*Collect. Math.* **48**, 1–2 (1997), 155–193



# An "infinite fern" in the universal deformation space of Galois representations[1]

B. Mazur

*Department of Mathematics, Harvard University, 1 Oxford Street, Cambridge, MA 02138, U.S.A.*

(In memory of R.H. Bing)

## Abstract

I hope this article will be helpful to people who might want a quick overview of how modular representations fit into the theory of deformations of Galois representations.

There is also a more specific aim: to sketch a construction of a "point-set topological" configuration (the image of an "infinite fern") which emerges from consideration of modular representations in the universal deformation space of all Galois representations. This is a configuration hinted at in [20], but now, thanks to some recent important work of Coleman [6, 7], it is something one can actually produce! The "infinite fern" is joint work with F.Q. Gouvêa, and will be the subject of slightly more systematic study in a future paper in which some consequences of its existence will be discussed.[2]

Although the "infinite fern" which appears in the last section of these notes is hardly as profound a point-set topological object as some of the classic

[1] These notes include material I presented at the *Journées Arithmétiques* held in Barcelona (July 1995). I am very grateful to the organizing committee and to the audience for the opportunity to present this material, and for the discussions afterwards. I am also thankful to J.-P. Serre for helpful comments about an early draft of this article.

[2] E.g., in the limited context that we analyze (assume that the absolutely irreducible residual representation in question comes from a modular form of "noncritical slope" on $\Gamma_0(p)$, and the corresponding "unramified outside $p$" deformation problem is "unobstructed") it follows from the existence of the "infinite fern" that the entire universal deformation ring may be reconstructed from modular representations.

constructions of R.H. Bing, I would like to think that he might have nevertheless enjoyed it. I want to dedicate this article to him, in appreciation of his mathematics and of his energetic enthusiasm.

## Contents

# Part I: The basics of the deformation theory of Galois representations

## §1. An example of a Galois deformation problem

Here is what the theory of deformations of Galois representations says about a specific, but I believe illuminating, example. Let $\overline{\mathbb{Q}}$ be an algebraic closure of $\mathbb{Q}$, and $G_{\mathbb{Q}} := \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. Let $K/\mathbb{Q}$ be the splitting field of the cubic polynomial

$$X^3 + aX + 1$$

in $\overline{\mathbb{Q}}$ where $a \in \mathbb{Z}$ has the property that $27 + 4a^3$ is a prime number $p$ (so $p = 23, 31, 59, \ldots$ arise in this way). This means that the cubic has discriminant $-p$, and $K/\mathbb{Q}$ is unramified outside $p$ (and $\infty$) with Galois group isomorphic to $S_3$, the symmetric group on three letters. Up to equivalence there is only one imbedding of $S_3$ in $\mathrm{GL}_2(\mathbf{F}_p)$ and therefore there is only one (continuous) representation

$$\overline{\rho} : G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbf{F}_p)$$

whose image may be identified with the natural projection $G_{\mathbb{Q}} \to \mathrm{Gal}(K/\mathbb{Q})$. The representation $\overline{\rho}$ is unramified outside $p$ (and $\infty$).

The basic "deformational" problem which may be posed concerning $\overline{\rho}$ is the following: "Classify" all equivalence classes of liftings of $\overline{\rho}$ to representations

$$\rho : G_{\mathbb{Q}} \to \mathrm{GL}_2(A)$$

where $A$ is any (commutative) complete noetherian local ring with residue field $\mathbf{F}_p$ and where the representation $\rho$ is unramified outside $p$ (and $\infty$).

Here is the "answer" to this basic problem: There is a universal complete noetherian local ring with residue field $\mathbf{F}_p$, call it $R = R(\overline{\rho})$, which is isomorphic to a power series ring in three variables over $\mathbb{Z}_p$, and there is a "universal" representation, call it

$$\rho^{\mathrm{univ}} : G_{\mathbb{Q}} \to \mathrm{GL}_2(R) \approx \mathrm{GL}_2\big(\mathbb{Z}_p\big[[t_1, t_2, t_3]\big]\big)$$

which is unramified outside $p$, and which lifts $\overline{\rho}$. The representation $\rho^{\mathrm{univ}}$ is universal in the sense that for any lifting $\rho$ as above, there is a unique local ring homomorphism $\Phi_\rho : R \to A$ such that $\rho$ is induced from the representation $\rho^{\mathrm{univ}}$ by composition with the homomorphism

$$\mathrm{GL}_2(R) \to \mathrm{GL}_2(A)$$

coming from $\Phi_\rho$. The classificational problem, then boils down to describing this "universal" representation $\rho^{\mathrm{univ}}$ as explicitly as one can. See [25], [4], [3] for an extensive discussion of this example. To concentrate, even more specifically, on this type of question, let us ask for representations

$$G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{Z}_p)$$

which are unramified outside $p$, and which lift $\overline{\rho}$. Let us give a coordinatization of $R$ in terms of three formal parameters, i.e., a ring-isomorphism $R \cong \mathbb{Z}_p\big[[t_1, t_2, t_3]\big]$, so that for every point $x$ in

$$\begin{aligned} X &:= \mathrm{Hom}_{\mathrm{alg}}(R, \mathbb{Z}_p) \\ &\cong \mathrm{Hom}_{\mathrm{alg}}\big(\mathbb{Z}_p[[t_1, t_2, t_3]], \mathbb{Z}_p\big) \\ &\cong p\mathbb{Z}_p \times p\mathbb{Z}_p \times p\mathbb{Z}_p\,, \end{aligned}$$

(i.e., for every point $x$ in the "cube with sides $p\mathbb{Z}_p$") we get an induced representation

$$\rho_x : G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{Z}_p)$$

lifting $\overline{\rho}$ and unramified outside $p$, and so that as $x$ runs through all points in the "cube" $X$, the representations $\rho_x$ run through all equivalence classes of liftings of $\overline{\rho}$ to $\mathbb{Z}_p$ (unramified outside $p$) in a "one-to-one" manner.

The underlying residual representations in this class of examples are somewhat "elementary" and have the added virtue of being modular: we may even give explicit formulas for some modular forms (of $CM$ type) which have $\overline{\rho}$ as associated residual representation mod $p$. Also, from what we have just said, we know the universal deformation ring up to isomorphism. One might therefore get the impression (an incorrect impression, in my opinion) that we are on the verge of a fairly decent understanding, at least, of the nature of liftings to $\mathbb{Z}_p$ of these representations $\overline{\rho}$ (or, even more modestly, of one of them: say the representation for $p = 23$). But the goal of this article is to introduce a structure whose understanding is key to understanding important arithmetic properties of the liftings of $\overline{\rho}$ ("infinite ferns" of modular representations in §18). This structure sits in the cube $X$ and has a complexity to it that I find bewildering. How can one describe, or study this structure in closer detail? I might add that the infinite ferns we find are not peculiar to the particular examples described above, for they make their appearance in the deformation space of any residual representation attached to a modular eigenform satisfying a mild condition, as we shall see in §18 below.

## §2. Galois representations and deformations of the Galois group of $\mathbb{Q}$ of degree two

Let $k$ be a finite field of characteristic $p$. Fix a finite set of primes $S$, and let $G_{\mathbb{Q},S}$ denote the Galois group of a maximal algebraic extension of $\mathbb{Q}$ which is unramified outside $S$. We consider **residual representations**

$$\overline{\rho} : G_{\mathbb{Q},S} \to \mathrm{GL}_2(k)\,,$$

and **deformations** of $\overline{\rho}$ to a commutative complete local noetherian ring $A$ with residue field $k$:

$$\rho : G_{\mathbb{Q},S} \to \mathrm{GL}_2(A).$$

The ring $A$ occurring in the display above will sometimes be referred to as the **coefficient-ring** of the representation $\rho$. If $\overline{\rho}$ is absolutely irreducible this deformation problem has a universal solution, i.e., as in the example described in §1, there is a ring $R = R(\rho)$ called the **universal deformation ring** of $\overline{\rho}$, and a representation, $\rho^{\mathrm{univ}} : G_{\mathbb{Q},S} \to \mathrm{GL}_2(R)$, called the **universal deformation** of $\overline{\rho}$, such that given any deformation $\rho$ of $\overline{\rho}$ to $A$, it is induced from $\rho^{\mathrm{univ}}$ by a unique local ring homomorphism $R \to A$. As usual with solutions to universal problems, the universal deformation ring is *unique up to unique isomorphism.* The particular nature of the universal deformation ring $R = R(\overline{\rho})$ where $\overline{\rho}$ is one of the *examples* of §1 (i.e., *those* rings $R$ are power series rings in three variables over $\mathbb{Z}_p$) is **not** general. The basic facts here[3] are these:

First let us define the *parity* of $\overline{\rho}$ : both $\det\overline{\rho}$ and $\overline{\rho}$ itself are called **odd** if $\det\overline{\rho}(c) = -1$, where $c$ is any choice of a complex conjugation in $G_{\mathbb{Q},S}$ and they are called **even** if $\det\overline{\rho}(c) = 1$.

If $p \in S$, and if $\overline{\rho}$ is absolutely irreducible one has the Theorem that for $\overline{\rho}$ *odd,* the Krull dimension of $R$ is $\geq 4$, (§1.10 Cor. 3 of [25]) and if the "deformation problem for $\overline{\rho}$ is unobstructed"[4] then $R$ is (noncanonically) isomorphic to a power series ring on three parameters over the ring of Witt vectors of $k$. That is:

$$R \approx W(k)\big[[t_1, t_2, t_3]\big]\,.$$

[3] for a fuller discussion of them, see [25], [17, 18, 19], and the forthcoming [12].

[4] the "deformation problem for $\overline{\rho}$ is unobstructed" just means that given any surjection $A_1 \to A_0$ of commutative complete local noetherian rings with residue field $k$, and any lifting $\rho_0$ of $\overline{\rho}$ to $A_0$, there is a lifting $\rho_1$ of $\rho_0$ to $A_1$. For a discussion of this notion, its consequences, and criteria for when it occurs, see [25].

For $\overline{\rho}$ *even,* the Krull dimension of $R$ is $\geq 2$, and if the "deformation problem for $\overline{\rho}$ is unobstructed", then $R$ is (noncanonically) isomorphic to a power series ring on one parameter over the ring of Witt vectors of $k$. That is:

$$R \cong W(k)\big[[t]\big]\,.$$

Fix a residual representation $\overline{\rho} : G_{\mathbb{Q},S} \to \mathrm{GL}_2(k)$ which is absolutely irreducible, and assume that $p \in S$.

## §3. Twisting by characters

Since we aren't after maximal generality here, but only wish to illustrate the theory, let us restrict attention to the special case of $k = \mathbf{F}_p$. In this case less notation is needed, with no real loss of understanding. So, keep assuming that $p \in S$, and let

$$\overline{\rho} : G_{\mathbb{Q},S} \to \mathrm{GL}_2(\mathbf{F}_p)$$

be our residual representation and $R(\overline{\rho})$ the universal deformation ring of the residual representation $\overline{\rho}$. If we denote by $\Lambda = R\big(\det(\overline{\rho})\big)$ the universal deformation ring of the determinant representation

$$\det(\overline{\rho}) : G_{\mathbb{Q},S} \to \mathrm{GL}_1(\mathbf{F}_p) = \mathbf{F}_p^*$$

the functor ("determinant") which allows one to pass from any deformation of $\overline{\rho}$ to a coefficient-ring $A$ to a deformation of $\det(\overline{\rho})$ gives us, by universality, a natural homomorphism of complete local rings

$$\imath : \Lambda \to R(\overline{\rho})\,,$$

i.e., $R(\overline{\rho})$ may be naturally viewed as $\Lambda$-algebra. The choice of notation $\Lambda$ may be defended as "traditional" for the ring $\Lambda$ is closely related to the *Iwasawa algebra.* Indeed, using the description of Class Field Theory in the case of $K = \mathbb{Q}$ that we recalled above, it is a straightforward (and possibly informative) exercise to give an explicit description of $\Lambda = R\big(\det(\overline{\rho})\big)$ as a power series ring on one parameter over a ring finite and flat over $\mathbb{Z}_p$. The operation of twisting by one-dimensional representations gives us a natural action by a one-parameter formal multiplicative group on $R(\overline{\rho})$: for complete definitions here, see §1.4 of [25], but briefly, given any deformation $\rho$ of $\overline{\rho}$ to a coefficient-ring $A$, and given any character $\chi$ of $G_{\mathbb{Q},S}$ to the group of 1-units in $A$, we way "twist" $\rho$ by $\chi$, i.e., we may form $\rho \otimes \chi$, which gives us another deformation of $\overline{\rho}$ to $A$. The same action can be defined on $\Lambda = R\big(\det(\overline{\rho})\big)$. The structure homomorphism $\imath$ above is equivariant for this action. This twisting operation assures that there is at least one "parameter" of the ring $R(\overline{\rho})$ that is *easy to understand.*

It is tempting to imagine that for *even* residual representations $\overline{\rho}$, this is the *only* parameter there is! (for yet further speculations about even representations, see §9 below).

## §4. Digression: ordinary Galois representations

It is often of interest to modify the deformation problem of a residual representation $\overline{\rho}$ by imposing certain conditions that the deformations of $\overline{\rho}$ must satisfy. One tends, thereby, to get a problem which also has a "universal" solution ("universal", subject to the condition in question), given by a deformation of $\overline{\rho}$ to a quotient ring of $R(\overline{\rho})$. Here is an illustrative example. Fix a choice of inertia group $I_p \subset G_{\mathbb{Q}_p} \subset G_{\mathbb{Q},S}$. A Galois representation $\rho : G_{\mathbb{Q},S} \to \mathrm{GL}_2(A)$ is **ordinary** if $\rho(I_p)$ is contained in the semi-Borel subgroup

$$\begin{pmatrix} 1 & * \\ 0 & * \end{pmatrix},$$

or, equivalently if $I_p$ fixes the vector $(1,0) \in A\times A$. For a discussion of this condition see [18] and §1.7 of [25].

