Pontificia Universidad
JAVERIANA
Colombia

Deformation theory of Galois representations

Juan Esteban Rodríguez Camargo

Advisors:
Jorge Andrés Plazas, Pontificia Universidad Javeriana.
Guillermo Mantilla Soler, Universidad de los Andes.

A thesis presented for the degree of
Bachelor in Mathematics

Department of Mathematics
Pontificia Universidad Javeriana
Colombia

Contents

Introduction

The main purpose of this document is to introduce the theory of deformations of Galois representations. The theory was first introduced by Mazur in [Maz89] in the 80's as a response to the work of Hida in p-adic families of Galois representations, and highlighted in the proof of Wiles of the Taniyama-Shimura conjecture in [Wil95]. We will principally follow the first six lectures of a graduate course taught by Fernando Q. Gouvêa in 1999 published in [Gou99]. Additionally, in Part II a sketch of the construction of Galois representations coming from elliptic curves and modular forms is presented, together with some equivalent statements of the modularity theorem following the book of Diamond and Shurman [DS05].

At first, we will make explicit the kind of profinite groups we are going to deal with, followed by the construction of our category of rings. More precisely, we shall define the Φ_p condition for profinite groups and the class of coefficient rings. Then, we define the deformation functor $\mathbf{D}_{\overline{\rho}}$ and focus on its representability; we will make use of the Schlessinger's Theorem on representability for the case of artinian coefficient rings $\mathcal{C}_{\Lambda}^{0}$. We also discuss the deformation ring of characters. Some important concepts are introduced, such as tangent space or obstruction, and we state some additional properties in the tame case and in the Galois case. For example, a more concrete dimension conjecture in terms of the number of infinite places of a number field.

The final chapter of part one is dedicated to imposing conditions on the deformation functor, specially being ordinary. This is a quite important feature which plays a huge role in the proof of modularity conjecture.

The second part can be though as an "additional part" which is developed in order to address the context of the main aplication. Here we introduce modular forms, modular curves and Hecke operators. In part three we give a sketch of the construction of Galois representations from cuspidal eigenforms of weight 2, as well as the construction of Galois representations coming from elliptic curves. We end the document with a quick look on the role of deformation theory of Galois representations in the proof of Wiles' theorem.

Finally, I would like to thank my advisors Jorge Andres Plazas and Guillermo Mantilla, they were my guides through this gorgeous world of Number Theory. Basically, the subject covered by this thesis is a consequence of their advise and patience, and my personal goal of fully understand Fermat's Last Theorem. I'd also thank professor Jesus Ochoa, who gave to me some of his time for the discussion of tools I had to learn during the creation of the document. I want to thank my mother, father and sister because they have been a huge pillar in my development as mathematician and human being. I finally thank all my professors during my bachelor, they were the ones who have given to me the basic knowledge to face my future as mathematician.

Part I

Deformation theory of representations

Chapter 1

Galois representations

In this chapter we introduce concepts arising naturally in the study of the absolute Galois group of $\mathbb{Q}$. Given a field K, let K^s be its separable closure and let G_K= $\mathrm{Gal}(K^s/K)$ be its absolute Galois group. Let L/K be a Galois extension of K, we denote the Galois group $\mathrm{Gal}(L/K)$ by $G_{L/K}$ endowed with the Krull topology. Our framework includes global fields (e.g number fields) and local fields (e.g finite extensions of $\mathbb{Q}_p$ for p prime). If $F/\mathbb{Q}_p$ is a finite extension, there exists a unique extension v_F of the valuation v_p of $\mathbb{Q}_p$ to F. We can normalize and suppose further that $v_p = ev_F$ with e denoting the ramification degree of the extension. The valuation ring and the prime ideal of the valuation ring of F are denoted by $\mathcal{O}_F$ and λ_F respectively, the residual field is written as k_F. If the context is clear we may write instead $\mathcal{O}$, λ and k.

Let $L/\mathbb{Q}$ be a number field, we denote the ring of integers of L by $\mathcal{O}_L$. Given $\lambda \subset \mathcal{O}_L$ a prime ideal or λ a prime at infinity we denote by L_λ the completion of L at λ. Let $\mathcal{O}_{L,\lambda}$ be the valuation ring of L_λ.

To describe the absolute Galois group of a field is not, in general, an easy problem. For instance, one of the biggest goals in number theory is to understand as much as possible the absolute Galois group of the rational numbers, the prototypical example of this challenge is the inverse Galois problem which asks whether every finite group is a Galois group over $\mathbb{Q}$, or equivalently whether for every finite group G there exists a continuous surjective homomorphism

$$G_{\mathbb{Q}} \longrightarrow G.$$

In contrast, the absolute Galois group of the finite field $\mathbb{F}_q$ is well understood. In fact, it is possible to give a complete description of this group in terms of the Frobenius automorphism, the final outcome is $G_{\mathbb{F}_q} \cong \hat{\mathbb{Z}}$. An intermediate problem is to describe the absolute Galois group of local fields; there is a partial description of $G_{\mathbb{Q}_p}$. Let $\mathbb{Q}_p^{ur}$ be the maximal unramified extension of $\mathbb{Q}_p$, then $G_{\mathbb{Q}_p^{ur}/\mathbb{Q}_p}$ is naturally isomorphic to $G_{\mathbb{F}_p} \cong \hat{\mathbb{Z}}$ via Frobenius elements. Define the *inertia subgroup* of $G_{\mathbb{Q}_p}$ to be the kernel of the natural homomorphism $G_{\mathbb{Q}_p} \to G_{\mathbb{F}_p}$, it is denoted by I_p . The subgroup I_p has a normal pro-p-Sylow subgroup W_p called the *wild inertia subgroup*, this corresponds to the extension $\overline{\mathbb{Q}_p}/\mathbb{Q}_p^{tm}$ where $\mathbb{Q}_p^{tm}$ is the maximal tamely ramified extension of $\mathbb{Q}_p$. The quotient group I_p/W_p is known as the *tame inertia group* and it is posible to give an isomorphism

$$I_p/W_p \cong \prod_{\ell \neq p} \mathbb{Z}_\ell \tag{1.0.1}$$

which depends non-canonically on a choice of roots of unity. We proceed as follows:

By definition $\mathbb{Q}_p^{tm} = \prod_{K/\mathbb{Q}_p} K$ where K runs over all finite tamely ramified Galois extensions of $\mathbb{Q}_p$. For each such K, let $K_u = \mathbb{Q}_p^{ur} \cap K$, hence we have the following tower of fields:

$$\begin{tikzcd}
 & \mathbb{Q}_p^{tm} \arrow[dl, dash] \arrow[dr, dash] & \\
 & & \mathbb{Q}_p^{ur} \arrow[ddl, dash] \\
K \arrow[dr, dash] & & \\
 & K_u \arrow[d, dash] & \\
 & \mathbb{Q}_p &
\end{tikzcd}$$

Since K/K_u is totally ramified, there exists $\pi \in K$ such that $v_K(\pi) = 1$ and $K = K_u[\pi]$. Let $e = [K : K_u]$ be the ramification degree of K over $\mathbb{Q}_p$, take $p^{\frac{1}{e}}$ some e-root of p in $\overline{\mathbb{Q}_p}$. In the splitting field F of $x^e - p$ over K the element $\pi/p^{1/e}$ is a unit, that is

$$v_F\left(\frac{\pi}{p^{1/e}}\right) = 0.$$

Let $g(x)$ be the minimal polynomial of $\pi/(p^{1/e})$ over K, then $g(x) \in \mathcal{O}_K[x]$, the degree of $g(x)$ divides e so is relative prime to p, therefore its reduction modulo λ_K is a separable polynomial over k_K. Thus $\pi/(p^{1/e}) \in \mathbb{Q}_p^{ur}$. This proves that

$$\mathbb{Q}_p^{tm} = \mathbb{Q}_p^{ur}(p^{1/e} : \ e \text{ prime to } p). \tag{1.0.2}$$

Fix a system of primitive e-th roots of unity (μ_e) for e prime to p. Define $K_e := \mathbb{Q}_p^{ur}(p^{1/e})$ and note that

$$G_{K_e/\mathbb{Q}_p^{ur}} \cong \mathbb{Z}/e\mathbb{Z} \tag{1.0.3}$$

via the system of roots (μ_e), the group $G_{K_e/\mathbb{Q}_p^{ur}}$ is generated by the automorphism $p^{1/e} \mapsto \mu_e p^{1/e}$. Therefore (1.0.2) and (1.0.3) imply

$$I_p/W_p = \varprojlim G_{K_e/\mathbb{Q}_p^{ur}} \cong \prod_{\ell \neq p} \mathbb{Z}_\ell.$$

The natural inclusions $\mathbb{Q} \to \mathbb{Q}_p \to \overline{\mathbb{Q}_p}$ extend to

$$\overline{\mathbb{Q}} \longrightarrow \overline{\mathbb{Q}_p}.$$

Nevertheless, the inclusion is not uniquely specified, with two of them differing by an element in $G_{\mathbb{Q}}$. Thus we have a family of conjugated subgroups

$$G_{\mathbb{Q}_p} \longrightarrow G_{\mathbb{Q}}.$$

We call $G_{\mathbb{Q}_p}$ the *decomposition group at p*. Let $K/\mathbb{Q}$ be a Galois extension, we say that K is *unramified at* p if I_p maps to 1 via $I_p \to G_{\mathbb{Q}_p} \to G_{\mathbb{Q}} \to G_{K/\mathbb{Q}}$, K is *tamely ramified at* p if W_p is mapped to 1. If our extension is unramified at p then we get a well defined conjugacy class of Frobenius elements via the maps $G_{\mathbb{Q}_p} \to G_{K/\mathbb{Q}}$.

Now we are mainly concerned in two sort of Galois groups, the absolute Galois group of p-adic local fields and Galois groups of extensions of $\mathbb{Q}$ with restrictions on ramification. Let S be a finite set of primes of $\mathbb{Q}$ containing the prime at infinity and let $\mathbb{Q}_S$ be the maximal unramified extension of $\mathbb{Q}$ outside S. This is a Galois extension and its Galois group is denoted by $G_{\mathbb{Q},S}$, its open subgroups can be describe in a similar way; let K be a number field contained in $\mathbb{Q}_S$ and S_1 be the set of primes of K lying over the primes of S (including the primes at infinity) and let K_{S_1} be the maximal extension of K unramified outside S_1, then $K_{S_1} = \mathbb{Q}_S$ and $G_{K,S_1}= G_{K_{S_1}/K}$ is a open subgroup of $G_{\mathbb{Q},S}$. Conversely, given a open subgroup H of $G_{\mathbb{Q},S}$ consider $K = \mathbb{Q}_S^H$ its fixed field and let S_1 be the set primes of K lying over S, then $H = G_{K,S_1}$.

The following theorems will motivate an important definition for profinite groups stated below

Theorem 1.0.1. *Let K be a number field and let S be a finite set of primes of K. Then there exist only finitely many extensions L/K of given degree n which are unramified outside S*

Proof. See section III.2 of [Neu99] □

Theorem 1.0.2. *If F is a finite extension of $\mathbb{Q}_p$, then G_F is topologically finitely generated.*

Theorems 1.0.1 and 1.0.2 imply the following result

Proposition 1.0.1. *Let Π be equal to G_F where $F/\mathbb{Q}_p$ is a finite extension or $G_{K,S}$ for K a number field and S a finite set of primes of K including the primes at infinity. Then for every prime p and every open subgroup $\Pi_0 \subseteq \Pi$ of Π, there are only finitely many continuous homomorphisms $\Pi_0 \longrightarrow \mathbb{Z}/p\mathbb{Z}$.*

Proof. If $\Pi = G_F$, denote by F' the fixed field of Π_0, then $\Pi_0 = G_{F'}$ is topologically finitely generated and it is clear that $\mathrm{Hom}(\Pi_0, \mathbb{Z}/p\mathbb{Z})$ is finite. On the other hand, if $\Pi = G_{K,S}$ let K' be the fixed field of Π_0 and S' be the set of primes of K' above S, thus $\Pi_0 = G_{K',S'}$. The non trivial elements of $\mathrm{Hom}(\Pi_0, \mathbb{Z}/p\mathbb{Z})$ are in correspondence with Galois extensions of K' of degree p, so Theorem 1.0.1 implies that there are only finitely many on them. □

Previuos proposition motivates the following definition

Proposition 1.0.2 (Φ_p-finiteness condition)**.** *Let Π be a profinite group and p a prime number. The following conditions on Π are equivalent*

i. The pro-p-completion of Π is finitely generated.

ii. The abelianization of the pro-p-completion of Π is a finitely generated $\mathbb{Z}_p$-module .

iii. The p-Frattini quotient of Π is finite.

iv. The set of continuous homomorphisms from Π to $\mathbb{F}_p$ is finite.

Definition 1.0.1. If every open subgroup of Π satisfies one of the conditions of the previous proposition, we say that Π satisfies the Φ_p-*finiteness condition*, or simply, the Φ_p condition.

Remark. In the local case it is not necessary all the power of Theorem 1.0.2. The conditions of Proposition 1.0.2 can be checked more easily by a explicit description of such extensions.

Finally, we will end this chapter introducing the notion of Galois representation which, in few words, are continuous representations of Galois groups. We would like to study the representations of the absolute Galois group of $\mathbb{Q}$, nevertheless, this group is quite difficult to work with. We evade this problem using some quotients and subgroups which arise naturally in number theory, these groups are $G_{K,S}$ for K and S as above, and absolute Galois groups of local fields. The condition Φ_p provides a setting where the theory becomes much more manageable as we shall see in next sections.

Definition 1.0.2. Let A be a topological ring and Π be a profinite group. A *representation* of Π over A (of rank n) is a continuous homomorphism

$$\rho : \Pi \longrightarrow \mathrm{GL}_n(A), \tag{1.0.4}$$

equivalently, a representation is given by a continuous action of Π on a free A-module M of rank n.

Definition 1.0.3. A *Galois representation* defined over A, unramified outside S (a finite set of primes of $\mathbb{Q}$ including infinity) is a representation of $G_{\mathbb{Q},S}$ over A. Two representations ρ_1 and ρ_2 are equivalent if there exists a matrix $P \in \mathrm{GL}_n(A)$ such that

$$\rho_2 = P^{-1}\rho_1 P.$$

Galois representations coming from modular forms and elliptic curves will be our main source of examples, indeed, the theory developed in this document is an essential part of the whole machinery required to proof Fermat's last theorem. Representations from elliptic curves and modular forms are defined over p-adic fields, specifically over the valuation ring of the p-adic field, then we may consider reduction modulo the maximal ideal and get a representation over a finite field. We are concern with those representations which are equivalent to ones coming from elliptic curves and modular forms.

The following natural question arises: Let k be a finite field and let $A \longrightarrow k$ be a surjective homomorphism, is it posible to lift a representation from k to A? If so, how could we characterize those liftings? And finally, what can we say about the liftings of modular representations?

An answer to these questions is provided by the theory of deformation of representations introduced by Mazur in [Maz89].

In summary, we will study representations of local Galois groups or finitely ramified Galois groups over some special rings. These rings will be profinite rings, thus we are able to deal with representations in three different ways:

- A continuous homomorphism $\rho : \Pi \longrightarrow \mathrm{GL}_n(A)$.
- A continuous action of Π over a free A-module of rank n.
- A continuous homomorphism $A[[\Pi]] \longrightarrow \mathrm{M}_n(A)$ of A-algebras.

  Here $A[[\Pi]]$ is the completed group algebra defined as

  $$A[[\Pi]] = \varprojlim_{H} A[\Pi/H]$$

  where H runs over all open subgroups of Π.

Chapter 2

The deformation functor

We are not interested in representations of profinite groups over any topological ring, we would prefer to restrict our attention to rings similar to valuations rings of p-adic local fields and their quotients. In order to define the corresponding category of rings, fix a prime number p and let k be a finite field of characteristic p. Let $\mathcal{C}$ be the category whose objects are complete noetherian local rings with residue field k and whose morphisms are homomorphisms of local rings which induce the identity on residual fields. This means that if A and B are objects of $\mathcal{C}$ with maximal ideals m_A and m_B respectively, and $f : A \longrightarrow B$ is a morphism of $\mathcal{C}$ then

$$f^{-1}(\mathfrak{m}_B) = \mathfrak{m}_A,$$

and the following diagram commutes

$$\begin{tikzcd}
A \arrow[rr, "f"] \arrow[dr, "\pi_A"'] & & B \arrow[dl, "\pi_B"] \\
& k &
\end{tikzcd}$$

where π_A and π_B are the projections from A and B onto k respectively. It is immediate to check that these morphisms are continuous in the topology induced by maximal ideals. We call the objects of $\mathcal{C}$ *coefficient rings* and their morphisms *coefficient ring homomorphisms.* Note that k is also an object in $\mathcal{C}$. There are both initial and final objects in $\mathcal{C}$; they are $W(k)$ and k respectively, with $W(k)$ the ring of *Witt vectors* of k [1]. In other words, for every coefficient ring A we have natural coefficient ring homomorphisms $W(k) \longrightarrow A$ and $A \longrightarrow k$. In particular, any coefficient ring has a canonical $W(k)$-algebra structure.

Let Λ be a coefficient ring. Sometimes we do not work with all coefficient rings but with coefficient rings which are Λ-algebras as well. We denote by $\mathcal{C}_\Lambda$ the subcategory of $\mathcal{C}$ consisting of coefficient rings which are Λ-algebras and whose morphisms are coefficient ring homomorphisms which preserve the structure of Λ-algebra. We refer to the objects of $\mathcal{C}_\Lambda$ as Λ-coefficient rings and their morphisms as Λ-algebra homomorphisms. Note that $\mathcal{C}_{W(k)} = \mathcal{C}$.

Let A be a coefficient ring and $\mathfrak{m}_A$ be its maximal ideal. Since A is Noetherian the ideal $\mathfrak{m}_A$ is finitely generated, let's say $\mathfrak{m}_A = \langle x_1, \ldots, x_n \rangle$. Since A is complete we get

$$A \cong \varprojlim_{n \in \mathbb{N}} A/\mathfrak{m}^n. \tag{2.0.1}$$

[1] Witt vectors are defined over more general rings. In the case of k a finite field, $W(k)$ is the valuation ring of the unramified extension of $\mathbb{Q}_p$ associated to k.

The successive quotients $\mathfrak{m}^n/\mathfrak{m}^{n+1}$ are finite dimensional vector spaces over k. Therefore, the quotients in the following sequence are finite

$$A/\mathfrak{m}^n \supseteq \mathfrak{m}/\mathfrak{m}^n \supseteq \mathfrak{m}^2/\mathfrak{m}^n \supseteq \cdots \supseteq \mathfrak{m}^{n-1}/\mathfrak{m}^n,$$

showing that $A/\mathfrak{m}^n$ is finite. Therefore A is a profinite ring.

Let Π be a profinite group satisfying the Φ_p condition and let $\overline{\rho} : \Pi \longrightarrow \mathrm{GL}_n(k)$ be a representation, we say that $\overline{\rho}$ is a *residual representation.* Let $A \longrightarrow B$ be a coefficient ring homomorphism, it induces a group homomorphism

$$\mathrm{GL}_n(A) \longrightarrow \mathrm{GL}_n(B).$$

Let $\Gamma_n(A)$ be the kernel of $\mathrm{GL}_n(A) \longrightarrow \mathrm{GL}_n(k)$.

Definition 2.0.1. Let A be a coefficient ring and $\rho_1, \rho_2 : \Pi \longrightarrow \mathrm{GL}_n(A)$ be representations. We say that ρ_1 and ρ_2 are strictly equivalent if there exists a matrix $M \in \Gamma_n(A)$ such that

$$\rho_2 = M^{-1}\rho_1 M.$$

Definition 2.0.2 (Deformation of a representation)**.** Let A be a coefficient ring and let $\overline{\rho} : \Pi \longrightarrow \mathrm{GL}_n(k)$ be a residual representation. A deformation of $\overline{\rho}$ to A is a strict equivalent class of representations $\{\theta_i : \Pi \longrightarrow \mathrm{GL}_n(A)\}_{i\in I}$ such that θ_i induces $\overline{\rho}$ in k for all $i \in I$, i.e.

$$\overline{\theta_i} = \overline{\rho} \text{ for all } i \in I \tag{2.0.2}$$

where $\overline{\theta_i}$ is the reduction of θ_i to k.

Remark. Two strict equivalent representations over A induce the same residual representation. Hence it is only necessary to check (2.0.2) for one element in the strict equivalent class.

Coefficient ring homomorphisms $A \longrightarrow B$ send strict equivalent representations of A to strict equivalent representations of B. Indeed, the group homomorphism $\mathrm{GL}_n(A) \longrightarrow \mathrm{GL}_n(B)$ gives a group homomorphism

$$\Gamma_n(A) \longrightarrow \Gamma_n(B).$$

Therefore, we may think deformations as a covariant functor in the following way: given a residual representation $\overline{\rho}$ define the *deformation functor* $\mathbf{D}_{\overline{\rho}} : \mathcal{C} \longrightarrow \text{Sets}$ to be the functor defined on objects by

$$\mathbf{D}_{\overline{\rho}} : A \rightsquigarrow \{\text{Deformations of } \overline{\rho} \text{ to } A\}.$$

If we restrict $\mathcal{C}$ to the subcategory $\mathcal{C}_\Lambda$ we write $\mathbf{D}_{\overline{\rho},\Lambda}$ for the restricted functor. If $\overline{\rho}$ is fixed we write for simplicity $\mathbf{D}$ and $\mathbf{D}_\Lambda$ instead $\mathbf{D}_{\overline{\rho}}$ and $\mathbf{D}_{\overline{\rho},\Lambda}$ respectively.

To study the deformation functor in the whole category $\mathcal{C}$ is not practical, luckily it is possible to simplify our setting. Consider the full subcategory $\mathcal{C}_\Lambda^0$ of $\mathcal{C}_\Lambda$ consisting of artinian local Λ-algebras with residue field k.

Lemma 2.0.1. *Every object in $\mathcal{C}_\Lambda$ is a pro-object of $\mathcal{C}_\Lambda^0$.*

Proof. Let A be a coefficient Λ-algebra and $\mathfrak{m}$ be its maximal ideal. Then $A/\mathfrak{m}^k$ is an artinian coefficient Λ-algebra since its maximal ideal is nilpotent. Therefore

$$A \cong \varprojlim_{k\in\mathbb{N}} A/\mathfrak{m}^k$$

proving our claim. □

If $\mathbf{F}$ is a functor from $\mathcal{C}_\Lambda$ to Sets, the sets $\mathbf{F}(A/\mathfrak{m}^k)$ will form a inverse limit of sets. The coefficient ring homomorphisms $A \longrightarrow A/\mathfrak{m}^k$ give compatible functions

$$\mathbf{F}(A) \longrightarrow \mathbf{F}(A/\mathfrak{m}^k).$$

This package of information defines a function

$$\mathbf{F}(A) \longrightarrow \varprojlim_{k\in\mathbb{N}} \mathbf{F}(A/\mathfrak{m}^k).$$

Definition 2.0.3. We say a functor $\mathbf{F} : \mathcal{C}_\Lambda \longrightarrow$ Sets is continuous if the canonical function

$$F(A) \longrightarrow \varprojlim_{k\in\mathbb{N}} \mathbf{F}(A/\mathfrak{m}^k)$$

is a bijection.

Lemma 2.0.2. $\mathbf{D}_\Lambda$ *is a continuous functor.*

Proof. First note that

$$\mathrm{GL}_n(A) = \varprojlim_{k\in\mathbb{N}} \mathrm{GL}_n(A/\mathfrak{m}^k)$$

and

$$\Gamma_n(A) = \varprojlim_{k\in\mathbb{N}} \Gamma_n(A/\mathfrak{m}^k).$$

Furthermore, the maps

$$\mathrm{GL}_n(A/\mathfrak{m}^{k+1}) \longrightarrow \mathrm{GL}_n(A/\mathfrak{m}^k), \quad \Gamma_n(A/\mathfrak{m}^{k+1}) \longrightarrow \Gamma_n(A/\mathfrak{m}^k)$$

are all surjective. The canonical map

$$\mathbf{D}_\Lambda(A) \longrightarrow \varprojlim_{k\in\mathbb{N}} \mathbf{D}_\Lambda(A/\mathfrak{m}^k)$$

maps a deformation ρ of $\overline{\rho}$ to a compatible sequence (ρ_k), where ρ_k is the corresponding deformation to $A/\mathfrak{m}^k$.

We will show that the canonical map is surjective. Let (ρ_k) be a coherent sequence of deformations, for each k choose θ_k a representation in the strict equivalent class ρ_k. Suppose that we have chosen $\theta_1, \dots, \theta_{k-1}$ such that θ_{i+1} reduces to θ_i. Consider the map

$$\pi_k : A/\mathfrak{m}^k \longrightarrow A/\mathfrak{m}^{k-1},$$

then $\pi_k \circ \theta_k$ and θ_{k-1} are strictly equivalent and there is a matrix $\overline{P} \in \Gamma_n(A/\mathfrak{m}^{k-1})$ such that

$$\theta_{k-1} = \overline{P}^{-1} \pi_k \circ \theta_k \overline{P}.$$

Take P a lifting of $\overline{P}$ to $\Gamma_n(A/\mathfrak{m}^k)$ and replace θ_k by $\theta'_k = P^{-1}\theta_k P$. Then θ'_k is in the same class of θ_k and reduces to θ_{k-1}. Therefore we get a compatible sequence of representations (θ_k) which represents the sequence of deformations (ρ_k). Take θ as the inverse limit of (θ_k) and define ρ to be the strict equivalent class of θ, so ρ is the desired element.

To prove injectivity choose two deformations ρ, ρ' such that $(\rho_k) = (\rho'_k)$. Take θ and θ' elements of ρ and ρ' respectively, we want to show that θ and θ' are strict equivalent. Let θ_k, θ'_k be the representations θ, θ' modulo $\mathfrak{m}^k$ respectively. So $\theta_1 = \theta'_1 = \overline{\rho}$. Suppose we have a coherent set of matrices $P_i \in \Gamma_n(A/\mathfrak{m}^i)$ for $i = 1, \dots, k-1$ such that

$$\theta_i = P_i^{-1}\theta_i' P_i \quad (1 \leq i \leq k-1).$$

We would like to take a lifting P_k of P_{k-1} to $\Gamma_n(A/\mathfrak{m}^k)$ such that $\theta_k = P_k^{-1}\theta_k' P_k$, then we could take P as the inverse limit of (P_k) and we are done. However, we need to guarantee that such matrix exists. Let $\mathcal{P}_k$ be the set of those matrices Q in $\Gamma_n(A/\mathfrak{m}^k)$ such that

$$\theta_k = Q^{-1}\theta_k' Q.$$

The homomorphisms $\Gamma_n(A/\mathfrak{m}^k) \longrightarrow \Gamma_n(A/\mathfrak{m}^{k-1})$ restricts to a map $\mathcal{P}_k \longrightarrow \mathcal{P}_{k-1}$. An important fact is that the sets $\mathcal{P}_k$ are all finite and non empty. These two conditions imply that

$$\mathcal{P} = \varprojlim_{k\in\mathbb{N}} \mathcal{P}_k \subset \Gamma_n(A)$$

is non empty. Then for $P \in \mathcal{P}$ we get

$$\theta = P^{-1}\theta' P$$

and our canonical map is injective. □

With the previous lemma in our hands, we now can restrict the study of deformations to artinian coefficient Λ-algebras and recover the whole theory via inverse limits. An important property of coefficient Λ-algebras is that they are quotients of power series over Λ as we will in upcoming sections.

Chapter 3

Criteria of representability

A question which Mazur solved in [Maz89] using techniques of Schelssinger exposed in [Sch68], is whether the deformation functor $\mathbf{D} = \mathbf{D}_{\overline{\rho}}$ is representable. We shall tackle this issue in next chapter. For now, we need some preliminaries: fix a residual representation $\overline{\rho}$ and suppose that the deformation functor is representable, so there exists a coefficient ring $\mathcal{R} = \mathcal{R}_{\overline{\rho}}$ and a natural equivalence of functors

$$\Phi : \mathbf{D} \longrightarrow \mathrm{Hom}(\mathcal{R}, \,\cdot\,),$$

i.e. compatible bijections

$$\mathbf{D}(A) \xrightarrow{\Phi(A)} \mathrm{Hom}(\mathcal{R}, A)$$

for every coefficient ring A. In particular, taking $A = \mathcal{R}$ we get a bijection

$$\mathbf{D}(\mathcal{R}) \xrightarrow{\Phi(\mathcal{R})} \mathrm{Hom}(\mathcal{R}, \mathcal{R}),$$

the identity corresponds to a unique deformation $\boldsymbol{\rho} \in \mathbf{D}(\mathcal{R})$. This deformation has the following property: for any deformation $\rho : \Pi \longrightarrow \mathrm{GL}_n(A)$ there exists a unique coefficient ring homomorphism $\varphi : \mathcal{R} \longrightarrow A$ such that $\rho = \varphi \circ \boldsymbol{\rho}$. We call $\boldsymbol{\rho}$ the *universal deformation* of $\overline{\rho}$, and $\mathcal{R}_{\overline{\rho}}$ the *universal deformation ring*.

If $\mathbf{D}$ is representable what can we say about $\mathbf{D}_\Lambda$? The answer is simple provide we know how to construct complete tensor products. If $\mathcal{R}$ represents $\mathbf{D}$ then $\mathcal{R}\hat{\otimes}_{W(k)}\Lambda$ represents $\mathbf{D}_\Lambda$. For the definition of complete tensor products see Appendix A.

3.1 Fiber products

Let $\mathcal{S}$ be a category, let A, B, C be objects of $\mathcal{S}$ and let $\alpha : A \longrightarrow C$, $\beta : B \longrightarrow C$ be morphisms.

$$\begin{tikzcd} A \arrow[dr, "\alpha"'] & & B \arrow[dl, "\beta"] \\ & C & \end{tikzcd}$$

The *fiber product* of A and B over C is a tuple $(A \times_C B, p, q)$ where $p : A \times_C B \longrightarrow A$, $q : A \times_C B \longrightarrow B$ are morphisms of $\mathcal{S}$ such that: $\alpha \circ p = \beta \circ q$, and for every triple (D, f, g)

$$f : D \longrightarrow A, \quad g : D \longrightarrow B$$

such that $\alpha \circ f = \beta \circ g$ we have a unique morphism $h : D \longrightarrow A \times_C B$ which makes commutative the following diagram

$$\begin{tikzcd}
& D \arrow[ddl, bend right, "f"'] \arrow[d, dotted, "h"] \arrow[ddr, bend left, "g"] & \\
& A \times_C B \arrow[dl, "p"'] \arrow[dr, "q"] & \\
A \arrow[dr, "\alpha"'] & & B \arrow[dl, "\beta"] \\
& C &
\end{tikzcd}$$

Proposition 3.1.1. *Fiber products exist in* $\mathcal{C}_\Lambda^0$.

Proof. Define

$$A \times_C B = \{(a, b) \in A \times B : \alpha(a) = \beta(b)\}.$$

Consider $\mathfrak{m} = \{(a, b) \in A \times_C B \ : \ a \in \mathfrak{m}_A \text{ and } b \in \mathfrak{m}_B\}$. Since A and B have finite length as Λ-module then so $A \times B$ and $A \times_C B$. This proves that $A \times_C B$ is artinian. Clearly $\mathfrak{m}$ is the unique maximal ideal of $A \times_C B$ and its quotient is k. □

Remark. The ring-theoretical fiber product of objects in $\mathcal{C}$ is probably not Noetherian, for instance taking $A = k[[X, Y]]$, $B = k$, $C = k[[X]]$ with $\alpha : A \longrightarrow C$ the map sending Y to 0, and $\beta : B \longrightarrow C$ the inclution. Then

$$A \times_C B = k + Yk[[X, Y]]$$

is not Noetherian.

A representable functor preserves fiber products. Moreover, a representable functor preserves finite limits. A necessary and sufficient condition for a functor to preserve finite limits is to preserve equalizers, and finite products. The reason is because every finite limite can be built recursively by finite products and equalizers.

