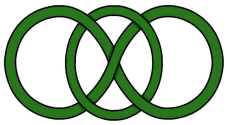
Università degli Studi di Genova

Dipartimento di Matematica

Laurea Magistrale in Matematica



Anno accademico 2023/2024

Deformations of Galois representations

Candidato
Greta Civani

Relatori
Prof. Stefano Vigni
Dott. Luca Mastella

Correlatore
Prof. Francesco Veneziano

Contents

Introduction

The theory of Galois groups and their representations lies at the heart of modern algebraic number theory. It can be considered as a powerful bridge between different areas of number theory, allowing mathematicians to translate problems of arithmetic nature into the language of linear algebra. The object of this thesis will be an introduction of deformation theory, whose theoretical results will be used to sketch a proof of the modularity theorem for elliptic curves and Fermat's Last Theorem.

We'll mainly refer to Mazur's study of deformation theory (see [7] and [8]). He was the first one to introduce the notion of deformation of a Galois representation with coefficient in a complete local noetherian ring. With this idea Mazur launched the new field of Galois deformation theory, which almost immediately found a spectacular application in Wile's proof of the Taniyama-Weil conjecture. Hence, Mazur's ideas are present in the very foundations of the strategy for establishing the modularity of Galois representations that has been extensively developed and generalized since Wiles's breakthrough on the modularity of elliptic curves.

One of the main reason to study Galois representation theory is its profound implications in areas like the theory of elliptic curves and modular forms. Indeed, for every elliptic curve E defined over $\mathbf{Q}$ and for every prime p, the absolute Galois group of $\mathbf{Q}$, $G_{\mathbf{Q}}$, acts on $\mathrm{Ta}_p(E)$, the p-adic Tate module of E. Fixing a basis of $\mathrm{Ta}_p(E)$ as $\mathbf{Z}_p$-module, we get the isomorphism $\mathrm{Ta}_p(E) \simeq \mathbf{Z}_p \times \mathbf{Z}_p$ denoting by $\mathbf{Z}_p$ the ring of p-adic integers. Then, from the action of $G_{\mathbf{Q}}$ we get a Galois representation

$$\rho_{E,p} \colon G_{\mathbf{Q}} \longrightarrow \mathrm{GL}_2(\mathbf{Z}_p).$$

Similarly, to every cuspidal newform $f = \sum_n a_n q^n \in S_2(\Gamma_1(N), \chi)$ of weight 2 we can attach a Galois representation that is defined over its Hecke field $K_f = \mathbf{Q}(\{a_n\}_{n \in \mathbf{N}})$, a totally real number field. More precisely, for every prime λ of K_f there exists a representation

$$\rho_{f,\lambda} \colon G_{\mathbf{Q}} \longrightarrow \mathrm{GL}_2(\mathcal{O}_{f,\lambda}),$$

where $\mathcal{O}_{f,\lambda}$ is the ring of integers of the completion $K_{f,\lambda}$. The modularity theorem for elliptic curves, formerly known as Shimura–Taniwama–Weil conjeture, roughly speaking states that these two representations agree. More precisely, we say that an elliptic curve $E/\mathbf{Q}$ is *modular* if there exists a prime ℓ, a newform $f \in S_2(\Gamma_1(N), \chi)$ and a prime $\lambda|\ell$ of K_f such that $K_{f,\lambda} \simeq \mathbf{Q}_\ell$ and $\rho_{E,\ell} \sim \rho_{f,\lambda}$. The modularity theorem asserts that every elliptic curve over Q is modular. Making use of deformation theory, in 1994 the British mathematician Andrew Wiles proved the following special case.

Theorem (Wiles)**.** *Every semistable elliptic curve $E/\mathbf{Q}$ is modular.*

It was thanks to Taylor's great help that Wiles completed the proof of his theorem. Meanwhile, the American mathematician Ken Ribet had already realized in 1990 that a solution of Fermat's Last Theorem could follow naturally once proved the modularity conjecture.

Theorem (FLT)**.** *The equation : $x^n + y^n = z^n$, where n is a natural number, has no non-trivial solution $a, b, c \in \mathbf{Z}$ such that $abc \neq 0$ for $n \geq 3$.*

Stated by the magistrate Pierre de Fermat in 1637, the theorem had been an open problem for centuries until the German Mathematician Gerhard Frey had a great intuition in 1986. For the first time, he realized that there was a connection between elliptic curves and FLT. The proof proceeds by contradiction. Assuming that there exists a prime number $p \geq 5$ and three integers a, b, c, not all zero, such that $a^p + b^p = c^p$ and $(a, b, c) = 1$, we can build the associated Frey's elliptic curve

$$E_{a^p,b^p,c^p} \colon y^2 = x(x - a^p)(x - b^p).$$

This curve is semistable and hence it is modular by Wiles's theorem. Therefore, there exists a new form $f \in S_2(\Gamma_1(N), \chi)$, a prime number ℓ and a prime $\lambda|\ell$ of K_f such that $\rho_{E,\ell} \sim \rho_{f,\lambda}$. By a theorem of Ribet (Theorem 4.7.5 in this thesis) there exists a newform $g \in S_2(\Gamma_0(2))$ such that the reductions mod ℓ of the associated representation satisfies $\bar{\rho}_{g,\ell} \sim \bar{\rho}_{f,\lambda} \sim \bar{\rho}_{E,\ell}$. However, it is known that the dimension of $S_2(\Gamma_0(2))$ as $\mathbf{C}$-vector space is 0. Therefore, there can't exist such a form g and we are led to a contradiction, finally proving FLT.

As we already said, at the base of the proof of Wiles's theorem there is deformation theory, which is the subject of this thesis. It studies all the possible 'deformations' of a fixed continuous residual representation

$$\bar{\rho} \colon \Pi \longrightarrow \mathrm{GL}_N(k),$$

where Π is a profinite group, k a finite field and N a positive natural number. By *deformation* of $\bar{\rho}$ we denote a continuous representation $\rho\colon \Pi \longrightarrow \mathrm{GL}_N(A)$, where A is a *coefficient ring*, i.e. a complete local Noetherian ring with residue field k, such that the diagram

$$\begin{array}{ccc} \Pi & \overset{\rho}{\dashrightarrow} & \mathrm{GL}_N(A) \\ & \searrow^{\bar{\rho}} & \downarrow{\scriptstyle \pi} \\ & & \mathrm{GL}_N(k) \end{array}$$

commutes ($\pi\colon \mathrm{GL}_N(A) \longrightarrow \mathrm{GL}_N(k)$ being the morphism induced by the canonical projection $A \to k$). Denoting by $\mathcal{C}$ the category of coefficients rings, whose morphisms are local ring homomorphisms which induce the identity map on k, we can define the *deformation functor*

$$\begin{aligned} D_{\bar{\rho}}\colon \mathcal{C} &\longrightarrow \mathrm{Sets} \\ A &\longmapsto \{\text{deformations of } \bar{\rho} \text{ to A}\}. \end{aligned}$$

Mazur–Ramakrishna's theorem states that under certain hypothesis the deformation functor is representable, namely there exists a coefficient ring $\mathcal{R}$ such that $D_{\bar{\rho}} \simeq \mathrm{Hom}(\mathcal{R}, -)$. This is an application of Schlessinger's theorem, which establishes the conditions that a set-valued functor on $\mathcal{C}$ must satisfy to be representable. The isomorphism of functors $D_{\bar{\rho}} \simeq \mathrm{Hom}(\mathcal{R}, -)$ leads to the existence of a deformation $\rho_{\mathcal{R}}\colon \Pi \longrightarrow \mathrm{GL}_N(\mathcal{R})$, which parametrizes all the others. It means that for every coefficient ring A and every deformation $\rho\colon \Pi \longrightarrow \mathrm{GL}_N(A)$ there exists a unique morphism $f\colon \mathcal{R} \longrightarrow A$ such that $\rho = f \circ \rho_{\mathcal{R}}$. Because of this universal property, we call $\mathcal{R}$ the *universal coefficient ring* and $\rho_{\mathcal{R}}$ the *universal deformation of* $\bar{\rho}$.

In the context of Wiles's proof, we consider deformations of a residual Galois representation $\rho_0\colon G_{\mathbf{Q}} \longrightarrow \mathrm{GL}_N(k)$, which we ask to satisfy certain conditions. For every finite set of primes Σ disjoint from the finite set S of primes at which ρ_0 ramifies, we look for all those deformations that have roughly speaking the 'same' local properties of ρ_0, obtaining a subfunctor $\mathcal{D}_\Sigma \subseteq D_{\rho_0}$. Moreover, restricting to the modular deformations of type $\mathcal{D}_\Sigma$, we get another sub-functor $\mathcal{D}_{\Sigma,\mathrm{mod}} \subseteq \mathcal{D}_\Sigma \subseteq D_{\rho_0}$. Both $\mathcal{D}_{\Sigma,\mathrm{mod}}$ and $\mathcal{D}_\Sigma$ are representable. Let us denote by $\mathbb{T}_{\mathcal{D}}$, $\mathcal{R}_{\mathcal{D}}$ their respective universal coefficient rings and ρ_Σ, $\rho_{\Sigma,\mathrm{mod}}$ their respective universal deformations. A numerical criterion (see Section 4.4) establishes that the unique morphism $\phi_{\mathcal{D}}\colon \mathcal{R}_{\mathcal{D}} \longrightarrow \mathbb{T}_{\mathcal{D}}$, such that $\rho_{\Sigma,\mathrm{mod}} = \phi_{\mathcal{D}} \circ \rho_\Sigma$, is indeed an isomorphism. For the univeral property, once again, it follows that all the deformations of type $\mathcal{D}_\Sigma$ are modular. Taylor's

contribution was fundamental in the proof of this criterion.

The connection with modularity theorem follows straightforward. Indeed, if there exists a prime number ℓ such that $\bar{\rho}_{E,\ell}$ is both modular and irreducible then $\bar{\rho}_{E,\ell}$ satisfies all the conditions required for ρ_0. Moreover, the deformation $\rho_{E,\ell}$ is of type $\mathcal{D}_\Sigma$ and hence, for the paragraph above, it is modular. We can conclude, thanks to the definition of modular elliptic curve, that E is modular. It is left to prove that such ℓ always exists. However, one at least one between $\bar{\rho}_{E,3}$ and $\bar{\rho}_{E,5}$ is irreducible (see Theorem 4.3.17). In both cases, we can conclude by Laglands-Tunnel Theorem 4.3.16 and Theorem 4.3.18 respectively that they are also modular.

Wiles and Taylor accomplished one of the greatest result ever: the solution of a theorem that had been challenging mathematicians of all times and all over the world. However, Wiles didn't receive the Fields Medal. The story tells that when, in 1993 and at the age of 40 years old, he first announced the solution to the mathematical community, the U.S. Nicholas Katz found an error in Wiles's argument. Sadly, by the time Wiles's corrected the error, he had already turned 41. The Fields Medal committee decided to stick to the established age limit: 40 years old. However, few years later they granted him with a one-time special honor, a silver plaque.

Content of this thesis

The first chapter lays the foundations introducing basic definitions of algebraic number theory. We will firstly introduce the notions of absolute value over a field, its associated valuation and the completion of a field with respect to an absolute value. We will, then, move our attention to projective (or inverse) limits and profinite groups, setting the basis for the study of the properties of Galois groups, focusing on infinite Galois extensions. Indeed, we will show how Galois groups can be naturally endowed with a topology, the Krull topology which makes them into profinite groups, and how the Galois correspondence can be extended to infinite field extensions. Furthermore, we will focus on the absolute Galois group of $\mathbf{Q}$ providing a detailed study on its 'local' behaviour, which we will lead us to the definition of maximal extension of $\mathbf{Q}$ unramified outside a set of primes. We will, then, introduce the concept of Galois representations and some of their basic properties. To conclude the chapter, we will, at last, recall some properties of local fields, which we'll be very useful in the last chapter.

The second chapter aims to introduce the notion of deformation of representations of profinite groups, with a particular focus on Galois representations. We'll start by laying the necessary basis introducing the category of coefficient rings and residual representations. This will be followed by a detailed exploration of the deformation functor. Finally, we will discuss the key result of this chapter: Schlessinger's theorem, which establishes the conditions under which a set valued functor on the category of coefficient rings is representable, leading to the definition of the Universal Deformation Ring. We will need some categorical tools, such that fiber products and the functorial interpretation of the Zariski tangent space of a coefficient ring. Morever, an important role will be played by the so called Mayer-Vietoris property, which is based on the universality of fiber products. Once the deformation functor is shown to be representable, we will introduce the notion of Univesal Deformation, which intuitively can be seen as the most 'general' deformation from which all the others can be derived via ring homomorphisms. We will explore the existence of such a universal object and study its properties in detail. At the end we will state Mazur–Ramakrishna's theorem, which is an application of Schlessinger's theorem to the deformation functor. We will give a detailed proof, splitting it in different steps and stating some technical lemmas.

The third chapter shifts its focus to exploring the Universal Deformation Ring of Galois representations. Moreover, we will examine how deformation theory interacts with cohomological properties of representations of profinite groups. A significant part of this chapter will be devoted to the study of the tangent space of the deformation functor and its relations to the cohomology groups associated with Galois representations. These connections will allow us to analyze the space of deformations from a more geometric perspective, providing a deeper understanding of both local and global aspects of Galois representations. Furthermore, we will define and analyze obstructed and unobstructed deformations problems, giving a characterization in terms of the dimensions of cohomology groups. The main result will be Boston's theorem, which states that under certain conditions the universal deformation ring of a Galois residual representation is isomorphic to $\mathbf{Z}_p[[T_1, T_2, T_3]]$, i.e. a formal power series in three variables.

The fourth and final chapter is devoted to the most significant applications of deformation theory. We will start from recalling some definitions and constructions about modular forms, such that congruence subgroups and modular forms, oldforms and newforms. We will explicitly build Galois representations attached to a newform, which will be at the base of the modularity theorem. We will then introduce many

equivalent definitions of modularity. In order, we'll define a modular elliptic curve in terms of modular curves, modular forms and Galois representations. We'll state Wiles's theorem and give a sketch of its proof. In particular, we will state the numerical criterion and focus on the deformation conditions that make the subfunctor $\mathcal{D}_\Sigma$ representable for every set of primes Σ. Moreover, we will give a construction of the modular universal ring $\mathbb{T}_\mathcal{D}$. Finally, we'll sketch the proof of Fermat's Last Theorem via Frey's curves.

