IMAGE OF PSEUDOREPRESENTATIONS AND COEFFICIENTS OF MODULAR FORMS MODULO p

JOËL BELLAÏCHE

ABSTRACT. We describe the image of general families of two-dimensional representations over compact semi-local rings. Applying this description to the family carried by the universal Hecke algebra acting on the space of modular forms of level N modulo a prime p, we prove new results about the coefficients of modular forms mod p. If $f = \sum_{n=0}^{\infty} a_n q^n$ is such a form, for which we can assume without loss of generality that $a_n = 0$ if $(n, Np) > 1$, calling $\delta(f)$ the density of the set of primes ℓ such that $a_\ell \neq 0$, we prove that $\delta(f) > 0$ provided that f is not zero (and if $p = 2$, not a multiple of Δ). More importantly, we prove, when $p > 2$, a *uniform* version of this result, namely that there exists a constant $c > 0$ depending only on N and p such that $\delta(f) > c$ for all forms f except for those in an explicit subspace of infinite codimension of the space of all modular forms mod p of level N. Forms in this subspace, called *special* modular forms mod p, are proved to be closely related to certain classes of modular forms mod p previously studied by the author, Nicolas and Serre, called cyclotomic and CM modular forms mod p.

CONTENTS

1. INTRODUCTION

This article has two parts. In the first, we describe the image of general families of two-dimensional representations of a pro-finite group. In the second, we use these descriptions to study the behavior of the coefficients at primes of modular forms modulo an odd prime p, focussing especially on results which are *uniform* in the modular form.

2000 *Mathematics Subject Classification.* 11R.
Joël Bellaïche was supported by NSF grants DMS 1405993.

1.1. **Image of family of representations.** Let Π be a profinite group, A a compact local ring of maximal ideal $\mathfrak{m}$. The residue field $\mathbb{F} = A/\mathfrak{m}$ is thus a finite field, and we assume throughout §1.1 that its characteristic p is different from 2.

The families we are interested in are families of two-dimensional representations of Π carried by A. As past work using family of Galois representations has made clear, it is important for many applications to consider not only families of representations that can be described as a representation of Π on a rank-two free A-module, but more generally two-dimensional pseudo-representations of Π over A. Hence we consider a family defined as a continuous two-dimensional pseudo-representation[1] (t, d) of Π over A.

We put certain restrictions to the family we consider. First, the residual representation of the family may be irreducible or the sum of two characters. In the latter case, we assume that those two characters are distinct, and also that Π satisfies the p-finiteness condition of Mazur. Second, we assume that as a topological $W(\mathbb{F})$-algebra, A is generated by $t(\Pi)$. Third, we assume that d is constant, that is for every $g \in \Pi$, $d(g)$ is the Teichmüller lift of $\bar{d}(g)$. The last two are not serious restrictions: the second assertion can always be made true by replacing A by its sub-algebra generated by $t(\Pi)$, the third by twisting (t, d) by a suitable character.

Though it is not always true that (t, d) comes from a representation $\rho : \Pi \to \mathrm{GL}_2(A)$, there always exists a Generalized Matrix Algebra (or GMA, see [3, §1] or below, §2.2) R over A and a representation $\rho : \Pi \to R^*$ with trace t and determinant d. We may assume that R is faithful (see below 2.2), and generated as an A-module by $\rho(\Pi)$, and if we do, R and ρ are unique up to unique isomorphism, R has a natural topology and the representation ρ is continuous.

We set $G := \rho(\Pi)$ and call this closed subgroup of R^* the *image* of our family (t, d). The aim is to describe as precisely as possible the group G. We shall handle this group using a slight generalization (from the case $R = M_2(A)$ to the case of arbitrary GMAs) of the remarkable theory of Lie Algebras of Pink (see §4). This theory attaches to every closed subgroup Γ of $SR^1 := \{x \in R^*,\ \det x = 1,\ x \equiv \mathrm{Id} \pmod{\mathrm{rad}R}\}$ a closed Lie subring $L = L(\Gamma)$ of $(\mathrm{rad}R)^0 = \{x \in \mathrm{rad}R, \mathrm{tr}\, x = 0\}$. Contrarily to the classical theory of Lie algebras, the subgroup Γ is not uniquely determined by $L = L(\Gamma)$. However, its closed derived subgroup Γ_2 is, as well as all the further terms of its descending central series, so that the knowledge of L gives us a good, if partial, grasp on what Γ is. We apply this theory to the subgroup $\Gamma = G \cap SR^1$, which has finite index in G.

We obtain a complete description of the Lie ring L after extending the scalars from $\mathbb{Z}_p$ to $W(\mathbb{F})$, the ring of Witt vectors of the finite field $\mathbb{F}$. Note that $W(\mathbb{F})/\mathbb{Z}_p$ is only a small extension, finite and unramified, which is harmless in the applications to modular forms (we do not extend the scalars to A, which would be much more destructive). The description of $W(\mathbb{F})L$ we obtain depends, unsurprisingly, of the nature of the projective image of

[1] We use Chenevier's notion [6] of pseudo-representations, which is the most general and the most elegant, though since we assume $p > 2$ for most of this paper, Chenevier's notion is equivalent to Rouquier's one.

the representation $\bar{\rho}$. There are five cases to consider, according to the projective image being *exceptional* (that is, either isomorphic to A_4, S_4, A_5) or *large* (that is isomorphic to $\mathrm{PGL}_2(\mathbb{F}_q)$ or $\mathrm{PSL}_2(\mathbb{F}_q)$ for some subfield $\mathbb{F}_q$ of $\mathbb{F}$), *dihedral of order* > 4, *dihedral of order 4*, *cyclic of order* > 2, *cyclic of order* 2.

Rather than giving all the results, which the reader will find in Theorems 6.4.1, 6.5.1, 6.6.1. 6.7.1 and 6.8.1, let us just illustrate them by giving two examples:

- in the **large** or **exceptional** projective image case, we prove that there exists a closed $W(\mathbb{F})$-submodule I_1 of A such that $I_1^2 \subset I_1$ and $W(\mathbb{F})L = \begin{pmatrix} I_1 & I_1 \\ I_1 & I_1 \end{pmatrix}^0$ is the set of matrices of trace 0 with coefficients in I_1;
- in the **cyclic of order** > 2 projective image case, we can write the GMA $R = \begin{pmatrix} A & B \\ C & A \end{pmatrix}$ with B, C two A-modules with a bilinear map $B \times C \to A$ denoted as multiplication, and we prove that there exists a $W(\mathbb{F})$-module I_1 such that $BC \subset I_1 \subset A$ satisfying $I_1^3 \subset I_1$ and $W(\mathbb{F})L = \begin{pmatrix} I_1 & B \\ C & I_1 \end{pmatrix}^0$.

Moreover, we prove in each case that the description of $W(\mathbb{F})L$ we obtain is optimal, in the sense that any $W(\mathbb{F})$-Lie algebra satisfying the given description can be obtained from a family of representations of the type considered. In other words, nothing more can be said on $W(\mathbb{F})L$.

In many cases (for instance when $\mathbb{F} = \mathbb{F}_p$ or when the projective image of $\bar{\rho}$ is large, or when this image is cyclic of order n such that $\gcd(n, p-1) > 2$, etc.) we obtain, better than a description of $W(\mathbb{F})L$, a description of L which we again prove to be optimal. We refer the reader to the Theorems cited above for the precise statements.

Recently there has been a surge in activity concerning the study of the image of families of Galois representations, represented by papers by Hida [12], Lang [15], and Conti-Iovita-Tilouine [8]. In these articles, the authors study the image of families of Galois representations attached to Hida or Coleman families of modular forms. Among the five possibilities concerning the projective image of $\bar{\rho}$ enumerated above, these authors only consider two, namely the cases when the projective image of $\bar{\rho}$ is large/exceptional or dihedral of order > 4. Their main result is that except if all forms in the family is CM, and under various supplementary assumptions, the image G of the family is large, in the following sense: there is an explicit subring A_0 of A such that the family of representations is virtually defined over A_0 (i.e. is defined over A_0 after restricting it to an open subgroup Π_0 of the Galois group, which is explicit in their work), and the image G_0 of Π_0 contains a non-trivial *congruence subgroup* of $\mathrm{SL}_2(A_0)$. (Actually, the result of Conti-Iovita-Tilouine is slightly weaker, as it only proves this for G_0 replaced by its Zariski closure).

In Section 7 (which is not used in the rest of the paper), we prove a similar result in the case where $\bar{\rho}$ is large or exceptional, dihedral of order > 4 and cyclic of order > 2. In the two remaining cases (cyclic of order 2, and dihedral of order 4), we show in section 9 that no result of this type is to be expected. Our result is more general than the ones mentioned above in that it works for almost arbitrary families of representations of

an arbitrary profinite group Π, instead of only specific families of representations of the absolute Galois group of $\mathbb{Q}$ (though it fails to deal with a few representations that Lang's result is able to deal with). Dually, our methods are much more elementary, in that we use only basic group theory and Pink's theory of Lie algebras, rather than the theory of classical and p-adic modular forms, the structure of the Galois group, and advanced Hodge-Tate theory as in the afore-mentioned articles.

1.2. **Coefficients of modular forms.**

1.2.1. *Individual density result.* Let $N \geq 1$ be an integer, p any prime, $k \in \mathbb{Z}/(p-1)\mathbb{Z}$. For $\mathbb{F}$ a finite extension of $\mathbb{F}_p$, we shall denote by $M_k(N, \mathbb{F})$ the algebra of modular forms of level $\Gamma_0(N)$, weight k, with coefficients in $\mathbb{F}$, in the sense of Swinnerton-Dyer. If $f = \sum_{n=0}^{\infty} a_n q^n$ is an element of $M_k(N, \mathbb{F})$, then the set $\{\ell \text{ prime }, a_\ell \neq 0\}$ is Frobenian, as was known already to Serre in the seventies (cf. [29]), and therefore has a density, which is a rational number between 0 and 1. We shall denote this number by $\delta(f)$, and refer to it as *the density of* f.

Let $\mathcal{F}_k(N, \mathbb{F})$ be the subspace of $M_k(N, \mathbb{F})$ of forms $f = \sum a_n q^n$ such that $a_n \neq 0 \Rightarrow (n, Np) = 1$. Equivalently, $\mathcal{F}_k(N, \mathbb{F})$ is the intersection of the kernels of the operators U_ℓ for ℓ prime, $\ell \mid Np$, defined by $U_\ell(\sum a_n q^n) = \sum a_{n\ell} q^n$ (those operators leave $M_k(N, \mathbb{F})$ stable, see [13].) When studying $\delta(f)$, there is no loss of generality in supposing $f \in \mathcal{F}_k(N, \mathbb{F})$, because for any $f = \sum_{n=0}^{\infty} a_n q^n \in M_k(N, \mathbb{F})$, the q-series

$$f' = \sum_{n=0, (n,Np)=1}^{\infty} a_n q^n$$

belongs to $\mathcal{F}_k(N^2, \mathbb{F})$ and obviously satisfies $\delta(f') = \delta(f)$. We shall henceforth restrict our attention to the subspace $\mathcal{F}_k(N, \mathbb{F})$ of $M_k(N, \mathbb{F})$.

Example. We let $\Delta \in \mathbb{F}_p[[q]]$ be the product $q \prod_{n \geq 1}(1 - q^n)^{24}$. It is the reduction mod p of the q-expansion of the unique normalized cuspidal eigenform of weight 12 and level 1, and $\Delta = \sum_{n \geq 1} \tau(n) q^n$ where τ is the reduction mod p of the usual Ramanujan τ-function. One has $\Delta \in M_{12}(N, \mathbb{F}_p)$. Let us denote by Δ' (depending implicitly of p and N) the q-series $\sum_{n \geq 1,\ (n,Np)=1} \tau(n) q^n$, which belongs to $\mathcal{F}_{12}(N, \mathbb{F})$. For $p = 2$, $N = 1$ one has $\Delta = \Delta' = \sum_{n \text{ odd}} q^{n^2}$

Theorem I. *Let $\mathbb{F}$ be a finite extension of $\mathbb{F}_p$, $k \in \mathbb{Z}/(p-1)\mathbb{Z}$ and $f \in \mathcal{F}_k(N, \mathbb{F})$. Assume that $f \neq 0$ (resp. $f \notin \mathbb{F}\Delta'$ if $p = 2$). Then $\delta(f) > 0$.*

The theorem will be proved in §10.3.

Corollary. *Let $f = \sum a_n q^n, g = \sum b_n q^n \in \mathcal{F}_k(N, \mathbb{F})$. Assume that $a_\ell = b_\ell$ for all primes ℓ except for a set of density 0 (and that $a_1 = b_1$ if $p = 2$). Then $f = g$.*

Proof — Since $\delta(f - g) = 0$, Theorem I implies $f - g = 0$ if $p > 2$, and $f - g \in \mathbb{F}\Delta'$ if $p = 2$. In this case, since $a_1(f - g) = 0$, $f - g = 0$ as well. □

1.2.2. *Uniformity?* We now turn to the main subject of this paper, the question of *uniformity* in the lower bound of Theorem I: when f varies in the infinite-dimensional space $\mathcal{F}_k(N,\mathbb{F})$, we know that $\delta(f)>0$, but is it possible that $\delta(f)$ goes to 0, or will $\delta(f)$ stay bounded away from 0, at least when f is supposed to stay in some large subset of $\mathcal{F}_k(N,\mathbb{F})$? This question of uniformity is not only natural, but of crucial importance if we hope to obtain new results for coefficients of weakly holomorphic modular forms of half-integral weight, such as the inverse Dedekind η-function, η^{-1}, whose coefficients are the value of the partition function $p(n)$. Indeed, those weakly holomorphic modular forms are in an appropriate sense limits of classical modular forms. We plan to go back to these applications in a subsequent paper.

Example 1.2.1. In the case $N=1$, $p=2$, the vector space $\mathcal{F}=\mathcal{F}_0(1,\mathbb{F}_p)$ has $(\Delta^n)_{n=1,3,5,7,\dots}$ as a basis. It was proved by the author (letter to Nicolas and Serre, July 2012) that for $p=2$, and any integer $r\geq 1$,

$$\delta(\Delta^{2^r+1})=2^{-\left\lfloor\frac{r-1}{2}\right\rfloor-2},\quad \delta(\Delta^{(2^{2r+1}+1)/3})=2^{-r-1} \tag{1.2.1}$$

Hence those forms (except perhaps a finite number of them) must be excluded if we want a positive lower bound for $\delta(f)$. For other odd powers of Δ, experimental computations done with SAGE and certain partial results strongly suggest a different and striking pattern: it seems that $\delta(\Delta^n)=1/8$ for all $n>1$ not of the form 2^r+1 or $\frac{2^{(2r+1)+1}}{3}$.

Though in this paper we are forced to exclude the case $p=2$ (both because Pink's theory requires $p>2$ and because our GMA methods require a multiplicity free hypothesis which is not satisfied if $p=2$), the example above, together with analogous computations done by Medvedovsky in the case $p=3$, showed that to obtain a uniform lower bound $\delta(f)>c>0$, it is necessary to exclude some exceptional forms f, and at the same time suggested that such a lower bound was otherwise possible. Indeed we prove:

Theorem II. *(cf. §10.6.) Let us assume that $p>2$. There exists a canonical subspace $\mathcal{F}_{k,spe}(N,\mathbb{F})$ of $\mathcal{F}_k(N,\mathbb{F})$, of infinite codimension, and a constant $c>0$ (depending only on $N,\mathbb{F}$) such that for every modular form $f\in\mathcal{F}_k(N,\mathbb{F})-\mathcal{F}_{k,spe}(N,\mathbb{F})$, one has $\delta(f)>c$.*

The constant c is effective (we can take $c=\frac{p-1}{pn}$ where n is the product of the orders of the image of all representations $\bar\rho\in\mathcal{R}(k,N,\mathbb{F})$, see below).

The definition of the subspace $\mathcal{F}_{\mathrm{spe}}(N,\mathbb{F})$, which we call the *subspace of special forms of* $\mathcal{F}$, is given in 10.4. This definition uses the image of the natural Galois pseudo-representation over the semi-local Hecke algebra A acting of $\mathcal{F}$, as well as the Pink's Lie algebra of that image. To analyze this subspace in more detail, we need to introduce some notations and recall some elementary facts.

1.2.3. *Decomposition of $\mathcal{F}_k(N,\mathbb{F})$.* For simplicity we shall often drop the level N, the weight k (which are fixed during all the discussion) and the finite field $\mathbb{F}$ from the notation and write $\mathcal{F}$ for $\mathcal{F}_k(N,\mathbb{F})$, $\mathcal{F}_{\mathrm{spe}}$ for $\mathcal{F}_{k,\mathrm{spe}}(N,\mathbb{F})$.

The space $\mathcal{F}$ is endowed with an action of the Hecke operators T_ℓ for $\ell \nmid Np$. After replacing $\mathbb{F}$ by a large enough finite extension, we may assume (cf. [13]) that all eigenvalues of these operators are in $\mathbb{F}$. Let $A_k(\mathbb{F})$ for $k \in \mathbb{Z}/(p-1)\mathbb{Z}$ be the closed $\mathbb{F}$-subalgebra of $\mathrm{End}_{\mathbb{F}}(\mathcal{F}_k(\mathbb{F}))$ generated by the Hecke operators T_ℓ for ℓ not dividing Np. The sequences $(\lambda_\ell)_{\ell \nmid Np}$ with $\lambda_\ell \in \mathbb{F}$ which are systems of eigenvalues for the operators T_ℓ of a common eigenvector in $\mathcal{F}$ are in bijection, by a theorem of Deligne, with a certain set $\mathcal{R} = \mathcal{R}(k, N, \mathbb{F})$ of semi-simple continuous Galois representations $\bar{\rho} : G_{\mathbb{Q},Np} \to \mathrm{GL}_2(\mathbb{F})$: the correspondence is given by $\lambda_\ell = \mathrm{tr}\, \bar{\rho}(\mathrm{Frob}_\ell)$ for all $\ell \nmid Np$. This set $\mathcal{R}(k, N, \mathbb{F})$ can be described as the set of all semi-simple representations $\bar{\rho} : G_{\mathbb{Q},Np} \to \mathrm{GL}_2(\mathbb{F})$ of determinant ω_p^{k-1} and Serre's level N. This is the content of Serre's conjecture, now a theorem of Khare and Wintenberger.

If $\bar{\rho}$ corresponds to a system of eigenvalues (λ_ℓ), we shall denote by $\mathcal{F}_{\bar{\rho}} = \mathcal{F}_{\bar{\rho}}(N, \mathbb{F})$ the *generalized eigenspace* in $\mathcal{F}$ for the T_ℓ ($\ell \nmid Np$) with eigenvalues λ_ℓ, that is the set of forms $f \in \mathcal{F}$ such that $\forall \ell \nmid Np,\ \exists n \in \mathbb{N},\ (T_\ell - \lambda_\ell)^n f = 0$.

We thus have a decomposition

$$\mathcal{F} = \bigoplus_{\bar{\rho} \in \mathcal{R}} \mathcal{F}_{\bar{\rho}} \tag{1}$$

of $\mathcal{F}$ into generalized eigenspaces.

1.2.4. *Special modular forms in $\mathcal{F}_{\bar{\rho}}$.* We define $\mathcal{F}_{\bar{\rho},\mathrm{spe}}$ as the space of modular forms in $\mathcal{F}_{\bar{\rho}}$ that are special, that is $\mathcal{F}_{\bar{\rho},\mathrm{spe}} = \mathcal{F}_{\bar{\rho}} \cap \mathcal{F}_{\mathrm{spe}}$. The following result refines the statement that $\mathcal{F}_{\mathrm{spe}}$ is of infinite codimension given in Theorem II.

Theorem III. *(cf. §10.5) Let $\bar{\rho}$ be any representation in $\mathcal{R}$. Assume that $p > 2$, and if $p = 3$, assume also that $\bar{\rho}$ is a twist of $1 \oplus \omega_3$, where ω_3 is the cyclotomic character. The space $\mathcal{F}_{\bar{\rho},spe}$ has infinite codimension in $\mathcal{F}_{\bar{\rho}}$.*

1.2.5. *Special modular forms, K-abelian forms, cyclotomic forms.* For many representations $\bar{\rho}$, we are able to give a much more precise description of $\mathcal{F}_{\bar{\rho},\mathrm{spe}}$.

Definition. Let $f = \sum a_n q^n \in \mathcal{F}$. Let K be a quadratic extension of $\mathbb{Q}$. We shall say that f is *cyclotomic* (resp. K-abelian) if there exists a finite cyclotomic extension $L/\mathbb{Q}$ (resp. an abelian extension L/K, Galois over $\mathbb{Q}$) such that such that for ℓ prime not dividing Np, the coefficient a_ℓ of f depends only on ℓ through $\mathrm{Frob}_{\ell, L/\mathbb{Q}}$.

Thus, a form f is cyclotomic if there exists $M \geq 1$ such that a_ℓ depends only on $\ell \pmod M$.

Example 1.2.2. In the case $p = 2$, $N = 1$, it was proved by Nicolas and Serre ([24]) that the forms Δ^n for $n = 2^r + 1$ and $n = (2^{2r+1} + 1)/3$ appearing in (1.2.1) are K-abelian, and it was proved by the author (letter to Serre and Nicolas, October 2013) that only for those odd values of n were Δ^n K-abelian (for $K = \mathbb{Q}(i)$ or $K = \mathbb{Q}(i\sqrt{2})$) but not cyclotomic. The forms Δ^n are known to be cyclotomic for $n = 1, 3, 5, 7, 19, 21$ and conjectured not to be so for other values of n. There also exists forms which are K-abelian or cyclotomic not of the form Δ^n: they have been classified and their density δ has been computed, and often goes to zero along infinite sequences of such forms.

Once again, though we exclude the case $p = 2$, this example suggested a close relation between the K-abelian and cyclotomic forms on the one hand, and the so-called special modular forms which we need to exclude in Theorem II, in the other hand. Indeed, we prove

Theorem IV. *(cf. Cor. 11.2.8, Cor. 11.3.4 and §11.4). We assume $p > 2$.*

- *If $\bar{\rho}$ has large projective image, the space of special modular forms $\mathcal{F}_{\bar{\rho},spe}$ is finite-dimensional.*
- *If $\bar{\rho}$ has a dihedral projective image which is of order n with $n > 4$, $4 \mid n$, then the space of special modular forms $\mathcal{F}_{\bar{\rho},spe}$ contains as a finite codimension subspace the space of K-abelian forms, where K is the quadratic extension of $\mathbb{Q}$ fixed by the unique quotient of order 2 of the projective image of $\bar{\rho}$.*
- *If $\bar{\rho}$ has cyclic projective image which is not of order 2, then the space of special modular forms $\mathcal{F}_{\bar{\rho},spe}$ is exactly the space of cyclotomic modular forms.*

Moreover, in all the cases considered above, the space $\mathcal{F}_{\bar{\rho},spe}$ is stable by all Hecke operators.

By contrast, in the remaining two degenerate cases where the projective image of $\bar{\rho}$ is $\mathbb{Z}/2\mathbb{Z}$ or $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, the space of special modular forms $\mathcal{F}_{\bar{\rho},\mathrm{spe}}$ is not in general stable by all the Hecke-operators, and while it may be proved to contain all[2] cyclotomic and K-abelian forms in $\mathcal{F}_{\bar{\rho}}$, I do not know at this point how much larger $\mathcal{F}_{\bar{\rho},\mathrm{spe}}$ is.

1.2.6. *A rough outline of the proofs.* To prove Theorems I, II, III and IV, we consider the Hecke algebra A acting on the space of modular forms $\mathcal{F}$ mod p. This is by construction a compact semi-local Hecke algebra, which carries a natural pseudo-representation (t, d) of the Galois group $G_{\mathbb{Q},Np}$. A crucial ingredient is the description of the image G of this pseudo-representation, or at least, of its Pink's Lie algebra, a special case of the general results described in 1.1 and proved in section 6.

A form f in $\mathcal{F}$ defines an open and closed subset N_f of the compact group G (namely $N_f = \{g \in G, a_1(\mathrm{tr}\,(g)f) \neq 0\}$) such that $\mu_G(N_f) = \delta(f)$ (as is shown by a simple application of Chebotarev, see §10.3), where μ_G is the probability Haar measure on G. Theorem I is thus reduced to checking that N_f is not empty (except when $f = 0$, or in the case $p = 2$, when f is proportional to Δ'), which is not hard (see §10.3).

To prove the other theorems we need to understand how $\mu_G(N_f)$ varies with f. Since we have more control on the finite index subgroup Γ of G that on G itself, we cut N_f into parts related to Γ-cosets. To be precise, if X is a set of representatives in G of G/Γ, so that $G = \coprod_{x\in X} x\Gamma$, we cut N_f into pieces $N_{f,x} := x^{-1}N_f \cap \Gamma$, so that $\mu_G(N_f) = \sum_{x\in X} \mu_G(N_{f,x})$ and our problem is to understand for a given x, how $\mu_G(N_{f,x})$ varies with f.

Since $N_{f,x}$ is a subset of Γ, we can transport the question to the Lie Algebra L of Γ, that is study instead $\mu_L(M_{f,x})$ where $M_{f,x} = \Theta(N_{f,x}) \subset L$, Θ being the 'logarithm' in Pink's

[2]In the case of projective image $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, there exists non-zero K-abelian forms, but no cyclotomic forms, in $\mathcal{F}_{\bar{\rho}}$, for exactly three quadratic fields K. In the case when the projective image is of order 2, there exists non-zero K-abelian forms for exactly one quadratic field, plus non-zero cyclotomic modular forms. For more about cyclotomic forms and K-abelian forms, see §11.

Lie theory. (Here I ignore, for simplicity, the fact that Θ is not always a measure-preserving bijection between Γ and L. This is remedied by replacing Γ and L by Γ_2 and L_2, their derived subgroup and derived Lie algebra respectively. However, this changes is the source of important, and essential, complications. See Remark 8.2.3 for a more detailed discussion of this fine point).

The Lie algebra L is an infinite-dimensional vector space over $\mathbb{F}_p$, and it turns out that $M_{f,x}$ is the complement in L of an algebraic hypersurface of L (here I am assuming $\mathbb{F} = \mathbb{F}_p$ for simplicity), that is the zero subset of a polynomial on L involving finitely many variables. Thus, $\mu_L(M_{f,x})$ is the proportion of points that does not lie on an hypersurface in a finite-dimensional space over $\mathbb{F}_p$. Unfortunately the dimension of the ambient space as well as the degree of that hypersurface depend on f, and the estimates given by the Weil's conjectures proved by Deligne are not sufficient to get the desired lower bound for $\mu_L(M_{f,x})$ in general.

However, when we choose for x the image c of a complex conjugation in G, we can show that the equation defining $M_{f,c}$ is, after a measure-preserving change of variables, affine. This is the main point of the proof of Theorem II, and is dealt with in a more general settings in §8.2. If we denote by $M'_{f,c}$ the transform of $M_{f,c}$ by this change of variable, $\mu_L(M_{f,c}) = \mu_L(M'_{f,c})$ and $M'_{f,c}$ is either empty, or an hyperplane of L, or L. In the last two cases, $\mu_L(M_{f,c}) \geq 1/p$, which gives us the desired lower bound. We need to determine for which forms f we have $M_{f,c}$ empty. This is done in section 8, relying on the explicit description of L given in section 6 which leads us to the notion of the essential subgroup A_{ess} of A, studied in §8 and to the definition of *special modular forms* (cf. §10.4), the forms f which are orthogonal to A_{ess}, and which happen to be the same as those for which $M_{f,c}$ is empty. This proves that forms f which are non-special, the quantity $\delta(f)$ is bounded below by a positive constant independent of f.

To prove that the special forms are rare (cf. §10.5), we need to show that A_{ess} is big, and a crucial ingredient, that we borrow from recent previous works of the author, Khare, Deo, Medvedovsky, inspired by Nicolas and Serre, is that each local component of A is noetherian and of Krull dimension at least 2 (except when $p = 2, 3$, where we only know that some components have dimension at least 2).

The author is grateful to G. Chenevier, A. Conti, S. Deo, J. Lang, A. Medvedovsky, P. Monsky, J.-L. Nicolas, J.-P. Serre, J. Tilouine for many useful and interesting discussions. He is also grateful to J. Lang, A. Medvedovsky and A. Conti for their careful reading of a previous version of this manuscript.

2. Pseudo-representations and GMA

2.1. **Reminder and complements on pseudo-representations of dimension 2.**

2.1.1. *Pseudo-representations of a group.* For the general definition of a *pseudo-representation* of a group Π with values in a commutative ring A, we refer the reader to [6]. In dimension

2, which is the only case we shall need, it is not long to recall the equivalent definition proposed in *loc. cit.*, Lemma 1.9: a (two-dimensional) *pseudo-representation* of Π with values in A is a pair of maps $t : \Pi \to A$, $d : \Pi \to A$, such that

(2.1.1) *d is a group homomorphism from Π to A^*.*

(2.1.2) *t is a central function from Π to A.*

(2.1.3) $t(1) = 2$.

(2.1.4) $t(xy) + d(y)t(xy^{-1}) = t(x)t(y)$ *for all* $x, y \in \Pi$.

If Π is a topological group, A a topological ring, one says that the pseudo-representation (t, d) is *continuous* if t and d are. If 2 is invertible in A, d can be recovered from t by the formula $d(x) = \frac{t(x)^2 - t(x^2)}{2}$. If ρ is any representation $\Pi \to \mathrm{GL}_2(A)$, then it is easy to check that $(\operatorname{tr}\rho, \det\rho)$ is a pseudo-representation of dimension 2.

The *kernel* of (t, d) is defined by

$$\operatorname{Ker}(t, d) := \{y \in \Pi, d(y) = 1 \text{ and } \forall x \in \Pi,\ t(xy) = t(x)\}.$$

By (2.1.1) and (2.1.2), this is a normal subgroup of Π, closed if (t, d) is continuous. We observe that if 2 is invertible in A, we can omit the condition on d in the definition of $\operatorname{Ker}(t, d)$ as it follows from the condition on t. Both the maps t and d factor through the quotient group $\Pi/\operatorname{Ker}(t, d)$, and they define a pseudo-representation of dimension 2 of $\Pi/\operatorname{Ker}(t, d)$ with values in A whose kernel is trivial.

2.1.2. *Pseudo-representations of an algebra.* Let R be an A-algebra (non-necessarily commutative), and let (T, D) be a pair of maps $R \to A$. We say that (T, D) is a *pseudo-representation* of dimension 2 of R with values in A, if

(2.1.5) *$D(1) = 1$, D is multiplicative (i.e. $D(xy) = D(x)D(y)$ for $x, y \in R$) and homogeneous of degree 2 (i.e. $D(ax) = a^2 D(x)$ for $a \in A$, $x \in R$).*

(2.1.6) *T is A-linear and $T(xy) = T(yx)$ for all $x, y \in R$.*

(2.1.7) $T(1) = 2$.

(2.1.8) $D(x + y) = D(x) + D(y) + T(x)T(y) - T(xy)$ *for all* $x, y \in R$.

Lemma 2.1.1. *If $R = A[\Pi]$, the map $(T, D) \mapsto (T_{|\Pi}, D_{|\Pi})$ is a bijection between the set of all pseudo-representations of dimension 2 of R and the sets of all pseudo-representations of dimension 2 of Π.*

Proof — The proof below is closely inspired by [6].

If (T, D) satisfies (2.1.5) to (2.1.8), it is clear that $(T_{|\Pi}, D_{|\Pi})$ satisfies (2.1.1) to (2.1.3). Set $f(x, y) := T(x)T(y) - T(xy)$ for $x, y \in R$, so that (2.1.8) becomes

(2.1.9) $D(x + y) = D(x) + D(y) + f(x, y)$ *for all* $x, y \in R$.

For $x, y, z \in R$ one has $D((x + y)z) = D(xz) + D(yz) + f(xz, yz)$ but also, since D is multiplicative $D((x + y)z) = D(x + y)D(z) = D(xz) + D(yz) + f(x, y)D(z)$, hence

(2.1.10) $f(xz, yz) = f(x, y)D(z)$ *for all* $x, y, z \in R$.

If y is invertible in R, of inverse $z = y^{-1}$, applying (2.1.10) gives $f(x, y)D(y^{-1}) = f(xy^{-1}, 1)$. Since for every x, $T(x) = f(x, 1)$ by (2.1.7), one obtains $T(xy^{-1}) = f(x, y)D(y^{-1}) = T(x)T(y)D(y)^{-1} - T(xy)D(y)^{-1}$, that is

(2.1.11) $T(xy) + D(y)T(xy^{-1}) = T(x)T(y)$ *for all* $x \in R$, $y \in R^*$.

In particular, the restrictions of T and D to Π satisfy (2.1.4), hence $(T_{|\Pi}, D_{|\Pi})$ is a pseudo-representation of Π of dimension 2.

Conversely, if (t, d) is a pseudo-representation of dimension 2 of Π with values in A, let us denote by T the unique A-linear map $A[\Pi] \to A$ which coincides with t on Π and by f the symmetric bilinear form on $A[\Pi]$ defined by

$$f(x, y) := T(x)T(y) - T(xy).$$

For $x \in \Pi$, one has $f(x, x) = T(x)^2 - T(x^2) = 2d(x)$ by (2.1.4) and (2.1.3). Therefore, there exists a unique quadratic form $D : A[\Pi] \to A$ such that

(2.1.12) $D(x + y) - D(x) - D(y) = f(x, y)$ *for all* $x, y \in R$,[3] *and*

(2.1.13) $D(g) = d(g)$ *for all* $g \in \Pi$.

Thus we have defined functions T, D from $A[\Pi]$ to A that extends t and d, and that satisfies (2.1.6) to (2.1.8), as well as $D(1) = 1$ and D homogeneous of degree 2. We now proceed to show that D is multiplicative.

From (2.1.4) one gets $f(x, y) = t(xy^{-1})d(y)$ for $x, y \in \Pi$ hence

(2.1.14) $f(zx, zy) = f(xz, yz) = f(x, y)d(z)$ *for* $x, y, z \in \Pi$.

This relation holds more generally for $x, y, z \in A[\Pi]$ by linearity. For $z \in \Pi$, the quadratic forms on $A[\Pi]$ given by $x \mapsto D(xz)$ and $x \mapsto D(x)D(z)$ have the same polarization (namely $f(x, y)d(z)$, using (2.1.14)), and agrees on the basis Π on $A[\Pi]$. They are therefore equal:

(2.1.15) $D(xz) = D(x)D(z)$ *for* $x \in A[\Pi]$, $z \in \Pi$.

Again, the quadratic forms $z \mapsto D(xz)$ and $z \mapsto D(x)D(z)$ have the same polarization by (2.1.14), and they agree on Π by (2.1.15), hence they are equal. Therefore (T, D) is a pseudo-representation of R with values in A, and the map $(t, d) \mapsto (T, D)$ is an inverse of the restriction map considered in the statement. □

There is a notion of kernel for a pseudo-representation (T, D) of an algebra R:

$$\underline{\mathrm{Ker}}\,(T, D) = \{y \in R,\ D(y) = 0 \text{ and } T(yx) = 0\ \forall x \in R\}.$$

We say that (T, D) is *faithful* if $\underline{\mathrm{Ker}}\,(T, D) = 0$. It is easy to see that $\underline{\mathrm{Ker}}\,(T, D)$ is a two-sided ideal of R, and that (T, D) factors through $R/\underline{\mathrm{Ker}}\,(T, D)$ and defines a faithful pseudorepresentation of that algebra with values in A.

If (T, D) is a pseudo-representation of $A[\Pi]$, and (t, d) is the pseudo-representation of π obtained by restriction, then the relation between the $\mathrm{Ker}\,(t, d)$ and $\underline{\mathrm{Ker}}\,(T, D)$ is as follows:

[3]This condition (2.1.12) is expressed by saying that $f(x, y)$ is the *polarization* of the quadratic form D.

Lemma 2.1.2. *For $g \in \Pi$, one has $g \in \mathrm{Ker}\,(t,d)$ if and only if $g-1 \in \underline{\mathrm{Ker}}\,(T,D)$.*

Proof — If $g \in \Pi$, by linearity of trace $t(gh) = t(h)$ for all $h \in \Pi$ if and only if $T(gy) = T(y)$ for all y in $R = A[\Pi]$. If the latter condition holds, then in particular $t(g) = 2$, and under this condition $d(g) = 1$ and $D(g-1) = 0$ are equivalent since $D(g-1) = d(g) - t(g) + 1$. □

However, in general $\underline{\mathrm{Ker}}\,(T,D)$ is strictly larger than the two-sided ideal generated by the elements $g-1$, $g \in \mathrm{Ker}\,(t,d)$. If (T,D) is faithful then $\mathrm{Ker}\,(t,d) = \{1\}$, but the converse is false in general.

We say that a pseudo-representation (T,D) of R is *Cayley-Hamilton* if for every $x \in R$, one has $x^2 - T(x)x + D(x) = 0$. A faithful pseudo-representation is Cayley-Hamilton, but the converse is false in general.