If $\rho$ is ordinary, then the action of $G_{\mathbb{Q}_p}$ on the vector $v = (1,0)$ is unramified. Making any choice of Frobenius element $\mathrm{Frob}_p$ in $G_{\mathbb{Q}_p}$ we may define a unit, which we denote $u_p(\rho) \in A^*$ by the formula $\mathrm{Frob}_p(v) = u_p(\rho)\cdot v$.

It is easy to see (Prop. 3 of §1.7 in [25]) that the problem of classifying all ordinary deformations of $\overline{\rho}$ is representable; hence we have a "universal" ordinary deformation $\rho^\circ$ of $\overline{\rho}$. Its coefficient-ring, which is a quotient ring of $R$, is called the **universal ordinary deformation ring** and is denoted $R^\circ$; that is, we have an ordinary deformation of $\overline{\rho}$,

$$\rho^\circ : G_{\mathbb{Q},S} \to \mathrm{GL}_2(R^\circ),$$

such that any ordinary deformation of $\overline{\rho}$ to a complete local ring $A$ is induced from $\rho^\circ$ by a homomorphism $R^\circ \to A$. Denote by $u^\circ$ the unit $u_p(\rho^\circ)$ in $R^\circ$.

## §5. The universal deformation space $X$

Let us return to the general deformation problem, and keep $\overline{\rho}$ as in §3 above. Consider the problem of lifting $\overline{\rho}$ to the ring of $p$-adic integers $\mathbb{Z}_p$. These liftings are "packaged" as the points of the topological space

$$X = X(\overline{\rho}) = \mathrm{Hom}_{\mathbb{Z}_p}\big(R(\overline{\rho}), \mathbb{Z}_p\big)\,,$$

where "$\mathrm{Hom}_{\mathbb{Z}_p}$" means continuous homomorphisms of $\mathbb{Z}_p$-algebras. The space $X$ may be viewed as the points over $\mathbb{Q}_p$ of the $p$-adic analytic variety underlying $\mathrm{Spec}\big(R(\overline{\rho})\big)$. With a mild abuse of language, we will be referring to $X$ itself as a *$p$-adic analytic space.* In the important case when the "deformation problem for $\overline{\rho}$ is unobstructed" (as in the examples described in §1, and also see §15 below) the space $X$ has the structure of $\mathbb{Q}_p$-analytic manifold (of dimension 3 and 1 in the case when $\overline{\rho}$ is odd or even, respectively). For the basics of $p$-adic analytic manifolds, see [29].

A point $x \in X$ corresponds to the deformation of $\overline{\rho}$ to $\mathbb{Z}_p$, i.e., to the equivalence class of representations,

$$\rho_x : G_{\mathbb{Q},S} \to \mathrm{GL}_2(\mathbb{Z}_p)$$

induced from the homomorphism $x : R(\overline{\rho}) \to \mathbb{Z}_p$ .

The structural homomorphism $\imath : \Lambda \to R(\overline{\rho})$ described in the previous section induces a natural mapping of $p$-adic analytic spaces

$$X \underset{\imath}{\to} \Delta = \mathrm{Hom}_{\mathbb{Z}_p}(\Lambda, \mathbb{Z}_p)\,,$$

and this homomorphism is equivariant with respect to the natural action (coming from twisting by characters, as described in the previous section) of the $p$-adic analytic group $\Phi := \mathrm{Hom}_{\mathrm{cont}}(G_{\mathbb{Q},S}, \Gamma)$ on the $p$-adic spaces $X$ and $\Delta$, where $\Gamma \subset \mathbb{Z}_p^*$ is the group of 1-units.

Let $V_x$ be the $\mathbb{Q}_p$-vector space $\mathbb{Q}_p \times \mathbb{Q}_p$ supplied with the $G_{\mathbb{Q},S}$-representation

$$\rho_x : G_{\mathbb{Q},S} \to \mathrm{GL}_2(\mathbb{Z}_p) \subset \mathrm{GL}_2(\mathbb{Q}_p) = \mathrm{Aut}(V_x)\,,$$

and by $V_{x,p}$ let us mean the same $\mathbb{Q}_p$-vector space, viewed as $G_{\mathbb{Q}_p}$-representation via the pullback of the action of $\rho_x$ to $G_{\mathbb{Q}_p}$. We want to understand the nature of these $G_{\mathbb{Q}_p}$-representations, and the invariants that can be extracted from them. We eventually want to view these invariants as ($p$-*adic analytic*) *functions of the point* $x$ in the $p$-adic analytic space $X$. This requires a certain digression:

## §6. Hodge-Tate-Sen weights attached to $G_{\mathbb{Q}_p}$-representations (of degree 2)

Consider a continuous $G_{\mathbb{Q}_p}$-representation space $W$ where $W$ is a two-dimensional $\mathbb{Q}_p$-vector space. Here is a somewhat idiosyncratic *motivation* for the Hodge-Tate theory: the "aim" of Hodge-Tate theory is to extract some numerical invariants of such representation spaces $W$ which are insensitive to any finite base change and to any unramified base change: that is, we want invariants of $W$ which depend only upon the isomorphism class of the representation $W$ when restricted to *any* open subgroup of the Galois group of the maximal unramified extension of $\mathbb{Q}_p$ in $G_{\mathbb{Q}_p}$. To emphasize that there are *indeed* some invariants of this nature, consider the subclass of $G_{\mathbb{Q}_p}$-representation spaces $W$ which are *reducible* (but not necessarily *completely reducible*). For such representation spaces $W$ there is a basis such that the associated $G_{\mathbb{Q}_p}$-representation $\eta$ can be written in the form

$$\eta(g) = \begin{pmatrix} R(g) & * \\ 0 & S(g) \end{pmatrix},$$

where $R$ and $S$ are continuous homomorphisms

$$R, S : G_{\mathbb{Q}_p} \to \mathbb{Z}_p^*;$$

$R$ and $S$ necessarily factor through $(G_{\mathbb{Q}_p})^{ab}$, the maximal abelian quotient of $G_{\mathbb{Q}_p}$. Since, by local class field theory, $(G_{\mathbb{Q}_p})^{ab}$ is a canonically isomorphic to $\hat{\mathbb{Q}}_p^*$, the profinite completion of $\mathbb{Q}_p^*$, and since we are only considering the isomorphism class of the representation $\eta$ after restriction to open subgroups of the inertia group in $G_{\mathbb{Q}_p}$, we are led to look for invariants of the pair of homomorphisms $R$ and $S$ restricted to arbitrary open subgroups of the group of units $\mathbb{Z}_p^*$ in $\mathbb{Q}_p^* \subset \hat{\mathbb{Q}}_p^* \cong (G_{\mathbb{Q}_p})^{ab}$.

To any continuous homomorphism

$$\mathbb{Z}_p^* \subset \mathbb{Q}_p^* \subset \hat{\mathbb{Q}}_p^* \cong (G_{\mathbb{Q}_p})^{ab} \xrightarrow{T} \mathbb{Z}_p^*, \tag{1}$$

one can attach a $p$-adic integer $t$ as follows:

Restrict $T$ to the subgroup $\Gamma$ of 1-units in $\mathbb{Z}_p^*$ (i.e., the multiplicative subgroup of $p$-adic integers congruent to 1 modulo $p$ if $p > 2$, and congruent to 1 modulo 4 if $p = 2$) and interpret $T$ as giving a continuous homomorphism

$$T : \Gamma \to \Gamma.$$

It is easy to see that if $p > 2$ the $p$-adic exponential map establishes a topological ($p$-adic analytic, in fact) isomorphism between the additive group $p\mathbb{Z}_p$ and $\Gamma$ (and between $p^2\mathbb{Z}_p$ and $\Gamma$ when $p = 2$) so that $\mathrm{Hom}(\Gamma, \Gamma)$ may be identified with

$$\mathrm{Hom}(\Gamma, \Gamma) = \mathrm{Hom}(\mathbb{Z}_p\, , \mathbb{Z}_p) = \mathbb{Z}_p\, . \tag{2}$$

The homomorphism $T \in \mathrm{Hom}(\Gamma, \Gamma)$ then corresponds to a $p$-adic integer $t \in \mathbb{Z}_p$ via the identifications of (2), the simple interpretation of $t$ being that $T$ viewed as an endomorphism of $\mathbb{Z}_p^*$ as in (1) above is just "raising to the *t-th* power" on an open subgroup of $\mathbb{Z}_p^*$. Call the $p$-adic integer $t$ the **weight** of $T$.

Now let $r, s$ denote the weights of $R$ and $S$, respectively.

This pair of elements $\{r, s\}$ which we view as an *unordered pair* of $p$-adic integers, is called the set of **generalized Hodge-Tate weights** attached to the $G_{\mathbb{Q}_p}$-representation $\eta$, or to the $G_{\mathbb{Q}_p}$-representation space $W$. For example, if $\eta$ is **ordinary** in the sense of §4 then at least one of its *generalized Hodge-Tate weights* (i.e., "$r$") is zero. Before we go on to more general $G_{\mathbb{Q}_p}$-representations, some comments are in order. Firstly, the set $\{r, s\}$ of *generalized Hodge-Tate weights* attached to the $G_{\mathbb{Q}_p}$-representation $\eta$ is determinable by $R$ and $S$ restricted to any open subgroup in $\Gamma$, and therefore the generalized Hodge-Tate weights are determinable by $\eta$ restricted to any open subgroup in the inertia group in $G_{\mathbb{Q}_p}$, as we had desired them to be. Secondly, the sum $r + s$ can be directly computed as the $p$-adic integer weight of the product $R \cdot S = \det(\eta)$ viewed as an endomorphism of $\Gamma$, and therefore it is not a very "new" invariant: it is in some sense "the logarithm of the determinant of $\eta$"; i.e., the interesting invariant of $\eta$ to be extracted from this discussion is, perhaps, the product $r \cdot s$, in that knowledge of both the determinant of $\eta$ (hence also $r + s$) and of $r \cdot s$ allows us to reconstruct the unordered pair $\{r, s\}$. If we choose to twist $\eta$ by a one-dimensional character

$$\chi : G_{\mathbb{Q}_p} \to (G_{\mathbb{Q}_p})^{ab} \cong \mathbb{Z}_p^* \to \mathbb{Z}_p^*$$

whose weight is $t$, then the generalized Hodge-Tate weights of $\eta \otimes \chi$ are $\{r+t, s+t\}$.

Now for the theory of Tate [36] and of Sen [33, 34]. Their results apply to arbitrary finite dimensional $G_{\mathbb{Q}_p}$-representation spaces, but we will keep focussed here only on $G_{\mathbb{Q}_p}$-representation spaces $W$ which are vector spaces of dimension 2 over $\mathbb{Q}_p$. The idea, though, is that $W$ is now allowed to be a general $G_{\mathbb{Q}_p}$-representation, reducible or irreducible. The theory of Tate and of Sen generalizes the above construction (in a quite surprising way!) and produces an unordered "pair of invariants" $\{r, s\}$ (with $r+s$ and $r \cdot s$ both in $\mathbb{Q}_p$) attached to any such $G_{\mathbb{Q}_p}$-representation space $W$ but with some "hitches" which we will describe below. The invariants $\{r, s\}$ are called the **Hodge-Tate-Sen weights**[5] of $W$ and they are dependent only upon the isomorphism class of the representation $W$ restricted to any open subgroup of the inertia group of $G_{\mathbb{Q}_p}$. Twisting $W$ by a character with weight $t$ translates the Sen weights to $\{r+t, s+t\}$ just as above. Also, the sum of the two invariants $r+s$ is, exactly as in the above discussion, the weight of the determinant of the representation, and so is not a "new" quantity.

Consequently, it is again $r \cdot s$ that is of particular interest.

Now for the "hitches":

**1)** Although $r+s$, and $r \cdot s$ lie in $\mathbb{Q}_p$, the invariants $r, s$ themselves might either lie in $\mathbb{Q}_p$ or, possibly, they might be $\mathbb{Q}_p$-conjugates in a field of degree 2 in $\overline{\mathbb{Q}}_p$.

**2)** Although we have no example of this, at present, the invariants $r, s$ might not be integral: as constructed, they may have denominators.

To my knowledge, we do not have a complete understanding, at present, of exactly what can happen here, and it would seem to me to be a worthwhile project to figure this out.

The way in which the Sen weights are constructed is briefly as follows. Since the natural action of $G_{\mathbb{Q}_p}$ on $\overline{\mathbb{Q}}_p$ preserves the natural valuation, it extends to a continuous action of $G_{\mathbb{Q}_p}$ on the completion, $\mathbb{C}_p$ of $\overline{\mathbb{Q}}_p$. By a $\mathbb{C}_p$-**semi-linear** $G_{\mathbb{Q}_p}$-representation $\mathcal{W}$ let us mean a finite dimensional $\mathbb{C}_p$ vector space, with continuous $G_{\mathbb{Q}_p}$-action satisfying the law $g(\lambda \cdot w) = g(\lambda) \cdot g(w)$ for $g \in G_{\mathbb{Q}_p}$, $\lambda \in \mathbb{C}_p$ and $w \in \mathcal{W}$.

