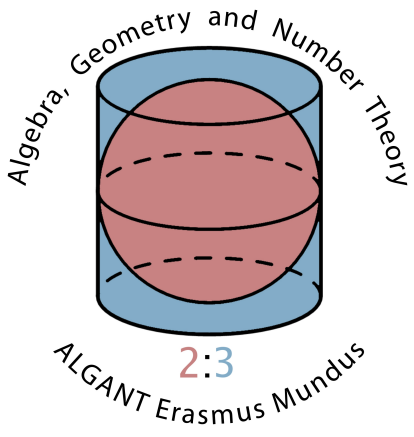
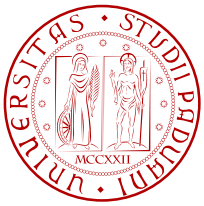


Deformations of Galois Representations

Clara Lacroce

Advised by Prof. Dr. Adrian Iovita



Università degli studi
di Padova

Concordia
University

ALGANT Master's Thesis - 20 July 2016

Abstract

Deformations of Galois representations

Clara Lacroce

In this thesis we study a paper by Barry Mazur ([11]) about deforming Galois representations. In particular we will prove that, if $\bar{\rho} : \Pi \to \mathrm{GL}_N(k)$ is an absolutely irreducible residual representation, a universal deformation ring $R = R(\Pi, k, \bar{\rho})$ and a universal deformation $\boldsymbol{\rho}$ of $\bar{\rho}$ to R exist. This result is part of the proof of the modularity conjecture.

The modularity conjecture is of great importance since it states a connection between modular forms and elliptic curves over $\mathbb{Q}$, providing a great tool to study the arithmetic properties of those elliptic curves. Andrew Wiles studied the conjecture as a part of the more general problem of relating two-dimensional Galois representations and modular forms and used [11] to complete his construction.

To better understand the proof of Mazur, we will analyze in detail the paper of Michael Schlessinger ([13]). This article, which is focused on functors over Artin rings, provides a criterion for a functor to be pro-representable. Moreover, it gives the definition of a "hull", which is a weaker property than pro-representability.

To Silvano Gregori,
who guided me to this world.

Acknowledgments

I am sincerely grateful to Professor *Adrian Iovita*, for the patience in dealing with me and for his constant help during the developing of this Thesis. A big thanks goes to him also for all the advice he gave me during the year in Canada and for the devotion and inspiring passion he shows in his work.

My warmest acknowledgment goes to *Maria Rosaria Pati*, friend and irreplaceable workmates. I am thankful for all her precious and infinite help: having the chance of working on Schlessinger's paper together it has been stimulating and challenging.

My deepest gratitude goes to *Lucas Berry*, for his perseverance and his constant and unconditional support, and *Mattia Tinotti*, for his incredible intuition and for the advice he always give me in LaTeX.

I would like to thank the graduate students of Concordia Math Department, my second family, in particular the number theorists *Fabian Franken*, for the corrections, *Patrick Meisner* and *Jake Chinis* for the suggestions.

I finally want to acknowledge my *family*, who always respect, support and encourage me in every choice of my life.

Contents

Chapter 1

Background Material

1.1 Group Theory

1.1.1 Inverse limits

We are now going to define the concept of inverse limit in the more general setting of category theory ([6]).

Definition 1.1. A ***directed set*** is a partially ordered set A in which for any $\alpha, \beta \in A$ there exists $\gamma \in A$ such that $\alpha \leq \gamma$ and $\beta \leq \gamma$.

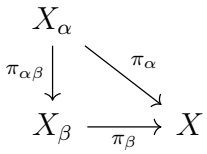
Definition 1.2. Let C be a category, an ***inverse system*** in C consists of a directed set A, a collection of objects $\{X_\alpha\}_{\alpha \in A}$ of C and a morphisms $\pi_{\beta\alpha} : X_\beta \to X_\alpha$ for any $\alpha \leq \beta$ such that:

(i) $\pi_{\alpha\alpha} = id_{X_\alpha}$ for all $\alpha \in A$

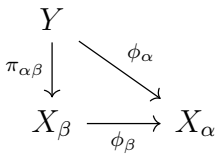
(ii) $\pi_{\beta\alpha} \cdot \pi_{\gamma\beta} = \pi_{\gamma\alpha}$ whenever $\alpha \leq \beta \leq \gamma$

Definition 1.3. Let C be a category and $(A, \{X_\alpha\}, \{\pi_{\beta\alpha}\})$ an inverse system in C. An object $X \in Ob(C)$ is called an ***inverse limit*** of this system if there exist morphisms $\pi_\alpha : X \to X_\alpha$ for $\alpha \in A$ with the following property:

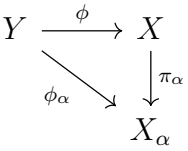
(i) For any $\alpha \leq \beta$ the following diagram commutes:



(ii) Given any $Y \in Ob(C)$ and morphisms $\phi_\alpha : Y \to X_\alpha$ such that the diagram:



commutes for $\alpha \leq \beta$, there exists unique morphism $\phi : Y \to X$ such that the following diagram commutes for all $\alpha \in A$:



If an inverse limit exists, it is unique up to C-isomorphism and is denoted by $\varprojlim X_\alpha$. In particular, inverse limits always exist in the categories of sets, groups and rings and admit the following description:

$$\varprojlim X_\alpha = \{(x_\alpha) \in \Pi X_\alpha \text{ s.t. } \pi_{\beta\alpha}(x_\beta) = x_\alpha \text{ for all } \alpha \leq \beta\}$$

1.1.2 Profinite Groups

Definition 1.4. A ***profinite group*** is a topological group that is isomorphic to the inverse limit of an inverse system of discrete finite groups. It is an Hausdorff, compact and totally disconnected topological group.

Definition 1.5. The ***profinite completion*** of a group G is the inverse limit

of G/N, where $N \triangleleft G$, $|G : N|$ finite.

We notice that, if F is a perfect field and $\bar{F}$ is its algebraic closure, $G_F = \mathrm{Gal}(\bar{F}/F)$ is a profinite group. More precisely, $G_F = \varprojlim \mathrm{Gal}(L/F)$ as L runs over finite Galois extensions of F contained in $\bar{F}$. In particular this works for $F = \mathbb{Q}$.

Let $p > 0$ be a prime integer, Π a profinite group. Following [11] we state the following definitions.

Definition 1.6. Π is said to satisfy the ***finitness condition*** ϕ_p if for every open subgroup of finite index $\Pi_0 \subset \Pi$ the following equivalent conditions hold:

(a) The pro-p-completion of Π_0 is topologically finitely generated (i.e. there is a finite number of generators whose closure generate the pro-p-completion of Π_0);

(b) The abelianized pro-p-completion of Π_0, given its natural $\mathbb{Z}_p$-module structure, is of finite type over $\mathbb{Z}_p$;

(c) There are only a finite number of continuous homomorhisms from Π_0 to $\mathbb{F}_p$, i.e. $\dim_{\mathbb{F}_p}(\mathrm{Hom}_{\mathrm{cont}}(\Pi_0, \mathbb{F}_p)) < \infty$

Examples of profinite groups Π satisfying ϕ_p for all p, are given by groups arising as algebraic fundamental groups of smooth (geometrically connected) schemes of finite type over $\mathbb{Z}$.
In particular, for K any number field and S any finite set of primes of K, we may take $\Pi = G_{K,S}$ the Galois group of the maximal field extension of K in an algebraic closure, which is unramified outside S (in fact any open subgroup $\Pi_0 \subset \Pi = G_{K,S}$ of finite index is again of the form G_{K_0,S_0} for some finite field extension K_0/K and the set of continuous homomorphism

$\mathrm{Hom}_{\mathrm{cont}}(G_{K_0,S_0}, \mathbb{Z}/p\mathbb{Z}) = \mathrm{Hom}_{\mathrm{cont}}(G^{\mathrm{ab}}_{K_0,S_0}, \mathbb{Z}/p\mathbb{Z}))$.
We may also take $\Pi = G_K$, the Galois group of an algebraic closure of any local field K.

1.2 Cohomology

Let G be a finite group, and let M be an abelian group on which G acts. We denote the action of $\sigma \in G$ on m by sending $m \in M$ to m^σ. Then we say that M is a ***(right) G-module*** if the action of G on M satisfies:

$$m^1 = m, \quad (m + m')^\sigma = m^\sigma + m'^\sigma, \quad (m^\sigma)^\tau = m^{\sigma\tau}$$

Let now M and N be G-modules. A G-module homomorphism is a homomorphism $\phi : M \to N$ commuting with the action of G, i.e.:

$$\phi(m^\sigma) = \phi(m)^\sigma \quad \text{for all } m \in M\,, \text{ for all } \sigma \in G$$

For a given G-module M, we are often interested in calculating the largest submodule of M on which G acts trivially.

Definition 1.7. The 0^{th} ***cohomology group of the*** G***-module*** M, which is denoted by M^G or $H^0(G, M)$, is the set:

$$H^0(G, M) = \{m \in M : m^\sigma = m \quad \forall \sigma \in G\}$$

i.e. it is the submodule of M consisting of all G-invariant elements.
Let:

$$0 \longrightarrow P \xrightarrow{\phi} M \xrightarrow{\psi} N \longrightarrow 0$$

be an exact sequence of G-modules (so ϕ and ψ are G-module homomorphisms with ϕ injective, ψ surjective, and $\mathrm{Im}(\phi) = \ker(\psi)$). It is easy to check that taking G-invariants gives an exact sequence:

$$0 \longrightarrow P^G \xrightarrow{\phi} M^G \xrightarrow{\psi} N^G$$

but the map on the right may not be surjective. In order to measure this lack of surjectivity, we make the following definitions:

Definition 1.8. Let M be a G-module. The ***group of 1-cochains*** (from G to M) is defined by:

$$C^1(G, M) = \{maps\ \xi : G \to M\}$$

The ***group of 1-cocycles*** (from G to M) is given by:

$$Z^1(G, M) = \{\xi \in C^1(G, M) : \xi_{\sigma\tau} = \xi_\sigma^\tau + \xi_\tau\ \forall \sigma, \tau \in G\}$$

The ***group of 1-coboundaries*** (from G to M) is defined by:

$$B^1(G, M) = \{\xi \in C^1(G, M) : \exists m \in M \text{ s.t. } \xi_\sigma = m^\sigma - m\ \forall \sigma \in G\}$$

It is easy to check that $B^1(G, M) \subset Z^1(G, M)$. The **1st** ***cohomology group*** of the G-module M is the quotient group:

$$H^1(G, M) = \frac{Z^1(G, M)}{B^1(G, M)}$$

In other words, $H^1(G, M)$ is the group of 1-cocycles $\xi : G \to M$ modulo the equivalence relation that two cocycles are identified if their difference has the form $\sigma \mapsto m^\sigma - m$ for some $m \in M$.

Remark 1.1. Notice that if the action of G on M is trivial, then:

$$H^0(G, M) = M \qquad \text{and} \qquad H^1(G, M) = \text{Hom}(G, M)$$

Proposition 1.1. *Let*

$$0 \longrightarrow P \xrightarrow{\phi} M \xrightarrow{\psi} N \longrightarrow 0$$

be an exact sequence of G-modules. Then there is a long exact sequence:

$$\begin{array}{l} H^0(G,P) \longrightarrow H^0(G,M) \longrightarrow H^0(G,N) \\ \hookrightarrow H^1(G,P) \longrightarrow H^1(G,M) \longrightarrow H^1(G,N) \end{array}$$

where the connecting homomorphism δ is defined as follows.
Let $n \in H^0(G, N) = N^G$ and choose an $m \in M$ such that $\psi(m) = n$ and define a cochain $\xi \in C^1(G, M)$ by:

$$\xi_\sigma = m^\sigma - m$$

Then the values of ξ are in P, so $\xi \in Z^1(G, P)$, and we define $\delta(n)$ to be the cohomology class in $H^1(G, P)$ of the 1-cocycle ξ.

Suppose now that H is a subgroup of G. Then any G-module is automatically an H-module. Further, if $\xi : G \to M$ is a 1-cochain, then by restricting the domain of ξ to H, we obtain an H-to-M cochain. It is clear that this process takes cocycles to cocycles and coboundaries to coboundaries, so in this way we obtain a ***restriction homomorphism***:

$$\text{Res} : H^1(G, M) \to H^1(H, M)$$

Suppose further that H is a normal subgroup of G. Then the submodule M^H of M consisting of elements fixed by H has a natural structure as a G/H-module. Let $\xi : G/H \to M^H$ be a 1-cochain from G/H to M^H. Then composing with the projection $G \to G/H$ and with the inclusion $M^H \subset M$ gives a G-to-M cochain:

$$G \longrightarrow G/H \xrightarrow{\xi} M^H \subset M$$

Again it is easy to see that if ξ is a cocycle or coboundary, then the new G-to-M cochain has the same property. This gives an ***inflation homomorphism***:

$$\mathrm{Inf} : H^1(G/H, M^H) \to H^1(G, M)$$

Proposition 1.2. *Let M be a G-module and let H be a normal subgroup of G. Then the following sequence* (Inflation-Restriction Sequence) *is exact:*

$$0 \longrightarrow H^1(G/H, M^H) \xrightarrow{\mathrm{Inf}} H^1(G, M) \xrightarrow{\mathrm{Res}} H^1(H, M)$$

Chapter 2

The modularity problem

In this chapter we will introduce the Modularity Theorem and we will recall some background material about the two main ingredients on this problem: elliptic curves and modular forms.
A genereal reference for the results shown in this chapter is [14] and [5]. For the modular forms' section we will refer also to [12], [8], [9], while a good reference for the last section is [4].

2.1 Elliptic curves

2.1.1 Definitions

Definition 2.1. An ***elliptic curve*** is a pair (E, O), where E is a nonsingular curve of genus one and $O \in E$. The elliptic curve E is defined over K, written E/K, if E is defined over K as a curve and $O \in E(K)$.

If E/K is an elliptic curve, then E can be realized in the projective plane by a Weierstrass equation, i.e. an equation of the form:

$$Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3$$

where the distinguished point is $O = [0, 1, 0]$ and $a_1, \ldots, a_6 \in \bar{K}$.
Using non-homogeneous coordinates $x = X/Y$ and $y = Y/Z$ we get:

$$E: \ y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

If $\mathrm{char}(\bar{K}) \neq 2$ we can simplify the equation by completing the square, and the substitution:

$$y \mapsto \frac{1}{2}(y - a_1x - a_3)$$

gives an equation of the form:

$$E: \ y^2 = 4x^3 + b_2x^2 + 2b_4x + b_6$$

where:

$$b_2 = a_1^2 + 4a_4, \quad b_4 = 2a_4 + a_1a_3, \quad b_6 = a_3^2 + 4a_6$$

We also define quantities:

$$\begin{aligned}
b_8 &= a_1^2a_6 + 4a_2a_6 - a_1a_3a_4 + a_2a_3^2 - a_4^2 \\
c_4 &= b_2^2 - 24b_4 \\
c_6 &= -b_2^3 + 36b_2b_4 - 216b_6 \\
\Delta &= -b_2^2b_8 - 8b_4^3 - 27b_6^2 + 9b_2b_4b_6 \\
j &= \frac{c_4^3}{\Delta} \\
\omega &= \frac{dx}{2y + a_1x + a_3} = \frac{dy}{3x^2 + 2a_2x + a_4 - a_1y}
\end{aligned}$$

It is easy to check that they satisfy the relations:

$$4b_8 = b_2b_6 - b_4^2 \quad \text{and} \quad 1728\Delta = c_4^3 - c_6^2$$

If further $\text{char}(\bar{K}) \neq 2, 3$, then the substitution:

$$(x, y) \mapsto \left(\frac{x - 3b_2}{36}, \frac{y}{108} \right)$$

eliminates the x^2 term, yielding the simpler equation:

$$E: \ y^2 = x^3 - 27c_4x - 54c_6$$

Definition 2.2. The quantity Δ is the ***discriminant*** of the Weierstrass equation, the quantity j is the ***j-invariant*** of the elliptic curve, and ω is the ***invariant differential*** associated to the Weierstrass equation.