2.2. **Generalized Matrix Algebras.** The notion of Generalized Matrix Algebra (GMA) is defined and studied in detail in [3, §1.3]. Here we will content ourselves with an *ad hoc* definition which is equivalent to the notion called GMA of type $(1,1)$ in the terminology of *loc. cit.*

Let A be a commutative ring. Suppose given two A-modules B and C, and a morphism of A-modules $m : B \otimes_A C \to A$ such that

(2.2.1) *for all $b, b' \in B$ and $c, c' \in C$, $m(b,c)b' = m(b',c)b$ and $m(b,c')c = m(b,c)c'$.*

With this data we define a not necessarily commutative A-algebra R, $R = A \oplus B \oplus C \oplus A$ as an A-module, endowed with the multiplication

$$(a,b,c,d) \times (a',b',c',d') = (aa' + m(b,c'), ab' + d'b, a'c + dc', dd' + m(b',c)),$$

for $a, a', d, d' \in A$, $b, b' \in B$, $c, c' \in C$: the distributivity of multiplication over addition is obvious, the unity for multiplication is $(1,0,0,1)$, and the associativity of multiplication is easily checked using (2.2.1). We call (A,B,C,m,R), or by abuse R, a *generalized matrix algebra*. A morphism of GMAs from (A,B,C,m,R) to (A',B',C',m',R') is the data (f_A, f_B, f_C) of a morphism of rings $f_A : A \to A'$ and two morphisms of A'-modules $f_B : B \otimes_A A' \to B'$ and $f_C : C \otimes_A A' \to C'$ such that $f_A(m(b,c)) = m'(f_B(b), f_C(c))$ for every $b \in B$, $c \in C$. A morphism of GMAs induces a morphism of A'-algebras $f_R : R \otimes_A A' \to R'$. When $A = A'$ and $f_A = \mathrm{Id}_A$, we say that this morphism is *over* A, or an *A-morphism*. A *sub-GMA* of (A,B,C,m,R) is a GMA (A',B',C',m',R') where $A' \subset A$, $B' \subset B$, $C' \subset C$ such that the these three inclusions maps define a morphism of GMAs. An *A-sub-GMA* is a sub-GMA where $A' = A$.

This meaning of these definitions becomes clearer if we decide to represent (a,b,c,d) as a matrix $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$, and to simply write bc or cb for $m(b,c)$, for then multiplication in R is computed as multiplication of ordinary matrices.

Lemma 2.2.1. *If in a GMA R, $BC = A$, then there are isomorphisms of A-modules form B and C onto A so that m corresponds to the multiplication $A \times A \to A$. In other words, there is an isomorphism over A of GMAs $R \simeq M_2(A)$.*

Proof — Let $b \in B$ and $c \in C$ such that $m(b,c) = 1$; by (2.2.1) one gets for $b' \in B$ that $b' = m(b,c)b' = m(b',c)b$ which shows that B is generated by b; moreover if for $a \in A$, $ab = 0$, then $m(ab,c) = am(b,c) = a = 0$. which shows that (b) is a basis of B. Similarly (c) is a basis of C and if we identify B and C with A using those basis, then m becomes the multiplication of A because $m(ab, a'c) = aa'm(b,c) = aa'$. □

We define the *trace* map $\mathrm{tr} : R \to A$ as $\mathrm{tr}\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) = a + d$ and the *determinant* map $\det : R \to A$ by $\det\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) = ad - bc$. It is clear that as in the case of usual matrix algebras, one has $\mathrm{tr}\,(rr') = \mathrm{tr}\,(r'r)$, $\det(rr') = \det(r)\det(r')$ and, if $p > 2$, $\det(r) = \frac{\mathrm{tr}\,(r)^2 - \mathrm{tr}\,(r^2)}{2}$.

It is easily checked that the pair of maps $(\mathrm{tr}\,, \det) : R \to A$ is a pseudo-representation of dimension 2 of R with values in A. We say that the *GMA* R is *faithful* (resp. *Cayley-Hamilton*) if $(\mathrm{tr}\,, \det)$ is. It is easily seen that T is faithful if and only if the map $m : B \otimes_A C \to A$ being *non-degenerate*, meaning that the only $b \in B$ such that $m(b,c) = 0$ for all $c \in C$ is $b = 0$, and the only $c \in C$ such that $m(b,c) = 0$ for all $b \in B$ is $c = 0$.

Lemma 2.2.2. *Assume that A is a domain, with fraction field K, and that $R = \begin{pmatrix} A & B \\ C & A \end{pmatrix}$ is a faithful GMA over A. Then there exists embedding of A-modules of B and C onto K, such that if B and C are identified with their image in K, $m : B \times C \to A$ is given by the multiplication of K.*

Proof — Since $m : B \otimes C \to A$ is non-degenerate, B and C have no torsion.

Fix $b_0 \in B - \{0\}, c_0 \in C - \{0\}$ such that $m(b_0, c_0) \neq 0$. Define a morphism of A-modules $i : B \to K$ by setting $i(b) = m(b, c_0)/m(b_0, c_0)$. If $i(b) = 0$, then $m(b, c_0) = 0$ so $m(b, c_0)b_0 = m(b_0, c_0)b = 0$, and $b = 0$ since B has no torsion; thus i is injective. Define $j : C \to K$ by setting $j(c) = m(b_0, c)$, which embeds C into K, and one easily checks that $m(b,c) = i(b)j(c)$. □

Lemma 2.2.3. *Assume that A is a domain, with fraction field K, and that $R = \begin{pmatrix} A & B \\ C & A \end{pmatrix}$ is a faithful GMA over A, and that $BC \neq 0$. Then $R \otimes_A K$ is isomorphic, as a GMA over K, to $M_2(K)$.*

This follows from the preceding lemma.

2.3. **Topological GMAs.** If A is a topological ring, a *topological GMA* is a GMA R over A provided with a topology that makes it a topological A-algebra. More concretely, if $R = \begin{pmatrix} A & B \\ C & A \end{pmatrix}$ is a GMA, making R a topological GMA amounts to giving a topology on B and C that makes them topological A-modules, and make the multiplication $m : B \times C \to A$ continuous.

For instance, if A is a noetherian local ring which is complete for the topology defined by its maximal ideal, and if R is finite as an A-module, then R provided with its finite A-module topology is a topological GMA.

We observe that for any topological ring A, $R = M_2(A)$ has a unique structure of topological GMA, namely the one given by the product topology on $M_2(A) = A^4$.

2.4. **Pseudo-representations and GMA-valued representations.** Let A be a complete local ring with maximal ideal $\mathfrak{m}$ and residue field $\mathbb{F}$. Let Π be a group, $(t,d):\Pi\to A$ a pseudo-representation.

The reduction $\bar{t},\bar{d}$ modulo $\mathfrak{m}$ of t, d form a pseudo-representation of dimension 2 of G with values in $\mathbb{F}$. We make the following definition:

Definition 2.4.1. We say that (t,d) is *residually multiplicity-free* if there exists a (necessarily unique up to isomorphism) semi-simple representation $\bar{\rho}:\Pi\to\mathrm{GL}_2(\mathbb{F})$ such that $\operatorname{tr}\bar{\rho}=\bar{t}$, $\det\bar{\rho}=\bar{d}$, and a $g_0\in\Pi$ such that $\bar{\rho}(g_0)$ is conjugate in $\mathrm{GL}_2(\mathbb{F})$ with a diagonal matrix with distinct diagonal terms.

By a theorem of Rouquier, Nyssen and Chenevier, there always exists a finite extension $\mathbb{F}'$ of $\mathbb{F}$ and a $\bar{\rho}:\Pi\to\mathrm{GL}_2(\mathbb{F}')$ such that $\operatorname{tr}\bar{\rho}=\bar{t}$, $\det\rho=\bar{d}$. If (t,d) is residually multiplicity-free we can take $\mathbb{F}'=\mathbb{F}$. Moreover, since the $\mathbb{F}$-algebra $\mathrm{End}_G(\bar{\rho})$ is contained in the commutant of $\bar{\rho}(g_0)$, which is isomorphic to $\mathbb{F}\times\mathbb{F}$, the representation $\bar{\rho}$ is either absolutely irreducible, or the direct sum of two distinct characters. Conversely, if there is a $\bar{\rho}:\Pi\to\mathrm{GL}_2(\mathbb{F})$ such that $\operatorname{tr}\bar{\rho}=\bar{t}$, $\det\bar{\rho}=\bar{d}$, then (t,d) is multiplicity free if $\bar{\rho}$ is the sum of two distinct characters, or at least becomes so after changing $\mathbb{F}$ by a quadratic extension if $\bar{\rho}$ is absolutely irreducible (or even just reducible when $\mathbb{F}$ is not of characteristic 2).

Proposition 2.4.2. *Assume that (t,d) is residually multiplicity-free.*

(i) *There exists a faithful GMA (A,B,C,m,R) over A, and a morphism of groups $\rho:\Pi\to R^*$ such that*

(2.4.1) *on Π, $\operatorname{tr}\rho=t$ and $\det\rho=d$,*

(2.4.2) *$A\rho(\Pi)=R$.*

(ii) *If (ρ,R) and (ρ',R') are as in (i), then there exists a unique isomorphism of A-algebras $\Psi:R\to R'$ such that $\Psi\circ\rho=\rho'$.*

(iii) *Given an element $g_0\in\Pi$ such that $\bar{\rho}(g_0)$ has two distinct eigenvalues λ_0,μ_0 in $\mathbb{F}$, there exists a faithful GMA (A,B,C,m,R) over A, and a morphism of groups $\rho:\Pi\to R^*$ satisfying* (2.4.1) *and* (2.4.2)*, and such that*

(2.4.3) *$\rho(g_0)$ is diagonal and $\rho(g_0)\equiv\begin{pmatrix}\lambda_0&0\\0&\mu_0\end{pmatrix}\pmod{\mathfrak{m}}$.*

(iv) *If $g_0\in\Pi$, (ρ,R) and (ρ',R') are as in (iii), the unique isomorphism of A-algebras, $\Psi:R\to R'$ such that $\Psi\circ\rho=\rho'$ (cf. (ii)) is an A-isomorphism of GMAs.*

(v) *If $\bar{\rho}$ is irreducible, then R is isomorphic to $M_2(A)$ as a GMA over A. If $\bar{\rho}$ is reducible, then one has $BC\subset\mathfrak{m}$.*

(vi) *If (ρ,R) is as in (i), then $\operatorname{Ker}\rho=\operatorname{Ker}(t,d)$, and denoting by $\tilde{\rho}:A[\Pi]\to R$ the morphism of A-algebras extending ρ, one has $\operatorname{Ker}\tilde{\rho}=\underline{\operatorname{Ker}}(T,D)$.*

(vii) *If A is noetherian, if Π is a profinite group satisfying the p-finiteness condition*[4]*, and if (t,d) is continuous then for (ρ,R) as in (i), R is of finite type as an A-module and if R is given its unique topology of A-algebra, the morphism $\rho:\Pi\to R^*$ is continuous.*

Proof — Let (T,D) be the pseudo-representation of $A[\Pi]$ with values in A extending (t,d), as in Lemma 2.1.1. Let R be the quotient of $A[\Pi]$ by $\underline{\mathrm{Ker}}\,(T,D)$, let $\tilde{\rho}$ be the natural projection $\tilde{\rho}:A[\Pi]\to R$ and let ρ be the restriction of $\tilde{\rho}$ to Π. Let g_0 be an element of Π as in (iii), let Π_0 be the subgroup generated by g_0 in Π and let $R_0\subset R$ be the A-subalgebra $A\rho(\Pi_0)$. As proved in [3, §1.4], the algebras R and R_0 are integral over A. By [3, §1.4] and the hypothesis made on g_0, if J_0 denotes the Jacobson radical of R_0, then there is an isomorphism of $\mathbb{F}$-algebra $R_0/J_0\simeq\mathbb{F}\bar{\rho}(\Pi_0)$. The algebra $\mathbb{F}\bar{\rho}(\Pi_0)$ is isomorphic to $\mathbb{F}\times\mathbb{F}$ and we can fix such an isomorphism that sends $\bar{\rho}(g_0)$ to $\left(\begin{smallmatrix}\lambda_0 & 0\\ 0 & \mu_0\end{smallmatrix}\right)$. The two obvious idempotents $(1,0)$ and $(0,1)$ of $\mathbb{F}\times\mathbb{F}$ can be lifted to idempotents e_1 and e_2 of R_0 such that $e_1e_2=0$, $e_1+e_2=1$. This makes R_0 and R GMAs with the properties stated in (i) and (iii). The uniqueness statement (ii) is clear, since if (ρ,R) is as in (i), R has to be a quotient of $A[\Pi]$ through which (T,D) factors, hence of the form $A[\Pi]/I$ with I a two-sided ideal contained in $\underline{\mathrm{Ker}}\,(T,D)$, but since R is faithful we must have $I=\underline{\mathrm{Ker}}\,(T,D)$. The uniqueness statement (iv) is equally easy, since a morphism Ψ as in (iv), which exists and is unique by (ii), preserves the diagonal matrix $\rho(g_0)$ which has diagonal terms that are distinct modulo $\mathfrak{m}$, hence preserves the idempotents e_1 and e_2 and is a morphism of GMA. Finally (v) in the irreducible case is a well-known result of Rouquier and Nyssen extended by Chenevier ([6, Theorem 2.22]) to the case of general pseudo-representation, and (v) in the reducible case follows from [3, Theorem 1.4.4].

Let us prove (vi). Since $\tilde{\rho}:A[\Pi]\to R$ is surjective, one has $\underline{\mathrm{Ker}}\,(T,D)=\tilde{\rho}^{-1}\underline{\mathrm{Ker}}\,(tr_R,\det_R)$. Since R is faithful, it follows that $\underline{\mathrm{Ker}}\,(T,D)=\mathrm{Ker}\,\tilde{\rho}$. Using Lemma 2.1.2, thus implies that $\mathrm{Ker}\,(t,d)=\mathrm{Ker}\,\rho$.

For (vii), let $A[[\Pi]]$ be the completed group algebra of the pro-finite group Π. Chenevier proves in [7, §4] that t and d can be extended into a continuous pseudo-representation $(\tilde{T},\tilde{D})$ of $A[[\Pi]]$ of dimension 2 with values in A. The restriction of $(\tilde{T},\tilde{D})$ to the sub-algebra $A[\Pi]$ is therefore the pseudo-representation (T,D) of $A[\Pi]$ corresponding to (t,d). From the definition of the linear kernel, one has $\underline{\mathrm{Ker}}\,(T,D)=\underline{\mathrm{Ker}}\,(\tilde{T},\tilde{D})\cap A[\Pi]$. Hence $R=A[\Pi]/\underline{\mathrm{Ker}}\,(T,D)$ is isomorphic to an A-sub-algebra of $A[[\Pi]]/\underline{\mathrm{Ker}}\,(\tilde{T},\tilde{D})$. The latter is a finite type A-module by [7, Lemma 4.5]. Since A is noetherian, R is of finite type as an A-module.

Let us prove now that ρ is continuous. Choose a finite family of elements $g_1,\dots,g_m$ of Π such that the $\rho(g_i)$ generate R. Consider the map $R\to A^n$, $x\mapsto\mathrm{tr}\,(x\rho(g_i))$. Since R is faithful, this map is an injection, and by the elementary properties of the natural topology

[4]Following Mazur [19, page 246], we say that a pro-finite group Π satisfies the *p-finiteness condition* if for every open subgroup H of Π, the largest pro-p quotient H_p of H is topologically of finite type. This condition is always satisfied for a profinite group Π which is topologically of finite type, and it is also known to hold for a Galois group $\Pi=G_{\mathbb{Q},S}$ where S is a finite set of places (*loc. cit.*).

of finite A-modules, it induces an homeomorphism of R onto its image. It therefore suffices to prove that the map $g \mapsto \operatorname{tr}(\rho(g)\rho(g_i))$ is continuous for $i = 1, \dots, m$, but this is clear since that map is just $t(gg_i)$. □

Definition 2.4.3. Any representation $\rho : \Pi \to R^*$ satisfying the property (i) of the above proposition will be called a (t,d)-*representation*. If in addition ρ satisfies condition (iii), we shall say that ρ is *adapted to* (g_0, λ_0, μ_0).

Remark 2.4.4. Without the assumption of p-finiteness on Π, the assertion (vii) of the preceding theorem is false. For a counter-example, let $A = \mathbb{F}_p[\epsilon]$ with $\epsilon^2 = 0$, V an infinite-dimensional $\mathbb{F}_p$-vector space seen as an A-module through the map $A \to \mathbb{F}_p, \epsilon \mapsto 0$, $b : V \times V \to \mathbb{F}$ a non-degenerate $\mathbb{F}$-bilinear form, and $m : V \times V \to A$ defined as ϵb. Then m satisfies condition (2.2.1), hence there is a GMA (A, V, V, m, R) which moreover is faithful. Define $\Pi = R^*$, and consider the restriction (t,d) of $(\operatorname{tr}, \det)$ to Π. This is a pseudo-representation of dimension 2, and $A[\Pi]/\underline{\operatorname{Ker}}\,(T,D) = R$ but R is not finite as an A-module.

Lemma 2.4.5. *Let R be a GMA over A and $\rho : \Pi \to R^*$ a representation of a group Π. Assume that there exists an element $g_0 \in \Pi$ such that $\rho(g_0)$ is diagonal, with diagonal terms distinct modulo $\mathfrak{m}$. Then $A\rho(\Pi)$ is a sub-A-GMA of R.*

Furthermore, if $R = M_2(A)$ and $\rho \mod \mathfrak{m}$ is absolutely irreducible, then $A\rho(\Pi) = R$.

Proof — If $\rho(g_0) = \left(\begin{smallmatrix} \lambda_0 & 0 \\ 0 & \mu_0 \end{smallmatrix}\right)$, then the matrix $e_1 := \left(\begin{smallmatrix} 1 & 0 \\ 0 & 0 \end{smallmatrix}\right) = \frac{\rho(g_0) - \mu_0\rho(1)}{\lambda_0 - \mu_0}$ belongs to $A\rho(\Pi)$, and similarly the matrix $e_2 := 1 - e_1 = \left(\begin{smallmatrix} 0 & 0 \\ 0 & 1 \end{smallmatrix}\right)$. Then $e_1 A\rho(G) e_1$ is an A-submodule of A that contains 1, so is A, and similarly for $e_2 A\rho(\Pi) e_2$. Define $B' := e_1 A\rho(\Pi) e_2$, a submodule of B, and $C' := e_1 A\rho(\Pi) e_2$, a submodule of C. Then $A\rho(G) = \begin{pmatrix} A & B' \\ C' & A \end{pmatrix}$ an A-sub-GMA of R.

For the *furthermore*, suppose by contradiction that either B' or C' is a proper submodule of $B = C = A$. Then $B'C'$ is a proper ideal of A, so is contained in $\mathfrak{m}$, which shows that $\operatorname{tr}\rho \pmod{\mathfrak{m}}$ is the sum of two characters $(\Pi \mapsto \mathbb{F}^*, g \mapsto e_1\rho(g)e_1 \pmod{\mathfrak{m}}$ for the first, the same with e_2 for the second), contradicting the hypothesis. □

3. Reminder of representation theory

3.1. **The classification of representations $\bar\rho$.** Let Π be a group, $\mathbb{F}$ a finite field, $\bar\rho : \Pi \to \mathrm{GL}_2(\mathbb{F})$ a representation which is either absolutely irreducible or the sum of two distinct characters. Let us set $\overline{G} = \bar\rho(\Pi) \subset \mathrm{GL}_2(\mathbb{F})$ and $\overline{\overline{G}}$ the *projective image* of $\bar\rho$, that is the image of $\overline{G}$ in $\mathrm{PGL}_2(\mathbb{F})$. The well-known classification of such representations according to their projective image is as follows.

Name	$\overline{\overline{G}}$ is isomorphic to	Subcase	Description of $\bar{\rho}$	Description of $\mathrm{ad}^0\bar{\rho}$
Cyclic	$\mathbb{Z}/n\mathbb{Z}$	$n=2$	$\bar{\chi}\oplus\bar{\chi}'$, with $\bar{\chi}^2=\bar{\chi}'^2$	$(\bar{\chi}/\bar{\chi}')^2\oplus 1$
		$n>2$	$\bar{\chi}\oplus\bar{\chi}'$, with $\bar{\chi}^2\neq\bar{\chi}'^2$	$\bar{\chi}/\bar{\chi}'\oplus 1\oplus\bar{\chi}'/\bar{\chi}$
Dihedral	D_n	$n>2$	irreducible, isomorphic to $\mathrm{Ind}_{\Pi_1}^{\Pi}\psi_1$ for a unique index 2 subgroup Π_1 of Π	$\epsilon_1\oplus\mathrm{Ind}_{\Pi_1}^{\Pi}\tau$, with $\mathrm{Ind}_{\Pi_1}^{\Pi}\tau$ irreducible
		$n=2$	irreducible, isomorphic to $\mathrm{Ind}_{\Pi_1}^{\Pi}\psi_i$ for three index two subgroups Π_1, Π_2 and Π_3	$\epsilon_1\oplus\epsilon_2\oplus\epsilon_3$
Large image	$\mathrm{PGL}_2(\mathbb{F}_q)$ or $\mathrm{PSL}_2(\mathbb{F}_q)$		irreducible	irreducible
Exceptional	A_4, S_4 or A_5			

In the table above, χ and χ' are two distinct characters of Π, ψ_i is a non-trivial character of Π_i for $i=1,2,3$, and ϵ_i is the character of Π of kernel Π_i for $i=1,2,3$, and τ is a non-trivial character of Π_1. The group D_n is the dihedral group of order $2n$.

3.2. **A group cohomology computation.**

Proposition 3.2.1. *In the large image and exceptional case, if V is adjoint representation of the natural representation of $\bar{G}$, one has $H^1(\bar{G},V)=0$.*

Proof — The representation V of $\overline{G}$ factors through $\overline{\overline{G}}$. Let Z be the kernel of $\overline{G}\mapsto\overline{\overline{G}}$. The inflation-restriction exact sequence is

$$0\to H^1(\overline{\overline{G}},V)\to H^1(\overline{G},V)\to H^1(Z,V)$$

and since Z is of order prime to p, and V is of order a power of p, the last term is 0. It therefore suffices to prove that $H^1(\overline{\overline{G}},V)=0$.

For $\overline{\overline{G}}=\mathrm{PGL}_2(\mathbb{F}_q)$ or $\overline{\overline{G}}=\mathrm{PSL}_2(\mathbb{F}_q)$, this follows from Matthias Wendt's answer to question 178025 of mathoverflow.

If $\overline{\overline{G}}$ is isomorphic to A_4 or S_4, then the result is clear if $p\geq 5$. If $p=3$, we argue as follows: Let K_4 be the Klein subgroup of A_4. One has an exact sequence $0\to H^1(A_4/K_4,V^{K_4})\to H^1(A_4,V)\to H^1(K_4,V)$. Since V is still irreducible as a representation of K_4, $V^{K_4}=0$. Since K_4 has order prime to 3, $H^1(K_4,V)=0$. Hence $H^1(A_4,V)=0$. For S_4 we use the sequence $H^1(S_4/A_4,V^{A_4})\to H^1(S_4,V)\to H^1(A_4,V)$ where the first and last term are 0.

If $\overline{\overline{G}}$ is isomorphic to A_5, the result is clear if $p\geq 7$. For $p=5$, $\overline{\overline{G}}$ is conjugate to $\mathrm{PSL}_2(\mathbb{F}_5)$, a case which has already been dealt with. For $p=3$, let us consider A_4 as the subgroup of A_5 fixing one letter, and note that since A_4 has index 5 which is prime to $|V|=27$, it suffices to prove that $H^1(A_4,V)=0$, which has already being done. □

4. Pink's Lie theory for GMAs

4.1. **Assumptions concerning the base ring A.**

In all this section, p is a prime. We suppose given

(4.1.1) *a topological ring A which is compact and semi-local and whose residue fields have characteristic p.*

By definition, A semi-local means that A is a finite product $\prod_{i=1}^{r} A_i$, where the A_i are local rings. We provide each of the ring A_i with its quotient topology from the topology of A. The A_i are compact rings, and are local. We shall call $\mathfrak{m}_i$ the maximal ideal of A_i and $\mathbb{F}_i = A_i/\mathfrak{m}_i$ its residue field. By an abuse of language which hopefully will not induce confusion, we shall also call $\mathfrak{m}_i$ the corresponding maximal ideal in A, namely $\prod_{j\neq i} A_j \times \mathfrak{m}_i$, so that we can write $A/\mathfrak{m}_i = \mathbb{F}_i$, and $(\mathfrak{m}_i)$, $i = 1, \ldots, r$ are the complete list of maximal ideals of A.

In general, the compact topology on A_i is not the $\mathfrak{m}_i$-adic topology. However:

Lemma 4.1.1. (i) *The topological ring A (and its factors A_i) is pro-finite (i.e. the open co-finite ideals J form a basis of neighborhood of 0)*

(ii) *The fields $\mathbb{F}_i$ are finite and the ideals $\mathfrak{m}_i$ are open in A_i.*

(iii) *Each ring A_i is $\mathfrak{m}_i$-adically separated and complete, and its $\mathfrak{m}_i$-adic topology is finer that its given topology.*

(iv) *One has A_i noetherian if and only if $\mathfrak{m}_i^2$ is open in A_i. In this case, the $\mathfrak{m}_i$-adic topology on A_i coincide with its given topology.*

Proof — Assertion (i) is [26, Prop. 5.1.2]. If we write $A_i = \operatorname{proj\,lim} A_i/J$ with J running among open cofinite ideals of A_i, then each A_i/J is local with maximal ideal $\mathfrak{m}_i/J$ and residue field $\mathbb{F}_i$. In particular $\mathbb{F}_i$ is finite. Moreover $\mathfrak{m}_i = \operatorname{proj\,lim} \mathfrak{m}_i/J$: the inclusion $\mathfrak{m}_i \subset \operatorname{proj\,lim} \mathfrak{m}_i/J$ is obvious, while if $x \in A_i$ is not in $\mathfrak{m}_i$, x is invertible, so its image in any A_i/J is not in $\mathfrak{m}_i/J$. Therefore we see that $\mathfrak{m}_i$ is closed in A_i, and since it is cofinite, it is also open. This proves (ii). For J any open co-finite ideal of A_i, A_i/J is finite local, hence Artinian, and there is an n such that $(\mathfrak{m}_i/J)^n = 0$ in A_i/J, that is $\mathfrak{m}_i^n \subset J$ in A_i. Hence the family $\mathfrak{m}_i^n$ is cofinal to the family of co-finite open ideals, and A_i is $\mathfrak{m}_i$-adically complete. Therefore, every open set for the given topology contains an ideal $\mathfrak{m}_i^n$ hence is also open for the $\mathfrak{m}_i$-adic topology. This proves (iii). Finally, note that $\mathfrak{m}_i^2$ is open if and only if $\mathfrak{m}_i/\mathfrak{m}_i^2$ is finite, i.e. by Nakayama if and only if $\mathfrak{m}_i$ is of finite type, i.e. if and only if A_i is noetherian. In this case, all the $\mathfrak{m}_i^n$ are cofinite, hence A_i is compact for the $\mathfrak{m}_i$-adic topology. The identity map $A_i \to A_i$ where the source is given the $\mathfrak{m}_i$-adic topology, and the target its original topology, which is continuous by (iii), is therefore closed, hence an homeomorphism. This proves (iv). □

The Jacobson radical $\mathrm{rad}A$ of A will be denoted by $\mathfrak{m}$. We have $\mathfrak{m} = \prod_{i=1}^{r} \mathfrak{m}_i = \cap_{i=1}^{r} \mathfrak{m}_i$. It follows from the lemma that A is $\mathfrak{m}$-complete and profinite for the $\mathfrak{m}$-adic topology.

From now on and throughout this section, we make the following assumption:

(4.1.2) *The prime p is odd.*

Since $p > 2$, if x is an element of $1+\mathfrak{m}$, there exists by Hensel's lemma a unique $y \in 1+\mathfrak{m}$ such that $y^2 = x$. We shall henceforth denote that element by $\sqrt{x}$. We observe that the map $x \mapsto \sqrt{x}$ is continuous.

4.2. **A slightly generalized setting for Pink's theory.** Pink's theory is concerned with certain closed subgroups of $\mathrm{GL}_2(A)$, the multiplicative group of invertible elements in the matrix algebra $M_2(A)$. To allow for more generality, we shall consider closed subgroups of the multiplicative group of units of a *generalized matrix algebra.*

To fix notation for the rest of this section,

(4.2.1) *Let* $R = \begin{pmatrix} A & B \\ C & A \end{pmatrix}$ *be a topological GMA over* A*, which is compact and Cayley-Hamilton (cf. §2.2).*

We denote by R^* the multiplicative group of invertible elements in R. Clearly, it is also the set of elements r of R such that $\det r \in A^*$. It follows that R^* is both open and closed in R, and, provided with the subspace topology, is a compact topological group. We denote by SR^* the set of elements in R^* with determinant 1. Obviously this is a closed normal subgroup of R^*.

We shall denote by $\mathrm{rad}R$ the Jacobson radical of the algebra R. It is a closed hence compact additive subgroup of R. We shall denote by R^1 the subgroup $1 + \mathrm{rad}R$. It is a closed normal subgroup of R^*.

We call SR^1 the intersection of SR and R^1 in R. Obviously SR^1 is a closed normal subgroup of R^*.

Remark 4.2.1. To fix ideas, we shall now give an explicit description of the various rings and groups introduced above, in the case where A is local. In this case there are two possibilities regarding the ideal $BC = m(B, C)$ of the ring A. Either $BC = A$, or $BC \subset \mathfrak{m}$.

When $BC = A$, then by Lemma 2.2.1, R is isomorphic as GMA to $M_2(A)$, so we can as well assume that $R = M_2(A)$ as a topological GMA. Its radical $\mathrm{rad}R$ is $M_2(\mathfrak{m}) = \mathfrak{m}M_2(A)$ and the quotient $R/\mathrm{rad}R$ is the simple algebra $M_2(\mathbb{F})$. The group R^1 is the multiplicative group of matrices in $M_2(A)$ which are congruent to Id modulo $\mathfrak{m}M_2(A)$. The group SR^1 is the subgroup of those whose determinant is 1. Note that in the literature, those groups R^1 and SR^1 are often denoted $\mathrm{GL}_2^1(A)$ and $\mathrm{SL}_2^1(A)$ respectively. In this case we are in the situation considered by Pink.

When $BC \subset \mathfrak{m}$, the radical $\mathrm{rad}R$ is $\begin{pmatrix} \mathfrak{m} & B \\ C & \mathfrak{m} \end{pmatrix}$ and the quotient $R/\mathrm{rad}R$ is the semi-simple algebra of diagonal matrices $\begin{pmatrix} \mathbb{F} & 0 \\ 0 & \mathbb{F} \end{pmatrix}$. The group SR^1 is the group of matrices $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ in R such that $a \equiv d \equiv 1 \pmod{\mathfrak{m}}$ and $ad - bc = 1$.

In the general case, if A is a finite product of local rings A_i, then R naturally decomposes as a product of GMA R_i and the radical $\mathrm{rad}R$ as a product of $\mathrm{rad}R_i$, for each of which one of the two description above holds.

Lemma 4.2.2. *If* $m \in \mathrm{rad}R$*,* $\mathrm{tr}\, m, \mathrm{tr}\, m^2, \det m \in \mathfrak{m}$.

Proof — We may assume that A is local, in which case we use the description of R and $\mathrm{rad}R$ given in the preceding remark. If $R = M_2(A)$, $m \in M_2(\mathfrak{m})$ and the result is clear.

If $BC \subset \mathfrak{m}$, then $m \in \begin{pmatrix} \mathfrak{m} & B \\ C & \mathfrak{m} \end{pmatrix}$ so $\mathrm{tr}\,(m) \in \mathfrak{m}$ and $\mathrm{tr}\,(m^2) \in \mathfrak{m}^2 + BC \subset \mathfrak{m}$, and finally $\det(m) = (\mathrm{tr}\,(m)^2 - \mathrm{tr}\,(m^2))/2 \in \mathfrak{m}$. □

Lemma 4.2.3. *One has* $\cap_n (\mathrm{rad}R)^n = 0$.

Proof — In the case $R = M_2(A)$, $(\mathrm{rad}R)^n = M_2(\mathfrak{m}^n)$ and since $\cap \mathfrak{m}^n = 0$ by Lemma 4.1.1(iii), the results follows. In the case $BC \subset \mathfrak{m}$, an element of $(\mathrm{rad}R)^n$ is a product of n matrices $\left(\begin{smallmatrix} a_i & b_i \\ c_i & d_i \end{smallmatrix}\right)$ with $a_i, d_i \in \mathfrak{m}$, $b_i \in B$, $c_i \in C$. The upper left coefficient of this product is the product of k a_i's, l b_j's and l c_k's with $k+2l = n$, hence is in $\mathfrak{m}^{k+l}$. Therefore the upper left coefficient of a matrix in $\cap_n (\mathrm{rad}R)^n$ is 0. Similar computations for the other coefficients allow to conclude. □

Notation: In the rest of this paper, we shall use freely the following notation: if S is a set of matrices, S^0 is the set of matrices of trace zero in S. If X, Y are two closed additive subgroups of R, we shall denote by $[X, Y]$ (resp. $X \cdot Y$ or XY) the *closure* of the subgroup generated by all commutators $[x, y]$ (resp. xy) for $x \in X,\ y \in Y$.

Remark 4.2.4. We observe that $(\mathrm{rad}R)^0$, provided with the Lie bracket $[r, r'] = rr' - r'r$, is a Lie algebra over A. Concretely, $(\mathrm{rad}R)^0 = \begin{pmatrix} \mathfrak{m} & \mathfrak{m} \\ \mathfrak{m} & \mathfrak{m} \end{pmatrix}^0$ when $R = M_2(A)$ and $(\mathrm{rad}R)^0 = \begin{pmatrix} \mathfrak{m} & B \\ C & \mathfrak{m} \end{pmatrix}^0$ when $BC \subset \mathfrak{m}$.

4.3. **Pink's Theta map.** Following Pink, define a continuous A-linear map

$$\Theta :\ R \to R,\ r \mapsto r - \frac{\mathrm{tr}\, r}{2}\mathrm{Id}.$$

Pink states eleven formulas involving Θ and tr . We state the analog in our more general situation of the formulas we need:

(4.3.1) *If* $x, y \in R$, $[\Theta(x), \Theta(y)] = \Theta(xy) - \Theta(yx)$.

(4.3.2) *If* $x \in SR$, $y \in R$, *one has* $\mathrm{tr}\,(x)\Theta(y) = \Theta(xy) + \Theta(x^{-1}y)$.

(4.3.3) *If* $x, y \in R$, *one has* $2\Theta(xy) = [\Theta(x), \Theta(y)] + \mathrm{tr}\,(x)\Theta(y) + \mathrm{tr}\,(y)\Theta(x)$.

(4.3.4) *If* $x, y \in R$, $\mathrm{tr}\,(\Theta(x)\Theta(y)) = \mathrm{tr}\,(xy) - \mathrm{tr}\,(x)\mathrm{tr}\,(y)/2$.

(4.3.5) *If* $x \in SR$, *one has* $\Theta(x^{-1}) = -\Theta(x)$.

(4.3.6) *If* $x, y, u, v \in (\mathrm{rad}R)^0$, *one has* $4\mathrm{tr}\,(xy)[u, v] = [y, [x, [u, v]]] + [x, [y, [u, v]]] + [[x, v], [y, u]] + [[y, v], [x, u]]$.

(4.3.7) *If* $x, y, u, v \in (\mathrm{rad}R)^0$, *one has* $4\mathrm{tr}\,([u, v]x)y = [y, [x, [u, v]]] - [x, [y, [u, v]]] + [[x, v], [y, u]] + [[y, v], [x, u]]$.

These formulas are proved by easy computations left to the reader, using the facts that in R, $\mathrm{tr}\,(xy) = \mathrm{tr}\,(yx)$ and that for any $x \in R$, the Cayley-Hamilton identity holds, namely $x^2 - \mathrm{tr}\,(x)x + \det(x) = 0$, with $\det(x) = (\mathrm{tr}\,(x)^2 - \mathrm{tr}\,(x^2))/2$. (Also useful is the formula $xy + yx - \mathrm{tr}\,(x)y - \mathrm{tr}\,(y)x + \mathrm{tr}\,(x)\mathrm{tr}\,(y) - \mathrm{tr}\,(xy) = 0$ for $x, y \in R$, which is obtained by bi-linearizing the Cayley-Hamilton identity).

Alternatively, we can use Proposition 1.3.13 of [3] which implies that every Cayley-Hamilton GMA R can be embedded in a trace-preserving way into $M_2(A')$ for A' some commutative ring containing A. This reduces the formulas to prove to the case of $M_2(A')$. In this case these formulas are stated in [25], though their proofs are also left to the reader.

Lemma 4.3.1. *The map Θ induces a homeomorphism from SR^1 onto $(\mathrm{rad}R)^0$. Its inverse is given by*

$$\Theta^{-1}\left(\begin{smallmatrix} a & b \\ c & -a \end{smallmatrix}\right) = \left(\begin{smallmatrix} a+\sqrt{1+bc+a^2} & b \\ c & -a+\sqrt{1+bc+a^2} \end{smallmatrix}\right) \tag{4.3.8}$$

or equivalently

$$\Theta^{-1}m = m + \sqrt{1+\mathrm{tr}\,(m^2)/2}Id. \tag{4.3.9}$$

Moreover one has

$$\mathrm{tr}\,(\Theta^{-1}m) = 2 + \textstyle\sum_{n\geq 1} 2^{1-n}\binom{1/2}{n}\mathrm{tr}\,(m^2)^n. \tag{4.3.10}$$

Proof — It is clear that Θ sends SR^1 into $(\mathrm{rad}R)^0$. If m in $(\mathrm{rad}R)^0$, $x \in SR^1$ and $\Theta(x) = m$ then one has $x = m + \lambda\mathrm{Id}$ for some $\lambda \in 1+\mathfrak{m}$ and using that $\det x = 1$, one gets $\lambda^2 = 1+\mathrm{tr}\,(m^2)/2$. Since $\mathrm{tr}\,m^2 \in \mathfrak{m}$ by Lemma 4.2.2, this equation defines a unique λ, which shows that for every $m \in (\mathrm{rad}R)^0$, there exists a unique x such that $\Theta(x) = m$, and proves the formula for Θ^{-1}. Formula (4.3.10) follows using Newton's Taylor expansion for $\sqrt{1+t}$.