Given a $G_{\mathbb{Q}_p}$-representation space $W$ as above, one proves that (even if $W$ is irreducible) the $\mathbb{C}_p$-**semi-linear** $G_{\mathbb{Q}_p}$-representation $\mathcal{W} = W \otimes_{\mathbb{Q}_p} \mathbb{C}_p$ with diagonal $G_{\mathbb{Q}_p}$-action is *always* reducible, and the Sen weights are simply the natural "weights" that one can extract from the two 1-dimensional $\mathbb{C}_p$-**semi-linear** $G_{\mathbb{Q}_p}$-representations occurring as irreducible constituents of $\mathcal{W}$.

## §7. The Sen mapping. The Sen "null subvariety" $X_0 \subset X$

Suppose given an absolutely irreducible residual representation (assumed either even or odd)

$$\overline{\rho} : G_{\mathbb{Q},S} \to \mathrm{GL}_2(\mathbf{F}_p)$$

whose deformation problem is unobstructed. Consider its universal deformation space (of $\mathbb{Z}_p$-deformations)

$$X = \mathrm{Hom}\big(R(\overline{\rho}), \mathbb{Z}_p\big)$$

[5] for short, we will refer to them as the **Sen weights** below

whose points $x \in X$ correspond to Galois representations

$$\rho_x : G_{\mathbb{Q},S} \to \mathrm{GL}_2(\mathbb{Z}_p)$$

whose pullbacks to $G_{\mathbb{Q}_p}$ we denote

$$\rho_{x,p} : G_{\mathbb{Q}_p} \to \mathrm{GL}_2(\mathbb{Z}_p)\,.$$

To each point $x \in X$ we then may associate, following the discussion in §6, an unordered pair $\{r_x, s_x\}$ of Sen weights. This, of course, is hardly ideal notation since we are not able to say which is $r_x$ and which is $s_x$. So let us introduce notation for the sum and product of $r_x$ and $s_x$ :

$$\delta(x) := r_x + s_x \qquad \text{(call } \delta \text{ the "}\textbf{log-determinant}\text{")}$$

$$\mathcal{S}(x) := r_x \cdot s_x \qquad \text{(call } \mathcal{S} \text{ the "}\textbf{Sen function}\text{")}\,.$$

The first of these, the "log-determinant" is simply the function giving the weight of the determinant $\det(\rho_x)$ and so (**a**) it is appropriately named and (**b**) as a mapping

$$\delta : X \to \mathbb{Q}_p$$

$\delta$ is "$p$-adic analytic" (in the sense that $\delta$ is the restriction to $X$ of a $p$-adic analytic function on the $p$-adic analytic variety attached to $\mathrm{Spec}(R(\overline{\rho}))$ ).

By a (delicate) theorem of Sen [34], the mapping

$$\mathcal{S} : X \to \mathbb{Q}_p$$

is also "$p$-adic analytic".

Recalling that $\Gamma \subset \mathbb{Z}_p^*$ is the subgroup of 1-units, let $\Phi = \mathrm{Hom}(G_{\mathbb{Q},S}, \Gamma)$ denote the subgroup of *wild characters* in $\mathrm{Hom}(G_{\mathbb{Q},S}, \mathbb{Z}_p^*)$. Since any wild character

$$\chi : G_{\mathbb{Q},S} \to \Gamma$$

factors through the maximal abelian, torsion free, pro-$p$-quotient group of $G_{\mathbb{Q},S}$, which by Class Field Theory is canonically identified with $\Gamma$, we may identify $\chi$ with a continuous endomorphism of $\Gamma$. Consequently the group $\Phi$ may be identified with $\mathrm{Hom}(\Gamma, \Gamma) = \mathbb{Z}_p$. If the wild character $\chi$ corresponds, in this identification to the $p$-adic integer $t \in \mathbb{Z}_p$, i.e., has weight $t$, we denote $\chi = \chi_t$.

The natural action of $\Phi$ on $X$ may be interpreted as a $p$-adic analytic action

$$\varphi : \mathbb{Z}_p \times X \to X\,, \tag{3}$$

given by $\varphi(t, x) := t * x$ where $\rho_y = \chi_t \otimes \rho_x$. If $\{r_x, s_x\}$ and $\{r_y, s_y\}$ are the Sen weights of $x$ and $y$ respectively, then the weights $\{r_y, s_y\}$ are the translates by $t$ of the weights $\{r_x, s_x\}$. Therefore we have:

$$\mathcal{S}(t * x) = t^2 + \delta(x) \cdot t + \mathcal{S}(x)\,.$$

Consequently, we have:

**Proposition**

*The Sen function $\mathcal{S}$ is nonconstant on any (nonempty) open subset of $X$.*

DEFINITION. The **Sen-null space** $X_0 \subset X$ is the locus of zeroes of the Sen function $\mathcal{S}$ on $X$.

Consider the restriction

$$\varphi_0 : \mathbb{Z}_p \times X_0 \to X \tag{4}$$

of the action (3) to the Sen null space $X_0$.

Let $X_{00} \subset X_0$ denote the subspace of Sen weights $\{0, 0\}$, i.e., the subspace of the Sen null space whose image under the mapping $\delta$ is 0.

**Proposition**

*The cardinality of any fiber $\varphi_0$ is $\leq 2$. The fibers of $\varphi_0$ of cardinality 1 are precisely the points of $X_{00}$.*

*Proof.* This is evident: given $x \in X$, the elements $(t, x_0)$ in $\varphi_0^{-1}(x) \subset \mathbb{Z}_p \times X_0$ are the points $(t, t * x)$ where $t$ is a root, in $\mathbb{Z}_p$, of the polynomial $t^2 - \delta(x) \cdot t + \mathcal{S}(x)$. □

*Remark.* If we were dealing with $p$-adic analytic spaces (but we are not: we are formally dealing with the $\mathbb{Q}_p$-points of analytic spaces) we could simply say that $\varphi_0$ exhibits $\mathbb{Z}_p \times X_0$ as a quadratic cover of $X$.

## §8. The picture, so far

We now review the discussion of §7, first assuming that $\overline{\rho}$ is *odd*. Then $R(\overline{\rho})$ is noncanonically isomorphic to $\mathbb{Z}_p\big[[t_1, t_2, t_3]\big]$, a power series ring in three variables over $\mathbb{Z}_p$. The $p$-adic analytic space $X$ is smooth, of dimension over $\mathbb{Q}_p$ equal to 3, i.e., $X = \mathrm{Hom}_{\mathbb{Z}_p}(R(\overline{\rho}), \mathbb{Z}_p)$ is noncanonically isomorphic to $\mathrm{Hom}_{\mathbb{Z}_p}\big(\mathbb{Z}_p[[t_1, t_2, t_3]], \mathbb{Z}_p\big)$ which is isomorphic to the $p$-adic manifold $p\mathbb{Z}_p \times p\mathbb{Z}_p \times p\mathbb{Z}_p$ : a triple $(x_1, x_2, x_3) \in p\mathbb{Z}_p \times p\mathbb{Z}_p \times p\mathbb{Z}_p$ corresponds, under this isomorphism, to the unique homomorphism $\varphi : \mathbb{Z}_p\big[[t_1, t_2, t_3]\big] \to \mathbb{Z}_p$ such that $\varphi(t_j) = x_j$ for $j = 1, 2, 3$. The subspace $X_0 \subset X$ of zeroes of the Sen function $\mathcal{S}$ (which is "locally nonconstant"; see the previous Proposition) is then the space of $\mathbb{Q}_p$ points of a $p$-adic analytic subvariety of dimension two. The mapping

$$\varphi_0 : \mathbb{Z}_p \times X_0 \to X$$

identifies $\mathbb{Z}_p \times X_0$ with the $\mathbb{Q}_p$ points of a ($p$-adic analytic, degree two) covering of $X$ obtained by extracting a square-root of the $p$-adic analytic function

$$\delta(x)^2 - 4\mathcal{S}(x)\,.$$

Of course, this does not preclude the possibility that $X_0$ might be empty (although we have no concrete example of this phenomenon). We do have large numbers of examples, however, of absolutely irreducible odd $\overline{\rho}$'s with unobstructed deformation theories where $X_0$ is non-empty. The examples of §1 have this property; and for a more interesting collection of $\overline{\rho}$'s (which are absolutely irreducible odd) with unobstructed deformation problems with non-empty $X_0$'s see §11.

### §9. Digression about even representations[6]

Now assume that $\overline{\rho}$ is *even.* For some interesting examples of deformation rings explicitly worked out for even residual representations see the recent PhD thesis of G. Böckle [2]. These are, in fact, the *only* cases I know of where a deformation problem for an even representation is completely computed. All the representations obtained in [2] are "*twist-finite*", meaning that after being twisted by a suitable one-dimensional character, they factor through a finite group. It would be of great interest to study some even Galois representation

$$\rho : G_{\mathbb{Q},S} \to \mathrm{GL}_2(\overline{\mathbb{Z}}_p)$$

which are not twist-finite. Is it the case that the two Sen weights of any even Galois representation $\rho$ are *equal*? (This is evidently so if $\rho$ is twist-finite.)

Are there examples of absolutely irreducible residual representations $\overline{\rho} : G_{\mathbb{Q},S} \to \mathrm{GL}_2(\mathbf{F}_p)$ with even determinant, such that $R(\overline{\rho})$ is not *finite and flat* over the ring $\Lambda = R(\det \overline{\rho})$?

In the present paper, we now make the hypothesis that our residual representation $\overline{\rho}$ is **odd**.

## Part II. Modular eigenforms, and modular representations in the universal deformation space

### §10. Eigenforms

By a classical cuspidal modular form of **type** $(N, k, \varepsilon)$ we mean a cuspidal modular form on $\Gamma_0(N)$ (or, as we shall sometimes say: "of level $N$") of some weight $k$ and

[6] I am thankful to A. Beilinson and R. Taylor for conversations regarding even representations which led to the questions posed in this section.

character $\varepsilon$. Such a modular form, $f(z)$, viewed as holomorphic function on the upper half plane is invariant under the translation $z \longmapsto z+1$, and letting $q = e^{2\pi i z}$, we may write its "Fourier" expansion, i.e., its Laurent expansion about the cusp $\infty$ :

$$f(z) = a_1 \cdot q + a_2 \cdot q^2 + \dots ,$$

with Fourier coefficients $a_j \in \mathbb{C}$.

By an **eigenform** (of type $(N, k, \varepsilon)$ ) we mean a cuspidal modular form of type $(N, k, \varepsilon)$ whose Fourier expansion has its first coefficient $a_1$ equal to 1, and which is an eigenform for the Hecke operators $T_\ell$ for $\ell$ not dividing $N$ and for the Atkin operators $U_q$ for $q$ dividing $N$. Under the assumption that $a_1 = 1$, the connection between the eigenvalue, $\lambda_\ell$, of the Hecke operator $T_\ell$ for prime numbers $\ell$ not dividing $N$ and $a_\ell$, the $\ell$-th Fourier coefficient of $f$, is quite simple, $\lambda_\ell = a_\ell$.

If $\mathcal{O}_f$ denotes the integral closure in $\mathbb{C}$ of the ring generated by the Fourier coefficients of the eigenform $f$, then it is standard that $\mathcal{O}_f$ is the ring of integers in a number field. For any maximal ideal $m \subset \mathcal{O}_f$, let $\mathcal{O}_{f,m}$ denote the completion of the integral closure $\mathcal{O}_f$ at the maximal ideal $m$ and let $K_{f,m}$ be the field of fractions of $\mathcal{O}_{f,m}$. Then $K_{f,m}$ is a discretely valued field of characteristic zero, and $\mathcal{O}_{f,m}$ is the discrete valuation ring of integers in $K_{f,m}$. Let $k_{f,m}$ denote the residue field of $\mathcal{O}_{f,m}$. Then $k_{f,m}$ is a finite field; let $p$ be its characteristic. There is a Galois representation

$$\rho_{f,m} : G_{\mathbb{Q},S} \to \mathrm{GL}_2(K_{f,m}) \tag{1}$$

"associated" to the eigenform $f$ where $S$ is the set of prime divisors of $p \cdot N$. This result, and the further elucidation of the basic properties of $\rho_{f,m}$, is due to a number of mathematicians, including Shimura (for weight 2; cf. [35]), Deligne (for weights $\geq 2$; cf. [10]), and Deligne-Serre (for weight 1; cf. [11]). For a detailed formulation of these properties in the case of modular forms of weight two and where they can be found proved in the literature, see [9] (Theorem 3.1 and the surrounding discussion there).

The defining property of $\rho_{f,m}$ (i.e., the property which defines the word "associated" in the previous paragraph) is the formula:

$$\lambda_\ell = a_\ell = \mathrm{Trace}\big(\rho_{f,m}(\mathrm{Frob}_\ell)\big) \tag{2}$$

for all prime numbers $\ell$ not dividing $N$. By the Chebotarev density theorem, the set of all Frobenius elements at primes $\ell$ not dividing $p \cdot N$ is dense in $G_{K,S}$. Therefore knowledge of the traces of the images of these elements under $\rho_{f,m}$ amounts to knowledge of the character function of the representation $\rho_{f,m}$. By (2), knowledge of these traces is simply knowledge of the Fourier coefficients $a_\ell$ of $f$ for prime numbers $\ell$ not dividing $N$. Since $\rho_{f,m}$ is completely reducible (in fact it is absolutely irreducible) the character function of the representation $\rho_{f,m}$ determines $\rho_{f,m}$. In summary, the representation $\rho_{f,m}$ is determined by $f$ and the maximal ideal $m \subset \mathcal{O}_f$.