Let $\mathbf{F} : \mathcal{S} \longrightarrow$ Sets be a set-valued functor. We have the following commutative square

$$\begin{tikzcd}
& \mathbf{F}(A \times_C B) \arrow[dl, "\mathbf{F}(p)"'] \arrow[dr, "\mathbf{F}(q)"] & \\
\mathbf{F}(A) \arrow[dr, "\mathbf{F}(\alpha)"'] & & \mathbf{F}(B) \arrow[dl, "\mathbf{F}(\beta)"] \\
& \mathbf{F}(C) &
\end{tikzcd}$$

By the universal property of fibre products we have a natural function

$$\mathbf{F}(A \times_C B) \longrightarrow \mathbf{F}(A) \times_{\mathbf{F}(C)} \mathbf{F}(B).$$

If this function is a bijection for every fibre product we say that $\mathbf{F}$ satisfies the *Mayer-Vietoris* property.

We return to our category $\mathcal{C}$. Suppose $\mathbf{F}$ is a continuous set-valued functor on $\mathcal{C}$. Then $\mathbf{F}$ is representable if and only if there exists a coefficient ring $\mathcal{R}$ such that for all object A in $\mathcal{C}^0$ we have

$$\text{Hom}(\mathcal{R}, A) = \mathbf{F}(A),$$

this is because objects of $\mathcal{C}$ are pro-objects of $\mathcal{C}^0$. If this condition holds we say that $\mathbf{F}$ is *pro-representable.*

There are two reasons to deal only with the subcategory $\mathcal{C}^0$. First, we can use inductive arguments in the length of the ring as a $W(k)$-algebra. Second, we cannot guarantee the existence of fiber products in $\mathcal{C}$.

The reason why we introduced fiber products is that they provide a criteria which is close to be a sufficient condition for representability. The appropiate theorem is due to Grothendieck:

Theorem 3.1.1 (Grothendieck)**.** *Let*

$$\mathbf{F} : \mathcal{C}^0_\Lambda \longrightarrow \mathit{Sets}$$

be a covariant functor such that $\mathbf{F}(k)$ *is a singleton. Then* $\mathbf{F}$ *is pro-representable if and only if*

i. $\mathbf{F}$ *satisfies the Mayer-Vietoris property.*

ii. $\mathbf{F}(k[\epsilon])$ *is a finite dimensional vector space.*

The ring $k[\epsilon]$ is by definition $k[[X]]/(X^2)$ whit $\epsilon = X(\mod X^2)$. We call it the *ring of dual numbers.*

See [Gro60] for the original and more general proof of Grothendieck and Appendix B for a down to earth proof following the above reference.

3.2 Tangent Space

Through this section we fix a coefficient ring Λ. A shall denote an element in $\mathcal{C}_\Lambda$ usually an artinan coefficient Λ-algebra, $\mathfrak{m}_A$ will be used for its maximal ideal.

As in the case of local rings, some set valued functors of $\mathcal{C}_\Lambda$ have an associated tangent space, both definitions agree when the functor is representable.

Definition 3.2.1. Let A be a coefficient Λ-algebra. The Zariski cotangent space t^*_A of A is the quotient

$$t_A* = \mathfrak{m}_A/\langle \mathfrak{m}_A^2, \mathfrak{m}_\Lambda\rangle.$$

The Zariski tangent space t_A is

$$t_A = \mathrm{Hom}_k(t^*_A, k) = \mathrm{Hom}_k(\mathfrak{m}_A/\langle \mathfrak{m}_A^2, \mathfrak{m}_\Lambda\rangle, k).$$

Since $\mathfrak{m}_A$ is finitely generated over A, t^*_A is a finite dimensional vector space. Let $f : A \longrightarrow B$ be a coefficient ring homomorphism, f induces a k-linear map $f_* : t^*_A \longrightarrow t^*_B$.

Proposition 3.2.1. *f is surjective if and only if f_* is surjective.*

Proof. If f is surjective clearly f_* is surjective. Conversely, suppose f_* is surjective. Consider the following diagram with exact rows

$$\begin{tikzcd}
0 \arrow[r] & \mathfrak{m}_\Lambda A/(\mathfrak{m}_\Lambda A \cap \mathfrak{m}_A^2) \arrow[r] \arrow[d] & \mathfrak{m}_A/\mathfrak{m}_A^2 \arrow[r] \arrow[d] & t^*_A \arrow[r] \arrow[d] & 0 \\
0 \arrow[r] & \mathfrak{m}_\Lambda B/(\mathfrak{m}_\Lambda B \cap \mathfrak{m}_B^2) \arrow[r] & \mathfrak{m}_B/\mathfrak{m}_B^2 \arrow[r] & t^*_B \arrow[r] & 0
\end{tikzcd}$$

Since $\mathfrak{m}_\Lambda/\mathfrak{m}_\Lambda^2 \longrightarrow \mathfrak{m}_\Lambda A/(\mathfrak{m}_\Lambda A \cap \mathfrak{m}_A^2)$ is surjective, the left column in the diagram is surjective. Therefore, $\mathfrak{m}_A/\mathfrak{m}_A^2 \longrightarrow \mathfrak{m}_B/\mathfrak{m}_B^2$ is surjective. This gives a surjection on the associated graded rings and Lemma 10.23 of [AM69, Ch. 10] implies that f is a surjection.

□

Corollary 3.2.1.1. *Every coefficient Λ-algebra is a quotient of a ring of power series over Λ.*

Proof. Take $\{x_1, \dots, x_l\}$ to be generators of $\mathfrak{m}_A$. Consider $R = \Lambda[[X_1, \dots, X_l]]$ and send $X_i \mapsto x_i$. □

Lemma 3.2.1. *Let A be a coefficient Λ-algebra. There are a natural bijections*

$$\mathrm{Hom}_k(\mathfrak{m}_A/\langle \mathfrak{m}_A^2, \mathfrak{m}_\Lambda\rangle, k) \cong \mathrm{Hom}_\Lambda(A, k[\epsilon]) \cong \mathrm{Der}_\Lambda(A, k).$$

Here $\mathrm{Der}_\Lambda(A, k)$ *denotes the set of Λ-derivations with values in k.*

Proof. First we are going to prove $\mathrm{Hom}_\Lambda(A, k[\epsilon]) \cong \mathrm{Der}_\Lambda(A, k)$. Let $\varphi : A \longrightarrow k[\epsilon]$ be a Λ-algebra homomorphism. Let $a, b \in A$ and $\overline{a}, \overline{b}$ be their reduction mod $\mathfrak{m}_A$ respectively. Denote by $\tilde{\varphi}(a)$ the element of k such that

$$\varphi(a) = \overline{a} + \epsilon\tilde{\varphi}(a).$$

Additivity of φ implies additivity of $\tilde{\varphi}$. Let $\lambda \in \Lambda$, then

$$\lambda(\overline{a} + \epsilon\tilde{\varphi}(a)) = \varphi(\lambda a) = \overline{\lambda a} + \epsilon\tilde{\varphi}(\lambda a). \tag{3.2.1}$$

Hence $\tilde{\varphi}$ is Λ-linear. Moreover,

$$\begin{array}{rcl} \varphi(ab) & = & \varphi(a)\varphi(b) \\ \overline{ab} + \epsilon\tilde{\varphi}(ab) & = & (\overline{a} + \epsilon\tilde{\varphi}(a))(\overline{b} + \epsilon\tilde{\varphi}(b)) \\ \overline{ab} + \epsilon\widetilde{\varphi}(ab) & = & \overline{ab} + \epsilon(\widetilde{\varphi}(a)\overline{b} + \overline{a}\widetilde{\varphi}(b)) \end{array}$$

implies

$$\widetilde{\varphi}(ab) = \widetilde{\varphi}(a)\overline{b} + \overline{a}\widetilde{\varphi}(b). \tag{3.2.2}$$

Therefore $\widetilde{\varphi}$ is a Λ-derivation. Conversely, if $\widetilde{\varphi}$ is a Λ-derivation define

$$\varphi := \pi + \epsilon\widetilde{\varphi}$$

where $\pi : A \longrightarrow k$ is the canonical projection. The above equations shows that φ is a coefficient ring homomorphism.

Now we are going to show $\mathrm{Der}_\Lambda(A, k) \cong t_A$. Let $\widetilde{\varphi}$ be a Λ-derivation, consider the restriction of $\widetilde{\varphi}$ to $\mathfrak{m}_A$. Equation (3.2.2) shows that $\mathfrak{m}_A^2$ is annihilated by $\widetilde{\varphi}$. Note that $\widetilde{\varphi}$ also annihilates $\mathfrak{m}_\Lambda$ because it is a Λ-derivation. So $\widetilde{\varphi}$ defines a k-linear function

$$\hat{\varphi} : \mathfrak{m}_A/\langle \mathfrak{m}_A^2, \mathfrak{m}_\Lambda\rangle \longrightarrow k.$$

Conversely, let $\hat{\varphi} : \mathfrak{m}_A/\langle \mathfrak{m}_A^2, \mathfrak{m}_\Lambda\rangle \longrightarrow k$ be an element in the tangent space and write its extension to $\mathfrak{m}_A$ identically. Let $a \in A$ and $\lambda \in \Lambda$ such that $\overline{a} = \overline{\lambda}$ in k. Define $\widetilde{\varphi}(a) := \hat{\varphi}(a - \lambda)$. Note that $\tilde{\varphi}$ does not depend on λ. Indeed, if λ' is such that $\overline{\lambda} = \overline{\lambda'}$ then $\hat{\varphi}(a - \lambda') = \hat{\varphi}(a - \lambda + \lambda - \lambda') = \hat{\varphi}(a - \lambda)$. Let $\omega \in \Lambda$ such that $\overline{\omega} = \overline{b}$, then

$$\begin{array}{rcl} \widetilde{\varphi}(ab) & = & \hat{\varphi}(ab - \lambda\omega) \\ & = & \hat{\varphi}((a - \lambda)b + \lambda(b - \omega)) \\ & = & \hat{\varphi}((a - \lambda)b) + \overline{\lambda}\hat{\varphi}(b - \omega) \\ & = & \hat{\varphi}((a - \lambda)\omega + (a - \lambda)(b - \omega)) + \overline{\lambda}\hat{\varphi}(b - \omega) \\ & = & \hat{\varphi}(a - \lambda)\overline{\omega} + \overline{a}\hat{\varphi}(b - \omega) \\ & = & \hat{\varphi}(a - \lambda)\overline{b} + \overline{a}\hat{\varphi}(b - \omega) \\ & = & \widetilde{\varphi}(a)\overline{b} + \overline{a}\widetilde{\varphi}(b). \end{array}$$

We also get

$$\begin{aligned}
\widetilde{\varphi}(\omega a) &= \hat{\varphi}(\omega a - \omega\lambda) \\
&= \hat{\varphi}(\omega(a-\lambda)) \\
&= \overline{\omega}\hat{\varphi}(a-\lambda) \\
&= \overline{\omega}\widetilde{\varphi}(a).
\end{aligned}$$

This proves that $\widetilde{\varphi}$ is a Λ-derivation.

□

Remark. All bijections described above are actually isomorphisms of vector spaces, but is necessary to endow $\mathrm{Hom}_\Lambda(A, k[\epsilon])$ with a canonical vector space structure.

We end this section endowing $\mathrm{Hom}_\Lambda(A, k[\epsilon])$ with a vector space structure. Indeed, we will define more generally the tangent space for functors $\mathbf{F}$ satisfying two additional properties. Then, we shall give a vector space structure to $\mathbf{F}(k[\epsilon])$.

Let $\mathbf{F}$ be a functor such that $\mathbf{F}(k)$ has only one element (note that deformation functors salisfy this property). We know that finite products exist in $\mathcal{C}^0_\Lambda$, indeed, the product of A and B is $A \times_k B$. Taking $k[\epsilon] = A = B$ we get a canonical function

$$\mathbf{F}(k[\epsilon] \times_k k[\epsilon]) \longrightarrow \mathbf{F}(k[\epsilon]) \times \mathbf{F}(k[\epsilon]). \tag{3.2.3}$$

Suppose this function is a bijection[1]. For $\alpha \in k$ consider

$$\widetilde{\alpha} : k[\epsilon] \longrightarrow k[\epsilon], \quad a + \epsilon b \mapsto a + \epsilon\alpha b.$$

and

$$\mathfrak{p} : k[\epsilon] \times_k k[\epsilon] \longrightarrow k[\epsilon], \quad (a + \epsilon b_1, a + \epsilon b_2) \mapsto a + \epsilon(b_1 + b_2).$$

A straightforward computation shows that $\tilde{\alpha}$ and $\mathfrak{p}$ are coefficient ring homomorphisms, even coefficient Λ-algebra homomorphisms. In particular, note that $\tilde{0}$ is the composition

$$k[\epsilon] \longrightarrow k \longrightarrow k[\epsilon].$$

The following commutative diagrams show that, as long as (3.2.3) is a bijection, $\mathbf{F}(k[\epsilon])$ has a vector space structure. Let $\mathfrak{s} : k[\epsilon] \times_k k[\epsilon] \longrightarrow k[\epsilon] \times_k k[\epsilon]$ be the "switching" map, i.e the map which permutes both components. Let $i_j : k[\epsilon] \longrightarrow k[\epsilon] \times_k k[\epsilon]$ be the inclusion in the j-th component.

$$\begin{tikzcd}
k[\epsilon] \arrow[rr, "\widetilde{\beta}"] \arrow[dr, "\widetilde{\alpha\beta}"'] & & k[\epsilon] \arrow[dl, "\widetilde{\alpha}"] \\
& k[\epsilon] &
\end{tikzcd}
\qquad
\begin{tikzcd}
k[\epsilon] \arrow[rr, "\widetilde{1}"] \arrow[dr, "id"'] & & k[\epsilon] \arrow[dl, "id"] \\
& k[\epsilon] &
\end{tikzcd}$$

$$\begin{tikzcd}
k[\epsilon] \times_k k[\epsilon] \arrow[d, "\mathfrak{s}"'] \arrow[dr, "\mathfrak{p}"] & \\
k[\epsilon] \times_k k[\epsilon] \arrow[r, "\mathfrak{p}"] & k[\epsilon]
\end{tikzcd}
\qquad
\begin{tikzcd}
k[\epsilon] \times_k k[\epsilon] \times_k k[\epsilon] \arrow[r, "\mathfrak{p} \times_k id"] \arrow[d, "id \times_k \mathfrak{p}"'] & k[\epsilon] \times_k k[\epsilon] \arrow[d, "\mathfrak{p}"] \\
k[\epsilon] \times_k k[\epsilon] \arrow[r, "\mathfrak{p}"] & k[\epsilon]
\end{tikzcd}$$

$$\begin{tikzcd}
k[\epsilon] \arrow[r, "id"] \arrow[d, "i_1"'] & k[\epsilon] \\
k[\epsilon] \times_k k[\epsilon] \arrow[r, "id \times_k \tilde{0}"] & k[\epsilon] \times_k k[\epsilon] \arrow[u, "\mathfrak{p}"']
\end{tikzcd}
\qquad
\begin{tikzcd}
k[\epsilon] \times_k k[\epsilon] \arrow[r] \arrow[d, "\widetilde{-1} \times_k id"'] & k \arrow[d] \\
k[\epsilon] \times_k k[\epsilon] \arrow[r, "\mathfrak{p}"] & k[\epsilon]
\end{tikzcd}$$

[1] This condition is usually named as the *tangent space hypothesis*.

$$\begin{tikzcd}
k[\epsilon] \times_k k[\epsilon] \arrow[r, "\widetilde{\alpha}\times_k\widetilde{\alpha}"] \arrow[d, "\mathfrak{p}"'] & k[\epsilon] \times_k k[\epsilon] \arrow[d, "\mathfrak{p}"] \\
k[\epsilon] \arrow[r, "\widetilde{\alpha}"] & k[\epsilon]
\end{tikzcd}$$

$$\begin{tikzcd}
k[\epsilon] \arrow[r, "\widetilde{\alpha+\beta}"] \arrow[d, "\Delta"'] & k[\epsilon] \\
k[\epsilon] \times_k k[\epsilon] \arrow[r, "\widetilde{\alpha}\times_k\widetilde{\beta}"] & k[\epsilon] \times_k k[\epsilon] \arrow[u, "\mathfrak{p}"']
\end{tikzcd}$$

Definition 3.2.2. Let $\mathbf{F} : \mathcal{C}^0_\Lambda \longrightarrow$ Sets be a covariant functor such that $\mathbf{F}(k)$ is a singleton and (3.2.3) is a bijection. The tangent space of $\mathbf{F}$ is the vector space $\mathbf{F}(k[\epsilon])$ and is denoted by $t_{\mathbf{F}}$.

Chapter 4

Representability of deformation functors

The plan for this chapter is to show that the deformation functor is representable under certain hypothesis on the residual representation $\overline{\rho}$. Grothendieck's Theorem is a possible but inefficient path, the main reason is that to check exactness for an arbitrary Mayer-Vietoris diagram of artinian rings is quite general and wild. We need a weaker criteria for representability (or pro-rerpesentability) in our category $\mathcal{C}^0_\Lambda$, and Schlessinger's Criteria fits perfectly in this framework.

4.1 Schlessinger's Theorem

We shall introduce some terminology in order to state the theorem, see [Sch68] for Schlessinger's original article where the proofs of the theorems in this section can be found.

We say that a coefficient ring homomorphism $p : A \longrightarrow B$ is *small* if it is surjective, $\ker p = \langle f \rangle$ with $\mathfrak{m}_A f = 0$ and $f \neq 0$. Every surjective coefficient ring homomorphism can be factorized in finitely many small homomorphisms.

Let $\mathbf{F} : \mathcal{C}^0_\Lambda \longrightarrow \text{Sets}$ be a covariant functor such that $\mathbf{F}(k)$ is a singleton. Let A_0, A_1, A_2 be artinian coefficient Λ-algebras and suppose we have coefficient ring homomorphisms

$$\begin{tikzcd}
A_1 \arrow[dr] & & A_2 \arrow[dl] \\
& A_0 &
\end{tikzcd} \tag{4.1.1}$$

Let $A_3 = A_1 \times_{A_0} A_2$ be their fiber product. We get a canonical map

$$\mathbf{F}(A_3) \longrightarrow \mathbf{F}(A_1) \times_{\mathbf{F}(A_0)} \mathbf{F}(A_2). \tag{4.1.2}$$

We define the following properties for the functor $\mathbf{F}$.

H1: If the map $A_2 \longrightarrow A_0$ is small, then (4.1.2) is surjective.

H2: If $A_0 = k$ and $A_2 = k[\epsilon]$, then (4.1.2) is bijective.

Remark. If **H**2 holds, take $A_1 = k[\epsilon]$. Then

$$\mathbf{F}(k[\epsilon] \times_k k[\epsilon]) \longrightarrow \mathbf{F}(k[\epsilon])_{\mathbf{F}(k)}\mathbf{F}(k[\epsilon])$$

is a bijection and we are able to define a vector space structure in $\mathbf{F}(k[\epsilon])$. We refer to the existence of this particular bijection as the *vector space hypothesis.*

H3: The vector space $t_{\mathbf{F}} = \mathbf{F}(k[\epsilon])$ is finite dimensional.

H4: If $A_1 = A_2$, $A_i \longrightarrow A_0$ are the same, and $A_i \longrightarrow A_0$ are small, then (4.1.2) is bijective.

Definition 4.1.1. A morphism of functors $\mathbf{F} \longrightarrow \mathbf{G}$ is *smooth* if for every surjective homomorphism $A \longrightarrow B$, the function

$$\mathbf{F}(A) \longrightarrow \mathbf{F}(B) \times_{\mathbf{G}(B)} \mathbf{G}(A)$$

is surjective.

Definition 4.1.2. Let R be a coefficient Λ-algebra. A *Hull* of $\mathbf{F}$ is a natural transformation $\vartheta : \mathrm{Hom}(R, \cdot\,) \longrightarrow \mathbf{F}$ such that ϑ is smooth and $\vartheta(k[\epsilon])$ is a bijection.

Yoneda's lemma implies that ϑ depends only on the image of the identity of R (if we extend the functor continuously to all $\mathcal{C}_\Lambda$)[1], call this element $\xi \in \hat{\mathbf{F}}(R)$. We also say that (R, ξ) is a *hull* of $\mathbf{F}$. A hull of a functor is unique in the following sense:

Theorem 4.1.1. *Let (R, ξ) and (R', ξ') be hulls of $\mathbf{F}$. Then there exists a (no canonical) isomorphism $u : R \longrightarrow R'$ such that $\hat{\mathbf{F}}(u)(\xi) = \xi'$.*

Theorem 4.1.2 (Schlessinger's Criteria)**.** *Let $\mathbf{F} : \mathcal{C}_\Lambda^0 \longrightarrow$ Sets be a covariant functor such that $\mathbf{F}(k)$ is a singleton. Then $\mathbf{F}$ has a hull if and only if the properties* **H**1*,* **H**2 *and* **H**3 *holds.*

Moreover, $\mathbf{F}$ is pro-representable if and only if in addition property **H**4 *holds.*

We usually will impose properties on the deformation functor so we are going to deal with subfunctors of $\mathbf{D}_{\overline{\rho}}$. We would like to know when such subfunctors are pro-representable. The next proposition is useful for that purpose

Proposition 4.1.1. *Let $\mathbf{F} : \mathcal{C}_\Lambda^0 \longrightarrow$ Sets be a set-valued covariant functor. Let $\mathbf{F}_1$ be a subfunctor of $\mathbf{F}$ such that $\mathbf{F}_1(k) = \mathbf{F}(k)$ is a singleton and suppose $\mathbf{F}$ is pro-representable. If $\mathbf{F}_1$ satisfies condition* **H**1*, then it satisfies the other three conditions, and therefore it is also pro-representable.*

We can also prove that the ring which pro-represents $\mathbf{F}_1$ is a quotient of the ring which represents $\mathbf{F}$. In [Maz97] Mazur suggests another approach to face this issue, we need one bit of language: in any category, we say that a diagram

$$\begin{tikzcd} & D \arrow[dl] \arrow[dr] & \\ A \arrow[dr, "\alpha"'] & & B \arrow[dl, "\beta"] \\ & C & \end{tikzcd}$$

is *cartesian* if the induced map $D \longrightarrow A \times_C B$ is an isomorphism. Now suppose $\mathbf{F}_1$ is a subfunctor of $\mathbf{F}$ such that $\mathbf{F}_1(k) = \mathbf{F}(k)$ is a singleton. Given a diagram in $\mathcal{C}_\Lambda^0$

$$\begin{tikzcd} A \arrow[dr, "\alpha"'] & & B \arrow[dl, "\beta"] \\ & C & \end{tikzcd}$$

consider the square

[1] Denote the extended functor by $\hat{\mathbf{F}}$.

$$\begin{tikzcd}
\mathbf{F}_1(A \times_C B) \arrow[r] \arrow[d] & \mathbf{F}_1(A) \times_{\mathbf{F}_1(C)} \mathbf{F}_1(B) \arrow[d] \\
\mathbf{F}(A \times_C B) \arrow[r] & \mathbf{F}(A) \times_{\mathbf{F}(C)} \mathbf{F}(B)
\end{tikzcd}$$

If every such diagram is cartesian, we say that $\mathbf{F}_1 \subset \mathbf{F}$ is *relatively representable.*

Proposition 4.1.2. *If* $\mathbf{F}_1 \subset \mathbf{F}$ *is relatively representable, then, for each* i, $\mathbf{F}_1$ *satisfies* $\mathbf{H}i$ *if* $\mathbf{F}$ *does. The analogous result holds for the tangent space hypothesis.*

4.2 Absolutely irreducible representations

The existence theorem of the universal ring proved by Mazur in [Maz97] holds for absolutely irreducible representations, so it is important to give conditions for a representation to be absolutely irreducible. Let $\overline{\rho} : \Pi \longrightarrow \mathrm{GL}_n(k)$ be a residual representation and let $C(\overline{\rho})$ be the center of $\overline{\rho}$ in $\mathrm{M}_n(k)$.

Definition 4.2.1. Let L be a field and let $\rho : \Pi \longrightarrow \mathrm{GL}_n(L)$ be a representation. We say that ρ is reducible if there exist a non-zero proper Π-invariant subspace of L^n, otherwise we say that ρ is irreducible. We call ρ absolutely irreducible if for every field extension L'/L the representation $\rho \otimes L'$ is irreducible.

Proposition 4.2.1. *Let* k *be a finite field and let* $\rho : \Pi \longrightarrow \mathrm{GL}_n(k)$ *be a continuous representation. The following are equivalent*

i. ρ *is absolutely irreducible.*

ii. $\rho \otimes \overline{k}$ *is irreducible, where* $\overline{k}$ *denotes the algebraic closure of* k*.*

Proof. Clearly (i) implies (ii). Let L''/k be a extension and let $L''/L'/k$ be an intermediate field, if $\rho \otimes L''$ is irreducible then $\rho \otimes L'$ is so; indeed, if $\rho \otimes L'$ has a proper non-zero invariant subspace E then $E \otimes L''$ is a proper non-zero invariant subspace of $\rho \otimes L''$.

For (ii) implies (i) suppose L'/k is an extension such that $\rho \otimes L'$ is reducible, without loss of generality we may assume that $\overline{k} \subset L'$. Let $H \subset \Pi$ be a set of representatives of the image of Π in $\mathrm{GL}_n(k)$ [2] and denote

$$\rho(g) = (r_{ij}^g), \quad g \in H.$$

Since $\rho \otimes L'$ is reducible there is a basis $e_j = (x_{ij})$ for $j = 1, \ldots, n$ such that $E = \langle e_1 \ldots, e_l \rangle$ $(0 < l < n)$ is a non-zero proper Π-invariant subspace, i.e. there are elements y_{ij}^g with

$$\rho(g)e_k = (r_{ij}^g)(x_{jk}) = \sum_{s=1}^{n} y_{sk}^g e_s$$

and such that $y_{sk}^g = 0$ for $k \leq l$ and $s > l$ for all $g \in H$. Let I be the ideal in $\overline{k}[x_{ij}, y_{sk}^g, z]$ generated by the previous equations together with the condition $\det(x_{ij})z = 1$, hence I is not the unit ideal and the Hilbert's Nullstellenzats implies the existence of a common zero for the elements of I in $\overline{k}$. The existence of this zero implies that $\rho \otimes \overline{k}$ is reducible.

□

[2] Actually what we need for the proof is H to be finite, so we could extend this result to representations of finite groups over arbitrary fields.

Theorem 4.2.1 (Schur's Lemma). *Let $\overline{\rho} : \Pi \longrightarrow \mathrm{GL}_n(k)$ be an absolutely irreducible residual representation. Then $C(\overline{\rho}) = k$.*

Proof. Note that $\overline{\rho} \otimes \overline{k}$ is irreducible. If $M : \overline{k}^n \longrightarrow \overline{k}^n$ is a endomorphism of representations, let λ be an eigenvalue of M, then $\ker(M - \lambda \,\mathrm{Id})$ is a non-zero invariant subspace of k^n and thus equal to k^n. This shows that $M = \lambda \,\mathrm{Id}$ and that $C(\overline{\rho}) = k$ in $\mathrm{GL}_n(k)$. □

The following propositions are important for representations defined in terms of elliptic curves and modular forms.

Proposition 4.2.2. *Let $\overline{\rho} : \Pi \longrightarrow \mathrm{GL}_2(k)$ be a irreducible representation such that its image contains an element of order 2 and determinant -1, then $C(\overline{\rho}) = k$.*

Proof. Let $g \in \Pi$ be an element such that $A = \overline{\rho}(g)$ has order two and whose determinant is -1. As above we denote by p the characteristic of the field k. We need to consider two cases.

Case $p \neq 2$. Consider the scalar's extension $\overline{\rho} \otimes \overline{k}$, the order of A and the condition on the determinant implies that the Jordan's form of the matrix A is

$$JAJ^{-1} = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

Let v_1, v_2 be a basis of eigenvectors of A with eigenvalues 1 and -1 respectively. If $M \in C(\overline{\rho}) \subset \mathrm{M}_n(k)$, then, in particular, $AM = MA$, and J diagonalizes M as well, i.e. v_1, v_2 is also a basis of eigenvectors of M. However, note that v_i can be taken with entries in k, indeed

$$\langle v_1 \rangle = \ker(A - \mathrm{Id}), \quad \langle v_2 \rangle = \ker(A + \mathrm{Id}).$$

Suppose that the eigenvalues of M are a_1, a_2 with $a_1 \neq a_2$ and $Mv_i = a_i v_i$. Then $M' = \frac{1}{a_1 - a_2}(M - a_2 \,\mathrm{Id})$ also commutes with $\overline{\rho}$ and $M'v_1 = v_1$, $M'v_2 = 0$. Therefore M' has entries in k and $\ker M'$ is a invariant subspace of $\overline{\rho}$ of dimension 1. This contradicts the assumption that $\overline{\rho}$ is irreducible.

Case $p = 2$.

The Jordan's canonical form of A is

$$JAJ^{-1} = \begin{pmatrix} 1 & r \\ 0 & 1 \end{pmatrix}$$

where $r \neq 0$. Note that we can choose a Jordan basis v_1, v_2 with entries in k because 1 is a eigenvalue of A. Let $M \in C(\overline{\rho}) \subset \mathrm{M}_n(k)$. In particular $MA = AM$, then a direct computation shows

$$JMJ^{-1} = \begin{pmatrix} a & b \\ 0 & a \end{pmatrix}.$$

Assume $M \notin k$, so $b \neq 0$. If $a = 0$, $\ker(M)$ is a $\overline{\rho}$-invariant subspace of $\overline{\rho}$, a contradiction. If $a \neq 0$, since the entries of J are in k we get that $a, b \in k$ and taking the kernel of $M' = M - a \,\mathrm{Id}$ we get an invariant subspace of dimension one, a contradiction.

□

Proposition 4.2.3. *Let $\overline{\rho} : \Pi \longrightarrow \mathrm{GL}_n(k)$ be a residual representation and let $f_{\overline{\rho}} : k[[\Pi]] \longrightarrow \mathrm{M}_n(k)$ be the corresponding continuous homomorphism of algebras. The following are equivalent*

i. $\overline{\rho}$ is absolutely irreducible

ii. $f_{\overline{\rho}}$ is surjective *iii.* $\overline{\rho}$ *is irreducible and* $C(\overline{\rho}) = k$.

Proof. **ii implies i.** If $f_{\overline{\rho}}$ is surjective then the extension to $\overline{k}$, $f_{\overline{\rho}} \otimes \overline{k} = f_{\overline{\rho} \otimes \overline{k}}$ remains surjective, so the $k[[\Pi]]$-module generated by a non-zero element in $\overline{k}^n$ is all $\overline{k}^n$ and therefore $\overline{\rho} \otimes \overline{k}$ is irreducible.

i implies iii. If $\overline{\rho}$ is absolutely irreducible then in particular $\overline{\rho}$ is irreducible and by Schur's Lemma $C(\overline{\rho}) = k$.

iii implies ii. Wedderburn's Theorem (Corollary 3.5 of Chapter XVII in Lang's Algebra [Lan02]) shows that the image of $f_{\overline{\rho}}$ is $\mathrm{End}_{C(\overline{\rho})}(k^n) = \mathrm{End}_k(k^n) = M_n(k)$.

□

4.3 Existence of the universal deformation ring

In this section we apply Schlessinger's criteria to the deformation functor $\mathbf{D}_{\overline{\rho}}$. Once all the groundwork is done, the statement of the main result of this section is the following:

Theorem 4.3.1 (Mazur, Ramakrishna)**.** *Suppose* Π *is a profinite group satisfying the* Φ_p *condition,* $\overline{\rho} : \Pi \longrightarrow \mathrm{GL}_n(k)$ *is a continuous representation, and* Λ *is a complete noetherian local ring with residue field* k*. Then the deformation functor* $\mathbf{D}_\Lambda$ *has a hull. Moreover, if* $C(\overline{\rho}) = k$ *then* $\mathbf{D}_\Lambda$ *is representable.*

Particularly, the condition $C(\overline{\rho}) = k$ holds for absolutely irreducible representations.

Corollary 4.3.1.1 (Mazur)**.** *Suppose* Π *is a profinite group satisfying the* Φ_p *condition and let* $\overline{\rho} : \Pi \longrightarrow \mathrm{GL}_n(k)$ *be an absolutely irreducible continuous representation. Then there exists a ring* $\mathcal{R}_{\overline{\rho}}$ *and a deformation* $\boldsymbol{\rho} : \Pi \longrightarrow \mathrm{GL}_n(\mathcal{R}_{\overline{\rho}})$ *such that: for every coefficient ring* A*, and for every deformation* $\rho : \Pi \longrightarrow \mathrm{GL}_n(A)$ *there is a unique coefficient ring homomorphism* $\varphi : \mathcal{R}_{\overline{\rho}} \longrightarrow A$ *such that* $\rho = \varphi \circ \boldsymbol{\rho}$*.*

The ring $\mathcal{R}(\Pi, k, \overline{\rho}) = \mathcal{R}_{\overline{\rho}}$ is called the *universal deformation ring* and the deformation $\boldsymbol{\rho}$ is the *universal deformation.* The ring $\mathcal{R}(\Pi, k, \overline{\rho})$ is unique in the following strong sense.