□

4.4. **The Lie algebra L attached to a subgroup of SR^1.** The object of Pink's theory is to understand the structure of the closed subgroups of $SL_2^1(A)$, using Lie-theoretic methods. Our objective here is to expand Pink's constructions and results to the case of subgroups of SR^1, where R is a GMA over A as above. We shall offer from this sub-section §4.4 to §4.7 a self-contained presentation, where arguments, whose details follow closely those of [25] are re-organized and somewhat simplified.

Let Γ be a closed subgroup of SR^1. Following Pink we define a closed subgroup L of $(\mathrm{rad}R)^0$ as the closure of the additive subgroup of $(\mathrm{rad}R)^0$ generated by $\Theta(\Gamma)$.

Obviously, $\Gamma \subset \Theta^{-1}(L)$ but we may not have equality. Observe that the subgroup L is not in general an A-submodule of $(\mathrm{rad}R)^0$.

Theorem 4.4.1 (Pink)**.** *One has $[L, L] \subset L$, that is L is a Lie subring of $(\mathrm{rad}R)^0$.*

Proof — It suffices to show that if $x, y \in \Gamma$, $[\Theta(x), \Theta(y)] \in L$, that is $\Theta(xy) - \Theta(yx) \in L$ by (4.3.1). Since xy and yx are in Γ, this is clear. □

Definition 4.4.2. We call $L = L(\Gamma)$ the *Pink's Lie algebra* of Γ.

Lemma 4.4.3 (Pink)**.** *For $\gamma \in \Gamma$, one has $\mathrm{tr}\,(\gamma)L \subset L$.*

Proof — This follows immediately from (4.3.2). □

4.5. **The pseudo-ring P attached to a closed subgroup Γ of SR^1.** For Γ and L as in the preceding section, we define

$$P = P(\Gamma) = \mathrm{tr}\,(L^2).$$

This is a closed additive subgroup of A. (Note that our P is denoted by C in [25]).

Theorem 4.5.1 (Pink)**.** *One has $PL \subset L$.*

Proof — By definition, P is the closure of the additive subgroup generated by the $\mathrm{tr}\,(\Theta(x)\Theta(y))$ for $x, y \in \Gamma$. By (4.3.4), one has $\mathrm{tr}\,(\Theta(x)\Theta(y)) = \mathrm{tr}\,(xy) - \mathrm{tr}\,(x)\mathrm{tr}\,(y)/2 \in \mathrm{tr}\,(\Gamma) + \mathrm{tr}\,(\Gamma)^2$. Thus $P \subset \mathrm{tr}\,(\Gamma) + \mathrm{tr}\,(\Gamma)^2$, and the theorem follows from the preceding lemma. □

Corollary 4.5.2. *The subgroup P of A is stable by multiplication; in other words, it is a pseudo-subring*[5] *of A. Moreover P is the smallest closed pseudo-subring of A containing $\mathrm{tr}\,(\gamma) - 2$ for all $\gamma \in \Gamma$.*

Proof — Since $PL \subset L$, one has $P^2 = P\mathrm{tr}\,(L \cdot L) = \mathrm{tr}\,(PL \cdot L) \subset \mathrm{tr}\,(L \cdot L) = P$, hence P is a pseudo-subring. Let us call by Q the subgroup of A generated by $\mathrm{tr}\,(\gamma) - 2$, $\gamma \in \Gamma$. Let us first show that $Q \subset P$. If $\gamma \in \Gamma$, $m = \Theta(\gamma)$, one has $\mathrm{tr}\,(\gamma) = 2 + \sum_{n \geq 1} 2^{1-n} \binom{1/2}{n} \mathrm{tr}\,(m^2)^n$ by (4.3.10). Since $\mathrm{tr}\,(m^2) \in P$ and P is stable by multiplication, $\mathrm{tr}\,(m^2)^n \in P$ for all n and since P is closed, $Q \subset P$. On the other hand, as seen in the proof of the preceding theorem, P is the closed subgroup of A generated by the elements $\mathrm{tr}\,(xy) - \mathrm{tr}\,(x)\mathrm{tr}\,(y)/2$ for $x, y \in \Gamma$, that is by the elements $\mathrm{tr}\,(xy) - 2 - (\mathrm{tr}\,(x) - 2)(\mathrm{tr}\,(y) - 2)/2 - (\mathrm{tr}\,(x) - 2) - (\mathrm{tr}\,(y) - 2) \in Q + Q^2$ Thus $Q \subset P \subset Q + Q^2$, and since P is a closed pseudo-ring, it follows that the closed pseudo-subring of A generated by Q is P. □

4.6. **Pink's converse theorem.**

Theorem 4.6.1 (Pink)**.** *Let L be a Lie subring of $(\mathrm{rad}R)^0$. Set $P = \mathrm{tr}\,(L \cdot L)$. If $PL \subset L$, then $H := \Theta^{-1}(L)$ is a closed subgroup of SR^1, and Θ is a homeomorphism of H onto L. In particular $L = L(H)$, and $P = P(H)$.*

Proof — If $PL \subset L$, then one sees as in the proof of Cor. 4.5 that P is a pseudo-subring and $\mathrm{tr}\,(h) - 2 \subset P$ for every $h \in H$. Thus $\mathrm{tr}\,(H)L \subset L$

If $x, y \in H$, $2\Theta(xy) = [\Theta(x), \Theta(y)] + \mathrm{tr}\,(x)\Theta(y) + \mathrm{tr}\,(y)\Theta(y)$ by (4.3.3). The first term is in L because L is a Lie subring, the last two are also in L since $\mathrm{tr}\,(H)L \subset L$. Therefore, $xy \in H$. Also by (4.3.5), $\Theta(x^{-1}) = -\Theta(x)$ so $x^{-1} \in H$. This shows that H is a subgroup of SR^1, obviously closed. □

[5] A *pseudo-subring* of a ring A is a subset P which is an additive subgroup of A and is closed under multiplication.

4.7. **Descending the central sequence.** Let Γ be a closed subgroup of SR^1, $L = L(\Gamma)$ its Pink's Lie algebra, $P = P(\Gamma) = \mathrm{tr}\,(L \cdot L)$ the attached pseudo-ring. We define:

- for $n \geq 1$, closed Lie subrings L_n of $(\mathrm{rad}R)^0$, defined by recurrence as follows: $L_1 = L$, $L_{n+1} = [L_n, L]$;
- for $n \geq 1$, closed subsets $H_n = \Theta^{-1}L_n$ of SR^1.
- for $n \geq 1$, closed subgroups Γ_n of SR^1 defined by recurrence as follows: $\Gamma_1 = \Gamma$, $\Gamma_{n+1} = (\Gamma_n, \Gamma)$ (closed commutators subgroup) for $n \geq 1$

Proposition 4.7.1 (Pink). *Let $n, m \geq 1$.*

(i) *If $n \geq 1$, $L_{n+1} \subset L_n$.*
(ii) *If $n, m \geq 1$, $[L_n, L_m] \subset L_{n+m}$.*
(iii) *If $n \geq 1$, for $h \in H_n$, $\mathrm{tr}\,(h) - 2 \in P$.*
(iv) *If $n \geq 1$, H_n is a closed subgroup of SR^1 and $\Theta : H_n \to L_n$ is an homeomorphism.*
(v) *If $n \geq 2$, $PL_n \subset L_{n+2}$.*
(vi) *If $n \geq 2$, Θ induces a bicontinuous isomorphism of groups $H_n/H_{n+1} \simeq L_n/L_{n+1}$.*

Proof — Assertions (i) and (ii) follows easily by induction from Theorem 4.4.1. For (iii), write $m = \Theta(h) \in L_n \subset L$. Then by (4.3.10), $\mathrm{tr}\,(h) - 2 = \sum_{n\geq 1} 2^{1-n}\binom{1/2}{n}\mathrm{tr}\,(m^2)^n \in P$.

For (iv), from $PL \subset L$ one proves by induction that $PL_n \subset L_n$. One therefore has $\mathrm{tr}\,(L_n \cdot L_n)L_n \subset \mathrm{tr}\,(L \cdot L)L_n = PL_n \subset L_n$. It then follows from Theorem 4.6.1 applied to the Lie subring L_n that $H_n = \Theta^{-1}(L_n)$ is a closed subgroup of L_n, and that Θ is a homeomorphism of H_n onto L_n.

Formula (v) follows from (4.3.6) for $n = 2$ and then by induction for all $n \geq 2$.

For (vi), if $x, y \in H_n$, then by (4.3.3),

$$\Theta(xy) - \Theta(x) - \Theta(y) = \frac{1}{2}([\Theta(x), \Theta(y)] - (\mathrm{tr}\,(x) - 2)\Theta(y) - (\mathrm{tr}\,(y) - 2)\Theta(x)).$$

Hence $\Theta(xy) - \Theta(x) - \Theta(y) \in L_{2n} + L_{n+2} \subset L_{n+1}$ by (i), (ii), (iii) and (v) (applicable since $n \geq 2$). This shows that Θ induces a group morphism from H_n to L_n/L_{n+1}. This morphism is surjective by (iv), and the kernel of this morphism is clearly H_{n+1}, hence (vi). □

The most important theorem of Pink's theory is Theorem 4.7.3 below, which shows that for $n \geq 2$, the terms Γ_n of the descending central sequence of Γ are determined by their Lie algebra L_n, hence by L.

First, we need a lemma:

Lemma 4.7.2 (Pink). *Let $n \geq 2$. For $x \in H_1, y \in H_{n-1}$ one has*

$$\Theta(xyx^{-1}y^{-1}) \equiv [\Theta(x), \Theta(y)] \pmod{L_{n+1}}.$$

In particular, $xyx^{-1}y^{-1} \in H_n$.

Proof — One writes

$$2\Theta(xyx^{-1}y^{-1}) = 2\Theta([x,y]x^{-1}y^{-1}) = [\Theta([x,y]), \Theta(x^{-1}y^{-1})] + \mathrm{tr}\,(x^{-1}y^{-1})\Theta([x,y])$$

by (4.3.3). Since obviously $[\Theta(x),\Theta(y)] = [x,y] = \Theta([x,y])$, this can be written

$$2\Theta(xyx^{-1}y^{-1}) = [[\Theta(x),\Theta(y)],\Theta(x^{-1}y^{-1})] + \mathrm{tr}\,(x^{-1}y^{-1})[\Theta(x),\Theta(y)]$$

Now $\Theta(x) \in L_1$, $\Theta(y) \in L_{n-1}$, so $[\Theta(x),\Theta(y)] \in L_n$ and $\Theta(x^{-1}y^{-1}) \in L_1$. Thus, the first term of the RHS is in L_{n+1}. As for the second term, $\mathrm{tr}\,(x^{-1}y^{-1}) - 2 \in P$, and since $PL_n \subset L_{n+2}$, one gets that the second term is $2[\Theta(x),\Theta(y)] \pmod{L_{n+1}}$ and the lemma follows. □

Theorem 4.7.3 (Pink)**.** *For $n \geq 2$, one has $\Gamma_n = H_n = \Theta^{-1}(L_n)$. Hence Θ realizes an homeomorphism of Γ_n on L_n for $n \geq 2$.*

Proof — We follow approximately Pink's method.

By definition $\Gamma_1 = \Gamma \subset H_1$. We prove by induction that $\Gamma_n \subset H_n$ for all n. Assuming $\Gamma_{n-1} \subset H_{n-1}$, we get for $x \in \Gamma$, $y \in \Gamma_{n-1}$, $\Theta(x) \in L_1$, $\Theta(y) \in L_{n-1}$, hence by the commutator relation $\Theta(xyx^{-1}y^{-1}) \in [L, L_{n-1}] + L_{n+1} \subset L_n$, and $xyx^{-1}y^{-1} \in H_n$. Since H_n is a closed subgroup of SR^1, and Γ_n is the closed subgroup generates by the $xyx^{-1}y^{-1}$ as above, one gets $\Gamma_n \subset H_n$.

Let Δ_n be the closed subgroup of $(\mathrm{rad}R)^0$ generated by $\Theta(\Gamma_n)$. We claim by induction that $\Delta_n + L_{n+1} = L_n$ for all $n \geq 1$. This is true for $n = 1$ because by definition $\Delta_1 = L_1$. For $n \geq 2$, since Γ_n is the subgroup generated by $xyx^{-1}y^{-1}$ for $x \in \Gamma$, $y \in \Gamma_{n-1}$, and Θ is a morphism from Γ_n to L_n/L_{n+1}, $\Delta_n + L_{n+1}$ is the closed subgroup of $(\mathrm{rad}R)^0$ generated by L_{n+1} and the elements $\Theta(xyx^{-1}y^{-1})$, that is, by the lemma, the elements $[\Theta(x),\Theta(y)]$. Since the closed subgroups generated by those elements is $[L_1, L_{n-1}] = L_n$, we get that $\Delta_n + L_{n+1} = L_n$.

For $n \geq 2$, since Θ is a morphism from H_n onto L_n/L_{n+1}, $\Theta(\Gamma_n) + L_{n+1}$ is already a closed subgroup of L_n, hence it is $\Delta_n + L_{n+1} = L_n$. We thus have shown, for all $n \geq 2$

$$\Theta(\Gamma_n) + L_{n+1} = L_n.$$

Applying this formula for n replaced by $n+1$ gives a description of L_{n+1} that we can plug in the LHS of the formula, getting $\Theta(\Gamma_n) + L_{n+2} = L_n$, and by induction on m, $\Theta(\Gamma_n) + L_{n+m} = L_n$ for all $m \geq 1$. Since $\cap_m L_{n+m} = 0$ (by Lemma 4.2.3) and $\Theta(\Gamma_n)$ is closed, one gets $\Theta(\Gamma_n) = L_n$, hence $\Gamma_n = H_n$ and the theorem. □

Thus, the knowledge of the Lie algebra L of Γ determines the derived subgroup Γ_2 of Γ. There is an other result of Pink, limiting the possibilities for the quotient Γ/Γ_2:

Theorem 4.7.4 (Pink)**.** *The composition law $*$ on L/L_2 defined by*

$$x * y = x(\sqrt{1 + \mathrm{tr}\,(y^2)/2}) + y(\sqrt{1 + \mathrm{tr}\,(x^2)/2})$$

makes L/L_2 a commutative group. The map Θ induces a bicontinuous morphism of groups $H_1/H_2 \to (L/L_2, *)$. The image Δ of $\Gamma/H_2 = \Gamma/\Gamma_2$ in L/L_2, which is obviously a subgroup of L/L_2 for the law $*$, topologically generates L/L_2 for the law $+$.

Since we shall only use this theorem in the case where $R = M_2(A)$ (see Prop. 4.8.2), we just refer to [25, Prop. 2.6] for the proof.

4.8. **Complements to Pink's theory.**

4.8.1. *Functoriality w.r.t. surjective morphism of rings.* Let J be a closed ideal of A. The ring A/J is still a compact semi-local topological ring, of radical $\mathfrak{m}/(\mathfrak{m} \cap J)$, with residue fields a subset of the set of residue fields of A, hence all finite of characteristic $p > 2$. In other words, A/J satisfies (4.1.1) and (4.1.2).

The A/J-algebra $R_J = R/JR = \begin{pmatrix} A/J & B/JB \\ C/JC & A/J \end{pmatrix}$ is a GMA which is obviously of finite type as an A/J-module, and also Cayley-Hamilton. We denote by π_J the surjective morphism of algebras $R \to R/JR$. This morphism induces a morphism of multiplicative groups $\pi_J : R^* \to R_J^*$ which is still surjective because an element of a GMA is invertible if and only if its determinant is. It also induces a surjection $R^1 \to R_J^1$ and a morphism $SR^1 \to SR_J^1$, which we again denote by π_J. Also π_J induces a map $\pi_J : (\mathrm{rad}R)^0 \to (\mathrm{rad}R_J)^0$.

If Γ is a closed subgroup of SR^1, let us denote by Γ_J the closed subgroup $\pi_J(\Gamma)$. Then we can apply Pink's theory to Γ_J and define sub-Lie-algebras $L_n(\Gamma_J)$ of $(\mathrm{rad}R_J)^0$. The functoriality mentioned in the title is the fact that

(4.8.1) *for all* $n \geq 1$, $\pi_J(L_n(\Gamma)) = L_n(\Gamma_J)$.

This is easy to see for $n = 1$ from the definition for L_1, and then by induction on n for any n.

4.8.2. *Multiplication by* $\mathrm{tr}\,(\Gamma)$.

Lemma 4.8.1. *For every* $\gamma \in \Gamma$, *and every* $n \geq 1$, *one has* $\mathrm{tr}\,(\gamma)L_n = L_n$.

Proof — It suffices to prove the first assertion for $n = 1$, because then, one has $L_{n+1} = [L_1, L_n] = [\mathrm{tr}\,(\gamma)L_1, L_n] = \mathrm{tr}\,(\gamma)[L_1, L_n] = \mathrm{tr}\,(\gamma)L_{n+1}$. For $n = 1$ we already know that $\mathrm{tr}\,(\gamma)L \subset L$, so we just need to show that $\mathrm{tr}\,(\gamma)^{-1}L \subset L$.

Note that $\mathrm{tr}\,(\gamma) \equiv 2 \pmod{\mathfrak{m}}$. Let $m = \Theta(\gamma)$. Then $\gamma = \Theta^{-1}(m)$ so that by (4.3.10), $\mathrm{tr}\,\gamma = 2 + \sum_{n\geq 1} 2^{1-n}\binom{1/2}{n}\mathrm{tr}\,(m^2)^n$ and $\mathrm{tr}\,(\gamma)^{-1} = 2^{-1} + \sum_{n\geq 1} b_n \mathrm{tr}\,(m^2)^n$ for some coefficients $b_n \in \mathbb{Z}_p$ that we need not compute. Since $\mathrm{tr}\,(m^2) \in P(\Gamma)$, $\mathrm{tr}\,(m^2)^n L \subset L$ hence $\mathrm{tr}\,(\gamma)^{-1}L \subset L$ which completes the proof of the first assertion. □

4.8.3. *A simple class of examples.* Let I be a closed pseudo-subring of A contained in $\mathfrak{m}$, that is a closed additive subgroup of $\mathfrak{m}$, stable by multiplication. Let $R = M_2(A)$ be the standard GMA. Then $L = \begin{pmatrix} I & I \\ I & I \end{pmatrix}^0$ is a $\mathbb{Z}_p$-Lie sub-algebra of $\begin{pmatrix} \mathfrak{m} & \mathfrak{m} \\ \mathfrak{m} & \mathfrak{m} \end{pmatrix}^0 = (\mathrm{rad}R)^0$. We will determine the closed subgroups Γ of $\mathrm{SL}_2^1(R)$ that have L as Pink's Lie algebra; actually there is only one such subgroup:

Proposition 4.8.2. *Let Γ be a closed subgroup of $SL_2^1(R)$ such that $L(\Gamma) = L = \begin{pmatrix} I & I \\ I & I \end{pmatrix}^0$. Then $\Gamma = \Theta^{-1}(L)$ and Θ realizes an homeomorphism from Γ onto L. More generally $\Gamma_n = \Theta^{-1}\left(\begin{pmatrix} I^n & I^n \\ I^n & I^n \end{pmatrix}^0\right)$ for every $n \geq 1$.*

Proof — If we set $X = \left(\begin{smallmatrix} 0 & 1 \\ 0 & 0 \end{smallmatrix}\right)$, $Y = \left(\begin{smallmatrix} 0 & 0 \\ -1 & 0 \end{smallmatrix}\right)$, $J = \left(\begin{smallmatrix} 1 & 0 \\ 0 & -1 \end{smallmatrix}\right)$, then the usual commutation relations are $[qX, q'Y] = qq'J$, $[qJ, q'X] = 2qq'X$ and $[qJ, q'Y] = -2qq'Y$, for any $q, q' \in I$. The additive subgroup generated by these elements, $L_2 = [L, L]$, is thus $\begin{pmatrix} I^2 & I^2 \\ I^2 & I^2 \end{pmatrix}^0$. Similarly one proves by induction that $L_n = \begin{pmatrix} I^n & I^n \\ I^n & I^n \end{pmatrix}^0$ for any n.

For $x \in L$, the power series defining $\sqrt{1 + \operatorname{tr} x^2/2} - 1$ has all its terms in I^2, hence is in I since I is closed under multiplication and topologically. Thus for $x, y \in L$, $y\sqrt{1 + \operatorname{tr} x^2} - y \in IL \subset L_2$ and it follows that $x * y \equiv x + y \pmod{L_2}$ (using the notation of Theorem 4.7.4.). The subgroup $\Theta(\Gamma) \pmod{L_2}$ of $(L/L_2, *)$ is thus also a subgroup for the additive law $+$, and therefore, by Theorem 4.7.4, is such that its topological closure is L/L_2. Since it is already closed, one has $\Theta(\Gamma) \equiv L \pmod{L_2}$. Since $\Theta(\Gamma)$ contains L_2, we obtain $\Theta(\Gamma) = L$. The proposition easily follows. □

4.8.4. *Haar measures.* For any compact group Δ, we denote by μ_Δ the Haar measure on Δ normalized so as to have a total mass 1.

Lemma 4.8.3. *Let H and H' be two compact groups, $(H_n)_{n \geq n_0}$ (resp. $(H'_n)_{n \geq n_0}$) a decreasing sequence of closed normal subgroups in H (resp. in H') such that $H_{n_0} = H$ and $\cap_n H_n = \{1\}$ (resp. $H'_{n_0} = H'$ and $\cap_n H'_n = \{1\}$). Let f be an homeomorphism from H to H' (not necessarily a group homomorphism) such that $f(1) = 1$ and for every h in H, $f(hH_n) = f(h)H'_n$. We assume that*

(i) *either the induced map $\bar{f}_n : H_n/H_{n+1} \to H'_n/H'_{n+1}$ is a morphism of groups,*
(ii) *or the H_n are open in H.*

Then f sends the Haar measure μ_H to the Haar measure $\mu_{H'}$.

Proof — By assumption, $\bar{f}_n : H_n/H_{n+1} \to H'_n/H'_{n+1}$ is either an isomorphism of groups, or a bijection between finite groups, hence in both cases sends the normalized Haar measure of H_n/H_{n+1} on the normalized Haar measure of H'_n/H'_{n+1}. Using this, and an induction over n and Fubini, one sees that the map $\bar{f} : H/H_n \to H'/H'_n$ preserves Haar measures.

To prove the lemma, it suffices to prove that $\mu_H(U) = \mu_{H'}(f(U))$ for any open set U in H. Since H is compact, U contains H_n for some n, and f induces a bijection $\bar{f}$ from the finite group H/H_n to the finite group H'/H'_n. If $\bar{U}$ is the image of U in H/H_n, we are reduced to prove that $\mu_{H/H_n}(\bar{U}) = \mu_{H'/H'_n}(\bar{f}(\bar{U}))$, which we have already done. □

Proposition 4.8.4. *In the situation of Theorem 4.7.3, the homeomorphism $\Theta : \Gamma_2 \to L_2$ sends the Haar measure μ_{Γ_2} to the Haar measure μ_{L_2}.*

Proof — We apply the preceding lemma to $f = \Theta$, $H = \Gamma_2$, $H' = L_2$, $n_0 = 2$, $H_n = \Gamma_n$, $H'_n = L_n$. □

Let us note for later use another application of Lemma 4.8.3.

Lemma 4.8.5. *Let V be a closed additive subgroup of R, $\sigma : V \to V$ a map satisfying $\sigma(0) = 0$ and the following property:*

$$\forall v, v' \in V, n \in \mathbb{N},\ v - v' \in \mathfrak{m}^n R \Longrightarrow \sigma(v) - \sigma(v') \in \mathfrak{m}^{n+1} R$$

Let $\Psi : V \to V$ be the map $\Psi(v) = v + \sigma(v)$. Then Ψ is an homeomorphism of V onto V and sends the Haar measure μ_V to itself.

Proof — If $v \neq v' \in V$, let n be an integer such that $v - v' \in \mathfrak{m}^n R$ but $v - v' \notin \mathfrak{m}^{n+1} R$. Then $\Psi(v) - \Psi(v') = (v - v') + (\sigma(v) - \sigma(v'))$ and since $\sigma(v) - \sigma(v') \in \mathfrak{m}^{n+1} R$, $\Psi(v) - \Psi(v')$ is not in $\mathfrak{m}^{n+1} R$ and in particular $\Psi(v) \neq \Psi(v')$. Hence Ψ is injective. If $v' \in V$, consider the map $h : V \to V, y \mapsto v' - \sigma(y)$. The hypothesis made on σ implies that this map has a fixed point in V, so there exists v such that $v' - \sigma(v) = v$, or $\Psi(v) = v'$. Hence Ψ is surjective. As Ψ is obviously continuous, and closed since V is compact, it is a homeomorphism. To show that Ψ preserves the Haar measure, we apply Lemma 4.8.3 with $H = H' = V$, $H_n = H'_n = V \cap (\mathfrak{m}^n R)$: for any n, the group H_n is open in V since $\mathfrak{m}^n R$ is open in R and the hypothesis implies that $\Psi(v + H_n) = \Psi(v) + H_n$. □

4.9. **Decomposition of Lie algebras.** In this subsection, R is a GMA over A satisfying the conditions of §4.2.

4.9.1. *Decomposable Lie algebras.* Let L be a closed subspace of $(\mathrm{rad} R)^0$.

(4.9.1) *We shall say that L is decomposable if, for any $\begin{pmatrix} a & b \\ c & -a \end{pmatrix} \in L$, one has $\begin{pmatrix} a & 0 \\ 0 & -a \end{pmatrix} \in L$ and $\begin{pmatrix} 0 & b \\ c & 0 \end{pmatrix} \in L$.*

We shall denote by Δ and ∇ the additive groups of diagonal matrices and anti-diagonal matrices in L. Thus, L is decomposable if and only if

(4.9.2) $L = \Delta \oplus \nabla$.

Since by definition matrices in L have trace 0 and diagonal terms are in the radical $\mathfrak{m}$ of A, we see that Δ has the form

(4.9.3) $\Delta = I_1 J$, *with I_1 a unique additive closed subgroup of $\mathfrak{m}$,*

where J denotes as usual the matrix $\left(\begin{smallmatrix} 1 & 0 \\ 0 & -1 \end{smallmatrix}\right)$. We take (4.9.3) as the definition of I_1. We thus have, if L is decomposable

$$L = I_1 J \oplus \nabla.$$

Let us set $P = \mathrm{tr}\,(L^2)$.

Lemma 4.9.1. *If L is decomposable, one has $P = \mathrm{tr}\,(\Delta^2) + \mathrm{tr}\,(\nabla^2) = I_1^2 + \mathrm{tr}\,(\nabla^2)$.*

Proof — If $m, m' \in L$, we can write $m = \delta + \epsilon$, $m' = \delta' + \epsilon'$ with $\delta, \delta' \in \Delta$ and $\epsilon, \epsilon' \in \nabla$. Then $\mathrm{tr}\,(mm') = \mathrm{tr}\,(\delta\delta') + \mathrm{tr}\,(\epsilon\epsilon')$ since the matrices $\delta\epsilon'$ and $\epsilon\delta'$ are anti-diagonal. Thus, $P \subset \mathrm{tr}\,(\Delta^2) + \mathrm{tr}\,(\nabla^2)$, and since the other inclusion is clear, this implies the result. □

Proposition 4.9.2. *Let $L = I_1 J \oplus \nabla \subset (\mathrm{rad}R)^0$ be a decomposable space. The following are equivalent:*

(4.9.4) *There exists a closed subgroup Γ of SR^1 such that L is the Lie algebra of Γ.*

(4.9.5) *One has:*

(4.9.5.1) $[\nabla, \nabla] \subset I_1 J$,

(4.9.5.2) $I_1[J, \nabla] \subset \nabla$,

(4.9.5.3) $\mathrm{tr}\,(\nabla^2) I_1 \subset I_1$,

(4.9.5.4) $\mathrm{tr}\,(\nabla^2)\nabla \subset \nabla$,

(4.9.5.5) $I_1^3 \subset I_1$,

Proof — The two first conditions (4.9.5.1) and (4.9.5.2) are equivalent to L being stable by Lie bracket. Since $P = I_1^2 + \mathrm{tr}\,(\nabla)^2$, the condition $PL \subset L$ is equivalent to the conjunction of (4.9.5.3), (4.9.5.4), (4.9.5.5) and $I_1^2\nabla \subset \nabla$. But this condition follows from (4.9.5.2): applied twice, this property gives $I_1^2[J, [J, \nabla]] \subset \nabla$, that is $I_1^2\nabla \subset \nabla$. Therefore the five conditions (4.9.5) together are equivalent to L being a Lie subring of $(\mathrm{rad}R)^0$ and $PL \subset L$. The proposition thus follows from Theorems 4.5.1 and 4.6.1. □

When L is decomposable, we set:

(4.9.6) $B_1 := \{b \in B, \exists c \in C, \begin{pmatrix} 0 & b \\ c & 0 \end{pmatrix} \in \nabla\}$,

(4.9.7) $C_1 := \{c \in C, \exists b \in B, \begin{pmatrix} 0 & b \\ c & 0 \end{pmatrix} \in \nabla\}$.

We have obviously $\nabla \subset \begin{pmatrix} 0 & B_1 \\ C_1 & 0 \end{pmatrix}$ but the inclusion may be strict.

4.9.2. *Strongly decomposable Lie algebra.* Let L be a closed subspace of $(\mathrm{rad}R)^0$.

(4.9.8) *We shall say that L is strongly decomposable if, for any $\begin{pmatrix} a & b \\ c & -a \end{pmatrix} \in L$, one has $\begin{pmatrix} a & 0 \\ 0 & -a \end{pmatrix} \in L$, $\begin{pmatrix} 0 & b \\ 0 & 0 \end{pmatrix} \in L$ and $\begin{pmatrix} 0 & 0 \\ c & 0 \end{pmatrix} \in L$.*

If we define B_1, C_1 and I_1 as above (4.9.6), one can reformulate (4.9.8) as

(4.9.9) $L = \begin{pmatrix} I_1 & B_1 \\ C_1 & I_1 \end{pmatrix}^0$.

If $P = \mathrm{tr}\,(L^2)$, then we see that

(4.9.10) $P = I_1^2 + B_1 C_1$

Proposition 4.9.3. *Let $L = \begin{pmatrix} I_1 & B_1 \\ C_1 & I_1 \end{pmatrix}^0 \subset (\mathrm{rad}R)^0$ be a strongly decomposable closed subgroup. The following are equivalent:*

(4.9.11) *There exists a closed subgroup* Γ *of* SR^1 *such that* L *is the Lie algebra of* Γ.

(4.9.12) *One has:*

(4.9.12.1) $B_1C_1 \subset I_1$,

(4.9.12.2) $I_1B_1 \subset B_1$ *and* $I_1C_1 \subset C_1$,

(4.9.12.3) $I_1^3 \subset I_1$,

Proof — If L is strongly decomposable, it is in particular decomposable, and we use the notation of §4.9.1: $L = I_1J \oplus \nabla$ with $\nabla = \begin{pmatrix} 0 & B_1 \\ C_1 & 0 \end{pmatrix}$. One thus has $[\nabla, \nabla] = B_1C_1J$ and $I_1[J, \nabla] = \begin{pmatrix} 0 & I_1B_1 \\ I_1C_1 & 0 \end{pmatrix}$, so (4.9.12.1) is equivalent to (4.9.5.1) and (4.9.12.2) is equivalent to (4.9.5.2).

Since $\mathrm{tr}\,(\nabla^2) = B_1C_1$, (4.9.5.3) reads $B_1C_1I_1 \subset I_1$, which is a consequence of the above. Similarly, (4.9.5.4) read $B_1C_1B_1 \subset B_1$ and $B_1C_1C_1 \subset C_1$, both of which follow from the above. Thus we see that (4.9.12) is equivalent to (4.9.5) and the proposition follows. □

5. Admissible pseudo-representations

5.1. **Hypotheses on the base ring** A**.** In all this section, we let $\mathbb{F}$ be a finite field of characteristic p, and we denote by $W(\mathbb{F})$ the ring of Witt vectors of $\mathbb{F}$. We suppose we are given

(5.1.1) *A topological* $W(\mathbb{F})$*-algebra* A *which is compact and semi-local, and such that the maps* $W(\mathbb{F}) \to A/\mathfrak{m}_i$*, where* $\mathfrak{m}_i$*,* $i = 1, \dots, r$ *are the maximal ideals of* A*, are surjective.*

Thus A satisfies the condition (4.1.1) with the small additional requirements that A is a topological $W(\mathbb{F})$-algebra and that the maps $W(\mathbb{F}) \to A/\mathfrak{m}_i$ are surjective, which implies that the residue fields $\mathbb{F}_i$, $i = 1, \dots, r$, are all equal at $\mathbb{F}$. We use the same notations as in the preceding section: $A = \prod_{i=1}^r A_i$ with the A_i's local, and we write (by abuse) $\mathfrak{m}_i$ for the maximal ideal of A_i.

We shall denote by $s : \mathbb{F} \to A$ the map obtained by taking the Teichmuller lift in $W(\mathbb{F})$ of an element of $\mathbb{F}$ and seeing it as an element of A through the structural map $W(\mathbb{F}) \to A$. The map s is a set-theoretical section of the residue map $A \to A/\mathfrak{m} = \mathbb{F}$, and preserve multiplication but not addition. The elements of A that belong to $s(\mathbb{F})$ will be called *constants*.

5.2. **Admissible pseudo-deformations.** We now proceed to define an admissible pseudo-deformation over A. It is a 4-tuple $(\Pi, \bar{\rho}, t, d)$ where

(5.2.1) Π *is a profinite group.*

(5.2.2) $\bar{\rho} = (\bar{\rho}_i)_{i=1}^r$ *is a family of isomorphism classes of continuous representations* $\bar{\rho}_i : \Pi \to GL_2(\mathbb{F})$*, each of them being either absolutely irreducible or the sum of two distinct characters.*

(5.2.3) (t,d) *is a continuous pseudo-representation of* Π *over* A *such that for* $i = 1,\dots,r$ *we have* $\operatorname{tr}\bar\rho_i \equiv t \pmod{\mathfrak{m}_i}$ *and* $\det\bar\rho_i \equiv d \pmod{\mathfrak{m}_i}$.

(5.2.4) *We have* $d(g) \in s(\mathbb{F})$ *for all* $g \in \Pi$

(5.2.5) *As a topological* $W(\mathbb{F})$*-algebra,* A *is generated by* $t(\Pi)$.

The condition (5.2.4) expresses the fact that this pseudo-representation has *constant determinant*. Even if we do not assume it, there is always a twist of (t,d) which has constant determinant, namely the twist by the character $g \mapsto \sqrt{d(g)^{-1}s(\bar d(g))}$.

If we denote by (t_i,d_i) the composition of (t,d) with $A \to A_i$, the condition (5.2.3) says that (t_i,d_i) is a *deformation* over A_i of the pseudo-representation $(\operatorname{tr}\bar\rho_i, \det\bar\rho_i)$ attached to $\bar\rho_i$, or as it is customary to say, a *pseudo-deformation* of $\bar\rho_i$ over A_i.

If $A \to A'$ is a surjective map, then A' with its quotient topology satisfies (5.1.1), and we can write $A' = \prod_{j\in J} A'_j$, where J is a subset of $\{1,\dots,r\}$ and the map $A \to A'$ is the product of surjective maps $A_j \to A'_j$ for $j \in J$. If we denote by (t',d') the composition of (t,d) with the map $A \to A'$, then it is clear that $(\Pi, (\bar\rho_j)_{j\in J}, t', d')$ is an admissible pseudo-deformation over the ring A'. In particular, for every $i = 1,\dots,r$, $(\Pi,\bar\rho_i,t_i,d_i)$ is an admissible pseudo-deformation over the local ring A_i.

5.3. **Equivalent formulations for** (5.2.5)**.** Following [16], let $\mathcal{C}$ be the category of topological $W(\mathbb{F})$-algebras B that are compact and local, and such that the map $W(\mathbb{F}) \to B/\mathfrak{m}_B$ is surjective, where $\mathfrak{m}_B$ is the maximal ideal of B. Given a topological group Π and a continuous representation $\bar\rho : \Pi \to \mathrm{GL}_2(\mathbb{F})$, we consider the functor $\mathcal{F}_{\bar\rho}$ from $\mathcal{C}$ to the categories of sets, such that $\mathcal{F}_{\bar\rho}(B)$ is the set of continuous pseudo-representation $(t,d) : \Pi \to B$ such that $t \equiv \operatorname{tr}\bar\rho \pmod{\mathfrak{m}_B}$, $d \equiv \det\bar\rho \pmod{\mathfrak{m}_B}$, and $d(g) \in s(\mathbb{F})$ for all $g \in \Pi$. By [16], this functor is representable by a ring $A_{\bar\rho,\mathrm{univ}}$.

Let $(\Pi,\bar\rho,t,d)$ be a pseudo-representation over $A = \prod_i A_i$ satisfying (5.2.2), (5.2.3) and (5.2.4), and let $i \in \{1,\dots,r\}$. Thus (Π,t_i,d_i) defines an element of $\mathcal{F}_{\bar\rho_i}(A_i)$ hence a map $A_{\bar\rho_i,\mathrm{univ}} \to A_i$.

Proposition 5.3.1. $(\Pi,\bar\rho,t,d)$ *satisfies* (5.2.5) *(i.e. is admissible) if and only if for* $i = 1,\dots,r$*, the morphisms* $A_{\bar\rho_i,univ} \to A$ *are surjective.*

This is clear.