Remark 2.1. The j-invariant is an invariant of the isomorphism class of the curve, and does not depend on the particular equation chosen (so j only depends on E and will be denoted by j_E). For algebraically closed fields the converse is true.

Let now $P = (x_0, y_0)$ be a point satisfying a Weierstrass equation:

$$f(x, y) = y^2 + a_1xy + a_3y - x^3 - a_2x^2 - a_4x - a_6 = 0$$

and assume that P is a singular point on the curve $f(x, y) = 0$.
Then we get:

$$\frac{\partial f}{\partial x}(P) = \frac{\partial f}{\partial y}(P) = 0$$

It follows that there are $\alpha, \beta \in \bar{K}$ such that the Taylor series expansion of $F(x, y)$ at P has the form:

$$f(x, y) - f(x_0 - y_0) = ((y - y_0) - \alpha(x - x_0))((y - y_0) - \beta(x - x_0)) - (x - x_0)^3$$

Definition 2.3. With notation as above, the singular point P is a ***node*** if

$\alpha \neq \beta$. In this case, the lines:

$$y - y_0 = \alpha(x - x_0) \qquad \text{and} \qquad y - y_0 = \beta(x - x_0)$$

are the tangent lines at P. Conversely, if $\alpha = \beta$, we say that P is a ***cusp***, in which case the tangent line at P is given by:

$$y - y_0 = \alpha(x - x_0)$$

Proposition 2.1. *We have the following results about elliptic curves:*

(a) The curve given by a Weierstrass equation satisfies:

(i) It is nonsingular if and only if $\Delta \neq 0$

(ii) It has a node if and only if $\Delta = 0$ *and* $c_4 \neq 0$

(iii) It has a cusp if and only if $\Delta = c_4 = 0$

In cases (ii) and (iii), there is only one singular point.

(b) Two elliptic curves are isomorphic over $\bar{K}$ *if and only if they both have the same* j*-invariant*

(c) Let $j_0 \in \bar{K}$*. There exists an elliptic curve defined over* $K(j_0)$ *whose* j*-invariant is equal to* j_0

Proposition 2.2. *If a curve* E *given by a Weierstrass equation is singular, then there exists a rational map* $\phi : E \to \mathbb{P}^1$ *of degree one.*

An algebraic map between two elliptic curves which sends the distinguished point of one to the distinguished point of the other is automatically a morphism of algebraic groups.

Definition 2.4. Let E_1, E_2 be elliptic curves. An ***isogeny*** from E_1 to E_2 is a morphism $\phi : E_1 \to E_2$ satisfying $\phi(O) = O$.
Two elliptic curves are isogenous if there is an isogeny from E_1 to E_2 with $\phi(E_1) \neq \{O\}$.

We can now consider an elliptic curve E given by a Weierstrass equation: $E \subset \mathbb{P}^2$ consists of the points $P = (x, y)$ satisfying the Weierstrass equation, together with the point $O = [0, 1, 0]$ at infinity. Now, if $L \subset \mathbb{P}^2$ is a line, L intersects E at exactly three points, say P, Q, R.
We define a composition law $\oplus$ on E by the following rule. Let $P, Q \in E$, let L be the line through P and Q, and let R be the third point of intersection of L with E. Let L' be the line through R and O. Then L' intersects E at R, O and a third point, that we denote by $P \oplus Q$.

Proposition 2.3. *The composition law $\oplus$ makes E into an abelian group with identity element O. Moreover, if E is defined over K, then:*

$$E(K) = \{(x, y) \in K^2 : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6\} \cup \{O\}$$

is a subgroup of E.

This means that an elliptic curve E/K has a natural structure of a commutative algebraic group with the distinguished K-rational point as the identity element.

2.1.2 Elliptic curves over $\mathbb{Q}_p$

Suppose that E is an elliptic curve defined over the p-adic field $\mathbb{Q}_p$. There is an equation W^{min} for E such that all the coefficients are in $\mathbb{Z}_p$ and $|\Delta|$

is minimal among all such equations for E. The associated discriminant depends only on E, it is denoted Δ_E^{min} and it divides the discriminant of every possible equation for E with coefficients in $\mathbb{Z}_p$.

Definition 2.5. If $\bar{E}$ is a smooth curve we say that E has a ***good reduction*** at p. If $\bar{E}$ has a unique singular point which is a node we say that E has ***multiplicative reduction*** at p. Otherwise $\bar{E}$ has a unique singular point which is a cusp and we say that E has ***additive reduction*** at p.
If E has good or multiplicative reduction we say that it has semi-stable reduction at p, or simply that E is ***semistable***.

If E has a *good reduction*, then p does not divide Δ_E^{min}, and the reduction $\bar{E}$ is an elliptic curve over $\mathbb{F}_p$.
If q is any power of p, and $\mathbb{F}_q$ is the field with q elements, we define the integer N_q to be the number of solutions to the equation W^{min} in the projective plane $\mathbb{P}^2(\mathbb{F}_q)$. Thus N_q is the order of the finite group $\bar{E}(\mathbb{F}_q)$. We define the integer a_q by the formula:

$$a_q = q + 1 - N_q$$

The integers a_q are completely determined by $a_p = \mathrm{Tr}(\rho(\mathrm{Frob}_p))$ as shown in the relation:

$$(1 - a_p p^{-s} + p^{1-2s})^{-1} = 1 + a_p p^{-s} + a_{p^2} p^{-2s} + a_{p^3} p^{-3s} + \dots$$

Definition 2.6. We define:

$$L(E/\mathbb{Q} - p, s) = (1 - a_p p^{-s} + p^{1-2s})^{-1}$$

to be the ***L-function*** associated to E over $\mathbb{Q}_p$.

Definition 2.7. We say that E as good ***ordinary reduction*** if p does not divide a_p, ***supersingular reduction*** otherwise.

When E has good reduction at p, we define its local conductor at p to be $m_p(E) = 0$.

If E has *multiplicative reduction* at p we can use p-adic analytic methods to describe j and to define the Tate's p-adic period associated to E over $\mathbb{Q}_p$.

Definition 2.8. We say that E has ***split*** (resp. ***non-split***) multiplicative reduction at p if the two tangent lines to the node on $\bar{E}(\mathbb{F}_p)$ have slopes defined over $\mathbb{F}_p$ (resp. $\mathbb{F}_{p^2}$).

Definition 2.9. We define the ***L-function*** $L(E/\mathbb{Q}_p, s)$ to be:

$$L(E/\mathbb{Q}_p, s) = \begin{cases} (1 - p^{-s})^{-1} & \text{if } E \text{ has split reduction} \\ (1 + p^{-s})^{-1} & \text{if } E \text{ has non-split reduction} \end{cases}$$

The conductor $m_p(E)$ is defined to be 1 in both cases.

If E has *additive reduction* at p, we define:

Definition 2.10. The ***L-function*** of E is:

$$L(E/\mathbb{Q}_p, s) = 1$$

For $p > 3$ the conductor $m_p(E)$ is set to be 2.

2.1.3 Elliptic curves over $\mathbb{Q}$

Let E be an elliptic curve defined over $\mathbb{Q}$. We define the global conductor by $N_E = \Pi_p p^{m_p(E)}$.

The curve E is said to be *semi-stable* if it is semi-stable over all p-adic fields $\mathbb{Q}_p$.

Using the fact that $\mathbb{Q}$ has class number 1, one can show E has a global minimal Weierstrass model W^{min} which gives the equation of a minimal Weierstrass model over each $\mathbb{Q}_p$. The associated discriminant, denoted Δ_E^{min}, depends only on E. The associated differential, denoted ω_E^{Neron}, is called the *Néron differential*.

Theorem 2.4 (Mordell-Weil Theorem)**.** *The group $E(\mathbb{Q})$ is a finitely generated abelian group. Hence:*

$$E(\mathbb{Q}) \cong T \oplus \mathbb{Z}^r$$

where T is the finite torsion subgroup of $E(\mathbb{Q})$, and $r \geq 0$ is the rank of E over $\mathbb{Q}$.

In [10], Mazur proved the following:

Theorem 2.5. *If $E/\mathbb{Q}$ is an elliptic curve, then its torsion group is isomorphic to one of the following possibilities:*

$$\mathbb{Z}/n\mathbb{Z},\ 1 \leq n \leq 10,\ n = 12, \qquad \mathbb{Z}/2n\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z},\ 1 \leq n \leq 4$$

Many of the deep results on $E(\mathbb{Q})$ and r are based on the relation with the L-functions.

Definition 2.11. We define the global L-function of the complex variable s by:

$$L(E/\mathbb{Q}, s) = \Pi_p L(E/\mathbb{Q}_p, s)$$

2.2 Modular forms

2.2.1 Definitions

Given the hupper half complex plane $\mathcal{H}$ and $SL_2(\mathbb{R})$ we can make $SL_2(\mathbb{R})$ act on $\mathbb{C}^* = \mathbb{C} \cup \{\infty\}$ in this way:

$$gz = \frac{az+b}{cz+d} \qquad for \qquad g = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}_2(\mathbb{R}), \qquad z \in \mathbb{C}^*$$

We get:

$$Im(gz) = \frac{Im(z)}{|cz+d|^2}$$

i.e. $\mathcal{H}$ is stable under the action of $SL_2(\mathbb{R})$.
We have that the element $-\mathbb{1} = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} \in \mathrm{GL}_2(\mathbb{R})$ acts trivially on $\mathcal{H}$, then we can think as it is the projective special linear group over $\mathbb{R}$ which operates.

Definition 2.12. $G = SL_2(\mathbb{R})/\mp 1$ is the ***Modular Group***.

Let $S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$, $T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$, S, T in G.

Theorem 2.6. *The group G is generated by S and T.*

We can now consider the subset D of $\mathcal{H}$ formed of all points z such that

$|z| > 1$ and $|Re(z)| \leq \frac{1}{2}$:

$$D = \left\{ z = x + iy : |z| > 1, |x| \leq \frac{1}{2} \right\}$$

It is possible to show that D is a fundamental domain for the action of G on $\mathcal{H}$. More precisely:

Theorem 2.7. *(1)* $\forall z \in \mathcal{H}, \exists g \in G : gz \in D$

(2) Suppose that two distinct point $z, z' \in D$ *are congruent mod* G*. Then:* $re(z) = \mp\frac{1}{2}$ *and* $z = z' + 1$ *or* $|z| = 1$ *and* $z' = -\frac{1}{z}$

(3) Let $z \in D$ *and let* $Stab(z) = \{g | g \in G, gz = z\}$ *the stabilizer of* z *in* G*. We get* $Stab(z) = 1$ *except in the following three cases:*

- $z = i$*, in which case* $Stab(z)$ *is the group of order 2 generated by* S
- $z = e^{2\pi i/3}$*, in which case* $Stab(z)$ *is the group of order 3 generated by* ST
- $z = e^{\pi i/3}$*, in which case* $Stab(z)$ *is the group of order 3 generated by* TS

Corollary 2.8. *By* (1) *and* (2) *follows that the canonical map from* D *to* $\mathcal{H}/G$ *is surjective and its restriction to the interior of* D *is injective.*

We can now state the following definition:

Definition 2.13. Let k be an integer, we say that a function f is ***weakly modular of weight*** $2k$ if f is meromorphic on $\mathcal{H}$ and:

$$f(z) = (cz + d)^{-2k} f\left(\frac{az + b}{cz + d}\right) \quad \forall \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z})$$

Proposition 2.9. *Let f be meromorphic on $\mathcal{H}$, f is weakly modular of weight $2k$ if and only if it satisfies the two relations:*

(a) $f(z+1) = f(z)$

(b) $f(-1/z) = z^{2k} f(z)$

Definition 2.14. A weakly modular function is a ***modular function*** if it is meromorphic at infinity. Moreover, we say that a modular function is of ***level*** N if it is a meromorphic funtion on $\mathcal{H}$ invariant under the group:

$$\Gamma(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \middle| a \equiv d \equiv 1, b \equiv c \equiv 0 \mod N \right\}$$

Definition 2.15. A modular function which is holomorphic everywhere is called a ***modular form***. If such a form is zero at infinity it is called a ***cusp form***.

A modular form of weight $2k$ is thus given by a series:

$$f(z) = \sum_{n=0} a_n q^n = \sum_{n=0} a_n e^{2\pi i n z}$$

which converges for $|q| < 1$ and verifies the identity (b) above. It is a cusp form if $a_0 = 0$.

2.2.2 The L-function associated to a cusp form

Let f be a cusp form on

$$\Gamma_1(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \middle| \begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix} \mod N \right\}$$

with Fourier expansion at $i\infty$ given by $\sum_{n=0}^{+\infty} a_n q^n$.

Definition 2.16. The L-function associated to f is defined by the formula:

$$L(f,s) = \sum_{n=1}^{+\infty} a_n n^{-s}$$

It is possible to prove that the infinite sum defining $L(f,s)$ converges absolutely in the right half-plane $Re(s) > \frac{3}{2}$.

2.2.3 Hecke Theory

Suppose $\Gamma = \Gamma_1(N)$, we start by recalling the definition of diamond operator.

Definition 2.17. For $d \in (\mathbb{Z}/N\mathbb{Z})^\times$, we denote by $\langle d \rangle$ the ***diamond operator***, which sends an elliptic curve (E,P) to the pair (E,dP), where P is a point on E of exact order N.

Suppose $\Gamma_1(N) \subset \Gamma \subset \Gamma_0(N)$.

Definition 2.18. If p is a prime not dividing the level N, we define the ***Hecke operator*** T_p on the space of cusp forms of weight 2 on Γ, $S_2(k)$ as:

$$T_p(f) = \frac{1}{p} \sum_{1=0}^{p-1} f\Big(\frac{\tau + i}{p}\Big) + p\langle p \rangle f(p\tau)$$

If p divides N, then we define the Hecke operator U_p analogously:

$$U_p(f) = \frac{1}{p} \sum_{1=0}^{p-1} f\Big(\frac{\tau + i}{p}\Big)$$

It is possible to check that the Hecke operators of the form T_p or U_q commute with each other and with the diamond operator. We denote by $\mathbb{T}$ the subring of $\mathrm{End}_{\mathbb{C}}(S_2(\Gamma))$ generated over $\mathbb{C}$ by all the Hecke operators T_p for $p \nmid N$, U_q for $q|N$, and $\langle d \rangle$ acting on $\S_2(\Gamma)$.

Definition 2.19. A modular form f is an ***eigenform*** if it is a simultaneous eigenvector of all the Hecke operators in $\mathbb{T}$, i.e. if there exists a $\mathbb{C}$ -algebra homomorphism $\lambda : \mathbb{T} \to \mathbb{C}$ such that $Tf = \lambda(T)f$, for all $T \in \mathbb{T}$.

Definition 2.20. We define the ***old*** subspace of $S_2(\Gamma)$ to be the space spanned by those functions which are of the form $g(az)$ where g is in $S_2(\Gamma_1(M))$ for some $M < N$ and aM divides N. We define the ***new*** subspace of $S_2(\Gamma)$ to be the orthogonal complement of the old subspace with respect to the Petersson scalar product (see [5] for the details). A normalized eigenform in the new subspace is called a ***newform of level*** N.

2.3 Galois representations

We can consider the surjection $\rho : G_{\mathbb{Q}_p} \to G_{\mathbb{F}_p}$ where $\mathbb{Q}_p$ is the p-adic field and $\mathbb{F}_p$ is a finite field.

Definition 2.21. We define the ***inertia group*** I_p to be the kernel of the morphism ρ above.

Definition 2.22. A d-dimensional representation of $G_{\mathbb{Q}}$ is a continuous homomorpshim $G_{\mathbb{Q}} \to \mathrm{GL}_d(K)$, where K is any topological field.

It is possible to give a complete description of the one-dimensional representations of $G_{\mathbb{Q}}$.

Definition 2.23. We say that a representation ρ of $G_{\mathbb{Q}}$ is ***unramified at*** p if it is trivial on the intertia group I_p, it is ***ramified*** otherwise.