Chapter 1

Galois groups and their representations

In this first chapter we are going to introduce the main objects of this thesis and give some of their basic properties. We will start by introducing valuations on a field, their attached absolute values and completions of fields.

Secondly, we will deal with projective limits and profinite groups since they play a fundamental role in the definition of a topology for infinite Galois groups. Indeed, we will show how the classical Galois correspondence can be extended to arbitrary extensions endowing Galois groups with a topology, called the Krull topology.

We will then study the absolute Galois group of $\mathbf{Q}$ and its local structure, which will help us to better understand the whole group. Fixed a prime p and considered the completion of $\mathbf{Q}$ with respect to p, $\mathbf{Q}_p$, we will define the inertia subgroup $I_p \subseteq G_{\mathbf{Q}_p}$ of the absolute Galois group of $\mathbf{Q}_p$. Then, for a finite set of primes S, we will introduce the maximal extension of $\mathbf{Q}$ unramified outside S and we will denote it by $\mathbf{Q}_S$.

Finally, we will introduce Galois representations, i.e. representations of the absolute Galois group of $\mathbf{Q}$ or $\mathrm{Gal}(\mathbf{Q}_S/\mathbf{Q})$: their deformations will be the main topic of this thesis

1.1 Absolute values, complete fields and valuations

In this first section K will denote a field and we will follow the structure of [9, Chapter 7].

1.1.1 Absolute values and completion of a field

Definition 1.1.1. An *absolute value* on K is a function

$$|\cdot|\colon K \longrightarrow \mathbf{R}$$

such that:

1. $|\ x\ | = 0 \iff x = 0$;
2. $|\ x\ | \geq 0$;
3. $|\ xy\ | = |\ x\ ||\ y\ |$;
4. $|\ x + y\ | \leq |\ x\ | + |\ y\ |$.

We can define a metric on K associated with an absolute value, making therefore K into a topological space.

Definition 1.1.2. A *metric* d associated with an absolute value $|\cdot|$ is a function

$$\begin{aligned} d\colon K \times K &\longrightarrow \mathbf{R} \\ (x, y) &\longmapsto |\ x - y\ |\ . \end{aligned}$$

Definition 1.1.3. Two absolute values on K are *equivalent* if they define the same topology on K.

Absolute values can be classified into two different types.

Definition 1.1.4. An absolute value in called *non-Archimedean* if

$$|\ x + y\ | \leq \max\{|\ x\ |, |\ y\ |\} \quad \forall x, y \in K.$$

Otherwise the absolute value is called *Archimedean.*

We, now, introduce the notion of completeness of K with respect to an absolute value $|\cdot|$.

Definition 1.1.5. Let $|\cdot|$ be an absolute value on K, a sequence $\{a_n\}_{n \in \mathbf{N}}$ in K is called a *Cauchy-sequence* if for all $\epsilon > 0$, there exists $N \in \mathbf{N}^+$ such that

$$n, m \geq N \implies |\ a_n - a_m\ | < \epsilon.$$

.

Definition 1.1.6. Let $|\cdot|$ be an absolute value and let d the metric associated with it. We say that K is a *complete field* with respect to the metric d if every Cauchy sequences $\{a_n\}_{n\in\mathbf{N}}$ in K converges to an element $a \in K$, i.e. :

$$\lim_{n\to\infty} d(a_n, a) = 0.$$

The next step is to embed any field endowed with an absolute value in a complete field. The following theorem ensures that this is possible.

Theorem 1.1.7. *Let K be a field and $|\cdot|$ be an absolute value on it. Then there exists a unique, up to K-isomorphism, complete field $\hat{K}$ with an absolute value $|\cdot|_{\hat{K}}$ such that K is embedded in $\hat{K}$ as a dense subfield and the absolute value on K is a restriction of the absolute value on $\hat{K}$.*

Definition 1.1.8. The field $\hat{K}$ is called the completion of K with respect to the absolute value $|\cdot|$.

1.1.2 Valuations

Before giving the definition of a valuation we must introduce the new symbol ∞ and state that for all $a \in K$, $a < \infty$, $a + \infty = \infty$ and $\infty + \infty = \infty$. Set this conventions, we are ready to give the following definition.

Definition 1.1.9. A *valuation* on K is a function

$$v\colon K \longrightarrow \mathbf{R} \cup \{\infty\}$$

such that for all $x, y \in K$:

1. $v(x) = \infty \iff x = 0$;
2. $v(xy) = v(x) + v(y)$;
3. $v(x + y) \geq \min\{v(x), v(y)\}$.

An equivalence class of valuations on K is also called a *place* of K.

Definition 1.1.10. A valuation v on K is called *discrete* if $v(K^*) = s\mathbf{Z}$ for a real $s > 0$. Moreover v is normalized if $s = 1$.

The following theorem shows that there is a connection between non-Archimedean absolute values on K and valuations.

Theorem 1.1.11. *Let $|\cdot|$ be an non-Archimedean absolute value on K, $s \in \mathbf{R}_{>0}$, then the function*

$$v_s\colon \begin{array}{ccc} K & \longrightarrow & \mathbf{R}\cup\{\infty\} \\ x & \longmapsto & \begin{cases} -s\cdot \log|x| & x\neq 0 \\ \infty & x=0 \end{cases} \end{array}$$

is a valuation on K. Viceversa, if v is a valuation on K, $q \in \mathbf{R}$, $q>1$, then the function :

$$|\cdot|_q\colon \begin{array}{ccc} K & \longrightarrow & \mathbf{R} \\ x & \longmapsto & \begin{cases} q^{-v(x)} & x\neq 0 \\ 0 & x=0 \end{cases} \end{array}$$

is an non-Archimedean absolute value on K.

We have the following result.

Theorem 1.1.12. *Let K be a field, v a valuation on K and $|\cdot|$ the correspondent non-Archimedean absolute value defined in the theorem above. Then we have:*

1. *$\mathcal{O} := \{x\in K\colon v(x)\geq 0\} = \{x\in K\colon \ |x|\leq 1\}$ is an integral domain and a maximal proper subring[1] of K called valuation ring. Moreover, if $x\neq 0$ then either $x\in\mathcal{O}$ or $x^{-1}\in\mathcal{O}$.*
2. *The set $\mathcal{O}^* = \{x\in K\colon v(x)=0\} = \{x\in K\colon \ |x|=1\}$ is the group of units of $\mathcal{O}$.*
3. *$m_v = \mathcal{O}\setminus\mathcal{O}^* = \{x\in K\colon v(x)>0\} = \{x\in K\colon \ |x|<1\}$ is the unique maximal ideal of $\mathcal{O}$, in particular $\mathcal{O}$ is a local ring.*

Definition 1.1.13. The field $f_v = \mathcal{O}/m_v$ is called the *residue field* of $\mathcal{O}$.

We are now ready to give the following definition.

Definition 1.1.14. A *local field* is a complete field with respect to the absolute value induced by a discrete valuation and whose residue field is finite.

Remark 1.1.15. When the valuation is discrete and normalized the valuation ring is called *discrete valuation ring* denoting it by DVR. One can check that a DVR satisfies any of the following equivalent conditions [1, Chapter 9].

[1] Let R be a ring and let $S\subset R$ be a proper subring of R. Then S is *maximal* if there are no proper subrings between S and R.

- It is a local principal ideal domain and not a field;
- it is a local Dedekind domain and not a field;
- it is a Noetherian local domain whose maximal ideal is principal and not a field;
- it is an integrally closed Noetherian local ring with Krull dimension one;
- it is a principal ideal domain with only one non-zero prime ideal, whose generator is called *uniformazing parameter* or *uniformizer*.

To clarify the ideas let us consider the two following examples.

Example 1.1.16. *Let F be a number field, let $\mathcal{P}$ be a prime of F lying over the prime $p \in \mathbf{Z}$ and consider the non-Archimedean absolute value*

$$|\cdot|_{\mathcal{P}} \colon F \longrightarrow \mathbf{R}$$

$$x \longmapsto p^{-\operatorname{ord}_{\mathcal{P}}(x)},$$

where $\operatorname{ord}_{\mathcal{P}}(x)$ is the exponent of $\mathcal{P}$ in the factorization of $x\mathcal{O}_F$ in the ring of integers $\mathcal{O}_F$ of F. Note that $\operatorname{ord}_{\mathcal{P}}(x)$ can be also negative in case $x\mathcal{O}_{\mathcal{F}}$ is a fractional ideal. We call $|\cdot|_{\mathcal{P}}$ the $\mathcal{P}$-adic absolute value. Using Theorem 1.1.11, it is easy to see that the valuation, call it $v_{\mathcal{P}}$, associated with $|\cdot|_{\mathcal{P}}$ is just the function mapping $x \in F$ to $\operatorname{ord}_{\mathcal{P}}(x)$ and 0 to ∞.

We denote $F_{\mathcal{P}}$ the completion of F with respect to the $\mathcal{P}$-adic absolute value and $\mathcal{O}_{\mathcal{P}}$ the discrete valuation ring. Thanks to Theorem 1.1.7, we know that there is an embedding of F into $F_{\mathcal{P}}$. One can check that, if we denote by $m_{\mathcal{P}}$ the maximal ideal of $\mathcal{O}_{\mathcal{P}}$, then the residue field $f_{\mathcal{P}} = O_{\mathcal{P}}/m_{\mathcal{P}}$ is finite and so $F_{\mathcal{P}}$ is what is called a local field.

Example 1.1.17. *Considering the previous example for $F = \mathbf{Q}$ and $\mathcal{P} = p$ a prime number, then we get the p-adic completion of $\mathbf{Q}$, that we denote $\mathbf{Q}_p$ and call the field of p-adic numbers. Then the discrete valuation ring of $\mathbf{Q}_p$, which we denote by $\mathbf{Z}_p$, is called the ring of p-adic numbers. Note that $\mathbf{Z}_p$ is the completion of $\mathbf{Z}$ with respect to the p-adic metric. Moreover, in this case, $m_p = p\mathbf{Z}_p$ and the residue field $f_p = \mathbf{Z}_p/p\mathbf{Z}_p$ is isomorphic to $\mathbf{F}_p$, i.e. the finite field of p elements.*

Considering the examples above, one could wonder if all the non-Archimedean absolute value on a number field F are of the form $|\cdot|_{\mathcal{P}}$ for some prime $\mathcal{P}$ of K. The answer is the following theorem by Ostrowski [9, Theorem 7.12] .

Theorem 1.1.18. *Let F be a number field. Each non trivial non-Archimedean absolute value on F is equivalent to a $\mathcal{P}$-adic absolute value for a unique prime $\mathcal{P}$ of F. Moreover, every Archimedean absolute value on F is equivalent to an absolute value coming from a real or complex embedding F.*

Remark 1.1.19. Let $\sigma\colon F \hookrightarrow \mathbf{R}$ be an embedding of F as in the theorem above. Then for very $x \in F$, we define $\mid x \mid_\infty = \mid \sigma(x) \mid_{\mathbf{R}}$, where $\mid \cdot \mid_{\mathbf{R}}$ denotes the euclidean absolute value on $\mathbf{R}$. The same construction hold replacing $\mathbf{R}$ with $\mathbf{C}$.

Let us now give two last important results about valuation.

Theorem 1.1.20. *Let K be a complete field with respect to an absolute value $\mid \cdot \mid_K$ and let L/K be an algebraic extension. Then*

- *there exists a unique absolute value $\mid \cdot \mid_L$ on L whose restriction to K is $\mid \cdot \mid_K$;*
- *if $[L : K] = n < \infty$ and $x \in L$ then $\mid x \mid_L = \mid N_{L/K}(x) \mid_K^{1/n}$, where $N_{L/K}$ denotes the norm[2] of α;*
- *assume that $\mid \cdot \mid_K$ is non-archimedean with valuation ring $\mathcal{O}_K$. The valuation ring $\mathcal{O}_L$ of $\mid \cdot \mid_L$ is the integral closure of $\mathcal{O}_K$ in L.*

Theorem 1.1.21. *Let K be a complete field with respect to a discrete valuation and let L/K be a finite separable extension. Then L is complete with respect to the extension of $\mid \cdot \mid_K$ on L.*

1.2 Projective limits and profinite groups

Projective limits generalize the operation of intersection. In order to define them we need to give some auxiliary definitions following [6, Subsection 2.1.2] and [5, Complements to Lecture 1].

Definition 1.2.1. A *directed set* is a pair $(I, \leq)$ where I is a set such that $I \neq \emptyset$ and $\leq$ is a pre-order, which is a reflexive and transitive binary relation with the property that every pair of elements has an upper bound, i.e. given $i, j \in I$ there exists $k \in I$ such that $i \leq k$ and $j \leq k$.

[2] If K is a field and L is a finite extension of K, then the field L is a finite dimensional K-vector space. Then if $\alpha \in L$, the multiplication map $m_\alpha\colon L \longrightarrow L$, $x \longmapsto \alpha \cdot x$, is a K-linear transformation. The norm $N_{L/K}(\alpha)$ is defined as the determinant of this linear transformation.

Definition 1.2.2. A *projective (or inverse) system* of sets over $(I, \leq)$ is a family $\{X_i, f_{i,j} \colon i, j \in I, i \leq j\}$, where the X_i are sets and $f_{i,j} \colon X_j \longrightarrow X_i$ are maps such that

1. $f_{i,i} = id_{X_i}$;
2. $f_{i,k} = f_{i,j} \circ f_{j,k}$.