Theorem 4.3.2 (Mazur)**.** *Suppose*

$$\overline{\rho} : \Pi \longrightarrow \mathrm{GL}_n(k)$$

is a continuous representation such that $C(\overline{\rho}) = k$*. If* $\overline{\rho}'$ *is a representation equivalent to* $\overline{\rho} \otimes \chi$*, where* χ *is a representation of dimension one, then there is a canonical isomorphism*

$$r(\overline{\rho}', \overline{\rho}) : \mathcal{R}(\Pi, k, \overline{\rho}) \longrightarrow \mathcal{R}(\Pi, k, \overline{\rho}')$$

mapping the universal deformation of $\overline{\rho}$ *to the universal deformation* $\overline{\rho}'$*. This system of canonical isomorphisms satisfies the natural compatibility conditions.*

Proof. In chapter 5 we will give the proof. □

Definition 4.3.1. Let $\overline{\rho}$ be a residual representation, and let ρ be a deformation of $\overline{\rho}$ to a coefficient Λ-algebra A. We define

$$C_A(\rho) = \mathrm{Hom}_\Pi(A^n, A^n) = \{P \in \mathrm{M}_n(A) : P\rho(g) = \rho(g)P \text{ for all } g \in \Pi\}.$$

In particular, $C(\overline{\rho}) = C_k(\overline{\rho})$.

In order to prove Theorem 4.3.1 we fix the following notation. Let A_0, A_1, A_2 be artinian coefficient Λ-algebras, and suppose we are given $\phi_1 : A_1 \longrightarrow A_0$ and $\phi_2 : A_2 \longrightarrow A_0$ morphisms of $\mathcal{C}^0_\Lambda$. Let

$$E_i = \mathrm{Hom}_{\overline{\rho}}(\Pi, \mathrm{GL}_n(A_i))$$

be the set of homomorphisms from Π to $\mathrm{GL}_n(A_i)$ which reduce to $\overline{\rho}$ modulo the maximal ideal. Then $\Gamma_n(A_i)$ acts on E_i by conjugation and we have

$$\mathbf{D}_\Lambda(A_i) = E_i/\Gamma_n(A_i).$$

Denote $A_3 = A_1 \times_{A_0} A_2$. The map in (4.1.2) is then

$$b : E_3/\Gamma_n(A_3) \longrightarrow E_1/\Gamma_n(A_1) \times_{E_0/\Gamma_n(A_0)} E_2/\Gamma_n(A_2).$$

Remark. If $A_2 \longrightarrow A_0$ is surjective then $\Gamma_n(A_2) \longrightarrow \Gamma_n(A_0)$ is also surjective.

For the remaining lemmas of the section we assume Π, $\overline{\rho}$ and Λ as in Theorem 4.3.1.

Lemma 4.3.1. *Property* **H**1 *is true.*

Proof. Suppose $A_2 \longrightarrow A_0$ is small. Let (ρ_1, ρ_2) be a pair of deformations to A_1 and A_2 which induce the same deformation in A_0, we want to show that we can paste them together to get a deformation to A_3. Let ϕ_1 and ϕ_2 be representatives of ρ_1 and ρ_2 respectively. There is a matrix $\overline{M} \in \Gamma_n(A_0)$ such that $\phi_1 = \overline{M}^{-1}\phi_2\overline{M}$ in A_0. Take $M \in \Gamma_n(A_2)$ a lifting of $\overline{M}$, then ϕ_1 and $M^{-1}\phi_2 M$ reduce to the same representation in A_0.

Note that GL_n is a representable functor from commutative rings to groups. Indeed, $\mathrm{GL}_n(A) = \mathrm{Hom}(\mathbb{Z}[x_{i,j}, y]/(\det(x_{i,j})y - 1), A)$. Therefore it preserves fibre products and

$$\mathrm{GL}_n(A_3) = \mathrm{GL}_n(A_1) \times_{\mathrm{GL}_n(A_0)} \mathrm{GL}_n(A_2).$$

Then ϕ_1 and $M^{-1}\phi_2 M$ induce a continuous homomorphism $\phi_3 : \Pi \longrightarrow \mathrm{GL}_n(A_3)$ whose strict equivalence class reduces to ρ_1 and ρ_2 in A_1 and A_2 respectively. □

Let $\phi_2 \in E_2$ and let $\phi_0 \in E_0$ be its image. Set

$$G_i(\phi_i) = \{g \in \Gamma_n(A_i) : \ g \text{ commutes with the image of } \phi_i \text{ in } \mathrm{GL}_n(A_i)\}.$$

Lemma 4.3.2. *If for all $\phi_2 \in E_2$ the map*

$$G_2(\phi_2) \longrightarrow G_0(\phi_0)$$

is surjective, then the map b is injective.

Proof. Suppose ϕ and ψ are elements of E_3 that induce elements ϕ_i and ψ_i in E_i for each $i = 0, 1, 2$. Saying that ϕ and ψ have the same image under b means that for each $i = 1, 2$ there is an $M_i \in \Gamma_n(A_i)$ such that $\psi_i = M_i^{-1}\phi_i M_i$. Mapping down to E_0 we see that

$$\psi_0 = \overline{M}_1^{-1}\phi_0\overline{M}_1 = \overline{M}_2^{-1}\phi_0\overline{M}_2,$$

and so that $\overline{M}_2\overline{M}_1^{-1}$ commutes with the image of ϕ_0, i.e., $\overline{M}_2\overline{M}_1^{-1} \in G_0(\phi_0)$. Now find $N \in G_2(\phi_2)$ which maps to $\overline{M}_2\overline{M}_1^{-1}$. Let $N_2 = N^{-1}M_2$. Then we have

$$N_2^{-1}\phi_2 N_2 = M_2^{-1}N\phi_2 N^{-1}M_2 = M_2^{-1}\phi_2 M_2 = \psi_2.$$

On the other hand, the image of N_2 in $\Gamma_n(A_0)$ is

$$\overline{N_2} = (\overline{M}_2\overline{M}_1^{-1})^{-1}\overline{M}_2 = \overline{M}_1.$$

Since M_1 and N_2 have the same image in $\Gamma_n(A_0)$, the pair (M_1, N_2) defines an element $M \in \Gamma_n(A_3)$ and we have $M^{-1}\phi M = \psi$. Thus, ϕ and ψ are strictly equivalent.

□

Lemma 4.3.3. *Property* **H**2 *is true.*

Proof. If $A_0 = k$ and $A_2 = k[\epsilon]$, then b is already surjective by **H**1. Injectivity will follow because $G_2(\phi_2) \longrightarrow G_0(\phi_0)$ is always surjective. Indeed, when $A_0 = k$, $\Gamma_n(k)$ consists only of the identity matrix. □

Lemma 4.3.4. *Property* **H**3 *is true.*

Proof. In chapter 5 we are going to show the existence of a canonical isomorphism of vector spaces $t_{\mathbf{D}} \cong H^1(\Pi, \mathrm{Ad}(\overline{\rho}))$, where $\mathrm{Ad}(\overline{\rho}))$ consists of $\mathrm{M}_n(k)$ with conjugation by $\overline{\rho}$.

Now, let Π_0 be the kernel of $\overline{\rho}$. Inflation-restriction sequence gives us an exact row

$$\begin{tikzcd} 0 \arrow[r] & H^1(\Pi/\Pi_0, \mathrm{Ad}(\overline{\rho})) \arrow[r] & H^1(\Pi, \mathrm{Ad}(\overline{\rho})) \arrow[r] & H^1(\Pi_0, \mathrm{Ad}(\overline{\rho})) . \end{tikzcd}$$

But Π/Π_0 is a finite group and $H^1(\Pi_0, \mathrm{Ad}(\overline{\rho})) = \mathrm{Hom}(\Pi_0, \mathrm{Ad}(\overline{\rho}))$. Since Π_0 acts trivially on $\mathrm{Ad}(\overline{\rho})$. The Φ_p-condition implies that $\mathrm{Hom}(\Pi_0, \mathrm{Ad}(\overline{\rho}))$ is finite dimensional showing that $H^1(\Pi, \mathrm{Ad}(\overline{\rho}))$ is a finite dimensional vector space over k.

□

Lemma 4.3.5. *If $C(\overline{\rho}) = k$, then for any i the group $G_i(\phi_i) \subset A_i$, i.e., $G_i(\phi_i)$ consists of the scalar matrices in $\Gamma_n(A_i)$.*

Proof. We are going to prove that actually for every deformation ρ of $\overline{\rho}$ to any artinian coefficient ring A we have $C_A(\rho) = A$.

Since the map $A \longrightarrow k$ is surjective, it factors as a sequence of small homomorphisms. Since we know that $C_k(\overline{\rho}) = k$, the lemma will follow, by induction, from the claim that if $C_B(\rho_B) = B$ and $A \longrightarrow B$ is small, then $C_A(\rho_A) = A$.

Take $c \in C_A(\rho_A)$. By our assumption, the image of c in $\mathrm{M}_n(B)$ is an scalar matrix. Suppose $c = r + tM$ where t is a generator of the kernel of $A \longrightarrow B$ and $M \in \mathrm{M}_n(A)$.

Now, for all $g \in \Pi$

$$(r + tM)\rho_A(g) = \rho_A(g)(r + tM)$$

therefore

$$\overline{M}\overline{\rho} = \overline{\rho}\overline{M}$$

where $\overline{M}$ is the reduction to k. Recall $C_k(\overline{\rho}) = k$. Therefore $M = s + M_1$ with s an scalar matrix and all entries of M_1 in $\mathfrak{m}_A$. Since $A \longrightarrow B$ is small we get $t\mathfrak{m}_A = 0$, it follows that $M = r + ts$ is a scalar matrix.

□

Lemma 4.3.6. *Suppose $C(\overline{\rho}) = k$, then* **H**4 *is true.*

Proof. From the previous lemma $G_i(\phi_i)$ consists only on scalar matrices and the statement follows. □

4.4 Case $n = 1$; Characters

A complete description of the universal deformation ring and the universal deformation for characters is given in this section. According to Theorem 4.3.2 the universal deformation ring is the same for all characters.

Let $\overline{\chi} : \Pi \longrightarrow k^*$ be a character and let $\chi_0 : \Pi \longrightarrow W(k)^*$ be its Teichmüller lifting[3], in this case it is just the lifting of k^* into the roots of unity of $W(k)^*$. Let A be any coefficient ring, the natural homomorphism $W(k) \longrightarrow A$ induces the Teichmuller lifting of $\overline{\chi}$ to A. Let χ be a deformation of $\overline{\chi}$ to A, then $\chi\chi_0^{-1}$ is a homomorphism of Π to $1 + \mathfrak{m}_A$.

The group $1 + \mathfrak{m}_A$ is an abelian pro-p-group because

$$1 + \mathfrak{m}_A = \varprojlim_{k\in\mathbb{N}} (1 + \mathfrak{m}_A)/(1 + \mathfrak{m}_A^k) = \varprojlim(1 + \mathfrak{m}_{A/\mathfrak{m}_A^k}).$$

Therefore $\chi\chi_0^{-1}$ factors through $\Gamma = \Pi^{ab,p}$, i.e. the abelianization of the pro-p-completion of Π. We have then the following result:

Lemma 4.4.1. *Deformations of $\overline{\chi}$ to A are in bijective correspondence with group homomorphisms $\Gamma \longrightarrow 1 + \mathfrak{m}_A$.*

Let Λ be a coefficient ring. Let $\Lambda[[\Gamma]]$ be the completed group algebra of Γ with coefficients in Λ

$$\Lambda[[\Gamma]] = \varprojlim_{H} \Lambda[\Gamma/H].$$

If $u \in \Gamma$, we write $[u]$ for the corresponding element in $\Lambda[\Gamma]$.

Proposition 4.4.1. $\Lambda[[\Gamma]]$ *is a coefficient* Λ*-algebra.*

Proof. It suffices to show that $\Lambda[\Gamma/H]$ is local because Γ is finitely generated as $\mathbb{Z}_p$ module. We contend that the kernel of augmentation and reduction $\epsilon : \Lambda[\Gamma] \longrightarrow k$ is the unique maximal ideal. Indeed, if $r \in \ker\epsilon$ then

$$r = \sum_{g\in\Gamma/H} a_g[g] = \sum_{g\in\Gamma/H} a_g([g] - [1]) + \sum_{g\in\Gamma/H} a_g$$

Therefore r is nilpotent provided $[g] - [1]$ is. Let p^α be the order of Γ/H, then

$$([g] - [1])^{p^\alpha} = [g^{p^\alpha}] + \sum_{s=1}^{p^\alpha-1} (-1)^s \binom{p^\alpha}{s} [g^{p^\alpha-s}] + (-1)^{p^\alpha}[1] = pr' + (1 + (-1)^p)[1]$$

where pr' is the summation term. In any situation (p even or p odd) we get that this term is divisible by p and hence is nilpotent.

□

We denote by $\gamma : \Pi \longrightarrow \Gamma$ the canonical projection.

Proposition 4.4.2. *The universal deformation ring of a character $\overline{\chi} : \Pi \longrightarrow k^*$ is*

$$\mathcal{R}(\Pi, k, \overline{\chi}) = \Lambda[[\Gamma]].$$

The universal deformation is given given by

$$\boldsymbol{\chi}(x) = \chi_0(x)[\gamma(x)].$$

[3] See [Ser79, Ch II. §4-§6] for the construction of Witt vectors $W(k)$ and the Teichmüller lifting, also called *multiplicatively system of representatives.*

Proof. We already know that $\Lambda[[\Gamma]]$ is a coefficient Λ-algebra and that $\boldsymbol{\chi}$ is a deformation of $\overline{\chi}$. Let $\chi : \Pi \longrightarrow A^*$ be a deformation of $\overline{\chi}$ and consider $\psi = \chi\chi_0^{-1}$. Then ψ is a character taking values in $1 + \mathfrak{m}_A$ which is a pro-p-group, hence ψ factors through Γ and defines a map $f_\chi : \Gamma \longrightarrow 1 + \mathfrak{m}_A$ which extends to a homomorphism of Λ-algebras $f_\chi : \Lambda[[\Gamma]] \longrightarrow A$. We then have $\chi = f_\chi \circ \boldsymbol{\chi}$, proving our claim. □

Chapter 5

Properties of representable deformation functors

From now on Π will denote a profinite group satisfying the Φ_p-condition and $\overline{\rho} : \Pi \longrightarrow \mathrm{GL}_n(k)$ a residual representation. Furthermore, through this chapter all residual representations will also satisfy $C(\overline{\rho}) = k$, in particular the universal deformation ring $\mathcal{R}_{\overline{\rho}}$ and the universal deformation $\boldsymbol{\rho}$ exist.

5.1 Functorial properties

These properties arise from the representavility of the deformation functor. First, we study the determinant

$$\det : \mathrm{GL}_n \longrightarrow \mathrm{GL}_1 .$$

The determinant sends Γ_n to Γ_1, therefore it gives a well defined morphism of functors $\mathbf{D}_{\overline{\rho}} \longrightarrow \mathbf{D}_{\det \overline{\rho}}$. Equivalently, by Yoneda's lemma, we have a well defined coefficient ring homomorphism

$$\mathcal{R}(\Pi, k, \det \overline{\rho}) \longrightarrow \mathcal{R}(\Pi, k, \overline{\rho}),$$

we have already shown that $\mathcal{R}(\Pi, k, \det \overline{\rho}) = \Lambda[[\Gamma]]$, where $\Gamma = \Pi^{ab,p}$ is the abelianization of the pro-p-completion of Π. This shows that the universal deformation rings has a canonical structure of $\Lambda[[\Gamma]]$ algebra. Let $\boldsymbol{\rho}$ be the universal deformation of $\overline{\rho}$, note that this coefficient ring homomorphism sends the universal deformation of $\det \overline{\rho}$ to $\det \boldsymbol{\rho}$.

Another example of this kind of property is conjugation. Suppose $\overline{\rho}$ and $\overline{\rho}'$ are residual equivalent representations. There exists a matrix $x \in \mathrm{GL}_n(W(k))$ (which we can think of as in $\mathrm{GL}_n(\Lambda)$) such that $\overline{\rho} = \overline{x}^{-1}\overline{\rho}'\overline{x}$. Conjugation by x is a morphism of functors (indeed it is an isomorphism)

$$\delta_x : \mathrm{GL}_n \longrightarrow \mathrm{GL}_n$$

which preservers Γ_n, so it reduces to a morphism of strict equivalent representations and therefore to a morphism

$$\delta_x : \mathbf{D}_{\overline{\rho}'} \longrightarrow \mathbf{D}_{\overline{\rho}}.$$

If $y \in \mathrm{GL}_n(W(k))$ is another matrix such that $\overline{\rho} = \overline{y}^{-1}\overline{\rho}'\overline{y}$ then the condition $C(\overline{\rho}) = k$ implies $y = \alpha x N$, where $\alpha \in W(k)^*$ is scalar matrix and $N \in \Gamma_n(W(k))$. Therefore conjugation by y induces the same functor at the level of deformations and $r(\delta_x)$ does not depend on x.

Then, we have a coefficient ring isomorphism

$$r(\overline{\rho}', \overline{\rho}) : \mathcal{R}(\overline{\rho}) \longrightarrow \mathcal{R}(\overline{\rho}')$$

sending $\boldsymbol{\rho}$ to $x^{-1}\boldsymbol{\rho}'x$. Note that the independence on the conjugation matrix implies that if $\overline{\rho}''$ is equivalent to $\overline{\rho}'$ then

$$r(\overline{\rho}'', \overline{\rho}') \circ r(\overline{\rho}'.\overline{\rho}) = r(\overline{\rho}'', \overline{\rho}).$$

Other important functorial property appears when tensoring representations. Let $\overline{\rho}_1$ and $\overline{\rho}_2$ be residual representations such that $C(\overline{\rho}_1) = C(\overline{\rho}_2) = C(\overline{\rho}_1 \otimes \overline{\rho}_2) = k$, we have universal deformation rings $\mathcal{R}(\overline{\rho}_1)$, $\mathcal{R}(\overline{\rho}_2)$, $\mathcal{R}(\overline{\rho}_1 \otimes \overline{\rho}_2)$, and universal deformations $\boldsymbol{\rho}_1$, $\boldsymbol{\rho}_2$, $\boldsymbol{\rho}_3$ of $\overline{\rho}_1$, $\overline{\rho}_2$, $\overline{\rho}_1 \otimes \overline{\rho}_2$ respectively.

Let ρ_1, ρ_2 be deformations of $\overline{\rho}_1$ and $\overline{\rho}_2$ to A_1 and A_2 respectively. We can consider the tensor product $\rho_1 \otimes \rho_2 : \Pi \longrightarrow \mathrm{GL}_n(A_1 \hat{\otimes}_\Lambda A_2)$, this is a deformation of $\overline{\rho}_1 \otimes \overline{\rho}_2$. Indeed, since tensoring sends $\Gamma_n(A_1) \otimes \Gamma_n(A_2) \longrightarrow \Gamma_n(A_1 \hat{\otimes}_\Lambda A_2)$ then it preserves strict equivalence representations. In particular, consider $A_1 = \mathcal{R}(\overline{\rho}_1)$, $A_2 = \mathcal{R}(\overline{\rho}_2)$, we then form the deformation $\boldsymbol{\rho}_1 \otimes \boldsymbol{\rho}_2$. Thus, we get a coefficient ring homomorphism

$$\mathcal{R}(\overline{\rho}_1 \otimes \overline{\rho}_2) \longrightarrow \mathcal{R}(\overline{\rho}_1) \hat{\otimes}_\Lambda \mathcal{R}(\overline{\rho}_2)$$

sending $\boldsymbol{\rho}_3$ to $\boldsymbol{\rho}_1 \otimes \boldsymbol{\rho}_2$.

Now, choose a lift ρ_1 of $\overline{\rho}_1$ to $\mathrm{GL}_n(\Lambda)$. By the universal property, this corresponds to a map $h_1 : \mathcal{R}(\overline{\rho}_1) \longrightarrow \Lambda$. The composition

$$h(\rho_1, \overline{\rho}_2) : \mathcal{R}(\overline{\rho}_1 \otimes \overline{\rho}_2) \longrightarrow \mathcal{R}(\overline{\rho}_1) \hat{\otimes}_\Lambda \mathcal{R}(\overline{\rho}_2) \xrightarrow{h_1 \otimes id} \mathcal{R}(\overline{\rho}_2)$$

is called *contraction by* ρ_1.

Particularly, if $\overline{\rho}_1 = \overline{\chi}_1$ is a character we may choose $\rho_1 = \chi_1$ as the Teichmüller lifting and get an isomorphism of coefficient rings

$$h(\chi_1, \overline{\rho_2}) : \mathcal{R}(\overline{\chi}_1 \otimes \overline{\rho}_2) \longrightarrow \mathcal{R}(\overline{\rho}_2)$$

sending the universal deformation of $\overline{\chi}_1 \otimes \overline{\rho}_2$ to $\chi_1 \otimes \boldsymbol{\rho}_2$. This is an isomorphism of rings with inverse $h(\chi_1^{-1}, \overline{\chi}_1 \otimes \overline{\rho}_2)$. Thus, we have coefficient ring isomorphisms $r(\overline{\rho_1}, \overline{\rho}_2) : \mathcal{R}(\overline{\rho}_2) \longrightarrow \mathcal{R}(\overline{\rho_1})$ of twisted representations satisfying the natural compatibility condition.

Finally, given $\rho : \Pi \longrightarrow \mathrm{GL}_n(R)$ we can consider the *contragredient representation*

$$\rho^{\#}(g) = (\rho(g)^{-1})^t$$

which is the transpose of the inverse. It is actually an isomorphism of GL_n, therefore it induces an isomorphism of functors

$$\mathbf{D}_{\overline{\rho}} \longrightarrow \mathbf{D}_{\overline{\rho}^{\#}},$$

and consequently an isomorphism of coefficient rings

$$\mathcal{R}_{\overline{\rho}^{\#}} \longrightarrow \mathcal{R}_{\overline{\rho}}.$$

5.2 The tangent space

In this section we will show the connection between the tangent space $t_{\mathbf{D}}$, cohomology and extension of modules. Basically the motivation is to give different points of view about how we can describe the tangent space, in particular we would wish to compute its dimension.

As in previous chapters, let $\overline{\rho} : \Pi \longrightarrow \mathrm{GL}_n(k)$ be a residual representation. Let $\mathbf{D} = \mathbf{D}_{\overline{\rho},\Lambda}$ be the deformation functor. We have defined the tangent space

$$t_{\mathbf{D}} = \mathbf{D}(k[\epsilon]).$$

If in addition $\overline{\rho}$ is representable by $\mathcal{R}$ then also

$$t_{\mathbf{D}} = \mathbf{D}(k[\epsilon]) = \mathrm{Hom}_\Lambda(\mathcal{R}, k[\epsilon]) = \mathrm{Hom}_k(\mathfrak{m}_\mathcal{R}/(\mathfrak{m}_\mathcal{R}, \mathfrak{m}_\Lambda), k)$$

Suppose ρ_1 is a deformation of $\overline{\rho}$ to $k[\epsilon]$, for $g \in \Pi$ we may write

$$\rho_1(g) = (1 + \epsilon b_g)\overline{\rho}(g)$$

with $b_g \in \mathrm{M}_n(k)$. The condition on the map ρ_1 to be a group homomorphism is equivalent for b_g to be a 1-cocicle of $Ad(\overline{\rho})$. Indeed,

$$\begin{aligned}
\rho_1(gh) &= \rho_1(g)\rho_1(h)\\
(1 + \epsilon b_{gh})\overline{\rho}(gh) &= (1 + \epsilon b_g)\overline{\rho}(g)(1 + \epsilon b_h)\overline{\rho}(h)\\
(1 + \epsilon b_{gh})\overline{\rho}(gh) &= (1 + \epsilon b_g)(1 + \epsilon\overline{\rho}(g) b_h \overline{\rho}(g)^{-1})\overline{\rho}(gh)\\
(1 + \epsilon b_{gh})\overline{\rho}(gh) &= (1 + \epsilon(b_g + \overline{\rho}(g) b_h \overline{\rho}(g)^{-1}))\overline{\rho}(gh).
\end{aligned}$$

Two representations ρ_1 and ρ_2 are strictly equivalent if and only if their respective associated cocycles b_g and b'_g are in the same cohomology class. Since $\Gamma_n(k[\epsilon]) = 1 + \epsilon\,\mathrm{M}_n(k)$, then, for $M \in \mathrm{M}_n(k)$,

$$\begin{aligned}
\rho_1(g) &= (1 - \epsilon M)\rho_2(g)(1 + \epsilon M)\\
(1 + \epsilon b_g)\overline{\rho}(g) &= (1 - \epsilon M)(1 + \epsilon b'_g)\overline{\rho}(g)(1 + \epsilon M)\\
(1 + \epsilon b_g)\overline{\rho}(g) &= (1 + \epsilon(b'_g + \overline{\rho} M \overline{\rho}(g)^{-1} - M))\overline{\rho}(g).
\end{aligned}$$

Therefore we get a natural bijection

$$t_{\mathbf{D}} \longrightarrow H^1(\Pi, \mathrm{Ad}(\overline{\rho})), \quad \rho_1 \mapsto b_g.$$

An straightforward computation shows that this correspondence is indeed an isomorphism of vector spaces. Therefore we have shown:

Proposition 5.2.1. *Let $\overline{\rho} : \Pi \longrightarrow \mathrm{GL}_n(k)$ be a residual representation, then there is a natural isomorphism of vector spaces*

$$t_{\mathbf{D}} \cong H^1(\Pi, \mathrm{Ad}(\overline{\rho})).$$

Moreover, if $C(\overline{\rho}) = k$ and $\mathcal{R}$ is its universal deformation ring, then we also get natural isomorphisms

$$t_{\mathbf{D}} \cong \mathrm{Hom}_k(\mathfrak{m}_\mathcal{R}/(\mathfrak{m}_\mathcal{R}^2, \mathfrak{m}_\Lambda), k) \cong \mathrm{Der}_\Lambda(\mathcal{R}, k)$$

where $\mathrm{Der}_\Lambda(\mathcal{R}, k)$ denotes Λ-derivations of $\mathcal{R}$ with values in k.

Corollary 5.2.1.1. *Let $\overline{\rho}$ be a residual representation such that $C(\overline{\rho}) = k$ and let d_1 be the dimension of $H^1(\Pi, \mathrm{Ad}(\overline{\rho}))$. Then $\mathcal{R} = \mathcal{R}(\Pi, k, \overline{\rho})$ is a quotient of a power series ring on d_1 variables which induces an isomorphism on tangent spaces.*

Proof. Let $\overline{e}_1, \dots, \overline{e}_{d_1}$ be a basis of the cotangent space of $\mathcal{R}$ and let $e_1, \dots, e_{d_1}$ be a lifting to the maximal ideal $\mathfrak{m}_{\mathcal{R}}$. Consider the coefficient Λ-algebra homomorphism

$$\Lambda[[X_1, \dots, X_{d_1}]] \longrightarrow \mathcal{R}$$

which sends $X_i \mapsto e_i$, then by Nakayama's lemma it is surjective and induces an isomorphism on tangent spaces. □

We finally describe the relation between the tangent space and extension of modules. At the end of chapter 1 we mentioned that we may think of representations as Π-modules over free A-modules where A is a coefficient ring, denote by $V_{\overline{\rho}}$ the Π-module given by $\overline{\rho}$.

Proposition 5.2.2. *Let $\overline{\rho}$ be a residual representation with representation module $V_{\overline{\rho}}$. Then the set of deformations of $\overline{\rho}$ to $k[\epsilon]$ is in bijective correspondence with the set of isomorphism classes of extensions of $k[[\Pi]]$-modules of $V_{\overline{\rho}}$ by $V_{\overline{\rho}}$, that is, isomorphism classes of exact sequences*

$$\begin{tikzcd} 0 \arrow[r] & V_{\overline{\rho}} \arrow[r] & E \arrow[r] & V_{\overline{\rho}} \arrow[r] & 0 \end{tikzcd}$$

of $k[[\Pi]]$-modules.

Proof. Suppose that we are given an element of $t_{\mathbf{D}}$, that is, a deformation of $\overline{\rho}$ to $k[\epsilon]$. Let M be $k[\epsilon]^n$ with the action of Π given by $\overline{\rho}$. Clearly M is of dimension $2n$ as a vector space over k. Consider the submodule ϵM and the module $M/\epsilon M$. These are both clearly n-dimensional over k, and are in fact isomorphic to $V_{\overline{\rho}}$. Hence we get an exact sequence

$$\begin{tikzcd} 0 \arrow[r] & V_{\overline{\rho}} \arrow[r] \arrow[d] & M \arrow[r] \arrow[d, "id"] & V_{\overline{\rho}} \arrow[r] \arrow[d] & 0 \\ 0 \arrow[r] & \epsilon M \arrow[r] & M \arrow[r] & M/\epsilon M \arrow[r] & 0 \end{tikzcd}$$

where the vertical arrows are isomorphisms of $k[[\Pi]]$-modules.

If ρ_1 and ρ_2 are strictly equivalents, say, $\rho_1 = (1 - \epsilon M)\rho_2(1 + \epsilon M)$ then $(1 + \epsilon M)$ is an isomorphism of $k[[\Pi]]$ modules between both actions and leaves ϵM and $M/\epsilon M$ invariant, so they give the same isomorphism class of extensions. For the converse, suppose we are given a $2n$-dimensional k-vector space E which fits into an exact sequence

$$\begin{tikzcd} 0 \arrow[r] & V_{\overline{\rho}} \arrow[r, "\alpha"] & E \arrow[r, "\beta"] & V_{\overline{\rho}} \arrow[r] & 0 . \end{tikzcd}$$

We then make E into a $k[\epsilon]$-module by defining multiplication by ϵ to be

$$\alpha \circ \beta : E \longrightarrow E.$$

It is easy to see that $(\alpha \circ \beta)^2 = 0$, since $\beta \circ \alpha = 0$. In addition, since both α and β are morphisms of $k[[\Pi]]$-modules, this $k[\epsilon]$-structure commutes with the action of Π. We can check that the $k[\epsilon]$-structure of E makes it a free $k[\epsilon]$-module of rank n.Indeed, take $e_1, \cdots, e_n$ to be the canonical basis of $V_{\overline{\rho}}$ and let $f_1, \dots, f_n$ be a lifting to E. Then $f_1, \dots, f_n$ is a basis of E over $k[\epsilon]$.

Fixing this basis we get a homomorphism

$$\rho_1 : \Pi \longrightarrow \mathrm{GL}_n(k[\epsilon])$$

which is clearly a deformation of $\overline{\rho}$.

It is straightforward to check that two different liftings of $e_1, \dots, e_n$ to E give strict equivalent deformations of $\overline{\rho}$. This proves our assertion.

□

It is well known that isomorphism classes of extensions of $V_{\overline{\rho}}$ by $V_{\overline{\rho}}$ are in bijective correspondence with elements in $\mathrm{Ext}^1_{k[[\Pi]]}(V_{\overline{\rho}}, V_{\overline{\rho}})$, under this bijection the correspondence between $t_{\mathbf{D}}$ and $\mathrm{Ext}^1_{k[[\Pi]]}(V_{\overline{\rho}}, V_{\overline{\rho}})$ is an isomorphism of vector spaces.

5.3 Obstruction problems

The natural way to construct deformations is by lifting the residual representation recursively. Therefore, we should be aware of when we are able to lift a deformation, this problem is called an *obstruction problem.*

Let A_1 and A_0 be objects of $\mathcal{C}^0_\Lambda$ and let $A_1 \longrightarrow A_0$ be a surjective homomorphism with kernel I. Suppose further that $\mathfrak{m}_{A_1} I = 0$, then I is a vector space over k. Note that every surjective homomorphism can be factorized into finitely many of these sort or coefficient ring homomorphisms, for instance in small homomorphisms.