Definition 2.24. We can distinguish three types of representations:

- ***Artin representations***: continuous representations $G_{\mathbb{Q}} \to \mathrm{GL}_d(\mathbb{C})$. Since all compact totally disconnected subgroups of $\mathrm{GL}_d(\mathbb{C})$ are finite, Artin representations have finite image. Hence they are semi-simple and they are unramified at all but finitely many primes.
- ***Mod ℓ representations***: continuous representations $G_{\mathbb{Q}} \to \mathrm{GL}_d(k)$ where k is a finite field of characteristic ℓ. Like Artin representations, they are unramified at all but finitely many primes.
- ***ℓ-adic representations***: continuous representations $G_{\mathbb{Q}} \to \mathrm{GL}_d(K)$ where K is a finite extension of $\mathbb{Q}_\ell$. We require an ℓ-adic representation to be unramified at all but finitely many primes

2.3.1 Representations associated to elliptic curves

Let $E[n](\bar{\mathbb{Q}})$ be the group of n-torsion points on $E(\bar{\mathbb{Q}})$, we know that $E[n](\bar{\mathbb{Q}}) \cong (\mathbb{Z}/n\mathbb{Z})^2$. Furthermore, $E[n](\bar{\mathbb{Q}})$ carries a natural action of $G_{\mathbb{Q}}$ and so we get a representation (defined up to conjugation):

$$\bar{\rho}_{E,n} : G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$$

If ℓ is a prime different from the characteristic of $\mathbb{Q}$, then we set $\mathcal{T}_l E = \varprojlim E[l^n](\bar{\mathbb{Q}})$, which is non canonically ismorphic to $\mathbb{Z}_\ell^2$. Since it has a natural continuous action of $G_{\mathbb{Q}}$, we get a representation:

$$\rho_{E,l} : G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{Z}_\ell)$$

We note that $\rho_{E,\ell^n} \cong \rho_{E,\ell} \mod \ell^n$, where $\rho_{E,\ell^n} : G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{Z}/\ell^n\mathbb{Z})$.

It is possible to show that the representations associated to elliptic curves

(i.e. the associated Tate Modules) have the following properties (see [5] for the details)

- Global properties:

  (a) The representation $\rho_{E,\ell}$ is absolutely irreducible for all ℓ. For fixed E, $\bar{\rho}_{E,\ell}$ is absolutely irreducible for all but finitely many ℓ.

  (b) If E does not have complex multiplication then $\rho_{E,\ell}$ (and hence $\bar{\rho}_{E,\ell}$ is surjective for all but finitely many ℓ).

  If $E/\mathbb{Q}$ is an elliptic curve, we get:

  (c) If $\ell > 163$ is a prime, then $\bar{\rho}_{E,\ell}$ is irreducible

  (d) If E is semistable then $\bar{\rho}_{E,\ell}$ is irreducible for $\ell > 7$

  (e) If E is semistable and $\bar{\rho}_{E,2}$ is trivial, then $\bar{\rho}_{E,\ell}$ is irreducible for $\ell > 3$.

- Local properties:
  Suppose E has good reduction at p:

  (a) If $\ell \neq p$, then $\rho_{E,\ell}$ is unramified at p, and we have the formula:

$$tr_{\rho_{E,\ell}}(\mathrm{Frob}_p) = p + 1 - \#\bar{E}_p(\mathbb{F}_p)$$

  In particular, $tr_{\rho_{E,\ell}}(\mathrm{Frob}_p)$ belongs to $\mathbb{Z}$ and is independent of $\ell \neq p$.

2.3.2 Representations associated to modular forms

Suppose $f = \sum a_n(f)q^n$ is a newform of weight two and level N_f. Let K_f denote the number field in $\mathbb{C}$ generated by the Fourier coefficients $a_n(f)$.

Using a construction of Shimura, we can associate to f an abelian variety A_f of dimension $[K_f : \mathbb{Q}]$. An appropriate choice of the basis of the Tate module associated to each prime ℓ provides a representation:

$$G_{\mathbb{Q}} \to \mathrm{GL}_2(K_f \otimes \mathbb{Q}_\ell)$$

ℓ-adic representations

Let ℓ be a fixed prime and K a finite extension of $\mathbb{Q}_\ell$ and let K'_f be the K-algebra in $\bar{\mathbb{Q}}_\ell$ generated by the Fourier coefficients of f. We fix the embeddings: $\bar{\mathbb{Q}} \hookrightarrow \mathbb{Q}_\ell$ and $\bar{Q} \hookrightarrow \mathbb{C}$.
We define:

$$\rho_f : G_{\mathbb{Q}} \to \mathrm{GL}_2(K'_f)$$

as the pushforward of $G_{\mathbb{Q}} \to \mathrm{GL}_2(K_f \otimes \mathbb{Q}_\ell)$ by the natural map $K_f \otimes \mathbb{Q}_\ell \to K'_f$. The ℓ-adic representation $\rho : G_{\mathbb{Q}} \to \mathrm{GL}_2(K')$ has the following properties (see [5] for the details):

(a) If $p \nmid N\ell$ then ρ is unramified at p and $\rho(\mathrm{Frob}_p)$ has characteristic polynomial $X^2 - a_p X + p\psi(p)$, where ψ is the homomorphism $(\mathbb{Z}/N\mathbb{Z})^\times \to K_f^\times$ defined by mapping d to the eigenvalue of $\langle d \rangle$ on f.

(b) $det(\rho)$ is the product of $\psi'_f : G_{\mathbb{Q}} \twoheadrightarrow \mathrm{Gal}(\mathbb{Q}(\xi_{N_f})/\mathbb{Q}) \to (K'_f)^\times$ with the ℓ-adic cyclotomic character ϵ, and $\rho(c)$ is conjugate to $\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$

(c) ρ is absolutely irreducible

(d) The conductor $N(\rho)$ is the prime-to-ℓ-part of N.

(e) Suppose that $p \neq \ell$ and $p||N$. Let χ denote the unramified character

$G_p \to (K')^\times$ satisfying $\chi(\mathrm{Frob}_p) = a_p$. If p does not divide the conductor of ψ, then $\rho|_{G_p}$ is of the form: $\begin{pmatrix} \chi\epsilon & * \\ 0 & \chi \end{pmatrix}$ If p divides the conductor of ψ, then $\rho|_{G_p}$ is of the form:

$$\chi^{-1}\epsilon\psi'|_{G_p} \oplus \chi$$

(f) If $\ell \nmid 2N$, then $\rho|_{G_\ell}$ is good. Moreover $\rho|G_p$ is ordinary if and only if a_ℓ is a unit in the ring of integers of K', in which case $\rho_{I_\ell}(\mathrm{Frob}_\ell)$ is the unit root of the polynomial $X^2 - a_\ell X + \ell\psi(\ell)$.

(g) If ℓ is odd and $\ell||N$, but the conductor of ψ is not divisible by ℓ, then $\rho|_{G_\ell}$ is ordinary and $\rho_{I_\ell}(\mathrm{Frob}_\ell) = a_\ell$.

Mod ℓ representations

Keeping the same notation, we define:

$$\bar{\rho}_f : G_{\mathbb{Q}} \to \mathrm{GL}_2(k_f)$$

to be the semi-simplification of the reduction of p_f. The analogous of the properties stated above hold for $\bar{\rho} = \bar{\rho}_f$, except that:

- The representation need not be absolutely irreducible (as in (c)). However, if ℓ is odd, one checks using (b) that $\bar{\rho}$ is irreducible if and only if it is absolutely irreducible.
- In (d) one only has divisibility of the prime-to-ℓ part of N_f by $N(\bar{\rho})$ in general.
- If p is a prime such that $p|N_f$, $p \ncong 1 \mod \ell$ and $\bar{\rho}_f$ is unramified at p. Then $\mathrm{Tr}(\bar{\rho}_f(\mathrm{Frob}_p))^2 = (p+1)^2$ in k_f.

Artin representations

The theory of Hecke operators and newforms extends to modular forms on $\Gamma_1(N)$ of arbitrary weight. We have the following theorem:

Theorem 2.10. *If $g = \sum a_n(g)q^n$ is a newform of weight one, level N_g and character ψ_g, then there is an irreducible Artin representation:*

$$\rho_g : G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{C})$$

of conductor N_g with the following property: if $p \nmid N_g$, then the characteristic polynomial of $\rho_g(\mathrm{Frob}_p)$ is $X^2 - a_p(g)X + \psi_g(p)$.

2.4 The Shimura-Taniyama conjecture

2.4.1 The conjecture

The Shimura-Taniyama conjecture, or the modularity conjecture, announced a deep connection between elliptic curves over the rational numbers and modular forms. There are several equivalent formulations of this conjecture which we will now present.

1. Geometric formulation of the Shimura-Tanyama conjecture.

Let E be an elliptic curve over $\mathbb{Q}$, then there exists a finite map $\phi : X_0(N) \to E$ defined over $\mathbb{Q}$ for some modular curve $X_0(N)$. More precisely, the integer N may be taken to be the conductor of $E/\mathbb{Q}$.

If this happens we say that the elliptic curve is modular and we call ϕ a modular parametrization.

2. Formulation of the Shimura-Tanyama conjecture in terms of L-functions.

The elliptic curve E over $\mathbb{Q}$ is modular if there exists a cuspidal eigenform f of weight 2 on $\Gamma_0(N)$, for some N, such that $L(E,s) = L(f,s)$.

3. Formulation of the Shimura-Tanyama conjecture in terms of Galois representations.

Let E be an elliptic curve over $\mathbb{Q}$. Then there is a cuspidal eigenform $f = \sum_{n=1}^{\infty} a_n q^n$, of weight two on $\Gamma_0(N)$, for some N such that:

$$\#E(\mathbb{F}_p) = p + 1 - a_p$$

for all but finitely many prime integers p.

This last formulation can be interpreted as follows.

Let ℓ be a prime integer and let us recall that we denoted $G_{\mathbb{Q}}$ the absolute Galois group of $\mathbb{Q}$. We denote by:

$$\rho_{E,\ell} : G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{Z}_\ell)$$

the two dimensional ℓ-adic representation obtained from the action of $G_{\mathbb{Q}}$ on the ℓ-adic Tate module of $E : \mathcal{T}_\ell(E) = \varprojlim_n E[\ell^n](\bar{\mathbb{Q}})$.

If we denote by f the cuspidal eigenform on $\Gamma_0(N)$ in the third formulation of the Shimura-Tanyama conjecture and by $\rho_{f,\ell} : G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{Q}_\ell)$ the ℓ-adic representation attached to f, then this very third formulation of the conjecture is equivalent to saying that the two Galois representations $\rho_{E,\ell}$ and $\rho_{f,\ell}$ are isomorphic for one (in fact for all) prime integer ℓ.

In fact the Shimura-Taniyama conjecture can be generalized to a con-

jecture that every ℓ-adic representation, satisfying suitable local conditions, arises from a modular form (see [7] for more details).

A first proof of the modularity conjecture was announced by A. Wiles in 1993, but after a detailed examination a serious gap was found in one part of the argument. A. Wiles and R. Taylor managed to fill in the gap completing Wiles' main argument with an additional step in 1995 ([16], [15]).
However that article did not prove the full modularity conjecture. In fact, they proved modularity only for all semistable curves over $\mathbb{Q}$, i.e. for elliptic curves E over $\mathbb{Q}$ having no additive reduction. This case was enough to imply Fermat's Last Theorem and Taylor and Wiles provided a proof for it.
A proof of the full modularity conjecture was later given by Breuil, Conrad, Harris and Taylor ([2]) in 2001.

The Shimura-Taniyama conjecture is of great importance from many points of view. Firstly, it gives the analytic continuation of $L(E, s)$ for a large class of elliptic curves. Secondly, the modular curve $X_0(N)$ is endowed with a natural collection of algebraic points arising from the theory of complex multiplication, and the existence of a modular parametrization allows the construction of points on E defined over abelian extensions of certain imaginary quadratic fields. There are various generalizations of the Shimura-Taniyama conjecture. Replacing $\mathbb{Q}$ by an arbitrary number field K, it predicts that an elliptic curve E over K is associated to an automorphic form on $\mathrm{GL}_2(K)$. When K is totally real, such an E is often uniformized by a Shimura curve attached to a suitable quaternion algebra over K, with exactly one split place at infinity (when K is of odd degree, or when E has at least one prime multiplicative reduction). In the context of function fields over finite fields, the modularity conjecture has an analogue which was established earlier by Drinfeld using methods different from those of Wiles.

2.4.2 The idea of the proof

The Shimura-Taniyama conjecture states that if $E/\mathbb{Q}$ is an elliptic curve and p is a prime integer, then there is a cuspidal normalized eigenform f with coefficients in $\mathbb{Q}$ such that $T_p(E)$ and $V_{f,p}$ are isomorphic as p-adic representations of $G_{\mathbb{Q}}$, where $V_{f,p}$ is the p-adic Galois representation associated to the eigenform.

The idea of the proof of the modularity conjecture is that if such an f exists, its p-adic Galois representation must be among the liftings of the continuous homomorphism $\bar{\rho}_E : G_{\mathbb{Q},S} \to \mathrm{GL}_N(\mathbb{F}_p)$ to $G_{\mathbb{Q},S} \to \mathrm{GL}_2(\mathbb{Z}_p)$, where $\bar{\rho}_E$ is the residual representation of the elliptic curve E, ρ_E, i.e. $\rho_E(\mathrm{mod}p)$. This is obviously not enough because we don't know if ρ_E comes from a modular form. What Wiles did was to prove that there exists a **universal** $G_{\mathbb{Q},S}$-representation $\rho_R : G_{\mathbb{Q},S} \to \mathrm{GL}_2(R)$ such that we can get all the other representations by specialization

$$\begin{array}{ccc} \rho_R : G_{\mathbb{Q},S} & \longrightarrow & \mathrm{GL}_2(R) \\ & \overset{\rho_E}{\searrow} & \downarrow \rho \\ & & \mathrm{GL}_2(\mathbb{Z}_p) \end{array}$$

Now, we consider the Hecke algebra which is the universal algebra generated by: $H := \mathbb{Z}_p[T_\ell, U_l]$, where $T_\ell : M_2(X) \to M_2(X)$ (modular forms of weight two).

One may notice that there is a bilinear pairing operating between the Hecke algebra and the modular forms of weight two, defined as follows:

$$\begin{aligned} <,>&: H \times S_2 \to \mathbb{Q}_p \\ &< T, f > \mapsto a_1(f|T) \end{aligned}$$

where S_2 is the vector space of modular forms of weight two, and a_1 is the first coefficient of the Fourier series associated to the form f (if we make T act on f, we get a cuspform of which we consider the first coefficient).
The pairing is bilinear and perfect, i.e. one can identify:

$$S_2 \cong H^V = \mathrm{Hom}_{\mathbb{Q}_p-\mathrm{vectspace}}(H, \mathbb{Q}_p)$$

In fact, we have a linear map:

$$f \mapsto (\varphi_f : T \mapsto < T, f >).$$

In particular, if we denote by $S_2^{E,N}$ the set of normalized eigenforms, we have that it is a subset of S_2 (but it is not a subgroup because in general the sum of two eigenforms is not an eigenform).

On the other side, let $f \in S_2^{E,N}$, we set $f|T = a_T f$ for $a_T \in \overline{\mathbb{Q}}_p$.
Then:

$$< T, f >= a_1(T|f) = a_1(a_T f) = a_t a_1(f) = a_T$$

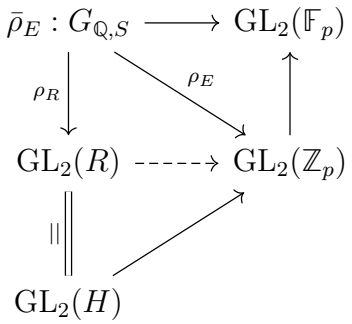
where the last equation holds because f is normalized. Therefore, we see that if f is a normalized eigenform then the map φ_f defined above is given by:

$$\varphi_f(T) = a_T.$$

and in particular we get that this map is a homomorphism of algebras.

Using this construction, we can now think about the normalized eigenforms as algebras homomorphisms between H and $\overline{\mathbb{Q}}_p$.
What Wiles and Taylor proved was that there is an isomorphism between the universal ring R and the Hecke algebra associated to the modular forms of weight 2, H.