Definition 1.2.3. Let $\{X_i, f_{i,j}\}$ be a projective system over $(I, \leq)$, the *projective (or inverse) limit* of $\{X_i, f_{i,j}\}$ is :

$$\varprojlim_{i \in I} X_i \coloneqq \{(x_i)_{i \in I} : f_{i,j}(x_j) = x_i \quad \forall i \leq j\}.$$

Remark 1.2.4. If the sets X_i have some structure (e.g. if they are groups, rings, modules, topological spaces, ...) we ask the transition maps $f_{i,j}$ to respect this structure. In this case the inverse limit $\varprojlim_{i \in I} X_i$ inherits that structure.
Consider, for example, a projective system of topological spaces, $\{X_i, f_{i,j}\}$, we can define on $\varprojlim_{i \in I} X_i$ the subspace topology induced by the product topology on $\prod_{i \in I} X_i$. If, instead, $\{G_i, f_{i,j}\}$ is a projective system of groups then $\varprojlim_{i \in I} G_i$ has a group structure with the component wise multiplication.

The following result holds.

Proposition 1.2.5. *Let $\{X_i, f_{i,j}\}$ be a projective system of not empty, Hausdorff and compact topological spaces on $(I, \leq)$, then $X = \varprojlim_{i \in I} X_i$ is not empty, Hausdorff and compact.*

Indeed, in most of the cases we will be working with finite groups G_i equipped with the discrete topology which makes them Haussdorf and compact spaces. So, thanks to the proposition above $\varprojlim_{i \in I} G_i$ is Haussdorf and compact.

We are now ready to give the definition of profinite group.

Definition 1.2.6. A *profinite group* is a Hausdorff, compact and totally disconnected topological group.

Remark 1.2.7. It is not difficult to check that in a profinite group, a subgroup is open if and only if it is closed and of finite index.

The following proposition gives a correspondence between profinite groups and inverse limits.

Proposition 1.2.8. *Let G be a profinite group. There is an isomorphism (which is also an homeomorphism)*

$$G \simeq \varprojlim_N G/N,$$

where N runs through all open normal subgroups of G. Viceversa, let $\{G_i, f_{i,j}\}$ a projective system of finite groups, then $G := \varprojlim_i G_i$ is a profinite group.

It follows from this proposition that one can give an alternative definition of profinite group.

Definition 1.2.9. A profinite group is a topological group that is isomorphic to the inverse limit of an inverse system of discrete finite groups.

The following theorem gives a further characterization of profinite groups.

Theorem 1.2.10. *Let G be a Hausdorff and compact topological group. The following conditions are equivalent.*

1. *G is profinite;*
2. *G has a set of open normal subgroups which is a full system of neighborhood of the identity.*

We can now give the following important example.

Example 1.2.11. *In the previous section we introduced the definition of p-adic integers, seen as the completion of $\mathbf{Z}$ with respect to the p-adic metric, i.e. $\mathbf{Z}_p = \{x \in \mathbf{Q}_p :| x |_p \leq 1\}$. It is easy to prove that*

1. *in $\mathbf{Q}_p$ any open ball is also closed and viceversa. A quite immediate consequence is that $\mathbf{Q}_p$ with the p-adic metric is totally disconnected. This makes $\mathbf{Z}_p$ a totally disconnected space as well since it is a subspace of $\mathbf{Q}_p$;*
2. *$\mathbf{Z}_p$ is compact: this is a generalization of Heine-Borel theorem for metric spaces, which states that a subspace of a metric space is compact if and only if it is closed and totally bounded;*
3. *$\mathbf{Q}_p$ is Hausdorff since it is a metric space. Hence, $\mathbf{Z}_p$ is Haussdorf because it is a subspace of $\mathbf{Q}_p$.*

Finally, these properties show that $\mathbf{Z}_p$ *is a profinite ring and by Proposition 1.2.8 we have*

$$\mathbf{Z}_p \simeq \varprojlim_n \mathbf{Z}_p/(p^n\mathbf{Z}_p) \simeq \varprojlim_n \mathbf{Z}/p^n\mathbf{Z}$$

since, as n *varies in* $\mathbf{N}$, $p^n\mathbf{Z}_p = \{x \in \mathbf{Q}_p\colon \mid x \mid_p < n+1\}$ *are all the open normal subgroups of* $\mathbf{Z}_p$.

To complete the basic definitions attached to profinite groups we can give the following ones.

Definition 1.2.12. Let G be a profinite group. The order of G is a supernatural number[3] defined in the following equivalent ways :

- it is the lcm (in the supernatural number sense) of the orders of all finite groups in some choice of inverse system of finite discrete groups whose inverse limit is G;
- it is the lcm of the orders of all finite groups arising as quotients of G by some open normal subgroup of it.

Definition 1.2.13. Let G be a profinite group and let H be a closed subgroup of G. Then the index of H in G can be defined in the following equivalent ways:

- it is the lcm (lowest common multiple) of the indexes $[G/U : HU/U]$ where U varies over the open normal subgroups of G;
- it is the lcm of the indexes $[G : V]$ where V ranges over the open normal subgroups of G containing H.

Definition 1.2.14. Let G be a profinite group and p a prime number. A p-Sylow subgroup of G is a closed subgroup H of G such that the order (in the sense of profinite groups) is a power of p and its index (in the sense of profinite group) is relatively prime to p.

[3] A supernatural number is defined as a formal product $\prod_p p^{n_p}$, where p runs over all the prime numbers and each n_p is either 0, a natural number or ∞. Then, if m and n are the supernatural numbers $\mathrm{lcm}(m,n) = \prod_p p^{\max\{m_p,n_p\}}$. If either m_p or n_p is ∞ then the max between them is ∞.

1.3 Infinite Galois extensions

For references see [5, Chapter 1] and [4, Chapter 9].

Definition 1.3.1. Let L/K be a field extension. We say that L/K is a *Galois extension* if it is normal and separable.

Let K be a field and $\bar{K}$ a fixed algebraic closure of K. If we assume that $\bar{K}/K$ is separable, then it is a Galois extension, called *absolute Galois extension of* K and denoting its Galois group by

$$G_K = \{\sigma\colon \bar{K} \to \bar{K} : \sigma \text{ is an automorphism and } \sigma(x) = x \quad \forall x \in K\}.$$

Since this group is usually infinite, the Galois correspondence for finite extensions which matches subgroups of the Galois group with subextensions doesn't work and must be generalized to infinite extensions. A solution for this problem is to introduce a topology on infinite Galois groups and then formulate the Galois correspondence in terms of closed subgroups.

1.3.1 Krull topology

Let L/K be a Galois extension, not necessarily finite. For very $\sigma \in \mathrm{Gal}(L/K)$ let us define the following fundamental system of neighborhoods of σ

$$\{U_\sigma(K') = \sigma\,\mathrm{Gal}(L/K') : K \subseteq K' \subseteq L \text{ and } K'/K \text{ finite and Galois}\}.$$

The set of neighborhoods of σ is then

$$N_{\mathrm{Gal}(L/K)}(\sigma) = \{H \subset \mathrm{Gal}(L/K) : H \supset U_\sigma(K') \text{ for some } K'\}.$$

In this way we put a topology on $\mathrm{Gal}(L/K)$ called the *Krull topology*. It is clear that this topology reduces to the discrete one when the field extension L/K is finite. Equipped with the Krull topology $\mathrm{Gal}(L/K)$ becomes a topological group since the group operations

$$\begin{aligned} \circ\colon \mathrm{Gal}(L/K) \times \mathrm{Gal}(L/K) &\longrightarrow \mathrm{Gal}(L/K) \\ (\sigma, \tau) &\longmapsto \sigma \circ \tau \end{aligned}$$

$$\begin{aligned} \mathrm{Gal}(L/K) &\longrightarrow \mathrm{Gal}(L/K) \\ \sigma &\longmapsto \sigma^{-1} \end{aligned}$$

are continuous.

The Krull topology makes $\mathrm{Gal}(L/K)$ into a compact, totally disconnected, Hausdorff space, i.e. a profinite group. It can be shown that $\mathrm{Gal}(L/K)$ is the inverse limit of the projective system of the quotients of $\mathrm{Gal}(L/K)$ by its normal open subgroups, i.e.

$$\{\mathrm{Gal}(K'/K) : K \subseteq K' \subseteq L, K'/K \text{ is finite and Galois}\},$$

where, whenever we have two finite subextensions $K' \subseteq K''$ of L/K, we consider the homomorphism

$$\mathrm{Gal}(K''/K) \longrightarrow \mathrm{Gal}(K'/K)$$

given by the restriction.
Hence

$$\mathrm{Gal}(L/K) = \varprojlim_{K'/K} \mathrm{Gal}(K'/K).$$

Therefore $\mathrm{Gal}(L/K)$ inherits the profinite topology, which can be proved to agree with the Krull topology introduced above.

The introduction of a topology on $\mathrm{Gal}(L/K)$ let us extend the Galois correspondence for arbitrary field extensions.

Theorem 1.3.2. *Let L/K be a Galois extension (finite or infinite), then the map*

$$K' \longmapsto \mathrm{Gal}(L/K')$$

defines a bijective inclusion-reversing correspondence between subextensions K'/K and closed subgroups of $\mathrm{Gal}(L/K)$*. The inverse correspondence is given by*

$$H \longmapsto L^H,$$

where L^H denotes the subfield of L consisting of those elements which are fixed by every element of H. In particular, the open subgroups, i.e. the closed subgroups of finite index, correspond to the finite subextensions. Moreover, H is a normal subgroup of $\mathrm{Gal}(L/K)$ *if and only if the extension L^H/K is Galois.*

1.4 The absolute Galois group of Q

1.4.1 Local structure of $G_{\mathbf{Q}}$

In this section we will analyze the absolute Galois group of the rational numbers studying its "local structure", i.e. considering the p-adic completion $\mathbf{Q}_p$ of $\mathbf{Q}$ for each prime number p and studying the relations between $\mathbf{Q}$ and $\mathbf{Q}_p$.

Indeed, for each prime number p there is a canonical inclusion of $\mathbf{Q}$ into $\mathbf{Q}_p$, but there are many ways to include $\bar{\mathbf{Q}}$ into $\bar{\mathbf{Q}}_p$. Let us call $i\colon \bar{\mathbf{Q}} \hookrightarrow \bar{\mathbf{Q}}_p$ a fixed inclusion map. Depending on the choice of the inclusion map, we get an embedding of $G_{\mathbf{Q}_p}$ into $G_{\mathbf{Q}}$, defined my the map

$$\begin{aligned} \Theta_p\colon G_{\mathbf{Q}_p} &\longrightarrow G_{\mathbf{Q}} \\ \sigma &\longmapsto \sigma \circ i. \end{aligned}$$

Indeed, since $\bar{\mathbf{Q}}$ is dense in $\bar{\mathbf{Q}}_p$, Θ_p is injective and we can then see $G_{\mathbf{Q}_p}$ as contained in $G_{\mathbf{Q}}$ by the identification

$$G_{\mathbf{Q}_p} \simeq \Theta_p(G_{\mathbf{Q}_p}) \subseteq G_{\mathbf{Q}}.$$

The image of $G_{\mathbf{Q}_p}$ through Θ_p is called a *decomposition group at p*. Identifying $G_{\mathbf{Q}_p}$ with its image in $G_{\mathbf{Q}}$ we have to keep in mind that its image is determined up to conjugation by the inclusion of $\bar{\mathbf{Q}}$ into $\bar{\mathbf{Q}}_p$ that we chose.

We'll mainly study the unramified field extensions of $\mathbf{Q}_p$, recalling firstly the following definition and theorem.

Definition 1.4.1. An extension L/K of local fields is said to be *unramified* if $[L : K] = [l : k]$, with $l = \mathcal{O}_L/\pi_L$ and $k = \mathcal{O}_K/\pi_K$, where $\mathcal{O}_L$ and $\mathcal{O}_K$ are the valuation rings of L and K respectively and π_L, π_K are uniformizers of L and K. That is equivalent to say that π_K is inert in L, i.e. it doesn't ramify in L (the ramification index $e = v_L(\pi_K) = 1$, which means that π_K is also a uniformizing element of L).

Theorem 1.4.2. *Fix a local field K with perfect residue field k. Then there is an equivalence of categories between the extensions of k and the unramified extensions of K.*

Therefore, if we consider the finite unramified extensions of $\mathbf{Q}_p$, these are in 1-1 correspondence with finite extensions of $\mathbf{F}_p$ thanks to the theorem above. However, $\mathbf{F}_p$ has a unique extension of degree n for every $n \in \mathbf{N}$, namely the splitting field of $x^{p^n} - x$. It follows that $\mathbf{Q}_p$ has a unique unramified extension of degree n for

each n, obtained as the splitting field of $x^{p^n} - x$, i.e. by adjoining the $(p^n - 1)$-st roots of unity contained in $\bar{\mathbf{Q}}_p$. Moreover, the maximal unramified extension $\mathbf{Q}_p^{ur}$ of $\mathbf{Q}_p$ corresponds to the algebraic closure of $\mathbf{F}_p$, and so is obtained by adjoining the p^{n-1}-th roots of unity for all n.

It follows that there is an isomorphsism

$$\mathrm{Gal}(\mathbf{Q}_p^{ur}/\mathbf{Q}_p) \simeq G_{\mathbf{F}_p}.$$

Thanks to this isomorphism we can consider the projection map

$$G_{\mathbf{Q}_p} \longrightarrow G_{\mathbf{Q}_p}/\,\mathrm{Gal}(\bar{\mathbf{Q}}_p/\mathbf{Q}_p^{ur}) \simeq \mathrm{Gal}(\mathbf{Q}_p^{ur}/\mathbf{Q}_p) \simeq G_{\mathbf{F}_p},$$

which clearly gives a surjective homomorphism. The kernel of this map is called the *inertia group at* p and we denote it by I_p. Then, if we consider an arbitrary extension K of $\mathbf{Q}_p$, we have the correspondent surjective homomorphism $G_{\mathbf{Q}_p} \longrightarrow \mathrm{Gal}(K/\mathbf{Q}_p)$ and the extension is called *unramified* if the image of I_p under this map is trivial, i.e. K in contained in $\mathbf{Q}_p^{ur}$.

Moreover, considering the following chain of inclusions of groups, defined up to conjugation,

$$I_p \subseteq G_{\mathbf{Q}_p} \subseteq G_{\mathbf{Q}},$$

we say that a Galois extension $K/\mathbf{Q}$ is *unramified at* p when the image of the intertia subgrouos I_p through the surjective homomorphism $G_{\mathbf{Q}} \longrightarrow \mathrm{Gal}(K/\mathbf{Q})$ is trivial.