Suppose we are given a homomorphism $\rho_0 : \Gamma \longrightarrow \mathrm{GL}_n(A_0)$. We can find a set-theoretic lift $\gamma : \Pi \longrightarrow \mathrm{GL}_n(A_1)$ that lifts ρ_0. To test whether this is a homomorphism, we would have to compute

$$c(g_1, g_2) = \gamma(g_1 g_2)\gamma(g_2)^{-1}\gamma(g_1)^{-1}$$

for every $g_1, g_2 \in \Pi$. We see that γ is an homomorphism if and only if $c(g_1, g_2) = 1$ for all g_1, g_2. Since it is a homomorphism modulo I, we do know that

$$c(g_1, g_2) = 1 + d(g_1, g_2)$$

with $d(g_1, g_2) \in \mathrm{M}_n(I) \cong \mathrm{Ad}(\overline{\rho}) \otimes I$. The following computation shows that actually $d(g_1, g_2)$ is a cocycle

$$\begin{aligned}
(1 + d(g_1g_2, g_3)) &= \gamma(g_1g_2g_3)\gamma(g_3)^{-1}\gamma(g_1g_2)^{-1} \\
&= \gamma(g_1g_2g_3)\gamma(g_2g_3)^{-1}\gamma(g_1)^{-1}\gamma(g_1)\gamma(g_2g_3)\gamma(g_3)^{-1}\gamma(g_2)^{-1}\gamma(g_1)^{-1} \\
&\quad (\gamma(g_1g_2)\gamma(g_2)^{-1}\gamma(g_1)^{-1})^{-1} \\
&= (1 + d(g_1, g_2g_3))\gamma(g_1)(1 + d(g_2, g_3))\gamma(g_1)^{-1}(1 - d(g_1, g_2)) \\
&= (1 + d(g_1, g_2g_3))(1 + \overline{\rho}(g_1)d(g_2, g_3)\overline{\rho}(g_1)^{-1})(1 - d(g_1, g_2)).
\end{aligned}$$

Replacing γ by a different lift changes this cocycle by a coboundary. If γ' is another lift then $\gamma(g) = (1 + e(g))\gamma'(g)$ with $e(g) \in I$, we compute

$$\begin{aligned}
(1 + d(g_1, g_2)) &= \gamma(g_1g_2)\gamma(g_2)^{-1}\gamma(g_1)^{-1} \\
&= (1 + e(g_1g_2))\gamma'(g_1g_2)\gamma'(g_2)^{-1}(1 - e(g_2))\gamma'(g_1)^{-1}(1 - e(g_1)) \\
&= (1 + e(g_1g_2))\gamma'(g_1g_2)\gamma'(g_2)^{-1}\gamma'(g_1)^{-1}(1 - \overline{\rho}(g_1)e(g_2)\overline{\rho}(g_1)^{-1})(1 - e(g_1)) \\
&= (1 + e(g_1g_2))(1 + d'(g_1, g_2))(1 - \overline{\rho}(g_1)e(g_2)\overline{\rho}(g_1)^{-1})(1 - e(g_1)) \\
&= (1 + d'(g_1, g_2) - \overline{\rho}(g_1)e(g_2)\overline{\rho}(g_1)^{-1} + e(g_1g_2) - e(g_1)).
\end{aligned}$$

All this proves that the cocycle $d(g_1, g_2)$ gives an element $\mathcal{O}(\rho_0)$ in the cohomology group $H^2(\Pi, \mathrm{Ad}(\overline{\rho}) \otimes_k I) \cong H^2(\Pi, \mathrm{Ad}(\overline{\rho})) \otimes_k I$, and this element is trivial if and only if there exists a homomorphism $\Pi \longrightarrow \mathrm{GL}_n(A_1)$ lifting ρ_0. We call $\mathcal{O}(\rho_0)$ the *obstruction class* of ρ_0 relatively to $A_1 \longrightarrow A_0$.

It is to be expected that the deformation theory of unobstructed representations, i.e. when $d_2 = 0$, behaves quiet well. The following theorem due to Mazur shows that this is indeed the case:

Theorem 5.3.1. *Suppose $C(\overline{\rho}) = k$ and let $\mathcal{R} = \mathcal{R}(\Pi, k, \overline{\rho})$ be the universal deformation ring representing the deformation functor $\mathbf{D}_\Lambda$. Let*

$$d_1 = \dim H^1(\Pi, \mathrm{Ad}(\overline{\rho})) \quad \text{and} \quad d_2 = \dim H^2(\Pi, \mathrm{Ad}(\overline{\rho})).$$

Then we have

$$\dim(\mathcal{R}/\mathfrak{m}_\Lambda \mathcal{R}) \geq d_1 - d_2. \tag{5.3.1}$$

Furthermore, if $d_2 = 0$ we have equality in (5.3.1), and in fact

$$\mathcal{R} \cong \Lambda[[X_1, X_2, \ldots, X_{d_1}]]$$

Proof. We already know that there is a surjective homomorphism of coefficient Λ-algebras

$$\Lambda[[X_1, \ldots, X_{d_1}]] \longrightarrow \mathcal{R}$$

which induces an isomorphism on tangent spaces. Reducing modulo the maximal ideal gives a surjective homomorphism

$$k[[X_1, \ldots, X_{d_1}]] \longrightarrow \mathcal{R}/\mathfrak{m}_\Lambda \mathcal{R}$$

which still induces an isomorphism on tangent spaces. Let J be the kernel of this surjection. Write $F = k[[X_1, \ldots, X_{d_1}]]$ and let m_F be its maximal ideal. We have an exact sequence

$$\begin{tikzcd} 0 \arrow[r] & J \arrow[r] & F \arrow[r] & \mathcal{R}/\mathfrak{m}_\Lambda \mathcal{R} \arrow[r] & 0 \end{tikzcd} .$$

What we need to prove is that the minimal number of generators of J is at most d_2, this because the dimension of $\mathcal{R}/\mathfrak{m}_\Lambda \mathcal{R}$ is $d_1 - \text{height}(J)$ and $\text{height}(J)$ is less than or equal to the minimal number of generators. Since $\mathfrak{m}_F J \subset J$, the sequence of k-vector spaces

$$\begin{tikzcd} 0 \arrow[r] & J/\mathfrak{m}_F J \arrow[r] & F/\mathfrak{m}_F J \arrow[r] & \mathcal{R}/\mathfrak{m}_\Lambda \mathcal{R} \arrow[r] & 0 \end{tikzcd}$$

is still exact. Hence the Krull dimension of $\mathcal{R}/\mathfrak{m}_\Lambda \mathcal{R}$ is at least $d_1 - \dim_k(J/\mathfrak{m}_F J)$ because the dimension as k-vector space of $J/\mathfrak{m}_F J$ is the minimal number of generators of J (Nakayama's lemma).

Let $\boldsymbol{\rho}_p$ be the image of the universal deformation $\boldsymbol{\rho}$ under the quotient map $\mathcal{R} \longrightarrow \mathcal{R}/\mathfrak{m}_\Lambda \mathcal{R}$. It is clear that $\boldsymbol{\rho}_p$ is the universal deformation over all the deformations to k-algebras. The construction above gives a cohomology class

$$\mathcal{O}(\boldsymbol{\rho}_p) \in H^2(\Pi, \mathrm{Ad}(\overline{\rho})) \otimes J/\mathfrak{m}_F J$$

which is the obstruction to lifting $\boldsymbol{\rho}_p$ to $F/\mathfrak{m}J$.

Consider the k-linear map

$$\mathrm{Hom}(J/\mathfrak{m}_F J, k) \overset{\alpha}{\to} H^2(\Pi, \mathrm{Ad}(\overline{\rho}))$$

given by

$$f \mapsto (1 \otimes f)(\mathcal{O}(\boldsymbol{\rho}_p)).$$

If we can show that α is injective, then we will have $\dim_k(J/\mathfrak{m}_F J) \leq d_2$ which implies our claim.

To prove injectivity, let f be a nonzero element in the kernel of α, let A be the quotient of $F/\mathfrak{m}_F J$ by the kernel of f and let I be the image of $J/\mathfrak{m}_F J$ in the quotient, so that $I = (J/\mathfrak{m}_F J)/\ker(f) = k$. We get an exact sequence

$$\begin{tikzcd} 0 \arrow[r] & I \arrow[r] & A \arrow[r] & \mathcal{R}/\mathfrak{m}\mathcal{R} \arrow[r] & 0 \end{tikzcd}$$

where I is isomorphic to k and which still induces an isomorphism on tangent spaces. But now the obstruction to lifting $\boldsymbol{\rho}_p$ to A vanishes. Thus we get a deformation of $\overline{\rho}$ to A lifting $\boldsymbol{\rho}_p$. But A is a k-algebra and $\boldsymbol{\rho}_p$ is universal among lifts to such rings, so this lift must be induced by an homomorphism $\mathcal{R}/\mathfrak{m}_\Lambda\mathcal{R} \longrightarrow A$. This means that the sequence splits, but Lemma 1.4 of [Sch68] contradicts this fact [1]. Thus, α is injective proving the inequality.

If $d_2 = 0$, then we can lift a deformation of the universal deformation relatively to

$$\Lambda[[X_1, \ldots, X_{d_1}]] \longrightarrow \mathcal{R}.$$

Universality of $\boldsymbol{\rho}$ shows that the above homomorphism splits and since $\Lambda[[X_1, \ldots, X_{d_1}]] \longrightarrow \mathcal{R}$ is an isomorphism on tangent spaces then the spliting homomorphism $\mathcal{R} \longrightarrow \Lambda[[X_1, \ldots, X_{d_1}]]$ does too. This shows the isomorphism $\Lambda[[X_1, \ldots, X_{d_1}]] \cong \mathcal{R}$.

□

The asertion of the equality in 5.3.1 is known as the *Dimension Conjecture.*

Finally, we will down-to-earth all this machinery in the Galois case for $n = 2$. Let K be a number field, S a finite set of primes containing all primes above p and all primes at infinity. Let $S_\infty \subset S$ be the set of primes at infinity and set $\Pi = G_{K,S}$. Let

$$\overline{\rho} : \Pi \longrightarrow \mathrm{GL}_n(k)$$

5 be a residual representation such that $C(\overline{\rho}) = k$, and let $\mathcal{R}$ be its universal deformation ring. In previous sections we have given a lower bound for the dimension of $\mathcal{R}/\mathfrak{m}_\Lambda\mathcal{R}$ in terms of the dimensions of two cohomology groups, the tool we will use in order to compute the difference $d_1 - d_2$ is the global Euler characteristic formula due to Tate, see [Hid00, Ch. 4] for a proof of the global and local Euler characteristic formula.

Take an extension $K/\mathbb{Q}$ of degree d and let S be a finite set of primes of K containing all primes at infinity. Let M be a finite $G_{K,S}$-module and suppose all primes dividing the order of M are in S. For each prime v of K let K_v be the completion at v, so if v is a prime at infinity then K_v is $\mathbb{R}$ or $\mathbb{C}$. The global Euler characteristic formula states that

$$\frac{|H^0(G_{K,S}, M)||H^2(G_{K,S}, M)|}{|H^1(G_{K,S}, M)|} = \frac{1}{|M|^d} \prod_{v \in S_\infty} |H^0(G_{K_v}, M)|.$$

In our situation M will be $\mathrm{Ad}(\overline{\rho})$, which has order a power of p and S contains all primes dividing p. Then the global Euler characteristic formula in terms of the dimension over k is

$$\begin{aligned} \dim H^0(G_{K,S}, \mathrm{Ad}(\overline{\rho})) - \dim H^1(G_{K,S}, \mathrm{Ad}(\overline{\rho})) + \dim H^2(G_{K,S}, \mathrm{Ad}(\overline{\rho})) = \\ = \sum_{v \in S_\infty} \dim H^0(G_{K_v}, \mathrm{Ad}(\overline{\rho})) - d \dim \mathrm{Ad}(\overline{\rho}). \end{aligned}$$

Write $d_i = \dim H^i(G_{K,S}, \mathrm{Ad}(\overline{\rho}))$ as before. Then the formula becomes

$$d_0 - d_1 + d_2 = \sum_{v \in S_\infty} \dim H^0(G_{K_v}, \mathrm{Ad}(\overline{\rho})) - dn^2$$

and therefore

[1] The argument involves the dimension of the tangent spaces.The dimension of t_A would be grater than the one of $t_{\mathcal{R}}$.

$$d_1 - d_2 = d_0 + dn^2 - \sum_{v \in S_\infty} \dim H^0(G_{K_v}, \mathrm{Ad}(\overline{\rho})).$$

We can compute d_0:

$$H^0(G_{K,S}, \mathrm{Ad}(\overline{\rho})) = (\mathrm{Ad}(\overline{\rho}))^{G_{K,S}} = k,$$

so $d_0 = 1$.

Then we have the following proposition

Proposition 5.3.1. *Let K be a number field of degree d over $\mathbb{Q}$, let $\overline{\rho} : G_{K,S} \longrightarrow \mathrm{GL}_n(k)$ be a residual representation such that $C(\overline{\rho}) = k$, and let $\mathcal{R}$ be its universal deformation ring. Then*

$$\text{Krull } \dim \mathcal{R}/\mathfrak{m}_\Lambda\mathcal{R} \geq 1 + dn^2 - \sum_{v \in S_\infty} \dim H^0(G_{K_v}, \mathrm{Ad}(\overline{\rho})). \tag{5.3.2}$$

We have already computed the case $n = 1$, i.e. when $\overline{\rho}$ is a character. We showed that

$$\mathcal{R} = \Lambda[[G_{K,S}^{ab,p}]].$$

Notice that

$$\mathcal{R}/\mathfrak{m}_\Lambda\mathcal{R} = k[[G_{K,S}^{ab,p}]],$$

so the Krull dimension of this ring is equal to the rank of $G_{K,S}^{ab,(p)}$ as a $\mathbb{Z}_p$-module, or equivalently, the rank of $\mathrm{Hom}(G_{K,S}, \mathbb{Z}_p)$ as $\mathbb{Z}_p$-module.

On the other hand, the formula above shows that the Krull dimension is at least $1 + r_2$, where r_2 is the number of complex primes of K. So we have shown that

$$\text{rank }_{\mathbb{Z}_p} \mathrm{Hom}(G_{K,S}, \mathbb{Z}_p) \geq 1 + r_2.$$

The assertion that these two numbers are equal is equivalent to the *Leopoldt Conjecture* for the field K. See Appendix C.

The next case we want to check is the one related to modular forms and elliptic curves: $n = 2$, p an odd prime, $K = \mathbb{Q}$, S containing p and ∞. In this case G_∞ is a group if order two generated by a complex conjugation σ. Since $\sigma^2 = 1$ and p is odd, $\overline{\rho}(\sigma)$ is a matrix of order 2 in $\mathrm{GL}_2(k)$, and hence we must have

$$\overline{\rho}(\sigma) \sim \pm \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \qquad \text{or} \qquad \overline{\rho}(\sigma) \sim \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

In the first case $\det \overline{\rho} = 1$, and we call $\overline{\rho}$ an *even* representation. In the second, $\det \overline{\rho} = -1$ and we say $\overline{\rho}$ is *odd.*

Now its easy to compute the dimension d_0 of $H^0(G_\infty, \mathrm{Ad}(\overline{\rho}))$. If $\overline{\rho}$ is even, then $\overline{\rho}$ is an scalar matrix and hence the action of G_∞ on $\mathrm{Ad}(\overline{\rho})$ is trivial, so $d_0 = 4$. If $\overline{\rho}$ is odd, then

$$\begin{aligned} \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} &= \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \\ \begin{pmatrix} a & b \\ -c & -d \end{pmatrix} &= \begin{pmatrix} a & -b \\ c & -d \end{pmatrix}. \end{aligned}$$

Hence $c = b = 0$ and $d_0 = 2$. Putting all together we have

Proposition 5.3.2. *Let p be an odd prime, let S be a set of rational primes including p and ∞, let $\overline{\rho} : G_{\mathbb{Q},S} \longrightarrow \mathrm{GL}_2(k)$ be a residual representation satisfying $C(\overline{\rho}) = k$, and let $\mathcal{R}$ be the universal deformation ring of $\overline{\rho}$. Then:*

- *if $\overline{\rho}$ is even, then* Krull dim $\mathcal{R}/\mathfrak{m}_\Lambda\mathcal{R} \geq 1$*, and*
- *if $\overline{\rho}$ is odd, then* Krull dim $\mathcal{R}/\mathfrak{m}_\Lambda\mathcal{R} \geq 3$*.*

Finally, we will use the local Euler characteristic formula to compute $d_1 - d_2$ in the local case. Let K be a finite extension of $\mathbb{Q}_p$ of order d and let M be a G_K-module of order m. Then

$$\frac{|H^0(G_K, M)||H^2(G_K, M)|}{|H^1(G_K, M)|} = p^{-dv_p(m)}$$

where v_p is the p-adic valuation in $\mathbb{Q}$. We will put $M = \mathrm{Ad}(\overline{\rho})$, denote $d_i = \dim_k H^i(G_K, \mathrm{Ad}(\overline{\rho}))$, the formula rewrites in dimensions as

$$d_0 - d_1 + d_2 = -dn^2.$$

If $C(\overline{\rho}) = k$ then $d_0 = 1$ and

$$d_1 - d_2 = 1 + dn^2.$$

Chapter 6

Explicit deformations

So far we have only determined the deformation ring and the universal deformation for characters. Throughout this chapter we will try to say more about $\mathcal{R}$, particularly in the tame case of Galois representations.

6.1 Some group theory

Just like in previous sections, let S be a finite set of primes of $\mathbb{Q}$ including p and ∞. Let $\mathbb{Q}_S$ be the maximal extension of $\mathbb{Q}$ unramified outside S, $\Pi = G_{\mathbb{Q},S}$ be the Galois group of $\mathbb{Q}_S$ over $\mathbb{Q}$ and $\overline{\rho} : \Pi \longrightarrow \mathrm{GL}_n(k)$ be a residual representation such that $C(\overline{\rho}) = k$.

Let Π_0 be the kernel of $\overline{\rho}$ and K be its fixed field. We have a tower of fields

$$\begin{tikzcd}
\mathbb{Q}_S \arrow[d, dash] \arrow[d, bend left, dash, "\Pi_0"] \arrow[dd, bend right=60, dash, "\Pi"'] \\
K \arrow[d, dash] \arrow[d, bend left, dash, "\Pi/\Pi_0 \cong \mathrm{Im}(\overline{\rho})"] \\
\mathbb{Q}
\end{tikzcd}$$

Let S_1 be the primes of K above S. Let $\boldsymbol{\rho} : \Pi \longrightarrow \mathrm{GL}_n(\mathcal{R})$ be the universal deformation of $\overline{\rho}$. Thus, the restriction of $\boldsymbol{\rho}$ to Π_0 gives an homomorphism $\Pi_0 \longrightarrow \Gamma_n(\mathcal{R})$. Since $\Gamma_n(A)$ is a pro-p-group for every coefficient ring A, $\Pi \longrightarrow \Gamma_n(\mathcal{R})$ factorizes through the pro-p-completion of Π_0. Therefore, let L be the maximal p-extension of K unramified outside S_1, denote the Galois group of L over $\mathbb{Q}$ by $\tilde{\Pi}$. We have shown that the universal deformation $\boldsymbol{\rho}$ factors through $\tilde{\Pi}$ and hence every deformation must factor through $\tilde{\Pi}$. We call $\tilde{\Pi}$ the *pro-p-completion of* Π *relatively to* $\overline{\rho}$. We can replace Π by $\tilde{\Pi}$ for the deformation theory of $\overline{\rho}$. Let P be the kernel of $\overline{\rho} : \tilde{\Pi} \longrightarrow \mathrm{GL}_n(k)$, so P is a pro-p-group and we get the exact sequence

$$\begin{tikzcd}
1 \arrow[r] & P \arrow[r] & \Pi \arrow[r] & \mathrm{Im}(\overline{\rho}) \arrow[r] & 1 .
\end{tikzcd}$$

Definition 6.1.1. We say that a residual representation $\overline{\rho}$ is tame if the order of $\mathrm{Im}(\overline{\rho})$ is not divisible by p.

Before considering a more general case we will study the tame representations, for this we must introduce some results in group theory.

Theorem 6.1.1 (Schur-Zassenhaus)**.** *Let G be a profinite group with normal pro-p-Sylow subgroup P of finite index in G. Let $\pi : G \longrightarrow G/P$ be the projection on the quotient. Then G contains a subgroup A such that π induces an isomorphism of A onto G/P. Furthermore, any two subgroups with this property are conjugated by an element of P.*

See [Rob96, Ch. 9]. The original statement is more general but this is enough for our purposes in the theory. An immediate consequence of this theorem is the following:

Proposition 6.1.1. *Let A be a finite group whose order is not divisible by p and let $\overline{\rho} : A \longrightarrow \mathrm{GL}_n(k)$ be a faithful residual representation such that $C(\overline{\rho}) = k$. Then Λ is the deformation ring of $\mathbf{D}_\Lambda$ and the unique lifting of $\overline{\rho}$ to $\mathrm{GL}_n(\Lambda)$ is the universal deformation of $\overline{\rho}$.*

The Schur-Zassenhaus theorem also implies that G is the semidirect product of P and G/P. If P is topologically finitely generated denote by $d(P)$ the minimal number of generators of P, it is called the *generator rank*. The kernel of the map from the free pro-p-group on $d(P)$ generators is still a pro-p-group which is finitely generated. The minimal number of generators of the kernel is called the *relation rank* and is denoted by $r(P)$.

The Burnside Basis Theorem shows that $d(P)$ is the dimension over $\mathbb{F}_p$ of the p-Frattini quotient $\overline{P} = \mathrm{Fr}(P)$ of P. Indeed, a section of a generator set of $\overline{P}$ is a generator set of P.

Boston improved this theorem for the case we are concern with, see [Bos91].

Theorem 6.1.2. *Let G be a profinite group with normal pro-p-Sylow subgroup P of finite index in G, and let A be a subgroup of G mapping isomorphically to G/P. Let A act on P and on $\overline{P}$ by conjugation. If $\overline{V}$ is an $\mathbb{F}_p[A]$-module of $\overline{P}$, then there exist an A-invariant subgroup V of P with $\dim_{\mathbb{F}_p} \overline{V}$ generators which maps onto $\overline{V}$ under π.*

In the case we are dealing with, the Galois case, one can give explicitly $d(P)$ and $r(P)$ in terms of number theoretic objects, see [CR01, pg. 295] for the formulas and some references. Even more, there is an exact sequence which helps to describe the structure of $\overline{P}$ as an $k[H]$-module, where $H = \mathrm{Im}(\overline{\rho})$.

Let Z_S be the set of non zero elements $x \in K$ such that the fractional ideal (x) is a p-th power and such that x is a p-th power in each completion K_v of K for $v \in S_1$. Both groups Z_S and $(K^*)^p$ are stable under the Galois group H. $Z_S/(K^*)^p$ is a $\mathbb{F}_p[H]$-modulo denoted by B_S. Let $\overline{E}$ be the units of K modulo p-th powers, and let $\overline{E}_v$ denote the group of units in K_v modulo p-th powers. If the class number of K is prime to p we deduce from global class field theory the existence of an exact sequence of $\mathbb{F}_p[H]$-modules

$$0 \longrightarrow B_s \longrightarrow \overline{E} \longrightarrow \bigoplus_{v \in S_1} \overline{E}_v \longrightarrow \overline{P} \longrightarrow 0$$

which give us the next theorem:

Theorem 6.1.3 (Boston-Mazur)**.** *For each rational prime ℓ, let H_ℓ be the decomposition subgroup of H at ℓ, and let H_∞ be the subgroup of H generated by a complex conjugation. Let $\mu_p(K)$ be the group of p-th roots of unity in K. If H has order prime to p, then we have the following isomorphisms of $\mathbb{F}_p[H]$ modules:*

$$\bigoplus_{v \in S_1} \overline{E}_v \cong \mathbb{F}_p[H] \oplus \left(\bigoplus_{\ell \in S} \mathrm{Ind}_{H_\ell}^H \mu_p \right)$$

$$\overline{E} \oplus \mathbb{F}_p \cong \mu_p \oplus \mathrm{Ind}_{H_\infty}^H \mathbb{F}_p.$$

A proof is found in [BM89]. We say an H-module is *prime to adjoint* if it does not have common factors with the adjoint representation. The importance on describing explicitly $\overline{P}$ lies in the relation among deforming representations and the adjoint representation $\mathrm{Ad}(\overline{\rho})$. Indeed, let

$$K_r = \ker\left(\Gamma_n(R) \longrightarrow \Gamma_n(R/\mathfrak{m}_R^r)\right),$$

then K_{r-1}/K_r is a $\mathbb{F}[H]$-module isomorphic to a multiple of the adjoint representation provided the order of H is prime to p.

6.2 Tame representations

Now we discuss the case when our residual representation $\overline{\rho}$ is tame. Consider $\tilde{\Pi}$ to be the pro-p-completion of Π relatively to $\overline{\rho}$. Making an abuse of language we can write $\overline{\rho} : \tilde{\Pi} \longrightarrow \mathrm{GL}_n(k)$. Let P be the kernel of $\overline{\rho}$, then P is a pro-p-group and since $\overline{\rho}$ is tame, by Schur Zassenhaus theorem, $\tilde{\Pi}$ is the semidirect product $P \rtimes A$ where A is some lifting of $H = \mathrm{Im}(\overline{\rho})$ to $\tilde{\Pi}$ (recall that two of such liftings are conjugated by an element in P).

Recall also that for any coefficient ring R the group $\Gamma_n(R)$ is a p-group. Let $\pi : \mathrm{GL}_n(R) \longrightarrow \mathrm{GL}_n(k)$ be the canonical projection, then $\pi^{-1}(H)$ splits as a semidirect product of $\Gamma_n(R)$ and H. This proves that H has a section in $\mathrm{GL}_n(R)$ and even more, that two of such sections are conjugated by an element in $\Gamma_n(R)$. In particular if we take $R = W(k)$, we obtain a inclusion $\sigma : A \cong H \longrightarrow \mathrm{GL}_n(W(k))$ which induces a representation

$$\sigma_1 : \tilde{\Pi} \longrightarrow \mathrm{GL}_n(W(k)).$$

It is clear that if we change the lifting of A the representation σ_1 differs by a conjugation of an element in $\Gamma_n(W(k))$. Let's fix σ and therefore σ_1, recall that every coefficient ring admits a unique structure of $W(k)$-algebra, composing with σ_1 we get representations $\sigma_R : \tilde{\Pi} \longrightarrow \mathrm{GL}_n(R)$ commuting with coefficient ring homomorphisms, i.e. for $\varphi : R \longrightarrow R'$ we have

$$\varphi \circ \sigma_R = \sigma'_R.$$

Then $\Gamma_n(R)$ has an action of A by conjugation via σ_R.

Define the functor $\mathbf{E}_{\overline{\rho}}$ on $\mathcal{C}$ by imposing

$$\mathbf{E}_{\overline{\rho}}(R) = \mathrm{Hom}_A(P, \Gamma_n(R)),$$

where $\mathrm{Hom}_A(P, \Gamma_n(R))$ denotes the set of continuous homomorphisms from P to $\Gamma_n(R)$ which commute with the A-action. Note that an element in $\gamma \in \mathrm{Hom}_A(P, \Gamma_n(R))$ gives a representation $\tilde{\Pi} \longrightarrow \mathrm{GL}_n(R)$ by

$$\gamma \rtimes \sigma_R : \tilde{\Pi} \cong P \rtimes A \longrightarrow \mathrm{GL}_n(R).$$

Theorem 6.2.1 (Boston)**.** *The functor $\mathbf{E}_{\overline{\rho}}$ is always representable. Furthermore,*

i. If $C(\overline{\rho}) = k$, the natural morphism of functors $\mathbf{E}_{\overline{\rho}} \longrightarrow \mathbf{D}_{\overline{\rho}}$ is an isomorphism.

ii. Otherwise, the morphism is smooth and induces an isomorphism on tangent spaces (is a hull of $\mathbf{D}_{\overline{\rho}}$).

Proof. First, we'll prove that $\mathbf{E}_{\overline{\rho}}$ is representable, then (ii) implies (i) since the condition $C(\overline{\rho}) = k$ implies that $\mathbf{D}_{\overline{\rho}}$ is representable. Nevertheless, we will give a direct proof of (i).

Choose generators $x_1, x_2, \ldots, x_d$ of P. The image of x_r in $\Gamma_n(R)$ is a matrix of the form

$$\begin{pmatrix} 1 + m_{11}^{(r)} & m_{12}^{(r)} & \cdots & m_{1n}^{(r)} \\ m_{21}^{(r)} & 1 + m_{22}^{(r)} & \cdots & m_{2n}^{(r)} \\ \cdots & & & \cdots \\ m_{n1}^{(r)} & m_{n2}^{(r)} & \cdots & 1 + m_{nn}^{(r)} \end{pmatrix}$$

where the $m_{ij}^{(r)}$ belong to $\mathfrak{m}_R$.

Consider the power series ring $W(k)[[T_{ij}^{(r)} : 1 \leq i, j \leq n, 1 \leq r \leq d]]$. Let $\mathcal{F}$ be the free pro-p-group on $x_1, \ldots, x_d$, so we get an exact sequence

$$\begin{tikzcd} 1 \arrow[r] & N \arrow[r] & \mathcal{F} \arrow[r] & P \arrow[r] & 1 \end{tikzcd} .$$

A continuous homomorphism from P to $\Gamma_n(R)$ is equivalent to a homomorphism from $\mathcal{F}$ to $\Gamma_n(R)$ such that N vanishes. Define a homomorphism from $\mathcal{F}$ to $\Gamma_n(W(k)[[T_{i,j}^{(r)}]])$ by sending x_r to

$$\left(\begin{array}{cccc} 1+T_{11}^{(r)} & T_{12}^{(r)} & \cdots & T_{1n}^{(r)} \\ T_{21}^{(r)} & 1+T_{22}^{(r)} & \cdots & T_{2n}^{(r)} \\ \cdots & & & \cdots \\ T_{n1}^{(r)} & T_{n2}^{(r)} & \cdots & 1+T_{nn}^{(r)} \end{array} \right) .$$

If we impose N to be in the kernel and the homomorphism to commute with the action of A, then we get a family of equations involving the variables $T_{ij}^{(r)}$. Let I be the closed ideal generated by all these equations. If we set $\mathcal{R} = W(k)[[T_{ij}^{(r)}]]/I$, we have a well defined homomorphism $\phi : P \longrightarrow \Gamma_n(\mathcal{R})$. It is easy to check that it is the universal representation and that $\mathcal{R}$ represents $\mathbf{E}_{\overline{\rho}}$.

Now we proceed to prove (i), let R be a coefficient ring and suppose $C(\overline{\rho}) = k$. We want to show that

$$\mathbf{E}_{\overline{\rho}}(R) \longrightarrow \mathbf{D}_{\overline{\rho}}(R)$$

is a bijection.

Surjectivity; let ρ be a deformation of $\overline{\rho}$ to R. Then ρ induces a lift of $A \longrightarrow \mathrm{GL}_n(R)$. Since all such liftings are conjugate by elements of $\Gamma_n(R)$, we can choose a homomorphism ψ in the strict equivalent class of ρ such that $\psi|_A = \sigma_R$. Then $\psi|_P$ is an element of $\mathbf{E}_{\overline{\rho}}(R)$ which maps to ρ.

Injectivity; suppose ϕ_1 and ϕ_2 produce strictly equivalent lifts ψ_1 and ψ_2 of $\overline{\rho}$. Since both ψ_1 and ψ_2 induce σ_R in A, the matrix realizing the strict equivalence must be an element in $\Gamma_n(R)$ acting trivially on A. Since $C(\overline{\rho}) = k$ then the matrices in $\Gamma_n(A)$ commuting with A are scalars. Hence they also act trivially by conjugation and $\psi_1 = \psi_2$ showing that $\phi_1 = \phi_2$.