Corollary 5.3.2. *If* $(\Pi,\bar\rho,t,d)$ *is an admissible pseudo-deformation over* A*, and if* Π *satisfies Mazur's finiteness* p*-condition (i.e. the maximal pro-*p*-quotient of every open subgroup of* Π *is topologically finitely generated), then* A *is noetherian.*

Proof — Since Π satisfies Mazur's p-finiteness condition, we know that $A_{\bar\rho_i,\mathrm{univ}}$ is noetherian by [16] in the case $\bar\rho_i$ absolutely irreducible, by [1] in the case $\bar\rho_i$ reducible and $p > 2$ and by [6] in the case $p = 2$. Thus A_i is noetherian for all i, and A is noetherian. □

Proposition 5.3.3. *Assume* $p > 2$*. In the definition of an admissible pseudo-representation, condition* (5.2.5) *can be replaced by the apparently weaker condition*

(5.3.1) *As a topological $W(\mathbb{F})$-module, A is generated by $t(\Pi)$.*

Indeed, the $W(\mathbb{F})$-module generated by $t(\Pi)$ is already a $W(\mathbb{F})$-algebra, for it contains $t(1) = 2$, hence 1 since $p > 2$, and it is stable by multiplication: if $x, y \in \Pi$, $t(x)t(y) = t(xy) + d(y)t(xy^{-1})$, and $d(y) \in W(\mathbb{F})$ by (5.2.4).

5.4. (t, d)**-representations attached to an admissible pseudo-deformation and their image.** If $(\Pi, \bar{\rho}, t, d)$ is an admissible pseudo-deformation, then for every $i \in \{1, \dots, r\}$, there exists, by Theorem 2.4.2, a unique up to unique isomorphism A_i-GMA R_i and a (t_i, d_i)-representation $\rho_i : \Pi \to R_i^*$. Let us remind that that means that there exist a faithful GMA $R_i = \begin{pmatrix} A_i & B_i \\ C_i & A_i \end{pmatrix}$ and a representation $\rho_i : \Pi \to \mathrm{GL}_2(A_i)$ of trace t_i and determinant d_i, and that given another GMA R_i' and representation ρ_i' satisfying the same conditions, there exists a unique isomorphism of A-algebras $f : R_i \to R_i'$ such that $f \circ \rho_i = \rho_i'$. We note that by Corollary 5.3.2 and Theorem 2.4.2, the ring A_i is noetherian, the algebra R_i is finite-type as an A_i-module, and when R_i is provided with its natural topology, the representation ρ_i is continuous.

Setting $R = \prod_{i=1}^r R_i$ and seeing this ring as an $A = \prod_{i=1}^r A_i$-algebra (component-wise), we get a continuous representation $\rho : \Pi \to R^*$ of trace t and determinant d which is unique up to unique isomorphism. We call this representation a (t, d)-representation.

Given such a representation ρ, we set

(5.4.1) $G = \rho(\Pi)$

(5.4.2) $\Gamma = G \cap SR^1$,

where SR^1 is defined as in §4.2. Note that G is a closed subgroup of R^* and Γ a closed subgroup of SR^1.

We denote by $\overline{G}$ the image of G by the map $R^* \to (R/\mathrm{rad}R)^*$

Lemma 5.4.1. *The sequence*

(5.4.3) $1 \to \Gamma \to G \to \overline{G} \to 1$

is exact. In particular, Γ is a finite index normal subgroup in G.

Proof — Though Γ is defined as $G \cap SR^1$, we claim that $\Gamma = G \cap R^1$. Indeed, let $g \in G \cap R^1$ and write $g = \rho(x)$ for $x \in \Pi$. Then $\det g = s(\overline{\det(g)})$ by (5.2.4). Since $g \in R^1$, $\det g \in 1 + \mathfrak{m} \subset A^*$ and $\overline{\det(g)} = 1$. Thus $\det(g) = s(1) = 1$ and $g \in \Gamma$.

Since the kernel of $G \to \overline{G}$ is $G \cap R^1$, the result follows. □

We also define

(5.4.4) $G_i = \rho_i(\Pi)$

The group G_i is the image of G by the map $R^* \to R_i^*$. The surjective maps $G \to G_i$ for $i = 1, \dots, r$ define a map $G \to \prod_{i=1}^r G_i$ which is always injective, but not necessarily surjective.

We observe that the choice of a representation ρ_i specifies a single representation $\tilde{\rho}_i : \Pi \to \mathrm{GL}_2(\mathbb{F})$ in the isomorphism class $\bar{\rho}_i$, as follows: consider the composition $\tilde{\rho}_i : \Pi \xrightarrow{\rho} R_i^* \to (R_i/\mathrm{rad}R_i)^*$. We know that $R_i/\mathrm{rad}R_i$ is $M_2(\mathbb{F})$ if $\bar{\rho}_i$ is absolutely irreducible and $\begin{pmatrix} \mathbb{F} & 0 \\ 0 & \mathbb{F} \end{pmatrix}$ otherwise, so $\tilde{\rho}_i$ can be considered in both cases as a semi-simple representation of G. The trace and determinant of $\tilde{\rho}_i$ are reduction mod $\mathfrak{m}_i$ of those of ρ_i, hence are identical to those of $\bar{\rho}_i$. Therefore, $\tilde{\rho}_i$ is a representation in the equivalence class $\bar{\rho}_i$. By a slight abuse of notations, when a representation ρ_i is fixed, we shall denote by $\bar{\rho}_i$ its reduction $\tilde{\rho}_i$.

6. Lie-theoretic study of admissible pseudo-deformations

6.1. **Hypothesis on the base ring A.** In this section, we let $\mathbb{F}$ be a finite field of characteristic $p > 2$, and we consider

(6.1.1) *A topological ring A which is compact and local, with residue field $\mathbb{F}$.*

Such a ring A is automatically a topological $W(\mathbb{F})$-algebra, and the map $W(\mathbb{F}) \to A \to A/\mathfrak{m} = \mathbb{F}$ is the residue map of $W(\mathbb{F})$, hence surjective. Hence our hypothesis implies (5.1.1), and actually is equivalent to it combined with the supplementary assertion that A is local (and $p > 2$).

Our aim is to study the image G of ρ, with a special attention to its subgroup Γ. The group G depends on the chosen (t,d)-representation $\rho : \Pi \to R^*$, but only up to unique isomorphism. We can choose to work with any (t,d)-representation $\rho : \Pi \to R^*$ that simplifies our analysis. According to (5.2.2), there is an element $g_0 \in \Pi$ such that $\bar{\rho}(g_0)$ has two distinct eigenvalues in $\mathbb{F}$, λ_0 and μ_0. Actually, there are in general many of them. Given such an element g_0 as well as an ordering (λ_0, μ_0) of the eigenvalues of $\bar{\rho}(g_0)$, there exists a (t,d)-representation $\rho : \Pi \to R^*$ adapted to (g_0, λ_0, μ_0). Let us remind that that means that $\rho(g_0)$ is a diagonal matrix which reduces modulo $\mathfrak{m}$ to $\begin{pmatrix} \lambda_0 & 0 \\ 0 & \mu_0 \end{pmatrix}$. We shall see that working with (t,d)-representations ρ which are adapted to a well-chosen element g_0 is often the right choice.

In order to study the group G, and its subgroup Γ, we shall make use of the generalization of Pink's theory exposed in the preceding section. Note that the GMA R is Cayley-Hamilton, since it is faithful, and that Γ is a closed subgroup of SR^1, so this theory applies and attaches to Γ a Lie subring $L = L(\Gamma)$ of $(\mathrm{rad}R)^0$. To L is attached a pseusoring $P = \mathrm{tr}\,(L^2)$ such that $PL \subset L$, and the full descending central sequence $L_1 = L$, $L_2 = [L, L]$, etc.

6.2. **Finding constant elements in G.** Given a faithful GMA R over A, the multiplicative section $s : \mathbb{F} \to A$ induces a set-theoretic section of the map $R \to R/\mathrm{rad}R$. This section, still denoted by $s : R/\mathrm{rad}R \to R$, sends a matrix $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ to $\left(\begin{smallmatrix} s(a) & s(b) \\ s(c) & s(d) \end{smallmatrix}\right)$ in the case $R = M_2(A)$ and $\left(\begin{smallmatrix} a & 0 \\ 0 & d \end{smallmatrix}\right)$ to $\left(\begin{smallmatrix} s(a) & 0 \\ 0 & s(d) \end{smallmatrix}\right)$ in the case $R = \begin{pmatrix} A & B \\ C & D \end{pmatrix}$ with $BC \subset \mathfrak{m}$. We shall call a matrix of R which lies in $s(R/\mathrm{rad}R)$ *constant*.

Note that the section s is multiplicative in the second case, but is not in the first, because multiplications of matrices involve addition of the coefficients in general, and s does not preserve addition. However, when m, m' are two matrices in $R/\mathrm{rad}R$ which are either diagonal or anti-diagonal, then $s(mm') = s(m)s(m')$ because in this case the multiplication of matrices only involve multiplication of the coefficients.

We consider again in this subsection an admissible pseudo-deformation $(\Pi, \bar{\rho}, t, d)$ over A. Given a (t,d)-representation $\rho : \Pi \to R^*$, we recall that by definition $G = \rho(\Pi)$, and $\Gamma = G \cap SR^1$.

Our aim is to find elements of the image G that are constant. It is important to observe that **the notion of constant element of G depends on the chosen (t,d)-representation ρ.** Therefore, our aim is, more precisely stated, for a given admissible pseudo-deformation $(\Pi, \bar{\rho}, t, d)$ to find a suitable (t,d)-representation $\rho : \Pi \to R^*$ such that the associated group G has enough constant elements.

Theorem 6.2.1. *Let g_0 be such that $\bar{\rho}(g_0)$ has distinct eigenvalues λ_0, μ_0 in $\mathbb{F}$, and let $\rho : \Pi \to R^*$ be any (t,d)-representation adapted to (g_0, λ_0, μ_0). Let D be the subgroup of $\overline{G}$ generated by $\bar{\rho}(g_0)$ and by the scalar matrices in $\overline{G}$. Then $s(D) \subset G$.*

Furthermore, let $n \in N(D) - Z(D)$, where $N(D)$ is the normalizer and $Z(D)$ is the centralizer of D in $\bar{G}$. Then, up to changing ρ into another (t,d)-representation adapted to (g_0, λ_0, μ_0), one has $s(n) \in G$. As a consequence, if $D = Z(D)$ then $s(N(D)) \subset G$.

Proof — By assumption $\rho(g_0)$ is diagonal and reduces modulo $\mathrm{rad}R$ to $\bar{\rho}(g_0) = \begin{pmatrix} \lambda_0 & 0 \\ 0 & \mu_0 \end{pmatrix}$. Let us write $\rho(g_0) = s(\bar{\rho}(g_0)) + m$ with $m \in \mathrm{rad}R$ a diagonal matrix.

Since $s(\bar{\rho}(g_0))$ and m commute, being two diagonal matrices, we get for every integer $n \geq 1$ (denoting by q the cardinality of $\mathbb{F}$):

$$\rho(g_0^{q^n}) = s(\bar{\rho}(g_0)^{q^n}) + \sum_{k=1}^{q^n} \binom{q^n}{k} s(\bar{\rho}(g_0)^{q^n-k}) m^k.$$

Denoting by v_p the p-valuation of an integer, one has $v_p\left(\binom{q^n}{k}\right) = nv_p(q) - v_p(k)$ if $k \geq 1$, as is well-known. The matrix m^k is diagonal with coefficients in $\mathfrak{m}^k$, and $s(\bar{\rho}(g_0)^{q^n-k})$ is diagonal with coefficients in A. Therefore, since $p \in \mathfrak{m}$, the term $\binom{q^n}{k} s(\bar{\rho}(g_0)^{q^n-k}) m^k$ for $k \geq 1$ is a diagonal matrix whose coefficients belong to $\mathfrak{m}^{nv_p(q)-v_p(k)+k}$, hence to $\mathfrak{m}^{nv_p(q)+1}$.

On the other hand, since $\bar{\rho}(g_0)$ is a diagonal matrix in $\mathrm{GL}_2(\mathbb{F})$, its order divides $q-1$, hence $\bar{\rho}(g_0)^q = \bar{\rho}(g_0)$ and $\bar{\rho}(g_0)^{q^n} = \bar{\rho}(g_0)$.

Therefore

$$\rho(g_0^{q^n}) \equiv s(\bar{\rho}(g_0)) \pmod{\mathfrak{m}^{nv_p(q)+1}}$$

Since $\rho(g_0^{q^n})$ belongs to G by definition, and $nv_p(q)+1$ tends to $+\infty$, we see that $s(\bar{\rho}(g_0))$ is the limit of a sequence of elements of G. Since G is closed,

$$s(\bar{\rho}(g_0)) \in G.$$

Let $h \in \Pi$ such that $\bar{\rho}(h)$ is a scalar matrix. Then we can write $\rho(h) = s(\bar{\rho}(h)) + m$ with $m \in \mathrm{rad}R$ a matrix commuting with $s(\bar{\rho}(h))$ (since $s(\bar{\rho}(h))$ is a scalar matrix in R). The

same argument as above then shows that $s(\bar{\rho}(h)) \in G$. Since D is generated by $\bar{\rho}(g_0)$ and the scalar matrices in D, and $s_{|D}$ is a morphism of groups, we have $s(D) \subset G$. This proves the first assertion of the theorem.

Now let N be the normalizer of D in $\bar{G}$, and Z its centralizer. If $N = Z$ there is nothing else to prove. If $N \neq Z$, then there is an anti-diagonal element in N, which shows that $\bar{\rho}$ is irreducible and we are in the case $R = M_2(A)$. It is easy to see that $|N| = 2|Z|$. Since Z consists of diagonal matrices, $|Z|$ divides $(q-1)^2$, and the order $|N|$ is prime to p. Considering the exact sequence $1 \to \Gamma \to G \to \overline{G} \to 1$, and the fact that Γ is a pro-p-group, we see by Zassenhaus' theorem that there is a map $s' : N \to G$ which is a section of $G \to \overline{G}$ over $N \subset \overline{G}$. The restriction of s' to D is a section over D of $G \to \overline{G}$. Since $|D|$ is prime to p, such a section is unique up to conjugation (again by Zassenhaus' theorem) by an element g of G. Replacing s' by $gs'g^{-1}$ we may assume that the section s' on N restricts to the section s on D.

Let us choose $n \in N - Z$. The element n normalizes D and therefore $s'(n)$ normalizes $s'(D) = s(D)$, which is a non-scalar diagonal subgroup of R^*. Therefore $s'(n)$ is either diagonal or anti-diagonal. If it was diagonal, then it would commute with $s(D)$, hence n would commute with D and be in Z, a contradiction. Therefore $s'(n)$ is anti-diagonal, say $s'(n) = \left(\begin{smallmatrix} 0 & b \\ c & 0 \end{smallmatrix}\right)$. Since $n^2 \in D$, $s'(n^2) = \left(\begin{smallmatrix} bc & 0 \\ 0 & bc \end{smallmatrix}\right)$ is in $s(D)$ and therefore $bc \in s(\mathbb{F})$. By conjugating ρ by the matrix $\left(\begin{smallmatrix} b & 0 \\ 0 & 1 \end{smallmatrix}\right)$, we may assume that $b = 1$ (with ρ still a (t,d)-representation adapted to g_0.) Thus $c \in s(\mathbb{F})$, and therefore $s'(n) = s(n)$. It follows that $s(n) \in G$, as claimed. □

Let us note two important consequences:

Corollary 6.2.2. *Let g_0 be such that $\bar{\rho}(g_0)$ has distinct eigenvalues λ_0, μ_0 in $\mathbb{F}$ and let ρ be adapted to (g_0, λ_0, μ_0), and let G, Γ, L be defined using this ρ. Then L is decomposable.*

Proof — Let us denote by $u : R \to R$ the *conjugation by* $s(\bar{\rho}(g_0))$, that is the map $m \to s(\bar{\rho}(g_0))ms(\bar{\rho}(g_0))^{-1}$. The map u is a $W(\mathbb{F})$-linear endomorphism of R. By the theorem $s(\bar{\rho}(g_0)) = \left(\begin{smallmatrix} s(\lambda_0) & 0 \\ 0 & s(\mu_0) \end{smallmatrix}\right)$ is in G, and therefore normalizes Γ, hence L. In other words, u stabilizes the additive subgroup L of R.

In order to simplify notation, let us set $r := s(\lambda_0/\mu_0) \in W(\mathbb{F})$. Clearly, u fixes diagonal matrices in R, and acts by multiplication by r (resp. r^{-1}) on matrices of the form $\left(\begin{smallmatrix} 0 & b \\ 0 & 0 \end{smallmatrix}\right)$ (resp. $\left(\begin{smallmatrix} 0 & 0 \\ c & 0 \end{smallmatrix}\right)$). It follows that u is killed by the polynomial $X(X-r)(X-r^{-1})$. If $\Sigma = \mathrm{Gal}(\mathbb{F}/\mathbb{F}_p) = \mathrm{Aut}_{\mathbb{Z}_p} W(\mathbb{F})$, then the polynomial $XQ(X)$ also kills u, with $Q(X) = \prod_{\sigma\in\Sigma}(X - \sigma(r))(X - \sigma(r)^{-1}) \in \mathbb{Z}_p[X]$. Since by assumption, $r \neq 1$, the value $Q(1)$ is invertible in $\mathbb{Z}_p$ and the operator $Q(u)/Q(1)$ of R is the projection onto diagonal matrices relatively to antidiagonal matrices. This operator, being in $\mathbb{Z}_p[u]$, stabilizes L, which shows that if a matrix is in L, its diagonal part is also in L. □

Corollary 6.2.3. *Let ρ be adapted to an element (g_0, λ_0, μ_0) as above, and let G, Γ, L defined using this ρ. Let $\mathbb{F}_q$ be a subfield of $\mathbb{F}$, and assume that there exists an integer n such*

that $\lambda_0^n/\mu_0^n \in \mathbb{F}_q^* - \{1,-1\}$. *Then* $W(\mathbb{F}_q)L$ *is strongly decomposable. More precisely,* L *is decomposable, and with* I_1, B_1, C_1 *as in §4.9.1, one has* $W(\mathbb{F}_q)L = \begin{pmatrix} W(\mathbb{F}_q)I_1 & W(\mathbb{F}_q)B_1 \\ W(\mathbb{F}_q)C_1 & W(\mathbb{F}_q)I_1 \end{pmatrix}^0$

Proof — We already know that L, hence $W(\mathbb{F}_q)L$, is decomposable. Using the notation of the previous proof, the hypothesis becomes $r^n \in s(\mathbb{F}_q^* - \{1,-1\})$ and it follows that $r^n - r^{-n}$ is invertible in $W(\mathbb{F}_q)$. The operator $(u^n - r^n)/(r^{-n} - r^n)$ acts on anti-diagonal matrices of R as the map $\left(\begin{smallmatrix} 0 & b \\ c & 0 \end{smallmatrix}\right) \mapsto \left(\begin{smallmatrix} 0 & 0 \\ c & 0 \end{smallmatrix}\right)$, and this operator stabilizes $W(\mathbb{F}_q)\nabla$. The result follows. □

6.3. **Consequences of Theorem 6.2.1 in the cases of cyclic or dihedral projective image of $\bar\rho$.**

6.3.1. *Well-adapted* (t,d)*-representations and splitting of the exact sequence* (5.4.3). We still consider an admissible pseudo-deformation $(\Pi, \bar\rho, t, d)$. In the cases $\bar\rho$ of abelian or dihedral projective image, we shall use the following terminology:

Definition 6.3.1. A (t,d)-representation ρ is said to be *well adapted* if

(i) The representation ρ is adapted to an element $g_0 \in \Pi$ such that $\bar\rho(g_0)$ together with the scalar matrices in $\overline{G}$ generate $\overline{G}$ in the cyclic case, and a subgroup of index 2 in $\overline{G}$ in the dihedral case.
(ii) $s(\overline{G}) \subset G$.
(iii) If $\overline{G}$ is non-abelian, then it contains a matrix of the form $\left(\begin{smallmatrix} 0 & b \\ c & 0 \end{smallmatrix}\right)$ with $bc^{-1} \in \mathbb{F}_p^*$.

Note that in the abelian case, (ii) follows from (i) by Theorem 6.2.1 and (iii) is empty.

Proposition 6.3.2. *Assume that the projective image of* $\bar\rho$ *is either cyclic or dihedral. Then there exists a* (t,d)*-representation* ρ *that is well adapted. Moreover, for such a* ρ *the restriction of* s *to* $\overline{G}$ *is a group-theoretic section of that exact sequence, and* G *is therefore the semi-direct product of* Γ *by* $\overline{G}$*, acting on* Γ *by* $g \cdot \gamma = s(g)\gamma s(g)^{-1}$.

Proof — Let D be the group $\overline{G}$ if $\bar\rho$ is reducible, and D be a subgroup of index 2 in $\overline{G}$ containing all scalar matrices if $\bar\rho$ is dihedral. In both cases, one has $D = Z(D)$ and D is diagonal in a certain basis, which implies that D modulo its subgroup of scalar matrices is cyclic, say generated by $\bar\rho(g_0)$. By (5.2.2), $\bar\rho(g_0)$ is not scalar, and thus has two distinct eigenvalues (λ_0, μ_0). Let us choose for ρ a (t,d)-representation adapted to (g_0, λ_0, μ_0) and, in the case $\bar\rho$ dihedral, chosen as to satisfy the second paragraph of Prop. 6.2.1. Then by Prop. 6.2.1, one has $s(N(D)) \subset G$ and since $N(D) = \overline{G}$, we see that s is a section of $1 \to \Gamma \to G \to \overline{G} \to 1$. Moreover ρ satisfies (i) and (ii) of the definition of a well adapted representation. Since $\overline{G}$ normalizes D but is not abelian, it must contain a matrix of the form $\left(\begin{smallmatrix} 0 & b \\ c & 0 \end{smallmatrix}\right)$. Up to conjugating $\overline{G}$ by $\left(\begin{smallmatrix} 1 & 0 \\ 0 & x \end{smallmatrix}\right)$, it contains the matrix $\left(\begin{smallmatrix} 0 & bx \\ cx^{-1} & 0 \end{smallmatrix}\right)$. One can choose $x \in \mathbb{F}^*$ such that $(bx)(cx^{-1})^{-1} = bc^{-1}x^2$ be in $\mathbb{F}_p^*$. Thus, conjugating ρ by $s\left(\left(\begin{smallmatrix} 1 & 0 \\ 0 & x \end{smallmatrix}\right)\right)$ doesn't affect properties (i) and (ii) and ensure property (iii). □

Corollary 6.3.3. *Assume that the projective image of $\bar\rho$ is either cyclic or dihedral. Then the exact sequence $1 \to \Gamma \to G \to \overline{G} \to 1$ is split.*

Note that a for well adapted ρ, the corresponding Lie Algebra L is decomposable (Cor. 6.2.2) and can be written $L = I_1 J \oplus \nabla$.

6.3.2. *Consequences in the cyclic case.*

Corollary 6.3.4. *Assume that the projective image of $\bar\rho$ is cyclic. Let ρ be a well adapted (t,d)-representation. Then one has (with the notation of §4.9.1)*

(6.3.1) $W(\mathbb{F})1 + W(\mathbb{F})I_1 + W(\mathbb{F})I_1^2 + W(\mathbb{F})\mathrm{tr}\,(\nabla^2) = A$.

(6.3.2) *The A-module generated by B_1 is B.*

(6.3.3) *The A-module generated by C_1 is C.*

Proof — By (5.3.1), $W(\mathbb{F})\mathrm{tr}\,(G) = A$. By Prop. 6.3.2, every element g in G can be written $g = \gamma \left(\begin{smallmatrix} \lambda_1 & 0 \\ 0 & \lambda_2 \end{smallmatrix}\right)$ with $\lambda_1, \lambda_2 \in s(\mathbb{F}^*) \subset W(\mathbb{F})$ and $\gamma \in \Gamma$. We can write $\gamma = \theta^{-1}\left(\left(\begin{smallmatrix} a & b \\ c & -a \end{smallmatrix}\right)\right)$, with $\left(\begin{smallmatrix} a & b \\ c & -a \end{smallmatrix}\right) \in L$. We have $\mathrm{tr}\, g = (\lambda_1 - \lambda_2)a + (\lambda_1 + \lambda_2)\sqrt{1 + a^2 + bc}$; the first term on the RHS is in $W(\mathbb{F})I_1$, and the second in $W(\mathbb{F})1 + W(\mathbb{F})P = W(\mathbb{F})1 + W(\mathbb{F})I_1^2 + W(\mathbb{F})\mathrm{tr}\,(\nabla^2)$ by Lemma 4.9.1. The first result follows.

For the second and third, if $g \in G$ is written $g = \gamma \left(\begin{smallmatrix} \lambda_1 & 0 \\ 0 & \lambda_2 \end{smallmatrix}\right)$ as above, then the anti-diagonal part of g is $\left(\begin{smallmatrix} 0 & \lambda_2 b \\ \lambda_1 c & 0 \end{smallmatrix}\right)$ which belongs to $\left(\begin{smallmatrix} 0 & W(\mathbb{F})B_1 \\ W(\mathbb{F})C_1 & 0 \end{smallmatrix}\right)$. Recalling that G generates R as an A-module, we get $AB_1 = B$ and $AC_1 = C$. □

6.3.3. *Consequences in the dihedral case.* We now make some general observations concerning the case where the projective image of $\bar\rho$ is dihedral. In this case, choosing a well adapted (t,d)-representation ρ defines an abelian subgroup of index 2 in $\overline{G}$, namely the subgroup D generated by $\bar\rho(g_0)$ and the scalar matrices in $\overline{G}$. When the projective image of $\bar\rho$ has order > 4, then this group D is the unique abelian subgroup of index 2 in $\overline{G}$, hence is independent of the choice of ρ, but when $\overline{G} = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, there are three possible index 2 subgroups D in $\overline{G}$, and each of them is associated with a well-adapted (t,d)-representation ρ.

In any case, we fix a well-adapted ρ, which fixes a cyclic subgroup D of index 2 in $\overline{G}$, and we define Π' as the inverse image of D by the map $\Pi \to \overline{G}$. Hence Π' is a subgroup of index 2 of Π. The image $G' = \rho(\Pi')$ lies in an exact sequence $1 \to \Gamma \to G' \to D \to 1$, and is exact sequence is split, a splitting being the restriction of s to D.

By Lemma 2.4.5, the sub-A-module $R' = AG'$ of R is a sub-A-GMA of $R = M_2(A)$, that is of the form $\begin{pmatrix} A & B \\ C & A \end{pmatrix}$ with B, C ideals of A. Since G contains anti-diagonal matrices with coefficients in $s(\mathbb{F}^*) \subset A^*$, and normalizes AG', one has $B = C$, and $R' = \begin{pmatrix} A & B \\ B & A \end{pmatrix}$. It is not hard to see that the ideal B depends only of the admissible pseudo-representation $(\Pi, \bar\rho, t, d)$ and the subgroup D of G', not on the choice of the well-adapted (t,d)-representation ρ: see e.g. Prop. 11.3.2 below.

We write as usual $L = I_1 J \oplus \nabla$, and B_1, C_1 for the subgroups of upper-right and lower-left coefficients of ∇; since elements in Γ have upper-right and lower-left coefficients in B, and Θ does not affect non-diagonal coefficients, we have $B_1 \subset B$, $C_1 \subset B$.

Corollary 6.3.5. *If $\bar\rho$ is dihedral, and ρ is a well adapted (t,d)-representation, then:*

(6.3.4) *There exists $\lambda \in s(\mathbb{F}_p^*)$ such that the subgroup ∇ of $\begin{pmatrix} 0 & B \\ B & 0 \end{pmatrix}$ is stable by the map $\left(\begin{smallmatrix} 0 & b \\ c & 0 \end{smallmatrix}\right) \mapsto \left(\begin{smallmatrix} 0 & \lambda c \\ \lambda^{-1} b & 0 \end{smallmatrix}\right)$. In particular $B_1 = C_1$.*

(6.3.5) *One has $W(\mathbb{F})1 + W(\mathbb{F})I_1 + W(\mathbb{F})I_1^2 + W(\mathbb{F})\mathrm{tr}\,(\nabla^2) + W(\mathbb{F})B_1 = A$.*

(6.3.6) *The A-module generated by B_1 is B.*

Proof — By definition of a well adapted representation, the group G contains a matrix $\left(\begin{smallmatrix} 0 & s(\beta) \\ s(\gamma) & 0 \end{smallmatrix}\right)$ with $s(\beta\gamma^{-1}) \in \mathbb{F}_p^*$. The conjugation by that matrix stabilizes Γ, L, and ∇, and is given by $\left(\begin{smallmatrix} 0 & b \\ c & 0 \end{smallmatrix}\right) \mapsto \left(\begin{smallmatrix} 0 & \lambda c \\ \lambda^{-1} b & 0 \end{smallmatrix}\right)$ with $\lambda = s(\beta\gamma^{-1})$. The first part of (6.3.4) follows and we have $C_1 = \lambda^2 B_1$. Since B_1 is a $\mathbb{Z}_p$-module, and $\lambda \in \mathbb{Z}_p^*$, one gets $C_1 = B_1$.

By (5.2.5), $W(\mathbb{F})\mathrm{tr}\,(G) = A$. Every element g in G can be written either $g = \gamma \left(\begin{smallmatrix} \lambda_1 & 0 \\ 0 & \lambda_2 \end{smallmatrix}\right)$ or $g = \gamma \left(\begin{smallmatrix} 0 & \lambda_1 \\ \lambda_2 & 0 \end{smallmatrix}\right)$ with $\lambda_1, \lambda_2 \in s(\mathbb{F}^*) \subset W(\mathbb{F})$. We can write $\gamma = \theta^{-1} \left(\begin{smallmatrix} a & b \\ c & -a \end{smallmatrix}\right)$, with $\left(\begin{smallmatrix} a & b \\ c & -a \end{smallmatrix}\right) \in L$. In the first case, we have $\mathrm{tr}\, g = (\lambda_1 - \lambda_2)a + (\lambda_1 + \lambda_2)\sqrt{1 + a^2 + bc}$; the first term on the RHS is in $W(\mathbb{F})I_1$, and the second in $W(\mathbb{F})1 + W(\mathbb{F})P = W(\mathbb{F})1 + W(\mathbb{F})I_1^2 + W(\mathbb{F})\mathrm{tr}\,(\nabla^2)$. In the second case, we have $\mathrm{tr}\,(g) = \lambda_2 b + \lambda_1 c \in W(\mathbb{F})B_1$. Formula (6.3.5) follows.

Finally, any $g \in G'$ can be written $g = \gamma \left(\begin{smallmatrix} \lambda_1 & 0 \\ 0 & \lambda_2 \end{smallmatrix}\right)$ as above, and the anti-diagonal part of g is $\left(\begin{smallmatrix} 0 & \lambda_1 b \\ \lambda_2 c & 0 \end{smallmatrix}\right)$ which belongs to $\begin{pmatrix} 0 & AB_1 \\ AB_1 & 0 \end{pmatrix}$. Recalling that by definition G' generates $\begin{pmatrix} A & B \\ B & A \end{pmatrix}$ as an A-module, we get $AB_1 = B$. □

6.4. **The structure of L when the projective image of $\bar\rho$ has order 2.** That is, we consider the case where $\bar\rho = \chi_1 \oplus \chi_2$ is reducible, with $\chi_1^2 = \chi_2^2$ (but still $\chi_1 \neq \chi_2$ by (5.2.2)). In this case, there is nothing more to say than what we have already said:

Theorem 6.4.1. *Let $(\Pi, \bar\rho, d, t)$ be an admissible pseudo-deformation such that the projective image of $\bar\rho$ has order 2 and let $\rho : \Pi \to R^*$, $R = \begin{pmatrix} A & B \\ C & A \end{pmatrix}$ a well adapted (t,d)-representation. Then there exists a closed subgroup I_1 of $\mathfrak{m}$, and a closed subgroup ∇ of $\begin{pmatrix} 0 & B \\ C & 0 \end{pmatrix}$ such that*

$$L = I_1 J \oplus \nabla$$

and

(6.4.1) $[\nabla, \nabla] \subset I_1 J$,

(6.4.2) $I_1[J, \nabla] \subset \nabla$,

(6.4.3) $\mathrm{tr}\,(\nabla^2) I_1 \subset I_1$,

(6.4.4) $\mathrm{tr}\,(\nabla^2)\nabla \subset \nabla$,

(6.4.5) $I_1^3 \subset I_1$,

(6.4.6) $W(\mathbb{F})1 + W(\mathbb{F})I_1 + W(\mathbb{F})I_1^2 + W(\mathbb{F})\mathrm{tr}\,(\nabla^2) = A$

(6.4.7) $AB_1 = B$.

(6.4.8) $AC_1 = C$.

Conversely, if $R = \begin{pmatrix} A & B \\ C & A \end{pmatrix}$ *is a faithful GMA over* A, I_1 *is any closed subgroup of* $\mathfrak{m}$, *and* ∇ *any closed subgroup of* $\begin{pmatrix} 0 & B \\ C & 0 \end{pmatrix}$ *satisfying the eight conditions above, then there exists an admissible pseudo-deformation* $(\Pi, \bar\rho, t, d)$ *with* $\bar\rho$ *of projective image of order* 2, *and a* (t,d)*-representation* $\rho : \Pi \to R^*$ *such that the Lie algebra attached to* ρ *is* $L = I_1 J \oplus \nabla$.

Proof — For the direct sense, if ρ is well adapted, and G, Γ, L attached to ρ, then L is decomposable by Corollary 6.2.2, so $L = I_1 J \oplus \nabla$ and since L is the Lie algebra of Γ, it satisfies the first five given conditions by Prop. 4.9.2. Moreover L satisfies the last three conditions by Corollary 6.3.4.

Conversely, if $L = I_1 J \oplus \nabla$ with I_1 and ∇ satisfying the eight conditions above, then by (6.4.1) to (6.4.5) and Prop. 4.9.2, L is a Lie subring of $(\mathrm{rad}R)^0$ and $\Gamma := \Theta^{-1}(L)$ is a closed subgroup of SR^1 whose Lie algebra is L. Let $\overline{G}$ be the diagonal subgroup $\{1, J\}$ of $\mathrm{GL}_2(\mathbb{F})$. It is clear that the conjugation by the subgroup $s(\overline{G})$ of R^* normalizes L, hence Γ. We can thus form the closed subgroup $G := \Gamma s(\overline{G})$ of R^*, a semi-direct product of $s(\overline{G})$ by Γ. The composition $G \to s(\overline{G}) \simeq \overline{G} \subset \mathrm{GL}_2(\mathbb{F})$ is a representation $\bar\rho : G \to \mathrm{GL}_2(\mathbb{F})$ which is the sum of two distinct characters and whose projective image has order 2.

The restriction (t,d) to G of the maps $(\mathrm{tr}\,, \det)$ on R is a pseudo-representation over G. We claim that $(G, \bar\rho, t, d)$ is an admissible pseudo-deformation. The only condition that is not trivial to check is that the closed $W(\mathbb{F})$-algebra generated by $\mathrm{tr}\,(G)$ is A. Let us call this $W(\mathbb{F})$-subalgebra by $\tilde A$. Since $\mathrm{tr}\,(1) = 2$, $\tilde A$ contains $W(\mathbb{F})1$. Since $\mathrm{tr}\,(\Theta^{-1}(JI_1)J) = I_1$, $\tilde A$ contains $W(\mathbb{F})I_1$. Also $\tilde A$ contains $\mathrm{tr}\,(\Gamma)$, hence it contains the closed sub-pseudoring generated by the elements $\mathrm{tr}\,(\gamma) - 2$, $\gamma \in \Gamma$, that is, it contains P by Cor. 4.5.2. Therefore $\tilde A$ contains $W(\mathbb{F})1 + W(\mathbb{F})I_1 + W(\mathbb{F})P = W(\mathbb{F})1 + W(\mathbb{F})I_1 + W(\mathbb{F})I_1^2 + W(\mathbb{F})\mathrm{tr}\,(\nabla^2)$, which is A by (6.4.6). This concludes the proof of the claim that $(G, \bar\rho, t, d)$ is an admissible pseudo-deformation.

Let us define ρ as the inclusion map $G \hookrightarrow R^*$. Then $\mathrm{tr}\,\rho = t$, $\det\rho = d$. We claim that $A\rho(G) = AG$ is the full algebra R. By Lemma 2.4.5, we know that $A\rho(G) = AG$ is a sub-A-GMA $\begin{pmatrix} A & B' \\ C' & A \end{pmatrix}$ of R, where B' is a sub-A-module of B and C' a sub-A-module of C. By definition, B' contains B_1 and C' contains C_1, so (6.4.7) and (6.4.8) imply that $B' = B$ and $C' = C$, so $AG = R$. It follows that $\rho : G \to R^*$ is a (t,d)-representation. It is clear that the Lie algebra attached to ρ is L, which proves the converse part of the theorem. □

6.5. **The structure of L when the projective image of $\bar\rho$ is cyclic of order > 2.** That is, $\bar\rho = \chi_1 \oplus \chi_2$ with $\chi_1^2 \neq \chi_2^2$. In this case, we shall only determine the structure of the Lie algebra $W(\mathbb{F}_q)L$ where $\mathbb{F}_q$ is a large enough subfield of $\mathbb{F}$.