It is easy to see that any homomorphism (1) after conjugation by an appropriate element in $\mathrm{GL}_2(K_{f,m})$ can be made to have, as range, the "maximal" compact subgroup $\mathrm{GL}_2(\mathcal{O}_{f,m}) \subset \mathrm{GL}_2(K_{f,m})$ :

$$G_{\mathbb{Q},S} \to \mathrm{GL}_2(\mathcal{O}_{f,m}) \subset \mathrm{GL}_2(K_{f,m})\,. \tag{3}$$

Reducing the homomorphism $G_{\mathbb{Q},S} \to \mathrm{GL}_2(\mathcal{O}_{f,m})$ "modulo the maximal ideal of $\mathcal{O}_{f,m}$". i.e., composing with the natural projection $\mathrm{GL}_2(\mathcal{O}_{f,m}) \to \mathrm{GL}_2(k_{f,m})$, we then get a representation

$$\overline{\rho} : G_{\mathbb{Q},S} \to \mathrm{GL}_2(k_{f,m})\,, \tag{4}$$

and, in the terminology of Part I, the representation $G_{\mathbb{Q},S} \to \mathrm{GL}_2(\mathcal{O}_{f,m})$ is a *deformation of* $\overline{\rho}$ to $\mathcal{O}_{f,m}$.

The representation $\overline{\rho}$ might be irreducible or not.

If $\overline{\rho}$ is *irreducible*, then its equivalence class, and the $\mathrm{GL}_2(\mathcal{O}_{f,m})$-equivalence class of the representation $G_{\mathbb{Q},S} \to \mathrm{GL}_2(\mathcal{O}_{f,m})$, are both uniquely determined by the equivalence class of the representation $\rho_{f,m}$ . In this situation, with a mild abuse of language we will then denote the representation to $\mathrm{GL}_2(\mathcal{O}_{f,m})$ as $\rho_{f,m}$ as well:

$$\rho_{f,m} : G_{\mathbb{Q},S} \to \mathrm{GL}_2(\mathcal{O}_{f,m})\,,$$

and with no abuse of language, we will refer to the equivalence class of $\overline{\rho}$ as $\overline{\rho}_{f,m}$ : $G_{\mathbb{Q},S} \to \mathrm{GL}_2(k_{f,m})$.

If $\overline{\rho}$ is *reducible,* then neither its equivalence class, nor the $\mathrm{GL}_2(\mathcal{O}_{f,m})$-equivalence class of the representation $G_{\mathbb{Q},S} \to \mathrm{GL}_2(\mathcal{O}_{f,m})$, are necessarily determined by the equivalence class of the representation $\rho_{f,m}$. It is only the "semi-simplification" of $\overline{\rho}$ that is determined by the equivalence class of the representation $\rho_{f,m}$.

From now on we will suppose given an eigenform $f$ of type $(N, k, \varepsilon)$ and a maximal ideal $m \subset \mathcal{O}_f$ for which $\overline{\rho} = \overline{\rho}_{f,m}$ is *absolutely irreducible.* Let $R = R(\overline{\rho}_{f,m})$ be the universal deformation ring of $\overline{\rho}_{f,m}$, and $X = \mathrm{Hom}_{\mathbb{Z}_p}(R, \mathbb{Z}_p)$ the associated universal deformation space, following the terminological conventions of §5 above. In particular, $\rho_{f,m}$ is a deformation of $\overline{\rho}_{f,m}$ to $\mathcal{O}_{f,m}$.

Embed the ring $\mathcal{O}_{f,m}$ in $\overline{\mathbb{Q}}_p$, and restrict the Galois representation $\rho_{f,m}$ to $G_{\mathbb{Q}_p}$. If $p$ does not divide $N$ it is known (cf. [14]) that the Sen weights of the representation

$\rho_{f,m}$ (restricted to $G_{\mathbb{Q}_p}$) are precisely 0 and $k-1$. In particular, if $\mathcal{O}_{f,m} = \mathbb{Z}_p$ the deformation $\rho_{f,m}$ corresponds to a point, call it $x_f$, in $X$ which lies in the analytic subspace $X_0 \subset X$, described in §7 above.

## §11. How "often" can we expect the deformation problem associated to $\rho_{f,m}$ to be unobstructed?

By work of Flach (cf. Th. 2 of [15]) we may expect the answer here to be "quite often". Here is a brief statement of Flach's result regarding this: Fix a modular cuspidal newform $f$ of weight two on $\Gamma_0(N)$ with trivial character. Assume that $f$ has rational integral Fourier coefficients. Therefore the ring $\mathcal{O}_f$ is $\mathbb{Z}$, and $f$ parametrizes an elliptic curve $E$ over $\mathbb{Q}$ with good reduction outside $\mathrm{Div}(N)$, the set of prime divisors of $N$. Let $\lambda := L(\mathrm{Sym}^2 f, 2)/\Omega$ denote the *nonzero* normalized special value at $s = 2$ of the $L$-function of the "symmetric square" of $f$; it is appropriately normalized to be a (nonzero) rational integer (See [15], [22], [40]). Let $E[p]$ denote the $\mathbf{F}_p$ vector space of dimension two consisting in the kernel of multiplication by $p$ in $E(\overline{\mathbb{Q}})$, viewed as a residual $G_{\mathbb{Q},S}$-representation

$$\overline{\rho}_{E,p} = \overline{\rho}_{f,p} : G_{\mathbb{Q},S} \to \mathrm{GL}_2(\mathbf{F}_p)$$

where $S = \{p\} \cup \mathrm{Div}(N)$.

**Theorem (Flach)**

*The residual representation $\overline{\rho}_{f,p}$ is unobstructed for all choices of $p$ not dividing the nonzero integer $6 \cdot N \cdot \lambda$ and satisfying these further hypotheses:*
*1) The residual representation $\overline{\rho}_{f,p}$ is surjective.*
*2) For all $\ell \in S$, $H^0\big(\mathbb{Q}_\ell,\ E[p] \otimes E[p]\big)$ vanishes.*

**Corollary 1**

*Let $f$ be a modular newform of weight two with integral Fourier coefficients. Assume $f$ to be not of CM-type. Let $\overline{\rho}_{f,p}$ be the residual representation in characteristic $p$ attached to $f$, as above. Let $E$ be the modular elliptic curve parametrized by $f$. Then there is a finite set of prime numbers $\mathcal{S}$ such that if $p \notin \mathcal{S}$ and*

$$H^0\big(\mathbb{Q}_p,\ E[p] \otimes E[p]\big)$$

*vanishes, then the deformation theory for $\overline{\rho}_{f,p}$ is unobstructed.*

*Proof.* By Serre's Theorem (Th. 2 of §4.2 in [30]) since $f$ is not of $CM$ type, condition 1 excludes only a finite number of primes $p$. Now consider condition 2 for prime numbers $\ell$ which divide $N$. After a finite base change, $K/\mathbb{Q}_\ell$, we may assume that $E_{/K}$ has semi-stable reduction. If $E_{/K}$ has good reduction, let $\alpha_\ell$, $\beta_\ell$ be the eigenvalues of Frobenius acting on the $p$-adic representation attached to $E$. The group $H^0\big(\mathbb{Q}_\ell, E[p] \otimes E[p]\big)$ vanishes if none of the numbers $\alpha_\ell^2 - 1,\ \beta_\ell^2 - 1$, or $\ell - 1$ are divisible by $p$. This will happen for all but a finite number of primes $p$. If, on the other hand, $E_{/K}$ has multiplicative reduction, let $q_K$ denote the "Tate parameter" attached to $E$, so that after a possible further quadratic extension of $K$, we may assume that the $p$-divisible group attached to $E_{/K}$ is isomorphic to the extension of $\mathbb{Q}_p/\mathbb{Z}_p$ by $\mu_{p^\infty}$ classified by $q_K$ and, in particular we have that $E[p]$ is a nontrivial extension of $\mu_p$ by $\mathbb{Z}/p\mathbb{Z}$ provided that ord $q_K$ is not a multiple of $p$. When $E[p]$ is a nontrivial extension of $\mu_p$ by $\mathbb{Z}/p\mathbb{Z}$, one sees that the subspace of $G_K$-invariant elements of $E[p] \otimes E[p]$ is equal to the subspace of $G_K$-invariant elements of $\mu_p \otimes \mu_p$ which vanishes for all but a finite number of choices of $p$. It follows that, in either case (good or multiplicative reduction over a suitably large field $K$) if $\ell$ divides $N, H^0\big(\mathbb{Q}_\ell, E[p] \otimes E[p]\big)$ vanishes for all but a finite number of primes $p$.

Thus there is a finite set of prime numbers $\mathcal{S}$ such that if $p \notin \mathcal{S}$ and if we also have that

$$H^0\big(\mathbb{Q}_p, E[p] \otimes E[p]\big)$$

vanishes, then the hypotheses of Flach's Theorem hold for $p$, and therefore by that Theorem, the deformation theory for $\overline{\rho}_{f,p}$ is unobstructed. $\square$

How often is it the case that $H^0\big(\mathbb{Q}_p, E[p] \otimes E[p]\big)$ vanishes? Here is a necessary and sufficient criterion for its nonvanishing (for $p$ an odd prime of good reduction for $E$).

**Lemma**

*Let $E$ be an elliptic curve over $\mathbb{Q}$ and $p$ an odd prime number of good reduction for $E$. Let $E(\mathbf{F}_p)$ denote the group of $\mathbf{F}_p$-valued points on the reduction of $E$ mod $p$, and let $a_p = 1 + p - |E(\mathbf{F}_p)|$. Then $H^0\big(\mathbb{Q}_p, E[p] \otimes E[p]\big)$ does not vanish if and only if*

*(i) $a_p \equiv \pm 1$ mod $p$, and*

*(ii) the $G_{\mathbb{Q}_p}$-representation on the group of $p$-torsion points $E[p]$ is semi-simple.*

*Proof.* Let $p$ be an odd prime of good reduction for $E$.

**Case 1.** Suppose first that $p$ is a prime of supersingular reduction for $E$, or equivalently, that $a_p \equiv 0 \bmod p$. In this case the representation of the inertia group at $p$ on $E[p] \otimes_{\mathbf{F}_p} \overline{\mathbf{F}}_p$ is the direct sum of the two one-dimensional representations given by the two "fundamental characters of level 2" (cf. §1.11 of [30]) which we will denote $\Theta$ and $\Theta^p$, it follows that the representation of the inertia group on $E[p] \otimes E[p] \otimes_{\mathbf{F}_p} \overline{\mathbf{F}}_p$ is then sum of one-dimensional characters $\Theta^2$, $\Theta^{p+1}$ (taken twice) and $\Theta^{2p}$; none of these characters is trivial, since $p$ is odd. Consequently $H^0\big(\mathbb{Q}_p, E[p] \otimes E[p]\big)$ vanishes.

**Case 2.** Now suppose that $p$ is a prime of good ordinary reduction for $E$. The $G_{\mathbb{Q}_p}$-representation on the group of $p$-torsion points $E[p]$ is given by

$$\begin{pmatrix} \psi^{-1}\chi & * \\ 0 & \psi \end{pmatrix},$$

where $\chi : G_{\mathbb{Q}_p} \to \mathbf{F}_p^*$ is the mod $p$ cyclotomic character, and $\psi$ is unramified. Moreover, $\psi(\mathrm{Frob}_p) \equiv a_p \bmod p$. In particular, the $\mathbf{F}_p$-dual of this representation is ordinary in the sense of §4.

A direct calculation shows that the tensor square of the above representation contains the identity representation if and only if the original representation is semi-simple and $\psi^2$ is trivial. □

*Remarks.*

**1) About condition (i):** For prime numbers $p > 5$, condition (i) above is equivalent to the condition

$$\text{(i)}' \qquad a_p = \pm 1$$

because the Hasse inequality $|a_p| \le 2\sqrt{p}$, together with the fact that $a_p = m \cdot p \pm 1$ for some integer $m$, forces $m$ to be zero when $p > 5$. The set of primes (of good reduction for $E$) for which condition (i)$'$ holds is of Dirichlet density zero. For this, see Theorem 20 of §8 of [31] which gives (among other things) the following more precise result:

If $P_E(x)$ is the number of primes $p \le x$ satisfying (i)$'$ for the elliptic curve $E$, then for any positive real number $\rho < 1/3$,

$$P_E(x) = O\Big(x/\log(x)^{1+\rho}\Big)$$

as $x \longmapsto \infty$.

In no case it is presently known that $P_E(x)$ tends to infinity with $x$. It may be that certain congruence conditions satisfied by the $a_p$ (which hold when the action of the Galois group of $\mathbb{Q}$ on division points of $E$ is "small") preclude $a_p = +1$ or $a_p = -1$ from occurring infinitely often. For example, if $E$ has a nontrivial $\mathbb{Q}$-rational torsion point, the case $a_p = +1$ occurs for at most one prime number $p$. If no such congruence conditions hold for $E$, it has been conjectured by Lang and Trotter [24] that $P_E(x)$ is asymptotic to $C\sqrt{x}/\log x$ for some constant $C > 0$ (whose value is predicted in loc. cit.). A prime number $p$ has been called *anomalous* for the elliptic curve $E$ if $a_p = +1$; this condition shows up in a number of arithmetic questions regarding $E$.

**2)** The general question of semi-simplicity of the $G_{\mathbb{Q}_p}$-representation on the group of $p$-torsion points $E[p]$ of a modular elliptic curve $E$ is the subject of Gross's deep study of the phenomenon of "companion forms" as defined by Serre; see [21]. It would be interesting to obtain some information about the distribution of prime numbers $p$ which, for fixed elliptic curve $E$, have the property that the $G_{\mathbb{Q}_p}$-representation on $E[p]$ is semi-simple.