Finally, we are going to prove (ii). To prove smoothness consider a surjective morphism $\varphi : R_2 \longrightarrow R_1$ of artinian coefficient rings. Since we can factor φ as a composition of small homomorphisms, it is enough to check the result for φ small. Suppose φ small and let $(f) = \ker \varphi$. We get the following diagram

$$\begin{tikzcd} \mathbf{E}_{\overline{\rho}}(R_2) \arrow[r] \arrow[d] & \mathbf{D}_{\overline{\rho}}(R_2) \arrow[d] \\ \mathbf{E}_{\overline{\rho}}(R_1) \arrow[r] & \mathbf{D}_{\overline{\rho}}(R_1) \end{tikzcd}$$

Let $\phi_1 \in \mathbf{E}_{\overline{\rho}}(R_1)$ and $\rho_2 \in \mathbf{D}_{\overline{\rho}}(R_2)$ be two elements such that they reduce to the same representation $\rho_1 \in \mathbf{D}_{\overline{\rho}}(R_1)$. Then, choosing a representation ψ_2 in the class of ρ, we may assume that the reduction of ψ_2 to R_1 is exactly $\phi_1 \rtimes \sigma_{R_1}$. We want an element in $\mathbf{E}_{\overline{\rho}}(R_2)$ which reduces to ρ_2 and ϕ_1. The restriction of ψ_2 to A has the form

$$\psi_2(a) = (1 + f b_a)\sigma_{R_2}(a), \quad a \in A.$$

Note that the conditions of ψ_2 to be a homomorphism and b_a to be a 1-cocicle in $\mathrm{Ad}(\overline{\rho})$ are equivalent. Since $p \nmid |A|$ then $H^1(A, \mathrm{Ad}(\overline{\rho})) = 0$ and there exist $M \in M_n(k)$ such that

$$b_a = M - \overline{\rho}(a) M \overline{\rho}(a)^{-1}.$$

Therefore if we conjugate ψ_2 by $1-fM$ we get a strict equivalent representation $\tilde{\psi_2}$ reducing to ψ_1 in R_1 such that the restriction to A is exactly σ_{R_2}. Hence the restriction of $\tilde{\psi_2}$ to P gives the desired element in $\mathbf{E}_{\overline{\rho}}(R_2)$.

To prove that it is an isomorphism on tangent spaces is the same as to show that

$$\mathbf{E}_{\overline{\rho}}(k[\epsilon]) \longrightarrow \mathbf{D}_{\overline{\rho}}(k[\epsilon])$$

is a bijection since the vector space structure in both cases is defined by the same maps. Surjectivity comes from the smoothness taking $R_2 = k[\epsilon]$ and $R_1 = k$. To prove injectivity note that we are considering homomorphisms $\phi : P \longrightarrow \Gamma_n(k[\epsilon]) = 1 + \epsilon \operatorname{Ad}(\overline{\rho})$. Then the only conjugate of ϕ by an element in $\Gamma_n(k[\epsilon])$ is itself proving the claim.

□

Chapter 7

Imposing conditions to deformations

We will follow the same notation as in the last chapters. To understand the universal deformation ring is not in general an easy challenge. The previous chapter gave us a way to construct that ring in the tame case, but we easily find some difficulties in this treatment, for instance, the group P is not in general easy to describe.

On the other hand, we are not always concerned with all deformations of a given residual representation. For example, conditions as modularity, semistability or fixed determinant are important in the proof of Fermat's Last Theorem and they play a role in the representation type. All this together motivates the notion of *deformation condition* first considered by Mazur in [Maz89].

7.1 Deformation conditions

Given a condition $\mathcal{Q}$ for deformations of $\overline{\rho}$ we would want to construct a functor attaching each coefficient ring R the set of deformations of $\overline{\rho}$ to R for which $\mathcal{Q}$ holds. Then the assignment

$$R \longrightarrow \{\text{deformations of } \overline{\rho} \text{ satisfying } \mathcal{Q}\}.$$

will be a subfunctor of $\mathbf{D}_{\overline{\rho}}$. We also want this functor to be representable if $\mathbf{D}_{\overline{\rho}}$ is so, here the notion of being *relatively representable* introduced in Chapter 4 is the vital one.

Before defining deformation condition, let's give some language. Let R and R' be artinian coefficient Λ-algebras. If we are given a deformation $\alpha : \Pi \longrightarrow \mathrm{GL}_n(R)$ and a homomorphism of coefficient Λ-algebras $\alpha : R \longrightarrow R'$ we get an induced deformation $\Pi \longrightarrow \mathrm{GL}_n(R')$ by composing ρ with α. We denote this deformation by $\alpha_*\rho$ and call it the *push-forward* of ρ by α.

Recall that a representation ρ of Π over a coefficient ring R of dimension n is the same as a free R-module M of rank n with a continuous action of Π. The push-forward of a representation would be the tensor product $M \otimes_R R'$, where the R-module structure is given by α. The residual representation corresponds to $V_{\overline{\rho}}$. Deformations are just isomorphism clases of Γ-modules (free of rank n w.r.t. R) over $V_{\overline{\rho}}$.

Definition 7.1.1. Let $\overline{\rho}$ be a residual representation of dimension n. A deformation condition on deformations of $\overline{\rho}$ is a property $\mathcal{Q}$ of n-dimensional (as free R-module) representations of Π defined over artinian coefficient Λ-algebras which satisfies the following conditions:

i. The residual representation $\overline{\rho}$ has property $\mathcal{Q}$.

ii. Given a deformation $\rho : \Pi \longrightarrow \mathrm{GL}_n(R)$ of $\overline{\rho}$ and a homomorphism of coefficient Λ-algebras $\alpha : R \longrightarrow R'$, if ρ has the property, then the push-forward $\alpha_*\rho$ also does.

iii. Let

$$\begin{tikzcd} & R_1 \times_{R_0} R_2 \arrow[dl, "p"'] \arrow[dr, "q"] & \\ R_1 \arrow[dr, "\alpha"'] & & R_2 \arrow[dl, "\beta"] \\ & R_0 & \end{tikzcd}$$

be a fiber product in $\mathcal{C}^0_\Lambda$, and let

$$\rho : \Pi \longrightarrow \mathrm{GL}_n(R_1 \times_{R_0} R_2)$$

be a deformation of $\overline{\rho}$. Then ρ has the property $\mathcal{Q}$ if and only if both $q_*\rho$ and $p_*\rho$ have property $\mathcal{Q}$.

iv. Let $\alpha : R \longrightarrow R'$ be an injective homomorphism of coefficient Λ-algebras and let $\rho : \Pi \longrightarrow \mathrm{GL}_n(R)$ be a deformation of $\overline{\rho}$. If $\alpha_*\rho$ has property $\mathcal{Q}$ then so does ρ.

Remark. Condition iv is a consequence of conditions ii and iii. This is shown in Lecture 6 of Galois Representations by Fernando Gouvêa, [CR01].

Definition 7.1.2. Let $\mathcal{Q}$ be a deformation condition for $\overline{\rho}$. We define a functor

$$\mathbf{D}_{\mathcal{Q}} : \mathcal{C}^{\mathbf{0}}_{\mathbf{\Lambda}} \longrightarrow \text{ Sets}$$

by setting, for each artinian coefficient Λ-algebra R,

$$\mathbf{D}_{\mathcal{Q}}(R) = \{\text{deformations of } \overline{\rho} \text{ to } R \text{ which satisfy property } \mathcal{Q}\}.$$

We can then extend $\mathcal{D}_{\mathcal{Q}}$ to all $\mathcal{C}_\Lambda$ by continuity: If R is a coefficient Λ-algebra,

$$\mathbf{D}_{\mathcal{Q}}(R) = \varprojlim_k \mathbf{D}_{\mathcal{Q}}(R/\mathfrak{m}^k).$$

Condition i causes $\mathbf{D}_{\mathcal{Q}}$ to be non-empty, whereas condition ii implies the functorial property.

Theorem 7.1.1. *If $\mathcal{Q}$ is a deformation condition for $\overline{\rho}$, then $\mathbf{D}_{\mathcal{Q}}$ satisfies conditions $\mathbf{H_1}$, $\mathbf{H_2}$ and $\mathbf{H_3}$ in Schlessinger's theorem. If $C(\overline{\rho}) = k$, then $\mathbf{D}_{\mathcal{Q}}$ also satisfies property $\mathbf{H_4}$ and therefore is representable by a ring $\mathcal{R}_{\mathcal{Q}}$ which is a quotient of the universal deformation ring $\mathcal{R}(\overline{\rho})$.*

Proof. It is enough to prove that $\mathbf{D}_{\mathcal{Q}} \subset \mathbf{D}_{\overline{\rho}}$ is relatively representable. Let

$$\begin{tikzcd} & R_1 \times_{R_0} R_2 \arrow[dl, "p"'] \arrow[dr, "q"] & \\ R_1 \arrow[dr, "\alpha"'] & & R_2 \arrow[dl, "\beta"] \\ & R_0 & \end{tikzcd}$$

be a fiber product in $\mathcal{C}^0_\Lambda$. We have to show that the following square is cartesian

$$\begin{tikzcd}
\mathbf{D}_{\mathcal{Q}}(R_1 \times_{R_0} R_2) \arrow[r] \arrow[d] & \mathbf{D}_{\mathcal{Q}}(R_1) \times_{\mathbf{D}_{\mathcal{Q}}(R_0)} \mathbf{D}_{\mathcal{Q}}(R_2) \arrow[d] \\
\mathbf{D}_{\overline{\rho}}(R_1 \times_{R_0} R_2) \arrow[r] & \mathbf{D}_{\overline{\rho}}(R_1)_{\mathbf{D}_{\overline{\rho}}(R_0)} \mathbf{D}_{\overline{\rho}}(R_2)
\end{tikzcd}$$

Let ρ be a deformation of $\overline{\rho}$ to $R_1 \times_{R_0} \times R_2$ and let (ρ_1, ρ_2) be an element of $\mathbf{D}_{\mathcal{Q}}(R_1) \times_{\mathbf{D}_{\mathcal{Q}}(R_0)} \mathbf{D}_{\mathcal{Q}}(R_2)$ such that

$$p_* \rho = \rho_1 \text{ and } q_* \rho = \rho_2.$$

Condition iii. implies that ρ has the property $\mathcal{Q}$ and therefore it is in $\mathbf{D}_{\mathcal{Q}}(R_1 \times_{R_0} R_2)$. Since all vertical maps are inclusions we get that the square is cartesian.

□

Suppose we have a deformation condition $\mathcal{Q}$. We consider the inclusion of tangent spaces

$$\mathbf{D}_{\mathcal{Q}}(k[\epsilon]) \subset \mathbf{D}_{\overline{\rho}}(k[\epsilon]) \cong H^1(\Pi, \mathrm{Ad}(\overline{\rho})).$$

Definition 7.1.3. We define $H^1_{\mathcal{Q}}(\Pi, Ad(\overline{\rho}))$, to be the subspace of $H^1(\Pi, \mathrm{Ad}(\overline{\rho}))$ corresponding to $\mathbf{D}_{\mathcal{Q}}(k[\epsilon])$.

7.2 Examples of deformation conditions

In this section we will give some examples of deformation conditions.

Fixed determinant

Definition 7.2.1. Let δ be a continuous homomorphism

$$\delta : \Pi \longrightarrow \Lambda^*$$

and for every coefficient Λ-algebra R let δ_R be the composition

$$\delta_R : \Pi \longrightarrow \Lambda^* \longrightarrow R^*.$$

We say a deformation ρ of $\overline{\rho}$ to R has determinant δ if $\det \rho = \delta_R$.

Lemma 7.2.1. *Suppose $\overline{\rho}$ has determinant δ. Then "*$\det = \delta$*" is a deformation condition.*

Proof. Conditions i. and ii. in Definition 7.1.1 clearly hold. We only have to check condition iii. Consider a fiber product as in Definition 7.1.1 and let ρ be a deformation of $\overline{\rho}$ to $R_1 \times_{R_0} R_2$ such that $p_* \rho$ and $q_* \rho$ have determinant δ. Therefore $p_* \det \rho = \delta_{R_1}$ and $q_* \det \rho = \delta R_2$ and since taking units preserves fiber products

$$\det \rho = \delta_{R_1 \times_{R_0} R_2}.$$

□

In the case of fixed determinant it is not difficult to describe the tangent space $H^1_{\mathcal{Q}}(\Pi, \mathrm{Ad}(\overline{\rho}))$.

Lemma 7.2.2. *Let n be the dimension of $\overline{\rho}$. Let $\mathrm{Ad}^0(\overline{\rho})$ be the sub Π-module consisting of the matrices of $\mathrm{Ad}(\overline{\rho})$ with trace 0. If $p \nmid n$ then the inclusion $\mathrm{Ad}^0(\overline{\rho}) \longrightarrow \mathrm{Ad}(\overline{\rho})$ induces an isomorphism*

$$H^1(\Pi, \mathrm{Ad}^0(\overline{\rho})) \longrightarrow H^1_{\det=\delta}(\Pi, \mathrm{Ad}(\overline{\rho})) \subset H^1(\Pi, \mathrm{Ad}(\overline{\rho})).$$

If $p|n$, then the homomorphism in cohomology $H^1(\Pi, \mathrm{Ad}^0(\overline{\rho})) \longrightarrow H^1(\Pi, \mathrm{Ad}(\overline{\rho}))$ still surjects onto $H^1_{\det=\delta}(\Pi, \mathrm{Ad}(\overline{\rho}))$.

Proof. First recall that the connection between deformations to $k[\epsilon]$ and elements of $H^1(\Pi, \mathrm{Ad}(\overline{\rho}))$ is given by

$$\rho(g) = (1 + \epsilon b_g)\overline{\rho}(g).$$

The following square commutes

$$\begin{tikzcd}
1 + \epsilon\,\mathrm{M}_n(k) \arrow[r] \arrow[d, "\det"] & \mathrm{M}_n(k) \arrow[d, "\mathrm{Tr}"] \\
1 + \epsilon k \arrow[r] & k
\end{tikzcd}$$

Taking determinants we get

$$\begin{aligned}
\det \rho(g) &= \det((1 + \epsilon b_g)\overline{\rho}(g)) \\
\delta_{k[\epsilon]}(g) &= \det((1 + \epsilon b_g))\delta_k(g) \\
\delta(g) &= \det((1 + \epsilon b_g))\delta(g) \\
1 &= \det(1 + \epsilon b_g).
\end{aligned}$$

This shows that $\mathrm{Tr}(b_g) = 0$ and that the cocycle comes from $\mathrm{Ad}^0(\overline{\rho})$. The same computation proves that cocycles of $\mathrm{Ad}^0(\overline{\rho})$ induce deformations with determinant δ, hence the induced map surjects onto $H^1_{\det=\delta}(\Pi, \mathrm{Ad}(\overline{\rho}))$.

Suppose $p \nmid n$, then $\mathrm{Ad}(\overline{\rho}) = \mathrm{Ad}^0(\overline{\rho}) \oplus k\,\mathrm{Id}$ and hence

$$H^1(\Pi, \mathrm{Ad}(\overline{\rho})) = H^1(\Pi, \mathrm{Ad}^0(\overline{\rho})) \oplus H^1(\Pi, k\,\mathrm{Id})$$

and the map $H^1(\Pi, \mathrm{Ad}^0(\overline{\rho})) \longrightarrow H^1(\Pi, \mathrm{Ad}^0(\overline{\rho}))$ is actually an inclusion.

□

Let $\Lambda[[\Gamma]]$ be the universal deformation ring of the trivial character and let $\boldsymbol{\epsilon}$ be the universal deformation. Now suppose that $C(\overline{\rho}) = k$, the universal deformation ring $\mathcal{R}_{\det=\delta}$ of the functor $\mathbf{D}_{\det=\delta}$ is a quotient of $\mathcal{R}_{\overline{\rho}}$. Nevertheless, we can recover $\mathcal{R}_{\overline{\rho}}$ provide we know $\mathcal{R}_{\det=\delta}$ and $p \nmid n$, indeed,

$$\mathcal{R}_{\overline{\rho}} = \mathcal{R}_{\det=\delta} \hat{\otimes}_{\Lambda} \Lambda[[\Gamma]]$$

and, if we denote the universal deformation with determinant δ by $\boldsymbol{\rho}_\delta$, then

$$\boldsymbol{\rho} = \boldsymbol{\rho}_\delta \otimes \boldsymbol{\epsilon}.$$

Let ρ be a deformation of $\overline{\rho}$ to R, then $\theta = (\delta_R)^{-1} \det \rho$ factorizes through

$$\begin{tikzcd}
\Pi \arrow[r] \arrow[dr] & 1 + \mathfrak{m}_R \arrow[d] \\
 & R^*
\end{tikzcd}$$

Since $1+\mathfrak{m}_R$ is an abelian pro-p-group, multiplication by n is an automorphism and $\theta^{1/n}$ is a continuous homomorphism from Π to $1+\mathfrak{m}_R$. Let $\varphi : \Lambda[[\Gamma]] \longrightarrow R$ be the morphism such that

$$\theta^{1/n} = \varphi_* \boldsymbol{\epsilon}.$$

Consider the deformation

$$\rho' = \theta^{-1/n}\rho,$$

therefore $\det \rho' = \theta^{-1}(\det \rho) = \delta_R$ and it is a deformation of $\overline{\rho}$ with determinant δ. By universality, there exists a morphism $\psi : \mathcal{R}_{\det=\delta} \longrightarrow R$ with

$$\rho' = \psi_* \boldsymbol{\rho}_\delta.$$

Then we may construct $\psi \otimes \varphi : \mathcal{R}_{\det=\delta} \hat{\otimes}_\Lambda \Lambda[[\Gamma]] \longrightarrow R$ and in this case

$$(\psi \otimes \varphi)_*(\boldsymbol{\rho}_\delta \otimes \boldsymbol{\epsilon}) = (\psi_* \boldsymbol{\rho}_\delta)(\varphi_* \boldsymbol{\epsilon}) = \rho' \theta^{1/n} = \rho.$$

The coefficient Λ-algebra homomorphism is unique as can be seen from the canonical maps $\mathcal{R}_{\det=\delta} \longrightarrow \mathcal{R}_{\det=\delta} \hat{\otimes}_\Lambda \Lambda[[\Gamma]]$ and $\Lambda[[\Gamma]] \longrightarrow \mathcal{R}_{\det=\delta} \hat{\otimes}_\Lambda \Lambda[[\Gamma]]$. This proves the claim.

Categorical deformation conditions

Another important class of deformation conditions comes from the categorical point of view, indeed, we can regard the representations of Π on a coefficient ring R as $\Lambda[[\Pi]]$ modules free over R. Moreover, we can restric to working with artinian coefficient Λ-algebras, so the module of the representation will be of finite length with respect to Λ. This motivates to consider the category of all Λ-modules of finite length with a continuous action of Π. Let $\mathcal{P}$ be a full subcategory closed under sub-objects, quotients and finite direct sums.

We say that a deformation of $\overline{\rho}$ to a artinian coefficient Λ-algebra *is of type* $\mathcal{P}$ if the related module is in $\mathcal{P}$, note that it does not depend on the lift.

Theorem 7.2.1 (Ramakrishna)**.** *Suppose $\overline{\rho}$ is of type $\mathcal{P}$. The condition of "being of type $\mathcal{P}$" is a deformation condition.*

Proof. We need to prove conditions *ii.* and *iii.*, that is, "being of type $\mathcal{P}$" is preserved by push-forwards and behaves well under fiber products. For the first condition, Let $\alpha : R \longrightarrow R'$ be a Λ-algebra homomorphism of artinian coefficient Λ-algebras and let $M = R^n$ and $M' = R'^n$ be endowed with the structure of Π-module and suppose M is in $\mathcal{P}$.

Let $\{a_1, \ldots, a_m\} \subset \mathfrak{m}_{R'}$ be a set of generators of R' over R. Then we get a surjective homomorphism

$$R[X_1, \ldots, X_m] \longrightarrow R'$$

sending $X_i \mapsto a_i$. Since R' is artinian a power of the maximal ideal vanishes, hence the map just above described factorizes through

$$\alpha_2 : B = R[X_1, \ldots, X_m]/\langle X_1^j, \ldots, X_m^j \rangle \longrightarrow R'$$

for some j. Denote $\alpha_1 : R \longrightarrow B$ and so $\alpha = \alpha_2 \circ \alpha_1$. The ring B is free over R, then the pullback $\alpha_{1,*}(M)$ is just M^r for r the rank of B over R. Since $\mathcal{P}$ is closed by finite direct sums $\alpha_{1,*}M = M^r$ is in $\mathcal{P}$. Note that $\alpha_{2,*}M^r = M'$ is a quotient of M^r, then it is also in $\mathcal{P}$.

For proving *iii.* let $R_3 = R_1 \times_{R_0} R_2$ be a fiber product of artinian coefficient Λ-algebras

$$\begin{tikzcd} & R_3 \arrow[dl, "p"'] \arrow[dr, "q"] & \\ R_1 \arrow[dr] & & R_2 \arrow[dl] \\ & R_0 & \end{tikzcd}$$

and let ρ_i be a deformation of $\overline{\rho}$ to R_i with corresponding module M_i with $p_*\rho_3 = \rho_1$ and $q_*\rho_3 = \rho_2$. Part *ii.* implies that if ρ_3 is in $\mathcal{P}$ then ρ_1, ρ_2 are in $\mathcal{P}$ as well. Conversely, suppose ρ_1, ρ_2 are in $\mathcal{P}$, note that R_3 is a subring of $R_1 \times R_2$, therefore M_3 is a submodule of $M_1 \oplus M_2$. Since M_1 and M_2 are in $\mathcal{P}$ and this category is invariant under taking sub-objects and finite direct sums then M_3 is in $\mathcal{P}$.

□

The description of $H^1_{\mathcal{P}}(\Pi, \mathrm{Ad}(\overline{\rho}))$ is clear in $\mathrm{Ext}_\Pi(V_{\overline{\rho}}, \overline{\rho})$, it consists on all the extensions

$$\begin{tikzcd} 0 \arrow[r] & V_{\overline{\rho}} \arrow[r] & E \arrow[r] & V_{\overline{\rho}} \arrow[r] & 0 \end{tikzcd}$$

with E an object of $\mathcal{P}$.

One of the most relevant examples of a categorical condition is given by considering those representations for which the correspoding $\mathbb{Q}_\ell$ group scheme is isomorphic to the $G_{\mathbb{Q}_\ell}$-module obtained from the generic fiber of a finite flat group scheme over $\mathrm{Spec}(\mathbb{Z}_\ell)$. See Chapter V of [CSS97] for an introduction on finite flat group schemes and Chapter XIII of the same reference for a discussion of the flat deformation functor.

Ordinary deformations

We now restrict to the case $n = 2$.

Definition 7.2.2. Fix Π and k as above, let R be a ring in $\mathcal{C}$, and choose a closed subgroup $I \subset \Pi$. Let

$$\rho : \Pi \longrightarrow \mathrm{GL}_2(R)$$

be a representation, and let $M = R^2$ with the Π-module structure determined by ρ. We say ρ is I-ordinary if the sub-R-module $M^I \subset M$ is free of rank 1 over R, a direct summand of M and the restriction of ρ to I is not trivial in M/M^I.

To check that being I-ordinary is invariant under strict equivalence, consider M and M' free R-modules of rank two with a continuous action of Π which are equivalent over $V_{\overline{\rho}}$, the Π-module corresponding to the residual representation, i.e. there is a Π-module isomorphism which makes the following triangle commutative

$$\begin{tikzcd} M \arrow[rr, "f"] \arrow[dr] & & M' \arrow[dl] \\ & V_{\overline{\rho}} & \end{tikzcd}$$

Then $f(M^I) = M'^I$ and M'^I is R-free of rank 1. If $M = M^I \oplus N$ then $M' = M'^I \oplus f(N)$. Besides, M/M^I and M'/M^I are isomorphic as I-modules, so the action of I in M'/M^I is not trivial. This proves that M' is I-ordinary.

Theorem 7.2.2. *Suppose $\overline{\rho}$ is I-ordinary. Then the condition of being I-ordinary is a deformation condition for $\overline{\rho}$.*

Proof. Let R and R' be artinian Λ-coefficient algebras and let $\alpha : R \longrightarrow R'$ be a Λ-coefficient homomorphism. Without loss of generality we can assume $\mathfrak{m}_R \neq 0$ and $\mathfrak{m}_{R'} \neq 0$, otherwise we are in the residual representation case. Let $\rho : \Pi \longrightarrow \mathrm{GL}_2(R)$ be an I-ordinary deformation of $\overline{\rho}$ and denote by M the module of one fixed representation in the class of ρ. We may assume, after conjugation, that for each $g \in I$ the matrix $\rho(g)$ has the form

$$\rho(g) = \begin{pmatrix} 1 & b(g) \\ 0 & d(g) \end{pmatrix}.$$

Since M^I is of rank 1, for some $g \in I$, $d(g)$ is not equal to 1 modulo $\mathfrak{m}_R$, otherwise, the reduction to k would be unipotent on I. Therefore $\alpha_*\rho$ has the following form for the elements of I

$$\rho(g) = \begin{pmatrix} 1 & \alpha(b(g)) \\ 0 & \alpha(d(g)) \end{pmatrix}.$$

Hence, for some $g \in I$ the reduction of $\alpha_*\rho(g)$ to k is not unipotent proving that $\alpha_*\rho$ is I-ordinary.

The third condition is about the behavior in fiber products. Let $R_3 = R_1 \times_{R_0} R_2$ be the fiber product in $\mathcal{C}^0_\Lambda$ of

$$\begin{tikzcd} & R_3 \arrow[dl, "p"'] \arrow[dr, "q"] & \\ R_1 \arrow[dr, "\varphi_1"'] & & R_2 \arrow[dl, "\varphi_2"] \\ & R_0 & \end{tikzcd}$$

Suppose ρ_3 is a deformation of $\overline{\rho}$ to R_3 such that the induced deformations ρ_1 and ρ_2 in R_1 and R_2, respectively, are I-ordinary. Let's fix representations ϕ_i in the strict equivalence class of ρ_i with $\phi_1 = p_*\phi_3$ and $\phi_2 = q_*\phi_3$. Let $e_i = (a_i, b_i)$ $(i = 1, 2)$ be generators of $(R_i \times R_i)^I$, then at least one of a_1 or b_1 is a unit, suppose a_1. Mapping e_i to $R_0 \times R_0$ we see that $\varphi_1(e_1)$ and $\varphi_2(e_2)$ differ by a unit in R_0. Therefore a_2 is also a unit and without loss of generality we can take $a_i = 1$. Then

$$(R_i \times R_i)^I = \langle (1, b_i) \rangle.$$

Hence

$$\varphi_1(1, b_1) = (1, \varphi_1(b_1)) = c\varphi_2(1, b_2) = c(1, \varphi_2(b_2))$$

for some unit $c \in R_0$, then $c = 1$ and $\varphi_1(e_1) = \varphi_2(e_2) = e_0$ and $e_3 = (e_1, e_2) \in R_3 = R_1 \times_{R_0} R_2$. We will see that actually the fixed subgroup of φ_3 is generated by e_3, it is immediate to check that the submodule generated by e_3 is free of rank 1 over R_3.

Let $x \in I$, then $p(\varphi_3(x)e_3) = \varphi_1(x)e_1 = e_1$, similarly $q(\varphi_3(x)e_3) = \varphi_2(x)e_2 = e_2$, this proves that $\varphi_3(x)e_3 = e_3$ and $\langle e_3 \rangle \subset (R_3 \times R_3)^I$. Conversely, take $e \in (R_3 \times R_3)^I$, then

$$p(e) = c_1 e_1 \quad \text{and} \quad q(e) = c_2 e_2.$$

Mapping to R_0 we get that

$$\varphi_1(c_1 e_1) = \varphi_1(c_1)e_0 = \varphi_2(c_2)e_0 = \varphi_2(c_2 e_2)$$

and $\varphi_1(c_1) = \varphi_2(c_2)$ showing that $c_3 = (c_1, c_2) \in R_3$ and therefore $e = c_3 e_3$. This completes the proof. □

We can then define the functor $\mathbf{D}_I$ of I-ordinary deformations. It is easy to see that if we extend this condition to finitely many closed subgroups $I_1, \ldots, I_k$ of Π, the remaining condition is actually a deformation condition. We can also consider *I-co-ordinary* deformations:

Definition 7.2.3. A representation $\rho : \Pi \longrightarrow \mathrm{GL}_2(R)$ is called I-co-ordinary if its representation space M has a submodule M_1 of rank 1 over R, stable under I, not a trivial I-module, and a direct summand of M, such that the quotient space M/M_1 is I-invariant.

We have the same result in this case.

Theorem 7.2.3. *Suppose $\overline{\rho}$ is I-co-ordinary. Then being I-co-ordinary is a deformation condition.*

Proof. Recall that a deformation ρ is I-ordinary if its restriction to I is conjugate to matrices of the following sort

$$\rho|_I \sim \begin{pmatrix} 1 & * \\ 0 & * \end{pmatrix}$$

with their reduction to k not trivial. On the other hand, ρ is I-co-ordinary if

$$\rho|_I \sim \begin{pmatrix} * & * \\ 0 & 1 \end{pmatrix}$$

and if it does not restrict trivially in k for elements in I. Therefore the contragredient deformation $\rho^{\#}$ is I-ordinary. This shows that "being I-co-ordinary" is a deformation condition. □

In the particular case when I is a normal subgroup, for instance $\Pi = G_{\mathbb{Q}_p}$ and I the inertia subgroup, we have a good characterization of the tangent space of $\mathbf{D}_I$.

Before stating the proposition, note that the definition of I-ordinariness is equivalent to

$$\rho|_I \sim \begin{pmatrix} 1 & * \\ 0 & \chi_2 \end{pmatrix}$$

with χ_2 a character which is not the trival one. Let $\overline{\rho} : \Pi \longrightarrow \mathrm{GL}_2(k)$ be a residual representation and suppose without loss of generality that it has the form

$$\overline{\rho} = \begin{pmatrix} \overline{\chi}_1 & * \\ 0 & \overline{\chi}_2 \end{pmatrix},$$

note that $\overline{\chi}_1$ factors through Π/I.

We want to describe the tangent space of the I-ordinary condition, $H^1_I(\Pi, \mathrm{Ad}(\overline{\rho}))$. Let $\rho : \Pi \longrightarrow \mathrm{GL}_2(k[\epsilon])$ be a deformation of $\overline{\rho}$, then ρ has a representative of the form

$$\rho = \begin{pmatrix} \chi_1 & * \\ 0 & \chi_2 \end{pmatrix}.$$

We write the associated cocycle of ρ as B_g, then

$$\rho(g) = (1 + \epsilon B_g)\overline{\rho}(g).$$

Write $B_g = \begin{pmatrix} a_g & b_g \\ c_g & d_g \end{pmatrix}$, then

$$\begin{aligned}\begin{pmatrix} \chi_1 & * \\ 0 & \chi_2 \end{pmatrix} &= (1+\epsilon B_g)\overline{\rho}(g) \\ &= \begin{pmatrix} \overline{\chi}_1 & * \\ 0 & \overline{\chi}_2 \end{pmatrix} + \epsilon \begin{pmatrix} a_g & b_g \\ c_g & d_g \end{pmatrix} \begin{pmatrix} \overline{\chi}_1 & * \\ 0 & \overline{\chi}_2 \end{pmatrix} \\ &= \begin{pmatrix} \overline{\chi}_1(1+\epsilon a_g) & * \\ \epsilon c_g \overline{\chi}_1 & *c_g + \overline{\chi}_2(1+\epsilon d_g) \end{pmatrix}.\end{aligned}$$

Therefore $c_g = 0$ for all $g \in \Pi$ and $\chi_1 = \overline{\chi}(1+\epsilon a_g)$ and $\chi_2 = \overline{\chi}_2(1+\epsilon d_g)$. Let $\mathrm{Ad}^+(\overline{\rho})$ be the subspace of endomorphisms of $V = V_{\overline{\rho}}$ for which V^I is an eigenspace. In our matrix notation these are just the upper triangular matrices. It is clear that $\mathrm{Ad}^+(\overline{\rho})$ is a subrepresentation of $\mathrm{Ad}(\overline{\rho})$. Since

$$\begin{pmatrix} \overline{\chi}_1 & * \\ 0 & \overline{\chi}_2 \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} \overline{\chi}_1^{-1} & * \\ 0 & \overline{\chi}_2^{-1} \end{pmatrix} = \begin{pmatrix} * & * \\ \overline{\chi}_1^{-1}\overline{\chi}_2 c & * \end{pmatrix},$$

the action on $\mathrm{Ad}(\overline{\rho})/\mathrm{Ad}^+(\overline{\rho})$ is $\overline{\chi}_1^{-1}\overline{\chi}_2$ which is not trivial. Then $H^0(\Pi, \mathrm{Ad}(\overline{\rho})/\mathrm{Ad}^+(\overline{\rho})) = 0$ and $H^1(\Pi, \mathrm{Ad}^+(\overline{\rho})) \longrightarrow H^1(\Pi, \mathrm{Ad}(\overline{\rho}))$ is injective. The computation of the cocycle B_g shows that $H^1_I(\Pi, \mathrm{Ad}(\overline{\rho})) \subset H^1(\Pi, \mathrm{Ad}^+(\overline{\rho}))$. Let $\mathrm{Ad}_I(\overline{\rho})$ be the endomorphisms of V whose kernel contains V^I, then in our basis these are the matrices with first column equal to zero. Note that $\mathrm{Ad}_I(\overline{\rho})$ is a subrepresentation of $\mathrm{Ad}^+(\overline{\rho})$ because I is normal and that we have a decomposition

$$\mathrm{Ad}^+(\overline{\rho}) = \mathrm{Ad}_I(\overline{\rho}) \oplus k\,\mathrm{Id}\,.$$

Therefore

$$H^1(\Pi, \mathrm{Ad}^+(\overline{\rho})) = H^1(\Pi, \mathrm{Ad}_I(\overline{\rho})) \oplus H^1(\Pi, k\,\mathrm{Id}) = H^1(\Pi, \mathrm{Ad}_I(\overline{\rho})) \oplus \mathrm{Hom}(\Pi, k).$$

A cocycle B_g of $\mathrm{Ad}^+(\overline{\rho})$ corresponds to an I-ordinary deformation if and only if $a_g = 0$ for all $g \in I$. Recall the exact inflation-restriction sequence

$$\begin{tikzcd} 0 \arrow[r] & \mathrm{Hom}(\Pi/I, k) \arrow[r] & \mathrm{Hom}(\Pi, k) \arrow[r] & \mathrm{Hom}(I, k) \end{tikzcd}$$

Note that a_g is the $\mathrm{Hom}(\Pi, k)$ part of B_g, then

$$H^1_I(\Pi, \mathrm{Ad}(\overline{\rho})) \cong H^1(\Pi, \mathrm{Ad}_I(\overline{\rho})) \oplus \mathrm{Hom}(\Pi/I, k) \subset H^1(\Pi, \mathrm{Ad}^+(\overline{\rho})) \subset H^1(\Pi, \mathrm{Ad}(\overline{\rho})).$$

7.3 Deformation conditions for global Galois representations

We turn back to Galois representations, so let S be a finite set of primes of $\mathbb{Q}$ containing ∞ and p. Let $\mathbb{Q}_S$ be the, maximal unramified extension of $\mathbb{Q}$ outside S and denote its Galois group by $G_{\mathbb{Q},S}$. We consider residual representations

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

for instance those arising from the p-torsion points of elliptic curves or the ones associated to modular forms. These representations are absolutely irreducible and have a deformation to $\mathcal{O}_\lambda$, with $\mathcal{O}$ the ring of integers of a number field, and λ a non-archimedean prime of $\mathcal{O}$. Moreover, they have as determinant a power of the cyclotomic character χ_p by a finite character. They also satisfy some ordinariness conditions for primes in S.