The following theorem describes how ramification works for number fields.

Theorem 1.4.3. *If $K/\mathbf{Q}$ is a finite extension, then K is ramified at finitely many primes. Every non trivial extension of $\mathbf{Q}$ is ramified at at least one prime.*

1.4.2 Extensions of Q unramified outside a finite set of primes

Let S be a finite set of primes including the prime at infinity and let us consider all the algebraic extensions of $\mathbf{Q}$ unramified outside S. If we compose all these extensions together we obtain the maximal extension of $\mathbf{Q}$ unramified outside S, that we denote by $\mathbf{Q}_S$ and whose Galois group $G_{\mathbf{Q},S} = \mathrm{Gal}(\mathbf{Q}_S/\mathbf{Q})$ is a quotient of $G_{\mathbf{Q}}$ by a closed subgroup. Since the property of being profinite is preserved under taking quotients by closed subgroups, $G_{\mathbf{Q},S}$ has a profinite structure. The same exact definition can be given for a number field K and a finite set of primes of K including

all the archimedean ones, obtaining the Galois group $G_{K,S}$, which is again a profinite group.

An important result for the Galois group $G_{K,S}$ is the Hermite-Minkowski theorem.

Theorem 1.4.4 (Hermite-Minkowski)**.** *Let K be a finite extension of $\mathbf{Q}$, let S be a finite set of primes and let d be a positive integer. Then there are only finitely many extensions F/K of degree d which are unramified outside S.*

A natural consequence of this theorem is that if we consider any open subgroup H of $G_{K,S}$ of finite index, the set $\mathrm{Hom}_{\mathrm{cont}}(H, \mathbf{F}_p)$ is finite. Indeed, every such H corresponds to some finite extension K'/K unramified outside S and so the index-p open subgroups of H correspond to certain degree-p extension of K' unramified away from the places of K' above S (note that for every $f \in \mathrm{Hom}_{\mathrm{cont}}(H, \mathbf{F}_p)$ such that $f \neq 0$ we have $H/\ker(f) \simeq \mathbf{F}_p$ and then $\ker(f)$ must be a index-p open subgroup of H). We can then conclude thanks to Hermite-Minkowski theorem, which tells us that there are only finitely many extensions of K' of degree p unramified outside S. This properties is called the *p-finiteness condition* and can be formulated in the following way.

Definition 1.4.5. Fix a prime number p, a profinite group Π is said to satisfy the *finiteness condition* Φ_p if for very open subgroup $\Pi_0 \subseteq \Pi$ of finite order, the following equivalent conditions hold.

1. There are only finitely many continuous homomorphisms from Π_0 to $\mathbf{F}_p$;
2. the pro-p completion of Π_0 is topologically finitely generated[4];
3. the abelianized pro-p completion of Π_0, given its natural $\mathbf{Z}_p$ module structure, is of finite type over $\mathbf{Z}_p$;

where the pro-p completion of Π_0 is :

$$\Pi_0^{(p)} = \varprojlim_N (\Pi_0/N).$$

where N runs over all normal closed subgroups whose index is a power of p.

We can then transfer the local structure of $G_{\mathbf{Q}}$ to $G_{\mathbf{Q},S}$, getting for each prime p a homomorphism $\phi_p \colon G_{\mathbf{Q}_p} \longrightarrow G_{\mathbf{Q},S}$ which is just the composition of the map $\Theta_p \colon G_{\mathbf{Q}_p} \longrightarrow G_{\mathbf{Q}}$ of the previous section with the projection map from $G_{\mathbf{Q}}$ to $G_{\mathbf{Q},S}$.

[4]If G is a topological group and S is a subset of G, we say that S *topologically generates* G if the closure of the subgroup generated by S coincides with G.

It follows directly from the definition of $G_{\mathbf{Q},S}$ that when the prime $p \notin S$ then the image of the inertia subgroup at I_p is trivial, and so the map ϕ_p can factor through $G_{\mathbf{Q}_p}/I_p$. There is a very difficult conjecture to prove, which says that

- if $p \notin S$ then the kernel of ϕ_p is exactly I_p;
- if $p \in S$ then ϕ_p is an inclusion.

The main reason why we want to carry the local structure over $G_{\mathbf{Q},S}$ is that very little is known about the topological structure of $G_{\mathbf{Q},S}$. In particular, we don't know anything about the topological finite generation of $G_{\mathbf{Q},S}$. We know, instead, that for each prime p the Galois group $G_{\bar{\mathbf{F}}_p}$ is topologically finitely generated the Frobenius automorphism

$$\varphi_p \colon \bar{\mathbf{F}}_p \longrightarrow \bar{\mathbf{F}}_p$$

$$x \longmapsto x^p$$

and that there is an isomorphism

$$G_{\mathbf{Q}_p}/I_p \simeq G_{\bar{\mathbf{F}}_p}.$$

We then call any lift of φ_p to $G_{\mathbf{Q}_p}$ a Frobenius automorphism, which is determined up to its class in $G_{\mathbf{Q}_p}/I_p$, i.e. up to conjugacy of an element in I_p.
Moreover, when $p \notin S$, the image of the inertia group I_p is trivial and so there is a well defined Frobenius element in $G_{\mathbf{Q},S}$, which generates the image of ϕ_p.

All this theory can be formulated exactly in the same way considering a number field K instead of $\mathbf{Q}$, a set of places S of K and considering the completion K_v of K, where v is a valuation on K. Then, as above, there is a continuous homomorphism

$$\phi_v \colon G_{K_v} \longrightarrow G_{K,S}.$$

Then, if $v \notin S$, ϕ_v factors through the quotient G_{K_v}/I_v. Moreover, if we call k_v the residue field of the valuation ring of K_v and $\bar{k}_v$ the residue field of the valuation ring of $\bar{K}_v$, then there is an isomorphism

$$G_{K_v}/I_v \simeq G_{k_v} = \mathrm{Gal}(\bar{k}_v/k_v).$$

As well as $G_{\mathbf{F}_p}$, G_{k_v} is topologically generated by the Forbenius automorphism

$$\phi_v \colon \bar{k}_v \longrightarrow \bar{k}_v$$

$$x \longmapsto x^{|k_v|}.$$

As above we can conclude that if $v \notin S$ then there is a well defined Frobenius element in $G_{K,S}$, which generates the image of ϕ_v.

1.5 Galois representations

1.5.1 Why studying Galois representaions?

Galois representations are a very important tool in algebraic number theory. We'll mostly need them for the study of elliptic curves and modular forms, showing first of all,in Subsection 4.1.3, how Galois representations attached to these objects are built. Moreover, in the last chapter, we'll use these representations to define the concept of modular elliptic curve. Roughly speaking, we'll say that an elliptic curve E defined over $\mathbf{Q}$ is modular if there exists a newform $f \in S_2(\Gamma_1(N), \chi)$ f weight 2 such that the representations attached to E and f agree. We'll state, then the modularity theorem 4.2.1, which asserts that every elliptic over $\mathbf{Q}$ is modular. Once given a sketch of the proof and proceeding by contradiction, we'll arrive at a solution of Fermat's Last Theorem. An important role will be played by Ribet's theorem 4.7.5, which, once again, relies on Galois representation.

The strength of representation theory is clear. Between 1993 and 1994, Andrew Wiles, using Galois representations, managed to solve one of the most difficult problem ever: Fermat's Last Theorem. Helped by the intuitions of many mathematicians, like Frey, Ribet and Taylor, Wiles's work marked the end of an era for algebraic number theory and showed to the mathematical community the great connection between arithmetic problems and Representation Theory.

1.5.2 Formal definitions

Consistently with Group representation theory, we can give the following definition of a *Galois representation*, following the work of [6, Chpater 2].

Definition 1.5.1. Let L/K be a Galois extension of fields. A *Galois representation* attached to L/K is a representation of the Galois group $\mathrm{Gal}(L/K)$, i.e. a vector space V over a field F and a group homomorphism

$$\rho\colon \mathrm{Gal}(L/K) \longrightarrow \mathrm{Aut}(V),$$

where $\mathrm{Aut}(V)$ is the group of automorphisms of V. Moreover if V is a topological space we say that the Galois representation is *continuous* if ρ is continuous, endowing $\mathrm{Gal}(L/K)$ with the Krull topology.

Definition 1.5.2. Let V be a vector space over a field F and ρ its associated Galis representation as in the definition above. Then

- if $F = \mathbf{C}$, ρ is called *Artin representation*;
- if F is a finite extension of $\mathbf{Q}_p$ for some p, then ρ is called *p-adic Gaòois representation.*

Remark 1.5.3. Let $n \in \mathbf{N}_{>0}$ and consider an n-dimensional vector space V over a field K. Then we can fix a base of the space such that $\mathrm{Aut}(V) \simeq \mathrm{GL}_n(K)$, where $\mathrm{GL}_n(K)$ is the group of the n-dimensional invertible matrices with entries in K.

The most natural choice would be to let V be either an algebraic extension of the finite field $\mathbf{F}_p$ or the field of complex numbers $\mathbf{C}$. However, these representations are not really interesting since their image is finite. More precisely, in both cases the continuity of ρ forces the map to factor through a finite subextensions $F \subseteq L$ of K. For this reason, later on we will often set $F = \mathbf{Q}_p$ or finite extensions of it. This choice allows the image of ρ not to be finite thanks to the profinite topology carried by $\mathbf{Q}_p$.

Definition 1.5.4. Let n be a positive inter and l a prime number. A n dimensional l-adic Galois representation is a continuous homomorphism

$$\rho\colon G_{\mathbf{Q},S} \longrightarrow \mathrm{GL}_n(L),$$

where L is a finite extension of the l-adic completion of $\mathbf{Q}_l$.

Example 1.5.5. *An important example of Galois representation is the* mod N*-Dirichlet character, a group homomorphism* $\chi_N\colon \mathrm{Gal}(\mathbf{Q}(\zeta_N)) \longrightarrow \mathbf{C}^* \simeq \mathrm{Aut}(\mathbf{C})$*, where* ζ_N *is a primitive* N*-th root of unity. Since* $\mathrm{Gal}(\mathbf{Q}(\zeta_N)) \simeq (\mathbf{Z}/N\mathbf{Z})^*$*, then* χ_N *can be seen as an homomorphism of groups from* $(\mathbf{Z}/N\mathbf{Z})^*$ *to* $\mathbf{C}^*$*. It can be extended to all* $\mathbf{Z}$ *defining* $\chi(n) = 0$ *for every* $n \in \mathbf{Z}$ *such that* $\gcd(n, N) > 1$ *and naturally* $\chi(n) = \chi_N(n)$ *for all* $n \in \mathbf{Z}$ *such that* $\gcd(n, N) = 1$*.*

Example 1.5.6. *Another important example of Galois representation is the p-adic cyclotomic character, where p is a fixed prime number. The roots of unity* $\mu_{p^n} = \{\zeta \in \bar{\mathbf{Q}}^* : \zeta^{p^n} = 1\}$ *form a cyclic group of order* p^n*, generated by any choice of a primitive* p^n*-th root of unity. Since all the primitive roots in* μ_{p^n} *are Galois-conjugate, the Galois group* $G_{\mathbf{Q}}$ *acts on* μ_{p^n} *by automorphisms. After fixing a primitive root of unity* ζ_{p^n}*, any other primitive element of* μ_{p^n} *can be written as a power of* ζ_{p^n}*, where the exponent is a unique element in* $(\mathbf{Z}/p^n\mathbf{Z})^*$*. We can then express the action of* $G_{\mathbf{Q}}$ *on* μ_{p^n} *in the following way*

$$\sigma \cdot \zeta_{p^n} \coloneqq \sigma(\zeta_{p^n}) = \zeta_{p^n}^{a(\sigma,n)}$$

where $a(\sigma, n) \in (\mathbf{Z}/p^n\mathbf{Z})^*$ is the unique element as above, depending on p and σ. This defines a group homomorphism called the p^n-th cyclotomic character:

$$\chi_{p^n} : G_{\mathbf{Q}} \longrightarrow (\mathbf{Z}/p^n\mathbf{Z})^*$$
$$\sigma \longmapsto a(\sigma, n),$$

Fixing σ and varying $n \in \mathbf{N}$, the $a(\sigma, n)$ form a compatible system in the sense that they give an element of the inverse limit $\varprojlim_n (\mathbf{Z}/p^n\mathbf{Z})^* \simeq \mathbf{Z}_p^*$. Thus the χ_{p^n} assemble to a continuous group homomorphism called the p-adic cyclotomic character:

$$\chi_p : G_{\mathbf{Q}} \longrightarrow \mathbf{Z}_p^*$$
$$\sigma \longmapsto (a(\sigma, n))_n.$$

Motivated by the definition of the cyclotomic character $\xi_p : G_{\mathbf{Q}} \longrightarrow \mathbf{Z}_p$, we can modify a bit the definition of Galois representation.

Definition 1.5.7. Let S be a finite set of primes and A some tpological ring. A Galois representation of rank $n \in \mathbf{N}_{>0}$, defined over A and unramified outside S, is a continuous group homomorphism

$$\rho : G_{\mathbf{Q},S} \longrightarrow \mathrm{GL}_n(A),$$

where we endow $G_{\mathbf{Q},S}$ with the profinite topology and $\mathrm{GL}_n(A)$ with the subspace topology of A^{d^2}.

Moreover, we say that two Galois representations ρ_1 and ρ_2 are equivalent if there exists a matrix $P \in \mathrm{GL}_n(A)$ such that $P^{-1}\rho_1 P = \rho_2$.

In order to study Galois representations, we need firstly to understand their local behaviour, i.e. their restrictions to the groups $G_{\mathbf{Q}_p}$ for every prime p.

Remark 1.5.8. By restriction of a Galois representation $\rho : G_{\mathbf{Q},S} \longrightarrow \mathrm{GL}_n(A)$ to the group $G_{\mathbf{Q}_p}$ we informally mean the pre-composition of ρ with $\phi_p : G_{\mathbf{Q}_p} \longrightarrow G_{\mathbf{Q},S}$ defined in Subsection 1.4.2.