We can in fact consider the following diagram:



In particular from the universality of R we get an algebra homomorphism corresponding to the representation ρ_E, $H = R \to \mathbb{Z}_p$, i.e. we get a normalized eigenform f corresponding to the homomorphism: $H \to \mathbb{Z}_p$. It follows that we can add in the diagram $\rho_f : G_{\mathbb{Q},S} \to \mathrm{GL}_2(\mathbb{F}_p)$.

In this way we have found an eigenform whose Galois representation is the one of the elliptic curve, so the proof of Shimura-Taniyama follows. The achievement of Mazur's article is to prove that this modular representation exists.

Chapter 3

Functors on Artin rings

We are now going to analyze in detail the article of Michael Schlessinger ([13]). Those results will be used for the proof of the existence of the universal deformation in the article of Mazur ([11]).

Let Λ be a complete Noetherian local ring, μ its maximal ideal, and $k = \Lambda/\mu$ the residue field. Let $\mathbf{C}$ be the category of Artin local Λ-algebras with residue field k; the morphisms are the ones of local Λ-algebras, i.e. are morphisms of Λ-moduli such that the preimage of the maximal ideal is the maximal ideal and induce the identity on the residue fields.

We want to investigate when a covariant functor $F : \mathbf{C} \to Sets$ is ***pro-representable***, i.e. when it has the form:

$$F(A) \cong \mathrm{Hom}_{\text{local } \Lambda-\text{alg}}(R, A) \qquad A \in C$$

where R is a complete local Λ-Algebra, with maximal ideal $\mathfrak{m}$, such that $R/\mathfrak{m}^n$ is in $\mathbf{C}$ for all $n \geq 1$.

In many interesting cases F is not pro-representable, but at least one may find an R as above and a morphism $\phi : \mathrm{Hom}(R, \cdot) \to F(A)$ of functors such

that $\mathrm{Hom}(R, A) \to F(A)$ is surjective for all A in $\mathbf{C}$. The minimal R with this property is called the "hull" of F and it is unique up to isomorphism. In the main theorem we will see a criterion for F to have a "hull" and also a simple criterion for which this hull pro-represents F.

3.1 Schlessinger's construction

Let Λ be as above, we define $\mathbf{C} = \mathbf{C}_\Lambda$ to be the catergory of Artinian local Λ-algebras having residue field k, i.e. "the structure morphism" $\Lambda \to A$ of such a ring A induces a trivial extension of residue fields. Morpshims in $\mathbf{C}$ are local morphisms of Λ-algebras.
Let $\hat{\mathbf{C}} = \hat{\mathbf{C}}_\Lambda$ be the category of complete Noetherian local Λ-algebras A for which $A/\mathfrak{m}^n$ is in $\mathbf{C}$ for all n. Notice that $\mathbf{C}$ is a full subcategory of $\hat{\mathbf{C}}$.
If $p : A \to B$, $q : C \to B$ are morphisms in $\mathbf{C}$, let $A \times_B C$ denote the ring (in $\mathbf{C}$) consisting of all pairs (a, c) with $a \in A$, $c \in C$, for which $pa = qc$, with coordinatewise multiplication and addition.
For any A in $\hat{\mathbf{C}}$ we denote by t_A^* the Zariski cotangent space of A over Λ:

$$t_A^* = \mathfrak{m}/\mathfrak{m}^2 + \mu A$$

where $\mathfrak{m}$ is the maximal ideal of A.

Remark 3.1. We identify the dual of t_A^* with the space of Λ-linear derivations of A into k, $\mathrm{Der}_\Lambda(A, k)$, i.e. we have:

$$\mathrm{Hom}_k(t_A^*, k) \cong \mathrm{Der}_\Lambda(A, k)$$

So, in order to show that there exists an isomorphism between the two sets above, we have to associate to each element η in $\mathrm{Hom}_k(t_A^*, k)$ a map D_η from

A to k which satisfies the conditions to be a derivation and that will be defined as:

$$\begin{aligned} &D_\eta : A \to k \\ &D_\eta(\lambda) = 0 \qquad \text{for } \lambda \in \Lambda \\ &D_\eta(f) = \eta([f]) \qquad \text{where } [f] = f \mod \mathfrak{m}^2 + \mu A \end{aligned}$$

and then extended as Λ-modules morphism.
In order to prove that this isomorphism actually exists, we first have to notice that $A = \varprojlim A/\mathfrak{m}^n$ (because we have a local ring which is complete), so it is enough to prove the statement for each level $A/\mathfrak{m}^k$ and show that the maps can be glued together in a way that respect the projections.
In particular, it is possible to show that:

- $\forall k \geq 1$, $A/\mathfrak{m}_A^k$ is generated as Λ-module by Λ and m_A
- $\forall x \in A/\mathfrak{m}_A^k$, $x = \lambda_0 + \sum_{i=1}^{s} \lambda_i t_i$ for λ_0, $\lambda_i \in \Lambda$ and $t_i \in \mathfrak{m}$, we define:

  $$D_{\eta,k} : A/\mathfrak{m}^k \to k$$

  with:

  $$D_{\eta,k}(x) = \sum \bar{\lambda}_i \eta([t_i])$$

  it is a good definition and it is a derivation.

- The following diagram is commutative:

$$\begin{array}{ccc} A/\mathfrak{m}_A^k & \longrightarrow & k \\ \uparrow & & \uparrow \\ A/\mathfrak{m}_A^{k+1} & \longrightarrow & k \end{array}$$

and it follows that:

$$D_\eta := \{D_{\eta,k}\} : \varprojlim A/\mathfrak{m}^k = A \longrightarrow k$$

where:

$$D_\eta((a_k)) = D_{\eta,k}(a_k)$$

Therefore we can associate to each homomorphism a function (which is a derivation) in the way described above.

Lemma 3.1. *A morphism $B \to A$ in $\hat{\boldsymbol{C}}$ is surjective if and only if the induced map from t_B^* to t_A^* is surjective.*

Proof. First, any element in $A/\mathfrak{m}^2$ is generated as a Λ-module, by the image of Λ in A and the maximal ideal $\mathfrak{m}$ of A. Thus the induced map from μ/μ^2 to $\mu A/(\mathfrak{m}^2 \cap \mu A)$ (with μ maximal ideal of Λ) is a surjection. In fact we have that $\mu \subseteq \mathfrak{m}^2 \cap A$ since $\mu^2 \subseteq \mathfrak{m}^2$, and $\mu^2 \subseteq \mu A$. If $x \in \mu A$, we can write $x = \alpha \cdot a$ for $\alpha \in \mu$ and $a \in A$: now $\bar{a} \in k$, so we get $x = \alpha \cdot a = \alpha(b + y) = \alpha b + \alpha y$, where $\alpha b \in \mu\Lambda$ and $\alpha y \in \mathfrak{m}^2 \cap \mu A$. Thus if $B \to A$ is a morphism in $\hat{\mathbf{C}}$ and $\mathfrak{m}$ and $\mathfrak{n}$ are the maximal ideals respectively of A and B, then the rows in the following diagrams are exact:

$$\begin{array}{ccccccccc}
0 & \to & \mu A/(\mu A \cap \mathfrak{m}^2) & \to & \mathfrak{m}/\mathfrak{m}^2 & \to t_A^* & \to & 0 \\
 & & \uparrow\alpha & & \uparrow\beta & \uparrow\gamma & & \\
0 & \to & \mu B/(\mu B \cap \mathfrak{n}^2) & \to & \mathfrak{n}/\mathfrak{n}^2 & \to t_B^* & \to & 0
\end{array}$$

We have that, since $\mathfrak{m}$ is maximal in A, $\mu A \subseteq \mathfrak{m}$ and the elements that go in $\mathfrak{m}^2$ are those of $\mu A \cap \mathfrak{m}^2$, so the map on the left is injective; moreover we notice that $\mathfrak{m}/\mathfrak{m}^2/\mu A/(\mathfrak{m}^2 \cap \mu A)$ is isomorphic to $\mathfrak{m}/(\mathfrak{m}^2 + \mu A)$, which is t_A^* (so the map on the right is surjective). So we have shown that the rows

of the diagram are exact.

Thus, in the diagram, α is surjective for all morphisms $B \to A$ in $\hat{\mathbf{C}}$ because $B \to A$ is a morphism of Λ-algebras and the following diagram commutes:

$$\begin{array}{ccc} \mu/\mu^2 & \longrightarrow & \frac{\mu B}{(\mu B \cap \mathfrak{n}^2)} \\ & \searrow & \downarrow \\ & & \frac{\mu A}{(\mu A \cap \mathfrak{m}^2)} \end{array}$$

($\Leftarrow$) It follows that, if γ is surjective, β is surjective as well. But the induced map $gr(B) \to gr(A)$ on the graded rings is a surjection (in general a basis of $\mathfrak{m}/\mathfrak{m}^2$ as vectorial k-space is a system of generators of $gr(A)$ as k-algebra).

Now, using [1] (§2, No. 8, Theorem 1), since B is complete, A is separated ($\cap \mathfrak{m}^i = 0$) and $\cup \mathfrak{m}^i = A$, we can conclude that $B \to A$ is surjective.

($\Rightarrow$) Conversely, suppose that $f : B \to A$ is surjective. In this case we get $f(\mathfrak{n}) = \mathfrak{m}$, i.e. we have that $\forall x \in \mathfrak{m} \quad \exists y \in B$ such that $f(y) = x$. In fact if $x \in \mathfrak{m}$ then $\exists y \in B$ such that $f(y) = x$. If $y \notin \mathfrak{n}$, then y is a unit and so it's x since f is morphism of rings, but this is a contradiction. Notice that the condition $f(\mathfrak{n}) = \mathfrak{m}$ is stronger than $f^{-1}(\mathfrak{m}) = \mathfrak{n}$, the one for local morphisms (for example, we can consider the function $f : \mathbb{Z}_p \to \mathbb{Z}_p[[x]]$). In this case $f^{-1}(\mathfrak{m}) = \mathfrak{n} = \mathbb{Z}_p \cap \mathfrak{m} = p\mathbb{Z}_p = n$ but $f(\mathfrak{n}) = f(p\mathbb{Z}_p) = p\mathbb{Z}_p \neq (x, p)$.

Since $f(\mathfrak{n}) = \mathfrak{m}$, $t_B^* = \mathfrak{n}/(\mathfrak{n}^2 + \mu B)$ and $t_A^* = \mathfrak{m}/(\mathfrak{m}^2 + \mu A)$, it follows that $t_B^* \to t_A^*$ is surjective.

□

Let $p : B \to A$ be a surjection in $\mathbf{C}$.

Definition 3.1. We say that p is a ***small extension*** if the kernel of p is a nonzero principal ideal (t) such that $\mathfrak{m} \cdot t = (0)$, where $\mathfrak{m}$ is the maximal ideal of B.

Definition 3.2. We say that p is a ***essential*** if for any morphism $q : C \to B$ in $\mathbf{C}$ such that pq is surjective, it follows that q is surjective.

From lemma 3.1 we obtain:

Lemma 3.2. *Let $p : B \to A$ be a surjection in $\mathbf{C}$. Then:*

(i) p is essential if and only if the induced map $p_* : t_B^* \to t_A^*$ is an isomorphism.

(ii) If p is a small extension, then p is not essential if and only if p has a section $s : A \to B$, with $ps = 1_A$.

Proof. (i) Let p_* be an isomorphism, $q : C \to B$ morphism. Then we have:

$$t_C^* \xrightarrow{q_*} t_B^* \xrightarrow{p_*} t_A^*$$

Since pq is surjective, by lemma 3.1 we get that $(pq)_* = p_* q_*$ is surjective, and so p_* is surjective. Now, applying lemma 3.1 again, we get that q is surjective, and so p is essential.
Conversely, let $\tilde{t_1}, \ldots, \tilde{t_r}$ be a basis for $t_A^* = \mathfrak{m}_A/(\mathfrak{m}_A^2 + \mu A)$, amd let $t_1, \ldots, t_r$ preimages in B (they are in the maximal ideal of B).
Let's now define $C := \Lambda[t_1, \ldots, t_r]$ as the Λ-algebra generated by the elements $t_1, \ldots, t_r$. We have that $C \subseteq B$. Moreover if we consider the restriction of p over C, we obtain a surjective map of Λ-algebras. Then we have that p is essential, so the map from C to B is surjective and

$C = B$.

Since $C := \Lambda[t_1, \ldots, t_r]$ we get that $\mathfrak{m}_C/(\mathfrak{m}_C^2 + \mu C)$ is generated by at most r elements, so $dim_K t_C^* \leq r$.

Then we get:

$$dim_K t_B^* = dim_K t_C^* \leq r = dim_K t_A^*$$

Moroever, since we have a surjection from B to A, we get that the map $t_B^* \to t_A^*$ is also surjective, so $dim_K t_B^* \geq dim_K t_A^*$. We can now conclude that $dim_K t_B^* = dim_K t_A^*$, and so $t_B^* \simeq t_A^*$.

(ii) Let's first suppose that p has a section s. In particular s can't be surjective, otherwise p would be injective and it is not possible since p is small. Then $ps = 1_A$ is surjective, so p is not essential.

Conversely, if p is not essential, then C is properly contained in B because p restricted at C is essential (it follows by (i) and by construction of C). Since by hypotesis we have that $m(t) = 0$, so $t^2 = 0$ and $\text{length}(t) = 1$, so we get:

$$\text{length}(B) = \text{length}(A) + \text{length}(t) = \text{length}(A) + 1$$

Then, since the restriction of p at C is surjective,

$$\text{length}(C) \geq \text{length}(A)$$

and

$$\text{length}(C) < \text{length}(B) = \text{length}(A) + 1$$

i.e. $\text{length}(C) \leq \text{length}(A)$.

We get that $\text{length}(C) = \text{length}(A)$ and, from the surjectivity of p restricted to C, we can conclude that $C \simeq A$. In particular, since the

isomorphism from A to C is a section of p, we can conclude. □

We shall consider only covariant functors F from $\mathbf{C}$ to *Sets*, such that $F(k)$ contains just one element.

Definition 3.3. By a ***couple*** for F we mean a pair (A, ξ) where $A \in \mathbf{C}$ and $\xi \in F(A)$. A ***morphism of couples*** $u : (A, \xi) \to (A', \xi')$ is a morphism $u : A \to A'$ in $\mathbf{C}$ such that $F(u)(\xi) = \xi'$. If we extend F to $\hat{\mathbf{C}}$ by the formula $\hat{F}(A) = \varprojlim F(A/\mathfrak{m}^n)$ we may speak analogously of ***pro-couples*** and morphisms of pro-couples.

For any ring R in $\hat{\mathbf{C}}$, we set $h_R(A) = \mathrm{Hom}(R, A)$ to define a functor h_R on $\mathbf{C}$. Now, if F is any functor on $\mathbf{C}$, and R is in $\hat{\mathbf{C}}$, we have a canonical isomorphism:

$$\hat{F}(R) \xrightarrow{\sim} \mathrm{Hom}(h_R, F)$$

To each element of $\hat{F}(R)$ we can in fact associate a morphism of functors $h_R \to F$.

Let $\xi = \varprojlim \xi_n$ element in $\hat{F}(R)$. Then each $u : R \to A$ factors through $u_n : R/\mathfrak{m}^n \to A$ for some n because $\ker(u) \supseteq \mathfrak{m}^n$. This is not true in general but it works in this case because A is Artinian, so $\mathfrak{m}_A^k = 0$ for some k and this implies that $u(\mathfrak{m}^k) \subseteq \mathfrak{m}_A^k$. So we can assign to $u \in h_R(A)$ the element $F(u_n)(\xi_n)$ of $F(A)$.

Viceversa, we can associate to $h_R \to F$ an element of $\hat{F}(R)$. We can in fact consider for each n the map:

$$h_R(R/\mathfrak{m}^n) \to F(R/\mathfrak{m}^n)$$

where an element in the domain is given by the canonical projection Π. The

images form an inverse system by construction.
This means that we can associate to $h_R \to F$ the inverse limit of those elements.