In general, let $\overline{\rho} : G_{\mathbb{Q},S} \longrightarrow \mathrm{GL}_n(k)$ be residual representation. A *global Galois deformation problem* $\mathcal{Q}$ is a set of deformation conditions $\mathcal{Q}_\ell$ on the restriction $\overline{\rho}|_{D_\ell}$ to the decomposition group at ℓ, for each $\ell \in S$ non-archimedean.

Lemma 7.3.1. *A global Galois deformation problem is a deformation condition for representations of $G_{\mathbb{Q},S}$.*

Proof. This is clear because pushouts and fiber products does not depend on the group itself, they are defined over coefficient Λ-algebra homomorphisms. □

The interpretation of the tangent space of the condition $\mathcal{Q}$ is described in terms of local conditions in the next theorem

Theorem 7.3.1. *The diagram*

$$\begin{tikzcd}
H^1_{\mathcal{Q}}(G_{\mathbb{Q},S}, \mathrm{Ad}(\overline{\rho})) \arrow[r] \arrow[d] & H^1(G_{\mathbb{Q},S}, \mathrm{Ad}(\overline{\rho})) \arrow[d] \\
\prod_{\ell\in S} H^1_{\mathcal{Q}_\ell}(G_{\mathbb{Q}_\ell}, \mathrm{Ad}(\overline{\rho})) \arrow[r] & \prod_{\ell\in S} H^1(G_{\mathbb{Q}_\ell}, \mathrm{Ad}(\overline{\rho}))
\end{tikzcd}$$

is cartesian.

Proof. Let ρ be a deformation of $\overline{\rho}$ to $k[\epsilon]$ such that for each non-archimidean $\ell \in S$ the restriction $\rho|_{D_\ell}$ has property $\mathcal{Q}_\ell$, by definition ρ has property $\mathcal{Q}$ and its cohomology class belongs to $H^1_{\mathcal{Q}}(G_{\mathbb{Q},S}, \mathrm{Ad}(\overline{\rho}))$.

□

We finish defining an special deformation condition. In this case we only consider the prime p. We say that a deformation of $\overline{\rho}$ is p-ordinary if its restriction to D_p is I_p-ordinary, where I_p is the inertia subgroup of D_p.

Part II

Some constructions from modular forms

Chapter 8

Basics on modular forms and modular curves

8.1 Modular forms and modular curves

In this section we will introduce some basic results related to modular forms and modular curves, if the reader is truly interested in learning modular forms I recommend [DS05], [Miy89], [Shi71]; the first one is great for a first course, the other two are better for advance students with a deep background in analysis and number theory.

Let $\mathfrak{H}$ be the complex upper half plane, i.e. the set

$$\mathfrak{H} = \{\tau \in \mathbb{C} : \mathrm{Im}(\tau) > 0\}.$$

Let $\mathrm{SL}_2(\mathbb{Z})$ be the set of 2×2 matrices with integer entries and determinant 1, this group acts on $\mathfrak{H}$ by Möbius transformations. Indeed, let $\gamma \in \mathrm{SL}_2(\mathbb{Z})$ and write

$$\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix},$$

then for $\tau \in \mathfrak{H}$ we define

$$\gamma(\tau) = \frac{a\tau + b}{c\tau + d}.$$

A straightforward computation shows that $\gamma_1(\gamma_2(\tau)) = (\gamma_1\gamma_2)(\tau)$ for $\gamma_i \in \mathrm{SL}_2(\mathbb{Z})$.

Let k be an integer and let $f : \mathfrak{H} \longrightarrow \mathbb{C}$ be a function. We say that f is *weight-k invariant* under $\mathrm{SL}_2(\mathbb{Z})$ if for all $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$,

$$f(\gamma(\tau)) = (c\tau + d)^k f(\tau). \tag{8.1.1}$$

Define the *factor of automorphy* $j(\gamma, \tau)$ to be

$$j(\gamma, \tau) = (c\tau + d).$$

Let $\alpha \in \mathrm{SL}_2(\mathbb{Z})$ and k be an integer, define the *weight-k operator* $[\alpha]_k$ to be the operator on functions $f : \mathfrak{H} \longrightarrow \mathbb{C}$ given by

$$f[\alpha]_k(\tau) = j(\alpha, \tau)^{-k} f(\alpha(\tau)),$$

note that to be weight-k invariant with respect to $\mathrm{SL}_2(\mathbb{Z})$ is equivalent to $f[\alpha]_k = f$ for all $\alpha \in \mathrm{SL}_2(\mathbb{Z})$.

Let f be weight-k invariant with respect to $\mathrm{SL}_2(\mathbb{Z})$. Equation (8.1.1) with $\gamma = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ shows that f is periodic with period 1. On the other hand, if $\gamma = -\operatorname{Id}$ then

$$f(\tau) = (-1)^k f(\tau)$$

Therefore, for k odd the only weight-k invariant function is 0.

Lemma 8.1.1. *The group* $\mathrm{SL}_2(\mathbb{Z})$ *is generated by the matrices*

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \text{ and } \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}.$$

Lemma 8.1.1 shows that in order to check if a function f is weight-k invariant, we just have to compute $f(\gamma(\tau))$ with γ equal to the matrices in the lemma. Let $f : \mathfrak{H} \longrightarrow \mathbb{C}$ be a meromorphic function and suppose f is weight-k invariant with respect to $\mathrm{SL}_2(\mathbb{Z})$. We saw that f is a periodic function and hence it has a Fourier expansion

$$f(\tau) = \sum_{n \in \mathbb{Z}} a_n q^n, \quad q = e^{2\pi i \tau}. \tag{8.1.2}$$

We say that f is *meromorphic at infinity* if the coefficients of the previous series are 0 for all $n < -N$, for some $N \in \mathbb{N}$. We say that f is *holomorphic at* ∞ if $a_n = 0$ for $n < 0$.

Definition 8.1.1. A *modular form of weight-k* is a function $f : \mathfrak{H} \longrightarrow \mathbb{C}$ with the following properties

1. f is holomorphic on $\mathfrak{H}$.
2. f is weight-k invariant with respect to $\mathrm{SL}_2(\mathbb{Z})$.
3. f is holomorphic at ∞.

If in addition f vanishes at ∞, i.e. $a_0 = 0$ in the Fourier expansion (8.1.2), we call f a *cuspidal form of weight-k.*

Similarly, we define an *automorphic form* to be a meromorphic function $f : \mathfrak{H} \longrightarrow \mathbb{C}$ which is weight-k invariant with respect to $\mathrm{SL}_2(\mathbb{Z})$ and meromorphic at ∞.

With more generality, define the *principal congruence subgroup of level N*

$$\Gamma(N) = \left\{ \gamma \in \mathrm{SL}_2(\mathbb{Z}) : \gamma \equiv \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \mod N \right\}.$$

A *congruence group* is subgroup Γ of $\mathrm{SL}_2(\mathbb{Z})$ containing $\Gamma(N)$ for some $N \in \mathbb{N}$, in this case we say that Γ is a *congruence subgroup of level N*. We define two family of congruence subgroups

$$\Gamma_1(N) = \left\{ \gamma \in \mathrm{SL}_2(\mathbb{Z}) : \gamma \equiv \begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix} \mod N \right\}$$
$$\Gamma_0(N) = \left\{ \gamma \in \mathrm{SL}_2(\mathbb{Z}) : \gamma \equiv \begin{pmatrix} * & * \\ 0 & * \end{pmatrix} \mod N \right\}.$$

We say that a function $f : \mathfrak{H} \longrightarrow \mathbb{C}$ is weight-k invariant with respect to a congruence subgroup Γ if

$$f(\gamma(\tau)) = (c\tau + d)^k f(\tau), \text{ for } \gamma \in \Gamma.$$

Let f be a meromorphic function on $\mathfrak{H}$ which is weight-k invariant with respect a congruence subgroup Γ, recall that $\Gamma(N) \subset \Gamma$ for some N. Thus, the matrix $\begin{pmatrix} 1 & N \\ 0 & 1 \end{pmatrix}$ belongs to Γ. Then, f is $N\mathbb{Z}$ periodic and has a Fourier expansion at ∞

$$f(\tau) = \sum_{n\in\mathbb{Z}} a_n e^{2\pi i n/N} = \sum_{n\in\mathbb{Z}} a_n q_N^n, \quad q_N = e^{2\pi i/N}, \tag{8.1.3}$$

this shows that being holomorphic at ∞ makes sense for meromorphic functions weight-k invariant with respect a congruence subgroup. Specifically, being holomorphic at infinity means that the coefficients $a_n = 0$ for $n < 0$ in the expansion (8.1.3).

Definition 8.1.2. A *modular form of weight-k with respect to* Γ is a function $f : \mathfrak{H} \longrightarrow \mathbb{C}$ such that

1. f is holomorphic on $\mathfrak{H}$.

2. f is weight-k invariant with respect to Γ.

3. $f[\alpha]_k$ is holomorphic at ∞ for all $\alpha \in \mathrm{SL}_2(\mathbb{Z})$.

   In addition, if $f[\alpha]_k$ vanishes at infinity for all $\alpha \in \mathrm{SL}_2(\mathbb{Z})$ we say that f is a *cuspidal form of weight-k with respect to* Γ.

The vector space of weight-k modular forms turns out to be 0 for k a negative integer and finite dimensional for $k \geq 0$. We denote the space of weight-k modular forms of Γ by $\mathcal{M}_k(\Gamma)$ and the space of weight-k cuspidal forms by $\mathcal{S}_k(\Gamma)$. The product of two modular forms of weight k and l gives a modular form of weight $k + l$. Therefore, they form a graded algebra $\mathcal{M}(\Gamma) = \bigoplus_{k\geq 0} \mathcal{M}_k(\Gamma)$. The cuspidal forms generate an ideal $\mathcal{S}(\Gamma)= \bigoplus_{k\geq 0} \mathcal{S}_k(\Gamma)$ of $\mathcal{M}(\Gamma)$.

Recall that a congruence subgroup Γ acts on $\mathfrak{H}$ by Möbius transformations, one can prove that the action of Γ is nice enough for the quotient space $Y(\Gamma) = \Gamma\backslash\mathfrak{H}$ to be a Hausdorff space [DS05, Ch. 2]. Denote by Γ_τ the isotropy group of τ in Γ, if $\Gamma_\tau \subset \{\pm \mathrm{Id}\}$ then a neighborhood of τ is mapped homeomorphically onto a neighborhood of $\Gamma\tau \in Y(\Gamma)$, otherwise we say that $\Gamma\tau$ is an *elliptic point* of Γ and the projection $\mathfrak{H} \longrightarrow Y(\Gamma)$ looks locally like an n-fold power centered at τ, $n = [\Gamma_\tau : \Gamma_\tau \cap \pm \mathrm{Id}]$. Nevertheless, one can show that the elliptic points are discrete in $\mathfrak{H}$ and that the whole quotient has structure of a Riemann surface.

Theorem 8.1.1. *Let* Γ *be a congruence subgroup and consider its action on* $\mathfrak{H}$. *Then the quotient*

$$Y(\Gamma) = \Gamma\backslash\mathfrak{H}$$

is a Riemann surface. We denote

$$Y_1(N) = Y(\Gamma_1(N)), \;\; Y_0(N) = Y(\Gamma_0(N)) \textit{ and } Y(N) = Y(\Gamma(N)).$$

Since $\mathrm{SL}_2(\mathbb{Z})$ acts transitively on $\mathbb{Q} \cup \{\infty\}$ where $\hat{\mathbb{C}} = \mathbb{C} \cup \{\infty\}$ is the Riemann sphere, we may consider the action of $\mathrm{SL}_2(\mathbb{Z})$ on the space $\mathfrak{H}^* = \mathfrak{H} \cup \mathbb{Q} \cup \infty$. Even more, we may define a system of neighborhoods around ∞ by $U_C = \{\tau : \mathrm{Im}(\tau) > C\}$ with $C > 0$, and use the action of $\mathrm{SL}_2(\mathbb{Z})$ to define system of neighborhoods around the rational numbers. Under this topology if Γ is a congruence subgroup, the quotient space

$$X(\Gamma) = \Gamma\backslash\mathfrak{H}^*$$

will be a compact Riemann surface. The number of orbits of Γ in $\mathbb{Q} \cup \{\infty\}$ is finite and are called *cusps*. We define analogously

$$X(N) = X(\Gamma(N)), \;\; X_1(N) = X(\Gamma_1(N)) \text{ and } \; X_0(N) = X(\Gamma_0(N)).$$

Definition 8.1.3. The Riemann surfaces $Y(\Gamma)$ are called *non-compact modular curves.* Their compactification $X(\Gamma)$ contructed by adding cusps are refered just as *modular curves.*

Take $\Gamma = \Gamma_1(N), \Gamma_0(N)$ or $\Gamma(N)$. The *divisor group* of the modular curve $X(\Gamma)$ is the free abelian group generated by the points of $X(\Gamma)$ and is denoted by $\operatorname{Div}(X(\Gamma))$. Then, an element in $\operatorname{Div}(X(\Gamma))$ has the form $D = \sum_{x \in X(\Gamma)} n_x(x)$ with $n_x \in \mathbb{Z}$ zero for all but finitely many x. The degree of a divisor is defined as

$$\deg(D) = \sum_{x \in X(\Gamma)} n_x,$$

the group of divisors of degree 0 is denoted by $\operatorname{Div}^0(X(\Gamma))$. Let $f : X(\Gamma) \longrightarrow \hat{\mathbb{C}}$ be a no-constant meromorphic function, we can associate to f a divisor counting the number of zeroes and poles with multiplicity

$$\operatorname{Div}(f) = \sum_{x \in f^{-1}(0)} e_x(x) - \sum_{x \in f^{-1}(\infty)} e_x(x)$$

where e_x is the ramification index of f at x. These divisors are called *principal divisors* and form a subgroup of $\operatorname{Div}(X(\Gamma))$ which is denoted by $\operatorname{Div}^\ell(X(\Gamma))$. A result on Riemann surfaces tells us that $\deg(\operatorname{Div}(f)) = 0$, so $\operatorname{Div}^\ell(X(\Gamma)) \subset \operatorname{Div}^0(X(\Gamma))$. The group $\operatorname{Div}^0(X(\Gamma)) / \operatorname{Div}^\ell(X(\Gamma))$ is called the *Picard group* and we write $\operatorname{Pic}^0(X(\Gamma))$ instead.

8.2 Eisenstein Series

The spaces of modular forms of $\mathrm{SL}_2(\mathbb{Z})$ are described using Eisenstein series. Let k be a integer greater than 2, the sum

$$G_k(\tau) = \sum_{c,d}{}' \frac{1}{(c\tau + d)^k}$$

converges uniformly and absolutely on compact sets of $\mathfrak{H}$[1]. G_k is a modular form of weight k, moreover, the algebra of modular forms $\mathcal{M}(\mathrm{SL}_2(\mathbb{Z}))$ is generated by G_4 and G_6 as algebra over $\mathbb{C}$ and is isomorphic to a polynomial ring on two variables.

$$\mathcal{M}(\mathrm{SL}_2(\mathbb{Z})) = \mathbb{C}[G_4, G_6] \cong \mathbb{C}[X, Y].$$

Let $g_2 = 60G_4$ and $g_3 = 140G_6$. One can show that

$$\Delta = g_2^3 - 27g_3^2$$

is a cuspidal form of weight 12 called the *discriminant.* The ideal of cuspidal forms of $\mathrm{SL}_2(\mathbb{Z})$ is generated by Δ

$$\mathcal{S}(\mathrm{SL}_2(\mathbb{Z})) = \mathcal{M}(\mathrm{SL}_2(\mathbb{Z}))\Delta.$$

[1] Primed sums indicate summing over all non-zero indices.

Define

$$J = 1728\frac{g_2^3}{\Delta},$$

this is called the *J-invariant*. Even if J is not a modular form, it is an automorphic form of weight-0 and its q-expansion at ∞ has a simple pole with residue 1. Moreover, it generates the function field of the modular curve $X(1)$:

$$\mathbb{C}(X(1)) = \mathbb{C}(J).$$

The space of weight-k modular forms $\mathcal{M}_k(\mathrm{SL}_2(\mathbb{Z}))$ has a decomposition as direct sum

$$\mathcal{M}_k(\mathrm{SL}_2(\mathbb{Z})) = \mathcal{S}_k(\mathrm{SL}_2(\mathbb{Z})) \bigoplus \mathbb{C}G_k.$$

In general, for the congruence subgroups $\Gamma = \Gamma(N), \Gamma_1(N)$ or $\Gamma_0(N)$ there are similar decompositions

$$\mathcal{M}_k(\Gamma) = \mathcal{S}_k(\Gamma) \bigoplus \mathcal{E}_k(\Gamma)$$

where $\mathcal{E}_k(\Gamma)$ is the *Eisenstein space*. For a description of these spaces see [DS05, Ch. 4]. From now on we will study only $\Gamma = \Gamma_1(N)$ or $\Gamma_0(N)$, the group $\Gamma_1(N)$ is normal in $\Gamma_0(N)$. Indeed, $\Gamma_1(N)$ is the kernel of

$$\Gamma_0(N) \longrightarrow (\mathbb{Z}/N\mathbb{Z})^*, \quad \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mapsto \overline{d}.$$

Since $\Gamma_1(N)$ is normal in $\Gamma_0(N)$, for all $\alpha \in \Gamma_0(N)$ and every modular form $f \in \mathcal{M}_k(\Gamma_1(N))$, the function $f[\alpha]_k$ is again in $\mathcal{M}_k(\Gamma_1(N))$. We then have a representation of $\Gamma_0(N)$ over $\mathcal{M}_k(\Gamma_1(N))$ whose kernel contains $\Gamma_1(N)$, therefore we actually have a representation of $\Gamma_0(N)/\Gamma_1(N) \cong (\mathbb{Z}/N\mathbb{Z})^*$ over $\mathcal{M}_k(\Gamma_1(N))$. Write G_N for the multiplicative group $(\mathbb{Z}/N\mathbb{Z})^*$. Recall from representation theory that the characters $\chi \in \hat{G}_N$ form an abelian group and we can decompose $\mathcal{M}_k(\Gamma_1(N))$ in eigenspaces

$$\mathcal{M}_k(\Gamma_1(N)) = \bigoplus_{\chi \in \hat{G}_N} \mathcal{M}_k(N, \chi).$$

Denote the trivial character by 1_N, then $\mathcal{M}_k(\Gamma_0(N)) = \mathcal{M}_k(N, 1_N)$. The subspace of cusp forms is also invariant by G_N as well as the Eisenstein spaces, so we have decompositions

$$\mathcal{S}_k(\Gamma_1(N)) = \bigoplus_{\chi \in \hat{G}_N} \mathcal{S}_k(N, \chi), \quad \mathcal{E}_k(\Gamma_1(N)) = \bigoplus_{\chi \in \hat{G}_N} \mathcal{E}_k(N, \chi).$$

Chapter 9

Hecke operators and eigenforms

9.1 Hecke operators

Before defining the Hecke operators, we have to talk about *double coset operators.* Let Γ_1, Γ_2 be congruence subgroups and let $\alpha \in \mathrm{GL}_2^+(\mathbb{Q})$. The set

$$\Gamma_1\alpha\Gamma_2 = \{\gamma_1\alpha\gamma_2 : \gamma_i \in \Gamma_i\}$$

is a *double coset* in $\mathrm{GL}_2^+(\mathbb{Q})$. For an element $\beta \in \mathrm{GL}_2^+(\mathbb{Q})$ we define the *weight-k operator* $[\beta]_k$ on functions $f : \mathfrak{H} \longrightarrow \mathbb{C}$:

$$(f[\beta]_k)(\tau) = (\det\beta)^{k-1} j(\beta,\tau)^{-k} f(\beta(\tau)), \quad \tau \in \mathfrak{H}.$$

The group Γ_1 acs on $\Gamma_1\alpha\Gamma_2$ by left multiplication, one can prove ([DS05, Section 5.1]) that the quotient $\Gamma_1\backslash\Gamma_1\alpha\Gamma_2$ is finite, let $\{\beta_j\}$ be a set of representatives. We can define the *double coset operator of weight-k* $[\Gamma_1\alpha\Gamma_2]_k$ on modular forms as

$$[\Gamma_1\alpha\Gamma_2]_k : \mathcal{M}_k(\Gamma) \longrightarrow \mathcal{M}(\Gamma_2), \quad f \mapsto f[\Gamma_1\alpha\Gamma_2]_k = \sum_j f[\beta_j]_k.$$

It does not depend on the set of representatives and sends cuspidal forms to cuspidal forms, i.e. it restricts

$$[\Gamma_1\alpha\Gamma_2]_k : \mathcal{S}_k(\Gamma_1) \longrightarrow \mathcal{S}_k(\Gamma_2).$$

Let $X_i = X(\Gamma_i)$. Double coset operators also give maps on divisors by the formula

$$[\Gamma_1\alpha\Gamma_2] : \mathrm{Div}(X_2) \longrightarrow \mathrm{Div}(X_1),\ \Gamma_2\tau \mapsto \sum_j \Gamma_1\beta_j(\tau),$$

this can be described by successive compositions of pushforwards and pullback maps on divisors.

Now we can define the Hecke operators, more specifically we will define the diamond operator $\langle n\rangle$ and the T_n operator, $n \in \mathbb{N}$. Let $\Gamma = \Gamma_1 = \Gamma_2 = \Gamma_1(N)$, for $\gcd(n,N) > 1$ we simply define $\langle n\rangle = 0$. For d prime to N consider $\alpha_d \in \Gamma_0(N)$ such that

$$\alpha \equiv \begin{pmatrix} * & * \\ 0 & d \end{pmatrix} \mod N$$

we define the *diamond operator* $\langle d\rangle$

$$\langle d\rangle : \mathcal{M}_k(\Gamma_1(N)) \longrightarrow \mathcal{M}_k(\Gamma_1(N)), \quad \langle d\rangle f = f[\Gamma\alpha_d\Gamma]_k = f[\alpha_d]_k.$$

In eigenspaces the action of the Diamond is given by the character, i.e. for $f \in \mathcal{M}(N, \chi)$ we get

$$\langle d \rangle f = \chi(d) f.$$

Let

$$\alpha = \begin{pmatrix} 1 & 0 \\ 0 & p \end{pmatrix},$$

we define the T_p operator as the double coset operator $\Gamma \alpha \Gamma$, i.e for $f \in \mathcal{M}(\Gamma_1(N))$

$$T_p f = f \left[\Gamma_1(N) \begin{pmatrix} 1 & 0 \\ 0 & p \end{pmatrix} \Gamma_1(N) \right]_k$$

It turns out that these operators commute, [DS05, Ch. 5]. Set $T_1 = 1$, define inductively

$$T_{p^r} = T_p T_{p^{r-1}} - p^{k-1} \langle p \rangle T_{p^{r-2}}, \text{ for } r \geq 2. \tag{9.1.1}$$

For $n \in \mathbb{N}$ decompose $n = \prod_{p^r || n} p^r$ and define

$$T_n = \prod_{p^r || n} T_{p^r}.$$

This definition of the T_n operators is motivated by the following Euler product

$$\sum_{n \in \mathbb{N}} T_n n^{-s} = \prod_p (1 - T_p p^{-s} + \langle p \rangle p^{k-1-2s})^{-1},$$

Bellow we will see that the L-functions attached to eigenforms have the same Euler product and the coefficients also satisfies the recursion formula (9.1.1). The *Hecke algebra of weight-k over $\mathbb{Z}$* is the set $\mathbb{T}_{\mathbb{Z}}$ of endomorphisms of $\mathcal{S}_k(\Gamma_1(N))$ generated by the Hecke operators

$$\mathbb{T}_{\mathbb{Z}} = \mathbb{Z}[\{T_n, \langle n \rangle : n \in \mathbb{N}\}],$$

we define analogously $\mathbb{T}_{\mathbb{C}}$ the *Hecke algebra over* $\mathbb{C}$.

9.2 Eigenforms

As mentioned above, there is an explicit description of the Eisenstein space of weight-k for $\Gamma_1(N)$ in [DS05, Ch. 4], the only remaining is to get a complete description of the space of cuspidal forms of weight-k $\mathcal{S}_k(\Gamma_1(N))$. A natural inner product for cuspidal forms $\mathcal{S}_k(\Gamma_1(N))$ is introduced in [DS05, Ch. 5] or [Miy89, Ch.2 pg. 44]. For all $n \in \mathbb{N}$ the diamond operator $\langle n \rangle$ will turn out to be a normal operator as well as the T_p operators for $p \nmid N$. The next theorem holds

Theorem 9.2.1. *There exists a basis of $\mathcal{S}_k(\Gamma_1(N))$ consisting on simultaneous eigenvectors for the Hecke operators $\{\langle n \rangle, T_p :\ n \in \mathbb{N}$ and $p \nmid N\}$.*

Moreover, for $M|N$ the inclusion $\Gamma_1(N) \subset \Gamma_1(M)$ implies $\mathcal{S}_k(\Gamma_1(M)) \subset \mathcal{S}_k(\Gamma_1(N))$, then some modular forms come from lower level subgroups. These are called *old forms* and their ortogonal complemet are the *new forms*, all Hecke operators preserve the spaces of old and new forms. The new forms which are eigenvectors for the Hecke operators $\{\langle n \rangle, T_p :\ n \in \mathbb{N}$ and $p \nmid N\}$ are also eigenvectors for all Hecke operators. This suggest a definition

Definition 9.2.1. Consider $\Gamma_1(N)$ and the space of modular forms $\mathcal{S}_k(\Gamma_1(N))$. An eigenform is a modular form which is an eigenvector for all Hecke operators. Let f be an eigenform, the matrix $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ belongs to $\Gamma_1(N)$, then f has a Fourier expansion

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

we say that f is a normalized eigenform if $a_1(f) = 1$.

The importance of normalized eigenforms is that the eigenvalues are the same as Fourier coefficients. More precisely, let f be a normalized eigenform with Fourier series

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

the eigenvalue of T_n attached to f is $a_n(f)$, i.e. $T_n f = a_n(f) f$. The precise definitions and theorems are exhibited in [DS05, Ch. 5] as statements or exercises.

Let $f \in \mathcal{M}_k(\Gamma_1(N))$ be a modular form with Fourier expansion

$$f(\tau) = \sum_{n=0}^{\infty} a_n(f) q^n.$$

The L-function attached to f is

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

The next theorem holds

Theorem 9.2.2. *Let $f \in \mathcal{M}_k(\Gamma_1(N))$ be a modular form and $L(s, f)$ be its L-series. The following are equivalent*

(a) f is a normalized eigenform in $\mathcal{M}_k(N, \chi)$.

(b) The L-series has an Euler product

$$L(s, f) = \prod_p (1 - a_p p^{-s} + \chi(p) p^{k-1-2s})^{-1}$$

Part III

Galois representations and Fermat's Last Theorem

Chapter 10

Representations and modularity

10.1 Elliptic curves and Galois representations

We can attach Galois representations to elliptic curves and to modular forms. Here we present the construction of these representations for elliptic curves.

Let E be an elliptic curve over $\mathbb{C}$, so we can think of E as a quotient of $\mathbb{C}$ by a lattice Λ of rank 2, or as the solutions of a cubic equation

$$y^2 = 4x^3 + a_4 x + a_6 \tag{10.1.1}$$

where the polynomial $f(x) = 4x^3 + a_4 x + a_6$ has no repeated roots. The previous correspondence is given by the Weierstrass function

$$\wp_\Lambda(z) = \frac{1}{z^2} + \sum_{\omega\in\Lambda}{}' \left(\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2} \right),$$

associating the lattice Λ with the differential equation

$$(\wp'_\Lambda)^2 = 4\wp_\Lambda^3 - g_2(\Lambda)\wp_\Lambda - g_3(\Lambda),$$

where $g_2(\Lambda) = 60G_4(\Lambda)$, $g_3(\Lambda) = 140G_6(\Lambda)$ and

$$G_k(\Lambda) = \sum_{\omega\in\Lambda}{}' \frac{1}{\omega^k},$$

see [DS05, Ch. 1]. We can deduce the following theorem for elliptic curves over $\mathbb{C}$

Theorem 10.1.1. *Let E be an elliptic curve over $\mathbb{C}$ and let $E[N]$ the subgroup of N-torsion points of E. Then E is isomorphic to*

$$E[N] \cong \mathbb{Z}/N\mathbb{Z} \times \mathbb{Z}/N\mathbb{Z}.$$

Suppose E is defined over $\mathbb{Q}$, let $\mathbb{Q} \subset K$ be a field extension. We denote the K-points of E by $E(K)$, so $E(\mathbb{Q})$ are the rational points of E and $E(\overline{\mathbb{Q}})$ the algebraic points. The group operation of E can be defined using rational functions over $\mathbb{Q}$, it then turns out that torsion points have algebraic coordinates and that the absolute Galois group $G_\mathbb{Q}$ acts linearly on N-torsion points for $N \in \mathbb{N}$. Let ℓ be a prime number and consider the following system of groups

$$\begin{tikzcd} 0 & E[\ell] \arrow[l, "m_\ell"'] & E[\ell^2] \arrow[l, "m_\ell"'] & \cdots \arrow[l, "m_\ell"'] & E[\ell^n] \arrow[l, "m_\ell"'] & {} \arrow[l] \end{tikzcd}$$

with m_ℓ the multiplication by ℓ. The Galois action commutes with the system, therefore $G_{\mathbb{Q}}$ acts on the Tate module

$$\mathrm{Ta}_\ell(E) = \varprojlim_{n\in\mathbb{N}} E[\ell^n] \cong \mathbb{Z}_\ell^2.$$

In other words, we have a Galois representation $\rho_{E,\ell} : G_{\mathbb{Q}} \longrightarrow \mathrm{GL}(\mathrm{Ta}_\ell(E)) \cong \mathrm{GL}_2(\mathbb{Z}_\ell)$. Those representations have some particular properties, the next theorem exhibit a few of them

Theorem 10.1.2. *Let ℓ be a prime and let E be an elliptic curve over $\mathbb{Q}$ with conductor N_E. The Galois representation $\rho_{E,\ell}$ is unramified for all $p \nmid \ell N_E$. The image of every Frobenius element* Frob_p *over $p \nmid \ell N_E$ satisfies the equation* [1]

$$x^2 - a_p(E)x + p = 0.$$

As a direct consequence, the determinant of $\rho_{E,\ell}$ is the cyclotomic character χ_ℓ. The *Hasse-Weil L*-function of the elliptic curve E is

$$L(s,E) = \sum_{n=1}^{\infty} \frac{a_n(E)}{n^s} = \prod_p (1 - a_p(E)p^{-s} + \mathbf{1}_E(p)p^{1-2s})^{-1}.$$

Here $\mathbf{1}_E$ is the trivial character of $\mathbb{Z}/N_E\mathbb{Z}$.