Theorem 6.5.1. *Let $(\Pi, \bar{\rho}, d, t)$ be an admissible pseudo-deformation such that the projective image of $\bar{\rho}$ is cyclic of order $m > 2$ and let $\rho : \Pi \to R^*$, $R = \begin{pmatrix} A & B \\ C & A \end{pmatrix}$ a well adapted (t,d)-representation. Let $\mathbb{F}_q$ be any subfield of $\mathbb{F}$ such that $\gcd(m, q-1) > 2$ (a condition always satisfied when $\mathbb{F}_q = \mathbb{F}$).*

Then there exists a closed $W(\mathbb{F}_q)$-submodule $\tilde{I}_1$ of $\mathfrak{m}$, and closed $W(\mathbb{F}_q)$-submodules $\tilde{B}_1$ of B and $\tilde{C}_1$ of C such that $W(\mathbb{F}_q)L = \begin{pmatrix} \tilde{I}_1 & \tilde{B}_1 \\ \tilde{C}_1 & \tilde{I}_1 \end{pmatrix}^0$ and

(6.5.1) $\tilde{B}_1\tilde{C}_1 \subset \tilde{I}_1$

(6.5.2) $\tilde{I}_1^3 \subset \tilde{I}_1$,

(6.5.3) $W(\mathbb{F})1 + W(\mathbb{F})\tilde{I}_1 + W(\mathbb{F})\tilde{I}_1^2 = A$

(6.5.4) $W(\mathbb{F})\tilde{B}_1 = B$ *and* $W(\mathbb{F})\tilde{C}_1 = C$.

Conversely, if $\tilde{I}_1$, $\tilde{B}_1$, $\tilde{C}_1$ are $W(\mathbb{F})$-submodules of $\mathfrak{m}$ satisfying those three conditions, and $L = \begin{pmatrix} \tilde{I}_1 & \tilde{B}_1 \\ \tilde{C}_1 & \tilde{I}_1 \end{pmatrix}^0$, then there exists an admissible pseudo-deformation $(\Pi, \bar{\rho}, t, d)$ such that the projective image of $\bar{\rho}$ is cyclic of order > 2 and a (t,d)-representation $\rho : \Pi \to R^*$ such that the Lie algebra attached to ρ is $W(\mathbb{F})L$.

Proof — Let $g_0 \in \Pi$ be such that $\bar{\rho}(g_0)$ generates the group $\overline{G}$ modulo scalar matrices, and let λ_0, μ_0 be the eigenvalues of $\bar{\rho}(g_0)$. Since the group $\overline{G}$ modulo scalar matrices has order > 2, one has $\lambda_0/\mu_0 \neq \pm 1$. By Cor. 6.2.2, L is decomposable, so we can write $L = I_1 J \oplus \nabla$ as usual, and by Cor. 6.2.3 (applied with $n = 1$), $W(\mathbb{F}_q)L$ is even strongly decomposable, and we can write $W(\mathbb{F}_q)L = \begin{pmatrix} W(\mathbb{F}_q)I_1 & W(\mathbb{F}_q)B_1 \\ W(\mathbb{F}_q)C_1 & W(\mathbb{F}_q)I_1 \end{pmatrix}^0$. Let us set $\tilde{I}_1 := W(\mathbb{F}_q)I_1$, $\tilde{B}_1 = W(\mathbb{F}_q)B_1$, $\tilde{C}_1 = W(\mathbb{F}_q)C_1$. By Prop. 4.9.2, one has $[\nabla, \nabla] \subset I_1 J$, which gives after taking the $W(\mathbb{F}_q)$-modules generated by the two terms of that inclusion, $\tilde{B}_1\tilde{C}_1 \subset \tilde{I}_1$; one has $I_1[J, \nabla] \subset \nabla$ which gives similarly $\tilde{I}_1\tilde{B}_1 \subset \tilde{B}_1$, $\tilde{I}_1\tilde{C}_1 \subset \tilde{C}_1$; and $I_1^3 \subset I_1$, which gives $\tilde{I}_1^3 \subset \tilde{I}_1$. By Prop. 6.3.4, $W(\mathbb{F})1 \oplus W(\mathbb{F})I_1 \oplus W(\mathbb{F})I_1^2 \oplus W(\mathbb{F})\tilde{B}_1\tilde{C}_1 = A$, and since $\tilde{B}_1\tilde{C}_1 \subset \tilde{I}_1$, one has simply $W(\mathbb{F})1 \oplus W(\mathbb{F})\tilde{I}_1 \oplus W(\mathbb{F})\tilde{I}_1^2 = A$. Since $W(\mathbb{F})B_1$ is stable by $W(\mathbb{F})\tilde{I}_1$, it is stable by A, i.e. an A-module. But by Prop. 6.3.4, the A-module generated by B_1, or by $W(\mathbb{F})B_1$ is B. Therefore $W(\mathbb{F})B_1 = B$ and similarly $W(\mathbb{F})C_1 = C$. This completes the proof of the direct sense of the theorem.

Conversely, suppose $L = \begin{pmatrix} \tilde{I}_1 & \tilde{B}_1 \\ \tilde{C}_1 & \tilde{I}_1 \end{pmatrix}^0$ satisfying the four given conditions. Then by Prop. 4.9.3, $\Gamma := \Theta^{-1}(L)$ is a closed subgroup of SR^1 of Lie algebra L (note that the condition (4.9.12.2), i.e. $\tilde{I}_1 B \subset B$ and $\tilde{I}_1 C \subset C$, is automatically satisfied since B and C are A-modules). Let $\overline{G}$ be any group of diagonal matrices in $\mathrm{GL}_2(\mathbb{F})$ whose quotient modulo scalar matrices is of order > 2. It is clear that $s(\overline{G})$ normalizes L, hence Γ, and we can form a subgroup $G := \Gamma s(\overline{G})$ of R^*. Then the construction of $\bar{\rho}$, t, d, ρ and the end of the proof of the converse is exactly as in the preceding theorem, so we leave details to the reader. □

6.6. **The structure of L when the projective image of $\bar\rho$ is $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}$.**

Theorem 6.6.1. *Let $(\Pi,\bar\rho,d,t)$ be an admissible pseudo-deformation such that the projective image of $\bar\rho$ is $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}$ and let $\rho:\Pi\to GL_2(A)$ a well adapted (t,d)-representation.*

There exists a closed subgroup I_1 of $\mathfrak{m}$, and a closed subgroup ∇ of $\begin{pmatrix}0&\mathfrak{m}\\ \mathfrak{m}&0\end{pmatrix}$ such that

$$L=I_1J\oplus\nabla$$

and

(6.6.1) $[\nabla,\nabla]\subset I_1J$,

(6.6.2) $I_1[J,\nabla]\subset\nabla$,

(6.6.3) $\mathrm{tr}\,(\nabla^2)I_1\subset I_1$,

(6.6.4) $\mathrm{tr}\,(\nabla^2)\nabla\subset\nabla$,

(6.6.5) $I_1^3\subset I_1$,

(6.6.6) *There exists $\lambda\in s(\mathbb{F}_p^*)$ such that ∇ is invariant by* $\begin{pmatrix}0&b\\ c&0\end{pmatrix}\mapsto\begin{pmatrix}0&\lambda c\\ \lambda^{-1}b&0\end{pmatrix}$

(6.6.7) $W(\mathbb{F})1+W(\mathbb{F})I_1+W(\mathbb{F})I_1^2+W(\mathbb{F})\mathrm{tr}\,(\nabla^2)+W(\mathbb{F})B_1=A$

Conversely, if I_1 is any closed subgroup of $\mathfrak{m}$, and ∇ any closed subgroup of $\begin{pmatrix}0&\mathfrak{m}\\ \mathfrak{m}&0\end{pmatrix}$ satisfying the seven conditions above, then there exists an admissible pseudo-deformation $(\Pi,\bar\rho,t,d)$ with $\bar\rho$ of projective image $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}$, and a (t,d)-representation $\rho:\Pi\to GL_2(A)$ such that the Lie algebra attached to ρ is $L=I_1J\oplus\nabla$.

Proof — For the direct sense, if ρ is well adapted, and G, Γ, L attached to ρ, then L is decomposable by Corollary 6.2.2, so $L=I_1J\oplus\nabla$ and since L is the Lie algebra of Γ, it satisfies conditions (6.6.1) to (6.6.5) by Prop. 4.9.2. Moreover L satisfies conditions (6.6.6) and (6.6.7) by Corollary 6.3.5.

Conversely, if $L=I_1J\oplus\nabla$ with I_1 and ∇ satisfying the seven conditions above, then by Prop. 4.9.2 L is a Lie subring of $\mathcal{M}_2(\mathfrak{m})$ and $\Gamma:=\Theta^{-1}(L)$ is a closed subgroup of SR^1 whose Lie algebra is L. Let $\overline{G}$ be the subgroup of $\mathrm{GL}_2(\mathbb{F})$ containing all matrices of the form $\left(\begin{smallmatrix}x&0\\0&x\end{smallmatrix}\right)$, $\left(\begin{smallmatrix}x&0\\0&-x\end{smallmatrix}\right)$, $\left(\begin{smallmatrix}0&\lambda x\\x&0\end{smallmatrix}\right)$, $\left(\begin{smallmatrix}0&-\lambda x\\0&\end{smallmatrix}\right)$. This is a subgroup of order $4|\mathbb{F}^*|$ which contains the subgroup of scalar matrices $\mathbb{F}^*$ of $\mathrm{GL}_2(\mathbb{F})$, and the quotient $\bar G/\mathbb{F}^*$ is $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}$. The Lie algebra L is stable by conjugation by $s(\overline{G})$ by (6.6.6). Therefore, so is Γ, and we can define a closed subgroup $G:=\Gamma s(\overline{G})$ of $\mathrm{GL}_2(A)$. We thus have a split exact sequence $1\to\Gamma\to G\to\overline{G}\to 1$. We define a representation $\bar\rho:G\to\mathrm{GL}_2(\mathbb{F})$ by composing the natural map $G\to\overline{G}$ with the inclusion $\overline{G}\to\mathrm{GL}_2(\mathbb{F})$. It is clear that $\bar\rho$ has projective image isomorphic to $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}$. We define a pseudo-repreresentation (t,d) on G by restricting the trace and determinant map on $\mathrm{GL}_2(A)$ to G.

We claim that $(G,\bar\rho,t,d)$ is an admissible pseudo-deformation. We just need to check that the closed $W(\mathbb{F})$-algebra $\tilde A$ generated by $t(G)$ is A. Since $\tilde A$ contains $t(\Gamma)$ and $t(J\Gamma)$, we see as in the proof of Theorem 6.5.1 that $\tilde A$ contains $W(\mathbb{F})1+W(\mathbb{F})I_1+W(\mathbb{F})I_1^2+W(\mathbb{F})\mathrm{tr}\,(\nabla^2)$. Moreover $\tilde A$ contains $\mathrm{tr}\,(\left(\begin{smallmatrix}0&\lambda\\1&0\end{smallmatrix}\right)\Gamma)$ and $\mathrm{tr}\,(\left(\begin{smallmatrix}0&-\lambda\\1&0\end{smallmatrix}\right)\Gamma)$. When $\gamma=\left(\begin{smallmatrix}a&b\\c&d\end{smallmatrix}\right)$ runs in $\Gamma=\Theta^{-1}(L)$,

$\left(\begin{smallmatrix} 0 & b \\ c & 0 \end{smallmatrix}\right)$ runs in ∇. Thus for any $\left(\begin{smallmatrix} 0 & b \\ c & 0 \end{smallmatrix}\right) \in \nabla$, tr $\left(\left(\begin{smallmatrix} 0 & \lambda \\ 1 & 0 \end{smallmatrix}\right)\gamma\right) = \lambda c + b$ and tr $\left(\left(\begin{smallmatrix} 0 & -\lambda \\ 1 & 0 \end{smallmatrix}\right)\gamma\right) = -\lambda c + b$ are in $\tilde{A}$, and therefore $b \in \tilde{A}$. Thus $\tilde{A}$ contains $W(\mathbb{F})B_1$ as well. By condition (6.6.7), $\tilde{A} = A$, and this proves the claim.

Let $\rho : G \to \mathrm{GL}_2(A)$ be the inclusion map. The representation ρ is of trace t and determinant d, and $A\rho(G) = M_2(A)$ by Lemma 2.4.5. So ρ is a (t,d)-representation. The image of ρ is G, its intersection with SR^1 is Γ, and the Lie algebra of Γ is L. This proves the converse part of the theorem. □

6.7. The structure of L when the projective image of $\bar{\rho}$ is a non-abelian dihedral group.

Theorem 6.7.1. *Let $(\Pi, \bar{\rho}, d, t)$ be an admissible pseudo-deformation such that the projective image of $\bar{\rho}$ is a non-abelian dihedral group of order $2m > 4$, $\rho : \Pi \to GL_2(A)$ a well adapted (t,d)-representation. Let $\mathbb{F}_q$ be any subfield of $\mathbb{F}$ such that $\gcd(m, q-1) > 2$ (a condition always satisfied when $\mathbb{F}_q = \mathbb{F}$).*

Then there exist closed $W(\mathbb{F}_q)$-submodules $\tilde{I}_1$ and $\tilde{B}_1$ of $\mathfrak{m}$ such that $W(\mathbb{F}_q)L = \begin{pmatrix} \tilde{I}_1 & \tilde{B}_1 \\ \tilde{B}_1 & \tilde{I}_1 \end{pmatrix}^0$ and

(6.7.1) $\tilde{B}_1^2 \subset \tilde{I}_1$

(6.7.2) $\tilde{I}_1\tilde{B}_1 \subset \tilde{B}_1$.

(6.7.3) $\tilde{I}_1^3 \subset \tilde{I}_1$,

(6.7.4) $W(\mathbb{F})1 + W(\mathbb{F})\tilde{I}_1 + W(\mathbb{F})\tilde{I}_1^2 + W(\mathbb{F})\tilde{B}_1 = A$

Conversely, if $\tilde{I}_1$ and $\tilde{B}_1$ are $W(\mathbb{F})$-submodules of $\mathfrak{m}$ satisfying those four conditions, and $L = \begin{pmatrix} \tilde{I}_1 & \tilde{B}_1 \\ \tilde{B}_1 & \tilde{I}_1 \end{pmatrix}^0$, then there exists an admissible pseudo-deformation (Π, t, d, ρ) such that the projective image of $\bar{\rho}$ is dihedral of order > 4 and a (t,d)-representation $\rho : \Pi \to R^*$ such that the Lie algebra attached to ρ is $L = W(\mathbb{F})L$.

Proof — We show as in the proof of Theorem 6.5.1 than $W(\mathbb{F}_q)L$ is strongly decomposable, and we can thus write with the usual notations $W(\mathbb{F}_q)L = W(\mathbb{F}_q)I_1 \oplus \begin{pmatrix} 0 & W(\mathbb{F}_q)B_1 \\ W(\mathbb{F}_q)C_1 & 0 \end{pmatrix}$. By Prop. 6.3.5, $B_1 = C_1$. Thus, setting $\tilde{I}_1 = W(\mathbb{F}_q)I_1$, $\tilde{B}_1 = W(\mathbb{F}_q)B_1$, one has $W(\mathbb{F}_q)L = \begin{pmatrix} \tilde{I}_1 & \tilde{B}_1 \\ \tilde{B}_1 & \tilde{I}_1 \end{pmatrix}^0$. By Prop. 4.9.2, one has $[\nabla, \nabla] \subset I_1 J$, which gives after taking the $W(\mathbb{F}_q)$-modules generated by the two terms of that inclusion, $\tilde{B}_1^2 \subset \tilde{I}_1$; one has $I_1[J, \nabla] \subset \nabla$ which gives similarly $\tilde{I}_1\tilde{B}_1 \subset \tilde{B}_1$, and $I_1^3 \subset I_1$, which gives $\tilde{I}_1^3 \subset \tilde{I}_1$. By Prop. 6.3.4, $W(\mathbb{F})1 + W(\mathbb{F})\tilde{I}_1 + W(\mathbb{F})\tilde{I}_1^2 + W(\mathbb{F})\tilde{B}_1^2\tilde{B}_1 = A$, and since $\tilde{B}_1^2 \subset \tilde{I}_1$, one has more simply $W(\mathbb{F})1 + W(\mathbb{F})\tilde{I}_1 + W(\mathbb{F})\tilde{I}_1^2 + W(\mathbb{F})\tilde{B}_1 = A$. This completes the proof of the direct sense of the theorem.

Conversely, suppose $L = \begin{pmatrix} \tilde{I}_1 & \tilde{B}_1 \\ \tilde{B}_1 & \tilde{I}_1 \end{pmatrix}^0$ satisfying the four given conditions, then by Prop. 4.9.3, $\Gamma := \Theta^{-1}(L)$ is a closed subgroup of SR^1 of Lie algebra L. Let $\overline{G}$ be for instance the group of all diagonal and anti-diagonal matrices in $\mathrm{GL}_2(\mathbb{F})$. It is clear that

$s(\overline{G})$ normalizes L, hence Γ, and we can form a subgroup $G := \Gamma s(\overline{G})$ of R^*. Then the construction of $\bar{\rho}$, t, d, ρ and the end of the proof of the converse is exactly as in the preceding theorem, so we leave details to the reader. □

6.8. **Structure of L in the large and exceptional image case.**

6.8.1. *Results.* This is the simplest case insofar as the description of L is concerned, but the case where the proofs are the hardest.

Theorem 6.8.1. *Let $(\Pi, \bar{\rho}, t, d)$ be an admissible pseudo-deformation. We assume that $\bar{\rho}$ is either of the large image type or of the exceptional type.*

Let $\mathbb{F}_q$ be a subfield of $\mathbb{F}$. If $\bar{\rho}$ is octahedral (resp. tetrahedral, resp. icosahedral), we assume that $\mathbb{F}_q$ contains cubic roots of unity (resp. either cubic or quartic roots of unity, resp. quintic roots of unity). We put no condition on $\mathbb{F}_q$ when $\bar{\rho}$ has large image.

Then there exists a (t,d)-representation ρ, and a closed $W(\mathbb{F}_q)$-submodule $\tilde{I}_1$ of $\mathfrak{m}$ such that

$$W(\mathbb{F}_q)L = \begin{pmatrix} \tilde{I}_1 & \tilde{I}_1 \\ \tilde{I}_1 & \tilde{I}_1 \end{pmatrix}^0,$$

and

(6.8.1) $\tilde{I}_1^2 \subset \tilde{I}_1$.

(6.8.2) $W(\mathbb{F})\tilde{I}_1 = \mathfrak{m}$.

Remark 6.8.2. Note that if we take $\mathbb{F}_q = \mathbb{F}$, and $\mathbb{F}$ large enough as we always do, the hypothesis of the theorem are obviously satisfied. Thus, the theorem describes the structure of $W(\mathbb{F})L$ for $\mathbb{F}$ large enough.

Corollary 6.8.3. *With the same notation as in the above theorem, one has $\Gamma = \Theta^{-1}(L)$. In the case where $\mathbb{F}_q = \mathbb{F}_p$, Γ is precisely the group of matrices $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ in $SL_2(A)$ such that $a \in 1 + \tilde{I}_1$, $b \in \tilde{I}_1$, $c \in \tilde{I}_1$, $d \in 1 + \tilde{I}_1$.*

Proof — This follows from the preceding theorem and Prop. 4.8.2. □

Remark 6.8.4. In the appendix of [20], Boston proves that if G is a closed subgroup of $\mathrm{SL}_2(A)$ such that the image of G in $\mathrm{SL}_2(A/\mathfrak{m}^2)$ is $\mathrm{SL}_2(A/\mathfrak{m}^2)$, then $G = \mathrm{SL}_2(A)$. This results follows easily from our classification result Theorem 6.8.1 (indeed, we are in the large image case so we can take $\mathbb{F}_q = \mathbb{F}_p$, and the hypothesis implies that $\tilde{I}_1$ maps surjectively to $\mathfrak{m}/\mathfrak{m}^2$, thus is $\mathfrak{m}$, which implies $\Gamma = \mathrm{SL}_2^1(A)$ by the corollary and $G = \mathrm{SL}_2(A)$). It does not seem that Boston's method generalizes to the other cases covered by Theorem 6.8.1.

6.8.2. *Proof of Theorem 6.8.1.* We fix $(\Pi, \bar{\rho}, t, d)$ an admissible pseudo-deformation, and we assume that $\bar{\rho}$ is either of the large image type or of the exceptional type. We call Z the subgroup of scalar matrices in $\mathrm{GL}_2(\mathbb{F})$, isomorphic to $\mathbb{F}^*$.

Lemma 6.8.5. *There exists a (t,d)-representation ρ such that:*

- *if $\bar{\rho}$ is octahedral, then $\overline{G} \subset Z GL_2(\mathbb{F}_q)$ and there exists an element $g_0 \in \Pi$ such that $\rho(g_0) = \begin{pmatrix} s(\lambda_0) & 0 \\ 0 & s(\mu_0) \end{pmatrix}$ with $\lambda_0, \mu_0 \in \mathbb{F}^*$, $(\lambda_0/\mu_0)^3 = 1$, $\lambda_0 \neq \mu_0$;*
- *if $\bar{\rho}$ is tetrahedral, then $\overline{G} \subset Z GL_2(\mathbb{F}_q)$ and there exists an element $g_0 \in \Pi$ such that $\rho(g_0) = \begin{pmatrix} s(\lambda_0) & 0 \\ 0 & s(\mu_0) \end{pmatrix}$ with $\lambda_0, \mu_0 \in \mathbb{F}^*$, $(\lambda_0/\mu_0)^3 = 1$ or $(\lambda_0/\mu_0)^4 = 1$, and $\lambda_0^2 \neq \mu_0^2$;*
- *if $\bar{\rho}$ is icosahedral, then $\overline{G} \subset Z GL_2(\mathbb{F}_q)$ and there exists an element $g_0 \in \Pi$ such that $\rho(g_0) = \begin{pmatrix} s(\lambda_0) & 0 \\ 0 & s(\mu_0) \end{pmatrix}$ with $\lambda_0, \mu_0 \in \mathbb{F}^*$, $(\lambda_0/\mu_0)^5 = 1$, $\lambda_0 \neq \mu_0$;*
- *if $\bar{\rho}$ has large image but the projective image of $\bar{\rho}$ is not isomorphic to $PSL_2(\mathbb{F}_3)$ or $PGL_2(\mathbb{F}_3)$, then $SL_2(\mathbb{F}_p) \subset \overline{G}$ and there exists an element $g_0 \in \Pi$ such that $\rho(g_0) = \begin{pmatrix} s(\lambda_0) & 0 \\ 0 & s(\mu_0) \end{pmatrix}$, $\lambda_0^2 \neq \mu_0^2$*

Proof — The image of $\overline{G}$ on $\mathrm{PGL}_2(\mathbb{F})$ contains an element of order 3 in the octahedral case (a 3-cycle in A_4), an element of order 3 and of order 4 in the tetrahedral case (a 3-cycle and a 4-cycle in S_4), an element of order 5 in the icosahedral case (a 5-cycle in A_5), and an element of order > 2 in the large image case. Choosing an element g_0 such that $\bar{\rho}(g_0)$ maps to that element, we can diagonalize $\bar{\rho}(g_0)$ and write $\bar{\rho}(g_0) = \begin{pmatrix} \lambda_0 & 0 \\ 0 & \mu_0 \end{pmatrix}$. Choosing a ρ adapted to (g_0, λ_0, μ_0) ensures that, in each case, the condition regarding $\rho(g_0)$. For such a ρ, $\bar{\rho}(g_0) = \begin{pmatrix} \lambda_0 & 0 \\ 0 & \mu_0 \end{pmatrix}$. On the other hand, we know that in the conjugacy class of $\bar{\rho}$ there is a representation $\bar{\rho}'$ satisfying $\bar{\rho}'(\Pi) \subset Z\mathrm{GL}_2(\mathbb{F}_q)$ in the exceptional cases and $\mathrm{SL}_2(\mathbb{F}_p) \subset \overline{G}$ in the large image case, and $\bar{\rho}'(g_0) = \begin{pmatrix} \lambda_0 & 0 \\ 0 & \mu_0 \end{pmatrix}$. (This is because, in the exceptional case, there is a conjugate of $\bar{\rho}$ whose projective image is defined over $\mathbb{F}_q$, and after a base change over $\mathbb{F}_q$, we may suppose that $\bar{\rho}'(g_0)$ is diagonal). The agreement of $\bar{\rho}$ and $\bar{\rho}'$ on g_0 implies that they are conjugate through a diagonal matrix. Conjugating ρ by a diagonal lift of that diagonal matrix doesn't affect the condition on $\rho(g_0)$ but ensures that $\overline{G} = \rho'(\Pi)$ satisfies the required condition. □

Since in any case the eigenvalues λ_0 and μ_0 of $\bar{\rho}(g_0)$ have distinct squares, Prop. 6.2.3 applies and ensures that $W(\mathbb{F}_q)L$ is strongly decomposable. That is, there exists three $W(\mathbb{F}_q)$-submodules of A, $\tilde{I}_1$, $\tilde{B}_1$ and $\tilde{C}_1$ such that

$$W(\mathbb{F}_q)L = \tilde{I}_1 J \oplus \begin{pmatrix} 0 & \tilde{B}_1 \\ \tilde{C}_1 & 0 \end{pmatrix}.$$

Lemma 6.8.6. *Let $\bar{g} = \begin{pmatrix} \bar{\alpha} & \bar{\beta} \\ \bar{\gamma} & \bar{\delta} \end{pmatrix} \in GL_2(\mathbb{F}_q) \cap (\overline{G}Z)$. Then there exists a lift $g = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in GL_2(A)$ of $\bar{g}$ such that*

(6.8.3) $\alpha^2 \tilde{B}_1 \subset \tilde{B}_1$, $\gamma^2 \tilde{B}_1 \subset \tilde{C}_1$, $\alpha\gamma \tilde{B}_1 \subset \tilde{I}_1$.

(6.8.4) $\beta^2 \tilde{C}_1 \subset \tilde{B}_1$, $\beta\delta \tilde{C}_1 \subset \tilde{I}_1$, $\delta^2 \tilde{C} \subset \tilde{B}_1$.

(6.8.5) $\alpha\beta\tilde{I}_1 \subset \tilde{B}_1$, $\gamma\delta\tilde{I}_1 \subset \tilde{C}_1$.

Proof — By hypothesis $\bar{g} = \bar{g}_1\bar{z}$ with $\bar{g}_1 \in G$ and $\bar{z}$ a scalar matrix in $\mathbb{F}^*$. Let g_1 be any lift of $\bar{g}_1$ in G, $z = s(\bar{z})$ which is a scalar matrix lifting $\bar{z}$, and set $g = g_1 z \in \mathrm{GL}_2(A)$ which is a lift of $\bar{g}$. Then $gLg^{-1} = g_1 L g_1^{-1} = L$ since z is scalar and $g_1 \in G$. Moreover, if $g = \left(\begin{smallmatrix} \alpha & \beta \\ \gamma & \delta \end{smallmatrix}\right)$, set $g' = \left(\begin{smallmatrix} \delta & -\beta \\ -\gamma & \alpha \end{smallmatrix}\right) = g^{-1}\det(g)$. Note that $\det(g) = \det(g_1)\det(z) = s(\det(\bar{g}_1))s(\det(\bar{z}))$ by (5.2.4), so $\det(g) = s(\det\bar{g}) \in W(\mathbb{F}_q)^*$. Then $gW(\mathbb{F}_q)Lg' = gW(\mathbb{F}_q)Lg^{-1} = W(\mathbb{F}_q)L$ since multiplication by $\det(g)^{-1}$ stabilizes $W(\mathbb{F}_q)L$.

The first line of the lemma then follows from the computation $g\left(\begin{smallmatrix} 0 & 1 \\ 0 & 0 \end{smallmatrix}\right)g' = \left(\begin{smallmatrix} -\alpha\gamma & \alpha^2 \\ -\gamma^2 & \alpha\gamma \end{smallmatrix}\right)$, the second line from $g\left(\begin{smallmatrix} 0 & 0 \\ 1 & 0 \end{smallmatrix}\right)g' = \left(\begin{smallmatrix} \beta\delta & -\beta^2 \\ \delta^2 & -\beta\delta \end{smallmatrix}\right)$, and the last line from $gJg^{-1} = \left(\begin{smallmatrix} * & -2\alpha\beta \\ -2\gamma\delta & * \end{smallmatrix}\right)$. □

Lemma 6.8.7. *There exists an element* $\bar{g} = \left(\begin{smallmatrix} \bar{\alpha} & \bar{\beta} \\ \bar{\gamma} & \bar{\delta} \end{smallmatrix}\right) \in GL_2(\mathbb{F}_q) \cap (\overline{G}Z)$ *such that* $\bar{\alpha}\bar{\beta} \neq 0$ *(resp.* $\bar{\alpha}\bar{\gamma} \neq 0$*, resp.* $\bar{\beta}\bar{\delta} \neq 0$*, resp.* $\bar{\gamma}\bar{\delta} \neq 0$*.)*

Proof — In the large image case, we can take for instance $\bar{g} = \left(\begin{smallmatrix} 1 & 1 \\ 1 & 2 \end{smallmatrix}\right) \in \overline{G} \cap \mathrm{GL}_2(\mathbb{F}_p)$.

We assume that we are in some of the exceptional cases. It suffices to find one matrix g_1 in $\overline{G}$ satisfying $\bar{\alpha}\bar{\beta} \neq 0$ for then since $\overline{G} \subset GL_2(\mathbb{F}_q)Z$, a suitable product of g_1 by a scalar matrix will belong to $\mathrm{GL}_2(\mathbb{F}_q)$ and obviously will still satisfies the required condition.

If all matrices in $\overline{G}$ had $\bar{\beta} = 0$, then the representation $\bar{\rho}$ would be reducible. Among the matrices such that $\bar{\beta} \neq 0$, if there is one with $\bar{\alpha} \neq 0$, we are done. Otherwise, all matrices with $\bar{\beta} \neq 0$ are of the form $\left(\begin{smallmatrix} 0 & \bar{\beta} \\ \bar{\gamma} & \bar{\delta} \end{smallmatrix}\right)$ and their square is $\left(\begin{smallmatrix} \bar{\beta}\bar{\gamma} & \bar{\beta}\bar{\delta} \\ * & * \end{smallmatrix}\right)$. Now $\bar{\gamma}$ is not 0 because the matrix is invertible, and if $\bar{\delta} \neq 0$ either, we are done. Otherwise, this means that all matrices with $\bar{\beta} \neq 0$ have both $\bar{\alpha}$ and $\bar{\delta}$ equal zero, that is are antidiagonal. But then it is easy to see that $\overline{G}$ is contained in the normalizer of the diagonal torus, a contradiction with the hypothesis that $\overline{G}$ is exceptional.

□

Lemma 6.8.8. *Let X be a closed $W(\mathbb{F}_q)$-submodule of A. Let $x \in A^*$ whose image in $A/\mathfrak{m} = \mathbb{F}$ lies in $\mathbb{F}_q$.*

- *If $xX \subset X$, then $xX = X$.*
- *If $x^2X = X$, then $xX = X$.*

Proof — Replacing x by x^{-1}, the hypothesis becomes $X \subset xX$, and the contention is still that $X = xX$. Then by induction $X \subset xX \subset \cdots \subset x^nX$ for all $n > 0$. Writing $x = s(\bar{x}) + m$ with $\bar{x} \in \mathbb{F}_q$ the reduction of x and $m \in \mathfrak{m}$, we get $x^{q^n} \equiv s(\bar{x}) \pmod{\mathfrak{m}^{nv_p(q)+1}}$ and so $X \subset xX \subset X + \mathfrak{m}^{nv_p(q)+1}X$. Since X is a closed subgroup, the intersection of all $X + \mathfrak{m}^{nv_p(q)+1}X$ when $n \geq 1$ is X, and we get $X \subset xX \subset X$, as desired. This proves the first point.

For the second point, note that if $x^2X = X$, then $x^{2n}X = X$. Choosing a sequence of positive integers n which converges to $1/2$ p-adically gives the result. □

Lemma 6.8.9. *There exists $x, y \in A^*$ such that the images of x and y in $A/\mathfrak{m} = \mathbb{F}$ are in $\mathbb{F}_q$, $\tilde{B}_1 = x\tilde{I}_1$, and $\tilde{C}_1 = y\tilde{I}_1$.*

Proof — Pick a matrix $\bar{g}$ as in Lemma 6.8.7 such that $\bar{\alpha}\bar{\gamma} \neq 0$. By Lemma 6.8.6, there is a lift $u \in A^*$ of $\bar{\alpha}\bar{\gamma}$ such that $u\tilde{B}_1 \subset \tilde{I}_1$. Also pick a matrix $\bar{g}'$ as in Lemma 6.8.7 such that $\bar{\alpha}'\bar{\beta}' \neq 0$. By Lemma 6.8.6, there is a lift $v \in A^*$ of $\bar{\alpha}\bar{\beta}$ such that $v\tilde{I}_1 \subset \tilde{B}_1$. Thus $uv\tilde{I}_1 \subset u\tilde{B}_1 \subset \tilde{I}_1$. The inclusion $uv\tilde{I}_1 \subset \tilde{I}_1$ is an equality by Lemma 6.8.8 (note that the image of uv in $A/\mathfrak{m}$ is $\bar{\alpha}\bar{\gamma}\bar{\alpha}'\bar{\beta}' \in \mathbb{F}_q^*$). Therefore, $u\tilde{B}_1 = \tilde{I}_1$ and the first result follows with $x = u^{-1}$. The second is similar. □

Now let $t = \sqrt{xy^{-1}/s(xy^{-1})} \in A^*$. We check easily that $\frac{x}{t} = yt\, s(xy^{-1})$. We conjugate ρ by the diagonal matrix $\left(\begin{smallmatrix} 1 & 0 \\ 0 & t \end{smallmatrix}\right)$. This doesn't affect any of the properties of $\bar{\rho}$ already stated, and doesn't change $\tilde{I}_1$ but changes $\tilde{B}_1$ into $\frac{1}{t}\tilde{B}_1 = \frac{x}{t}\tilde{I}_1$ and $\tilde{C}_1$ into $t\tilde{C}_1 = yt\tilde{I}_1 = yt\, s(xy^{-1})\tilde{I}_1$. Replacing x by $\frac{x}{t}$, we get:

(6.8.6) *There exists $x \in A^*$ such that the image of x in $A/\mathfrak{m} = \mathbb{F}$ is in $\mathbb{F}_q$, such that $\tilde{B}_1 = \tilde{C}_1 = x\tilde{I}_1$.*

Now we again pick a matrix $\bar{g}$ as in Lemma 6.8.7 such that $\bar{\alpha}\bar{\gamma} \neq 0$. By Lemma 6.8.6, for some lift α, γ of $\bar{\alpha}, \bar{\gamma}$, one has $\alpha^2\tilde{B}_1 \subset \tilde{B}_1$ and $\gamma^2\tilde{B}_1 \subset \tilde{C}_1 = \tilde{B}_1$. By the first point of Lemma 6.8.8, this means $\alpha^2\tilde{B}_1 = \tilde{B}_1$ and $\gamma^2\tilde{B}_1 = \tilde{B}_1$, and by the second point $\alpha\tilde{B}_1 = \tilde{B}_1$ and $\gamma\tilde{B}_1 = \tilde{B}_1$. Therefore $\alpha\gamma\tilde{B}_1 = \tilde{B}_1$. On the other hand, by Lemma 6.8.6, $\alpha\gamma\tilde{B}_1 \subset \tilde{I}_1$, and thus $\tilde{B}_1 \subset \tilde{I}_1$. The converse inclusion $\tilde{I}_1 \subset \tilde{B}_1$ is proved similarly using a matrix with $\bar{\alpha}\bar{\beta} \neq 0$. We have therefore proved:

(6.8.7) $\tilde{B}_1 = \tilde{C}_1 = \tilde{I}_1$, $L = \begin{pmatrix} \tilde{I}_1 & \tilde{I}_1 \\ \tilde{I}_1 & \tilde{I}_1 \end{pmatrix}^0$.

From (4.9.12.2), one has $\tilde{I}_1\tilde{B}_1 \subset \tilde{B}_1$, that is

(6.8.8) $\tilde{I}_1^2 \subset \tilde{I}_1$.

Proposition 6.8.10. *One has $W(\mathbb{F})\tilde{I}_1 = \mathfrak{m}$.*

Proof — By [11, Theorem 7.16(b)], it is enough to prove that the natural composed map $f : W(\mathbb{F})\tilde{I}_1 \hookrightarrow \mathfrak{m} \to \mathfrak{m}/\mathfrak{m}^2$ is surjective. To prove this, it is enough to prove that for each non-zero linear form $l : \mathfrak{m}/\mathfrak{m}^2 \to \mathbb{F}$, the composition $l \circ f : W(\mathbb{F})\tilde{I}_1 \to \mathbb{F}$ is surjective, which is the same as being non-zero. Such a linear form l (geometrically, a tangent vector to the unique closed point of $\operatorname{Spec} A$) induces a surjective morphism of rings $A \to A/\mathfrak{m}^2 \to \mathbb{F}[\epsilon]$ where the second map sends $m \in \mathfrak{m}/\mathfrak{m}^2$ to $l(m)\epsilon$. We need to prove that the image of $\tilde{I}_1$ in that map is non zero. By functoriality (see §4.8.1), the image of $\tilde{I}_1$ in $\mathbb{F}[\epsilon]$ is the same as the $\tilde{I}_1$ obtained for the admissible pseudo-deformation $(\Pi, \bar{\rho}, t', d')$ over $\mathbb{F}[\epsilon]$, where t', d' are t, d composed with the map $A \to \mathbb{F}[\epsilon]$.