**3)** For any cuspidal newform $f$ on $\Gamma_1(N)$, let *Obs* $(f)$ denote the set of prime ideals $\mathcal{P}$ in the ring generated by its Fourier coefficients $\mathcal{P} \subset \mathcal{O}_f$ for which the residual representation $\overline{\rho}_{f,\mathcal{P}}$ is absolutely irreducible and its deformation problem is obstructed.

**Question:** Is *Obs* $(f)$ finite?

For no cuspidal newform $f$ do we know the answer to this question. The above discussion gives:

**Corollary 2**

*Let $f$ be a cuspidal newform of weight two and trivial character, with integral Fourier coefficients. Assume $f$ to be not of $CM$-type. Let $\overline{\rho}_{f,p}$ be the residual representation in characteristic $p$ attached to $f$, as above. Then the set of primes $p$ for which $\overline{\rho}_{f,p}$ is absolutely irreducible and the deformation theory for $\overline{\rho}_{f,p}$ is unobstructed, is of Dirichlet density 1.*

There are other cases where one can prove that *Obs* $(f)$ is relatively "restricted". For example,

**Proposition**

*If $f$ is $\Delta = \Sigma\, \tau(n) q^n$, the unique cuspidal newform of weight 12 of level 1, then we have the following inclusion:*

$$Obs(\Delta) \subset \{11, 13\} \;\cup\; \{\text{primes } p \,|\, \tau(p) \equiv 0 \bmod p\}\,.$$

*Proof.* This is simply Proposition 2 of [26], its hypotheses holding thanks to the Theorem (due to Wiles and Taylor-Wiles) quoted in §15 below. Note that the prime 691 which appears in the conclusion of Proposition 2 of [26] is not in *Obs* $(\Delta)$ since $\overline{\rho}_{\Delta,691}$ is not absolutely irreducible. □

In particular the primes $p$ in *Obs* $(\triangle)$ which are less than 3 million are contained in the set $\{11, 13, 2411\}$.[7]

## §12. The "slope" of an eigenform (*this is* **not** *an invariant of the attached Galois representation*).

Let $M$ be an integer prime to $p$, and $N = M \cdot p$. Fix $f$ an eigenform of type $(N, k, \varepsilon)$, and $m \subset \mathcal{O}_f$ a maximal ideal of residual characteristic $p$. For prime numbers $q$ dividing $N$, let $\lambda_q$ denote the eigenvalue of the Atkin operator $U_q$ acting on $f$. One thing to bear in mind, however, about the difference between these $\lambda_q$'s (for prime numbers $q$ dividing $N$) and the $\lambda_\ell$'s (for $\ell$ prime to the level $N$) is that although the $\lambda_\ell$'s are retrievable from the Galois representation (as the traces of Frobenius elements) the $\lambda_q$'s are not as we shall presently see.

The single most important operator, for us, is the Atkin operator $U_p$ where $p$ is the residual characteristic of our chosen maximal ideal $m$. By our notational conventions, we have:

$$U_p f = \lambda_p \cdot f\,,$$

and we view the $U_p$-eigenvalue $\lambda_p$ as an element of $\mathcal{O}_{f,m} \subset K_{f,m}$.

Let "$\mathrm{ord}_p$" denote the valuation on $K_{f,m}$ normalized so that $\mathrm{ord}_p(p) = 1$. By the **slope** of $f$ we mean the non-negative rational number $\mathrm{ord}_p(\lambda_p) \in \mathbb{Q}$.

Given any newform $\varphi$ of type $(M, k, \varepsilon)$ with $M$ prime to $p$, there are *two* eigenforms $f, f'$ of weight $k$ and level $N = M \cdot p$ all of whose $T_\ell$-eigenvalues for $\ell$ not dividing $N = p \cdot M$ and $U_q$-eigenvalues for $q$ dividing $M$ are equal, and are equal to those of $\varphi$, and whose $U_p$ eigenvalues are the *two* roots $\lambda_p$ and $\lambda'_p$ (respectively) of the polynomial

$$X^2 - \tau_p X + \varepsilon(p) \cdot p^{k-1} \tag{1}$$

where $\tau_p$ is the $T_p$-eigenvalue of the modular form $\varphi$.

---

[7] That 2411 is a supersingular prime for $\triangle$ has been known for a while. Gouvêa made a computation showing 2411 to be the only supersingular prime $p$ for $\triangle$ in the range $11 \leq p < 125{,}000$ and more recently this computation has been extended to the $11 \leq p < 3{,}000{,}000$ by Blair Kelly III.

Explicitly,

$$f(z) = \varphi(z) - \lambda'_p \cdot \varphi(pz) \qquad \text{and}$$
$$f'(z) = \varphi(z) - \lambda_p \cdot \varphi(pz)$$

(so that $f, f'$ represent a basis which diagonalizes the operator $U_p$ acting on the two-dimensional space of old forms on $\Gamma_0(N)$ spanned by $B_1(\varphi) = \varphi$ and $B_p(\varphi)$, where $B_d$ is the standard "degeneracy operator" $B_d(\psi)(z) = \psi(d \cdot z)$; cf. [1]).

The $U_p$-eigenvalues $\lambda_p$ and $\lambda'_p$ of $f$ and $f'$ respectively are then also equal to the two eigenvalues of the Frobenius element at $p$ acting on the Galois representations attached to $\varphi$.

The Galois representations coming from $f$ and $f'$ are equivalent (these Galois representations are both equivalent to the Galois representation attached to $\varphi$) and yet the $U_p$-eigenvalues of $f$ and $f'$ need not be equal[8] since we have

$$\lambda_p \cdot \lambda'_p = \varepsilon(p)p^{k-1}$$

and, in particular,

$$\text{slope}(f) + \text{slope}(f') = k - 1\,.$$

We refer to $f$ and $f'$ as **twins** (since the Galois representation attached to $f$ is equivalent to the Galois representation attached to $f'$) and in the case where one has a larger slope than the other, we refer to the one with the larger slope as the **evil twin.** For the present article it is convenient to restrict the usage of the term "twin" to precisely the above set-up: that is, to the case where both twins $f$ and $f'$ arise from the same *newform* $\varphi$ of level $M$, i.e., where $f$ and $f'$ are, in fact, "new" for all primes distinct from $p$ which divide their level (although in later treatments one may well want to relax this requirement).

Although there is some ambiguity about how many different modular eigenforms with how many different $U_p$-eigenvalues can be attached to the same Galois representation, we shall prepare to state two propositions which are relatively easy to prove, and which limit the situation.

**Proposition 1**

*Let $\varphi$ be a (cuspidal) newform of level $M$ prime to $p$ with Fourier coefficients lying in $\overline{\mathbb{Q}}_p$. Let $g$ be any eigenform of level $N = p \cdot M$, with Fourier coefficients lying in $\overline{\mathbb{Q}}_p$, whose associated $p$-adic Galois representation is equivalent to that of $\varphi$. Then $g$ is equal to one of the twins $f$ or $f'$ above.*

[8] in fact, Ulmer conjectures that they are never equal; see the discussion at the end of this section.

*Remark.* It follows, of course, that the only possible $U_p$-eigenvalues of eigenforms of level $N = p \cdot M$ whose associated Galois representations are isomorphic to that of $\varphi$ are the $\mathrm{Frob}_p$-eigenvalues $\lambda_p$ and $\lambda'_p$ of the Galois representation attached to $\varphi$.

*Proof.* The proof is a direct consequence of "Strong Multiplicity One", for the application of which we will use the language of [1]. Note, though, that [1] works in the classical context, where the modular forms in question have Fourier coefficients in the field of complex numbers, while our forms have Fourier coefficients in $\overline{\mathbb{Q}}_p$. To make the transition, simply "choose" some imbedding, $\overline{\mathbb{Q}}_p \to \mathbb{C}$. That being said, there is a unique divisor, $N'$ of $p \cdot N$ and a unique newform $\gamma$ on $\Gamma_0(N')$ which "gives rise to" the eigenform $g$ (i.e., such that $g$ lies in the space of oldforms of $\Gamma_0(N)$ spanned by the image of $\gamma$ under the set of degeneracy operators $B_d : \Gamma_0(N') \to \Gamma_0(N)$ for positive integers $d$ dividing $N/N'$; for the definition of the degeneracy operators $B_d$, cf [1]). Since the $p$-th Fourier coefficient of $\varphi$ is (after our hypotheses) equal to the $p$-th Fourier coefficient of $\gamma$ for almost all prime numbers $p$, it follows from an application of Lemma 24 of §5 of [1] that $N' = M$ and $\varphi = \gamma$. Consequently, $g$ is in the span of $B_1(\varphi)$ and $B_p(\varphi)$ and is therefore either $f$ or $f'$. □

When does a modular eigenform $f$ of weight $k$ on $\Gamma_0(p{\cdot}M)$ with trivial character $\varepsilon$ have a twin $f'$?

**Proposition 2**

*If $f$ is a modular eigenform of weight $k$ on $\Gamma_0(p{\cdot}M)$ with character $\varepsilon$ of conductor dividing $M$, and if $\lambda_p^2 \neq \varepsilon(p) \cdot p^{k-2}$, then there is a modular eigenform $\varphi$ of level $M$ whose attached Galois representation is equivalent to that of $f$.*

*Proof.* This follows from Ogg's [28] Lemma 4 (c). □

**Corollary**

*If $f$ is an eigenform of type $(p \cdot M, k, \varepsilon)$ where $M$ is prime to $p$, and $\varepsilon$ is of conductor dividing $M$, and if the slope of $f$ is different from $(k-2)/2$ then there is an eigenform $\varphi$ of type $(M, k, \varepsilon)$ whose attached Galois representation is equivalent to that of $f$. If $\varphi$ is a newform, then $f$ has a twin $f'$.*

Is it possible for the twin $f'$ to be *equal* to $f$? Equivalently, is it possible for the polynomial

$$X^2 - \tau_p X + \varepsilon(p) \cdot p^{k-1} \tag{1}$$

to have a double root, i.e., for $(\lambda_p)^2$ to be $\varepsilon(p) \cdot p^{k-1}$?

Ulmer [38] shows that the Conjecture of Birch and Swinnerton-Dyer for a class of elliptic curves over function fields would imply that double roots are impossible for newforms of weight 3, and he conjectures that double roots are never possible; see the discussion in [38] about this and about a recent result of Bas Edixhoven which proves that double roots are impossible for $k = 2$, trivial character and $p > 2$. For this latter result see [8].

In any event if the slope $\alpha$ is distinct from $(k-1)/2$, the polynomial (1) clearly cannot have a double root, and the twins $f$ and $f'$ are indeed distinct.

## §13. Modular representations

We will be principally interested in **modular** representations (a concept which will be formally defined below) and it is important for us, in dealing with these representations, to "carry along" the information of the $U_p$-eigenvalue of the corresponding eigenform, since this information is not exactly recoverable from the Galois representation itself. For the purposes of this article let us make the following somewhat restricted definition of modularity.

Fix a positive integer $N = p \cdot M$ with $M$ relatively prime to $p$. Let $S$ denote the set of prime divisors of $N$.

DEFINITION. Let $A$ be a coefficient ring with residue field $k$. Let $\overline{\rho} : G_{\mathbb{Q},S} \to \mathrm{GL}_2(k)$ be an absolutely irreducible residual representation. A deformation of $\overline{\rho}$ to the coefficient-ring $A$,

$$\rho : G_{\mathbb{Q},S} \to \mathrm{GL}_2(A)\,,$$

is called **modular with "$U_p$-eigenvalue"** $\lambda_p \in A$ (**and of "level"** $N$), if there is:

(i) a classical modular (cuspidal) eigenform $f$ of some weight $k$, some character $\varepsilon$, and of level $N$, and

(ii) a homomorphism $h : \mathcal{O}_f \to A$, taking the $U_p$-eigenvalue of $f$ to $\lambda_p \in A$, such that

(iii) if $m \subset \mathcal{O}_f$ is the inverse image under $h$ of the maximal ideal of $A$, then $\rho_{f,m}$ induces the deformation $\rho$ via $h$, or equivalently, we have a commutative diagram

$$\begin{tikzcd} G_{\mathbb{Q},S} \arrow[r, "\rho_{f,m}"] \arrow[dr, "\rho"'] & \mathrm{GL}_2(\mathcal{O}_{f,m}) \arrow[d, "h"] \\ & \mathrm{GL}_2(A)\,. \end{tikzcd}$$

If the above happens, then the residual representation $\overline{\rho}$ is $\overline{\rho}_{f,m}$.

*Remarks.* It *will* be important a bit later that the levels $N$ we deal with are divisible by $p$ and are not divisible by $p^2$. The reason why there are "quotation-marks" around the words "level" and "$U_p$-eigenvalue" in the definition above is to remind us that a modular representation may be represented by a number of different modular forms $f$, of *possibly different* levels and $U_p$-eigenvalues. In fact, this will be the source of all the fun in §18 below.

Clearly, if $\rho_0$ is a deformation of $\overline{\rho}$, and $\rho_1$ a deformation of $\rho_0$, then if $\rho_1$ is modular, so is $\rho_0$. In particular, if there exists a modular deformation of $\overline{\rho}$, then $\overline{\rho}$ itself is modular. A necessary condition for $\overline{\rho}$ to be modular is that it be odd.[9]

## §14. Families of modular representations

As we shall see, modular representations will come in "families", and we will be giving formal definitions of two distinct types of "families" that arise.