In general, for any algebraically closed field K, we may define elliptic curves in two equivalent ways, three if char $K \neq 2,3$. Two of these definitions are in terms of explicit algebraic equations with certain conditions, and the other one only involves algebro-geometric properties:

Definition 10.1.1. Let K be an algebraically closed field. An *elliptic curve* $(E, \mathcal{O})$ is a non-singular curve E of genus 1 with a marked point $\mathcal{O}$.

Equivalently, an elliptic curve is the curve given by the zero locus in $\mathbb{P}^2(K)$ of a non-singular Weierstrass equation [2]

$$y^2z + a_1xyz + a_3yz^2 = x^3 + a_2x^2z + a_4xz^2 + a_6z^3, \tag{10.1.2}$$

with the point $\infty := [0:1:0]$ marked. If char $K \neq 2,3$ then (10.1.2) can be reduced to the form

$$y^2z = x^3 + c_4xz^2 + c_6z^3. \tag{10.1.3}$$

Let $F \subset K$ be a subfield of K, if the coefficients of 10.1.2 can be taken in F, we say that E is an elliptic curve defined over F.

There are two standar paths in order to define the addition law on elliptic curves. One is using intersections of lines with the curve E, we are able to define this by rational polynomials. However, even if this approach is more elemental, checking the group laws is quite messy. The other one involves the group of divisors of the curve and the main idea is to show a bijection between the Picard group $\mathrm{Pic}^0(E)$ and E itself, then, one transports the group law from $\mathrm{Pic}^0(E)$ to E. Both ways are equivalent, and if $K = \mathbb{C}$ this group law corresponds to the one induced by the quotient $\mathbb{C}/\Lambda$ in the algebraic curve.

We also have a nice behavior in the torsion points of E

[1] The $a_{p^\alpha}(E)$ are defined in terms of the number of points in extensions of $\mathbb{F}_p$ of the reduction of E modulo p, it turns out that the $a_{p^\alpha}(E)$ yield a multiplicative relation we can factor in the L-function. See [DS05, Ch. 8.3].

[2] This actually means that every elliptic curve is isomorphic to a plane curve described by some Weierstrass equation, sending $\mathcal{O}$ to the point at infinity.

Theorem 10.1.3. *Let K be an algebraic closed field, and let $(E, \mathcal{O})$ be an elliptic curve over K. For $N \in \mathbb{N}$, denote the N-torsion points of E by $E[N]$. Then*

$$E[N] = \bigoplus_{p^\alpha || N} E[p^\alpha] \tag{10.1.4}$$

- *If* $\mathrm{char} K \nmid p$ *we have*

$$E[p^\alpha] \cong \mathbb{Z}/p^\alpha\mathbb{Z} \times \mathbb{Z}/p^\alpha\mathbb{Z}.$$

- *If* $\mathrm{char} K = p$ *then*

$$E[p^\alpha] \cong \left\{ \begin{array}{l} \mathbb{Z}/p^\alpha\mathbb{Z}, \\ 0. \end{array} \right.$$

If $\mathrm{char} K = p \neq 0$ and $E[p] = 0$ we say that E is *supersingular*, otherwise E is called *ordinary.*

Once again, if E is defined over $F \subset K$, the algebraic equations of the addition law are rational functions over F. Hence, the torsion points have algebraic coordinates showing that it is enough to work in $\overline{F}$. The representations attached to elliptic curves over general fields F are defined similarly as in the rational-complex case, via the Tate modules of E and the absolute Galois group of F. In particular, one can apply some reduction theorems from $\mathbb{Q}$ to $\mathbb{F}_p$ and deduce, for instance, unramification and flatness of Galois representations attached to an elliptic curve E, studying the Galois representations attached to the reductions of E modulo p.

10.2 Galois representations from modular forms

To attach Galois representations to modular forms requires more work than to elliptic curves. Here we will present the idea in the case of cuspidal forms of weight $k = 2$. The case $k > 2$ was made by Delinge and the case $k = 1$ by Delinge-Serre, Eisenstein series will become also eigenforms and their attached representations are reducible. See [DS05, Ch. 9.6] for the representations attached to Eisenstein series.

For each congruence subgroup $\Gamma_1(N)$ and $\Gamma_0(N)$ we have the modular curves $X_1(N)$ and $X_0(N)$. In general, let M be a compact Riemann surface of genus g, there is an abelian variety of dimension g associated to M called the *Jacobian variety* of M, denoted by $\mathrm{Jac}(M)$. This abelian varierty is defined in terms of the dual of holomorphic differentials $\Omega^1_{\mathrm{hol}}(M)$ and the first homology group $H_1(M, \mathbb{Z})$. Indeed, the group $H^1(M, \mathbb{Z})$ is $\mathbb{Z}$-free of rank $2g$ generated by $2g$ loops on M. Path integrals over M give elements in $\Omega^1_{\mathrm{hol}}(M)^\wedge$, then we may think of $H_1(M, \mathbb{Z})$ lying inside $\Omega^1_{\mathrm{hol}}(M)^\wedge$. It turns out also that $\Omega^1_{\mathrm{hol}}(M)$ has dimension g over $\mathbb{C}$ by the Riemann-Roch Theorem.

All this implies that $\Omega^1_{\mathrm{hol}}(M)^\wedge / H_1(M, \mathbb{Z})$ is a complex torus of dimension g which is by definition $\mathrm{Jac}(M)$. Fix a point $x_0 \in M$ and let $x \in M$, the map $\mathrm{Div}^0(M) \longrightarrow \mathrm{Jac}(M)$ given by

$$\sum_{x \in M} n_x(x) \mapsto \sum_{x \in M} n_x \int_{x_0}^{x}$$

is well defined.

Theorem 10.2.1. *The above map descends to* $\mathrm{Pic}^0(M)$, *inducing an isomorphism*

$$\mathrm{Pic}^0(M) \longrightarrow \mathrm{Jac}(M),\ \left[\sum_x n_x x\right] \mapsto \sum_x n_x \int_{x_0}^{x}.$$

Furthermore, the injection $M \longrightarrow \mathrm{Div}^0(M),\ x \mapsto x - x_0$ induces also an injection $x \mapsto [x - x_0]$ in $\mathrm{Pic}^0(M)$. Composing with the isomorphism of Abel's theorem we have an injection

$$X \longrightarrow \mathrm{Jac}(M)$$

which turns out to be holomorphic. In the particular case of $g = 1$, M is an elliptic curve and the injection is actually an isomorphism of abelian varieties.

In the case of modular curves, the vector spaces $\Omega^1_{\mathrm{hol}}(X_i(N))$ and $S_2(\Gamma_i(N))$ are naturally isomorphic. Hence, we can think of $H_1(X_i(N), \mathbb{Z})$ as a lattice of rank $2g$ inside $S_2(\Gamma_i(N))^\wedge$ and $\mathrm{J}_i(N) = \mathrm{Jac}(X_i(N)) = S_2(\Gamma_i(N))^\wedge/(H_1(X_i(N), \mathbb{Z}))$. Hecke operators act on $S_2(\Gamma_i(N))^\wedge$ and their action remains $H_1(X_i(N), \mathbb{Z})$ stable, this shows that the Hecke algebra of weight-2 cuspidal forms is integral finitely generated over $\mathbb{Z}$. In particular, if $f \in S_2(N, \chi)$ is a normalized eigenform the following is a ring homomorphism

$$f_* : \mathbb{T}_{\mathbb{Z}} \longrightarrow \mathbb{C},\ T \mapsto Tf. \tag{10.2.1}$$

The image is a integral $\mathbb{Z}$-module of finite rank, the field generated by the image of f_* is the *number field of* f and is denoted by K_f.

Denote by I_f the kernel of f_* in (10.2.1), then $\mathrm{J}_1(N)/I_f\mathrm{J}_1(N)$ is an abelian variety of dimension $d = [K_f : \mathbb{Q}]$, we write A_f for this object. In particular, the Hecke operator T_n acts as $a_n(f)$ in A_f.

All this machinery is necessary to show the existence of Galois representations attached to cuspidal eigenforms for $k = 2$. The idea is similar to elliptic curves: we use the N-torsion points of $\mathrm{J}_1(N)$ and A_f. We explain quickly this construction, see [DS05, Ch. 7 - 9] for a more detailed treatment of this. The next theorem explains the behaviour of the Hecke operators on the modular curves $X_1(N)$ and $X_0(N)$ and their reductions $\tilde{X}_i(N)$ modulo p

Theorem 10.2.2 (Eichler-Shimura relations)**.** *Let* $p \nmid N$. *The following diagrams commutes* [3]*:*

$$\begin{tikzcd}
\mathrm{Pic}^0(X_1(N)) \arrow[r, "T_p"] \arrow[d] & \mathrm{Pic}^0(X_1(N)) \arrow[d] \\
\mathrm{Pic}^0(\tilde{X}_1(N)) \arrow[r, "\sigma_{p,*}+\tilde{\langle p\rangle}_*\sigma_p^*"] & \mathrm{Pic}^0(\tilde{X}_1(N))
\end{tikzcd}$$

In particular,

$$\begin{tikzcd}
\mathrm{Pic}^0(X_0(N)) \arrow[r, "T_p"] \arrow[d] & \mathrm{Pic}^0(X_0(N)) \arrow[d] \\
\mathrm{Pic}^0(\tilde{X}_0(N)) \arrow[r, "\sigma_{p,*}+\sigma_p^*"] & \mathrm{Pic}^0(\tilde{X}_0(N))
\end{tikzcd}$$

Igusa's theorem, [DS05, Ch. 8], states that $X_1(N)$ has good reduction for $p \nmid N$. This implies, modulo more algebraic geometry, that the group of p^n-torsion points $\mathrm{Pic}^0(X_1(N))[p^n]$ and $\mathrm{Pic}^0(\tilde{X}_1(N))[p^n]$ are isomorphic. The *Tate ℓ module of* $X_1(N)$ is

[3] As we mentioned in section 9.1, the Hecke operators act on divisors. The vertical maps are reduction of the algebraic modular curves over $\mathbb{Q}$, σ_p is the Frobenius map and the labels $\alpha_{p,*}$ and α_p^* mean the pushforward and pullback of σ_p respectively. A tilde symbol over an operator in $X_i(N)$ is its reduction to $\tilde{X}_i(N)$.

$$\mathrm{Ta}_\ell(\mathrm{Pic}^0(X_1(N))) = \varprojlim_{n\in\mathbb{N}} \mathrm{Pic}^0(X_1(N))[\ell^n] \cong \mathbb{Z}_\ell^{2g}. \tag{10.2.2}$$

The Galois group $G_\mathbb{Q}$ acts on $\mathrm{Pic}^0(X_1(N))$ in a natural way and this action is compatible with (10.2.2). Hence, we get a representation

$$\rho_{\ell,X_1(N)} : G_\mathbb{Q} \longrightarrow \mathrm{Aut}(\mathrm{Ta}_\ell(\mathrm{Pic}^0(X_1(N)))) \cong GL_{2g}(\mathbb{Z}_\ell).$$

The Eichler-Shimura relations implies the following theorem

Theorem 10.2.3. *Let ℓ be a prime and N be a positive integer. The Galois representation $\rho_{\ell,X_1(N)}$ is unramified at every prime $p \nmid \ell N$. For any such p let Frob_p be a Frobenius element of p, then $\rho_{\ell,X_1(N)}$ satisfies the polynomial equation*

$$x^2 - T_p x + \langle p\rangle p = 0.$$

The ℓ^n-torsion points will surject the ℓ^n torsion points of A_f and the kernel of

$$\mathrm{Pic}^0(X_1(N))[\ell^n] \longrightarrow A_f[\ell^n]$$

is stable under $G_\mathbb{Q}$. Therefore, $\rho_{\ell,X_1(N)}$ projects to a representation

$$\rho_{A_f,\ell} : G_\mathbb{Q} \longrightarrow \mathrm{Aut}(\mathrm{Ta}_\ell(A_f)).$$

Write $V_\ell(A_f) = \mathrm{Ta}_\ell(A_f) \otimes \mathbb{Q}$. Denote the image of f_* in (10.2.1) by $\mathcal{O}_f$, then $K_f = \mathcal{O}_f \otimes \mathbb{Q}$. The $G_\mathbb{Q}$-module $V_\ell(A_f)$ turns out to be a free $\mathcal{O}_f \otimes \mathbb{Q}_\ell \cong K_f \otimes_\mathbb{Q} \mathbb{Q}_\ell$-module of rank 2. Moreover, the ring $K_f \otimes_\mathbb{Q} \mathbb{Q}_\ell$ is isomorphic to

$$K_f \otimes_\mathbb{Q} \mathbb{Q}_\ell \cong \prod_{\lambda|\ell} K_{f,\lambda}.$$

This implies that the representation ρ_{ℓ,A_f} can be thought as a continuous group homomorphism

$$\rho_{\ell,A_f} : G_\mathbb{Q} \longrightarrow \mathrm{GL}_2(K_f \otimes_\mathbb{Q} \mathbb{Q}_\ell) \cong \prod_{\lambda|\ell} \mathrm{GL}_2(K_{f,\lambda}).$$

The above discution and Igusa's theorem imply the following theorem:

Theorem 10.2.4. *Let $f \in S_2(N,\chi)$ be a normalized eigenform with number field K_f. Let ℓ a prime. For each maximal ideal λ of $\mathcal{O}_{K_f}$ lying over ℓ there is a 2-dimensional Galois representation*

$$\rho_{f,\lambda} : G_\mathbb{Q} \longrightarrow \mathrm{GL}_2(K_{f,\lambda}).$$

This representation is unramified at every prime $p \neq \ell N$. For any such p let Frob_p be a Frobenius element over p. Then $\rho_{f,\lambda}(\mathrm{Frob}_p)$ satisfies the polynomial equation

$$x^2 - a_p(f)x + \chi(p)p = 0.$$

In particular, if $f \in S_2(\Gamma_0(N))$ then the relation is $x^2 - a_p(f)x + p = 0$.

Theorem 10.2.4 generalizes to weights different from 2

Theorem 10.2.5. *Let $f \in S_k(N, \chi)$ be a normalized eigenform with number field K_f. Let ℓ be a prime. For each maximal ideal λ of $\mathcal{O}_{K_f}$ lying over ℓ there exists a 2-dimensional Galois representation*

$$\rho_{f,\lambda} : G_{\mathbb{Q}} \longrightarrow \mathrm{GL}_2(K_{f,\lambda}).$$

This representation is unramified at all primes $p \nmid \ell N$. For any such p let Frob_p *be a Frobenius element over p, then the characteristic equation of $\rho_{f,\lambda}(\mathrm{Frob}_p)$ is*

$$x^2 - a_p(f)x + \chi(p)p^{k-1} = 0.$$

Even if the module of a continuous representations $\rho : G_{\mathbb{Q}} \longrightarrow \mathrm{GL}_2(K_{f,\lambda})$ is not a free rank-2 module over $\mathcal{O}_{K_f,\lambda}$, we can reduce ρ to a representation $\tilde{\rho} : G_{\mathbb{Q}} \longrightarrow \mathrm{GL}_2(\mathcal{O}_{K_f,\lambda})$, after some restriction to an $\mathcal{O}_{K_f,\lambda}$-submodule and a choice of $\mathcal{O}_{K_f,\lambda}$-basis. Briefly, take A to be the image of $\mathcal{O}^2_{K_f,\lambda}$ by ρ. Then, A is a compact $\mathcal{O}_{f,\lambda}$ module contaning $\mathcal{O}_{K_f,\lambda}$, hence it is contained in $\frac{1}{M}\mathcal{O}_{K_f,\lambda}$ for some M. This shows that A is an $\mathcal{O}_{K_f,\lambda}$-module of rank 2. A choice of a basis of A gives us the desire representation equivalent to ρ:

$$\tilde{\rho} : G_{\mathbb{Q}} \longrightarrow \mathrm{GL}_2(\mathcal{O}_{K_f,\lambda}).$$

10.3 Versions of the Modularity Theorem

There are may versions of modularity, some concerning L-functions of elliptic curves and modular forms, another related to Galois representations, and others which are more geometric. Here we state some versions of modularity, for the definition of a complex elliptic curve recall section 10.1 and for the definition of the J invariant of an elliptic curve see [DS05, Ch. 2], for a better and more complete approach to the theory of elliptic curves [Sil09] is highly recommended.

The first version of modularity stated here is a geometric one. The connection towards L-functions and galois representations is due to the Hecke operators acting on the Jacobian variety $J_1(N)$ and the abelian varieties A_f. In [DS05, Ch. 8] the reader can find the idea behind and some other references.

Theorem 10.3.1 (Modularity Theorem, version $X_{\mathbb{C}}$). *Let E be a complex elliptic curve with $j(E) \in \mathbb{Q}$. Then for some N there exist a surjective morphism of complex Riemann surfaces*

$$X_0(N) \longrightarrow E.$$

The minimal N in the rational version of the previuos version of modularity (that is, $X_1(N)$ and E as algebraic varieties over $\mathbb{Q}$ instead as Riemann surfaces) is called the *analytic conductor* of the elliptic curve E. It turns out to be equal to the algebraic conductor, so we refer to both simply as the *conductor* of E. The other versions of modularity are the following ones:

Theorem 10.3.2 (Modularity Theorem, version a_p). *Let E be an elliptic curve over $\mathbb{Q}$ with conductor N_E. Then for some newform $f \in S_2(\Gamma_0(N_E))$,*

$$a_p(f) = a_p(E) \text{ for all primes } p.$$

The Euler product of L-series of eigenforms and elliptic curves leads to the following equivalent version of modularity

Theorem 10.3.3 (Modularity Theorem, version L). *Let E be an elliptic curve over $\mathbb{Q}$ with conductor N_E. Then for some newform $f \in S_2(\Gamma_0(N_E))$,*

$$L(s, f) = L(s, E)$$

To state the final version of modularity involving Galois representation we need to say when a Galois representation to $\mathbb{Q}_\ell$ is modular:

Definition 10.3.1. An irreducible Galois representation

$$\rho : G_{\mathbb{Q}} \longrightarrow \mathrm{GL}_2(\mathbb{Q}_\ell)$$

such that $\det \rho = \chi_\ell$ is *modular* is there exists a newform $f \in S_2(\Gamma_0(M_f))$ such that $K_{f,\lambda} = \mathbb{Q}_\ell$ for some maximal ideal of $\mathcal{O}_{K_f}$ lying over ℓ and such that $\rho_{f,\lambda} \sim \rho$.

Theorem 10.3.4 (Modularity Theorem, version R)**.** *Let E be an elliptic curve over $\mathbb{Q}$. Then $\rho_{E,\ell}$ is modular for some ℓ.*

This last version can be improved to a stronger theorem.

Theorem 10.3.5 (Modularity Theorem, strong version R)**.** *Let E be an elliptic curve over $\mathbb{Q}$ with conductor N_E. Then for some newform $f \in S_2(\Gamma_0(N_E))$ with number field $K_f = \mathbb{Q}$,*

$$\rho_{f,\lambda} = \rho_{E,\ell} \textit{ forr all } \ell.$$

Version R implies version a_p of modularity in the following way: let $f \in S_2(\Gamma_0(M_f))$ be a normalized eigenform with number field K_f and λ a maximal ideal of $\mathcal{O}_{K_f}$ such that $K_{f,\lambda} = \mathbb{Q}_\ell$. Suppose $\rho_{f,\lambda} \sim \rho_{E,\ell}$, then the trace of $\rho_{E,\ell}(\mathrm{Frob}_p)$ is equal to the trace of $\rho_{f,\lambda}(\mathrm{Frob}_p)$ for all $p \nmid \ell M_f N_E$. The work of Carayol in [Car86] implies the equality for all prime p.

On the other hand, version a_p implies strong version R. Let ℓ be a prime number, version a_p implies that the caracteristic polynomials of $\rho_{f,\lambda}$ and $\rho_{E,\ell}$ are the same in Frobenius elements for all but finitely many p. The Chebotarev density theorem says that both characteristic polynomials are equal in a dense subset of $G_{\mathbb{Q}}$ and therefore they are equal for all element in $G_{\mathbb{Q}}$. Since the representation from f is odd and irreducible, both representations $\rho_{E,\ell}$ and $\rho_{f,\lambda}$ must be equivalent, this is the content of Exercise 9.6.1 in [DS05].

Chapter 11

Role of deformation theory in Wiles' proof

Wiles' proof of the Taniyama-Shimura conjecture is the outcome of the combined effort of many mathematicians through our history, specially in the last century when the main advances in algebraic number theory, class field theory, elliptic curves, modular forms and representation theory were made. Nevertheless, we must not forget the importance of the whole-picture view of Wiles which allowed him to give a proof of the modularity conjecture therefore proving Fermat's last theorem. In this chapter we want to highlight the importance of deformation theory in Wiles' result; the main work is [Wil95].

Roughly speaking, two of the vital facts for the Wiles' proof are the following: one is that representations for which certain conditions related with semistability of elliptic curves hold are modular in a slightly more general sense than the one defined in section 10.2. The second concerns the special case of semistable elliptic curves, this is, for E a semistable elliptic curve over $\mathbb{Q}$, $\overline{\rho}_{E,3}$ or $\overline{\rho}_{E,5}$ is absolutely irreducible. If $\overline{\rho}_{E,3}$ turns out to be irreducible, then it will be modular because of a Theorem of Langlands and Tunnell. Otherwise, if $\overline{\rho}_{E,5}$ is irreducible, Wiles was able to change the elliptic curve E by another semistable elliptic curve E' such that

- $\overline{\rho}_{E,5} \cong \overline{\rho}_{E',5}$,
- $\overline{\rho}_{E',3}$ is irreducible.

The modularity of E will follow from the modularity of some 3-torsion points representation. Certainly the work in the proof cannot be reduced to one or two simple pages, it involves lots of deep mathematics results which could not be summarized in this chapter. Therefore I invite the reader to review the literature, for instance [CSS97], for a good overwiew of proof and more references. We shall follow very closely the overview of the proof in [CSS97].

We begin discussing modularity at the level of coefficient rings. As in part I, let p be a prime number and let k be a finite field of characteristic p. Let $N > 0$ be an integer and let $S_2(N)$ denote the space of weight 2 cusp forms for $\Gamma_1(N)$. Let

$$\mathbb{T}(N) := \mathbb{Z}[T_\ell, \langle d \rangle] \subset \mathrm{End}(S_2(N))$$

be the $\mathbb{Z}$-subalgebra of $\mathrm{End}(S_2(N))$ generated by the Hecke operators T_ℓ and the diamond operators $\langle d \rangle$ where ℓ runs over all primes not dividing pN, and d runs over $(\mathbb{Z}/N\mathbb{Z})^*$.

Definition 11.0.1. A Galois representation

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

over a coefficient ring A is *modular* if there exists an integer $N > 0$ and a homomorphism $\pi : \mathbb{T}(N) \longrightarrow A$ such that ρ is unramified outside Np, and for every prime $\ell \nmid Np$ we have

$$Tr(\rho(\mathrm{Frob}_\ell)) = \pi(T_\ell) \quad \text{and} \quad \det(\rho(\mathrm{Frob}_\ell)) = \pi(\langle \ell \rangle)\ell.$$

Note that this is a deformation condition in the sense of Definition 7.1.1, provided the residual representation is modular. Let $\overline{\rho} : G_{\mathbb{Q}} \longrightarrow \mathrm{GL}_2(k)$ be a residual representation.

We are going to impose some contidions on our representation $\overline{\rho}$, these arise naturally from elliptic curves and modular forms. A necessary one is Fixed Determinant.

Condition A. $\overline{\rho}$ has determinant χ_p, where χ_p is the Teichmüller lifting.

Definition 11.0.2. A Galois representation

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

is *semistable* at a prime ℓ if one of the following conditions holds

- $\ell = p$ and ρ is either flat or ordinary at p[1].
- $\ell \neq p$ and $\rho|_{I_\ell} \sim \begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix}$

We say that a Galois representation is semistable if it is semistable at every prime. Again, this turns out to be a deformation condition.

Condition B. $\overline{\rho}$ is semistable.

Now we define the appropiate deformation condition $\mathcal{D}$. Let $S := \{\ell \neq p : \overline{\rho} \text{ is ramified at } \ell\}$ (a finite set). Let $\Sigma_{\mathcal{D}}$ be a finite set of primes disjoint from S. We say that a deformation ρ of $\overline{\rho}$ is of type $\mathcal{D}$ if the following conditions hold

- ρ has determinant χ_p,
- ρ is unramified outside $S \cup \{p\} \cup \Sigma_{\mathcal{D}}$,
- ρ is semistable outside $\Sigma_{\mathcal{D}}$,
- if $p \notin \Sigma_{\mathcal{D}}$ and if $\overline{\rho}$ is flat at p, then ρ is also flat at p.

The second item leads us to factor the deformations through $G_{\mathbb{Q},S'}$, where $S' = S \cup \{p\} \cup \Sigma_{\mathcal{D}}$, a group where our theory works.

In order for the deformation functor to be modular we need to impose the absolutely irreducible condition on the residual representation $\overline{\rho}$.

Condition C. $\overline{\rho}$ is absolutely irreducible.

Hence, Mazur's theory associates the universal deformation rind $\mathcal{R}_{\mathcal{D}}$ of deformations of $\overline{\rho}$ of type $\mathcal{D}$, and an universal deformation $\rho_{\mathcal{D}}$ of type $\mathcal{D}$. Define the additional condition:

Condition D. $\overline{\rho}$ is modular and $\overline{\rho}|_{G_{\mathbb{Q}(\sqrt{-3})}}$ is absolutely irreducible.

Hence, we also have the ring $\mathbb{T}_{\mathcal{D}}$ of universal modular deformations of $\overline{\rho}$ of type $\mathcal{D}$, and an universal modular deformation $\rho_{\mathcal{D},\mathrm{mod}}$ of type $\mathcal{D}$. The universal property of $\mathcal{R}_{\mathcal{D}}$ gives us a canonical map

[1] This definition of "ordinary" in this case does not coincide with the one introduced in this document, however it is quite similar and is found in Chapter 1 of [CSS97].

$$\varphi_{\mathcal{D}} : \mathcal{R}_{\mathcal{D}} \longrightarrow \mathbb{T}_{\mathcal{D}}.$$

Wiles proved the following theorem

Theorem 11.0.1. *Suppose $\overline{\rho}$ satisfies conditions A to D. Then the canonical map $\varphi_{\mathcal{D}} : \mathcal{R}_{\mathcal{D}} \longrightarrow \mathbb{T}_{\mathcal{D}}$ is an isomorphism of complete intersection rings.*

Corollary 11.0.1.1. *Suppose $\overline{\rho}$ satisfies conditions A to D. Then every deformation of $\overline{\rho}$ of type $\mathcal{D}$ is modular.*

The strategy of Wiles for proving the above theorem was comparing both rings with other complete discrete valuarion ring and using a numerical criterion, which is highly no trivial.

Appendix A

Complete tensor product

We will introduce the construction of the completed tensor product of R-modules for a topological ring R. Let N and M be R-modules and let $\{N_\mu\}$, $\{M_\nu\}$ be basis of open submodules at 0 of N and M respectively. Define a topology for $N \otimes_R M$ by declaring as open the following submodules

$$(N \otimes M)_{\mu,\nu} = \operatorname{Im}(N_\mu \otimes_R M + N \otimes_R M_\nu \longrightarrow N \otimes_R M), \text{ for all } \mu, \nu.$$

We have the following commutative diagram with exact rows and columns

$$\begin{tikzcd}
N_\mu \otimes M_\nu \arrow[r] \arrow[d] & N \otimes M_\nu \arrow[r] \arrow[d] & N/N_\mu \otimes M_\nu \arrow[r] \arrow[d] & 0 \\
N_\mu \otimes M \arrow[r] \arrow[d] & N \otimes M \arrow[r] \arrow[d] & N/N_\mu \otimes M \arrow[r] \arrow[d] & 0 \\
N_\mu \otimes M/M_\nu \arrow[r] \arrow[d] & N \otimes M/M_\nu \arrow[r] \arrow[d] & N/N_\mu \otimes M/M_\nu \arrow[r] \arrow[d] & 0 \\
0 & 0 & 0 &
\end{tikzcd}$$

A diagram chasing argument shows that

$$\ker(N \otimes M \longrightarrow N/N_\mu \otimes M/M_\nu) = (N \otimes M)_{\mu,\nu}$$

We define the *completed tensor product* of N and M, denoted by $N\hat{\otimes}_R M$ as the completion of $N \otimes M$ with respect to the submodules $(N \otimes M)_{\mu,\nu}$, or equivalently as the inverse limit

$$N\hat{\otimes}_R M = \varprojlim_{\mu,\nu} N \otimes M/(N \otimes M)_{\mu,\nu} = \varprojlim_{\mu,\nu} N/N_\mu \otimes M/M_\nu.$$

Now, let A, B be coefficient Λ-algebras. We contend that $A\hat{\otimes}_\Lambda B$ is a coefficient Λ-algebra. Let $\mathfrak{m}_A$ and $\mathfrak{m}_B$ be the maximal ideals of A and B respectively, making an abuse of language, a system of open submodules in $A \otimes_\Lambda B$ is $\{\mathfrak{m}_A^k \otimes B + A \otimes \mathfrak{m}_B^l\}$ for $k, l \in \mathbb{N}$. Take $\mathfrak{M} = \mathfrak{m}_A \otimes B + A \otimes \mathfrak{m}_B$. We contend that $A\hat{\otimes}_\Lambda B$ is the $\mathfrak{M}$-adic completion of $A \otimes_\Lambda B$, since $\mathfrak{M}$ is finitely generated $A \otimes_\Lambda B$-module and $A \otimes_\Lambda B/\mathfrak{M} = k$ is a field, then $A\hat{\otimes}_\Lambda B$ will be noetherian; this is a consequence of Corollary 10.25 of [AM69].

Since the pairs $\{(k, k) : k \in \mathbb{N}\}$ are cofinal in $\mathbb{N} \times \mathbb{N}$ then

$$A\hat{\otimes}_\Lambda B = \varprojlim_{k,l} A/\mathfrak{m}_A^k \otimes B/\mathfrak{m}_B^l = \varprojlim_{k} A/\mathfrak{m}_A^k \otimes B/\mathfrak{m}_B^k$$

$$\mathfrak{m}_A^{2n} \otimes B + A \otimes \mathfrak{m}_B^{2n} \subseteq \mathfrak{M}^{2n} \subseteq \mathfrak{m}_A^n \otimes B + A \otimes \mathfrak{m}_B^n.$$

This proves that the topology given by the neighborhoods $\mathfrak{m}_A^n \otimes B + A \otimes \mathfrak{m}_B^n$ is the same as the $\mathfrak{M}$-adic topology and $A \hat{\otimes}_\Lambda B$ is just the $\mathfrak{M}$-adic completion. We have

$$A \otimes_\Lambda B / \mathfrak{M} \cong k \otimes_k k = k,$$

so $\mathfrak{M}$ is maximal. We have also that $1 + \mathfrak{M}$ are units in $A \hat{\otimes}_\Lambda B$, therefore $\hat{\mathfrak{M}}$, the $\mathfrak{M}$-adic completion of $\mathfrak{M}$, is the unique maximal ideal of $A \hat{\otimes}_\Lambda B$ proving that it is a coefficient Λ-algebra.

Appendix B

Grothendieck's theorem

The reader can see [Gro60] for a more general treatment of the concepts introduced in this Appendix. We being with the statement of the theorem, for the definitions of $\mathcal{C}^0_\Lambda$, tangent space of $\mathbf{F}$ and Mayer-Vietoris property go to Chapters 2 and 3.

Theorem B.1 (Grothendieck)**.** *Let*

$$\mathbf{F} : \mathcal{C}^0_\Lambda \longrightarrow \mathit{Sets}$$

be a covariant functor such that $\mathbf{F}(k)$ *is a singleton. Then* $\mathbf{F}$ *is pro-representable if and only if*

i. $\mathbf{F}$ *satisfies the Mayer-Vietoris property.*

ii. $\mathbf{F}(k[\epsilon])$ *is a finite dimensional vector space.*

Let us introduce some notation and results before giving a proof of this theorem. Through this Appendix $\mathbf{F}$ shall denote a covariant functor such that $\mathbf{F}(k)$ is a point.