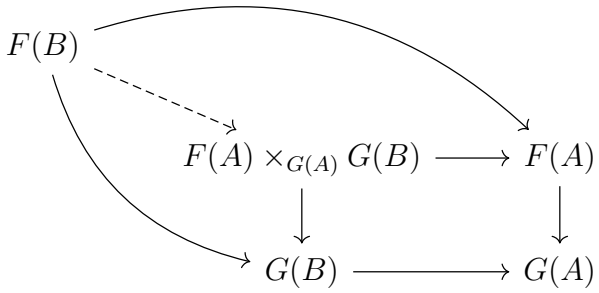
Definition 3.4. We say that a pro-couple (R, ξ) for F ***pro-represents*** F if the morphism $h_R \to F$ induced by ξ is an isomorphism.

Unfortunately, many interesting functors are not pro-representable: an attempt of looking for some kind of "universal object" is given by the definition below.

Definition 3.5. A morphism $F \to G$ of functors is ***smooth*** if for any surjection $B \to A$ in $\mathbf{C}$, the morphism:

$$F(B) \to F(A) \times_{G(A)} G(B)$$

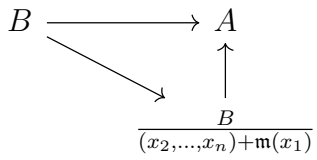
obtained by the following contruction



is surjective.

Remark 3.2. It is enough to check surjectivity in the equation 3.5 for small extensions $B \to A$.
In fact the idea is that every surjective morphism $f : B \to A$ factor through a small extension. In fact B is Noetherian and $\ker(f) = (x_1, \ldots, x_n)$ is finitely

generated, so we get that $\ker(f) \supseteq (x_2, \ldots, x_n) + \mathfrak{m}(x_1)$, so f factors through:



and the map $B/(x_2, \ldots x_n) + \mathfrak{m}(x_1) \to A$ is a small extension (in fact its kernel goes to zero if multiplied by the maximal ideal).
So, if we use induction on the length, we prove the remark.

Remark 3.3. If $F \to G$ is smooth, then $\hat{F} \to \hat{G}$ is surjective, in the sense that $\hat{F}(A) \to \hat{G}(A)$ is surjective fo all A in $\hat{C}$. Since $\hat{F}(A) = \varprojlim F(A/\mathfrak{m}^n)$, we prove the remark working by induction on each level.
If $n = 1$, then our function is surjective because we have just one element in the domain and one in the codomain.
Now, we have $A/\mathfrak{m}^{n+1} \twoheadrightarrow A/\mathfrak{m}^n$, we want to show that, given that the function $F(A/\mathfrak{m}^n) \to G(A/\mathfrak{m}^n)$ is surjective, also $F(A/\mathfrak{m}^{n+1}) \to G(A/\mathfrak{m}^{n+1})$ is surjective.
From the fact that $F \to G$ is smooth, it follows the surjectivity of the function

$$F(A/\mathfrak{m}^{n+1}) \to F(A/\mathfrak{m}^n) \times_{G(A/\mathfrak{m}^n)} G(A/\mathfrak{m}^{n+1})$$

But now we have that the function:

$$F(A/\mathfrak{m}^n) \times_{G(A/\mathfrak{m}^n)} G(A/\mathfrak{m}^{n+1}) \to G(A/\mathfrak{m}^{n+1})$$

is surjective, so our statement follows by composition.

Proposition 3.3. *(i) Let $R \to S$ be a morphism in $\hat{C}$. Then $h_S \to h_R$ is smooth if and only if S is a power series ring over R.*

(ii) *If $F \to G$ and $G \to H$ are smooth morphisms of functors, then the composition $F \to H$ is smooth.*

(iii) *If $u : F \to G$ and $v : G \to H$ are morphisms of functors, then the composition $F \to H$ is smooth*

(iv) *If $F \to G$ and $H \to G$ are morphisms of functors such that $F \to G$ is smooth, then $F \times_G H \to H$ is smooth.*

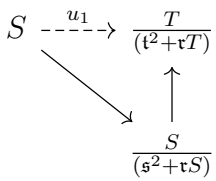
Proof. (i) ($\Rightarrow$) Suppose $h_S \to h_R$ is smooth. Let $\mathfrak{r}$ (resp $\mathfrak{s}$) be the maximal ideal in R (resp S), and pick $x_1, \dots x_n$ in S such that $\bar{x}_1, \dots, \bar{x}_n$ is a basis for $t^*_{S/R} = \mathfrak{s}/(\mathfrak{s}^2 + \mathfrak{r}S)$ (relative cotangent space).

Set $T = R[[X_1, \dots X_n]]$ and denote the maximal ideal of T by $\mathfrak{t}$. We want to show that $T \cong S$.

First we notice that T is Noetherian and local because R has those properties, and T is complete with respect to the $\mathfrak{t}$-adic topology by the definition of the power series ring.

We have that $x_1, \dots, x_n$ generate S as an R-module: in fact we have that the $\bar{x}_1, \dots, \bar{x}_n$ generate $S/(\mathfrak{s}^2 + \mathfrak{r}S)$ as $R/\mathfrak{r}$-vector space. So S is generated by $x_1, \dots x_n$ as R-module.

It follows that in order to define a morphism of R-modules on S it is enough to define the images of $x_1, \dots x_n$. We can define a morpshim of R-algebras $u_1 : S \to T/(\mathfrak{t}^2 + \mathfrak{r}T)$ obtained by mapping x_1 on the residue class of X_i. We notice that u_1 as it is induced by the following commutative diagram:



Now, since $h_S \to h_R$ is smooth, by considering the R-algebras surjective morphism $T/\mathfrak{t}^2 \twoheadrightarrow T/(\mathfrak{t}^2 + \mathfrak{r}T)$, we get the surjectivity of:

$$h_S(T/\mathfrak{t}^2) \twoheadrightarrow h_S(T/(\mathfrak{t}^2 + \mathfrak{r}T)) \times_{h_R(T/(\mathfrak{t}^2+\mathfrak{r}T)} h_R(T/\mathfrak{t}^2)$$

We note that:

$$h_S(T/(\mathfrak{t}^2 + \mathfrak{r}T)) \subseteq h_S(T/(\mathfrak{t}^2 + \mathfrak{r}T)) \times_{h_R(T/(\mathfrak{t}^2+\mathfrak{r}T)} h_R(T/\mathfrak{t}^2)$$

because R is projective as an R-module (it is a module over itself). By smoothness u_1 lifts to $u_2 : S \to T/\mathfrak{t}^2$.
Applying the same idea again we can lift to $u_3 : S \to T/(\mathfrak{t}^3, u_4, \dots)$ etc. Since T is complete, we get $u : S \to T$ which induces an isomorphism of $t^*_{S/R}$ with $t^*_{T/R}$ (by choice of u_1) so that u is a surjection by lemma 3.1. Furthermore, if we choose $y_i \in S$ such that $uy_i = X_t$, we can set $vX_i = y_i$ and produce a local morphism $v : T \to S$ of algebras such that $uv = 1_T$; in particular v is an injection.
Clearly v induces a bijection on the cotangent spaces, so v is also a surjection (see lemma 3.1). Hence v is an isomorphism of $T = R[[X_1, \dots X_n]]$ with S.

($\Leftarrow$) Conversely, let $S = R[[X_1, \dots, X_n]]$, then we have that the function $h_{R[[X_1,\dots,X_n]]} \to h_R$ is smooth.
In fact, if we consider the function $s : B \twoheadrightarrow A$, then the map:

$$h_{R[[X_1,\dots,X_n]]}(B) \to h_{R[[X_1,\dots,X_n]]}(A) \times_{h_R(A)} h_R(B)$$

is surjective.

In particular, to $(g, f) \in h_{R[[X_1,\dots,X_n]]}(A) \times_{h_R(A)} h_R(B)$ we associate the element of $h_{R[[X_1,\dots,X_n]]}(B)$ given by :

$$\begin{aligned} R \ni\ r &\mapsto f(r) \\ X_i &\mapsto s^{-1}(g(X_i)) \end{aligned}$$

with $g \mid_R = s \circ f$ acording to the following diagram:

$$\begin{array}{ccc} & h_R(B) & f \\ & \downarrow & \downarrow \\ h_{R[[\dots]]} & \longrightarrow\ h_R(A) & s \circ f \\ & \searrow\!\!\searrow & \\ g & \longmapsto\ g \mid R & \end{array}$$

The proof of (i), (iii), (iv) is formal and similar to the first one.

□

Remark 3.4. Let $k[\epsilon]$, where $\epsilon^2 = 0$, denote the ring of dual numbers over k. For any functor F, the set $F(k[\epsilon])$ is called the tangent space to F, and it is denoted by t_F.

In particular, if $F = h_R$, then it exists a canonical isomorphism $t_F \cong t_R$:

$$\mathrm{Hom}_k(t_R^*, k) = t_R \cong t_{h_R} = h_R(Kk[\epsilon]) = \mathrm{Hom}_\Lambda(R, k[\epsilon])$$

In fact, if we consider $g \in \mathrm{Hom}_\Lambda(R, k[\epsilon])$, we can associate the morphism which sends $[t] \in \mathfrak{m}_R/(\mathfrak{m}_R^2 + \mu R)$ to the coefficient of ϵ in $g(t)$ (t representative in $[t]$). In particular, this is a morphism of k-vector spaces from t^* to k, in

fact:

$$k_1[t] = [\lambda_1 t] \mapsto \text{coef. of } \epsilon \text{ in } g(\lambda_1 t) = \bar{\lambda}_1 g(t)_\epsilon = k_1 g(t)_\epsilon$$
$$[t_1] + [t_2] \mapsto \text{coef. of } \epsilon \text{ in } g(t_1 + t_2) = g(t_1)_\epsilon + g(t_2)_\epsilon$$

where in both cases we used the fact that $g \in \mathrm{Hom}_\Lambda(R, k[\epsilon])$.
Conversely, given $f \in \mathrm{Hom}_k(t_R^*, k)$, we consider the diagram:

$$\begin{array}{ccc} R & \dashrightarrow & k[\epsilon] \\ & \searrow & \uparrow \\ & & \frac{R}{(\mathfrak{m}_R^2 + \mu R)} \end{array} \qquad \begin{array}{c} \bar{\lambda}_1 + \bar{\lambda}_2 f(\bar{t})\epsilon \\ \uparrow \\ \bar{\lambda}_1 + \bar{\lambda}_2 \bar{t} \end{array}$$

For $\bar{t} \in \mathfrak{m}_R/(\mathfrak{m}_R^2 + \mu R)$.
We can define the map from R to $k[\epsilon]$ as the composition of the maps above and we get a Λ-module morphism. Usually t_F will have an intrinsic vector space structure.

Definition 3.6. A pro-couple (R, ξ) for a functor F is called a *pro-representable hull* of F, or just a ***hull*** of F, if the induced map $h_R \to F$ is smooth, and if the induced map $t_R \to t_F$ of tangent spaces is a bijection.

Remark 3.5. If (R, ξ) pro-represents F, then (R, ξ) is a hull of F. In fact, from the fact that $h_R \to F$ is an isomorphism it follows that $h_R \to F$ is smooth ($B \to A$ is surjective, so $h_R(B) \to h_R(A) \times_{F(A)} F(B)$ is surjective), so $t_F = F(k[\epsilon]) \cong h_R(k[\epsilon]) \cong t_R$.
If (R, ξ) pro-represents F, then (R, ξ) is unique up to canonical isomprhism (while if it is hull it is unique uo to non canonical isomorphisms).

Remark 3.6. If $f : R \to R$ is a surjective endomorphism and R is Noetherian, then f is injective.

We can easily prove this statement using tools from commutative algebra. If we consider the chain:

$$\ker(f) \subseteq \ker(f^2) \subseteq \dots$$

since R is Noetherian we must have $\ker(f^n) = \ker(f^{n+1}) = \dots$ for some n. Now we claim that $\ker(f^n) \cap \mathrm{Im}(f^n) = 0$. We just have to show one inclusion. Let $x \in \ker(f) \cap Im(f^n)$. Then $f^n(x) = 0$ and there exists $y \in M$ such that $x = f^n(y)$. So, by substitution, we get that $f^{2n}(y) = 0$, which means that $y \in \ker(f^{2n}) = \ker(f^n)$, hence $f^n(y) = 0$. This implies that $x = 0$, so our claim follows.
Now, since f is surjective, it follows that $\mathrm{Im}(f^n) = M$. However, we have that $\ker(f^n) \subset M$, so that $0 = \ker(f) \cap M = \ker(f)$, so F is injective and hence an isomorphism.

Proposition 3.4. *Let (R, ξ) and (R', ξ') be hulls of F. Then there exists an isomorphim $u : R \to R'$ such that $F(u)(\xi) = \xi'$.*

Proof. If (R, ξ) is hull, then the morphism $h_R \to F$ inudeced by ξ is smooth and so it is surjective. It follows that in particular $h_R(R') \to F(R')$ is surjective, so, since $\xi \in F(R')$, $\exists u \in h_R(R')$ such that $F(u_n)(\xi_n) = \xi'_n$. So, applying the previous theorem, we get a morphisms of couple $u : (R, \xi) \to (R', \xi')$. Moreover, since (R, ξ) is a hull, we have a bijection $t_R \cong t_F$.
In the same way, if we consider (R', ξ'), we get that exists a morphism of couple $u' : (R', \xi') \to (R, \xi)$ and $t'_R \cong t_F$ is a bijection. So we get that $t_R \cong t_F \cong t'_R$, so $t_R \cong t'_R$. It follows that $u'u$ induces an isomorphism on t^*_R so that $u'u$ is a endomorphism of R by lemma 3.1. But by the remark 3.6 we know that a surjective endomorphism of any Noetherian ring is an isomorphism and we can conclude. □

Remark 3.7. Let (R, ξ) be a hull of F. Then R is a power series ring over Λ if and only if F maps surjections $B \to A$ in $\mathbf{C}$ into surjections $F(B) \to F(A)$. In fact the state condiction on F is equivalent to the smoothness of the natural morphism $F \to h_\Lambda$. By applying the proposition 3.3 (ii) and (iii) to the diagram:

$$\begin{array}{ccc} h_R & \longrightarrow & h_\Lambda \\ & \searrow \quad \swarrow & \\ & F & \end{array}$$

we can conclude that $h_R \to h_\Lambda$ is smooth if and only if $F \to h_\Lambda$ is.
Now, using proposition 3.3 (i) we can can conclude that R is a power series ring over Λ.

Lemma 3.5. *Suppose F is a functor such that*

$$F(k[V] \times_k k[W]) \xrightarrow{\sim} F(k[V]) \times F(k[W])$$

for vector spaces V and W over k, where $k[V]$ denotes the ring $k \oplus V$ of $\boldsymbol{C}$ in which V is a square zero ideal. Then $F(k[V])$, and in particular $t_F = F([k[\epsilon])$, has a canonical vector space structure, such that $F(k[V]) \cong t_F \otimes V$.

Proof. We prove our statement in the particular case: $k[V] = k[W] = k[\epsilon]$. In this case we have, by hypothesis:

$$b : F(k[\epsilon] \times_k k[\epsilon]) \xrightarrow{\sim} F(k[\epsilon]) \times F(k[\epsilon])$$

In this case, we get the following results.