In other words, we have reduced the proof of the proposition to the case $A = \mathbb{F}[\epsilon]$, and in this case we just have to prove that $\tilde{I}_1 \neq 0$. We proceed by contradiction. Assume $\tilde{I}_1 = 0$. Then by (6.8.7), $L = 0$, so $\Gamma \subset \Theta^{-1}(L)$ is the trivial group and the reduction map $G \to \bar{G}$

is an isomorphism. The morphism $r : \bar{G} \simeq G \subset \mathrm{GL}_2(A)$ is thus a deformation to $A = \mathbb{F}[\epsilon]$ of the tautological representation $\bar{G} \subset \mathrm{GL}_2(\mathbb{F})$. Such deformations are parametrized by $H^1(\bar{G}, V)$, where V is the trace-zero adjoint representation of the tautological representation of $\bar{G}$, and this cohomology group is trivial by Prop. 3.2.1. Therefore, the trace of r is constant, that is $\mathrm{tr}\,(G) \subset \mathbb{F}$, in contradiction with the hypothesis (5.2.5) that $\mathrm{tr}\,(G)$ generates $A = \mathbb{F}[\epsilon]$ as an $\mathbb{F}$-algebra. □

Together, this proposition, (6.8.7) and (6.8.8) complete the proof of Theorem 6.8.1.

7. Congruence-large image

This section is not used in the rest of the paper. Its aim is to establish a connection between our results on the structure of the image of pseudo-deformation and a series of recent results by Hida [12], Lang [15] and Conti-Iovita-Tilouine [8] concerning the image of the Galois representation carried by certain p-adic families of modular forms, ordinary in the work of first two named authors, of positive slope for the last group. Our setting is more general as we work with families of 2-dimensional representations of arbitrary profinite groups, over arbitrary noetherian compact local domain. The aim of this section is to show that we can obtain, in this general setting, results that are quite close (and sometimes stronger) to those proved for families of modular forms.

In all this section, A is a compact noetherian local ring with maximal ideal $\mathfrak{m}$ and residue field $\mathbb{F}$ finite of characteristic $p > 2$. We also assume that A is a domain, of fraction field K.

7.1. **The notion of congruence-large image.**

Definition 7.1.1. Let R be a GMA over A. If I is an ideal of A, the *principal congruence subgroup* $\Gamma_R(I)$ of I is the subgroup of R^* defined as the kernel of the map $SR \to (R/IR)^*$. A closed subgroup of R^* is called *a congruence subgroup* if it contains $\Gamma_R(I)$ for some non-zero ideal I of A.

By definition, $\Gamma_R(I)$ is the set of matrices $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ in R such that $a, d \equiv 1 \pmod{I}$, $b \in IB$, $c \in IC$ and $ad - bc = 1$. When $R = M_2(A)$, we retrieve the usual notion of the group of matrices congruent to the identity modulo I.

Lemma 7.1.2. *Let R be a topological GMA over A, Γ a closed subgroup of SR^1. Then Γ is a congruence subgroup if and only if $L(\Gamma)$ contains $\begin{pmatrix} I & I \\ I & I \end{pmatrix}^0$ for some non-zero ideal I of A.*

Proof — First, a trivial computation gives $\Theta(\Gamma_R(I)) = \left(\begin{smallmatrix} I & I \\ I & I \end{smallmatrix}\right)^0$, hence $L(\Gamma_R(I)) = \left(\begin{smallmatrix} I & I \\ I & I \end{smallmatrix}\right)^0$. By Prop 4.8.2, $\Theta^{-1}\left(\left(\begin{smallmatrix} I & I \\ I & I \end{smallmatrix}\right)^0\right)$ is the unique closed subgroup of SR^1 whose Lie algebra is $\left(\begin{smallmatrix} I & I \\ I & I \end{smallmatrix}\right)^0$, hence $\Theta^{-1}\left(\left(\begin{smallmatrix} I & I \\ I & I \end{smallmatrix}\right)^0\right) = \Gamma_R(I)$ (this can also be obtained by a direct computation).

Let Γ be a closed subgroup of SR^1. If Γ contains $\Gamma_R(I)$, then $L = L(\Gamma)$ contains $\Theta(\Gamma_R(I)) = \left(\begin{smallmatrix} I & I \\ I & I \end{smallmatrix}\right)^0$. Conversely, assume that $L(\Gamma)$ contains $\left(\begin{smallmatrix} I & I \\ I & I \end{smallmatrix}\right)^0$. Then L_2 contains $\left(\begin{smallmatrix} I^2 & I^2 \\ I^2 & I^2 \end{smallmatrix}\right)^0$ and $\Gamma = \Theta^{-1}(L_2)$ by Theorem 4.7.3, so Γ contains $\Gamma_R(I^2)$. □

Lemma 7.1.3. *Let Π be a group, (t,d) a 2-dimensional pseudo-representation of Π over A which is not the sum of two characters. Let R_1 and R_2 be two faithful GMA over A, finite-type as A-modules, and let $\rho_1 : \Pi \to R_1^*$, $\rho_2 : \Pi \to R_2^*$ be two representations both of trace t and determinant d. Then $\rho_1(\Pi)$ is a congruence subgroup of R_1 if and only if $\rho_2(\Pi)$ is a congruence subgroup of R_2.*

Proof — By Lemma 2.2.2, we can assume that both R_1 and R_2 are sub-algebras of $M_2(K)$. Seen as representations over K, ρ_1 and ρ_2 have the same trace and determinant, hence are conjugate. Let $g \in \mathrm{GL}_2(K)$ such that $\rho_2 = g\rho_1 g^{-1}$. Since R_1 and R_2 are of finite type, there exists $z \in A - \{0\}$ such that $zgR_1g^{-1} \subset R_2$.

If $\gamma - 1 \in IzR_1$, we have $g(\gamma-1)g^{-1} \in IzgR_1g^{-1} \subset IR_2$, and hence $g\gamma g^{-1} \in 1 + IR_2 \subset R_2$, so $g(\gamma-1)g^{-1} \in \Gamma_{R_2}(I)$. Therefore, $\Gamma_{R_1}(Iz) \subset g^{-1}\Gamma_{R_2}(I)g$, and it follows that if $\rho_2(\Pi)$ contains a congruence subgroup of R_2^*, $\rho_1(\Pi) = g^{-1}\rho_2(\Pi)g$ contains a congruence subgroup of R_1^*. □

Definition 7.1.4. We say that an two-dimensional pseudo-representation (t,d) of a group Π over A has *congruence-large image* if for one (equivalently for any) representation $\rho : \Pi \to R^*$, with R a faithful finite-type GMA over A, such that $\mathrm{tr}\,\rho = t$ and $\det\rho = d$, $\rho(\Pi)$ is a congruence subgroup of R^*.

7.2. **Sufficient conditions for a congruence-large image.**

Definition 7.2.1. We say that a representation $\bar\rho : \Pi \to \mathrm{GL}_2(\mathbb{F})$ is *regular* if there exists an element g_0 in Π such that $\bar\rho(g_0)$ is diagonalizable of eigenvalues λ and μ in $\mathbb{F}_p^*$, with $\lambda^2 \neq \mu^2$.

Remark 7.2.2. If $\bar\rho$ is regular, it has an element of order > 2 in its projective image, which therefore cannot be cyclic of order 2, or dihedral of order 4. In the other cases (cyclic of order > 2, dihedral of order > 4, large or exceptional), there exist many regular representations, for instance all that have $\mathbb{F}_p$ as field of definition.

The notion of regularity is related to the notion of an *H-regular representation* of Lang ([15]) and of an *$(H,\mathbb{Z}_p)$-regular representation* of Conti-Iovita-Tilouine of [8]. Let us recall that H-regular means that H is a subgroup such that there is an element $g_0 \in H$ such that $\bar\rho(g_0)$ is diagonalizable with distinct eigenvalues λ, μ, while $(H,\mathbb{Z}_p)$-regular requires in addition that $\lambda^2 \neq \mu^2$ and $\lambda, \mu \in \mathbb{F}_p$. It is obvious that $(H,\mathbb{Z}_p)$-regular (for any H) implies regular in our sense, while regular implies Π-regular, but not in general H-regular for a proper subgroup H of Π.

Theorem 7.2.3. *Assume that A is a domain, and that Π satisfies Mazur's p-finiteness condition. Let $(\Pi, \bar\rho, t, d)$ be an admissible pseudo-deformation such that $\bar\rho$ is regular. Moreover, we assume that*

- *If $\bar\rho$ is reducible, t is not the sum of two continuous characters $\Pi \to A^*$.*

- *If $\bar\rho$ is dihedral, then if Π' is the unique subgroup of index 2 of Π such that $\bar\rho(\Pi')$ is abelian, $t_{|\Pi'}$ is not the sum of two characters.*

Then there exists a subring A_0 of A, which is a compact noetherian local ring of maximal ideal $\mathfrak{m}\cap A_0$, and an open subgroup Π_0 of Π, containing $\operatorname{Ker}\bar\rho$, such that

- $t(\Pi_0)\subset A_0$, $d(\Pi_0)\subset A_0^*$.
- $(\Pi_0, \bar\rho_{|\Pi_0}, t_{|\Pi_0}, d_{|\Pi_0})$ *is an admissible pseudo-deformation over A_0, and has congruence-large image.*

Proof — We choose a $g_0\in\Pi$ as in the definition 7.2.1 and a (t,d)-representation $\rho:\Pi\to R^*$ with $R=\begin{pmatrix}A & B\\ C & A\end{pmatrix}$ adapted to g_0. In particular, if D_0 denotes the subgroup of $\bar\rho(\Pi)$ generated by $\bar\rho(g_0)$, then D_0 is a group of diagonal matrices and $s(D_0)\subset G$ by Theorem 6.2.1. We write $\bar\rho(g_0)=\left(\begin{smallmatrix}\lambda & 0\\ 0 & \mu\end{smallmatrix}\right)$.

By Cor. 6.2.3, L is strongly decomposable. We write $L=\begin{pmatrix}I_1 & B_1\\ C_1 & I_1\end{pmatrix}^0$ with I_1, B_1 and C_1 closed subgroups of A, B and C respectively.

We define

$$A_0:=\mathbb{Z}_p+I_1+I_1^2.$$

By (4.9.12.3), A_0 is a subring of A, and it is clearly a compact local ring of maximal ideal $\mathfrak{m}_0=p\mathbb{Z}_p+I_1+I_1^2=\mathfrak{m}\cap A_0$. By (4.9.12.2), both B_1 and C_1 are A_0-modules.

We define

$$\Pi_0=\bar\rho^{-1}(D_0).$$

This is obviously a subgroup of finite index in Π, containing $\operatorname{Ker}\bar\rho$. The restriction of $\bar\rho$ to Π_0 is a reducible representation, sum of two distinct characters.

We claim that the closed $\mathbb{Z}_p$-subalgebra of A generated by $t(\Pi_0)$ is A_0. Indeed, let us call A_0' that subring. Any element of Π_0 can be written $s(d)\gamma$, with $d\in D_0$ and $\gamma\in\Gamma\subset\Theta^{-1}(L)$, and thus has trace in $\mathbb{Z}_p+I_1+P=\mathbb{Z}_p+I_1+I_1^2$ (by (4.9.10) and (4.9.12.1)). Thus we see that $t(\Pi_0)\subset A_0$, hence $A_0'\subset A_0$. On the other hand, A_0' contains $\mathbb{Z}_p$ by definition. It therefore contains $\operatorname{tr}(\gamma)-2$ for every $\gamma\in\Gamma$, hence it contains P by Cor. 4.5.2. And it contains $\operatorname{tr}(s(g_0)^n\Gamma)$ for any n, hence I_1. Thus $A_0=A_0'$.

It follows easily that $(\Pi_0,\bar\rho_{|\Pi_0},t_{|\Pi_0},d_{|\Pi_0})$ is an admissible pseudo-deformation over A_0. By Cor. 5.3.2, and since Π_0 satisfies the p-finiteness condition (because Π does), A_0 is a noetherian ring.

We define R_0 as the A_0-sub-GMA $\begin{pmatrix}A_0 & B_1\\ C_1 & A_0\end{pmatrix}$ of R. Since this is a sub-GMA of $M_2(K)$, R_0 is faithfull provided that $B_1\neq 0$ and $C_1\neq 0$, and this follows from the hypothesis made on (t,d). One has clearly $\rho(\Pi_0)\subset R_0^*$. Moreover $\rho(\Pi_0)$ generates R_0 as an A_0-module, since clearly the $s(g_0)^n$ generates the subring of diagonal matrices $\begin{pmatrix}A_0 & 0\\ 0 & A_0\end{pmatrix}$ of R_0, and $\rho(\Pi_0)$ contains Γ, whose projection on anti-diagonal matrices topologically generates as an additive group, hence as an A_0-module, $\nabla=\begin{pmatrix}0 & B_1\\ C_1 & 0\end{pmatrix}$. Thus, the restriction $\rho_{|\Pi_0}$ of ρ to Π_0 is a $(t_{|\Pi_0},d_{|\Pi_0})$-representation.

Its image $\rho(\Pi_0)$ contains Γ, hence also $\Gamma_2 = \Theta^{-1}(L_2)$. From the description of L, it follows that $L_2 = \begin{pmatrix} B_1C_1 & I_1B_1 \\ I_1C_1 & B_1C_1 \end{pmatrix}$. Since I_1 contains B_1C_1, L_2 contains $B_1C_1J \oplus \begin{pmatrix} 0 & B_1^2C_1 \\ B_1C_1^2 & 0 \end{pmatrix} \supset B_1C_1R_0^0$, and it follows that the image of $\rho_{|\Pi_0}$ contains the congruence subgroup $\Gamma_{R_0}(B_1C_1)$. □

Remark 7.2.4. With the notation of the preceding theorem and its proof, let K be the fraction field of A, and K_0 be the fraction field of A_0. The representation $\rho : \Pi \to R^*$ induces a representation $\rho_K : \Pi \to \mathrm{GL}_2(K)$ since $R \otimes_A K = M_2(K)$. Similarly, $\rho_{\Pi_0} : \Pi_0 \to R_0^*$ induces a representation $\rho_{K_0} : \Pi_0 \to \mathrm{GL}_2(K_0)$. The representations ρ_{K_0} and ρ_K have the same trace and determinant on Π_0. Therefore there exists $g \in \mathrm{GL}_2(K)$ such that $g\rho_K g^{-1} = \rho_{K_0}$ on Π_0. The conclusion of our theorem implies that $\rho_K(\Pi_0)$ contains $1 + JR_0$ for some non-zero ideal J. It follows from Lemma 7.1.3 that $\rho_K(\Pi_0)$ contains $1 + J'M_2(A_0)$ for some ideal J'. Hence $g\rho(\Pi_0)g^{-1}$ contains the congruence subgroup $\Gamma_{M_2(A_0)}(J')$.

This is the way the conclusion of the main theorem of Lang [15, Theorem 2.4] is stated, as well as the main theorem of [8].

On the other hand, the hypotheses of Lang are that $\Pi = G_{\mathbb{Q}}$, A a local domain finite over the Iwasawa algebra $\mathbb{Z}_p[[T]]$, (t, d) the pseudo-representation carried by a Hida's family which is residually absolutely irreducible – a very special case of the situation we are studying. She assumes in addition that the family is not CM, an hypothesis which is equivalent (under other running assumptions) to our assumption that $t_{|\Pi'}$ is not the sum of two characters. Finally she is assuming that (t, d) is Π_0-regular, an hypothesis which does not imply our regularity assumption (it allows, it seems, for some $\bar{\rho}$ with projective image dihedral of order 4), nor is implied by ours.

To summarize Theorem 7.2.3 implies the congruence-large image result of [15, Theorem 2.4] in many cases though not in all cases, and it implies the congruence-large image result of [8] in all cases.

In the references [15] and [8], the congruence-large image result are made more precise by an explicit description of the subring A_0 of A and the subgroup Π_0 of Π, in terms of the *conjugate self-twist* of (t, d) (see [15, definition 2.1]). Our method also gives an explicit description of Π_0 and A_0, though a different one. It would be interesting to compare these descriptions.

8. The essential submodule attached to an admissible pseudo-deformation

In this section, we assume that A satisfies the condition (5.1.1). We also assume throughout that $p > 2$.

8.1. **Definition of the essential submodule.**

Definition 8.1.1. Let $(\Pi, \bar{\rho}, t, d)$ be an admissible pseudo-deformation over A. Let $\rho : \Pi \to R^*$ be a (t, d)-representation, and define G, Γ, L accordingly, with L_2 the derived Lie

algebra of L. We call S the set of elements $g \in G$ such that $\mathrm{tr}\,(g) = 0$ and $-\det(g)$ is a square in A^*. We shall say that $(\Pi, \bar{\rho}, t, d)$ is *weakly odd* if the set S is non empty.

In all this section we shall assume that $(\Pi, \bar{\rho}, t, d)$ is weakly odd.

Definition 8.1.2. With the same notation as in the preceding definition, define

$$A_{\mathrm{ess}} = \sum_{g \in S} W(\mathbb{F})\mathrm{tr}\,(gL_2) \subset A.$$

We call this $W(\mathbb{F})$-submodule A_{ess} of A the *essential submodule* of A attached to $(\Pi, \bar{\rho}, t, d)$.

Note that the condition of being weakly odd, and the $W(\mathbb{F})$-submodule A_{ess} of A depend only on (Π, t, d), and not on the (t, d)-representation $\rho : \Pi \to R^*$, for if $\rho' : \Pi \to R'^*$ is another (t, d)-representation, then there exists an isomorphism $f : R \to R'$ preserving trace and determinant such that $\rho' = f \circ \rho$; the group $G' = \rho'(\Pi)$ is the image $f(G)$, and $\Gamma' = f(\Gamma)$, $L' = f(L)$, $L'_2 = f(L_2)$. It is clear that f realizes a bijection between S and S' and for every $g \in S$ a bijection between the subgroups $\sum_{g \in S} gL_2$ of R and $\sum_{g' \in S'} g'L'_2$ of R'. Since f preserves traces, it follows that

$$A_{\mathrm{ess}} = \sum_{g \in S} W(\mathbb{F})\mathrm{tr}\,(gL_2) = \sum_{g' \in S'} W(\mathbb{F})\mathrm{tr}\,(g'L'_2).$$

The real motivation for introducing the submodule A_{ess} is its essential rôle in analyzing the density of modular forms modulo p, see section 10 below. Meanwhile, A_{ess} can be considered as a very rough measure of how big the image G of the pseudo-deformation is: the bigger G, the bigger Γ, L and L_2, and the more numerous the $g \in G$ such that $g^2 = 1$, hence the bigger A_{ess}. In this sense, most of the results below can be seen as big image theorems, though of a different type than the big image theorem of the previous section.

Lemma 8.1.3. *Let $(\Pi, \bar{\rho}, t, d)$ be an admissible pseudo-deformation and $\rho : \Pi \to R^*$ a (t, d)-representation such that $J = \left(\begin{smallmatrix} 1 & 0 \\ 0 & -1 \end{smallmatrix}\right) \in G$ (and therefore $L = I_1 J \oplus \nabla$ is decomposable). Let Δ_2 and ∇_2 be the subgroups of diagonal and anti-diagonal matrices in L_2.*

(8.1.1) *One has $L_2 = \Delta_2 \oplus \nabla_2$, $\Delta_2 = [\nabla, \nabla]$ and $\nabla_2 = [\Delta, \nabla]$.*

One can write $\Delta_2 = I_2 J$ for some closed subgroup I_2 of I_1, and one has a decomposition:

(8.1.2) *$L_2 = I_2 J \oplus \nabla_2$.*

(8.1.3) *One has $I_2 \subset I_1$, $\Delta_2 \subset \Delta$, $\nabla_2 \subset \nabla$.*

(8.1.4) *For every $\gamma \in \Gamma$, one has $\mathrm{tr}\,(J\gamma L_1) = I_1$ and $\mathrm{tr}\,(J\gamma L_2) = I_2$.*

Proof — One has $L_2 = [L, L] = [\Delta \oplus \nabla, \Delta \oplus \nabla] = [\nabla, \nabla] + [\Delta, \nabla]$ since $[\Delta, \Delta] = 0$ (two diagonal matrices commute). But $[\nabla, \nabla]$ consists of diagonal matrices, and $[\Delta, \nabla]$ of antidiagonal ones. This proves (8.1.1) and (8.1.2). Since $L_2 \subset L$, (8.1.3) is clear

Let us prove (8.1.4). By decomposition (8.1.2), one has $\mathrm{tr}\,(J\gamma L_1) = \mathrm{tr}\,(\gamma) I_1 + \mathrm{tr}\,(J\gamma\nabla)$, and by Lemma 4.8.1, $\mathrm{tr}\,(\gamma) I_1 = I_1$. It therefore suffices to prove that $\mathrm{tr}\,(J\gamma\nabla) \subset I_1$. For this, let us denote by $\epsilon \in \nabla$ the anti-diagonal part of γ or of $\Theta(\gamma)$, and by η any matrix in ∇. One needs to show that $\mathrm{tr}\,(J\gamma\eta) = \mathrm{tr}\,(J\epsilon\eta) \in I_1$. Since ϵ and η are anti-diagonal, one

has $\mathrm{tr}\,(J\epsilon\eta) = -\mathrm{tr}\,(J\eta\epsilon)$, and thus $\mathrm{tr}\,(J\epsilon\eta) = \mathrm{tr}\,(J[\epsilon,\eta])/2$. Since $[\nabla,\nabla] = \Delta_2 = I_2 J$, one has $[\epsilon,\eta] \in I_2 J$ and one gets $\mathrm{tr}\,(J\epsilon\eta) \in \mathrm{tr}\,(JJI_2) = I_2 \subset I_1$, which completes the proof of (8.1.4) for L_1. The proof for L_2 is exactly the same. □

Lemma 8.1.4. *If $(\Pi, \bar\rho, t, d)$ is an admissible pseudo-deformation over A, and $f : A \to A'$ a surjective morphism of rings, then A' is a again a compact semi-local ring (for the quotient topology), and setting $t' = f \circ t$, $d' = f \circ d$, $(\Pi, \bar\rho, t', d')$ is an admissible pseudo-deformation over A'. Moreover, if A_{ess} (resp. A'_{ess}) is the essential submodule of $(\Pi, \bar\rho, t, d)$ (resp. of $(\Pi, \bar\rho, t', d')$), then $f(A_{ess}) = A'_{ess}$.*

This is clear.

In particular, if $A_{i,\mathrm{ess}}$ is the essential sub-module of $(\Pi, \bar\rho_i, t_i, d_i)$, then the projection $A \to A_i$ sends A_{ess} onto $A_{i,\mathrm{ess}}$. Note however that the map $A_{\mathrm{ess}} \to \prod_{i=1}^r A_{i,\mathrm{ess}}$ is not in general surjective.

Fix an admissible pseudo-deformation $(\Pi, \bar\rho, t, d)$ and $\rho : \Pi \to R^*$ a (t,d)-representation.

Definition 8.1.5. Let $\bar S$ be the set of elements $\bar g \in \overline{G}$ such that $\mathrm{tr}\,(\bar g) = 0$ and $-\det(g)$ is a square in $(A/\mathfrak{m})^*$.

Note that the reduction map $G \to \overline{G}$ obviously induces a map $S \to \bar S$.

Proposition 8.1.6. *The natural reduction map $S \to \bar S$ is surjective. For $g \in S$, the subgroup $\mathrm{tr}\,(gL_2)$ of A only depends on the image $\bar g$ of g in $\bar S$. Moreover, for every $g \in S$, there exists a GMA R', an isomorphism of A-algebras $f : R \to R'$ preserving traces and determinants, such that $f(g) = s(\lambda)J$ for some $\lambda \in \mathbb{F}^*$, and such that if ρ' denotes the R'-valued (t,d)-representation $\rho' = f \circ \rho$, and L'_2, I'_2 are defined using ρ', then one has $W(\mathbb{F})\mathrm{tr}\,(gL_2) = W(\mathbb{F})\mathrm{tr}\,(JL'_2) = W(\mathbb{F})I'_2$.*

Proof — Let $\bar g \in \bar S$. By (5.2.4), there exists $\lambda \in \mathbb{F}^*$ such that $\det(\bar g) = -\lambda^2$ with $\lambda \in \mathbb{F}^*$. Denotes by $\bar g_i$ the image of the element $\bar g$ of $(R/\mathrm{rad}R)^*$ in $(R_i/\mathrm{rad}R_i)^*$. By definition of $\bar S$, there exists an element $g_0 \in \Pi$ such that $\bar\rho_i(g_0) = \bar g_i$ for $i = 1, \dots, r$.

Since $\mathrm{tr}\,(\bar\rho_i(g_0)) = 0$, the eigenvalues of $\bar\rho_i(g_0)$ in $R_i/(\mathrm{rad}R_i)$ are $\pm\lambda$, two distinct elements of $\mathbb{F}^*$. Let us choose a (t,d)-representation $\rho'_i : \Pi \to R_i'^*$ adapted to $(g_0, \lambda, -\lambda)$ (Prop. 2.4.2(iii)); let us set $R' = \prod_{i=1}^r R'_i$ and $\rho' = \prod_{i=1}^r \rho'_i$, and let us denote by G', Γ', L', etc the group-theoretic and Lie theoretic data attached to ρ'. Then $\bar\rho'(g_0) = \lambda J$ and by Theorem 6.2.1, $\rho'(g_0) = s(\lambda)J \in G'$.

Moreover, any lift $g' \in G'$ of $\bar\rho'(g_0) = \lambda J$ is of the form $s(\lambda)J\gamma$ with $\gamma \in \Gamma'$, so by (8.1.4), $W(\mathbb{F})\mathrm{tr}\,(g'L_2) = W(\mathbb{F})\mathrm{tr}\,(J\gamma L_2) = W(\mathbb{F})I'_2$, which is independent of g'. There exists (Prop. 2.4.2(ii)) an isomorphism of A-algebras $f : R \to R'$ such that $f \circ \rho = \rho'$, preserving trace and determinant. By definition, if g is a lift of $\bar g = \bar\rho(g_0)$ in S, then $g' := f(g)$ is a lift of $\bar\rho'(g_0)$ in S', and $f(L_2) = L'_2$, so that $\mathrm{tr}\,(gL_2) = \mathrm{tr}\,(g'L'_2) = I'_2$, which is independent of g. □

Corollary 8.1.7. *One has* $A_{ess} = \sum_{\bar{g}\in\bar{S}} W(\mathbb{F})\mathrm{tr}\,(gL_2)$ *where in the summand* $\mathrm{tr}\,(gL_2)$, g *is an arbitrarily chosen lift of* $\bar{g}$ *in* S. *In particular,* A_{ess} *is a closed submodule of* A.

Proof — The first assertion follows from the definition of A_{ess} and the proposition. Since the $\mathbb{Z}_p$-module $\mathrm{tr}\,(gL_2)$ is compact, so is $W(\mathbb{F})\mathrm{tr}\,(gL_2)$. Since the set $\bar{S}$ is finite, it follows that A_{ess} is compact, hence closed in A. □

8.2. **The key measure computation.** In this subsection, we assume in addition to the preceding hypotheses that A is an $\mathbb{F}$-algebra (equivalently, that $pA = 0$). Therefore, in the results stated above, each time there is a $W(\mathbb{F})X$ where X is an additive subgroup of A or of R, it can just be replaced by $\mathbb{F}X$.

For any compact group X, we denote by μ_X the Haar measure on X of total mass 1. We fix an admissible weakly odd pseudo-deformation $(\Pi, \bar{\rho}, t, d)$.

Theorem 8.2.1. *Let* $l : A \to \mathbb{F}$ *be a linear form that is not identically* 0 *on* A_{ess}. *Then*

$$(8.2.1)\quad \mu_\Pi((l\circ t)^{-1}(\mathbb{F}^*)) \geq \tfrac{p-1}{pn},$$

where $n = |\overline{G}|$.

Since l does not vanish on A_{ess}, then by Prop. 8.1.6, for some (t,d)-representation ρ, l does not vanish on I_2. For the rest of this proof, we fix such a representation ρ and the attached groups G, Γ, L, L_2, I_2.

Since ρ is a surjective morphism of groups, the Haar measure μ_G is the direct image of the measure μ_Π by ρ. Since $t = \mathrm{tr}_G \circ \rho$, (8.2.1) is equivalent to:

$$(8.2.2)\quad \mu_G\left((l\circ \mathrm{tr}_G)^{-1}(\mathbb{F}^*)\right) \geq \tfrac{p-1}{pn},$$

which is the same thing as

$$(8.2.3)\quad \mu_G\left((l\circ \mathrm{tr}_G)^{-1}(0)\right) \leq \tfrac{1}{pn} + \tfrac{n-1}{n}.$$

To prove this, it is clearly enough to prove that

$$(8.2.4)\quad \mu_G\left((l\circ \mathrm{tr}_G)^{-1}(0)\cap J\Gamma\right) \leq \tfrac{1}{pn},$$

since $\mu_G(G - J\Gamma) = \frac{n-1}{n}$, $G - J\Gamma$ being the union of $n-1$ Γ-cosets each of measure $1/n$. Let m_J be the injective map $\Gamma \to G$, $\gamma \mapsto J\gamma$, whose image is the coset $J\Gamma$, and let μ_Γ be the Haar measure of total measure 1 on Γ. Clearly, (8.2.4) is equivalent to

$$(8.2.5)\quad \mu_\Gamma\left((l\circ \mathrm{tr}_G\circ m_J)^{-1}(0)\right) \leq \tfrac{1}{p}$$

Now consider the exact sequence $1 \to \Gamma_2 \to \Gamma \to \Gamma/\Gamma_2 \to 1$. By Fubini's theorem, to prove (8.2.5) it is enough to prove that for all $\gamma \in \Gamma/\Gamma_2$,

$$(8.2.6)\quad \mu_{\Gamma_2}\left((l\circ \mathrm{tr}_G\circ m_{J\gamma})^{-1}(0)\right) \leq \tfrac{1}{p}$$

where $m_{J\gamma}$ is the map $\Gamma_2 \to G$, $\gamma_2 \mapsto J\gamma\gamma_2$ and μ_{Γ_2} the Haar measure on Γ_2 of total measure 1. Since $\Theta^{-1} : L_2 \to \Gamma_2$ is a measure-preserving homeomorphism (Prop. 4.8.4), it suffices to prove

$$(8.2.7)\quad \mu_{L_2}\left((l\circ \mathrm{tr}_G\circ m_{J\gamma}\circ\Theta^{-1})^{-1}(0)\right) \leq \tfrac{1}{p}$$

To simplify notation let us define the map

$$h_\gamma = \mathrm{tr}_G \circ m_{J\gamma} \circ \Theta^{-1} : L_2 \xrightarrow{\Theta^{-1}} \Gamma_2 \xrightarrow{m_{J\gamma}} R^* \xrightarrow{\mathrm{tr}} A,$$

so that (8.2.7) becomes

$$(8.2.8)\ \mu_{L_2}\left((l \circ h_\gamma)^{-1}(0)\right) \leq \tfrac{1}{p}$$

To prove (8.2.8), we shall use the following result:

Proposition 8.2.2. *Fix $\gamma \in \Gamma$.*

(i) *There exists a measure preserving homeomorphism $\Psi = \Psi_\gamma : L_2 \to L_2$ such that $h_\gamma \circ \Psi^{-1} : L_2 \to A$ is $\mathbb{F}_p$-affine.*

(ii) *The image of h_γ is the $\mathbb{F}_p$-affine subspace $\mathrm{tr}\,(J\gamma) + I_2$ of A.*

Proof —

Let us define a map $\Psi : L_2 \to L_2$ by setting

$$\Psi(m) = m + \sigma(m) \text{ with } \sigma(m) = (\sqrt{1 + \mathrm{tr}\,(m^2)/2} - 1)\frac{\mathrm{tr}\,(J\gamma)}{\mathrm{tr}\,(\gamma)}J.$$

Let us check that Ψ is well-defined. Write $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$. First, one has $\mathrm{tr}\,(\gamma) = a + d \equiv 2 \pmod{\mathfrak{m}}$, hence $\mathrm{tr}\,(\gamma)$ is invertible in A, and the formula defining $\Psi(m)$ makes sense as an element of R. We need to check that it is indeed in L_2. By definition, $\Theta(\gamma) = \left(\begin{smallmatrix} (a-d)/2 & b \\ c & (d-a)/2 \end{smallmatrix}\right)$ is in L, and since L is decomposable, $\left(\begin{smallmatrix} (a-d)/2 & 0 \\ 0 & (d-a)/2 \end{smallmatrix}\right)$ is in L; on the other hand and one computes $\mathrm{tr}\,(J\gamma)J = \left(\begin{smallmatrix} a-d & 0 \\ 0 & d-a \end{smallmatrix}\right)$, so $\mathrm{tr}\,(J\gamma)J \in L$. One has $\mathrm{tr}\,(\gamma)^{-1}L = L$ by Lemma 4.8.1, hence $\frac{\mathrm{tr}\,(J\gamma)}{\mathrm{tr}\,(\gamma)}J$ is in L. On the other hand $\sqrt{1 + \mathrm{tr}\,(m^2)/2} - 1 = \sum_{n=1}^{\infty}\binom{n}{1/2}\frac{tr(m^2)^n}{2^n}$, and $\mathrm{tr}\,(m^2) \in \mathrm{tr}\,(L_2^2)$ and thus sends L into $L_5 \subset L_2$ as we see easily using (4.3.7). Hence $(\sqrt{1 + \mathrm{tr}\,(m^2)/2} - 1)\frac{\mathrm{tr}\,(J\gamma)}{\mathrm{tr}\,(\gamma)}J$ is in L_2, so $\sigma(m)$ is in L_2 and Ψ is well-defined.

If m, m' are in $L_2 \subset \mathfrak{m}^2 R$, and $m - m' \in \mathfrak{m}^n R$ then one sees that

$$\sqrt{1 + \mathrm{tr}\,(m^2)/2} - \sqrt{1 + \mathrm{tr}\,(m'^2)/2} = \sum_{n=1}^{\infty}\binom{n}{1/2}\frac{\mathrm{tr}\,(m^2)^n - \mathrm{tr}\,(m'^2)^n}{2^n} \in \mathfrak{m}^{n+2},$$

hence $\sigma(m) - \sigma(m') \in \mathfrak{m}^{n+2}L \subset \mathfrak{m}^{n+3}R$. Therefore, by Lemma 4.8.5, $\Psi : L_2 \to L_2$ is a measure-preserving homeomorphism.

For $m \in L_2$, one has

$$\begin{aligned} h_\gamma(m) &= \mathrm{tr}\,(J\gamma\Theta^{-1}(m)) \\ &= \mathrm{tr}\,(J\gamma m) + \mathrm{tr}\,(J\gamma)\sqrt{1 + \mathrm{tr}\,(m^2)/2} \\ &= \mathrm{tr}\,(J\gamma) + \mathrm{tr}\,(J\gamma\Psi(m)). \end{aligned}$$

Therefore $h_\gamma(\Psi^{-1}(m)) = \mathrm{tr}\,(J\gamma) + \mathrm{tr}\,(J\gamma m)$, which shows that $h_\gamma \circ \Psi^{-1}$ is an affine map as stated in (i), whose image is the affine space $\mathrm{tr}\,(J\gamma) + \mathrm{tr}\,(J\gamma L_2) = \mathrm{tr}\,(J\gamma) + I_2$ by (8.1.4). □

Using the proposition and the map Ψ it introduces, we see that to prove (8.2.8), it is enough to prove that

$$(8.2.9)\ \mu_{L_2}\left((l \circ h_\gamma \circ \Psi^{-1})^{-1}(0)\right) \leq \tfrac{1}{p}$$

But $h_\gamma \circ \Psi^{-1}$ is a $\mathbb{F}_p$-affine map. So $l \circ h_\gamma \circ \Psi^{-1}$ is an $\mathbb{F}_p$-affine map on L_2 with values in $\mathbb{F}$ and with image the $\mathbb{F}_p$-affine subspace $l(\mathrm{tr}\,(J\gamma)) + l(I_2)$. Since $l(I_2) \neq 0$, the image S of our map $l \circ h_\gamma \circ \Psi^{-1}$ is an affine $\mathbb{F}_p$-subspace of positive dimension of $\mathbb{F}$. The measure $\mu_{L_2}\left((l \circ h_\gamma \circ \Psi^{-1})^{-1}(0)\right)$ is 0 if S does not contain 0, and $1/|S|$ otherwise. In any case, it is less than $\frac{1}{p}$ which proves (8.2.9) and the theorem.

Remark 8.2.3. If we assume that $\Theta(\Gamma) = L$, then we can prove that the inequality $\mu_\Pi((l \circ t)^{-1}(\mathbb{F}^*)) \geq \frac{p-1}{pn}$, holds not only when $l(I_2) \neq 0$, but more generally when $l(I_1) \neq 0$. Indeed, to prove (8.2.5) for such an l, that is that $\mu_\Gamma\left((l \circ \mathrm{tr}_G \circ m_J)^{-1}(0)\right) \leq \frac{1}{p}$, it is enough to prove that $\mu_L\left((l \circ \mathrm{tr}_G \circ m_J \circ \Theta^{-1})^{-1}(0)\right) \leq \frac{1}{p}$. But the map $\mathrm{tr}_G \circ m_J \circ \Theta^{-1}$ is very simple: it sends a matrix $m = \left(\begin{smallmatrix} a & b \\ c & -a \end{smallmatrix}\right)$ to $\mathrm{tr}\,(J\Theta^{-1}m) = 2a$. In particular, this map is linear, and its image is the group I_1. Thus if l is non-zero on I_1, the map $(l \circ \mathrm{tr}_G \circ m_J \circ \Theta^{-1})^{-1}(0)$ is a $\mathbb{F}_p$-affine map from L to $\mathbb{F}$ whose image has positive dimension, and we conclude easily.

8.3. **A sufficient condition for the largeness of $A_{\mathbf{ess}}$.** In this subsection (and for the rest of this section) we assume that A is local.

Definition 8.3.1. An admissible pseudo-deformation $(\Pi, \bar\rho, t, d)$ is said to be *virtually abelian* if there exists an open subgroup Π_0 of Π such that the restriction $(t_{|\Pi_0}, d_{|\Pi_0})$ factors trough an abelian quotient of Π_0.