There are families which are, in a certain sense, projective limits of modular representations. These correspond to closed subschemes of $\mathrm{Spec}(R)$ in which modular representations are dense (in a strong sense). Such families will be called *pro-modular representations* and will be defined precisely in the next section. The most interesting of these families have been constructed by Hida ("the ordinary locus") in the case that $\overline{\rho}$ itself is modular and "ordinary".

There are also certain *p-adic analytic families* contained in the universal deformation space $X = \mathrm{Hom}(R(\overline{\rho}), \mathbb{Z}_p)$. It was conjectured in [20] that any classical eigenform is contained in a specific one-parameter analytic family. A qualitative form of this has been recently proved by Coleman [7] as will briefly be described in §16 below.

## §15. Pro-modular representations

A deformation $\rho$ of $\overline{\rho}$ to a coefficient-ring $A$ will be called **pro-modular with "$U_p$-eigenvalue"** $\lambda_p \in A$ (**of "level"** $N$) if we may write $A = \mathrm{proj.\,lim}\,.A_n$ for a sequence of coefficient-rings

$$\ldots \to A_{n+1} \to A_n \to \ldots \to A_0\,,$$

[9] We have insisted, in our definition of modularity, that $p^2$ does not divide the level $N$. If we had accepted all levels $N$, then a celebrated conjecture of Serre would say that the oddness of $\det(\overline{\rho})$ is also a sufficient condition.

such that if $\rho_n$ is the deformation of $\overline{\rho}$ to $A_n$ induced by $\rho$ via the projection $A \to A_n$ then $\rho_n$ is modular with $U_p$-eigenvalue $\lambda_{p,n} \in A_n$ (of level $N$) for all $n \geq 0$, and we have

$$\lim_{n\to\infty} \lambda_{p,n} = \lambda_p \,.$$

We will be interested principally in understanding the locus, in the universal deformation space $X = \mathrm{Hom}(R(\overline{\rho}), \mathbb{Z}_p)$, of the modular, and pro-modular representations with *non-zero* $U_p$-eigenvalues.

If $\overline{\rho}$ is a modular (absolutely irreducible) residual representation with nonzero $U_p$-eigenvalue, Hida has produced a coefficient-ring, call it $\mathbf{T}^\circ$, constructed as a certain completion of a Hecke algebra, which is a finite flat $\wedge$-algebra and he has produced a deformation $\rho^{\mathrm{Hida}}$ of $\overline{\rho}$ to $\mathbf{T}^\circ$ which is pro-modular in the above sense with $U_p$-eigenvalue $u^{\mathrm{Hida}}$ which is a unit in $\mathbf{T}^\circ$. For a discussion of this theory, and for an extensive bibliography of the relevant literature, see [22]. Hida also shows that the specialization of $\rho^{\mathrm{Hida}}$ to integral weights $k = 2, 3, \ldots$ are representations attached to classical modular eigenforms. Hida's pro-modular deformation is ordinary (e.g., see §7.5 of [22]) and therefore there is a natural homomorphism

$$\varphi : R^\circ \to \mathbf{T}^\circ \,,$$

which is easily seen to be surjective. Moreover, the image of the unit $u^\circ$ (as described in §4 above) under $\varphi$ is the $U_p$-eigenvalue $u^{\mathrm{Hida}}$. In [27] (see also §6 of [26]) it was conjectured that this homomorphism is an isomorphism. The recent results of Wiles and Taylor-Wiles establish this type of result (and of course much more). Their results include, for example, the following special case:

**Theorem (Wiles, Taylor-Wiles):**

*Let $L = \mathbb{Q}(\sqrt{p^*})$ where $p^* = (-1)^{(p-1)/2} \cdot p$. Let $\overline{\rho}$ be an ordinary modular residual representation of level $p$, such that $\overline{\rho}$ restricted to $G_L$ is absolutely irreducible. Then $\varphi : R^\circ \to \mathbf{T}^\circ$ is an isomorphism. The universal ordinary deformation $\rho^\circ$ of $\overline{\rho}$ to $R^\circ$ is pro-modular, with $U_p$-eigenvalue $u^\circ$.*

*Proof.* This is contained in Theorem 3.3 of [39]. See also the Theorem in the appendix of [37]. Despite the fact that the above Theorem is a statement about eigenforms of arbitrary weights its proof (in [39]) ultimately rests on an understanding of the weight two case. Here is a sketch of how to deduce the Theorem from statements in weight two: The homomorphism $\varphi$ is surjective since $\mathbf{T}^\circ$ is generated as $\wedge$-algebra by the elements $T_\ell$ for $\ell \neq p$ and by $U_p$ and each of these elements is in the image of $R^\circ$ as can easily be seen (cf. §5 of [26]). Let $J = \ker(\varphi)$ and consider the exact sequence of $\wedge$-modules,

$$0 \to J \to R^\circ \to \mathbf{T}^\circ \to 0\,.$$

Now use Wiles' results in weight two (e.g., the Theorem 3.21 given in [9]) to get that under the hypotheses stated in the Theorem above $\varphi$ induces an isomorphism "in weight two", i.e., if $s_2 : \wedge \to \mathbb{Z}_p$ is the homomorphism "specialization to weight two", then $\varphi \otimes \mathbb{Z}_p : R^\circ \otimes_\wedge \mathbb{Z}_p \to \mathbf{T}^\circ \otimes_\wedge \mathbb{Z}_p$ is an isomorphism, where the tensor product with $\mathbb{Z}_p$ is via $s_2$. Tensoring the exact sequence above with $\mathbb{Z}_p$ over $\wedge$ (via $s_2$) and using the fact that $\mathbf{T}^\circ$ is flat over $\wedge$, we get that $J \otimes_\wedge \mathbb{Z}_p$ vanishes, and hence so does $J$ by Nakayama's lemma. □

## §16. $p$-adic analytic families of modular representations

This part of the theory is in great flux at the moment. For example, Coleman has already proven theorems a good deal stronger (see [7]) than those needed in this section.

Fix $M$ a positive integer prime to $p$, and put $N = p \cdot M$.

Let $X = \mathrm{Hom}_{\mathbb{Z}_p}\big(R(\overline{\rho}), \mathbb{Z}_p\big)$ be the universal deformation space of an absolutely irreducible, modular, residual representation $\overline{\rho}$ of "level" $N = p \cdot M$. Although this is not really necessary, assume that the deformation problem for $\overline{\rho}$ is unobstructed.

The $p$-adic **disc** $D$ **of radius** $\nu$ **about** $k_0$ in $\mathbb{Z}_p$ is the open sub-set $D = \{s \in \mathbb{Z}_p \,|\, s \equiv k_0 \bmod p^\nu\}$ viewed as $p$-adic manifold. Any such will be simply called a "disc". We view the ring of rational integer $\mathbb{Z}$ as a subring of $\mathbb{Z}_p$. By an **arithmetic progression** $\mathcal{K}$ in a disc $D$ we mean an arithmetic progression of positive integers $\kappa = \kappa_0 + m \cdot t$ where $t = 0, 1, 2, \ldots$ which happen to lie in $D \subset \mathbb{Z}_p$. The "m" in this formula will be referred to as the **modulus** of the arithmetic progression.

An element $\tau \in R(\overline{\rho})$ may be viewed as a function on $X$ in the evident way: $\tau(\varphi) := \varphi(\tau)$ where $\varphi : R(\overline{\rho}) \to \mathbb{Z}_p$ is a $\mathbb{Z}_p$-algebra homomorphism, i.e., $\varphi$ is an element of $X$. If $D$ is a disc as above, a function $f : D \to X$ will be called **strictly analytic** if, for all $\tau \in R(\overline{\rho})$, the composite function $\tau \circ f : D \to \mathbb{Z}_p$ can be expressed as a power series

$$\tau \circ f(w) = \sum_{\nu \geq 0} a_\nu(\tau) w^\nu\,, \quad a_\nu(\tau) \in \mathbb{Z}_p$$

(convergent for all $w \in D$).

DEFINITION 1. A $p$-**adic analytic family of modular representations** $(D; z, u)$ in the universal deformation space $X$ **of level** $N$ is a disc $D$, as above, a strictly analytic mapping of $D$ to $X$

$$z : D \to X\,,$$

together with a strictly analytic, nowhere-vanishing, function

$$u : D \to \mathbb{Z}_p\,,$$

such that for an arithmetic progression of integers $\mathcal{K}$ lying in $D$, which is topologically dense in $D$, the representation $\rho_k$ associated to the point $x = z(k) \in X$ is modular of level $N = p \cdot M$ weight $k$, and character $\varepsilon$, with $U_p$-eigenvalue $u(k)$, for $k \in \mathcal{K}$. [*Merely for convenience of notation,*] we make the additional hypothesis that the character $\varepsilon$ is constant and that $\mathrm{ord}_p(u(k)) = \alpha \in \mathbb{Q}$ is constant, i.e., independent of $k \in \mathcal{K}$; we shall say that the $p$-adic analytic family has **character** $\varepsilon$, and **slope** $\alpha$. An arithmetic progression $\mathcal{K}$, topologically dense in $D$, with the properties described above exhibiting $(D; z, u)$ as a $p$-adic analytic family of modular forms will be referred to as an **arithmetic progression of modular forms** attached to the family.

DEFINITION 2. A **modular arc** in $X$ is the image $C := z(D) \subset X$ of a $p$-adic analytic family of modular representations.

**Lemma**

*Let $C \subset X$ be a modular arc. Then $C$ is contained in the Sen null space $X_0 \subset X$. Restricting the log-determinant mapping $\delta : X \to \mathbb{Z}_p(x \longmapsto r_x + s_x$ as defined in §7 above) to the modular arc $C$, we have that the composition,*

$$D \xrightarrow{z} C \xrightarrow{\delta} \mathbb{Z}_p\,,$$

*is the mapping $d \longmapsto d + 1$.*

*Proof.* For $k$ in the dense subset $\mathcal{K} \subset D$ we do have that $z(k)$ lies in $X_0$ and the composition $\delta(z(k)) = k + 1$. By continuity of $z$ and $\delta$ the second statement follows; by Sen's Theorem [34] it follows that all of $z(D)$ lies in $X_0$ since the dense subset $z(\mathcal{K})$ does. □

The following result is a straightforward application of Robert Coleman's work; in particular, of Corollary 10.4.2. in [7] (draft of Aug. 1995), and of [6].

**Theorem**

*Let $\alpha$ be a non-negative rational number, and $k_0$ an integer such that $k_0 > \alpha + 1$. Let $f$ be an eigenform of level $N = p \cdot M$ weight $k_0$, and trivial character. Suppose that $f$ is "new away from $p$". Let $m \subset \mathcal{O}_f$ be a maximal ideal of residual characteristic $p$ such that the completion $\mathcal{O}_{f,m}$ is isomorphic to $\mathbb{Z}_p$. Suppose further that $(\lambda_p)^2 \neq p^{k_0-1}$, where $\lambda_p$ is the $U_p$-eigenvalue of $f$. Let $\rho = \rho_{f,m}$ and suppose that $\overline{\rho} := \overline{\rho}_{f,m}$ is absolutely irreducible. Let $X = \mathrm{Hom}_{\mathbb{Z}_p}(R(\overline{\rho}), \mathbb{Z}_p)$ be the universal deformation space of $\overline{\rho}$, and denote by $x_0 \in X$ the point corresponding to $\rho$.*

*Then there is a $p$-adic analytic family of modular representations $(z, u)$ defined on some disc $D$ such that $z(k_0) = x_0 \in X = X(\overline{\rho})$, and $u(k_0) = \lambda_p$.*

**Note.** In the case where $u_p(\rho)$ is a *unit,* i.e., where $\rho$ is ordinary, this result follows immediately from Hida's theory, and in that case the family is better than $p$-adic analytic: it is pro-modular, and "parametrized" by $\mathrm{Spec}(R^\circ)$, a subscheme of $\mathrm{Spec}(R)$.

*Proof.* Coleman's Corollary 10.4.2 in [7] gives us a ($p$-adic analytically) parametrized family of $p$-adic overconvergent eigenforms $f_k$ of fixed slope $\alpha$, parametrized by $p$-adic weight $k$ ($k$ in a disc $D$) such that $f_{k_0} = f$, and such that the Fourier coefficients $a_n(k) :=$ *$n$-th* Fourier coefficient of $f_k$ is a $p$-adic analytic function on $D$ for each $n \geq 0$ taking values in $\mathcal{O}_{f,m}$ and such that for each $n$ the image of $a_n(k)$ in the residue field of $\mathcal{O}_{f,m}$ is independent of $k$. By its construction together with a prior result of Coleman [6] if $k \in \mathbb{Z}$ is strictly greater than $\alpha + 1$, then the overconvergent modular form $f_k$ is a *classical* eigenform on $\Gamma_0(N)$ with character $\varepsilon_k$ where $\varepsilon_k$ depends only on $k$ modulo $p-1$. Restricting to those $k$'s with $k \equiv k_0$ modulo $p-1$ and $k > \alpha + 1$, we have that $f_k$ is a classical eigenform on $\Gamma_0(N)$. Moreover, letting

$$\rho_k : G_{\mathbb{Q},S} \to \mathrm{GL}_2(\mathcal{O}_{f,m})$$

denote the Galois representation attached to $f_k$ we have that the underlying residual representation is $\overline{\rho}$, which by hypothesis is absolutely irreducible. We can determine $k_0$ modulo $p-1$ by the formula $\det(\overline{\rho}) = \omega^{k_0-1}$, where $\omega$ is the character given by the action of $G_{\mathbb{Q},S}$ on the group $\mu_p$ of $p$-th roots of unity. Let $x_k$ denote the point in the universal deformation space $X$ which classifies $\rho_k$. We must show that the function $z : k \longmapsto x_k$ uniquely extends to a continuous function from $D$ to $X$. Recall that any element $\tau \in R(\overline{\rho})$ may be viewed as $\mathbb{Z}_p$-valued function on the universal deformation space

$$X = \mathrm{Hom}_{\mathbb{Z}_p\text{-alg}}(R(\overline{\rho}), \mathbb{Z}_p)\,.$$

To check that the function $z : D \to X$ is continuous it suffices to check that the compositions $\tau \circ z : D \to \mathbb{Z}_p$ are continuous for all $\tau \in R(\overline{\rho})$, or equivalently for a set $\mathcal{T}$ of $\tau \in R(\overline{\rho})$ which generate $R(\overline{\rho})$ as $\mathbb{Z}_p$-algebra. It follows from the "Schur-type result" proven by Carayol [5] or by Serre [32] (compare also the weaker Prop. 4 in §1.8 of [25]) that the Hecke operators $T_\ell$ for prime numbers $\ell \neq p$ generate $R(\overline{\rho})$. It follows from the previous discussion, the composite functions $(T_\ell \circ z)(k) = a_\ell(k)$ are $p$-adic analytic functions for all $\ell$, which proves the Theorem. □

## §17. The geometry of modular arcs

For the discussion below, we will simplify things a bit and assume that $M = 1$, i.e., that we are dealing with eigenforms of level $N = p$. The discussion from now on in this article is joint work with F. Q. Gouvêa: it simply makes explicit some of the structure which we had already conjectured to be the case in [20], and which now is indeed the case, thanks to Coleman's work. Gouvêa and I will be treating this subject and its applications, in more detail in forthcoming publications.