In particular, if $p \notin S$, we saw that $\phi_p(I_p) = \mathrm{id}_{\mathbf{Q}_S}$ and then the lift of the Frobenius element φ_p (which is unique up to conjugation by I_p) is well defined in $G_{K,S}$. Therefore, the image of restriction of ρ to $G_{\mathbf{Q}_p}$ is given by the image of the Frobenius element φ_p. Furthermore, we can observe that, set a prime p, if $I_p \subseteq \ker(\rho)$ (meaning that $\phi_p(I_p) \subseteq \ker(\rho)$) then the image of the Frobenius element $\rho(\varphi_p)$ is well defined. This motivates the follwing definition.

Definition 1.5.9. Let $\rho\colon G_{\mathbf{Q},S} \longrightarrow \mathrm{GL}_n(A)$ be a Galois representation and p a prime number. Then ρ is said to be *unramified* at p if $I_p \subseteq \ker(\rho)$.

Remark 1.5.10. We can extend the definition of Galois representation to the whole absolute Galois group $G_{\mathbf{Q}}$, saying again that a Galois representation $\rho\colon G_{\mathbf{Q}} \longrightarrow \mathrm{GL}_n(A)$ is unramified at a prime p if $I_p \subseteq \ker(\rho)$, where now I_p is properly a subgroup of $G_{\mathbf{Q}}$ thanks to the inclusion map Θ_p defined in Subsection 1.4.1.

Remark 1.5.11. It is worth noting that we can give a more general definition of unramified Galois representation. Let L/K be an extension of number field and denote by $\mathcal{O}_L$ and $\mathcal{O}_K$ the ring of integers of L and K respectively. Then for every $\mathfrak{P}$ prime of L, which lies over a prime $\mathcal{P}$ of K, the decomposition group of $\mathfrak{P}$ is $D_{\mathfrak{P}} = \{\sigma \in \mathrm{Gal}(L/K) : \sigma(\mathfrak{P}) = \mathfrak{P}\}$. Then the well defined reduction map $D_{\mathfrak{P}} \longrightarrow \mathrm{Gal}((\mathcal{O}_L/\mathfrak{P})/(\mathcal{O}_K/\mathcal{P}))$ is surjective. The kernel of this map is the inertia group, which we denote by $I_{\mathfrak{P}}$. Recalling that $\mathcal{O}_K/\mathcal{P} \simeq \mathbf{F}_q$ for some q prime, then $D_{\mathfrak{P}}/I_{\mathfrak{P}} \simeq \mathrm{Gal}((\mathcal{O}_L/\mathfrak{P})/(\mathcal{O}_K/\mathcal{P})) \simeq \mathrm{Gal}(\mathbf{F}_{q^n}/\mathbf{F}_q)$ for some $n \in \mathbf{N}$. Finally, we say that a Galois representation $\rho\colon \mathrm{Gal}(L/K) \longrightarrow \mathrm{GL}_n(A)$ is unramified at the prime $\mathcal{P}$ of K if $I_{\mathfrak{P}} \subseteq \ker(\rho)$ for all primes $\mathfrak{P}$ above $\mathcal{P}$.

Now if, instead of extensions of number fields we consider Galois extensions of local fields, since $\mathcal{O}_L$ and $\mathcal{O}_K$ are local Dedekind domains, they both have just one prime ideal which is also maximal, call them m_L and m_K respectively. Then D_{m_L} coincides with $\mathrm{Gal}(L/K)$ because $\sigma(m_L) = m_L$ for every $\sigma \in \mathrm{Gal}(L/K)$.

Finally we can repeat the construction above for $G_{\mathbf{Q}}$ defining in the same way the decomposition group $D_{\mathfrak{P}}$ for every prime $\mathfrak{P}$ of $\bar{\mathbf{Z}}$ over $p \in \mathbf{Z}$. We get then that $D_{\mathfrak{P}}/I_{\mathfrak{P}} \simeq G_{\mathbf{F}_p}$ and we define (up to $I_{\mathfrak{P}}$) $\mathrm{Frob}_{\mathfrak{P}}$ as the element in $D_{\mathfrak{P}}$ whose class in $D_{\mathfrak{P}}/I_{\mathfrak{P}}$ is the one of the Frobenius automophormism of $G_{\mathbf{F}_p}$.

Remark 1.5.12. We can give an alternative and equivalent definition of Galois representation. If we consider the free A-module A^n for $n \in \mathbf{N}^*$, we can define a continuous action of $G_{\mathbf{Q},S}$ (or respectively of $G_{\mathbf{Q}}$) on A^n, in the following way

$$\begin{aligned} G_{\mathbf{Q},S} \times A^n &\longrightarrow A^n \\ (\sigma, m) &\longmapsto \rho(\sigma)(m), \end{aligned}$$

where $\rho\colon G_{\mathbf{Q},S} \longrightarrow \mathrm{GL}_n(A)$ is a representation.

Viceversa, if we are given a finite free A-module M of rank n with a continuous action of $G_{\mathbf{Q},S}$ we can give a representation by choosing a basis for M.

We can now go a little further. Given a topological group G, a profinite ring A and a finite free A-module M, together with a continuous action of G on M, there

is a topological isomorphism

$$M \simeq \varprojlim_H M^H,$$

where $H \subseteq G$ is a open normal subgroup and M^H are the elements of M which are fixed by every element of H. Moreover, since $G_{\mathbf{Q},S}$ is a profinite group, a subgroup H of $G_{\mathbf{Q},S}$ is open if and only if it's closed and of finite index. So if we consider the finite quotient $G' \coloneqq G_{\mathbf{Q},S}/H$ we can define the group ring

$$A[G'] = \Big\{ \sum_{g \in G'} a_g g : a_g \in A \quad \forall g \in G' \Big\}$$

endowed with the following operations:

- addition: $\sum_{g \in G'} a_g g + \sum_{h \in G'} b_h h = \sum_{k \in G'} (a_k + b_k) k$;
- multiplication: $(\sum_{g \in G'} a_g g)(\sum_{h \in G'} b_h h) = \sum_{k \in G'} c_k k$, where $c_k = \sum_{gh=k} a_g b_h$.

and where the identity element with respect to the multiplication is $1_A 1_{G'}$ and the set of invertible elements is $\Big\{ \sum_{g \in G'} 1_A g \Big\}$. We define the completed group ring

$$A[[G_{\mathbf{Q},S}]] = \varprojlim_H A[G_{\mathbf{Q},S}/H].$$

Thanks to the fact that $M \simeq \varprojlim_H M^H$, M naturally acquires a structure of $A[[G_{\mathbf{Q},S}]]$-module.

Therefore, given a Galois representation

$$\rho \colon G_{\mathbf{Q},S} \longrightarrow \mathrm{GL}_n(A),$$

one can extend it to $A[[G_{\mathbf{Q},S}]]$ getting a continuous homomorphism of A-algebras

$$\rho_A \colon A[[G_{\mathbf{Q},S}]] \longrightarrow \mathrm{M}_n(A).$$

Viceversa, since $G_{\mathbf{Q},S}$ is isomorphic to the set of invertible elements of $A[[G_{\mathbf{Q},S}]]$, the restriction to $G_{\mathbf{Q},S}$ of any such homomorphism of A-algebras gives a Galois representation.

1.5.3 Some properties of local fields

In this last part of this introductory chapter we will study a little more local fields and their properties.

First of all, we could wonder if, given a prime ℓ, the finite extensions of the l-adic field $\mathbf{Q}_l$ are complete fields too. In order to answer this question we need some preliminary results.

Lemma 1.5.13 (Kranser's lemma)**.** *Let K be a field of caharacteristic 0 complete with respect to a non-trivial non-Archimedean absolute value corresponding to a valuation v. Assume $\alpha, \beta \in \bar{K}$ are such that for all non-identity embeddings $\sigma \in \mathrm{Hom}_K(K(\alpha), \bar{K})$ we have that $v(\alpha - \beta) < v(\sigma(\alpha) - \alpha)$. Then $K(\alpha) \subset K(\beta)$.*

The first application of Kranser's lemma is the following proposition.

Proposition 1.5.14. *With K as above, let $P(x) \in K[x]$ be a monic irreducible polynomial of degree $n \in \mathbf{N}$ with distinct roots $\alpha_1, \ldots, \alpha_n$. Then any other monic polynomial $Q(x) \in K[x]$ of degree n that is sufficiently close[5] to $P(x)$ will be irreducible over K with roots $\beta_1, \ldots, \beta_n$ and (renumbering) $K(\alpha_i) = K(\beta_i)$.*

We can use this fact to show that every finite extension of $\mathbf{Q}_l$ arises as the completion of a number field.

Corollary 1.5.15. *Let L be a finite extension of $\mathbf{Q}_\ell$ of degree n. Then there is a number field K and an absolute value $|\cdot|_K$ on K such that $\hat{K} \simeq L$. Moreover $n = [L : \mathbf{Q}_l] = [K : \mathbf{Q}]$.*

Proof. By the primitive element theorem we know that every extension of $\mathbf{Q}_\ell$ is simple. Then let $L = \mathbf{Q}_\ell(\alpha)$ and let P be the minimal polynomial of α over $\mathbf{Q}_\ell$. Since $\mathbf{Q}$ is dense in $\mathbf{Q}_\ell$, we can choose $Q(x) \in \mathbf{Q}[x]$ and β a root of $Q(x)$ as in the proposition, so that $\mathbf{Q}_\ell(\alpha) = \mathbf{Q}_\ell(\beta)$. Let $K = \mathbf{Q}(\beta)$. Clearly K is a number field of degree n (by the proposition above, $Q(x)$ is irreducible over K). Since $K \subseteq \mathbf{Q}_\ell(\beta) = L$, we can endow K with the non-archimedean absolute value obtained by restricting the one of L. Let us denote by $\hat{K}$ the completion of K with respect to this absolute value: $\hat{K}$ and L are complete and K is contained and dense in both of them. It follows that $\hat{K} = L$. □

[5]Sufficiently close means that if we consider the space of degree $\leq n$ polynomials as homeomorphic to K^n as a topological space; close then means in the obvious metric induced by the place v.

Remark 1.5.16. For a field L as in Corollary 1.5.15, the ring $\mathcal{O}_L = \mathcal{O}_{\hat{K}}$ is well-defined independently by K and $|\cdot|_K$. Moreover, an important result of algebraic number theory proves that $\mathcal{O}_L$ is a lattice in L, that means that there is a $\mathbf{Z}_\ell$ basis of $\mathcal{O}_L$ which is also a $\mathbf{Q}_\ell$ basis of L.

Let now K be any number field, not necessarily Galois, over $\mathbf{Q}$ and let $\mathcal{O}_K$ be its ring of integers. Let $\ell \in \mathbf{Z}$ be a rational prime. The factorization of the ideal $\ell\mathcal{O}_K$ in $\mathcal{O}_K$ is

$$\ell\mathcal{O}_K = \prod_{\lambda|\ell} \lambda^{e_\lambda},$$

where each of the λ above is a maximal ideal of $\mathcal{O}_K$ over the prime ℓ. Similarly to $\mathbf{Z}_\ell$, for each λ the ring of λ-*adic integers* is defined as the inverse limit

$$\mathcal{O}_{K,\lambda} = \varprojlim_n (\mathcal{O}_K/\lambda^n)$$

and the field of λ-*adic numbers* is the field of quotients K_λ of $\mathcal{O}_{K,\lambda}$. One can view $\mathbf{Z}_\ell$ as a subring of $\mathcal{O}_{K,\lambda}$ and $\mathbf{Q}_\ell$ as a subfield of K_λ. We can define the residue degree $f_\lambda = [k_\lambda : \mathbf{F}_\ell]$, where $k_\lambda = \mathcal{O}_K/\lambda \simeq (\mathcal{O}_{K,\lambda}/\lambda\mathcal{O}_{K,\lambda})$. Then, since $[K_\lambda : \mathbf{Q}_\ell] = e_\lambda f_\lambda$, the containments $\mathbf{Z}_\ell \subseteq \mathcal{O}_{K,\lambda}$ and $\mathbf{Q}_\ell \subseteq K_\lambda$ are equalities when $e_\lambda f_\lambda = 1$. Moreover, there is a ring isomorphism

$$K \otimes_{\mathbf{Q}} \mathbf{Q}_\ell \simeq \prod_{\lambda|\ell} K_\lambda.$$

The proof of this isomorphism illustrates properties of inverse limits and tensor product. Indeed, we have

$$\mathcal{O}_K \otimes_{\mathbf{Z}} \mathbf{Z}_\ell \simeq \varprojlim_n \{\mathcal{O}_K \otimes_{\mathbf{Z}} \mathbf{Z}/\ell^n\mathbf{Z}\} \simeq \varprojlim_n \{\mathcal{O}_K/\ell^n\mathcal{O}_K\}.$$

But $\mathcal{O}_K/\ell^n\mathcal{O}_K = \mathcal{O}_K/(\prod_\lambda \lambda^{ne_\lambda}) =^{6} \prod_\lambda (\mathcal{O}_K/\lambda^{ne_\lambda})$. Thus

$$\mathcal{O}_K \otimes_{\mathbf{Z}} \mathbf{Z}_\ell \simeq \varprojlim_n \{\prod_\lambda \mathcal{O}_K/\lambda^{ne_\lambda}\} \simeq \prod_\lambda \varprojlim_n \{\mathcal{O}_K/\lambda^{ne_\lambda}\} \simeq \prod_\lambda \mathcal{O}_{K,\lambda}$$

and this gives

$$\begin{aligned} K \otimes_{\mathbf{Q}} \mathbf{Q}_\ell &\simeq \mathcal{O}_K \otimes_{\mathbf{Z}} \mathbf{Q} \otimes_{\mathbf{Q}} \mathbf{Q}_\ell \simeq \mathcal{O}_K \otimes_{\mathbf{Z}} \mathbf{Q}_\ell \simeq \mathcal{O}_K \otimes_{\mathbf{Z}} \mathbf{Z}_\ell \otimes_{\mathbf{Z}_\ell} \mathbf{Q}_\ell \\ &\simeq \prod_\lambda (\mathcal{O}_{K,\lambda} \otimes_{\mathbf{Z}_\ell} \mathbf{Q}_\ell) \simeq \prod_\lambda K_\lambda. \end{aligned}$$

[6] Chinese Remainder Theorem.