- Sum:

$$\begin{array}{ccccc} F(k[\epsilon]) \times F(k[\epsilon]) & \xrightarrow{b^{-1}} & F(k[\epsilon] \times_k k[\epsilon]) & \xrightarrow{F^+} & F(k[\epsilon]) \\ \downarrow & & & & \downarrow \\ t_F \times t_F & & \dashrightarrow & & t_F \end{array}$$

where:

$$\begin{aligned} F^+ : k[\epsilon] \times_k k[\epsilon] &\to k[\epsilon] \\ (a + b\epsilon, a + c\epsilon) &\mapsto a + (b + c)\epsilon \end{aligned}$$

- Scalar multiplication:

$$\begin{array}{ccccc} F(k[\epsilon]) \cong F(k) \times F(k[\epsilon]) & \xrightarrow{b^{-1}} & F(k \times_k k[\epsilon] \cong F(k[\epsilon]) & \xrightarrow{F_{m\lambda}} & F(k[\epsilon]) \\ \downarrow & & & & \downarrow \\ t_F & & \dashrightarrow & & t_F \end{array}$$

where:

$$\begin{aligned} F_{m\lambda} : k[\epsilon] &\to k[\epsilon] \\ a + b\epsilon &\mapsto a + \lambda b\epsilon \end{aligned}$$

□

3.2 The Main Theorem

3.2.1 Statement

Theorem 3.6. *Let F be a functor from $\boldsymbol{C}$ to Sets such that $F(k) = (e)$ (=one point). Let $A' \to A$ and $A'' \to A$ be morphisms in $\boldsymbol{C}$, and consider*

the map

$$F(A' \times_A A'') \to F(A') \times_{F(A)} F(A'') \tag{3.1}$$

Then:

(1) F has a hull if and only if F has properties (H_1), (H_2), (H_3) below:

(H_1) *3.1 is a surjection whenever $A'' \to A$ is a small extension.*

(H_2) *3.1 is a bijection when $A = k$, $A'' = k[\epsilon]$.*

(H_3) *$dim_k(t_F) < \infty$*

(2) F is pro-representable if and only if, for any small extension $A' \to A$, F has the additional property (H_4):

(H_4) $F(A' \times_A A') \xrightarrow{\sim} F(A') \times_{F(A)} F(A')$

3.2.2 Preliminary results

Remark 3.8. First we notice that if $F \cong h_R$, then 3.1 is an isomorphism for all $A' \to A$ and $A'' \to A$ morphisms, i.e. the three conditions are necessary for the pro-representability. In fact we have the maps:

$$\begin{aligned} \phi : h_R(A' \times_A A'') &\to h_R(A') \times_{h_R(A)} h_R(A^2) \\ f &\mapsto \quad (g', g'') \\ t(r) = (v(r), w(r)) &\leftarrow\!\shortmid \quad (v, w) \end{aligned}$$

where $g'(r) = \Pi_1 \circ f(r)$ and $g''(r) = \Pi_2 \circ f(r)$, for the projections Π_1, Π_2. In particular we get that if F is pro-representable, then the four conditions hold.

Remark 3.9. The condition (H_2) implies that t_F is a vector space by lemma 3.5.

We want to prove that from (H_2) follows that the function:

$$F(A' \times k[W]) \to F(A') \times F(k[W])$$

is an isomorphism $\forall A'$, $\forall W$. In order to do that we proceed by induction on the dimension of W.
If $dimW = 1$, then $k[W] = k[\epsilon]$ and $F(A' \times k[W]) \to F(A') \times F(k[W])$ is a bijection by H_2.
Let now $dimW = n + 1$, then we can rewrite $k[W] \cong k[W'] \times_k k[\epsilon]$ where $dimW' = n$. We get that:

$$\begin{aligned} F(A' \times_k k[W]) &\cong F((A' \times_k k[W']) \times_k k[\epsilon]) \\ &\cong F(A' \times_k k[W']) \times F(k[\epsilon]) \\ &\cong F(A') \times F(k[W']) \times F(k[\epsilon]) \\ &\cong F(A') \times F(k[W'] \times_k k[\epsilon]) \end{aligned}$$

Where we have used (H_2) in the first and third passage and the inductive hypotesis in the second one.

Remark 3.10. By induction on $\text{length}(A'') - \text{length}(A)$ it follows from (H_1) that 3.1 is surjective $\forall A'' \to A$ surjection.

Remark 3.11. We can view condition (H_4) in the following way. For each A in $\mathbf{C}$ and each ideal I in A such that $\mathfrak{m}_A I = (0)$, we have a ring isomorphism:

$$A \times_{A/I} A \xrightarrow{\sim} A \times_k k[I]$$

induced by the map:

$$(x, y) \mapsto (x, x_0 + y - x)$$

where x and y are in A and x_0 is in the k residue of x. It is in fact easy to check that the map is:

- *injective*: $(x, x_0 + y - x) = (0, 0) \quad \Rightarrow \quad x = 0$ and $y = 0$
- *surjective*: one element of $A \times_k k[I]$ is of the form $(a, k+x)$, with $x \in I$: $x^2 \cong 0$. It follows that $\bar{a} = k$, i.e. we have elements of the type $(a, \bar{a}+x)$ with $x \in I$, $x^2 \cong 0$. So the element $(a, \bar{a} + x)$ is the image of $(a, x + a)$.
- *respect the additive structure*: $(x_1 + x_2, y_1 + y_2) \mapsto (x_1 + x_2, \overline{x_1 + x_2} + y_1 + y_2 - x_1 - x_2)$ which is equal to $(x_1, \overline{x_1} + y_1 - x_1) + (x_2, \overline{x_2} + y_2 - x_2)$

Now, given a small extension $p : A' \to A$ with kernel I we get, by (H_2) and the isomorpshim above, the map:

$$F(A') \times (t_F \otimes I) \to F(A') \times_{F(A)} F(A')$$

In fact we get:

$$A' \times_{A'/I} A' \cong A' \times_k k[I] \quad \Rightarrow \quad F(A' \times_{A'/I} A') \cong F(A' \times_k k[I])$$

so, by applying (H_2), we have that:

$$F(A' \times_{A'/I} k[I]) \quad \text{is in bijection with} \quad F(A' \times_{A'/I} A'), \quad \text{and} \quad A'/I \cong A.$$

Now we can consider the diagram:

$$\begin{array}{ccc} F(A' \times_{A'/I} A') & \xrightarrow{\sim} & F(A' \times_k k[I]) \\ \downarrow & & \updownarrow \wr \\ F(A') \times_{F(A'/I)} F(A') & \dashleftarrow & F(A') \times F(k[I]) \end{array}$$

which is easily seen to determine, $\forall \eta \in F(A)$, a group action of $t_F \otimes I$

on the subset $F(p)^{-1}(\eta)$ of $F(A')$. Moreover, (H_2) implies that this action is transitive, while (H_4) is precisely the condition that this action makes $F(p)^{-1}(\eta)$ a principal homogeneous space under $t_F \otimes I$.

3.2.3 Proof of the Theorem

We can finally prove the Schlessinger Criterion.

Proof. (1) ($\Leftarrow$) We first suppose that F satisfies the conditions (H_1), (H_2), (H_3).

Let $t_1, \dots, t_r$ a basis for the dual of t_F and let $S = \Lambda[[T_1, \dots, T_r]]$, with $\mathfrak{n}$ maximal ideal of S. We will construct R as the projective limit of successive quotients of S.

Let:

$$R_2 = \frac{S}{\mathfrak{n}^2 + \mu S} \cong k[\epsilon] \times_k \cdots \times_k k[\epsilon] = k[t_F^*]$$

In fact we have that t_S^* can be identified with t_F^* because they are vector spaces of the same dimension. In particular, we have:

$$F(R_2) \cong F(k[t_F^*]) \overset{(H_2)}{\cong} t_F \otimes t_F^*$$

and since $\sum t_i^v \otimes t_i \in t_F \otimes t_F^*$ we can choose $\xi_2 = \sum t_i^v \otimes t_i$ and using a similar construction as in 3.4, we know that it induces a map from h_{R_2} to F.

Now, since $t_F^* \cong t_S^* \cong t_{R_2}^*$, we get that ξ_2 induces a bijection between t_{R_2} and t_F (dual of the isomorphism used to identify the t_i as basis for the space t_F^*).

We can now work by induction. Suppose we have found (R_q, ξ_q), with $R_q = S/J_q$.

We are looking for an ideal J_{q+1} in S, minimal among those ideals J in S satisfying the following conditions:

(a) $\mathfrak{n}J_q \subseteq J \subseteq J_q$

(b) ξ_q lifts to S/J

We want to show that the collection of those ideals is non-empty and closed under intersection. Since J_q satisfies the conditions, the collection is non empty. Moreover, the first condition is obviously closed under arbitrary intersections, so we just need to check the second one.

We first notice that the ideals J correspond to subspaces of the finite dimensional vector space $J_q/\mathfrak{n}J_q$. This follows from the fact that we have a Noetherian ring and we are considering an S-module. In fact, we remark that in general, if $S \supseteq M$, for an S-module M such that $\mathfrak{n}M = 0$, then M is an $S/\mathfrak{n} = k$-module.

It follows that it suffices to check the condition for finite (so pairwise) intersection.

Let's now J, K be ideals that satisfy these conditions. Since we are in $J_q/\mathfrak{n}J_q$, we may enlarge J so that $J + K = J_q$, without changing the intersection $J \cap K$. Then:

$$S/J \times_{S/J_q} S/K \cong S/(J \cap K)$$

In fact we have the following commutative diagram:

$$\begin{array}{ccc} S/J & \longrightarrow & S/(J+K) \\ \uparrow & & \uparrow \\ Z & \longrightarrow & S/K \end{array}$$

where

$$Z = S/J \times_{S/(J+K)} S/K$$

and exists because of the property of the pull-back.

Now, using H_1 and remark 3.10, we get that we can lift ξ_q at $S/J \cap K$, so $J \cap K = J_q \cap K$ satisfies our condition.

Thus we can choose J_q to be the intersection of all the elements of the collection considered above, and we get:

$$R_{q+1} = S/J_{q+1}$$

and

$$\xi_{q+1} \in F(R_{q+1})$$

where ξ_{q+1} can be arbitrarily chosen as long as it projects onto $\xi_q \in F(R_q)$.

Now let $J = \cap J_q$ for $q = 2, 3, \ldots$, we have $R = S/J$.

We have that $\mathfrak{n}^q \subseteq J_q$, and, in fact:

$$J_q \supseteq \mathfrak{n}J_{q-1} \supseteq \mathfrak{n}(\mathfrak{n}J_{q-2}) \supseteq \cdots \supseteq \mathfrak{n}^{q-3}\mathfrak{n}J_2$$

and $J_2 \supseteq \mathfrak{n}^2$, which proves our statement. Since this is true, we have that the J_q/J form a basis for the topology in R, so that $R = \varprojlim \xi_q$.

Now, due to the choice made for R_2, we get that $t_F \cong t_R$, so we just need to check that $h_R \to F$ is smooth.

Let $p : (A', \eta') \to (A, \eta)$ a morphism of couples, where p is a small extension, $A = A'/I$ and $u : (R, \xi) \to (A, \eta)$ is a given morphism. We first notice that we can restrict our analysis to

the case in which we have a small extension (remark 3.2). We want to lift u to a morphism $(R,\xi) \to (A',\eta')$. We show that, despite we want a morphism of couple, we only need a morphism of algebras $u' : R \to A'$ such that $pu' = u$. In fact we have that the condition $F(u')(\xi) = \eta$ is always satisfied since η' and $F(u')(\xi)$ are in $F^{-1}(p)(\eta)$, and this in particular follows by the fact that:

- $F(p)(\eta') = \eta$ since p is a moprhism of couples
- $F(p)(F(pu')(\xi)) = F(pu')(\xi) = F(u)(\xi) = \eta$ and this holds since the action is transitive (in fact $\exists\, \sigma \in t_F \otimes I$ such that $[F(u')(\xi)]^\sigma = \eta'$)

We get that, given such a u', $\exists\, \sigma \in t_F \otimes I$ such that $[F(u')(\xi)]^\sigma = \eta'$ and then by the diagram below we get that $v' = (u')^\sigma$ satsfies $F(v')(\xi) = \eta'$, $pv' = u$.
We have the following commutative diagram:

$$\begin{array}{ccc} h_R(A') \times (t_F \otimes I) & \longrightarrow & h_R(A') \times_{h_R(A)} h_R(A') \\ \downarrow & & \downarrow \\ F(A') \times (t_F \otimes I) & \longrightarrow & F(A') \times_{F(A)} F(A') \end{array}$$

In fact, since $t_F \otimes I$ acts transitively on $F(p)^{-1}(\eta)$, $\exists \sigma \in t_F \otimes I$ such that $\sigma(F(u')(\xi)) = \eta'$. Now, since $u' \in h_R(p)^{-1}(u')$, we get that $\sigma u' = v' \in h_R(p)^{-1}(u)$, i.e. $pv' = u$.
Moreover, $F(v')(\xi) = F(\sigma u')(\xi) = \sigma(F(u')(\xi)) = \eta'$, where the last equality follows from the fact that $t_F \otimes I$ must commute with the morphism $h_R \to F$ induced by ξ.
Now, u factors as $(R,\xi) \to (R_q,\xi_q) \to (A,\eta)$ for some q, thus it is

enough to complete the diagram:

$$\begin{array}{ccc} R_{q+1} & \longrightarrow & A' \\ \downarrow & & \downarrow p \\ R_q & \longrightarrow & A \end{array}$$

or, equivalently, the diagram:

$$\begin{array}{ccc} \Lambda[[T_1,\ldots,T_r]] = S & \xrightarrow{w} & R_q \times_A A' \\ \downarrow & \overset{v}{\nearrow} & \downarrow pr_1 \\ R_{q+1} & \longrightarrow & R_q \end{array}$$

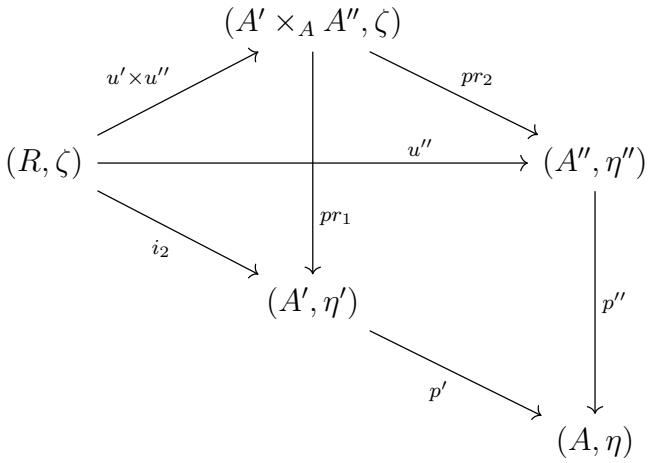
where w has been chosen so as to make the square commute. If the small extension pr_1 has a section, then v obviously exists (is obtained by composing the section with the projection $R_{q+1} \to R_q$). Otherwise, by lemma 3.1(ii) , pr_1 is essential and since the composition is surjective w is a surjection by essentiality (to establish the existence of v it is enough that $\ker(w) \supseteq J_{q+1}$, so that w factors through $R_{q+1} = S/J_{q+1}$). Now, using (H_1) applied to the projections of $R_q \times_A A'$ on its factors, $\xi \in F(R_q)$ lifts back to $R_q \times_A A'$, so $\ker(w) \supseteq J_{q+1}$, by choice of J_{q+1}. Thus w factors through $S/J_{q+1} = R_{q+1}$, and v exists.

This completes the proof that (R, ξ) is a hull of F.

($\Rightarrow$) Conversely, suppose that a pro-couple (R, ξ) is a hull of F.

To verify (H_1), let $p' : (A', \eta') \to (A, \eta)$ and $p'' : (A'', \eta'') \to (A, \eta)$ be morphisms of couples, where p'' is a surjection. Now, since $h_R \to F$ is smooth (it is induced by ξ and we have an hull), then it is also surjective (is a functor map and it is smooth, so we can use the remark). This implies that there exists a $u' \in h_R$ such

that $u' : (R, \xi) \to (A', \eta)$, and hence by smoothness of $h_R \to F$ applied to p'', there exists $u'' : (R, \xi) \to (A'', \eta'')$ rendering the following diagram commutative:



If we consider the map: $u' \times u : (R, \xi) \to (A' \times_A A'', \zeta)$, we see that $\zeta = F(u' \times u'')(\xi)$ projects onto η' and η'', so that (H_1) is satisfied.

We can now suppose that $(A, \eta) = (k, e)$, and $A'' = k[\epsilon]$. In order to show that we have a bijection we show that ζ is unique. If ζ_1 and ζ_2 in $F(A' \times_k k[\epsilon])$ we have the same projections η' and η'' on the factors, then choosing u' as above we get morphisms:

$$u' \times u_i : (R, \xi) \to (A' \times_k k[\epsilon], \zeta_i) \qquad for\ i = 1, 2$$

by smoothness applied to the projection of $A' \times_k k[\epsilon]$ on A'.

Since $t_F \cong t_r$ we have that $u_1 = u_2$, so that also $\zeta_1 = \zeta_2$, which proves (H_2).