In view of the Theorem of §16, and, more specifically, the discussion occurring within its proof, an eigenform $f$ of level $p$, of weight $k_0$, trivial character, and slope $\alpha < k_0$ gives rise to an analytic family of slope $\alpha, (D; z, u)$, such that $z(k_0)$ is the Galois representation attached to $f, u(k_0)$ is the $U_p$-eigenvalue of $f$, and the related arithmetic progression $\mathcal{K}$ may be taken (and *will* be taken) to be the following. Let $r_0$ denote the integer $0 \leq r_0 < p-1$ such that $k_0 \equiv r_0 \bmod p-1$. Let $P$ denote the arithmetic progression

$$P := \left\{ r_0 + (p-1) \cdot t \,|\, t \in \mathbb{Z},\ t > (\alpha + 1 - r_0)/(p-1) \right\}.$$

We take $\mathcal{K} := P \cap D$. It will be important for us that $\mathcal{K}$, so defined, is determined entirely by the data $D, \alpha$, and the underlying residual representation $\overline{\rho}$ (the determinant of $\overline{\rho}$ is used to compute $r_0$ as mentioned in the proof of the theorem of §16). Of course, $\mathcal{K}$ is just an arithmetic progression of the form $k_0 + (p-1)p^\nu \cdot m$ for $m$ ranging through integers $\geq$ some fixed integer $m_0$.

**Lemma 1**

*Let $(D; z, u)$ be an analytic family of slope $\alpha$ with its associated dense arithmetic progression "of modular forms" $\mathcal{K} \subset D$ as above, and let $(D'; z', u')$ of slope $\alpha'$ be another, with associated dense arithmetic progression "of modular forms" $\mathcal{K}' \subset D'$. Let $C$, and $C'$ be their respective images in $X_0$. Let $D \cap D'$ be the intersection. If $C \cap C'$ is infinite, then the $p$-adic analytic families $(D \cap D'; z, u)$ and $(D \cap D'; z'u')$ are equal.*

*Proof.* By the Lemma of §16 (which says that, up to translation by 1, $z$ and $z'$ are liftings of the log-determinant projections $\delta : C \to D$, and $\delta : C' \to D'$) it follows that $z$ and $z'$ agree on the inverse images

$$z^{-1}(C \cap C') = z'^{-1}(C \cap C')$$

and this common inverse image $Y$ lies in $D \cap D'$; moreover, $z_{|Y}(= z'_{|Y})$ maps $Y$ homeomorphically onto $C \cap C'$. Since $D \cap D'$ is therefore infinite (hence non-empty) one of the discs $D, D'$ is included in the other, say $D \subset D'$. Without loss of generality, we may restrict $z'$ and $u'$ to the subdisc $D$ in $D'$, i.e., we may (and do) now assume that $D = D'$. Since $z$ and $z'$ are both strictly analytic on the compact disc $D$ and $Y$ is infinite, it follows that $z = z'$ on the whole disc $D$, and therefore the modular arcs $C = z(D)$ and the restriction of $C' = z'(D)$ are equal. Now let $\mathcal{K}_0 = \mathcal{K} \cap \mathcal{K}'$ which, by the discussion at the beginning of this section, is again an arithmetic progression of modulus $(p-1)p^{\nu}$, where $\nu$ is the radius of $D$. For each $k_0 \in \mathcal{K}_0$ for which $u(k_0) \neq u'(k_0)$ we have that the Galois representation "classified" by the point $z(k_0) = z'(k_0) \in X$ corresponds to two eigenforms of level $p$ (and trivial character $\varepsilon$) with distinct $U_p$-eigenvalues $u(k_0)$ and $u'(k_0)$. By the Proposition 1 of §12 these must be twins and therefore $k_0 = \alpha + \alpha' + 1$, i.e., $k_0$ is uniquely determined. In particular $u$ and $u'$ can differ on *at most one point in* $\mathcal{K}_0$. Since $\mathcal{K}_0$ is infinite, and $u$ and $u'$ are strictly analytic on $D$, it follows that $u = u'$ on $D$. □

**Corollary**

*Any modular arc $C \subset X$ is the image of a* unique *$p$-adic analytic family.*

Definition. The **slope** of a modular arc is the slope of the (unique) family of which it is the image.

**Lemma 2**

*Let $(D; z, u)$ be an analytic family of slope $\alpha$ with its associated dense arithmetic progression "of modular forms" $\mathcal{K} \subset D$ as above, and let $(D'; z', u')$ of slope $\alpha'$ be another, with associated dense arithmetic progression "of modular forms" $\mathcal{K}' \subset D'$. Let $C$, and $C'$ be their respective images in $X_0$. If $\alpha \neq \alpha'$, then the intersection of $z(\mathcal{K})$ and $z'(\mathcal{K}')$ is either empty or else it consists of a single element.*

*Proof.* This argument is very similar to the proof of Lemma 1. If $x$ is in the intersection of $z(\mathcal{K})$ and $z'(\mathcal{K}')$ it follows that $x$ is associated to two classical modular eigenforms, call them $f$ and $f'$, both of level $p$, of some common weight $k$ and of slopes $\alpha$ and $\alpha'$ respectively. Since $\alpha$ is assumed distinct from $\alpha'$, it follows that $f$ and $f'$ are distinct eigenforms. It follows from Proposition 2 of §12 that $f$ and $f'$ are twins, so $k = \alpha + \alpha' + 1$; i.e., the weight $k$ is uniquely determined and therefore so is $x$. □

**Question.** Is it true that any two modular arcs (level $p$) which meet in $X$ have the property that one lies inside the other, or else their intersection consists of a single point (corresponding to a classical newform of level 1)?

## §18. The modular locus of level $p$ in $X$ contains the image of an "infinite fern"

We keep to the simplest case, i.e., the "$M$" of previous §'s is assumed to be 1. Let $S = \{p\}$. Fix, then, $\overline{\rho}$, an absolutely irreducible Galois representation

$$\overline{\rho} : G_{\mathbb{Q},\{p\}} \to \mathrm{GL}_2(\mathbf{F}_p)$$

which is assumed modular in the sense that $\overline{\rho}$ is the residual representation of some eigenform of level $p$. Assume that the deformation problem for $\overline{\rho}$ is unobstructed. We also want $\overline{\rho}$ to satisfy the following hypothesis. Say that an eigenform $f$ of weight $k$ and slope $\alpha$ is of **noncritical slope** if $0 < \alpha < k - 1$.

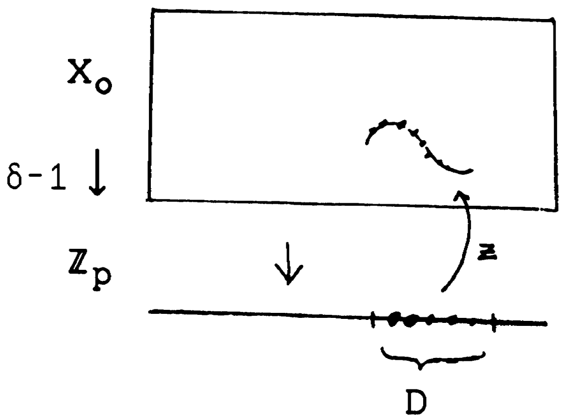
**Hypothesis.** The residual representation $\overline{\rho}$ is "modular of level $p$, with trivial character" in the sense that there is an eigenform $f$ of level $p$, trivial character, and noncritical slope such that if $\mathcal{O}_f$ is the ring of Fourier coefficients of $f$, there is a maximal ideal $m \subset \mathcal{O}_f$ such that the completion $\mathcal{O}_{f,m}$ is isomorphic to $\mathbb{Z}_p$ and such that the residual representation $\overline{\rho}_{f,m}$ attached to $f$ and the maximal ideal $m$ is equivalent to $\overline{\rho}$.

As in the preceding §'s, we denote by $X$ the universal deformation space of $\overline{\rho}$, and recall the Sen null space $X_0 \subset X$ defined in §7.

By the (**level** $p$) **modular locus** $\Omega \subset X_0$ let us mean the *set-theoretic* union in $X_0$ of all modular arcs (of level $p$) in $X$. As defined, $\Omega$ is a countable union of analytic arcs in $X_0$. The structure of $\Omega$ was provisionally sketched in [20] (i.e., before Coleman's Theorem had been proved) and has an intriguing point-set topological character.

By the above **Hypothesis,** there is a point $x \in X$ whose associated representation $\rho_x$ is $\rho_{f,m}$, i.e., is a "modular point of level $p$" with trivial character $\varepsilon$ and such that $f$ has noncritical slope. By Coleman's work, i.e., the Theorem of §16 cited above, there is a $p$-adic analytic modular family of level $p$, $(D; z, u)$ with trivial character $\varepsilon$, whose slope is equal to $\alpha =$ the slope of the eigenform $f$, such that $z(k) = x \in X$, and such that $u(k)$ is the $U_p$-eigenvalue of $f$. Denote by $C$ the modular arc in $X$ which is the image $z(D) \subset X$, and let $\mathcal{K} \subset D$ denote the dense arithmetic progression possessing the properties postulated in Definition 1 of §16.

**Diagram 1. A modular arc in the analytic surface $X_0$ (the dots representing the arithmetic progression of modular eigenforms $\mathcal{K} \subset D$)**




The modular arc $C$ of slope $\alpha$

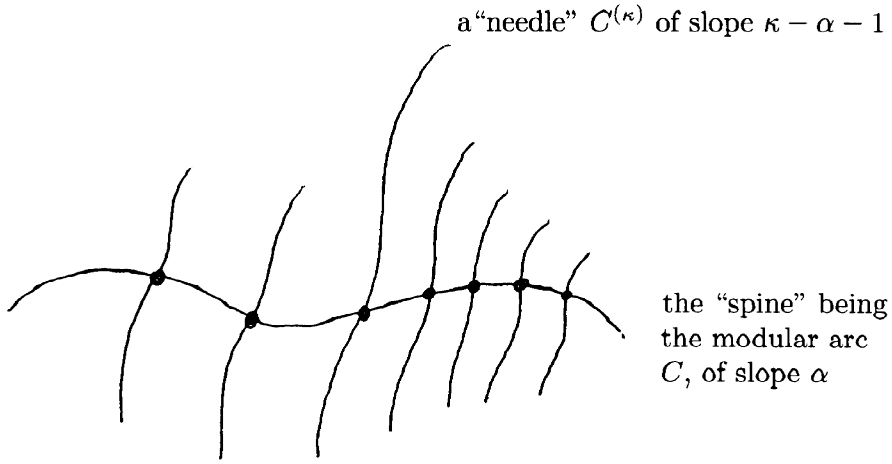
Let $\mathcal{K}_0 \subset \mathcal{K}$ denote the subset of integers $\kappa$ of the arithmetic progression $\mathcal{K} \subset \mathcal{D}$ such that $\kappa > \alpha + 1$, and $\kappa \neq 2\alpha + 2$. The subset $\mathcal{K}_0$ is topologically dense in $D$, since $\mathcal{K}$ is. The associated modular form $f_\kappa$ of level $p$ for $\kappa \in \mathcal{K}_0$ is not new, i.e., $f_\kappa$ comes from a newform $\varphi_\kappa$ of level 1 (Proposition 2 of §12). Consequently, attached to each $f_\kappa$ for $\kappa \in \mathcal{K}_0$ we have its "evil twin" $f'_\kappa$ as in §12, whose slope is $\alpha' = \kappa - 1 - \alpha$. Therefore $f'_\kappa$ is of noncritical slope, since $f_k$ is. For all $\kappa \in \mathcal{K}_0$, we then have that $\alpha' \neq \alpha$ and therefore, $f_\kappa$ and $f'_\kappa$, having distinct slopes, are indeed distinct. Of course $f_\kappa$ and $f'_\kappa$, being twins, correspond to equivalent Galois representations, and therefore they correspond to same point, call it $x_\kappa$ in $C \subset X_0 \subset X$.