Chapter 2

Deformations of representations of profinite groups

In this second chapter we will use all the preliminary notions introduced above and category theory will be our main tool. The main references are [5, Chapters 2-3] and [2, Chapter 8].

The basic situation we want to study is as follows. We are given a profinite group Π, a finite field k of positive characteristic, a non zero natural number n and a continuous (residual) representation $\bar{\rho}\colon \Pi \longrightarrow \mathrm{GL}_n(k)$. We want to try to understand all the possible lifts of this representation to $\mathrm{GL}_n(A)$, where A is a coeffiecient ring, i.e. a complete noetherian local ring with residue field k. Our main goal will be to explain what 'all possible lifts' means to make our question more precise.

Denote by $\mathcal{C}$ the category of coefficient rings, whose morphisms are local ring homomorphism which reduce to the identity on the residue field k; we define the deformation functor

$$D_{\bar{\rho}}\colon \mathcal{C} \longrightarrow \mathrm{Sets}$$

$$A \longmapsto \{\text{deformations of } \bar{\rho} \text{ to } A\}.$$

Our aim will be to prove that, under certain hypothesis, this functor is representable, i.e. there exists a coefficient ring $\mathcal{R}$, called the *universal deformation ring*, such that $D_{\bar{\rho}}$ is naturally isomorphic to the functor $h_{\mathcal{R}} \coloneqq \mathrm{Hom}(\mathcal{R}, -)$. This will lead to the existence of a *universal deformation*, namely a representation $\rho_{\mathcal{R}}\colon \Pi \longrightarrow \mathrm{GL}_n(\mathcal{R})$ such that all the other deformations are parametrized by it. This will mean that for every coefficient ring A and every lift ρ to $\mathrm{GL}_n(A)$ there exists a unique morphism $f\colon \mathcal{R} \longrightarrow A$ such that $\rho = f \circ \rho_{\mathcal{R}}$.

2.1 Coefficient rings

Let us start from considering a representation

$$\rho\colon \Pi \longrightarrow \mathrm{GL}_n(A),$$

where Π is a profinite group and A is some topological ring. Since impose the homomorphism ρ to be a continuous map, it is natural to require A to be a profinite ring as well. Then we ask A to be

- local with unique maximal ideal m_A and finite residue field $k = A/m_A$ of positive characteristic;
- Noetherian;
- complete, i.e. $A \simeq \varprojlim_N A/m_A^n$.

The third condition makes the ring A to carry a profinite topology. Indeed, since the residue field of A is finite then A/m^n is finite for every $n \in \mathbf{N}$. So if we endow each A/m^n with the discrete topology, we get that A is the inverse limit of an inverse system of discrete finite groups. This way, the ring A satisfies the request to carry a profinite topology. Then, since

$$\mathrm{GL}_N(A) = \varprojlim_n \mathrm{GL}_N(A/m_A^n),$$

$\mathrm{GL}_N(A)$ inherits a profinite topology, a basis of which consisting of normal subgroups made up of $N \times N$ matrices with coefficients in A which reduce to the identity matrix when going modulo a fixed power of m_A.

We now give the following definition.

Definition 2.1.1. A *coefficient ring* is a complete Noetherian local ring with finite residue field.

For our purposes we fix all the coefficient rings to have the same residue field k of positive characteristic p. Moreover, we ask the homorphisms between coefficient rings to satisfy the residue structure.

Definition 2.1.2. A *coefficient ring homomorphism* is a ring homomorphism between two coeffiecient rings R_1 and R_2

$$\varphi\colon R_1 \longrightarrow R_2$$

such that

1. φ is a local homomorphism, i.e. if m_{R_1} and m_{R_2} are the maximal ideals of R_1 and R_2 respectively, then $\varphi(m_{R_1}) \subseteq m_{R_2}$;

2. φ induces the identity on the residue field k.

Let then $\mathcal{C}$ be the category whose objects are coefficient rings and whose morphisms are coefficient ring homomorphisms. Moreover, let $\mathcal{C}^0$ be the subcategory of $\mathcal{C}$ such that

- its objects are artinian local rings with residue field k;

- $\mathcal{C}^0$ is a full subcategory, which means that every morphism between objects of $\mathcal{C}$ that are also objects of $\mathcal{C}^0$ are also morphisms of $\mathcal{C}^0$.

Remark 2.1.3. Thanks to a result in commutative algebra ([1, Theorem 8.1]), we know that any Artinian ring is Noetherian with Krull dimension equal to zero. Moreover, any Artinian local ring is complete because its maximal ideal is nilpotent. Hence, the set of objects of $\mathcal{C}^0$ is a subset of the set of coefficient rings and $\mathcal{C}^0$ is actually a subcategory of $\mathcal{C}$.

Furthermore, if A is a coefficient ring then it is complete, i.e. $A \simeq \varprojlim_n A/m_A^n$, where each A/m_A^n is finite and therefore Artinian. For every $n \in \mathbf{N}$, the quotient A/m_A^n has the unique maximal ideal m_A/m_A^n and then it is an object of $\mathcal{C}^0$. This means that every object of $\mathcal{C}$ is an inverse limit of objects of the subcategory $\mathcal{C}^0$. Therefore, we say that the objects of $\mathcal{C}$ are *pro-objects* of $\mathcal{C}^0$

Sometimes we will be considering the category whose objects are coefficients ring which are also algebras over another coefficient ring Λ. We will denote this category by $\mathcal{C}_\Lambda$, whose morphisms are coefficient ring homorphisms which are also Λ-algebra homomorphisms. In this case $\mathcal{C}_\Lambda^0$ will denote the subcategory of $\mathcal{C}_\Lambda$ of Artinian Λ-algebras.

2.2 Deformation functor

2.2.1 Residual representation and its deformations

We'll now introduce a functor from the categories above to the category of Sets. However, first of all, we need to introduce the concept of residual representation and its deformations. Let us then start with the definition of residual representation.

Definition 2.2.1. Let Π be a profinite group and let k be a finite field of characteristic $p > 0$. A *residual representation* is a continuous group homomorphism

$$\bar{\rho}\colon \Pi \longrightarrow \mathrm{GL}_n(k).$$

From now on, we fix the residual $\bar{\rho}$ representation and the finite field k. Moreover, we assume that every coefficient ring has residue field k.

Remark 2.2.2. If we consider a group representation

$$\rho\colon \Pi \longrightarrow \mathrm{GL}_n(A),$$

where A is a coefficient ring, then we can compose it with the natural projection

$$\pi\colon A \longrightarrow k$$

obtaining a map from $\mathrm{GL}_n(A)$ to $\mathrm{GL}_n(k)$ that we will informally called π again. We then define $\Gamma_n(A) = \ker(\pi)$. It is easy to see that $\Gamma_n(A) = 1 + \mathrm{M}_n(m_A)$, i.e. it consists of matrices whose off-diagonal elements are in m_A and whose diagonal elements belong to $1 + m_A$.

Thanks to this we can define when two representations are equivalent.

Definition 2.2.3. Two representations $\rho_1, \rho_2\colon \Pi \longrightarrow \mathrm{GL}_n(A)$ are *strictly equivalent* if there exists a matrix $P \in \Gamma_n(A)$ such that $\rho_1 = P^{-1}\rho_2 P$.

Remark 2.2.4. Note that two strictly equivalent representations give the same residual representation when composed with the projection π.

We are now ready to define what a deformation is.

Definition 2.2.5. Let $\bar{\rho}$ be a residual representation and let A be a coefficient ring. A *deformation* of $\bar{\rho}$ to A is a strict equivalence class of continuous homomorphisms $\rho\colon \Pi \longrightarrow \mathrm{GL}_n(A)$, which reduce to $\bar{\rho}$ when composed with the projection π, i.e. the following diagram is commutative

$$\begin{array}{ccc} \Pi & \overset{\rho}{\dashrightarrow} & \mathrm{GL}_n(A) \\ & \searrow^{\bar{\rho}} & \downarrow \pi \\ & & \mathrm{GL}_n(k). \end{array}$$

Remark 2.2.6. If a representation ρ satisfies the condition that $\pi \circ \rho = \bar{\rho}$, then all the representation in its strict equivalence class satisfy this equality. This 'allows' us to interchange a homomorphism with its strict equivalence class.

Remark 2.2.7. We can rephrase the concept of deformation in a more 'relative' way. Fixing again a residual representation $\bar{\rho}$, we can consider and fix a coefficient ring A and a deformation of $\bar{\rho}$ to A, call it ρ_A. Then we can define the category $\mathcal{C}(A)$ of coefficient rings R endowed with a coefficient ring map $h_R\colon R \longrightarrow A$, which is called A-*augmentation*. Then a *deformation of* ρ_A to the coefficient ring $R \in \mathcal{C}(A)$ is a strict equivalence class of homomorphisms $\rho\colon \Pi \longrightarrow \mathrm{GL}_n(R)$ such that the following diagram commutes.

$$\begin{array}{ccc} \Pi & \overset{\rho}{\dashrightarrow} & \mathrm{GL}_n(R) \\ & \searrow^{\rho_A} & \downarrow{\scriptstyle h_R} \\ & & \mathrm{GL}_n(A). \end{array}$$

Again, we say that two representation ρ, $\rho'\colon \Pi \longrightarrow \mathrm{GL}_n(R)$ are strictly equivalent if $\rho = P^{-1}\rho' P$ for some matrix $P \in \ker(h_R)$.

2.2.2 The deformation functor

We can now define a functor associated the category $\mathcal{C}$ of coefficient rings.

Definition 2.2.8. Let $\bar{\rho}$ be a fixed residual representation. The functor

$$\begin{aligned} D_{\bar{\rho}}\colon \mathcal{C} &\longrightarrow \mathrm{Sets} \\ A &\longmapsto \{\text{deformations of } \bar{\rho} \text{ to A}\} \end{aligned}$$

is called the *deformation functor*.

Remark 2.2.9. Most of times we will fix a residual representation and so we will denote the deformation functor just by D. If we work with the category $\mathcal{C}_\Lambda$ then we will write $D_{\bar{\rho},\Lambda}$ to indicate the deformation functor. It is not difficult to check that D and D_Λ are functors.

Remark 2.2.10. We can rephrase this construction by using the equivalent definition of group representation given in Remark 1.5.12, i.e. fixing a k-vector space $\bar{V}$ of finite dimension and endowing it with a continuous action of the group Π. Now, if A is a coefficient ring with residue field k, we say that a deformation V of $\bar{V}$ is a couple (V, α), where V is a free A-module of finite rank with a continuous action of Π and $\alpha : V \otimes_A k \simeq \bar{V}$ is an isomorphism as Π-representation spaces, i.e. it commutes with the action of Π. Then, we define the deformation functor as

$$\begin{aligned} D_{\bar{V}}\colon \mathcal{C} &\longrightarrow \mathrm{Sets} \\ A &\longmapsto \{\text{deformations of } \bar{V} \text{ to A}\}. \end{aligned}$$

The functors $D_{\bar{V}}$ and $D_{\bar{\rho}}$ are naturally isomorphic since if we fix a k-basis of $\bar{V}$ we can identify the automorphism group $\mathrm{Aut}_k(\bar{V})$ with $\mathrm{GL}_n(k)$ where n is the dimension of $\bar{V}$ over k. Then the Π-action on $\bar{V}$ gives a continuous residual representation $\bar{\rho}\colon \Pi \longrightarrow \mathrm{GL}_n(k)$.

Considering that the objects of $\mathcal{C}$ are pro-objects of the subcategory $\mathcal{C}^0$, we would like to prove that the functor D is completely determined by its values on the full subcategory $\mathcal{C}^0$. Firstly, note that if $A \simeq \varprojlim_n A/m_A^n$ is a coefficient ring with projection maps $\pi_{n,n+1}\colon A/m_A^{n+1} \longrightarrow A/m_A^n$ ($n \in \mathbf{N}$) and F is a set-valued covariant functor on $\mathcal{C}$, then $\{F(A/m_A^n), F(\pi_{n,m})\colon n, m \in \mathbf{N}, n < m\}$ is a projective system. Moreover, for the universal property of inverse limit we get a map $\Phi\colon F(A) \longrightarrow \varprojlim_n F(A/m_A^n)$.

Definition 2.2.11. Let F be a set-valued covariant functor on the category $\mathcal{C}$ or $\mathcal{C}_\Lambda$ for some coefficient ring Λ. We say that F is *continuous* when the morphism

$$\Phi\colon F(A) \longrightarrow \varprojlim_n F(A/m_A^n)$$

is an isomorphism for every $A \in \mathcal{C}$ or $\mathcal{C}_\Lambda$.

Theorem 2.2.12. *The functors D and D_Λ are continuous.*

Proof. We will prove the thesis just for the functor D. We have to show that for every $A \in \mathcal{C}$ the map

$$\Phi\colon D(A) \longrightarrow \varprojlim_k D(A/m_A^k)$$

is a bijectiction. First of all recall that Φ maps a deformation ρ to A to a compatible sequence $\{\rho_k\}_{k\in\mathbf{N}}$, where each ρ_k is a deformation of $\bar{\rho}$ to A/m_A^k obtained by reducing ρ modulo m_A^k, more precisely reducing modulo m_A^k any of the representation in the strict equivalence class of ρ.

In order to prove surjectivity we have to show that any compatible sequence $\{\rho_k\}_{k\in\mathbf{N}}$ comes from a deformation ρ to A. Let then $\{\rho_k\}_{k\in\mathbf{N}}$ be such a sequence and let us build an appropriate system of representatives by induction.