Now we know that $t_R \cong t_F$ and the dimension is finite since R is Noetherian, so (H_3) holds as well.

(2) The necessity of the four conditions is already been proved in a remark. Suppose now that F satisfies conditions (H_1) to (H_4).

By part (1) we know that F has a hull (R, ξ). We shall prove that $h_R(A) \xrightarrow{\sim} F(A)$ by induction on length(A). Consider a small extension $p : A' \to A = A'/I$ and assume that $h_R(A) \xrightarrow{\sim} F(A)$. For each $\eta \in F(A)$, we have that $h_R(p)^{-1}(\eta)$ and $F(p)^{-1}(\eta)$ are both formally principal homogeneous spaces under $t_F \otimes I$ (see remark 3.11). Now $h_R(A')$ maps onto $F(A')$ because it is smooth, so we have $h_R(A') \xrightarrow{\sim} F(A')$, which proves the induction step.

□

Chapter 4

Deforming Galois Representations

We can finally analyze the work of Barry Mazur about Universal deformation rings ([11]).

Given a continuous homomorphism $\bar{\rho} : G_{\mathbb{Q},S} \to \mathrm{GL}_2(\mathbb{F}_p)$, the idea is to try to study, in a systematic way, the possible liftings of $\bar{\rho}$ to p-adic representations $\rho_0 : G_{\mathbb{Q},S} \to \mathrm{GL}_2(\mathbb{Z}_p)$.

More precisely, given the following continuous morphism:

$$\Pi \to \mathrm{GL}_N(A)$$

we can consider $V = A^N$ and we have an action of $\Pi \to V$ such that, if $\sigma \in \Pi$, $v \in V$, $\sigma \cdot v = \rho(\sigma) \cdot v \in V$. From this we get an action:

$$\Pi \times V \to V$$
$$(\sigma, v) \mapsto \sigma v$$

which is continuous (on one side we have the m-adic topology, on the other the pro-finite topology). So, we can view $\rho : \Pi \to \mathrm{GL}_N(A)$ as an action of Π on a Π-module $V = A^N$.

On the other side, let W be a free A-module with the action of Π defined as:

- $\forall \sigma \in \Pi,\ x, y \in W,\ \sigma(ax + by) - a(\sigma x) + b(\sigma y)$ for $a, b \in A$
- $\sigma, \tau \in \Pi,\ x \in W,\ \sigma(\tau x) = (\sigma\tau)x$
- $1\Pi x = 1$

We can now fix a basis $(e_1, e_2, \dots e_N)$ of W.
Then, $\forall \sigma \in \Pi,\ \sigma e_i = \sum_{j=1}^{N} a_{ji}(\sigma) \cdot e_j$ and by:

$$\sigma \mapsto (a_{ij}(\sigma))_{i,j} \in \mathrm{GL}_N(A)$$

we get:

$$\rho_B : \Pi \to \mathrm{GL}_N(A)$$

We remark that ρ_B depends by the basis, and not only by the module.
We have seen that:

$$Rep_{A,N}(\Pi)/_\sim \overset{\sim}{\leftarrow} \{\rho : \Pi \to \mathrm{GL}_N(A)\}/_\sim$$

Now, we can consider the category, $\hat{\mathbf{C}}_k(A)$, of the Noetherian algebras that are complete, local and such that $A/\mathfrak{m} \cong k$.
Now, if we choose an $N \in \mathbb{N}$ and a residual representation $\bar{\rho} : \Pi \to \mathrm{GL}_N(k)$, we can consider the deformation functor:

$$\begin{aligned} D_\rho : \hat{\mathbf{C}}_k(A) &\to Sets \\ A &\mapsto \frac{\mathrm{Hom}_{\bar{\rho}}(\Pi, \mathrm{GL}_N(A))}{\ker(\mathrm{GL}_N(A) \to \mathrm{GL}_N(k))} \end{aligned}$$

We want to show that this functor is representable, i.e. $\exists (R, \phi_R) \in \hat{\mathbf{C}}_k(A)$ such that $D_\rho(-) = \mathrm{Hom}_k((R, \phi_R), -)$.

Furthermore, we are interested in the automorphisms of this functor. We can view them as a functor:

$$\begin{aligned} \mathrm{Aut}(D_\rho) : \hat{\mathbf{C}}_k(A) &\to \mathit{Groups} \\ A &\mapsto \mathrm{Aut}(D_\rho(A)) \end{aligned}$$

and we can look at this functor in the following way. For evey $\phi \in D_\rho(A)$ we have a module $M(\phi)$ and an associated ring $R = A[\Pi]$, and the automorphisms, viewed as R-modules of $M(\phi)$, are:

$$\begin{aligned} \mathrm{Aut}_R(M(\phi)) = G(\phi) &= \{\alpha \in G \,|\, \alpha\phi = \phi^\alpha\} \\ &= \{\lambda Id_N,\, \lambda \in A^\times\} \cong \mathbf{Gm}(A) \end{aligned}$$

where $A^\times$ is the set of scalars that are units in A, $\mathbf{Gm}(A)$ is the multiplicative group of A and the equation on the second line holds if the representation is absolutely irreducible. Thus, we get $\mathrm{Aut}(D_\rho)(A) \cong \mathbf{Gm}(A)$.

4.1 Deformations

In this section, Π will denote a profinite group satisfying the condition ϕ_p, and k will refer to a finite field of characteristic p. Let $\hat{\mathbf{C}}$ denote the category of complete Noetherian local rings with residue field k. We refer to an object of $\hat{\mathbf{C}}$ as a "local ring in $\hat{\mathbf{C}}$", and a morphism of the category is a homomorphism of complete local rings inducing the identity on residue fields. We can finally define the main objects that we will study in this chapter.

Definition 4.1. Let N be a positive integer. If A is a local ring in $\hat{\mathbf{C}}$, two continuous homomorphisms from Π to $\mathrm{GL}_N(A)$ are ***strictly equivalent*** if one can be brought to another by conjugation with an element in the kernel

of the reduction map $\mathrm{GL}_N(A) \to \mathrm{GL}_N(k)$.

Definition 4.2. A ***representation*** of Π in $\mathrm{GL}_N(A)$ is a strictly equivalence class of continuous homomorphisms from Π to $\mathrm{GL}_N(A)$. Thus, if $A = k$, a representation is nothing more than a continuous homomorphism. By abouse of notation we will sometimes write $\rho_0 : \Pi \to \mathrm{GL}_N(A)$ where ρ_0 is a representation.

Definition 4.3. If $A_1 \to A_2$ is a morphism in the category $\hat{\mathbf{C}}$ and if ρ_1 and ρ_2 are representations of Π in $\mathrm{GL}_N(A_1)$ and in $\mathrm{GL}_N(A_2)$ respectively, we say that ρ_1 is a ***deformation*** of ρ_2 if any homomorpshim from Π to $\mathrm{GL}_N(A_1)$ in the strict equivalence class ρ_1, composed with the induced homomorphism $\mathrm{GL}_N(A_1) \to \mathrm{GL}_N(A_2)$, yields a homomorpshim in the strict equivalence class ρ_2.

Definition 4.4. A ***residual representation*** of dimension N is a continuous homomorphism $\bar{\rho} : \Pi \to \mathrm{GL}_N(k)$, i.e. a representation of Π in $\mathrm{GL}_N(k)$.
Two residual representations are ***equivalent*** if one can be brought into the other by conjugation by an element in $\mathrm{GL}_N(k)$; they are ***twist equivalent*** if one, after tensoring with a suitable one-dimensional representation, can be made equivalent to the other.

4.2 Cohomological interpretation of Zariski tangent A-modules

One of the basic tools of deformation theory is the cohomological interpretation of the Zariski tangent space. This allows us to "control" the somewhat abstract universal deformation rings that occur by means of concrete cohomological calculations.

Let Π satisfy the p-finiteness condition as above, $\bar{\rho} : \Pi \to \mathrm{GL}_N(k)$ a continuous residual representation with k a finite field of characteristic p, and Λ a coefficient-ring with residue field k. We fix an homomorphism $\rho : \Pi \to \mathrm{GL}_N(A)$, and we consider the deformation problem relative to ρ, i.e. the functor:

$$D_\rho : \hat{\mathbf{C}}_\Lambda(A) \to Sets$$

More specifically, we consider the Zariski tangent A-module, $t_{D_\rho,A}$, which we will denote by t_ρ.

Following the idea sketched in the introduction to this chapter, we interpret it from a cohomological point of view. Let V be the free A-module of rank N, i.e. $V = A^N$, endowed with an A-linear action given via composition of $\rho : \Pi \to \mathrm{GL}_N(A)$ with the natural action of $\mathrm{GL}_N(A)$ on V. Let now $\mathrm{End}_A(V)$ denote the free A module (of rank N^2) consisting of A-linear endomorphisms of V. The action of Π on V induces an action, the adjoint action, of Π on $\mathrm{End}_A(V)$ given by the formula:

$$(\sigma \cdot e)(v) = \rho(\sigma)(e(\rho(\sigma)^{-1}(v))$$

where $\sigma \in \Pi$, $e \in \mathrm{E}_A(V)$ and $v \in V$.

Proposition 4.1. *There is a natural isomorphism of A-modules*

$$t_\rho \cong H^1(\Pi, \mathrm{End}_A(V))$$

Proof. Let $\Gamma := \ker\{\mathrm{GL}_N(A[\epsilon]) \to \mathrm{GL}_N(A)\}$, we have the following short exact sequence of groups:

$$1 \longrightarrow \Gamma \longrightarrow \mathrm{GL}_N(A[\epsilon]) \longrightarrow \mathrm{GL}_N(A) \longrightarrow 1$$

Since we can rewrite every element $T \in \mathrm{GL}_N(A)$ as $T = Id + \epsilon M_N(A)$, we notice that we have an injection $\mathrm{GL}_N(A) \subset \mathrm{GL}_N(A[\epsilon])$, from which we derive a natural splitting.
In this way, we can view $\mathrm{GL}_N(A[\epsilon])$ as a semidirect product $\mathrm{GL}_N(A) \ltimes \Gamma$.
In fact, if we consider:

$$\begin{aligned} \mathrm{GL}_N(A[\epsilon]) &\to \Gamma \times \mathrm{GL}_N(A) \\ u &\mapsto (u\phi(u)^{-1}, \phi(u)) \end{aligned}$$

where we notice that:

$$\phi(u\phi(u)^{-1}) = \phi(u)\phi(u)^{-1} = 1$$

Moreover, letting $M_N(A)$ denote the underlying additive group of the A-algebra of $N \times N$ matrices with entries in A, there is a natural isomorphism of commutative groups:

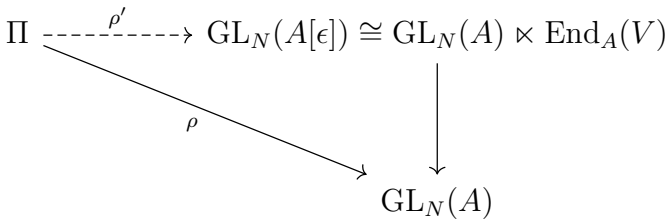
$$\begin{aligned} \Gamma = 1 + \epsilon \cdot M_N(A) \cong M_N(A) \cong \mathrm{End}_A(V) \\ 1 + \epsilon \cdot m \mapsto m \end{aligned}$$

Therefore, using these isomorphisms, one may rewrite $\mathrm{GL}_N(A[\epsilon])$ as the semidirect product:

$$\mathrm{GL}_N(A[\epsilon]) \cong \mathrm{GL}_N(A) \ltimes M_N(A)$$

where the action of $\mathrm{GL}_N(A)$ on $M_N(A)$ is the standard adjoint action (i.e. it is by conjugation).
Now, if we consider the set $D_\rho(A[\epsilon])$ of deformations lifting ρ to $A[\epsilon]$, we have that this is the set of equivalence classes (relative to ρ) of homomorphisms

$\rho' : \Pi \to \mathrm{GL}_N(A[\epsilon])$ fitting into the diagram:



where the composition is ρ.

Since we are considering the case of strict equivalence and we have an action of $\Gamma \subset \mathrm{GL}_N(A[\epsilon])$, once we fix a ρ_0 we can obtain every ρ' by conjugation: $\rho' = \gamma\rho\gamma^{-1}$.

For any other ρ', we define the *difference cocycle*:

$$c_{\rho'} : \Pi \to \Gamma \cong \mathrm{End}_A(V)$$

$$c_{\rho'}(g) = \rho'(g) \cdot \rho_0(g)^{-1} \in \Gamma \qquad \text{for } g \in \Pi$$

where in particular we notice that $\rho'(g) \in \mathrm{GL}_N(A[\epsilon])$ and $\rho_0(g)^{-1} \in \mathrm{GL}_N(A)$, so the product is actually in Γ. Moreover, this is actually a cocycle, i.e. it satisfies the property:

$$c_{\rho'}(g_1 g_2) = c_{\rho'}(g_1) c_{\rho'}(g_2)^{g_1}$$

In fact we have that:

$$\begin{aligned} c_{\rho'}(g_1g_2) &= \rho'(g_1g_2) \cdot \rho_0(g_1g_2)^{-1} = \rho'(g_1)\rho'(g_2)\rho_0(g_2)^{-1}\rho_0(g_1)^{-1} = \\ &= \rho'(g_1)c_{\rho'}(g_2)\rho_0(g_1)^{-1} = \rho'(g_1)\rho_0(g_1)^{-1}\rho_0(g_1)c_{\rho'}(g_2)\rho_0(g_1)^{-1} = \\ &= c_{\rho'}(g_1)c_{\rho'}(g_2)^{g_1} \end{aligned}$$

This proves that we have a bijection between the set of liftings ρ' of ρ , and

the set $Z^1(\Pi, \mathrm{End}_A(V))$ of 1- cocycles on Π with the values in the Π-module $\mathrm{End}_A(V) \cong M_N(A)$, where the action of Π on $\mathrm{End}_A(V)$ is the adjoint action as described above. So we have construct a map:

$$\{\rho' : \Pi \to \mathrm{GL}_N(A[\epsilon])\} \to Z^1(\Pi, \mathrm{End}_A(V))$$

Under this bijection, liftings ρ' and ρ'' of $\bar{\rho}$ are strictly equivalent if and only if their associated cocycles $c_{\rho'}$ and $c_{\rho''}$ are cohomologous. In fact, we know that if $N \in M_N(A)$, then $(1 + N\epsilon)^{-1} = (1 + N\epsilon) \in \mathrm{GL}_N(A[\epsilon])$, so it follows that the cocycles given by ρ' and $\rho'' = (1 + N\epsilon)\rho(1 - N\epsilon)^{-1}$ differ by the cobundary $N - gN$. We remark that, since this process can be reversed, we have injectivity.
We get:

$$\{\rho' : \Pi \to \mathrm{GL}_N(A[\epsilon])\}/\Pi \to \frac{Z^1(\Pi, \mathrm{End}_A(V))}{B^1(\Pi, \mathrm{End}_A(V))} = H^1(\Pi, \mathrm{End}_A(V))$$

□

We can now state the following proposition:

Proposition 4.2. *Let A be an Artinian coefficient Λ-algebra. Then the Zariski tangent A-module t_ρ is finite.*

Proof. Let A be Artinian. The proposition before is enough to show that the A-module $H^1(\Pi, \mathrm{End}_A(V))$ is finite.
Let $\Pi_0 \subset \Pi$ be the kernel of ρ. Since A is Artinian, Π_0 is an open subgroup of finite index in Π.
The A-module $H^1(\Pi, \mathrm{End}_A(V))$ fits into an exact sequence:

$$H^1(\Pi/\Pi_0, \mathrm{End}_A(V)) \longrightarrow H^1(\Pi, \mathrm{End}_A(V)) \longrightarrow \mathrm{Hom}(\Pi_0, \mathrm{End}_A(V))$$

Now, the A-module $H^1(\Pi/\Pi_0, \mathrm{End}_A(V))$ is finite since both Π/Π_0 and $\mathrm{End}_A(V)$ are finite. On the other hand, also $\mathrm{Hom}(\Pi_0, \mathrm{End}_A(V))$ is finite, since Π satisfies the p-finiteness condition. It follows that $H^1(\Pi, \mathrm{End}_A(V))$ is finite. □

4.3 The Main Theorem

We want to establish the existence of a universal deformation of any absolutely irreducible N-dimensional residual representation $\bar{\rho}$. Specifically, there is a complete Noetherian local ring $R = R(\Pi, k, \bar{\rho}) \in \hat{\mathbf{C}}$ with residue field k, together with a deformation: $\boldsymbol{\rho} : \Pi \to \mathrm{GL}_N(R)$ of $\bar{\rho}$ which is universal in the sense that for any $A \in \hat{\mathbf{C}}$ and deformation ρ_0 of $\bar{\rho}$ to A, there is a unique morphism $R \to A$ in $\hat{\mathbf{C}}$ such that the induced homomorphism $\mathrm{GL}_N(R) \to \mathrm{GL}_N(A)$ brings $\boldsymbol{\rho}$ to ρ_0. We shall show that the pair $(R, \boldsymbol{\rho})$ is determined up to canonical isomorphism by the twist-equivalence class of $\bar{\rho}$.