The Theorem of §16 then applies anew to the points $x_\kappa$ in the analytic arc $C \subset X_0$ corresponding to each of these modular eigenforms $f'_\kappa$ for $\kappa$ ranging through

$\mathcal{K}_0 \subset D$. In particular, we may imbed each $x_\kappa$ in its own *p-adic* analytic modular arc $C^{(\kappa)} \subset X_0$ of level $p$, of trivial character, and of slope $\alpha^{(\kappa)} = \kappa - \alpha - 1$. This gives us an infinite collection of modular arcs, indexed by $\kappa$ running through the set $\mathcal{K}_0$. □

We already have the image of this kind of configuration (the beginning of a "fern") contained in the modular locus $\Omega \subset X$:

**Diagram 2. The "simple fern" mapping to the analytic surface $X_0$.**




For a canonical picture which most handily allows us to discuss things, let us accept the convention that Diagram 2 represents the topological space given by the union of $C$ and the $C^{(\kappa)}$ with the indicated intersections, and given the weakest topology such that the injections of $C$ and of each of the $C^{(\kappa)}$'s induces homeomorphisms onto their images.

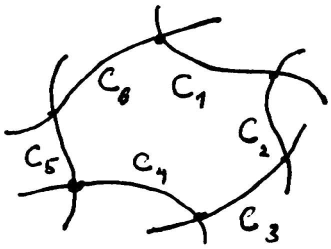
What we haven't yet any information about is

(i) whether or not the mapping of the "simple fern" to $\Omega$ is injective; equivalently we don't know anything about the nature of the intersections of some needle $C^{(\kappa_0)}$ with the other needles $C^{(\kappa)}$ in $\Omega \subset X$,

(ii) even if it were injective, the extent to which this mapping fails to be a homeomorphism onto its image (and I can't imagine that it will actually be a homeomorphism!).

To ask a somewhat more flexible question along the lines of (i) let us introduce the notion of an $n$-gon of modular arcs:

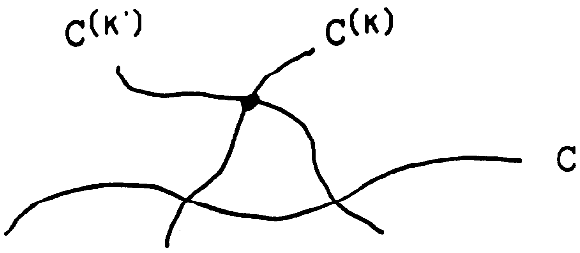
Definition. Let $n$ be an integer $> 1$. An *$n$-gon* of modular arcs is a sequence of modular arcs $C_1, C_2, \ldots, C_n$ (of level $p$) in $X$ such that for $i \neq j$, the arcs $C_i$ and $C_j$ have at most finite intersection, and $C_i$ and $C_{i+1}$ meet (for $i = 1, \ldots, n-1$) as do $C_n$ and $C_1$:




I don't know of any example of an $n$-gon (any $n > 1$) of modular arcs. Do they exist?

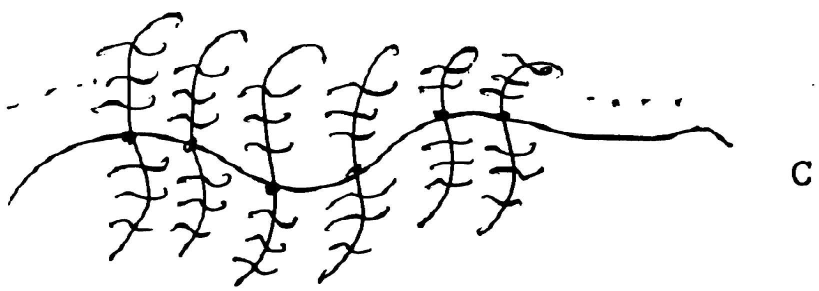
For example, if, in the image in $\Omega$ of Diagram 2 there are two distinct needles $C^{(\kappa)}$ and $C^{(\kappa\prime)}$ with non-trivial intersection, we would have a "3-gon" ("triangle", one should rather say) of modular arcs. Do 3-gons exist?

**Diagram 3. Are there nontrivial intersections?**



The configuration we have produced so far (Diagram 2) consists of an analytic arc $C$ (which we will call the **spine**) and a countable set of analytic arcs $C^{(\kappa)}$ (the **needles**) intersecting the spine in a topologically dense set. Of course, this procedure "iterates" and so each of these $C^{(\kappa)}$'s may be viewed in turn as spines in their own right, and therefore (by iterated application of the Theorem of §16) they have needles of their own intersecting themselves densely, and so on. The configuration of all these modular arcs is contained in $\Omega$. As with the simple fern we may envision the ultimate union of iterated "spines and needles" of modular arcs in $\Omega$ that has been produced by this process as the *image* of an "infinite fern" as shown below, in $\Omega \subset X_0$.

**Diagram 4. The "infinite fern".**



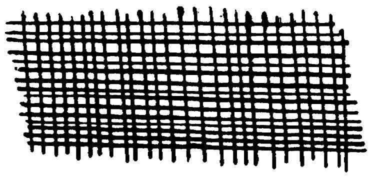

Nevertheless, here, in contrast to the case of the image of the simple fern, we do *not* even know whether the mapping of Diagram 4 to $\Omega$ brings distinct arcs to distinct arcs in $\Omega$. A natural question that comes to mind in this regard is whether the image of the infinite fern "forms something like a weave-pattern". To ask this more precisely we shall make a definition:

DEFINITION. For $\mathcal{A}, \mathcal{B} \subset \mathbb{Z}_p$ countable dense subsets, denote by $W(\mathcal{A}, \mathcal{B})$ the topological subspace

$$W(\mathcal{A}, \mathcal{B}) := \mathcal{A} \times \mathbb{Z}_p \cup \mathbb{Z}_p \times \mathcal{B} \subset \mathbb{Z}_p \times \mathbb{Z}_p\,.$$

If $Y$ is two-dimensional $p$-adic manifold, and $W \subset Y$ a topological subspace, we shall say that the pair $(Y, W)$ is a **dense weave** (locally at a point $y \in Y$) if there are countable dense subsets $\mathcal{A}, \mathcal{B} \subset \mathbb{Z}_p$ and a $p$-adic analytic isomorphism of a neighborhood $\mathcal{Y}$ of $y \in Y$ onto an open subset $\mathcal{O} \subset \mathbb{Z}_p \times \mathbb{Z}_p$ which brings $\mathcal{Y} \cap W$ homeomorphically onto $\mathcal{O} \cap W(\mathcal{A}, \mathcal{B})$.

**Diagram 5. A "dense weave".**



**Question.** Is the pair $(X_0, \Omega)$ locally a dense weave at some points $x_0$ of $X_0$?

**Further Questions:**

**1)** Let $\overline{\Omega}$ denote the topological closure of $\Omega$ in $X_0$. Are there $\overline{\rho}$'s for which $\overline{\Omega}$ contains a non-empty open subset of $X_0$? Are there $\overline{\rho}$'s for which $\overline{\Omega}$ is equal to $X_0$?

**2)** If $X_0$ contains one point attached to modular eigenforms of level $p^2$ (or $p^n$ for $n > 1$) does it contain an infinite number of such points?

**3)** (**Katz modular forms**; cf [23], [17]). Any element of $\overline{\Omega}$, and even of the saturation of $\overline{\Omega}$ under the twist-action described in §5, is represented by a "Katz modular eigenform" (in the kernel of $U_p$). Is every point of $X$ so represented?

## References

1. O. Atkin and J. Lehner, Hecke operators on $\Gamma_0(m)$, *Math. Ann.* **185** (1970), 134–160.
2. G. Böckle, *Universal deformations of even Galois representations and relations to Maass wave forms,* PhD thesis, Univ. of Ill. at Urbana-Champaign, 1995.
3. N. Boston, Explicit deformation of Galois representations, *Invent. Math.* **103** (1991), 181–196.
4. N. Boston and B. Mazur, Explicit universal deformations of Galois representations, *Algebraic number theory in honor of K. Iwasawa,* Advanced Studies in Pure Math. series, **17** Academic Press, 1989, 1-21.
5. H. Carayol, Formes modulaires et représentations galoisiennes à valeurs dans un anneau local complet, *p-adic Monodromy and the Birch-Swinnerton-Dyer Conjecture* (eds. B. Mazur and G. Stevens) Contemporary Mathematics **165**, Amer. Math. Soc., 1994, 213-237 .
6. R. Coleman, Classical and overconvergent modular forms, preprint, to appear in *Invent. Math.*
7. R. Coleman, $p$-adic Banach spaces and families of modular forms, preprint (August 1995), to appear in *Invent. Math.*
8. R. Coleman and B. Edixhoven, Simplicity of Frobenius eigenvalues and the galois representations associated to modular forms, to appear.

9. H. Darmon, F. Diamond and R. Taylor, Fermat's Last Theorem, *Current Developments in Mathematics*, (eds. R. Bott, A. Jaffe, S.T. Yau), International Press, 1995.
10. P. Deligne, Formes modulaires et représentations $\ell$-adiques, *Lecture Notes in Math.* **179** (1971), 139–172. Springer-Verlag.
11. P. Deligne and J.P. Serre, Formes modulaires de poids 1, *Ann. Sci. École Norm. Sup.* **7** (1974), 507–530.
12. C. Doran and S. Wong, *The deformation theory of Galois representations*, in preparation.
13. N. Elkies, The existence of infinitely many supersingular primes for every elliptic curve over $\mathbb{Q}$, *Invent. Math.* **89** (1987), 561–567.
14. G. Faltings, Hodge-Tate structure and modular forms, *Math. Ann.* **278** (1987), 133–149.
15. M. Flach, A finiteness theorem for the symmetric square of an elliptic curve, *Invent. Math.* **109** (1992), 193–223.
16. J.M. Fontaine and B. Mazur, Geometric Galois representations, *Proceedings of the Conference on Elliptic Curves and Modular Forms, Hong Kong, Dec. 18-21 1993*, (eds. J. Coates and S.T. Yau), International Press, 1995, 41-78.
17. F. Gouvêa, *Arithmetic of $p$-adic modular forms*, Lecture Notes in Math. 1304, Springer-Verlag, 1988.
18. F. Gouvêa, On the ordinary Hecke algebra, *J. Number Theory* **41** (1992), 178–198.
19. F. Gouvêa, Deforming Galois representations: a survey, *Seminar on Fermat's Last Theorem*, (ed. V.K. Murty) Canadian Math Soc. Conference Proceeding (to appear).
20. F. Gouvêa and B. Mazur, Families of modular eigenforms, *Math. Comp.* **56** (1992), 793–806.
21. B. Gross, A tameness criterion for Galois representations associated to modular forms mod $p$, *Duke Math. J.* **61** (1990), 445–517.
22. H. Hida, *Elementary theory of $L$-functions and Eisenstein series*, London Math. Soc. (Student Texts) **26** , Cambridge Univ. Press, 1993.
23. N. Katz, $p$-adic properties of modular schemes and modular forms, pp. 69–190 in Modular functions of one variable, *Lecture Notes in Math.* **350**, Springer-Verlag, 1973.
24. S. Lang and H. Trotter, *Frobenius distributions in $GL_2$-extensions,* Lecture Notes in Math. 504, Springer-Verlag, 1976.
25. B. Mazur, Deforming Galois representations, pp. 385–437 in *Galois groups over* $\mathbb{Q}$ (eds. Y. Ihara, K. Ribet, J.P. Serre), Mathematical Sciences Research Institute Publications **16**, Springer-Verlag, 1989.
26. B. Mazur, Two-dimensional $p$-adic Galois representations unramified away from $p$, *Comp. Math.* **74** (1990), 115–133.
27. B. Mazur and J. Tilouine, Représentations galoisiennes, différentielles de Kähler et conjectures principales, *Publ. Math. IHES* **71** (1969), 65–103.
28. A. Ogg, On the eigenvalues of Hecke operators, *Math. Ann.* **179** (1969), 101–108.
29. J.P. Serre, *Lie algebras and Lie groups*, Lecture Notes in Math. 1500, Springer-Verlag, 1992.
30. J.P. Serre, Propriétés galoisiennes des points d'ordre fini des courbes elliptiques, *Invent. Math.* **15** (1972), 259–331.
31. J.P. Serre, Quelques applications du théorème de densité de Chebotarev, *Publ. Math. I.H.E.S.* **54** (1985), 123–201.

32. J.P. Serre, Représentations linéaires sur des anneaux locaux, d'après Carayol, Preprint 1995.
33. S. Sen, Continuous cohomology and $p$-adic Galois representations, *Invent. Math.* **62** (1981), 89–116.
34. S. Sen, Analytic variation of $p$-adic Hodge structure, *Ann. of Math.* **127** (1988), 647–661.
35. G. Shimura, *Introduction to the Arithmetic Theory of Automorphic Functions,* Princeton Univ. Press, 1971.
36. J. Tate, $p$-Divisible groups, pp. 158–183 in *Proceedings of a Conference on Local Fields,* (held in Driebergen 1966), Springer, 1967.
37. R. Taylor and A. Wiles, Ring-theoretic properties of certain Hecke algebras, *Ann. of Math.* **141** (1995), 553–572.
38. D. Ulmer, A construction of local points on elliptic curves over modular curves, *Int. Math. Research Notices (IMRN)* **7** (1995), 349–363.
39. A. Wiles, Modular elliptic curves and Fermat's Last Theorem, *Ann. of Math.* **141** (1995), 443–551.
40. D. Zagier, Modular parametrization of elliptic curves, *Canad. Math. Bull.* **28** (1985), 372–384.