- For $k = 1$ the forced choice is to set $\rho_1 = \bar{\rho}$;
- . Let $h \in \mathbf{N}^*$ and suppose we have set the homomorphisms $r_1, r_2, ..., r_h$ for which represent the classes of $\rho_1, \rho_2, ..., \rho_h$ and form a coherent system. Let us now choose r_{h+1}. Since it is a sitable sequence, if r' is a representantive of ρ_{h+1},

we must have $r' \equiv r_h \pmod{m^h}$, i.e. it must exists a matrix $M_h \in \Gamma(A/m_A^h)$ such that $M_h^{-1}(r'(\text{mod } m^h))M_{\equiv} r_h$. Since the reduction map $\Gamma_n(A/m_A^{h+1}) \longrightarrow \Gamma_n(A/m_A^h)$ is surjective, we can then choose a lift of M_h to $\Gamma(A/m_A^{h+1})$, call it M_{h+1}. Then we can extend the sequence setting $r_{h+1} = M_{h+1}^{-1} r' M_{h+1}$. By induction we obtain an appropriate sequence of representative homomorphisms $r_k \colon \Pi \longrightarrow \mathrm{GL}_n(A/m_A^k)$ as k varies in $\mathbf{N}$.

Recalling that $\mathrm{GL}_n(A) = \varprojlim_k \mathrm{GL}_n(A/m_A^k)$, the inverse limit of the projective system $\{r_k\}_{k\in\mathbf{N}}$ gives a deformation $\rho \colon \Pi \longrightarrow \mathrm{GL}_n(A)$, whose reduction modulo m^h is ρ_h. To prove that Φ is injective we have to show that taken two deformations ρ and ρ' to A such that their reduction ρ_k and ρ'_k are strictly equivalent for every k, then ρ and ρ' are strictly equivalent. Since for every $k \in \mathbf{N}$, ρ_k and ρ'_k are strictly equivalent, we have that $\rho_k = M_k^{-1}\rho'_k M^k$ for some $M_k \in \Gamma(A/m^k)$. Since $\Gamma(A) = \varprojlim_k \Gamma(A/m_A^k)$ we can choose $M_{k+1} \equiv M_k \pmod{m^k}$ giving a coherent sequence and so an element $M \in \Gamma(A)$ such that $\rho = M^{-1}\rho' M$. □

2.3 Representability of the deformation functor

In this section we will study further the properties of the deformation functor, focusing on its representability. Let us then start with the definition of representable functor.

Definition 2.3.1. Let $\mathcal{C}$ be a locally small category, i.e. a category in which for every objects A, B the collection of morphisms $\mathrm{Hom}(A, B)$ is a set. For every object $A \in \mathcal{C}$ let $h_A \coloneqq \mathrm{Hom}(A, -)$ be the functor that maps an object X of $\mathcal{C}$ to the set $\mathrm{Hom}(A, X)$ and such that, if $X, Y \in \mathcal{C}$ and $\varphi : X \longrightarrow Y$ is a morphism, $h_A(\varphi)$ is just the post-composition with φ,i.e.

$$h_A(\varphi) \colon \mathrm{Hom}(A, X) \longrightarrow \mathrm{Hom}(A, Y)$$
$$f \longmapsto \varphi \circ f.$$

Then, we say that a functor

$$F \colon \mathcal{C} \longrightarrow \mathrm{Sets}$$

is *representable* if it is naturally isomorphic to the functor h_A for some $A \in \mathcal{C}$, i.e. for every $X \in \mathcal{C}$ there is an isomorphism $\eta_X : F(X) \longrightarrow \mathrm{Hom}(A, X)$, such that if

$Y \in \mathcal{C}$ and $\varphi : X \longrightarrow Y$ is a morphism in $\mathcal{C}$, the following diagram commutes

$$\begin{array}{ccc} F(X) & \xrightarrow{\eta_X} & \mathrm{Hom}(A, X) \\ {\scriptstyle F(\varphi)}\downarrow & & \downarrow{\scriptstyle \varphi\circ -} \\ F(Y) & \xrightarrow{\eta_Y} & \mathrm{Hom}(A, Y). \end{array}$$

Then we say that a representation of F is a pair (A, Φ) where A is an object of $\mathcal{C}$ and

$$\Phi\colon \mathrm{Hom}(A, -) \longrightarrow F$$

is a natural isomorphism.

For the rest of this chapter, our main goal will be to establish if the deformation functor $D_{\bar{\rho}}$ is representable, i.e. if there exist a coefficient ring $\mathcal{R}_{\bar{\rho}}$ and a natural isomorphism between $\mathrm{Hom}(\mathcal{R}_{\bar{\rho}}, -)$ and $D_{\bar{\rho}}$. Since the residual representation $\bar{\rho}$ is fixed, we will just call $\mathcal{R}_{\bar{\rho}} = \mathcal{R}$ and $\rho_{\mathcal{R}}\colon \Pi \longrightarrow \mathrm{GL}_n(\mathcal{R})$ its deformation.

If we assume that our functor is represented by $\mathcal{R}$, then for every coefficient ring R and every coefficient ring homomorphism $\varphi\colon \mathcal{R} \longrightarrow R$ the following diagram commutes

$$\begin{array}{ccc} D(\mathcal{R}) & \xrightarrow{\eta_{\mathcal{R}}} & \mathrm{Hom}(\mathcal{R}, \mathcal{R}) \\ \downarrow & & \downarrow{\scriptstyle \varphi\circ -} \\ D(R) & \xrightarrow{\eta_R} & \mathrm{Hom}(\mathcal{R}, R). \end{array}$$

Therefore, the identity map in $\mathrm{Hom}(\mathcal{R}, \mathcal{R})$ must correspond to a unique deformation $\rho_{\mathcal{R}}$ to $\mathcal{R}$ and the map from $D(\mathcal{R})$ to $D(R)$ must be the post-composition with φ, i.e. if ρ is a deformation to R, then $\rho = \varphi \circ \rho_{\mathcal{R}}$, where we informally used the same letter φ for the map $\mathrm{GL}_n(\mathcal{R}) \longrightarrow \mathrm{GL}_n(R)$. Moreover, since the map η_R is bijection, for every coefficient ring R and every deformation ρ to R there exists a unique coefficient ring homorphism $\varphi\colon \mathcal{R} \longrightarrow R$ such that $\rho = \varphi \circ \rho_{\mathcal{R}}$. Hence, every deformation of $\bar{\rho}$ to a coefficient ring is 'parametrized' by $\rho_{\mathcal{R}}$. For this reason $\rho_{\mathcal{R}}$ is called the *universal deformation of* $\bar{\rho}$ and $\mathcal{R}$ is the *universal deformation ring*.

In order to prove that the deformation functor is indeed representable, we need to introduce some tools and results of category theory, starting from *fiber products*.

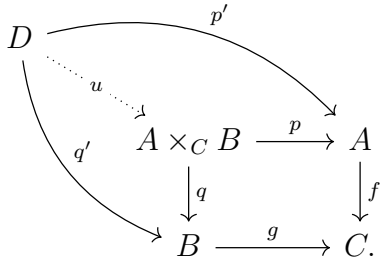
2.3.1 Fiber product and Mayer-Vietoris property

Definition 2.3.2. Let $\mathcal{C}$ be a category, A, B, C be objects of $\mathcal{C}$ and $f\colon A \longrightarrow C$, $g\colon B \longrightarrow C$ be morphisms. Then a *fiber product* (or *pullback*) of f and g consists

of an object which we denote by $A \times_C B$ and two morphisms $p : A \times_C B \longrightarrow A$, $q : A \times_C B \longrightarrow B$ such that the following diagram commutes

$$\begin{array}{ccc} A \times_C B & \xrightarrow{q} & B \\ {\scriptstyle p}\downarrow & & \downarrow{\scriptstyle g} \\ A & \xrightarrow{f} & C \end{array}$$

in a *universal* way, which means that for every other triple (D, p', q'), where $p\colon D \longrightarrow A$ and $q'\colon D \longrightarrow B$, there must exist a unique morphism $u : D \longrightarrow A \times_C B$ such that the following diagram commutes



Let us see some examples of pullbacks.

Example 2.3.3. *In the category of commutative rings the fiber product between A and B over C is the subring of $A \times B$ defined as*

$$A \times_C B = \{(a, b) \in A \times_C B : f(a) = g(b)\},$$

where the maps p and q are just the projections to A and B respectively.

Remark 2.3.4. Not every category has fiber products. For example, let us consider the category $\mathcal{C}$ of coefficient rings and let $A = k[[X, Y]]$, $B = k$ and $C = k[[X]]$ where k is a field. Then A, B and C are local, complete and Noetherian rings, i.e. they are objects of $\mathcal{C}$. Let us then consider the inclusion and the projection maps

$$g\colon k \longrightarrow k[[X]], \quad f\colon k[[X, Y]] \longrightarrow k[[X]].$$

The fiber product of $A \times_C B$ is the sub-ring $k \oplus Yk[[X, Y]]$ of $k[[X, Y]]$. This sub-ring is complete and local with maximal ideal $m = Yk[[X, Y]]$, but it is not noetherian, because the k-vector space $m/m^2 \simeq k[[X]]$ is infinite dimensional. In fact, if $A \times_C B$ was Noetherian then we could apply Nakayama's lemma to the finitely generated $k[[X, Y]]$-module $Yk[[X, Y]]$ obtaining that m/m^2 is a finitely dimensional k-vector space, which is a contradiction.

Let us now consider a set-valued functor F on a category $\mathcal{C}$ with fiber products. By the functoriality of F, the following diagram

$$\begin{array}{ccc} F(A \times_C B) & \xrightarrow{F(q)} & F(B) \\ {\scriptstyle F(p)}\downarrow & & \downarrow{\scriptstyle F(g)} \\ F(A) & \xrightarrow{F(f)} & F(C) \end{array}$$

is commutative and so, by the universal property of the fiber product, there exists a map

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

Definition 2.3.5. Let $\mathcal{C}$ be a category with fiber products and let F be a set-valued functor on it; then F is said to satisfy the *Mayer-Vietoris property* if the map $\Phi_{A\times_C B}$ is a bijection.

Remark 2.3.6. If we are working with a category $\mathcal{C}$ in which fiber products exist, then the Mayer-Vietoris property is a necessary condition for a set-valued functor on $\mathcal{C}$ to be representable. Indeed, using again the universal property of fiber product, we have that for very $D \in \mathcal{C}$ there is a map

$$\begin{aligned} \mathrm{Hom}(D, A \times_C B) &\longrightarrow \mathrm{Hom}(D, A) \times_{\mathrm{Hom}(D,C)} \mathrm{Hom}(D, B) \\ h &\longrightarrow (\pi_1 \circ h, \pi_2 \circ h), \end{aligned}$$

which is well defined and a bijection, being π_1 and π_2 the projections of $A \times_C B$ on A and B respectively. Then if F is a representable functor represented by the object $\mathcal{R}$, we can use the bijection above to build the following commutative diagram

$$\begin{array}{ccc} \mathrm{Hom}(\mathcal{R}, A \times_C B) & \longleftrightarrow & \mathrm{Hom}(\mathcal{R}, A) \times_{\mathrm{Hom}(\mathcal{R},C)} \mathrm{Hom}(\mathcal{R}, B) \\ \updownarrow & & \updownarrow \\ F(A \times_C B) & \xleftarrow{\Phi_{A\times_C B}} & F(A) \times_{F(C)} F(B) \end{array} .$$

Since the higher horizontal arrow and the two vertical ones are bijections, as a consequence of the commutativity of the diagram, the map $\Phi_{A\times_C B}$ is a bijection, too. Hnece, F satisfies the Mayer-Vietoris property.

Remark 2.3.7. Recall that, as shown in Section 2.1, every object of the category of coefficient rings $\mathcal{C}$ is a pro-object of $\mathcal{C}_0$. Then, as we showed above, a continuous

functor F on $\mathcal{C}$ is completely determined by its values on $\mathcal{C}^0$. Therefore, we can 'restrict' the study of the representability of F to the subcategory $\mathcal{C}^0$, wondering if there exist an objects $\mathcal{R}$ of $\mathcal{C}$ such that for every $A \in \mathcal{C}^0$ we have $F(A) \simeq \mathrm{Hom}(\mathcal{R}, A)$. It may happen that $\mathcal{R}$ is not an object of $\mathcal{C}^0$ and in this case we say that F is *pro-representable* on the subcategory $\mathcal{C}^0$.

2.3.2 The Zariski tangent space and its functorial interpretation

Before stating the main theorem of this chapter, that will give us sufficient conditions for a set-valued covariant functor to be representable, we have to introduce another object, namely the Zariski tangent space of a coefficient ring. From now on we will be working with the subcategory $\mathcal{C}_\Lambda$, where Λ is a fixed coefficient ring and m_Λ is its maximal ideal.

It may be useful to recall firstly the definition of *tangent space* of a local ring $\mathbf{R}$. If $\mathbf{m}$ is the maximal ideal of $\mathbf{R}$, the *cotangent space* of $\mathbf{R}$ is defined as the quotient $\mathbf{m}/\mathbf{m^2}$. It is obviously a vector space over the residue field $\mathbf{R}/\mathbf{m}$. Its dual space (as a $(\mathbf{R}/\mathbf{m})$-vector space) is called the tangent space of $\mathbf{R}$. Similarly we can give the following definition.

Definition 2.3.8. Let $R \in \mathcal{C}_\Lambda$ and let m_R be its maximal ideal, then the *Zariski cotangent space of* R is

$$t_R^* = m_R/(m_R^2, m_\Lambda R),$$

where $m_\Lambda R$ denotes the ideal of R generated by the image of m_Λ in R through the structural algebra homomorphism $\Lambda \longrightarrow R$. The *Zariski tangent space of* R is then the dual space

$$t_R = \mathrm{Hom}_k(t_R^*, k).$$

Remark 2.3.9. It's worth noting that the definition above is consistent since t_R^* is a $(\Lambda/m_\Lambda \simeq k)$-vector space. Moreover, since R is Noetherian m_R is finitely generated and therefore t_R^* is a finite dimensional k-vector space and hence so is t_R.

We want now to give a functorial interpretation of the Zariski tangent space. We have then to introduce the following Λ-algebra

$$k[\epsilon] = k \oplus k\epsilon \simeq k[X]/X^2,$$

which is a local ring with maximal ideal generated by ϵ, which has square zero. We have the following result.