Lemma 8.3.2. *Let $(\Pi, \bar\rho, t, d)$ be a weakly odd admissible pseudo-deformation. Assume that A is a domain. If $A_{ess} = 0$, then $(\Pi, \bar\rho, t, d)$ is virtually abelian.*

Proof — Let us pick $g_0 \in S$ and choose $\rho : \Pi \to R^*$ a (t,d)-representation adapted to g_0. Thus L is decomposable and $W(\mathbb{F})\mathrm{tr}\,(gL_2) = W(\mathbb{F})I_2 \subset A_{\mathrm{ess}}$ so by hypothesis $I_2 = 0$.

If $\epsilon = \left(\begin{smallmatrix} 0 & b \\ c & 0 \end{smallmatrix}\right)$ and $\epsilon' = \left(\begin{smallmatrix} 0 & b' \\ c' & 0 \end{smallmatrix}\right)$ are in ∇, then $[\epsilon, \epsilon'] \in I_2 J = 0$, so $bc' - b'c = 0$. If $a \in I_1$, then $[aJ, \epsilon] = \left(\begin{smallmatrix} 0 & 2ab \\ -2ac & 0 \end{smallmatrix}\right) \in \nabla$, so we also have $2abc' + 2ab'c = 0$. Adding $2a$ times the first equation to the second gives $abc' = 0$, for every a, ϵ, ϵ' as above. Remember ([3, §1.3]) that since A is a domain, we may assume that if $R = \begin{pmatrix} A & B \\ C & A \end{pmatrix}$, for $b \in B$ and $c \in C$, $bc = 0 \Rightarrow b = 0$ or $c = 0$. It follows that we are in one of the three possibilities: either $I_1 = 0$ or $C_1 = 0$ (i.e. ∇ is upper triangular) or $B_1 = 0$.

If $I_1 = 0$, then $L = \nabla$, and $L_2 = [\nabla, \nabla] = \Delta_2 \subset I_1 J = 0$. Thus L is commutative. It follows that $\Theta^{-1}(L)$ is commutative and Γ is commutative. Let $\Pi_0 = \mathrm{Ker}\,\bar\rho$. Then $\rho(\Pi_0) = \Gamma$ is commutative, which proves that $(t_{|\Pi_0}, d_{|\Pi_0})$ factors trough an abelian quotient of Π_0.

If $C = 0$, all matrices in ∇ are upper-triangular and it follows that L itself, and $\Gamma \subset \Theta^{-1}(L)$ as well, are contained in the set of triangular matrices. If again we set $\Pi_0 = \mathrm{Ker}\,\bar\rho$, we see that $t_{|\Pi_0} = \mathrm{tr}\,\rho_{|\Pi_0}$ is the sum of two characters, hence factors through an abelian quotient.

The case $B = 0$ is dealt with the same way. □

Proposition 8.3.3. *Let $(\Pi, \bar{\rho}, t, d)$ be a weakly odd admissible pseudo-deformation, which is not virtually abelian. Assume that A is a domain. Let $g_0 \in \bar{S}$, and $\rho : \Pi \to R^*$ a (t,d)-representation adapted to g_0. Assume that for this representation, either $W(\mathbb{F})B_1$ or $W(\mathbb{F})C_1$ is not a finite-type $W(\mathbb{F})$-module. Then A_{ess} is not a finite type $W(\mathbb{F})$-module either.*

Proof — Assume by contradiction that A_{ess} is a finite type $W(\mathbb{F})$-module. Since $W(\mathbb{F})I_2 \subset A_{\mathrm{ess}}$, so is $W(\mathbb{F})I_2$. By the preceding lemma, $I_2 \neq 0$, and since $PI_2 \subset I_2$ and A is a domain, it follows that $W(\mathbb{F})P$ is a finite type $W(\mathbb{F})$-module. Therefore $W(\mathbb{F})P + W(\mathbb{F})I_2$ is a finite type $W(\mathbb{F})$-module. But if $\left(\begin{smallmatrix} 0 & b \\ c & 0 \end{smallmatrix}\right)$ and $\left(\begin{smallmatrix} 0 & b' \\ c' & 0 \end{smallmatrix}\right)$ are any elements in ∇, then $bc' - b'c \in I_2$ and $bc' + b'c \in P$, so bc' is in $I_2 + P$, and $I_2 + P$ contains B_1C_1, so $W(\mathbb{F})I_2 + W(\mathbb{F})P$ contains $W(\mathbb{F})B_1C_1$. But $W(\mathbb{F})B_1$ and $W(\mathbb{F})C_1$ are non-zero (otherwise the deformation would be virtually abelian) and by assumption one of them is not a finite $W(\mathbb{F})$-module, so it follows that $W(\mathbb{F})B_1C_1$ is not a finite $W(\mathbb{F})$-module, a contradiction. □

8.4. **The essential subgroup in the reducible case.** In this subsection we keep assuming that A is local and we fix an admissible weakly odd pseudo-deformation $(\Pi, \bar{\rho}, t, d)$, and we assume throughout that $\bar{\rho}$ is reducible.

(8.4.1) *There exists two continuous characters $\chi_1, \chi_2 : \Pi \to \mathbb{F}^*$, such that $\bar{\rho} \simeq \chi_1 \oplus \chi_2$.*

Let us chose a (t,d)-representation which is well-adapted in the sense of Definition 6.3.1. Thus the group $\bar{G}$ is a diagonal subgroup of $\mathrm{GL}_2(\mathbb{F})$, and $s(\bar{G}) \subset G$. Since $\bar{\rho}$ is weakly odd there exists in $\bar{G}$ an element of order 2 other than ± 1, and since this element is diagonal, it is either J or $-J$. There is no loss of generality in supposing that $J \in \bar{G}$, hence $J = s(J) \in G$.

Proposition 8.4.1. *One has $A_{ess} = W(\mathbb{F})I_2$.*

Proof — Indeed, $A_{\mathrm{ess}} = \sum_{\bar{g} \in \bar{S}} W(\mathbb{F})\mathrm{tr}\,(\bar{g}L_2)$. But the only such $\bar{g}$ in the diagonal subgroup $\overline{G}$ are of the form λJ and possibly $-J$, so $W(\mathbb{F})\mathrm{tr}\,(\bar{g}L_2) = W(\mathbb{F})\mathrm{tr}\,(s(\lambda)JIL_2) = W(\mathbb{F})I_2$. □

Proposition 8.4.2. *Assume that A is a domain and is not a finite $W(\mathbb{F})$-module. Then if $(\Pi, \bar{\rho}, t, d)$ is not virtually abelian, A_{ess} is not a finite $W(\mathbb{F})$-module.*

Proof — Since $A = W(\mathbb{F}) \oplus W(\mathbb{F})I_1 + W(\mathbb{F})P$ (Prop. 6.3.4), either $W(\mathbb{F})I_1$ or $W(\mathbb{F})P$ is not finite as a $W(\mathbb{F})$-module. If $W(\mathbb{F})I_1$ is not finite, then neither is $W(\mathbb{F})I_1^2$ since A is a domain, and since $I_1^2 \subset P$, neither is $W(\mathbb{F})P$. So in any case $W(\mathbb{F})P$ is not finite as a $W(\mathbb{F})$-module.

Under our hypotheses $A_{\mathrm{ess}} = W(\mathbb{F})I_2$ is not zero by Prop. 8.3.2. Since $PI_2 \subset I_2$, and A is a domain, $W(\mathbb{F})I_2$ is not finite as a $W(\mathbb{F})$-module. □

Theorem 8.4.3. *Assume that the character χ_1/χ_2 is not of order 2, or in other words that the projective image of $\bar\rho$ is not $\mathbb{Z}/2\mathbb{Z}$. Then A_{ess} is an ideal of A, and more precisely it is the reducibility ideal of the pseudo-representation (t,d) (see* [3, §1.5]*).*

Proof — By Theorem 6.5.1, one has $W(\mathbb{F})L = \begin{pmatrix} \tilde I_1 & B \\ C & \tilde I_1 \end{pmatrix}^0$ for some $W(\mathbb{F})$-module $\tilde I_1$. It follows that $W(\mathbb{F})I_2 = BC$. □

8.5. **The essential subgroup in the dihedral case.** In this subsection we still assume that A is local and we fix an admissible weakly odd pseudo-deformation $(\Pi, \bar\rho, t, d)$, and we assume throughout that

(8.5.1) *The projective image of $\bar\rho$ is dihedral.*

As in §6.3.3, we choose a well-adapted (t,d)-representation $\rho : \Pi \to \mathrm{GL}_2(A)$ which encompasses the choice of a subgroup D of index 2 in $\bar G$ consisting of diagonal matrices. We recall that the inverse image of D by the map $G \mapsto \bar G$ is an index 2 subgroup G' of G, and that $R' = AG'$ is a sub-GMA of $R = M_2(A)$ which has the from $R' = \left(\begin{smallmatrix} A & B \\ B & A \end{smallmatrix}\right)$ for B an ideal of A.

8.5.1. *Largeness of A_{ess}.*

Proposition 8.5.1. *Assume that A is a domain and is not a finite $W(\mathbb{F})$-module, that $(\Pi, \bar\rho, t, d)$ is not virtually abelian, and* (8.5.1)*. Then A_{ess} is not a finite $W(\mathbb{F})$-module.*

Proof — We first claim that $W(\mathbb{F})B_1$ is not a finite $W(\mathbb{F})$-module. Indeed, it is non-zero otherwise $(\Pi, \bar\rho, t, d)$ would be virtually abelian. Moreover, $W(\mathbb{F})I_1 + W(\mathbb{F})P + W(\mathbb{F})B_1$ is not a finite $W(\mathbb{F})$-module. Therefore at least one of the three terms is not a finite $W(\mathbb{F})$-module. If it is the third, then we are done, and if it is one of the two first, we are also done since $I_1B_1 \subset B_1$ and $PB_1 \subset B_1$.

The proposition then follows from Prop. 8.3.3 □

8.5.2. *Description of A_{ess} in the case $4 \mid n$, $n > 4$.* Let n be the order of the projective image of $\bar\rho$. Since $\bar\rho$ is dihedral, $n \geq 4$ and n is even.

(8.5.2) *We assume that $n > 4$, and that $4 \mid n$.*

Under this assumption, the image of the diagonal group D in $\mathrm{PGL}_2(\mathbb{F})$ has even order, and thus contains an element of order 2. Fix a lift $\bar g$ of that element in D. This element $\bar g$ has trace zero, hence is of the form λJ for some $\lambda \in \mathbb{F}^*$, and is an element of $\bar S$. An element of $\overline{G} - D$ also has trace 0. We shall make the following supplementary assumption:

(8.5.3) *There exists an element $\bar g'$ of $\overline{G} - D$ such that $-\det \bar g'$ is a square in $\mathbb{F}^*$, or in other words, such that $\bar g' \in \bar S$.*

This assumption will be harmless in the applications (see §10 below), since if not true, we can always choose an element $\bar g'$ in $\overline{G} - D$ and extend the scalars from $\mathbb{F}$ to the quadratic extension $\mathbb{F}'$ of $\mathbb{F}$ generated by $\sqrt{-\det \bar g'}$.

Theorem 8.5.2. *Assume* (8.5.1), (8.5.2) *and* (8.5.3). *Then* $A_{ess} = \mathfrak{m}B$. *In particular* A_{ess} *is an ideal of* A.

Proof — Since $n > 4$, $W(\mathbb{F})L = \begin{pmatrix} W(\mathbb{F})I_1 & W(\mathbb{F})B_1 \\ W(\mathbb{F})B_1 & W(\mathbb{F})I_1 \end{pmatrix}^0$ by Theorem 6.7.1. It follows that $W(\mathbb{F})L_2 = \begin{pmatrix} W(\mathbb{F})B_1^2 & W(\mathbb{F})I_1B_1 \\ W(\mathbb{F})I_1B_1 & W(\mathbb{F})B_1^2 \end{pmatrix}^0$.

We claim that

$$A_{\text{ess}} = W(\mathbb{F})B_1^2 + W(\mathbb{F})I_1B_1.$$

Indeed, $W(\mathbb{F})\text{tr}\,(s(\bar{g})L_2) = W(\mathbb{F})I_2 = W(\mathbb{F})B_1^2 \subset A_{\text{ess}}$, and $W(\mathbb{F})\text{tr}\,(s(\bar{g}')L_2) = W(\mathbb{F})I_1B_1 \subset A_{\text{ess}}$, and if there are other elements $\bar{g}''$ in $\bar{S}$, they are either diagonal or anti-diagonal, contributing the same summand $W(\mathbb{F})B_1^2$ or $W(\mathbb{F})I_1B_1$.

To prove that A_{ess} is an ideal, we recall that $A = W(\mathbb{F}) + W(\mathbb{F})I_1 + W(\mathbb{F})I_1^2 + W(\mathbb{F})B_1$, so we only need to check that A_{ess} is stable by multiplication by I_1 and B_1. We have $I_1A_{\text{ess}} = W(\mathbb{F})I_1B_1^2 + W(\mathbb{F})I_1^2B_1$, and since $I_1B_1 \subset B_1$, we see that $I_1A_{\text{ess}} \subset A_{\text{ess}}$. We have $B_1A_{\text{ess}} = W(\mathbb{F})B_1^3 + W(\mathbb{F})I_1B_1^2$, and since $W(\mathbb{F})B_1^2 \subset W(\mathbb{F})I_1$ and $I_1B_1 \subset B_1$, we see that $B_1A_{\text{ess}} \subset A_{\text{ess}}$.

Since $B_1 \subset B$ and B is an A-ideal, it is clear that $A_{\text{ess}} \subset B$. We claim that the ideal (of A) generated by B_1 is B.

Since A_{ess} is an ideal, we get $A_{\text{ess}} = B^2 + I_1B$. Since $\mathfrak{m} = W(\mathbb{F})I_1 + W(\mathbb{F})I_1^2 + B$, we have $\mathfrak{m}B = I_1B + I_1^2B + B^2 = A_{\text{ess}} + I_1^2B$. But since B is an ideal, $I_1B \subset B$ and $I_1^2B \subset I_1B \subset A_{\text{ess}}$, so $\mathfrak{m}B = A_{\text{ess}}$. □

8.6. **The essential subgroup in the large image or exceptional case.** We assume that A is local, and we assume that $\bar{\rho}$ has large or exceptional projective image. In this case, things are pretty simple:

Theorem 8.6.1. *If* $\bar{\rho}$ *has large or exceptional projective image, then* $A_{ess} = \mathfrak{m}^2$.

Proof — By Theorem 6.8.1, one has for a suitable (t, d)-representation ρ, $W(\mathbb{F})L = \begin{pmatrix} \mathfrak{m} & \mathfrak{m} \\ \mathfrak{m} & \mathfrak{m} \end{pmatrix}^0$. Since $\begin{pmatrix} \mathfrak{m} & \mathfrak{m} \\ \mathfrak{m} & \mathfrak{m} \end{pmatrix}^0$ is invariant by any trace-preserving automorphism of R, it follows that $W(\mathbb{F})L = \begin{pmatrix} \mathfrak{m} & \mathfrak{m} \\ \mathfrak{m} & \mathfrak{m} \end{pmatrix}^0$ for *any* (t, d)-representation ρ. For any $g \in S$ we therefore have $W(\mathbb{F})\text{tr}\,(gL_2) = W(\mathbb{F})I_2 = \mathfrak{m}^2$, and $A_{\text{ess}} = \mathfrak{m}^2$. □

9. An example

The aim of this section is to provide an example of an admissible pseudo-representation whose image is 'complicated', and which violates the conclusions (and of course, the hypotheses) of certain theorems we have proved earlier. It can be safely skipped.

Let $\mathbb{F}$ be a finite field of characteristic $p > 2$. Let $A = \mathbb{F}[[X]]$, with maximal ideal $\mathfrak{m} = X\mathbb{F}[[X]]$.

9.1. **A two-generator closed subgroup Γ of $SL_2^1(A)$ and its Lie algebra.** Define

$$g = \begin{pmatrix} X+\sqrt{1+X^2} & 0 \\ 0 & -X+\sqrt{1+X^2} \end{pmatrix} \text{ and } h = \begin{pmatrix} \sqrt{1-X^2} & X \\ -X & \sqrt{1-X^2} \end{pmatrix}.$$

Note that those two matrices belongs to $\mathrm{SL}_2^1(A)$. Let Γ be the topological closure of the subgroup of $SL_2^1(A)$ generated by g and h.

Lemma 9.1.1. *With $J = \left(\begin{smallmatrix} 1 & 0 \\ 0 & -1 \end{smallmatrix}\right)$, one has $JgJ = g$ and $JhJ = h^{-1}$. One has $J\Gamma J = \Gamma$. With $J' = \left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)$, one has $J'gJ' = g^{-1}$ and $J'hJ' = h^{-1}$. One has $J'\Gamma J' = \Gamma$.*

Proof — The first and third sentences consist of two trivial computations each and the second and fourth sentences follow. □

Lemma 9.1.2. *Suppose that $\gamma = \begin{pmatrix} a(X) & b(X) \\ c(X) & d(X) \end{pmatrix}$ is in Γ. Then $a(X) = d(-X)$ and $b(X) = c(-X)$.*

Proof — The equalities $a(X) = d(-X)$ and $b(X) = c(-X)$ are clearly true for the matrices g and h, and also g^{-1} and h^{-1}. If these equalities are true for $\gamma = \begin{pmatrix} a(X) & b(X) \\ c(X) & d(X) \end{pmatrix}$ and $\gamma' = \begin{pmatrix} a'(X) & b'(X) \\ c'(X) & d'(X) \end{pmatrix}$, then $\gamma\gamma' = \begin{pmatrix} aa'+bc' & ab'+bd' \\ a'c+c'd & dd'+b'c \end{pmatrix}$ and one sees that $(aa' + bc')(X) = a(X)a'(X) + b(X)c'(X) = d(-X)d'(-X) + c(-X)b'(-X) = (dd' + b'c)(-X)$, and $(ab' + bd')(X) = a(X)b'(X) + b(X)d'(X) = d(-X)c'(-X) + c(-X)a'(-X) = (a'c + c'd)(-X)$. Therefore they are true for any element of the subgroup generated by g and h, and of its closure, hence the lemma. □

Define a subspace L of R as follows:

$$L = \{\left(\begin{smallmatrix} a & b \\ c & -a \end{smallmatrix}\right), a, b, c \in \mathfrak{m} = X\mathbb{F}[[X]],\ a(X) = -a(-X),\ b(X) = c(-X)\}.$$

In other words, $L = X\mathbb{F}[[X^2]]J \oplus \nabla$, with $\nabla = \{\left(\begin{smallmatrix} 0 & b \\ c & 0 \end{smallmatrix}\right), b, c \in \mathfrak{m} = X\mathbb{F}[[X]],\ b(X) = c(-X)\}$. In particular, L is decomposable, but not strongly decomposable.

Lemma 9.1.3. *The Pink's Lie algebra $L(\Gamma)$ of Γ is L.*

Proof — First we prove that $L(\Gamma) \subset L$. It suffices to prove that $\Theta(\gamma) \in L$ for every $\gamma \in \Gamma$. If $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$, then by Lemma 9.1.2, $a(X) = d(-X)$ and $b(X) = c(-X)$, and $\Theta(\gamma) = \begin{pmatrix} (a(X)-a(-X))/2 & b(X) \\ c(X) & (a(X)-a(-X))/2 \end{pmatrix}$, which is clearly in L.

Next, observe that by Lemma 9.1.1, $L(\Gamma)$ is decomposable. We write $L(\Gamma) = I_1 J \oplus \nabla_1$, with ∇_1 anti-diagonal. Also, $\Theta(g) = \begin{pmatrix} X/2 & 0 \\ 0 & -X/2 \end{pmatrix}$ belongs to $L(\Gamma)$, so $X \in I_1$ and $4\mathrm{tr}\,(\Theta(g)^2) = X^2$ belongs to the closed sub-pseudoring $P(\Gamma)$ of A. It follows that $X^2\mathbb{F}[[X^2]] \subset P(\Gamma)$. Since I_1 is stable by $P(\Gamma)$, we get $I_1 = X\mathbb{F}[[X^2]]$. From $\Theta(h) \in L(\Gamma)$ and $L(\Gamma)$ decomposable, we get $\left(\begin{smallmatrix} 0 & X \\ -X & 0 \end{smallmatrix}\right) \in \nabla_1$. Since ∇_1 is stable by taking the Lie bracket with $XJ \in L(\Gamma)$, we see that $\left(\begin{smallmatrix} 0 & X^2 \\ X^2 & 0 \end{smallmatrix}\right)$, $\left(\begin{smallmatrix} 0 & X^3 \\ -X^3 & 0 \end{smallmatrix}\right)$, etc. belong to ∇_1, and finally $\nabla_1 = \{\left(\begin{smallmatrix} 0 & b \\ c & 0 \end{smallmatrix}\right), b, c \in \mathfrak{m} = X\mathbb{F}[[X]],\ b(X) = c(-X)\}$. Hence $L(\Gamma) = L$. □

9.2. **Construction of two admissible pseudo-deformations.** We define

$$G = \Gamma \coprod J\Gamma.$$

It follows from the first part of Lemma 9.1.1 that G is a closed subgroup of $\mathrm{GL}_2(A)$, containing Γ as a subgroup of order 2, and that G is the semi-direct product of $\{1, J\}$ by Γ.

Let Π be any pro-finite group with a continuous surjective morphism onto G (for example $\Pi = G$ with the identity). Let ρ be the composition $\Pi \to G \to \mathrm{GL}_2(A)$. Let $t = \mathrm{tr}\,\rho$, $d = \det \rho$. Let $\bar{\rho} : \Pi \to \mathrm{GL}_2(\mathbb{F})$ be the reduction modulo $\mathfrak{m}$ of ρ. Then $\bar{\rho}$ is a continuous semi-simple representation of Π with image (and projective image) isomorphic to $\mathbb{Z}/2\mathbb{Z}$.

Lemma 9.2.1. *$(\Pi, \bar{\rho}, t, d)$ is an admissible pseudo-deformation. The projective image of $\bar{\rho}$ is cyclic of order 2.*

Proof — The representation $\bar{\rho}$ is the sum of the trivial character and a character of order 2 of Π, so $\bar{\rho}$ satisfies (5.2.2). The property (5.2.3) is obvious. One has $d(\Gamma) = 1$, $d(G - \Gamma) = d(J\Gamma) = -1$, which makes clear that (5.2.4) holds. For (5.2.5), one has $\mathrm{tr}\,(Jg) = 2X$, hence the smallest closed subring of A containing $\mathrm{tr}\,(G)$ contains $\mathbb{F}[X]$, hence is A. □

Let H be the subgroup of order 8 of $\mathrm{GL}_2(A)$ generated by J and J'. By Lemma 9.1.1, H normalizes Γ. We define $G' = \Gamma H$, a semi-direct product of H by Γ. Let Π' be any pro-finite group with a continuous surjective morphism onto G' (for example $\Pi' = G'$ with the identity). Let ρ' be the composition $\Pi' \to G' \to \mathrm{GL}_2(A)$. Let $t' = \mathrm{tr}\,\rho'$, $d' = \det \rho'$. Let $\bar{\rho}' : \Pi' \to \mathrm{GL}_2(\mathbb{F})$ be the reduction modulo $\mathfrak{m}$ of ρ'. Then $\bar{\rho}'$ is a continuous semi-simple representation of Π' with image isomorphic to H.

Lemma 9.2.2. *$(\Pi', \bar{\rho}', t', d')$ is an admissible pseudo-deformation. The projective image of $\bar{\rho}'$ is dihedral of order 4.*

Proof — The proof if the same as above, except for the projective image, which is the image of H in $\mathrm{PGL}_2(\mathbb{F})$. This image is generated by the image of J and J', elements of order 2 that commute in $\mathrm{PGL}_2(\mathbb{F})$ since in $\mathrm{GL}_2(\mathbb{F})$ one has $J'JJ' = -J$. □

9.3. **Counter-examples to over-optimistic statements.** We now use the admissible pseudo-deformations $(\Pi, \bar{\rho}, t, d)$ and $(\Pi', \bar{\rho}', t', d')$ to construct counter-examples.

First, we show that Theorem 7.2.3 is false if we do not assume that $\bar{\rho}$ is regular. More precisely, we show that it does not hold true, first in a case where $\bar{\rho}$ has projective image cyclic of order 2, and second in a case where it has projective image dihedral of order 4.

Proposition 9.3.1. *Let $(\Pi, \bar{\rho}, t, d)$ be the admissible pseudo-deformation constructed in the above subsection. There is no subgroup Π_0 of Π containing $\mathrm{Ker}\,\bar{\rho}$, and subring A_0 of A such that the pseudo-representation (t, d) of Π_0 takes value in A_0, is admissible,*

and $(t_{|\Pi_0}, d_{\Pi_0})$ *has congruence-large image. The same holds with* $(\Pi, \bar\rho, t, d)$ *replaced by* $(\Pi', \bar\rho', t', d')$ *constructed in the above subsection.*

Proof — If Π_0 is a subgroup as in the statement, then either $\Pi_0 = \Pi$ or $\Pi_0 = \operatorname{Ker}\bar\rho$ has index 2 in Π. The second case is excluded since $\bar\rho_{|\operatorname{Ker}\bar\rho}$ is the trivial representation of dimension 2, which is not multiplicity free. Thus $\Pi_0 = \Pi$ and $A_0 = A$. We just have to show that for the unique (t, d)-representation ρ, $\rho(\Pi_0) = G$ does not contain any congruence subgroup. But if it did, Γ would contain a congruence subgroup and L would contain a sub-module of the form $\begin{pmatrix} I & I \\ I & I \end{pmatrix}^0$ for some non-zero ideal I of A. Since up-left coefficients of L are odd elements of $\mathbb{F}[[X]]$, I would contain only odd functions, but this is absurd since I is stable by multiplication by X.

The same result for $(\Pi', \bar\rho', t', d')$ is proved similarly. □

Second, we show that it may be false that A_{ess} is an ideal of A.

Proposition 9.3.2. *The* $\mathbb{Z}_p$*-submodule* A_{ess} *of* A *attached to the admissible pseudo-deformation* $(\Pi_0, \bar\rho, t, d)$ *is not an ideal of* A*.*

Proof — By Prop. 8.4.1 we have $A_{\text{ess}} = I_2 \subset I_1$. Since I_1 consists of odd elements of $A = \mathbb{F}_p[[X]]$, so does I_2, but no non-zero ideal of A consists only of odd elements. □

9.4. **The group G as a Galois group.** Lest the reader think that the pathological example $(\Pi, \bar\rho, t, d)$ is allowed only by our too lenient definition of an admissible representation, and does not happen in the concrete applications to number theory, we show that when $p = 3$ (to fix ideas) one can take in the above example for Π the absolute Galois group $G_{\mathbb{Q},3}$ and for (t, d) the quotient by a prime ideal of height one of the canonical pseudo-representation of $G_{\mathbb{Q},3}$ over the Hecke algebra of modular forms modulo 3.

Let $G_{\mathbb{Q}(\mu_3),3}$ be the Galois group of the maximal algebraic extension of $\mathbb{Q}(\mu_3) = \mathbb{Q}(\sqrt{-3})$ unramified outside the unique place above 3. This is a subgroup of order 2 of $G_{\mathbb{Q},3}$, and $G_{\mathbb{Q},3}$ is a semi-direct product of $\{1, c\}$, where c is any complex conjugation, by $G_{\mathbb{Q}(\mu_3),3}$.

Let $G^3_{\mathbb{Q}(\mu_3),3}$ be the largest quotient of $G_{\mathbb{Q}(\mu_3),3}$ which is a pro-3-group. The structure of that group is known. Let c be a complex conjugation in $G_{\mathbb{Q},3}$.

Lemma 9.4.1. *There exists an element* $x \in G^3_{\mathbb{Q}(\mu_3),3}$ *such that* $G^3_{\mathbb{Q}(\mu_3),3}$ *is a free pro-3-group with* x *and* cxc *as pro-generators.*

The freeness of $G^3_{\mathbb{Q},3}$ is due to Shafarevich, see [30, page 82, example after theorem 5]. The rest of the lemma is proven in [22].

Consider the unique continuous morphism of groups $f : G^3_{\mathbb{Q}(\mu_3),3} \to \Gamma$ sending x to $(gh)^{1/2}$ and cxc to $(gh^{-1})^{1/2}$ (the square root $z^{1/2}$ for z an element of the pro 3-group Γ is defined as usual as the limit z^{a_n} where a_n is a sequence of natural integers converging 3-adically to 1/2). Since the group generated by $(gh)^{1/2}$ and $(gh^{-1})^{1/2}$ contains g and h, f is surjective. Using the structural surjective map $G_{\mathbb{Q}(\mu_3),3} \to G^3_{\mathbb{Q}(\mu_3),3}$, we see f as a

surjective morphism $G_{\mathbb{Q}(\mu_3),3} \to \Gamma$. Since $f(cxc) = Jf(x)J^{-1}$ in G by Lemma 9.1.1, and $J^2 = c^2 = 1$, we can extend f into a surjective morphism $f : G_{\mathbb{Q},3} \to G$ sending c onto J. We thus get a pseudo-character $(t = \mathrm{tr} \circ f, d = \det \circ f)$ on the Galois group $\Pi = G_{\mathbb{Q},3}$ which is an admissible pseudo-deformation of $\bar{\rho} = 1 \oplus \omega_3$ and whose image is G. As seen above, this Galois pseudo-deformation is a counter-example to the assertion that A_{ess} is an ideal and that (t, d) has congruence-large image.

Finally, note that if $R_{\bar{\rho}}$ denotes the universal deformation of $\bar{\rho}$ as a pseudo-representation in characteristic p and with constant determinant, and $A_{\bar{\rho}}$ denotes the Hecke algebra of modular forms modulo 3 and level 1, the natural map $R_{\bar{\rho}} \to A_{\bar{\rho}}$ is an isomorphism by [22], and both rings are isomorphic to $\mathbb{F}_3[[Y, Z]]$. Thus, the pseudo-deformation (t, d) induces a surjective map $R_{\bar{\rho}} = A_{\bar{\rho}} \to A = \mathbb{F}_3[[X]]$, such that (t, d) is the composition of the natural pseudo-character $(t_{\bar{\rho}}, d_{\bar{\rho}})$ with this map.

10. Density of modular forms

In this section we prove the main results of our work, the ones regarding the density of modular forms, namely Theorems I, II and III.

We revert to the notation of the introduction: p is prime, $N \geq 1$ an integer, $k \in \mathbb{Z}/(p-1)\mathbb{Z}$ and $\mathbb{F}$ a (large enough) finite extension of $\mathbb{F}_p$. The space of modular forms on $\mathbb{F}$ of weight k, level N, and coefficients null at indices not prime to Np is denoted by $\mathcal{F}$. We note that to prove Theorems I, II and III, we can without loss of generality replace $\mathbb{F}$ by a finite extension. We shall always assume that the finite field $\mathbb{F}$ is large enough below.

10.1. **The Hecke algebra of mod p modular forms.** The space $\mathcal{F}$ is endowed with an action of the Hecke operators T_ℓ for $\ell \nmid Np$. Let $A = A_k(N, \mathbb{F})$ be the topological closure[6] of the $\mathbb{F}$-subalgebra of $\mathrm{End}_{\mathbb{F}}(\mathcal{F})$ generated by the Hecke operators T_ℓ for ℓ not dividing Np.

For every $k \in \mathbb{Z}/(p-1)\mathbb{Z}$, the $\mathbb{F}$-algebra $A = A_k(N, \mathbb{F})$ is *semi-local*. More precisely, if $\mathbb{F}$ is large enough, its maximal ideals are in bijection with a certain set $\mathcal{R} = \mathcal{R}(k, N, \mathbb{F})$ of semi-simple continuous Galois representations $\bar{\rho} : G_{\mathbb{Q},Np} \to \mathrm{GL}_2(\mathbb{F})$ up to $\mathbb{F}$-isomorphism: the correspondence is given by $\lambda_\ell = \mathrm{tr}\, \bar{\rho}(\mathrm{Frob}_\ell)$. This set $\mathcal{R}(k, N, \mathbb{F})$ can be described as the set of all semi-simple representations $\bar{\rho} : G_{\mathbb{Q},Np} \to \mathrm{GL}_2(\mathbb{F})$ of determinant ω_p^{k-1} and Serre's level N. This is the content of Serre's conjecture, now a theorem of Khare and Wintenberger.

Still assuming that $\mathbb{F}$ is large enough, and $\bar{\rho} \in \mathcal{R}(k, N, \mathbb{F})$, we shall denote by $A_{\bar{\rho}}$ the corresponding local component of $A = A_k(N, \mathbb{F})$, that is the localization of $A_k(N, \mathbb{F})$ at the maximal ideal corresponding to $\bar{\rho}$. The generalized eigenspace $\mathcal{F}_{\bar{\rho}} = \mathcal{F}_{\bar{\rho}}(N, \mathbb{F})$ for the T_ℓ, $\ell \nmid Np$, with generalized eigenvalues λ_ℓ (already considered defined in the introduction) is equivalently the localization of the $A = A_k(N, \mathbb{F})$-module $\mathcal{F} = \mathcal{F}_k(N, \mathbb{F})$ at that maximal ideal $\mathfrak{m}_{\bar{\rho}}$ corresponding to $\bar{\rho}$.

Then, $A_{\bar{\rho}}(\mathbb{F})$ is a compact local $\mathbb{F}$-algebra with residue field $\mathbb{F}$. The image of the elements T_ℓ of A in that localization $A_{\bar{\rho}}$ shall also by denoted by T_ℓ. The image of $T_\ell \in A_{\bar{\rho}}$ in the

[6]The topology on $\mathcal{F}$ is the discrete topology and the topology on $\mathrm{End}_{\mathbb{F}}(\mathcal{F})$ is the compact-open topology

residue field $\mathbb{F}$ is $\mathrm{tr}\,(\bar\rho(\mathrm{Frob}_\ell)) = \lambda_\ell$. Equivalently, the $A_{\bar\rho}$-module $\mathcal{F}_{\bar\rho}$ can be described as the generalized eigenspace in $\mathcal{F}_k(\mathbb{F})$ for the T_ℓ, $\ell \nmid Np$, with generalized eigenvalues λ_ℓ. To summarize, we have decompositions

$$A = \prod_{\bar\rho\in\mathcal{R}} A_{\bar\rho}, \quad \mathcal{F} = \bigoplus_{\bar\rho\in\mathcal{R}} \mathcal{F}_{\bar\rho}. \tag{2}$$

Recall that we have a perfect pairing $\mathcal{F}\times A\to\mathbb{F}$, $(f,t)\mapsto a_1(tf)$, which induces a perfect pairing $\mathcal{F}_{\bar\rho}\times A_{\bar\rho}\to\mathbb{F}$.

We note that the ring A thus satisfies all hypotheses made in Section 8. Moreover we have the following results on the structure of A:

Proposition 10.1.1. *The rings $A_{\bar\rho}$ are always infinite, and have Krull dimension ≥ 1. If $p>3$, or if $p=3$ and $\bar\rho$ is a twist of $1\oplus\omega_3$ (ω_3 the cyclotomic character), or if $p=2$ and $\bar\rho$ is a twist of $1\oplus 1$, the Krull dimension of $A_{\bar\rho}$ is at least 2.*

Proof — See [13] for the first assertion, [4] and [10] for the case $p>3$ and [21] in the case $p=3$, [24] in the case $p=2$. □

It is expected that $A_{\bar\rho}$ always has dimension exactly 2, and this is known in many cases, see the references above.

10.2. **The canonical Galois pseudo-representation over A.**

Proposition 10.2.1. *There exists a unique continuous pseudo-representation (t,d) of dimension 2 of $G_{\mathbb{Q},Np}$ with values in A such that $t(\mathrm{Frob}_\ell) = T_\ell$ for all $\ell\nmid Np$. One has $d=\omega_p^{k-1}$ and $t(c)=0$.*

For a proof of the proposition, which is well-known to specialists, see [2] where the case $p=2$ is dealt with – the case $p>2$ is exactly the same. We denote by $(t_{\bar\rho}, d_{\bar\rho})$ the composition of (t,d) with the map $A\to A_{\bar\rho}$, and observe that by definition, $t_{\bar\rho} = \mathrm{tr}\,\bar\rho \pmod{\mathfrak{m}_{\bar\rho}}$ and $d_{\bar\rho} = \det\bar\rho \pmod{\mathfrak{m}_{\bar\rho}}$.

Corollary 10.2.2. *The pseudo-deformation $(G_{\mathbb{Q},Np}, (\bar\rho_i)_{i=1,\dots,r}, t, d)$ is admissible.*

Proof — Condition (5.2.1) is trivial. The hypothesis (5.2.2) is satisfied because the representations $\bar\rho_i$ are odd, hypotheses (5.2.3) and (5.2.4) are clear, and (5.2.5) follows from the fact that $t(G_{\mathbb{Q},Np})$ contains T_ℓ for all prime ℓ not dividing Np and those operators, by construction, generates A as an $\mathbb{F}$-algebra. □

Corollary 10.2.3. *The ring A is noetherian.*

Proof — Since $G_{\mathbb{Q},Np}$ satisfies the p-finiteness condition ([18]), this follows from the preceding corollary and Cor. 5.3.2. □

We observe that if $p = 2$, the ideal generated by all the T_ℓ, $\ell \nmid Np$, in A is the maximal ideal. It is also the orthogonal of the eigenform Δ, which is up to a scalar the only form in $\mathcal{F}_k(\mathbb{F})$ killed by all Hecke operators. We shall denote that ideal by $\mathfrak{m}_1$ since it is the maximal ideal of A corresponding to the trivial representation $\bar{\rho} = 1 \oplus 1$.