4.3.1 Statement

Proposition 4.3 (Existence and uniqueness)**.** *(a) If $\bar{\rho}$ is absolutely irreducible, a universal deformation ring $R = R(\Pi, k, \bar{\rho})$ and a universal deformation $\boldsymbol{\rho}$ of $\bar{\rho}$ to R exist. The pair $(R, \boldsymbol{\rho})$ is uniquely determined up to canonical isomorphism by the twist-equivaence class of $\bar{\rho}$ in the following sense:*

Given two twist-equivalent residual representations $\bar{\rho}$ and $\bar{\rho}'$, there is a canonical isomorphism

$$r(\bar{\rho}', \bar{\rho}) : R(\Pi, k, \bar{\rho}) \xrightarrow{\sim} R(\Pi, k, \bar{\rho}')$$

bringing the universal deformation $\boldsymbol{\rho}$ *of* $\bar{\rho}$ *to the universal deformation* ρ' *of* $\bar{\rho'}$*. The system of canonical isomorphisms have the homomorphic property:*

(i) $r(\bar{\rho}, \bar{\rho})$ *is the identity, for all* $\bar{\rho}$

(ii) $r(\bar{\rho''}, \bar{\rho'}) \times r(\bar{\rho'}, \bar{\rho}) = r(\bar{\rho''}, \bar{\rho})$

(b) If $\bar{\rho}$ *is not absolutely irreducible, then a "versal" deformation of* $\bar{\rho}$ *exists, i.e. there is a hull. This means that we can find an object* $R \in \hat{\boldsymbol{C}}$ *and a deformation* $\boldsymbol{\rho}$ *of* $\bar{\rho}$ *to* R *such that any deformation* ρ_0 *of* $\bar{\rho}$ *to any object* A *in* $\hat{\boldsymbol{C}}$ *is induced by a not necessarily unique morphism* $R \to A$ *of* $\hat{\boldsymbol{C}}$*; however, if* A *is the "dual numbers"* $k[\epsilon]$*, the morphism* $R \to A$ *bringing* $\boldsymbol{\rho}$ *to* ρ_0 *is unique.*

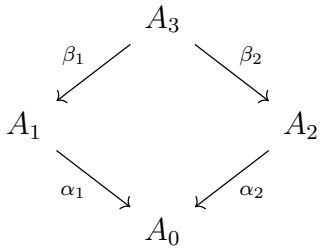
The isomorphism-type of the hull R *is unique, but* R *itself is not determined up to canonical isomoprhism.*

4.3.2 Preliminary results

We are going to prove only the existence of universal and versal deformation ring.

Before actually proceed with the proof we are going to state some preliminary results that will be used for proving our statement.

Let A_0, A_1, A_2, A_3 Artinian rings in $\hat{\mathbf{C}}$ such that $A_3 \cong A_1 \times_{A_0} A_2$, i.e. we get the following cartesian diagram:



Suppose now that $A_1 \to A_0$ is a small extension, i.e. a surjective map whose kernel is a nonzero principal ideal (t) such that $\mathfrak{m}_{A_1} \cdot (t) = 0$.
Let:

$$E_i = \mathrm{Hom}_{\bar{\rho}}(\Pi, \mathrm{GL}_N(A_i)) \qquad \text{for } i = 0, \ldots, 3$$

where $\bar{\rho}$ means continuous homomorphisms which are liftings of $\bar{\rho}$.
Set

$$G_i = \ker(\mathrm{GL}_N(A_i) \to \mathrm{GL}_N(k)) \qquad \text{for } i = 0, \ldots, 3$$

We recall that an element of G_i is of the from $Id_N + M_{N\times N}(\mathfrak{m}_A)$.
G_i acts naturally on E_i by conjugation of the range $\mathrm{GL}_N(A_i)$ and the orbit-space E_i/G_i may be indetified with the space of deformations of $\bar{\rho}$ to A_i.
Since E_i is functorial, we get the natural morphism:

$$b : E_3/G_3 \to E_2/G_2 \times_{E_0/G_0} E_1/G_1$$

We are now going to state five important lemmas that will be used in the proof of the main theorem.

Lemma 4.4. *If $\alpha : A_1 \to A_0$ is surjective, then it induces a surjection $\alpha : G_1 \to G_0$.*

Proof. Let $\alpha : A_1 \to A_0$ be surjective, then, since we have local rings, it follows that the induced group homomorphism $\alpha : \mathrm{GL}_N(A_0) \to \mathrm{GL}_N(S)$ is surjective. Let $i_j : \mathrm{GL}_N(A_j) \to \mathrm{GL}_n(k)$ for $j = 0, 1$.
For $Y \in G_0$, we want to show that it comes from an $X \in G_1$. Since $Y \in G_0$ it follows by definition that $i_0(Y) = I_N$. Now, using the surjectivity of α, we get that $\exists X \in \mathrm{GL}_N(A_1)$ such that $\alpha(X) = Y$.
Using the fact that α is a morphism in the category, we know that $i_0 \cdot \alpha = i_1$, hence $i_1(X) = i_0(\alpha(X)) = i_0(Y) = I_n$ and $X \in G_1$. □

Lemma 4.5. *Since the map $G_1 \to G_0$ is surjective, it follows that b is surjective.*

Proof. Let $([a_2, a_1]) \in E_2/G_2 \times_{E_0/G_0} E_1/G_1$ and let $\alpha_i : A_i \to A_0$ for $i = 1, 2$. Using the definition of fiber product, we have that $[\alpha_1(a_1)] = [\alpha_2(a_2)]$ in E_0/G_0, i.e. there exists $X \in G_0$ such that $\alpha_1(a_1) = X\alpha_2(a_2)X^{-1}$. Since α_2 is surjective, applying the previous lemma we get that $\alpha_2 : G_2 \to G_0$. It follows that there exists $X_2 \in G_2$ with $\alpha_2(X_2) = X$. Thus $\alpha_1(a_1) = \alpha_2(X_2 a_2 X_2^{-1})$. Therefore $(a_1, X_2 a_2 X_2^{-1}) \in E_3/G_3$ and

$$b([(a_1, X_2 a_2 X_2^{-1})]) = ([X_2 a_2 X_2^{-1}], [a_1]) =)[a_2, a_1]$$

□

Let π_1 denote an element in E_1 and π_0 its image in E_0. Set $G_i(\pi_i)$ to be the subgroup of G_i consisting of all elements commuting with the image of π_i in $\mathrm{GL}_N(A_i)$, for $i = 0, 1$.

Lemma 4.6. *If, for all $\pi_2 \in E_2$ the natural mapping $G_2(\pi_2) \to G_0(\pi_0)$ is surjective, then b is injective.*

Proof. Let $\beta_i : A_3 \to A_i$ for $i = 1, 2$.
Let $\pi_3, \tilde{\pi}_3 \in E_3$, with:

$$([\pi_2], [\pi_1]) = b([\pi_3]) = b([\tilde{\pi}_3]) = ([\tilde{\pi}_1], [\tilde{\pi}_3])$$

where $\pi_1 = \beta_1(\pi_3)$, $\pi_2 = \beta_2(\pi_3)$, $\tilde{\pi}_1 = \beta_1(\tilde{\pi}_3)$ and $\tilde{\pi}_2 = \beta_2(\tilde{\pi}_3)$. Then there exist $X_1 \in G_1$ and $X_2 \in G_2$ with $X_1 \pi_1 X_1^{-1} = \tilde{\pi}_1$ and $X_2 \pi_2 \pi_2^{-1} = \tilde{\pi}_2$. Let now $\bar{X}_1, \bar{X}_2$ be the images under α_1, α_2 of X_1 and X_2 in G_0.
Let $\pi = \alpha_1(\pi_1) = \alpha_2(\pi_2)$ and $\tilde{\pi} = \alpha_1(\tilde{\pi}_1) = \alpha_2(\tilde{\pi}_2)$. Then, we get that

$\bar{X}_1\pi\bar{X}_1^{-1} = \tilde{\pi} = \bar{X}_2\pi\bar{X}_2^{-1}$ and $\bar{X}_2^{-1}\bar{X}_1 \in G_0(\pi_0)$.
By hypothesis, there exists $Y \in G_2(\pi_2)$ with $\bar{Y} = \bar{X}_2^{-1}\bar{X}_1$. Let $\tilde{X}_2 = X_2Y$, then we get:

$$\tilde{X}_2\pi_2\tilde{X}_2^{-1} = X_2Y\pi_2Y^{-1}X_2^{-1} = X_2\pi_2X_2^{-1} = \tilde{\pi}_2$$

and

$$\bar{\tilde{X}}_2 = \bar{X}_2\bar{Y} = \bar{X}_2\bar{X}_2^{-1}\bar{X}_1 = \bar{X}_1$$

Thus X_1 and $\tilde{X}_2$ define an element X_3 in G_3 and we get $X_3\pi_3X_3^{-1} = \tilde{\pi}_3$. Hence $[\pi_3] = [\tilde{\pi}_3]$ in E_3/G_3. □

Lemma 4.7. *If $A_0 = k$ and $A_2 = k[\epsilon]$ for $\epsilon^2 = 0$, then the map b is injective.*

Proof. Let $\pi_2 \in E_2$. Since $A_0 = k$ by hypothesis and $\alpha_2(\pi_2) = \rho$, we have that $G_0 = G(k) = \{I_n\}$, and thus $G_0(\rho) = \{I_n\}$. Hence the map $G_2(\pi_2) \to G_0(\rho)$ is surjective. Applying the previous lemma we get that b is injective. □

Lemma 4.8. *If $\bar{\rho}$ is absolutely irreducible, then $G_i(\pi)$ consists in the subgroup of scalar matrices in $G_i \subset \mathrm{GL}_N(A_i)$ for $i = 0, 1$.*

Proof. Given $\rho : \Pi \to \mathrm{GL}_N(A)$ we can consider the group $M = A^N$ and view it as a ring $R = A[\Pi]$ so that saying that $\bar{\rho}$ is irreducible is equivalent to say that it is simple.
Now, let $\gamma \in G_0(\pi_0)$: we can view γ as a matrix in $\mathrm{GL}_N(A_0)$ that gives us a morphism $M \to M$; in particular, if it commutes with π_0, it is a R-modules morphism. Thus, since it is a non-zero morphism of R-modules, it is an isomoprhism by Schur's Lemma. Now, in order to be isomoprhic as Π-module, $G_i(\pi)$ has to be a scalar. □

4.3.3 Proof of the Theorem

We can finally prove our Theorem.

Proof. Following the construction and the notation above, we want to prove our Theorem by showing that the Schlessinger criterion holds.
With the first two preliminary lemmas, we have already shown that, since $A_1 \to A_0$ is small extension, our functor b is a surjection, and condition (H_1) always holds.
On the other hand, using the results in the section of the Zariski tangent space, we know that also condition (H_3) always holds.
In order to prove that (H_2) holds, we have to show that the functor is bijective if $A_0 = k$ and $A_2 = k[\epsilon]$. We already know that the surjectivity holds, so under those assumption it is enough to prove that b is injective. This follows from lemma 4.7.
To complete our proof we just need to check that (H_4) holds when $\bar{\rho}$ is absolutely irreducible. If $\bar{\rho}$ is absolutely irreducible, lemma 4.8 implies that the morphism in lemma 4.6 is surjective for all surjective maps $A_1 \to A_0$, hence (H_4) follows.
If $\bar{\rho}$ is absolutely irreducible, we refer to $R = R(\pi, k\bar{\rho})$ as the universal deformation ring of $\bar{\rho}$. The universal deformation ring is unique in the sense that it is determined up to canonical isomorphism. In the more general case in which $\bar{\rho}$ is not necessarily absolutely irreducible, the "versal deformation ring" R is determined up to (noncanonical) isomorphism (which induces the "identity mapping" on Zariski tangent space).
Having obtained the universal deformation ring R, it is now easy to construct the universal deformation $\boldsymbol{\rho}$. In particular, for evey power of the maximal ideal $\mathfrak{m}$ of R, we have a deformation ρ_n of $\bar{\rho}$ to $R/\mathfrak{m}^n$ which can be realized

by a compatible family of liftings $R_n : \Pi \to \mathrm{GL}_N(R/\mathfrak{m}^n)$, using the surjectivity of the homomorphisms $\mathrm{GL}_N(R/\mathfrak{m}^{n+1}) \to \mathrm{GL}_N(R/\mathfrak{m}^n)$. The universal deformation $\boldsymbol{\rho}$ of $\bar{\rho}$ is then just the strict equivalence class of the inverse limit $\varprojlim r_n$. □

Bibliography

[1] Bourbaki, Nicolas; *Algébre commutative*, Chapitre III, Actualité s Sci. Ind (1923)

[2] Breuil, Christope; Conrad, Brian; Diamond, Fred; Taylor, Richard; *On the modularity of elliptic curves over $\mathbb{Q}$: wild 3-adic exercises*, J. American Mathematical Society., 14(4)(2001),843–939 (electronic)

[3] Cornell, Gary; Silverman, Joseph; Stevens, Glenn; *Modular Forms and Fermat's Last Theorem*, Springer-Verlag, New York, Inc (1997)

[4] Darmon, Henri; *The Shimura-Taniyama Conjecture*, Article in the Encyclopedia of Mathematics (1999)

[5] Darmon, Henry; Diamond, Fred; Taylor, Richard; *Fermat's Last Theorem*, Current Developments in Mathematics 1 (1995), International Press, 1-157

[6] Ershov, Mikhail; *Notes on invese limits*, University of Virginia.

[7] Fontaine, Jean-Marc; Mazur, Barry; *Geometric Galois representations*, in J. Coates, S.T Yau, eds. Elliptic Curves, Modular Forms and Fermat's Last Theorem, International Press, Cambridge, 1995.

[8] Iwaniek, Henryk; *Topics in classical automorphic forms*, American Mathematical Society, (1997)

[9] Kani, Ernst; *Lectures on applications in modular forms to Number Theory*, Notes for Queen's University, (2005)

[10] Mazur, Barry; *Modular curves and the Eisenstein ideal*, Publ. Math. IHES 47 (1977), 33-186

[11] Mazur, Barry *Deforming Galois representations*, in: *Galois Groups over* $\mathbb{Q}$, Y. Ihara, K. Ribet, J-P serre, eds, MSRI Publ. 16, Springer-Verlag, New York, Berlin, Heidelberg (1989), 385-437

[12] Serre, Jean Pierre; *A course in Arithmetic*, Graduate Texts in Math. 7, Springer Verlag, New York, Berlin, Heidelberg, (1973)

[13] Schlessinger, Michael; *Functors on Artin rings*, Trans American Mathematical Society 130 (1968), 208-222

[14] Silverman, Joseph; *The arithmetic of Elliptic Curves*, Springer-Verlag, (1986)

[15] Taylor, Richard; Wiles, Andrew; *Ring-theoretic properties of certain Hecke algebras*, Ann. of Math. (2), 141(3)(1995),553–572

[16] Wiles, Andrew; *Modular elliptic curves and Fermat's last theorem*, Ann. of Math. (2), 141(3)(1995), 443–551