ell$ is an element of sign 1 but not the identity, that is if and only if $\ell \equiv 1 \pmod{3}$ but $\ell$ does not split in $L$.

A.4. **Sketch of the proof of Proposition 31.** We have seen during the proof of Theorem 24, before using Prop. 31, that the ideal $m_A$ was generated by $T_2'$ and $T_7'$.

Hence:

**Lemma 32.** For $f \in M$, the index of nilpotence $g(f)$ of $f$ is the smallest $n$ such that $T_{\ell_0} \cdots T_{\ell_n} f = 0$ for any choice of primes $\ell_0, \ldots, \ell_n$ in the set $\{2, 7\}$.

Thus we are reduced to study the operators $T_2'$ and $T_7'$.

**Lemma 33** (Nicolas-Serre). One has the following recurrence relations:

\[
T_2' \Delta^k = \tilde{T}_2 \Delta^k - T_2' \Delta^{k-3} \quad \text{for } k \geq 3
\]

\[
T_7' \Delta^k = \tilde{T}_7 \Delta^k - \tilde{T}_7 T_7' \Delta^{k-3} + (T_7' - \tilde{T}_7) T_7' \Delta^{k-4} - (\tilde{T}_7 + \tilde{T}_7^2) (T_7' \Delta^{k-5} + (\tilde{T}_7^2 + \tilde{T}_7) T_7' \Delta^{k-6} + (\tilde{T}_7^2 + \tilde{T}_7^3) T_7' \Delta^{k-7})
\]

for $k \geq 7$

More generally, Nicolas and Serre prove that $T_p' \Delta^k = \sum_{i=0}^{p-1} c_{p,i}(\tilde{T}_p' \Delta^{k-i})$ for all $k \leq p$, with the $c_{p,i}$ polynomials of one variable of degree at most $i$. The proof is similar to the one of Theorem 3.1 of [19]. Nicolas has computed the $c_{p,i}$ for small values of $p$ (up to $p = 37$). The details have not yet been published.

**Definition 34.** If $0 \neq f = \sum a_k \Delta^k \in M$, we define the *content* $c(f)$ of $f$, as $c(f) = \max_{k,a_k \neq 0} c(k)$. If $f = 0$ we define $c(0) = -\infty$.

**Lemma 35.** For every $f \in M$, one has $c(T_2' f) \leq c(f) - 1$, and $c(T_7' f) \leq c(f) - 2$.

For the proof, we are immediately reduced to the case $f = \tilde{T}_2 \Delta^k$ with $3 \nmid k$.

In this case, one proves that if we write $T_2' \Delta^k = \sum_{i=0}^{n} a_i \Delta^k$ with $a_n \neq 0$, then $n = k - (3^v + 1)/2$ where $v = v_3(k-1)$ (it follows easily that $c(n) = c(k-1)$ and that $a_i \neq 0$ implies $c(i) \leq c(k) - 1$. It follows immediately that $c(T_2' \Delta^k) = c(k) - 1$.

Similarly, if we write $T_7' \Delta^k = \sum_{i=0}^{n} a_i \Delta^k$ with $a_n \neq 0$, then $n = k - (3^v + 3)/2$ where $v' = \min(v_3(k-1), v_3(k-2))$ (it follows easily that $c(n) = c(k) - 2$ and
$a_i \neq 0$ implies $c(i) \leq c(k) - 2$, so that $c(T^k_1 \Delta) = c(k) - 2$. The proof of those assertions is by induction, using Lemma 33. The details, which are elementary but quite long and technical, and are reminiscent of the work of Nicolas and Serre in characteristic 2, will appear in a future paper devoted to the theory of modular forms modulo 3.

Let $n \geq c(\Delta^k)$ and $g = T^{T}_{\ell_0} \ldots T^{T}_{\ell_n} \Delta^k = 0$. By applying the lemma $n + 1$ times, one gets $c(g) < 0$ hence $c(g) = -\infty$ and $g = 0$. This proves Proposition 27.

References


E-mail address: jbellaic@brandeis.edu

Mathematics Department, Brandeis University, 415 South Street, Waltham, MA 02454-9110, U.S.A

E-mail address: shekhar@math.ucla.edu

Department of Mathematics, UCLA, 520 Portola Plaza, Los Angeles, CA 90095-1555