Lemma 10.2.4. *The closed $\mathbb{F}$-subspace generated by $t(G_{\mathbb{Q},Np})$ is A when $p > 2$ and $\mathfrak{m}_1$ when $p = 2$.*

Proof — When $p > 2$, the lemma is just (5.3.1). When $p = 2$, the same argument gives that the closed $\mathbb{F}$-subspace generated by $t(G_{\mathbb{Q},Np})$ is an ideal, and contains all the T_ℓ, $\ell \nmid Np$. Thus it is $\mathfrak{m}_1$ or A. But $t(G_{\mathbb{Q}_{Np}}) \subset \mathfrak{m}_1$ because $t \pmod{\mathfrak{m}_1} = \mathrm{tr}\,(1+1) = 0$. □

10.3. **Proof of Theorem I.** We now give the proof of Theorem I. Let $f \in \mathcal{F}_k(\mathbb{F})$, $f \neq 0$. If $p = 2$ we assume in addition that $f \notin \mathbb{F}\Delta'$. We want to show that $\delta(f) > 0$.

Let l_f be the $\mathbb{F}$-linear form on $A_k(\mathbb{F})$ defined by $l_f(T) = a_1(Tf)$. In other words, l_f is the linear form on $A_k(\mathbb{F})$ corresponding to $f \in \mathcal{F}_k(\mathbb{F})$ through the perfect duality $A_k(\mathbb{F}) \times \mathcal{F}_k(\mathbb{F}) \to \mathbb{F}$, $(T, f) \mapsto a_1(Tf)$, and in particular, l_f is non-zero. Let H_f be the closed hyperplane $\mathrm{Ker}\, l_f$ of $A_f(\mathbb{F})$. If $p = 2$, our supplementary assumption means that H_f is not the maximal ideal $\mathfrak{m}_1$.

If μ denotes the Haar measure of total mass 1 on the compact group $G_{\mathbb{Q},Np}$, we claim that

$$(10.3.1)\ \ \delta(f) = 1 - \mu(t^{-1}(H_f)).$$

To prove the claim, note that for ℓ a prime not dividing Np, one has $a_\ell(f) = 0 \Leftrightarrow a_1(T_\ell f) = 0 \Leftrightarrow a_1(t(\mathrm{Frob}\,\ell)f) = 0 \Leftrightarrow t(\mathrm{Frob}_\ell) \in H_f \Leftrightarrow \mathrm{Frob}_\ell \in t^{-1}(H_f)$. Observe that H_f, being closed and of finite index, is open in A_f, and therefore $t^{-1}(H_f)$ is open in $G_{\mathbb{Q},Np}$. Thus Chebotarev's density theorem implies that the density of primes ℓ such that Frob_ℓ is not in $t^{-1}(H_f)$ is $1 - \mu(t^{-1}(H_f))$, and the claim follows.

To finish the proof, we therefore just have to prove that $t^{-1}(H_f)$ is a proper subset of $G_{\mathbb{Q},Np}$. We do not have $t^{-1}(H_f) = G_{\mathbb{Q},Np}$, because that would mean $t(G_{\mathbb{Q},Np}) \subset H_f$, contradicting Lemma 10.2.4. This completes the proof of Theorem I.

10.4. **Definition of special modular forms.** *From now on, we assume $p > 2$.* The admissible pseudo-deformation $(G_{\mathbb{Q},Np}, (\bar{\rho}_i), t, d)$ over A defines a closed $\mathbb{F}$-subspace A_{ess} of A (cf. §8). We say that a modular form $f \in \mathcal{F}$ is *special* if $a_1(tf) = 0$ for all $t \in A_{\mathrm{ess}}$. Thus, special modular forms in $\mathcal{F}$ form a $\mathbb{F}$-sub-vector space $\mathcal{F}_{\mathrm{spe}}$, which is the orthogonal of A_{ess} for the perfect pairing $A \times \mathcal{F} \to \mathbb{F}$.

For $\bar{\rho} \in \mathcal{R}$, we set as in the introduction $\mathcal{F}_{\bar{\rho},\mathrm{spe}} = \mathcal{F}_{\bar{\rho}} \cap \mathcal{F}_{\mathrm{spe}}$. The admissible pseudo-deformation $(G_{\mathbb{Q},Np}, \bar{\rho}, t_{\bar{\rho}}, d_{\bar{\rho}})$ over $A_{\bar{\rho}}$ defines a closed $\mathbb{F}$-subspace $A_{\bar{\rho},\mathrm{spe}}$ of $A_{\bar{\rho}}$, which is the image of A_{spe} by the projection map $A \to A_{\bar{\rho}}$. Thus, $\mathcal{F}_{\bar{\rho},\mathrm{spe}}$ is the orthogonal complement of $A_{\bar{\rho},\mathrm{ess}}$ for the perfect pairing $A_{\bar{\rho}} \times \mathcal{F}_{\bar{\rho}} \to \mathbb{F}$.

10.5. **Proof of Theorem III.** Given a representation $\bar{\rho} \in \mathcal{R}$ (which in the case $p = 3$ is a twist of $1 \oplus \omega_3$), we need to show that $\mathcal{F}_{\bar{\rho},\mathrm{spe}}$ is of infinite codimension in $\mathcal{F}_{\bar{\rho}}$, or equivalently, that $A_{\bar{\rho},\mathrm{ess}}$ is infinite-dimensional.

Proposition 10.5.1. *If $(G_{\mathbb{Q},Np}, \bar{\rho}, t, d)$ is a virtually abelian admissible pseudo-deformation over a noetherian local compact domain A such that $pA = 0$ for some odd prime p, then the Krull dimension of A is at most 1.*

Proof — Let K the fraction field of A. Let $\rho : G_{\mathbb{Q},Np} \to R^*$ be a (t,d)-representation. By Lemma 2.2.3, ρ can be seen as a representation $G_{\mathbb{Q},Np} \to \mathrm{GL}_2(K)$.

Let M be a finite Galois extension of $\mathbb{Q}$ such that (t,d) factors through an abelian quotient of $G_{M,Np}$. The representation $\rho : G_{M,Np} \to \mathrm{GL}_2(K)$ becomes reducible over a quadratic extension K' of K, so there are two characters $\chi_1, \chi_2 : G_{M,Np} \to (K')^*$ such that $\rho = \chi_1 \oplus \chi_2$ as a representation over K'. Since $\chi_i(g)$ for $i = 1, 2$ are the roots of the polynomials $X^2 - t(g)X + d(g) \in A[X]$, $\chi_i(g)$ belongs to the integral closure A' of A in K'. Since A is a complete noetherian local ring, then by a theorem of Nagata, A' is a finite type module over A and is a complete noetherian local ring as well.

We claim that the characters $\chi_i : G_{M,Np} \to (A')^*$ for $i = 1, 2$ are continuous. Indeed, if they are equal they are continuous since $2\chi_1 = t$. If not, there is a g_0 such that $\chi_1(g_0) \neq \chi_2(g_0)$. By the continuity of the roots of polynomial, there exists a neighborhood U of 1 and two continuous functions ψ_1, ψ_2 on g_0U (with values in $(A')^*$) such that $X^2 - t(g)X + d(g) = (X - \psi_1(g))(X - \psi_2(g))$ on g_0U $\psi_i(g_0) = \chi_i(g_0)$ for $i = 1, 2$. Shrinking U if necessary, we may assume that U is an open subgroup of $G_{M,Np}$ and that $g \mapsto \psi_i(gg_0)\chi_i(g_0)^{-1}$ is a character on U. By uniqueness of the decomposition of a representation into sum of characters over a field (K'), it follows that for $i = 1, 2$, there exists $j = 1, 2$ such that $\psi_i(gg_0)\chi_i(g_0)^{-1} = \chi_j(g)$ on U. It follows that the χ_i are continuous on U, hence everywhere.

Let $\Gamma = \mathrm{Gal}(M/\mathbb{Q})$. Since the functions t and $d = \chi_1\chi_2 = \det \bar{\rho}$ on $G_{M,Np}$ are invariant by conjugation of the argument by any element of $\mathrm{Gal}(M/\mathbb{Q})$, there exists a subgroup Γ' of Γ of index 1 or 2 such that

(10.5.1) *for every $\gamma \in \Gamma'$, $\chi_i^\gamma = \chi_i$ and for every $\gamma \in \Gamma - \Gamma'$, $\chi_i^\gamma = \det \bar{\rho}\chi_i^{-1}$.*

Let R_{univ} be the universal deformation ring in characteristic p of the character $\bar{\chi}_1 : G_{M,Np} \to \mathbb{F}^*$ satisfying condition (10.5.1). The character $\chi_1 : G_{M,Np} \to (A')^*$ defines a morphism of $\mathbb{F}$-algebras $R_{\mathrm{univ}} \to A'$ whose image A_0 is the closed $\mathbb{F}$-subalgebra of A' generated by $\chi_1(G_{M,Np})$. For $g \in G_{M,Np}$, we can write $\chi_1(g) = \bar{\chi}_1(g) + x$ with $\bar{\chi}_1(g) \in \mathbb{F}^*$ and x in the maximal ideal of A', and $\chi_2(g) = \det \bar{\rho}(g)(\bar{\chi}_1(g) + x)^{-1} = \bar{\chi}_1(g)(1 - \bar{\chi}_1(g)^{-1}x + \bar{\chi}_2(g)^{-2}x^2 - \dots)$. Thus $\chi_2(g)$ is in A_0, and so is $t(g)$. Since A is the closed $W(\mathbb{F})$-subalgebra generated by the image of t, we see that $A \subset A_0 \subset A'$. Since A' is finite as an A-module, Cohen-Seidenberg's theorem ensures that A, A' and A_0 have the same Krull dimension. Thus to prove the proposition it suffices to prove that A_0 has dimension at most 1, and for this it is enough to prove that R_{univ} has dimension at most 1. This follows easily from Class Field Theory. □

By Prop. 10.1.1, the ring $A_{\bar\rho}$ has Krull dimension at least 2 under the hypothesis on $\bar\rho$ of Theorem III. Let B be the reduced ring of the ring of a 2-dimensional irreducible component of $\operatorname{Spec} A_{\bar\rho}$. Then B is a quotient of $A_{\bar\rho}$, which is domain of dimension 2. To prove that $A_{\bar\rho,\mathrm{ess}}$ is infinite (as a set or $\mathbb{F}$-vector space), it is enough to prove that the image B_{ess} of $A_{\bar\rho,\mathrm{ess}}$ in B is infinite. The subspace B_{ess} is the essential subspace of the admissible pseudo-deformation $(G_{\mathbb{Q},Np},\bar\rho,t,d)$ over B, which is not virtually abelian by the above proposition. Therefore, B_{ess} is infinite by Propositions 8.4.2, 8.5.1, 8.6.1, and Theorem III is proved.

10.6. **Proof of Theorem II.** Let $f\in\mathcal{F}$ be a modular form which is not in $\mathcal{F}_{\mathrm{spe}}$. This means that the linear form $l: A\to\mathbb{F}$, $t\mapsto a_1(tf)$ is not zero on the subspace A_{ess} of A. By Theorem 8.2.1

$$\mu_{G_{\mathbb{Q},Np}}((l\circ t)^{-1}(\mathbb{F}^*))\geq\frac{p-1}{pn},$$

that is by (10.3.1)

$$\delta(f)\geq\frac{p-1}{pn},$$

where $n=|\overline{G}|$. This proves the main part of Theorem II. This theorem also states that $\mathcal{F}_{\mathrm{spe}}$ is of infinite codimension in $\mathcal{F}$. To prove this, it is sufficient to prove that for one $\bar\rho\in\mathcal{R}$, $\mathcal{F}_{\mathrm{spe},\bar\rho}=\mathcal{F}_{\mathrm{spe}}\cap\mathcal{F}_{\bar\rho}$ is of infinite codimension in $\mathcal{F}_{\bar\rho}$. The results follow from Theorem III for any $\bar\rho\in\mathcal{R}$ if $p>3$, and also for $p=3$ if we choose for $\bar\rho$ the representation $1\oplus\omega_3$, which always belong to $\mathcal{R}(N,3,\mathbb{F})$ since it is the representation attached to the eigenform $\Delta\pmod 3$.

11. Cyclotomic and K-abelian modular forms

We keep the notation of the preceding section. We do not assume $p>2$ unless explicitly mentioned. We fix a representation $\bar\rho\in\mathcal{R}$.

For $f\in\mathcal{F}_{\bar\rho}$, we denote by I_f the annihilator ideal of f in $A_{\bar\rho}$, and by A_f the quotient $A_{\bar\rho}/I_f$. The perfect duality $A_{\bar\rho}\times\mathcal{F}_{\bar\rho}\to\mathbb{F}$ induces a perfect duality $A_f\times A_{\bar\rho}f\to\mathbb{F}$. The space $A_{\bar\rho}f$ is finite, because the action of the Hecke operators is locally finite; it follows that the ring A_f is finite, and it is therefore a local artinian $\mathbb{F}$-algebra. We obtain an admissible pseudo-deformation $(G_{\mathbb{Q},Np},\bar\rho,t_f,d_f)$ on A_f by post-composing $t_{\bar\rho}$ and $d_{\bar\rho}$ with the surjective map $A_{\bar\rho}\to A_f$.

11.1. **Fields of determination of a modular form $f\in\mathcal{F}_{\bar\rho}$.** For S a finite set of primes, let us denote by $\mathbb{Q}_S$ the maximal algebraic extension of $\mathbb{Q}$ unramified outside S and ∞, and by $G_{\mathbb{Q},S}$ the group $\mathrm{Gal}(\mathbb{Q}_S/\mathbb{Q})$. If S is the set of primes dividing an integer N, we also use N instead of S in these notations.

Let us denote by L_f the subfield of $\mathbb{Q}_{Np}$ fixed by $\operatorname{Ker}(t_f,d_f)$. Note that L_f is a Galois extension of $\mathbb{Q}$, unramified outside Np and ∞, such that $\mathrm{Gal}(L_f/\mathbb{Q})=G_{\mathbb{Q},Np}/\operatorname{Ker}(t_f,d_f)$.

Lemma 11.1.1. *The field L_f is finite over $\mathbb{Q}$.*

Proof — Let $\rho_f : G_{\mathbb{Q},Np} \to R_f^*$ be a (t_f, d_f)-representation. By assertion (vii) of Proposition 2.4.2, R_f is of finite type as a module over A_f, hence is finite as a set, and by assertion (vi) of the same, the kernel of $\mathrm{Ker}\,(\rho_f)_{|G_{\mathbb{Q},Np}}$ is $\mathrm{Ker}\,(t_f, d_f)$. Therefore, $\mathrm{Gal}(L_f/\mathbb{Q}) = \rho_f(G_{\mathbb{Q},N,p})$ and since the later is a subset of the finite set R_f, it is finite. □

Theorem 11.1.2. *Let L be a Galois extension of $\mathbb{Q}$ contained in $\bar{\mathbb{Q}}$, unramified outside a finite set S of primes dividing Np and ∞. The following properties are equivalent:*

(i) *For every prime $\ell \notin S$, the form $T_\ell f$ depends on ℓ only through the conjugacy class $Frob_{\ell,L/\mathbb{Q}} \in \mathrm{Gal}(L/\mathbb{Q})$.*

(i') *For almost every prime ℓ, the form $T_\ell f$ depends on ℓ only through the conjugacy class $Frob_{\ell,L/\mathbb{Q}} \in \mathrm{Gal}(L/\mathbb{Q})$.*

(ii) *For every prime $\ell \notin S$, the coefficient $a_\ell(f)$ depends on ℓ only through the conjugacy class $Frob_{\ell,L/\mathbb{Q}} \in \mathrm{Gal}(L/\mathbb{Q})$.*

(ii') *For almost every prime ℓ, the coefficient $a_\ell(f)$ depends on ℓ only through the conjugacy class $Frob_{\ell,L/\mathbb{Q}} \in \mathrm{Gal}(L/\mathbb{Q})$.*

(iii) *One has $L_f \subset L$.*

Definition 11.1.3. If L satisfies the conditions of the above theorem, we shall say that L is a *determination field* of f.

Obviously, there is always a smallest determination field, namely L_f, and it is finite over $\mathbb{Q}$ and unramified outside Np. However, it is sometimes convenient to consider also other determination fields.

Proof. We see the pseudo-representation (t_f, d_f) of $\mathrm{Gal}(\mathbb{Q}_{Np}/\mathbb{Q})$ as a pseudo-representation of $\mathrm{Gal}(\mathbb{Q}_S/\mathbb{Q})$ by inflation. Let us call π the surjective map $\mathrm{Gal}(\mathbb{Q}_S/\mathbb{Q}) \to \mathrm{Gal}(L/\mathbb{Q})$. To ease notations, let us denote by Frob_ℓ the element $\mathrm{Frob}_{\ell,\mathbb{Q}_s/\mathbb{Q}}$. Thus $\pi(\mathrm{Frob}_\ell) = \mathrm{Frob}_{\ell,L/\mathbb{Q}}$.

Since $t_f(\mathrm{Frob}_\ell f) = T_\ell f$, the assertion (i) (resp. (i')), is equivalent to

(11.1.1) *$t_f(Frob_\ell)$ depends only on $\pi(Frob_\ell) = Frob_{\ell,L/\mathbb{Q}}$ for all ℓ not in L (resp. for almost all ℓ)*

By Chebotarev's density theorem, both these assertions are equivalent to:

(11.1.2) *The map t_f factors through π,*

which amounts to $\mathrm{Ker}\,\pi \subset \mathrm{Ker}\,t_f$, that is $L_f \subset L$. We thus have proved the equivalence between (i), (i') and (iii).

Since the coefficient a_ℓ of f is the coefficient a_1 of $T_\ell(f)$, it is obvious that (i) implies (ii). Since (ii) obviously implies (ii'), it just remains to prove that (ii') implies (i'). For every prime ℓ not in S, one has

$$a_1(T_f(\mathrm{Frob}_\ell)f) = a_1(T_\ell f) = a_\ell(f),$$

so (ii') means that for almost all ℓ, $a_1(t_f(\mathrm{Frob}_\ell)f)$ depends only on $\mathrm{Frob}_{\ell,L/\mathbb{Q}} = \pi(\mathrm{Frob}_\ell)$. Using Chebotarev, this means that there exists a continuous map $\beta : \mathrm{Gal}(L/\mathbb{Q}) \to \mathbb{F}$ such that

(11.1.3) *for all* $\gamma \in \mathrm{Gal}(\mathbb{Q}_S/\mathbb{Q})$, $a_1(t_f(\gamma)f) = \beta(\pi(\gamma))$.

Let q be a prime number not in S.

$$\begin{aligned} a_q(T_\ell f) &= a_1(T_\ell T_q f) \\ &= a_1(t_f(\mathrm{Frob}_{\ell,\mathbb{Q}_S/\mathbb{Q}})t_f(\mathrm{Frob}_{q,\mathbb{Q}_S/\mathbb{Q}})f) \\ &= a_1(t_f(\mathrm{Frob}_{\ell,\mathbb{Q}_S/\mathbb{Q}}\mathrm{Frob}_{q,\mathbb{Q}_S/\mathbb{Q}}f) + q^{k-1}a_1(t_f(\mathrm{Frob}_{\ell,\mathbb{Q}_S/\mathbb{Q}}\mathrm{Frob}^{-1}_{q,\mathbb{Q}_S/\mathbb{Q}})f) \\ &= \beta(\mathrm{Frob}_{\ell,L/\mathbb{Q}}\mathrm{Frob}_{q,L/\mathbb{Q}}) + q^{k-1}\beta(\mathrm{Frob}_{\ell,L/\mathbb{Q}}\mathrm{Frob}^{-1}_{q,L/\mathbb{Q}}) \end{aligned}$$

Thus the coefficient a_q (for q any prime not in S), as well as the coefficient a_1 of the form $T_\ell f$ depends on ℓ only through $\mathrm{Frob}_{\ell,L/\mathbb{Q}}$. Since by the corollary of Theorem I a modular form is determined by its coefficient at primes (excluding a finite set) and at 1 , it follows that the form $T_\ell f$ itself depends on ℓ only through $\mathrm{Frob}_{\ell,L/\mathbb{Q}}$. In other words, we have proved (i'). □

11.2. **Cyclotomic modular forms.**

Proposition 11.2.1. *Let* $f = \sum_n a_n q^n \in \mathcal{F}_{\bar\rho}(\mathbb{F})$. *The following are equivalent:*

(i) *f has a determination field which is abelian over $\mathbb{Q}$.*

(ii) *There exists an integer $M \geq 1$ such that for all prime ℓ not dividing Np, a_ℓ depends on ℓ only trough $\ell \pmod M$.*

(iii) *There exists an integer $M \geq 1$ such that for all prime ℓ not dividing Np $T_\ell f$, depends on ℓ only trough $\ell \pmod M$.*

If they hold, we can take M in (ii) and (iii) such that all prime factors of M divide Np.

Proof — This is a special case of Theorem 11.1.2, taking into account the Kronecker-Weber theorem that every number field abelian over $\mathbb{Q}$ is a subfield of a cyclotomic field $\mathbb{Q}(\zeta_M)$. □

Definition 11.2.2. We say that f is *cyclotomic* if it satisfies the conditions of the above proposition.

Definition 11.2.3. Let us denote by I_{cycl} the ideal generated by the elements $t_{\bar\rho}(xyx^{-1}y^{-1}s) - t_{\bar\rho}(s)$ for $x, y, s \in G_{\mathbb{Q},Np}$.

Since $A_{\bar\rho}(\mathbb{F})$ is noetherian the ideal I_{cycl} is finitely generated and closed. Clearly, I_{cycl} is the smallest ideal I of $A_{\bar\rho}$ such that $G/\mathrm{Ker}\,(t_I, d_I)$ is abelian, where t_I is the composition $t : G \to A \to A/I$ and similarly for d.

Example 11.2.4. In the case $p = 2$, $\bar\rho = 1 \oplus 1$, the ideal I_{cycl} is principal, and generated by the square of the element $T_5 + T_3 + T_3^3 + T_3^5 + T_3^9 + T_3^{11} + T_3^{129} + \ldots$: see [2].

Proposition 11.2.5. *A form f is cyclotomic if and only if it is annihilated by I_{cycl}.*

Proof — A form f is killed by I_{cycl} if and only if $I_{\mathrm{cycl}} \subset I_f$ which is visibly equivalent to $G_{\mathbb{Q},Np}/\mathrm{Ker}\, t_f$ being abelian, or L_f being an abelian extension of $\mathbb{Q}$. □

Proposition 11.2.6. *If $\bar\rho$ is irreducible, the only cyclotomic form in $\mathcal{F}_{\bar\rho}(\mathbb{F})$ is 0.*

Proof — Recall that if $\bar\rho$ is irreducible, it is absolutely irreducible, hence its image $\bar\rho(G_{\mathbb{Q},Np})$ is not abelian. If there is a non-zero cyclotomic form f in $\mathcal{F}_{\bar\rho}(\mathbb{F})$, then the pseudo-representation $(t_f, d_f) : G_{\mathbb{Q},Np} \to A_f$ reduces modulo the maximal ideal of A_f to the pseudo-representation $(\operatorname{tr}\bar\rho, \det\bar\rho) : G_{\mathbb{Q},Np} \to \mathbb{F}$, and it follows that the group $G_{\mathbb{Q},Np}/\operatorname{Ker} t_{\bar\rho}$ is a quotient of $G_{\mathbb{Q},Np}/\operatorname{Ker} t_f$, hence is abelian. Since $\bar\rho$ is semi-simple, $\operatorname{Ker}\bar\rho = \operatorname{Ker}\operatorname{tr}\bar\rho$, hence $G_{\mathbb{Q},Np}/\operatorname{Ker} t_{\bar\rho} \simeq \bar\rho(G_{\mathbb{Q},Np})$ is abelian, a contradiction. □

For the rest of this subsection we assume that $p > 2$ (for similar but more complicated results in the case $p = 2$, $N = 1$, see [2]), and that the projective image of $\bar\rho$ is cyclic, in other words that $\bar\rho$ is reducible. Let $\rho : G_{\mathbb{Q},Np} \to R^*$ be a (t, d)-representation with $R = \begin{pmatrix} A & B \\ C & A \end{pmatrix}$.

Proposition 11.2.7. *One has $I_{cycl} = BC$. In other terms, I_{cycl} is just the reducibility ideal of the pseudo-representation $t_{\bar\rho}$ (see* [3, §1.5]*).*

Proof — Let I be any ideal of $A_{\bar\rho}$, and let $(G_{\mathbb{Q},Np}, \bar\rho, t_I, d_I)$ be the admissible pseudo-deformation obtained by reducing the pseudo-deformation over $A_{\bar\rho}$ modulo I. Let $\rho_I : G_{\mathbb{Q},Np} \to R_I^*$ be a (t_I, d_I)-representation attached to the admissible pseudo-deformation $(G_{\mathbb{Q},Np}, \bar\rho, t_I, d_I)$ adapted to an element of $G_{\mathbb{Q},Np}$ for which ρ is also adapted. Then $R_I = \begin{pmatrix} A/I & B_I \\ C_I & A/I \end{pmatrix}$ and there is a natural surjective morphism of algebras $R \otimes_A A/I = R/IR \to R_I$ inducing identity maps $A/I \to A/I$ on the diagonal components, and maps $B/IB \to B_I$, $C/IB \to C_I$ on the non-diagonal components. Note that the map $R/IR \to R_I$, as well as the maps $B/IB \to B_I$ and $C/IC \to C_I$ need not be injective (this is because R/IR may not be faithful.) The ideal B_IC_I of A/I is nevertheless the image in A/I of the ideal BC of A, because the map $R \mapsto R_I$ preserves multiplication of matrices (see [3, §1.5] for more detailed proofs of the assertion of this paragraph).

By construction I_{cycl} is the smallest ideal I of A such that $G_{\mathbb{Q},Np}/\operatorname{Ker}(t_I, d_I)$ is abelian. One has $\operatorname{Ker}(\rho_I)_{|G} = \operatorname{Ker} t_I$ because R_I is faithful. Hence $G_{\mathbb{Q},Np}/\operatorname{Ker} t_I \simeq \rho_I(G_{\mathbb{Q},Np})$, and I_{cycl} is the smallest ideal I of A such that $\rho_I(G_{\mathbb{Q},Np})$ is abelian, or again, since R_I is generated by $\rho_I(G_{\mathbb{Q},Np})$ as an A/I-module, the smallest ideal I such that R_I is commutative. It is easy to see that the GMA $R_I = \begin{pmatrix} A/I & B_I \\ C_I & A/I \end{pmatrix}$ is commutative if and only if $B_I = C_I = 0$. Since the product $B_I \times C_I \to A/I$ is a non-degenerate pairing, this is equivalent to $B_IC_I = 0$, that is by the above paragraph, to $BC \subset I$. Thus $BC = I_{\mathrm{cycl}}$. □

Corollary 11.2.8. *Assume as above that the projective image of $\bar\rho$ is cyclic, but also that it is not of order 2. Then $I_{cycl} = A_{\bar\rho,ess}$. In other words, a form $f \in \mathcal{F}_{\bar\rho}$ is cyclotomic if and only if it is special.*

Proof — This follows from the preceding proposition and Theorem 8.4.3. □

11.3. **K-abelian forms.** In this subsection, we assume $p > 2$. For K-abelian forms in the case $p = 2$, see [24] and an article in preparation by J. Bellaïche, J.-L. Nicolas, and Jean-Pierre Serre. Let K be a quadratic extension of $\mathbb{Q}$.

Definition 11.3.1. A form $f \in \mathcal{F}_\rho$ is *K-abelian* if it has a field of determination L which is an abelian extension of K.

Note that the composition of two Galois extensions of $\mathbb{Q}$ which contain K and are abelian over K is also a Galois extension of $\mathbb{Q}$ which contains K and is abelian over K. It follows that if f and f' are K-abelian, $f + f'$ is K-abelian as well: if L and L' are fields of determination of f and f', then LL' is a field of determination of $f + f'$. Thus the set of K-abelian forms is a vector space. It is also obviously stable by the Hecke operators T_ℓ. Hence its orthogonal complement for the duality $A_{\bar\rho} \times \mathbb{F}_{\bar\rho} \to \mathbb{F}$ is an ideal I_{Kab}.

From now on, **we assume that the projective image of $\bar\rho$ is dihedral of order > 4.** Thus the projective image of $\bar\rho$ has a unique quotient of order 2, which corresponds to a quadratic extension K of $\mathbb{Q}$. Thus $G_{K,Np}$ is a subgroup of index 2 in $G_{\mathbb{Q},Np}$ and the projective image of $\bar\rho(G_{K,Np})$ is cyclic. We choose a well-adapted $(t_{\bar\rho}, d_{\bar\rho})$-representation $\rho : G_{\mathbb{Q},Np} \to \mathrm{GL}_2(A_{\bar\rho})$. By §6.3.3, the $A_{\bar\rho}$ algebra generated by $\rho(G_{K,Np})$ is a sub-GMA of $M_2(A_{\bar\rho})$, of the form $R = \begin{pmatrix} A_{\bar\rho} & B \\ B & A_{\bar\rho} \end{pmatrix}$ for some proper ideal B of $A_{\bar\rho}$.

Proposition 11.3.2. *One has $B = I_{Kab}$.*

Proof — By definition, I_{Kab} is the smallest ideal I of $A_{\bar\rho}$ such that the image of $G_{K,Np}$ in the quotient $G_{\mathbb{Q},Np}/\mathrm{Ker}\,(t_I, d_I)$ is abelian. Since the representation $\rho_I : G_{\mathbb{Q},Np} \to \mathrm{GL}_2(A_{\bar\rho}/I)$ obtained by reducing ρ modulo I has trace t_I and determinant d_I, and since the GMA $M_2(A/I)$ is faithful, ρ_I realizes an isomorphism $G_{\mathbb{Q},Np}/\mathrm{Ker}\,(t_I, d_I) \to \rho_I(G_{\mathbb{Q},Np}) \subset \mathrm{GL}_2(A_{\bar\rho}/I)$, and the image of $G_{K,Np}$ into $G_{\mathbb{Q},Np}/\mathrm{Ker}\,(t_I, d_I)$ is $\rho_I(G_{K,Np})$. Thus, $I_{\mathrm{Kab}} \subset I$ if and only if the group $\rho(G_{K,Np})$ is abelian, if and only if the $A_{\bar\rho}/I$-subalgebra of $M_2(A_{\bar\rho}/I)$ generated by $\rho_I(G_{K,Np})$ is commutative, if and only if the image of $R = \begin{pmatrix} A_{\bar\rho} & B \\ B & A_{\bar\rho} \end{pmatrix}$ in $M_2(A_{\bar\rho}/I)$ is commutative. Clearly, the latter condition is equivalent to $B \subset I$. Thus $B = I_{\mathrm{Kab}}$. □

Corollary 11.3.3. *Assume that the projective image of $\bar\rho$ is dihedral of order > 4, and divisible by 4. The one has $A_{\bar\rho,ess} = \mathfrak{m}_{\bar\rho} I_{Kab}$.*

Proof — By Theorem 8.5.2, one has $A_{\bar\rho,\mathrm{ess}} = \mathfrak{m}_{\bar\rho} B$. The corollary follows. □

Corollary 11.3.4. *Assume that the the projective image of $\bar\rho$ is dihedral of order > 4, and divisible by 4. A form $f \in \mathcal{F}_{\bar\rho}$ is special if and only if $(T_\ell - \lambda_\ell)f = 0$ is K-abelian for every prime ℓ not dividing Np (here $\lambda_\ell = \mathrm{tr}\,(\bar\rho(Frob_\ell))$). In particular, the space $\mathcal{F}_{\bar\rho,spe}$ contains the space of K-abelian forms as a finite dimensional subspace.*

Proof — This is just a translation of the preceding corollary, using that $\mathfrak{m}_{\bar\rho}$ is finitely generated since $A_{\bar\rho}$ is noetherian. □

11.4. **The case of a large or exceptional $\bar{\rho}$.** In this case it is easy to see that there are no cyclotomic forms in $\mathcal{F}_{\bar{\rho}}$, nor K-abelian forms for any K. The space $A_{\bar{\rho},\mathrm{ess}}$ is the ideal $\mathfrak{m}_{\bar{\rho}}^2$, hence $\mathcal{F}_{\bar{\rho},\mathrm{spe}}$ is the space of forms which are killed by $(T_\ell - \lambda_\ell)^2$ for all ℓ not dividing Np. This space is finite-dimensional since $A_{\bar{\rho}}/\mathfrak{m}_{\bar{\rho}}^2$ is finite-dimensional.

References

[1] J. Bellaïche, *Pseudo-deformations*. Math Z. 270 (2012), no. 3–4, 1163–1180.
[2] J. Bellaïche, *Une représentation galoisienne universelle attachée aux formes modulaires modulo 2*, C. R. Math. Acad. Sci. Paris 350 (2012), no. 9–10, 443–448.
[3] J. Bellaïche & G. Chenevier, *Families of Galois representations and Selmer groups*, Astérisque 324 (2009), Société Mathématique de France.
[4] J. Bellaïche & C. Khare, *Level 1 Hecke algebras of modular forms modulo p*, Compos. Math. 151 (2015), no. 3, 397–415.
[5] J. Bellaïche & K. Soundararajan, *The number of non-zero coefficients of modular forms mod p*, Algebra Number Theory 9 (2015), no. 8, 1825–1856
[6] G. Chenevier, *The p-adic analytic space of pseudocharacters of a profinite group and pseudorepresentations over arbitrary rings*, Proceedings of the LMS Durham Symposium, Automorphic forms and Galois representations, 2011
[7] G. Chenevier, *The p-adic analytic space of pseudocharacters of a profinite group and pseudorepresentations over arbitrary rings*, first version of the above, https://arxiv.org/abs/0809.0415v1, 2008.
[8] A. Conti, C. Iovita, J. Tilouine, *Big image of Galois representations associated with finite slope p-adic families of modular forms*, arXiv:1508.01598, 2015, to appear.
[9] C. W. Curtis & I. Reiner *Representation theory of finite groups and associative algebras*, Pure and Applied Mathematics, Vol. XI, Interscience Publishers, a division of John Wiley & Sons, New York-London, 1962
[10] S. Deo, *Hecke algebras of modular forms modulo p*, to appear in Algebra Number Theory.
[11] D. Eisenbud, *Commutative algebra. With a view toward algebraic geometry.* Graduate Texts in Mathematics, 150. Springer-Verlag, New York, 1995
[12] H. Hida, *Image of Λ-adic Galois representations modulo p.* Invent. Math. 194 (2013), no. 1, 1–40.
[13] N. Jochnowitz, *A study of the local components of the Hecke algebra mod l*, Trans. Amer. Math. Soc. 270 (1982), no. 1, 253–267.
[14] C. Khare, *Mod p modular forms*, Number theory (Tiruchirapalli, 1996), 135–149, Contemp. Math., 210, Amer. Math. Soc., Providence, RI, 1998.
[15] J. Lang, *On images of Galois representations in non-CM Hida families.* Algebra Number Theory, Volume 10, No. 1, (2016), 155–194.
[16] B. de Smit & H. W. Lenstra Jr.,*Explicit construction of universal deformation rings.* Modular forms and Fermat's last theorem (Boston, MA, 1995), 313–326, Springer, New York, 1997. 11F80
[17] H. Matsumura, *Commutative algebra*, 2nd edition. Mathematics Lecture Note Series, 56. Benjamin/Cummings Publishing Co., Inc., Reading, Mass., 1980.
[18] B. Mazur, *Deforming Galois representations*, Galois groups over $\mathbb{Q}$ (Berkeley, CA, 1987), 385–437, Math. Sci. Res. Inst. Publ., 16, Springer, New York, 1989.
[19] B. Mazur, *An introduction to the deformation theory of Galois representations.* Modular forms and Fermat's last theorem (Boston, MA, 1995), 243–311, Springer, New York, 1997
[20] B. Mazur & A. Wiles, *on p-adic analytic families of Galois representations*, Compositio Mathematica, 59 (2), 1986, 231–264.
[21] A. Medvedovsky, *Lower bounds on dimensions of mod-p Hecke algebras*, PhD Thesis, Brandeis University 2015.
[22] A. Medvedovsky, *Mod-3 modular forms*, in preparation.
[23] J.-L. Nicolas & J.-P. Serre, *L'ordre de nilpotence des opérateurs de Hecke modulo 2*, C.R.A.S. 350 (2012), no. 7-8, 343–348.
[24] J.-L. Nicolas & J.-P. Serre, *Formes modulaires modulo 2 : structure de l'algèbre de Hecke*, C.R.A.S. 350 (2012), no. 9-10, 449–454.
[25] R. Pink, *Classification of pro-p subgroups of SL_2 over a p-adic ring, where p is an odd prime*, Compositio Math. 88 (1993), no. 3, 251–264
[26] L. Ribes & P. Zalesskii, *Profinite groups.* Second edition. Ergebnisse der Mathematik und ihrer Grenzgebiete. 3. Folge. A Series of Modern Surveys in Mathematics, 40, Springer-Verlag, Berlin, 2010
[27] R. Rouquier, *Caractérisation des caractères et pseudo-caractères*, J. Algebra 180(2) (1996), 571–586.
[28] J.-P. Serre, *Congruences et formes modulaires [d'après H. P. F. Swinnerton-Dyer]*, Séminaire Bourbaki, 24e année (1971/1972), Exp. No. 416, pp. 319–338. Lecture Notes in Math., Vol. 317, Springer, Berlin, 1973.

[29] J.-P. Serre, *Divisibilité de certaines fonctions arithmétiques*, Enseignement Math. (2) 22 (1976), no. 3-4, 227–260.
[30] I. R. Shafarevich, *Extensions with prescribed ramification points*, Publications Mathématiques de l'IHES, 18 (1963), 71–95.

E-mail address: jbellaic@brandeis.edu

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