Definition B.1. Let $\mathcal{C}^0_\Lambda$ be the category of artinian coefficient Λ-algebras. Let A be an object of $\mathcal{C}^0_\Lambda$ and let $\xi \in \mathbf{F}(A)$. We say that the pair (A, ξ) is *minimal* if for every pair (A', ξ') with $\xi' \in \mathbf{F}(A')$ and every monomorphism $v : A' \longrightarrow A$ such that $\mathbf{F}(v)(\xi') = \xi$ we get that v is an isomorphism. We say that a pair (A', ξ') *dominates* (A, ξ) if there is a morphism $v : A' \longrightarrow A$ such that $\mathbf{F}(v)(\xi') = \xi$.

Remark. Since the objects in $\mathcal{C}^0_\Lambda$ are artinian, there exist minimal pairs in this category. Moreover, every pair is dominated by a minimal pair.

Lemma B.1. *The followings are equivalent*

i. $\mathbf{F}$ *is left exact, i.e. it preserves finite limits.*

ii. $\mathbf{F}$ *preserves equalizers and finite products.*

iii. $\mathbf{F}$ *has the Mayer-Vietoris property.*

Proof. Every finite limit can be constructed by equalizers and finite products, so (*ii*) implies (*i*). Clearly (*i*) implies (*iii*) because fiber products are finite limits. Finally for (*iii*) impies (*ii*), k is a final object then finite products can be seen as fiber products over k. Equalizers can be constructed as follows:

Given two morphisms $u, v : A \longrightarrow B$ let $A \times_B A$ be their fiber product. Then, consider the maps $p : A \times_B A \longrightarrow A \times_k A$ and $\Delta : A \longrightarrow A \times_k A$ (diagonal), and let E be their fiber product. One can checks that E is the equaliser of u and v.

□

Lemma B.2. *Suppose (A', ξ') dominates (A, ξ) with a morphism $v : A' \longrightarrow A$.*

i. If (A, ξ) is minimal then v is surjective.

ii. If (A', ξ') is minimal and $\mathbf{F}$ is left exact then v is unique.

Proof. For (i) we factorize v as

$$\begin{tikzcd} A' \arrow[r, "\pi"] \arrow[dr, "v"'] & A'/\ker v \arrow[d, "\overline{v}"] . \\ & A \end{tikzcd}$$

Therefore $(A'/\ker v, \mathbf{F}(\pi)(\xi'))$ dominates (A, ξ) with $\overline{v}$ a monomorphism, so $\overline{v}$ is an isomorphism and v a surjection.

For (ii), let $u, v : A' \longrightarrow A$ be two morphisms such that $\mathbf{F}(u)(\xi') = \mathbf{F}(v)(\xi') = \xi$. Let $Eq : E \longrightarrow A'$ be an equalizer for u, v. Since $\mathbf{F}$ is left exact, there exists $\zeta \in \mathbf{F}(E)$ such that $\mathbf{F}(Eq)(\zeta) = \xi$. Then (E, ζ) dominates (A', ξ') and by (i) Eq is surjective and so $u = v$.

□

Proof of Theorem B.1. If $\mathbf{F}$ is pro-representable then $\mathbf{F}$ preserves finite limits, in particular fiber products, and the tangent space $\mathbf{F}(k[\epsilon])$ is equal to the tangent space of some coefficient Λ-algebra, so it is a finite dimensional vector space over k.

Conversely, it is immediate to note that the set of minimal pairs (A, ξ) forms a directed set using fiber products and minimal dominance. Unicity in Lemma B.2 shows that it induces a well defined inverse surjective system in the rings A. Let

$$R := \varprojlim_{(A,\xi)} A.$$

Surjectivity of the system proves that R is a complete local ring with residue field k. We wish to prove that R represents $\mathbf{F}$ and that it is actually a noetherian ring. For each minimal pair (A, ξ) we have a natural transformation

$$\vartheta^A : \mathrm{Hom}(A, \cdot\,) \longrightarrow \mathbf{F}$$

such that for each ring homomorphism $\varphi : A \longrightarrow B$ we define

$$\vartheta^A_B(\varphi) := \mathbf{F}(\varphi)(\xi).$$

If $v : A' \longrightarrow A$ induces a dominance of (A', ξ') over (A, ξ) then we get a canonical morphism of functors $\mathrm{Hom}(A, \cdot\,) \longrightarrow \mathrm{Hom}(A', \cdot\,)$ which is compatible with the natural transformations described above. Hence we get a directed system of functors $\mathrm{Hom}(A, \cdot\,)$ and a canonical natural transformation

$$\vartheta : \varinjlim_{(A,\xi)} \mathrm{Hom}(A, \cdot\,) \longrightarrow \mathbf{F}.$$

We claim that ϑ is an equivalence of functors. Let B be an object of $\mathcal{C}^0_\Lambda$, we must show that

$$\vartheta_B : \varinjlim_{(A,\xi)} \mathrm{Hom}(A, B) \longrightarrow \mathbf{F}(B)$$

is a bijection. Let $\zeta \in \mathbf{F}(B)$, then (B, ζ) is dominated by a minimal pair (A, ξ) and therefore ϑ_B is surjective. Let (A_i, ξ_i) be minimal pairs and $\varphi_i : A_i \longrightarrow B$ $(i = 1, 2)$ such that $\mathbf{F}(\varphi_1)(\xi_1) = \mathbf{F}(\varphi_2)(\xi_2)$. Let (A_3, ξ_3) be a minimal pair dominating (A_1, ξ_1) and (A_2, ξ_2). Hence by Lemma B.2 we have the commutative diagram

$$\begin{tikzcd}
A_3 \arrow[r] \arrow[d] & A_1 \arrow[d, "\varphi_1"] \\
A_2 \arrow[r, "\varphi_2"'] & B
\end{tikzcd}$$

Then φ_1 and φ_2 induce the same element in the direct limit and ϑ_B is injective.

Finally, it remains to show that

$$\varinjlim_{(A,\xi)} \operatorname{Hom}(A, \cdot\,) = \operatorname{Hom}(R, \cdot\,)$$

because if this equality holds, by finite dimensionality of the tangent space, the maximal ideal of R is finitely generated and R is noethetian. The natural homomorphisms $R \longrightarrow A$ where (A, ξ) is minimal give compatible functions

$$\operatorname{Hom}(A, \cdot\,) \longrightarrow \operatorname{Hom}(R, \cdot\,)$$

and thus we get a canonical function

$$\varinjlim_{(A,\xi)} \operatorname{Hom}(A, \cdot\,) \longrightarrow \operatorname{Hom}(R, \cdot\,) \tag{.1}$$

which is clearly inyective. For proving that it is also surjective, let B be an artinian Λ-algebra and let $\psi : R \longrightarrow B$ be a local ring homomorphism. The image $\overline{R}$ of R in B is then an artinian coefficient Λ-algebra and is a projective limit of quotients of artinian Λ-algebras

$$\overline{R} = \varprojlim_{(A,\xi)} A/I_\xi$$

However, since $\overline{R}$ is of finite length this new inverse system is stationary. Quotients of minimal pairs are minimal pairs, then there exists (A, ξ) minimal and an isomorphism $\varphi : A \longrightarrow \overline{R}$ such that the following diagram commutes

$$\begin{tikzcd}
R \arrow[r, "\pi_A"] \arrow[dr] & A \arrow[d, "\varphi"] \\
 & \overline{R}
\end{tikzcd}$$

Therefore we have the following diagram and thus we have a surjection in (.1).

$$\begin{tikzcd}
R \arrow[r, "\pi_A"] \arrow[dr, "\psi"'] & A \arrow[d, "\varphi"] \\
 & B
\end{tikzcd}$$

□

Appendix C

Leopoldt's Conjecture

In this Appendix we write the original statement of Leopold's conjecture and a proof of the equivalence with the conjecture regarding the Krull's dimension of the quotient $\mathcal{R}/\mathfrak{m}_\Lambda\mathcal{R}$, where $\mathcal{R}$ is the universal deformation ring of the functor $\mathbf{D}_\Lambda$, in the case of characters; $n = 1$.

Fix a prime number p. Let K be a number field and S be a finite set of primes containing the primes above p and ∞, write S_∞ for the archimedean primes of K. Let E denote the unit group $\mathcal{O}_K^*$ of K. For $\mathfrak{p}$ a non-archimedean prime[1] denote by $U_\mathfrak{p}^{(1)} = 1 + \mathfrak{p}$ the group of principal units in $K_\mathfrak{p}$. Leopold's conjecture states that the rank $r_p(E)$ as $\mathbb{Z}_p$ module of

$$\overline{E} \cap \prod_{\mathfrak{p}|p} U_\mathfrak{p}^{(1)}$$

is $r_1 + r_2 - 1$, with E seen diagonally embedded. In the above formula r_1 and r_2 are the number of real and complex places of K respectively.

In order to show the equivalence betweem Leopoldt's conjecture and the dimension conjecture in Proposition 5.3.1 we need some notation. Let K_S^{ab} be the maximal abelian extension of K unramified outside S[2], and let M_p be the maximal abelian p-extension of K unramified outside S. Let H be the maximal unramified extension of K contained in M_p.

Let $\tilde{H}$ be the maximal abelian unramified extension of K. Global class field theory tells us that

$$G_{\tilde{H}/K} \cong Cl_K$$

where Cl_K is the class group of K. Hence, $H = \tilde{H} \cap M_p$ is the maximal abelian unramified p-extension of K, the Galois group $G_{H/K}$ corresponds to the p-Sylow subgroup of Cl_K, which we denote by $Cl_K(p)$. Thus, we have an exact sequence

$$\begin{tikzcd} 1 \arrow[r] & G_{M_p/H} \arrow[r] & G_{M_p/K} \arrow[r] & Cl_K(p) \arrow[r] & 1 . \end{tikzcd}$$

Moreover, $\tilde{H} \subset K_S^{ab}$ and let S_1 be the primes of H lying above the primes of S, keep the notation $S_{1,\infty}$ for the archimedean primes of S_1. We get a morphism of exact sequences

$$\begin{tikzcd} 1 \arrow[r] & G_{M_p/H} \arrow[r] & G_{M_p/K} \arrow[r] & Cl_K(p) \arrow[r] & 1 \\ 1 \arrow[r] & G_{H,S_1}^{ab} \arrow[r] \arrow[u] & G_{K,S}^{ab} \arrow[r] \arrow[u] & Cl_K \arrow[r] \arrow[u] & 1 \end{tikzcd}$$

[1] We may refer to non-archemedean primes as finite primes as well.

[2] In this context, given an extension L/K and infinite primes $\sigma|\alpha$ of L and K respectively, we say that α ramifies if $L_\sigma \neq K_\alpha$, otherwise we say that the extension is unramified at σ.

The vertical maps are the projection of the groups in the low row to their pro-p-completion.

In the language of class formations, see [Neu86] or [Neu99], let I_K and $C_K = I_K/K^*$ be the idèle group and the idèle class group of K respectively. The group I_K is set-theoretically the subset of the product of the completions of K at all primes, including the infinite primes, $\prod_{\mathfrak{p}} K_{\mathfrak{p}}$ consisting in tuples $(a_{\mathfrak{p}})_{\mathfrak{p}}$ for which

$$a_{\mathfrak{p}} \in U_{\mathfrak{p}} \text{ for all but finitely many } \mathfrak{p}.$$

The set $U_{\mathfrak{p}}$ is $K_{\mathfrak{p}}$ for $\mathfrak{p}$ an infinite prime and the subgroup of units of $K_{\mathfrak{p}}$ for $\mathfrak{p}$ finite. A modulus $\mathfrak{m}$ is a formal product

$$\mathfrak{m} = \prod_{\mathfrak{p}} \mathfrak{p}^{n_{\mathfrak{p}}}$$

with $n_{\mathfrak{p}} \in \mathbb{N}$ for $\mathfrak{p}$ finite, $n_{\mathfrak{p}} \in \{0,1\}$ for $\mathfrak{p}$ infinite and all but finitely many of the exponents are 0. Denote

$$I_K^{\mathfrak{m}} = \prod_{\mathfrak{p}} U_{\mathfrak{p}}^{(n_{\mathfrak{p}})},$$

where

$$U_{\mathfrak{p}}^{(n_{\mathfrak{p}})} = \begin{cases} 1 + \mathfrak{p}^{n_{\mathfrak{p}}} \text{ for } \mathfrak{p} \text{ finite, } U_{\mathfrak{p}}^{(0)} = U_{\mathfrak{p}} \text{ the units of } \mathcal{O}_{K_{\mathfrak{p}}}, \\ \mathbb{R}^* \text{ if } \mathfrak{p} \text{ is real and } n_{\mathfrak{p}} = 0, \\ \mathbb{R}^+ \text{ if } \mathfrak{p} \text{ is real and } n_{\mathfrak{p}} = 1, \\ \mathbb{C}^* \text{ if } \mathfrak{p} \text{ is complex.} \end{cases}$$

Define $C_K^{\mathfrak{m}} = I_K^{\mathfrak{m}} K^*/K^* \subset C_K$. In particular, we get an isomorphism $Cl_K \cong C_K/C_K^{1}$. Set $\infty = \prod_{\mathfrak{p}|\infty} \mathfrak{p}$ and $\mathfrak{m} = \prod_{\mathfrak{p} \in S \setminus S_\infty} \mathfrak{p}$, then we get by global class field theory

$$G_{K_S^{ab}/H} \cong G_{H,S_1}^{ab} \cong \varprojlim_{s \in \mathbb{N}} C_K^1/C_K^{\mathfrak{m}^s \infty}. \tag{.1}$$

Furthermore,

$$\begin{aligned} C_K^1/C_K^{\mathfrak{m}^s\infty} &= (I_K^1 K^*/K^*)/(I_K^{\mathfrak{m}^s\infty} K^*/K^*) \\ &= (I_K^1 K^*)/(I_K^{\mathfrak{m}^s\infty} K^*) \\ &= I_K^1/(I_K^{\mathfrak{m}^s\infty} E). \end{aligned}$$

Therefore, the product

$$\prod_{\mathfrak{p} \in S \setminus S_\infty} U_{\mathfrak{p}} \prod_{\mathfrak{p} \in S_\infty} U_{\mathfrak{p}}/U_{\mathfrak{p}}^{(1)} \tag{.2}$$

surjects onto G_{H,S_1}^{ab}. The image of $\prod_{\mathfrak{p} \in S \setminus S_\infty} U_{\mathfrak{p}}$ has kernel $\overline{E} \cap \prod_{\mathfrak{p} \in S \setminus S_\infty} U_{\mathfrak{p}}$. Indeed, let $(a_{\mathfrak{p}})_{\mathfrak{p} \in S \setminus S_\infty} \in \prod_{\mathfrak{p} \in S \setminus S_\infty} U_{\mathfrak{p}}$ be an element mapping to 1 in $I_K^1/(I_K^{\mathfrak{m}^s}\infty)$ for all $s \in \mathbb{N}$. Equation (.1) implies that there are $(b_{\mathfrak{p}}^s)_{\mathfrak{p}} \in I_K^{\mathfrak{m}^s\infty}$ and $r_s \in E$ such that

$$(a_{\mathfrak{p}}) = (b_{\mathfrak{p}}^s) r_s, \text{ for all } s \in \mathbb{N}.$$

Thus, the $\mathfrak{p}$ part of r_s for $\mathfrak{p} \in S \setminus S_\infty$ converges in $U_{\mathfrak{p}}$ and $(a_{\mathfrak{p}}) \in \overline{E} \cap \prod_{\mathfrak{p} \in S \setminus S_\infty} U_{\mathfrak{p}}$. Conversely, since E is mapped to 1 and the map is continuous, the clousure of E is mapped to 1. Hence

$$\prod_{\mathfrak{p}\in S\backslash S_\infty} U_\mathfrak{p}/(\overline{E}\cap \prod_{\mathfrak{p}\in S\backslash S_\infty} U_\mathfrak{p})$$

is mapped injectively to G^{ab}_{H,S_1} and its cokernel is finite since it is a quotient of the product over the infinite-primes part of (.2). Note that $\overline{E}\subset \prod_{\mathfrak{p}\in S\backslash S_\infty} U_\mathfrak{p}$ but keep the intersection in the formula.

We have the following exact sequence

$$1 \longrightarrow \prod_{\mathfrak{p}\in S\backslash S_\infty} U_\mathfrak{p}/(\overline{E}\cap \prod_{\mathfrak{p}\in S\backslash S_\infty} U_\mathfrak{p}) \longrightarrow G^{ab}_{H,S_1} \longrightarrow I \longrightarrow 1$$

with I a finite elemental abelian 2-group, i.e. a finite vector space over $\mathbb{F}_2$. Tensoring with $\mathbb{Z}_p$ give us

$$1 \longrightarrow (\prod_{\mathfrak{p}\in S\backslash S_\infty} U_\mathfrak{p}/(\overline{E}\cap \prod_{\mathfrak{p}\in S\backslash S_\infty} U_\mathfrak{p}))\otimes\mathbb{Z}_p \longrightarrow G^{ab}_{H,S_1}\otimes\mathbb{Z}_p \longrightarrow I\otimes\mathbb{Z}_p \longrightarrow 1\,. \qquad (.3)$$

Since $G_{M_p/H}$ is the pro-p-completion of G^{ab}_{H,S_1} then

$$G^{ab}_{H,S_1}\otimes\mathbb{Z}_p = G_{M_p/H}.$$

It only remains to compute the first term in the exact sequence (.3). We have

$$(\prod_{\mathfrak{p}\in S\backslash S_\infty} U_\mathfrak{p}/(\overline{E}\cap \prod_{\mathfrak{p}\in S\backslash S_\infty} U_\mathfrak{p}))\otimes\mathbb{Z}_p = (\prod_{\mathfrak{p}\in S\backslash S_\infty} U_\mathfrak{p}\otimes\mathbb{Z}_p)/(\overline{E}\cap \prod_{\mathfrak{p}\in S\backslash S_\infty} U_\mathfrak{p}\otimes\mathbb{Z}_p).$$

Given a field L denote its p^∞-roots of unity by $\mu_{p^\infty}(L)$. Let $\mathfrak{p}\in S\backslash S_\infty$, if $\mathfrak{p}\nmid p$ then

$$U_\mathfrak{p}\otimes\mathbb{Z}_p = \mu_{p^\infty}(K_\mathfrak{p}).$$

On the other hand, if $\mathfrak{p}|p$ then

$$U_\mathfrak{p}\otimes\mathbb{Z}_p = U^{(1)}_\mathfrak{p}.$$

This shows that

$$\prod_{\mathfrak{p}\in S\backslash S_\infty} U_\mathfrak{p}\otimes\mathbb{Z}_p = \prod_{\substack{\mathfrak{p}\in S\backslash S_\infty\\ \mathfrak{p}\nmid p}} \mu_{p^\infty}(K_\mathfrak{p}) \times \prod_{\mathfrak{p}|p} U^{(1)}_\mathfrak{p}.$$

Consider the following exact diagram

$$\begin{tikzcd}
 & 1 & 1 & 1 & \\
1 \arrow[r] & K \arrow[r] \arrow[u] & \mathcal{S} \arrow[r] \arrow[u] & \mathcal{U} \arrow[r] \arrow[u] & 1 \\
1 \arrow[r] & \prod\limits_{\substack{\mathfrak{p}\in S\backslash S_\infty\\ \mathfrak{p}\nmid p}} \mu_{p^\infty}(K_\mathfrak{p}) \arrow[r] \arrow[u] & \prod\limits_{\mathfrak{p}\in S\backslash S_\infty} U_\mathfrak{p}\otimes\mathbb{Z}_p \arrow[r] \arrow[u] & \prod\limits_{\mathfrak{p}|p} U^{(1)}_\mathfrak{p} \arrow[r] \arrow[u] & 1 \\
1 \arrow[r] & J \arrow[r] \arrow[u] & \overline{E}\cap \prod\limits_{\mathfrak{p}\in S\backslash S_\infty} U_\mathfrak{p}\otimes\mathbb{Z}_p \arrow[r] \arrow[u] & \overline{E}\cap \prod\limits_{\mathfrak{p}|p} U^{(1)}_\mathfrak{p} \arrow[r] \arrow[u] & 1 \\
 & 1 \arrow[u] & 1 \arrow[u] & 1 \arrow[u] &
\end{tikzcd}$$

where J and K are the kernels of the corresponding maps in the rows, and $\mathcal{S}$ and $\mathcal{U}$ are the quotients of the corresponding groups in the columns. The product of the roots of unity is finite, hence the rank of $\mathcal{S}$ as $\mathbb{Z}_p$-module is equal to the rank of $\mathcal{U}$ as $\mathbb{Z}_p$-module.

Sequence .3 and the previuos remark show that

$$\text{rank}_{\mathbb{Z}_p}(G_{M_p/H}) = \text{rank}_{\mathbb{Z}_p}(\mathcal{S}) = \text{rank}(\mathcal{U}).$$

Since for $\mathfrak{p}|p$ we have $\text{rank}_{\mathbb{Z}_p}(U_{\mathfrak{p}}^{(1)}) = f_{\mathfrak{p}}e_{\mathfrak{p}}$, then

$$\text{rank}_{\mathbb{Z}_p}\left(\prod_{\mathfrak{p}|p} U_{\mathfrak{p}}^{(1)}\right) = \sum_{\mathfrak{p}|p} \text{rank}_{\mathbb{Z}}(U_{\mathfrak{p}}^{(1)}) = \sum_{\mathfrak{p}|p} f_{\mathfrak{p}}e_{\mathfrak{p}} = [K : \mathbb{Q}].$$

This shows that

$$r_p(E) + \text{rank}_{\mathbb{Z}_p}(G_{M_p/H}) = [K : \mathbb{Q}] = r_1 + 2r_2.$$

The group E has rank $r_1 + 2r_2 + 1$ as $\mathbb{Z}$-module, therefore $r_p(E) \leq r_1 + 2r_2 - 1$. Now,

$$\text{rank}_{\mathbb{Z}}(\text{Hom}(G_{K,S}, \mathbb{Z}_p)) = \text{rank}(\text{Hom}(G_{M_p/H}), \mathbb{Z}_p) = \text{rank}(G_{M_p/H}).$$

With the notation as in chapter 5, the Krull dimension of $\mathcal{R}/\mathfrak{m}_\Lambda\mathcal{R}$ is $\text{rank}_{\mathbb{Z}_p}(\text{Hom}(G_{K,S}, \mathbb{Z}_p))$. Therefore

$$\text{Krull dim}(\mathcal{R}/\mathfrak{m}\mathcal{R}) = r_1 + 2r_2 - r_p(E) \geq 1 + r_2$$

which is the same bound found in Proposition 5.3.1 for $n = 1$. This finally proves that the Leopoldt's conjecture is equivalent to the Dimension Conjecture of deformation rings of characters, i.e. that

$$r_p(E) = r_1 + 2r_2 - 1 \text{ if and only if Krull dim}(\mathcal{R}/\mathfrak{m}_\Lambda\mathcal{R}) = 1 + r_2.$$

List of Symbols

$A[[\Pi]]$ Complete A-algebra of Π. 7

A_f Abelian variety attached to f. 64

$Ad(\overline{\rho})$ Adjoint representation. 29

$C(\overline{\rho})$ Center of $\overline{\rho}$ in $M_n(k)$. 20

G_K Absolute Galois group of a field K. 4

G_{K,S_1} Galois group of K_{S_1}/K. 6

$G_{L/K}$ Galois group of the extension L/K. 4

$G_{\mathbb{Q},S}$ Galois group of $\mathbb{Q}_S/\mathbb{Q}$. 6

$H^1_{\mathcal{Q}}(\Pi, Ad(\overline{\rho}))$ Tangent space of the deformation condition $\mathcal{Q}$. 43

I_p Inertia subgroup of $G_{\mathbb{Q}_p}$. 4

J J-invariant. 56

K^s Separable closure of a field K. 4

K_f Number field of the normalized eigenform f. 64

K_{S_1} Maximal unramified extension of K outside S_1. 6

L_λ Localization of L at λ. 4

T_n Hecke operator for $n \in \mathbb{N}$. 58

T_p Hecke operator for p prime. 58

$V_{\overline{\rho}}$ Space of the representation $\overline{\rho}$. 30

$W(k)$ Ring of Witt vectors. 8

W_p Wild inertia subgroup of I_p. 4

$X(\Gamma)$ Modular curve with respect to Γ. 55

$Y(\Gamma)$ Non-compact modular with respect to Γ. 55

$[\Gamma_1\alpha\Gamma_2]_k$ Double coset operator of weight-k. 57

$[\alpha]_k$ Weight-k operator. 52

$[\beta]_k$ Weight-k operator for elements in $GL_2^+(\mathbb{Q})$. 57

Δ Discriminant cuspidal form. 55

$\Gamma(N)$ Principal congruence subgroup of level N. 53

$\Gamma_n(A)$ Kernel of the reduction map of $\mathrm{GL}_n(A)$. 9

Λ Fixed Coefficient Ring. 8

$\mathbb{F}_q$ Field with q elements. 4

$\mathbb{Q}_S$ Maximal unramified extension outside S. 5

$\mathbb{Q}_p^{tm}$ Maximal tamely ramified extension of $\mathbb{Q}_p$. 4

$\mathbb{Q}_p^{ur}$ Maximal unramified description of $\mathbb{Q}_p$. 4

$\mathbb{T}_\mathbb{C}$ Complex Hecke algebra. 58

$\mathbb{T}_\mathbb{Z}$ Hecke algebra over $\mathbb{Z}$. 58

$\mathfrak{H}$ Complex upper half plane. 52

λ_F Prime ideal of the valuation ring $\mathcal{O}_F$. 4

$\langle n \rangle$ Diamond opertor. 57

$\mathbf{D}$ Deformation functor. 9

$\mathbf{D}_I$ I-ordinary functor. 48

$\mathbf{D}_\Lambda$ Deformation functor. 9

$\mathbf{Div}(X(\Gamma))$ Divisor group of $X(\Gamma)$. 55

$\mathbf{Div}^0(X(\Gamma))$ Degree 0 divisor subgroup. 55

$\mathbf{Div}^\ell(X(\Gamma))$ Principal divisors of $X(\Gamma)$. 55

$\mathbf{Jac}(M)$ Jacobian variety of M. 63

$\mathbf{Pic}^0(X(\Gamma))$ Picard group of $X(\Gamma)$. 55

$\mathcal{E}_k(\Gamma)$ Eisenstein space. 56

$\mathcal{M}(\Gamma)$ Algebra of modular forms. 54

$\mathcal{M}_k(\Gamma)$ Weight-k modular forms with respect to Γ. 54

$\mathcal{O}_F$ Valuation ring of the local field F. 4

$\mathcal{O}_L$ Ring of integers of the global field L. 4

$\mathcal{O}_{L,\lambda}$ Valuation ring of L_λ. 4

$\mathcal{S}(\Gamma)$ Ideal of cuspidal forms. 54

$\mathcal{S}_k(\Gamma)$ Weight-k cuspidal forms with respect to Γ. 54

$\overline{\rho}$ Residual representation. 9

$\boldsymbol{\rho}$ Universal deformation. 12

$\mathcal{C}$ Category of coefficient rings. 8

$\mathcal{C}^0_\Lambda$ Category of artinian coefficient Λ-algebras. 9

$\mathcal{C}_\Lambda$ Category of coefficient Λ-algebras. 8

$\mathcal{O}(\rho_0)$ Obstruction class of ρ_0. 31

$\mathcal{R}_{\overline{\rho}}$ Universal deformation ring. 12

$j(\gamma, \tau)$ Factor of automorphy. 52

$k[\epsilon]$ Ring of dual numbers. 14

k_F Residual field of the valuation ring $\mathcal{O}_F$. 4

t_A Tangent space of the ring A. 14

t_A^* Cotangent space of the ring A. 14

$t_{\mathbf{F}}$ Tangent space of the functor $\mathbf{F}$. 17

v_F Normalized valuation of the local field F. 4

Bibliography

[AM69] M F Atiyah and I G Macdonald. *Introduction to commutative algebra.* Addison-Wesley Publishing Co., Reading, Mass. - London-Don Mills, Ont., 1969.

[BM89] Nigel Boston and Barry Mazur. Explicit universal deformations of Galois representations. In *Algebraic number theory*, volume 17 of *Adv. Stud. Pure Math.*, pages 1–21. Academic Press, Boston, MA, 1989.

[Bos91] Nigel Boston. Explicit deformation of Galois representations. *Inventiones mathematicae*, 103(1):181–196, 1991.

[Car86] Henri Carayol. Sur les représentations l-adiques associées aux formes modulaires de Hilbert. *Ann. Sci. École Norm. Sup.(4)*, 19(3):409–468, 1986.

[CF67] Edited by JWS Cassels and A Fröhlich. *Algebraic number theory.* Academic Press, 1967.

[Con13] Keith Conrad. Galois descent. Notes available at http://www. math. uconn. edu/ kconrad/blurbs/galoistheory/galoisdescent. pdf, 2013.

[CR01] Edited by Brian David Conrad and Karl Rubin. *Arithmetic algebraic geometry*, volume 9. American Mathematical Soc., 2001.

[CSS97] Edited by Gary Cornell, Joseph H Silverman, and Glenn Stevens. *Modular forms and Fermat's last theorem.* Springer Science & Business Media, 1997.

[DS05] Fred Diamond and Jerry Michael Shurman. *A first course in modular forms.* Graduate Texts in Mathematics, 228. Springer-Verlag, 2005.

[Gou99] Fernando Q Gouvêa. Deformations of Galois representations. Appendix 1 by M. Dickinson, Appendix 2 by T. Weston and Appendix 3 by M. Emerton. *Arithmetic algebraic geometry (Park City, UT, 1999)*, 9:233–406, 1999.

[Gro60] Alexander Grothendieck. Technique de descente et théorèmes d'existence en géométrie algébriques. II. Le théorème d'existence en théorie formelle des modules. *Séminaire Bourbaki*, 5:369–390, 1960.

[Hid00] Haruzo Hida. *Modular forms and Galois cohomology*, volume 69 of *Cambridge Studies in Advanced Mathematics.* Cambridge University Press, 2000.

[Lan02] Serge Lang. *Algebra. Revised third edition*, volume 211 of *Graduate Texts in Mathematics.* Springer-Verlag, New York, 2002.

[Maz89] Barry Mazur. Deforming Galois representations. In *Galois Groups over* $\mathbb{Q}$, volume 16 of *Math. Sci. Res. Inst. Publ.*, pages 385–437. Springer, New York, 1989.

[Maz97] Barry Mazur. An introduction to the deformation theory of Galois representations. In *Modular forms and Fermat's last theorem*, pages 243–311. Springer, 1997.

[Miy89] Toshitsune Miyake. *Modular forms. Translated from the Japanese by Yoshitaka Maeda.* Springer-Verlag, Berlin, 1989.

[Neu86] Jürgen Neukirch. *Class field theory*, volume 280 of *Grundlehren der Mathematischen Wissenschaften.* Springer-Verlag, Berlin, 1986.

[Neu99] Jürgen Neukirch. *Algebraic number theory*, volume 322 of *Grundlehren der Mathematischen Wissenschaften.* Springer-Verlag, Berlin, 1999.

[Rob96] Derek Robinson. *A Course in the Theory of Groups. Second edition*, volume 80 of *Graduate Texts in Mathematics.* Springer-Verlag, New York-Berlin, 1996.

[Sch68] Michael Schlessinger. Functors of Artin rings. *Transactions of the American Mathematical Society*, 130(2):208–222, 1968.

[Ser79] Jean-Pierre Serre. *Local fields. Translated from the French by Marvin Jay Greenberg*, volume 67 of *Graduate Texts in Mathematics.* Springer-Verlag, New York-Berlin, 1979.

[Shi71] Goro Shimura. *Introduction to the arithmetic theory of automorphic functions*, volume 11 of *Publications of the Mathematical Society of Japan.* Princeton University Press, Princeton, NJ, 1971.

[Sil09] Joseph H Silverman. *The arithmetic of elliptic curves*, volume 106 of *Graduate Texts in Mathematics.* Springer-Verlag, New York, second edition, 2009.

[Wil95] Andrew Wiles. Modular elliptic curves and Fermat's last theorem. *Annals of mathematics*, 141(3):443–551, 1995.