Proposition 2.3.10. *Suppose F is a functor represented by R, then, there is a natural set bijection*

$$\mathrm{Hom}_k(m_R/(m_R^2, m_\Lambda R), k) \longleftrightarrow \mathrm{Hom}_\Lambda(R, k[\epsilon]),$$

where Hom_k *means k-vector space homomorphisms and* Hom_Λ *denotes homomorphisms of coefficient Λ-algebras.*

Proof. If we take a map $f \in \mathrm{Hom}_\Lambda(R, k[\epsilon])$, since it is a local morphism, the maximal ideal $f(m_R) \subseteq (\epsilon)$. Then $f(m_R^2) = 0$ because $(\epsilon)^2$=0. Moreover, since $k = \Lambda/m_\Lambda$ and f, as a morphism of coefficient rings, induces the identity on K then $m_\Lambda R$ must be mapped to zero as well. This means that the ideal $(m_R^2, m_\Lambda R)$ in contained in the kernel of f and so f factorizes as

$$R \xrightarrow{\pi} R/(m_R^2, m_\Lambda R) \longrightarrow k[\epsilon],$$

where π denotes the naatural quotient map. This factorization shows that there is a bijection

$$\begin{aligned} \mathrm{Hom}_\Lambda(R/(m_R^2, m_\Lambda R), k[\epsilon]) &\longrightarrow \mathrm{Hom}_\Lambda(R, k[\epsilon]) \\ g &\longmapsto g \circ \pi. \end{aligned}$$

Now observe that $R/(m_R^2, m_\Lambda)$ decomposes as k-vector space as

$$R/(m_R^2, m_\Lambda R) \simeq k \oplus m_R/(m_R^2, m_\Lambda R).$$

Since if $x \in R/(m_R^2, m_\Lambda R)$, $x^2 = 0$, a Λ-algebra coefficient morphism from $k \oplus m_R/(m_R^2, m_\Lambda R)$ to $k[\epsilon] = k \oplus \epsilon k$ respects, as a k-linear morphism, the direct sum decomposition and it is the idenitity on the first summand. Therefore there is a bijection

$$\mathrm{Hom}_\Lambda(R, k[\epsilon]) \longleftrightarrow \mathrm{Hom}_k(m_R/(m_R^2, m_\Lambda R), \epsilon k).$$

Identifying the one dimensional k-vector spaces ϵk with k we obtain the thesis. □

Thanks to this bijection we can say that, if F is a functor on $\mathcal{C}_\Lambda$ represented by the ring $\mathcal{R}$, then $F(k[\epsilon]) = \mathrm{Hom}_\Lambda(\mathcal{R}, k[\epsilon]) = \mathrm{Hom}_k(m_\mathcal{R}/(m_\mathcal{R}^2, m_\Lambda \mathcal{R}), k) = t_R$ at least as sets.

We would like now to make this bijection into a k-linear isomorphism, but in order to do that we have to endow $F(k[\epsilon])$, which a priori is just a set, with a k-linear structure.

The scalar multiplication can be defined easily. For every $\alpha \in k$ we can consider the bijective map

$$f_\alpha \colon k[\epsilon] \longrightarrow k[\epsilon]$$

$$x + \epsilon y \longmapsto x + \alpha y \epsilon.$$

Then applying the functor F to f_α we get a scalar multiplication on $F(k[\epsilon])$. The addition map is harder to be defined. Suppose first of all that $F(k)$ is a singleton. Indeed, we need the map

$$\Phi_{k[\epsilon]\times_k k[\epsilon]} \colon F(k[\epsilon] \times_k k[\epsilon]) \longrightarrow F(k[\epsilon]) \times F(k[\epsilon])$$

to be a bijection. As for the multiplication we start by considering the map

$$+ \colon k[\epsilon] \times_k k[\epsilon] \longrightarrow k[\epsilon]$$

$$(x_1 + y_1\epsilon, x_2 + y_2\epsilon) \longmapsto x_1 + x_2 + (y_1 + y_2)\epsilon$$

and the we define the addition map on $F(k[\epsilon])$ by the composition:

$$F(k[\epsilon]) \times F(k[\epsilon]) \xrightarrow{\Phi_{k[\epsilon]\times_k k[\epsilon]}} F(k[\epsilon] \times_k k[\epsilon]) \xrightarrow{F(+)} F(k[\epsilon]).$$

This proves the following proposition.

Proposition 2.3.11. *Let $F \colon \mathcal{C}_\Lambda^0 \longrightarrow$ Sets be a covariant functor such that $F(k)$ consists of a single element. Suppose that the natural map*

$$\Phi_{k[\epsilon]\times_k k[\epsilon]} \colon F(k[\epsilon] \times_k k[\epsilon]) \longrightarrow F(k[\epsilon]) \times F(k[\epsilon])$$

is a bijection. Then $F(k[\epsilon])$ has a natural vector space structure over k.

Remark 2.3.12. The hypothesis that $F(k)$ is a singleton is necessary to give $F(k[\epsilon])$ the structure of vector space. Indeed, we want to define a sum operation

$$F(k[\epsilon]) \times F(k[\epsilon]) \longrightarrow F(k[\epsilon])$$

using the bijective map $\Phi_{k[\epsilon]\times_k k[\epsilon]}$, which a priori has image in the fiber product $F(k[\epsilon]) \times_{F(k)} F(k[\epsilon])$. But thanks to the fact that $F(k)$ is a singleton this fiber product coincides with the cartesian product of the set $F(k[\epsilon])$ with itself. Indeed, in the category of Sets the fiber product is the same as in the category of commutative rings of Example 2.3.3 (in our case $A = B = F(k[\epsilon])$ and the maps $f, g : F(k[\epsilon]) \longrightarrow F(k)$ are constant).

Remark 2.3.13. When $F\colon \mathcal{C}_\Lambda^0 \longrightarrow$ Sets is represented by the ring $\mathcal{R}$ then $F(k) = \mathrm{Hom}_\Lambda(R,k) = \{*\}$ and $\Phi_{k[\epsilon]\times k[\epsilon]}$ is a bijection by Remark 2.3.6. The k-vector space structure, given by Proposition 2.3.11, of $F(k[\epsilon])$ corresponds to the one of $\mathrm{Hom}_\Lambda(\mathcal{R}, k[\epsilon])$ which is a k-vector space in the following way: if $a \in k$ and $f \in \mathrm{Hom}_\Lambda(\mathcal{R}, k[\epsilon])$ then $a \cdot f$ is defined as $(a \cdot f)(x) = a \cdot f(x)$.

Remark 2.3.14. If $F\colon \mathcal{C}_\Lambda^0 \longrightarrow$ Sets is represented by $\mathcal{R}$, then for the discussion above $t_F \simeq t_R$, where t_R is the tangent space of the ring $\mathcal{R}$.

We can then give these definitions.

Definition 2.3.15. The hypothesis that the map $\Phi_{k[\epsilon]\times_k k[\epsilon]}$ is a bijection is called *the tangent space hypothesis over* k and we denote it by T_k. When it is satisfied $t_F = F(k[\epsilon])$ is called the *tangent space of the functor* F.

Definition 2.3.16. The functor

$$F\colon \mathcal{C}_\Lambda^0 \longrightarrow \text{Sets}$$

is said to be *nearly representable* if it satisfies the tangent space hypothesis and the tangent space t_F of F is finite dimensional.

It will turn out that many functors we will be considering will not be representable but they will be nearly representable.

Remark 2.3.17. We could extend the definition of the Zariski tangent space to the relative case fixing a coefficient Λ-algebra A and a covariant functor $F\colon \mathcal{C}_\Lambda(A) \longrightarrow$ Sets and supposing that $F(A)$ consists of a single point.

Let then $A[\epsilon] := A \oplus \epsilon A \simeq A[X]/X^2$ be the free A-module of rank 2 with basis $\{1, \epsilon\}$ and where $\epsilon \equiv X \pmod{X^2}$. Then we can consider $A[\epsilon]$ as an A-augmented coefficient Λ-algebra, where the A-augmentation is just the projection going modulo (ϵ). Then $A[\epsilon]$ is an object of the category $\mathcal{C}_\Lambda(A)$. Exactly as above, we can define a scalar multiplication map f_α and an addition map $+$ on $A[\epsilon]$. Then if the map

$$\Phi_{A[\epsilon]\times_A A[\epsilon]}\colon F(A[\epsilon] \times_A A[\epsilon]) \longrightarrow F(A[\epsilon]) \times F(A[\epsilon])$$

is a bijection, we can define the Zariski tangent A-module

$$t_{F,A} = F(A[\epsilon]).$$

Since any coefficient Λ-algebra has a natural k-augmentation, we can think of the absolute case as a particular case of the relative one, where $A = k$.

2.4 Schlessinger's theorem

Following the original work of Schlessinger (see [11]), in this section we will study the conditions that a covariant functor

$$F\colon \mathcal{C}_\Lambda^0 \longrightarrow \text{Sets}$$

must satisfy to be (pro-)representable and it will be evident how the tangent space hypothesis is connected to these conditions. Moreover, the main object of this section will be Schlessinger's theorem, which is basically an optimization of the following theorem of Grothendieck (see [5, Theorem 2.5]).

Theorem 2.4.1 (Grothendieck)**.** *Let $F\colon \mathcal{C}_\Lambda^0 \longrightarrow$ Sets be a covariant functor such that $F(k)$ is a singleton. Then F is pro-representable if and only if*

1. *F satisfies the Mayer-Vietoris property;*
2. *$F(k[\epsilon])$ is a finite dimensional k-vector space.*

The weakness of this theorem is that we really need to check that for every commutative diagram

$$\begin{array}{ccc} A \times_C B & \xrightarrow{q} & B \\ \downarrow{\scriptstyle p} & & \downarrow{\scriptstyle g} \\ A & \xrightarrow{f} & C \end{array}$$

the map $\Phi_{A\times_C B}\colon F(A \times_C B) \longrightarrow F(A) \times_{F(C)} F(B)$ is a bijection and this is clearly hard to do in general. Schlessinger's criterion weaknesses this condition: it cuts down the number of diagrams for which one must check the Mayer-Vietoris property. However, before stating this theorem we need the following definition.

Definition 2.4.2. Let A and C be objects of $\mathcal{C}_\Lambda$. Then a coefficient homomorphism $f\colon A \longrightarrow C$ is *small* if it is surjective and $\ker(f)$ is a principal ideal annihilated by m_A, i.e. $m_A \ker(f) = 0$.

Remark 2.4.3. It is easy to check that any surjective homomorphism in $\mathcal{C}_\Lambda^0$ factors trough a sequence of small homomorphisms. Indeed, let us consider $s\colon A \longrightarrow B$ a surjective homommorphism of complete artinian local rings which is not an isomorprhism. Let $I = \ker(s)$, then since A is noetherian I is finitely generated, let us say $I = (t_1, ..., t_n)$. Since A is artinian there exists $p_1 \in \mathbf{N}$ minimal such that $t_1 m_A^{p_1} = 0$. Let us then consider $q_1 \in t_1 m_A^{p_1 - 1}$. Then the map $A \longrightarrow A/(q_1)$ is small.

If we iterate this argument replacing A with $A/(q_1) = C_1$ and considering the map $C_1 \longrightarrow B$ (which is still surjective) we get a sequence

$$A \longrightarrow C_1 \longrightarrow C_2 \longrightarrow \ldots \longrightarrow C_n \longrightarrow B$$

of small maps through which s factors. At a certain point B is reached. Indeed, A is artinian and noetherian and so it has finite length.Then, since we have $l(A) \geq n + l(B)$[1], if B wasn't reached then we would get a contradiction.

We are now ready to state Schlessinger's theorem.

Theorem 2.4.4 (Schlessinger)**.** *Let $F\colon \mathcal{C}_\Lambda^0 \longrightarrow$ Sets be a covariant functor such that $F(k)$ consists exactly of one element and let us then consider the following commutative diagram*

$$\begin{array}{ccc} A \times_C B & \xrightarrow{q} & B \\ \downarrow{\scriptstyle p} & & \downarrow{\scriptstyle g} \\ A & \xrightarrow{f} & C. \end{array}$$

Then F is pro-representable if the following four conditions hold

($\mathbf{H_1}$) *if the map $f : A \longrightarrow C$ is small then $\Phi_{A\times_C B}$ is surjective;*

($\mathbf{H_2}$) *if $C = k$ and $B = k[\epsilon]$, then $\Phi_{A\times_C B}$ is bijective;*

($\mathbf{H_3}$) *the k-vector space $t_F = F(k[\epsilon])$ is finite-dimensional;*

($\mathbf{H_4}$) *if $A = B$, the maps f and g are the same and both small, then $\Phi_{A\times_C B}$ is bijective.*

In particular, there exists an object $\mathcal{R}$ of $\mathcal{C}_\Lambda$ such that $F(A) \simeq \mathrm{Hom}(\mathcal{R}, A)$ for every A in C_Λ^0.

Remark 2.4.5. It is important to note that the statement of the theorem above is consistent. Indeed, if $\mathbf{H_2}$ holds, then applying it to the case $A = B = k[\epsilon]$ shows that T_k is satisfied and this allows us to think of $t_F = F(k[\epsilon])$ as a k-vector space.

Remark 2.4.6. It is worth noting that if a functor F is representable then we showed above that for every object A, B and C of $\mathcal{C}_\Lambda^0$ the map $\Phi_{A\times_C B}$ is a bijection and $t_F \simeq t_{\mathcal{R}}$. Therefore, F satisfies conditions $\mathbf{H_1}, \mathbf{H_2}, \mathbf{H_3}, \mathbf{H_4}$ and then Schlessinger's theorem gives necessary and sufficient conditions for a functor to be representable.

[1]Let M be a module over a ring R, the length of M is $l_A(M) = sup\{t : \exists \;\; 0 = M_0 \subset M_1 \subset M_2 \subset ... \subset M_t = M\}$, where each M_i is a sub-module of M and the inclusions in the chain are strict.

Remark 2.4.7. One can easily prove that if $\mathbf{H_1}$ is valid, then $\Phi_{A\times_C B}$ is surjective for every surjective map $f\colon A \longrightarrow B$, thanks to the factorization into small maps showed in Remark 2.4.3.

Very often functors on $\mathcal{C}_\Lambda^0$ satisfy the first three conditions $\mathbf{H_1}, \mathbf{H_2}, \mathbf{H_3}$, but they don't satisfy condition $\mathbf{H_4}$. These functors are 'very close' to be pro-representable, in the sense of the follwing definition.

Definition 2.4.8. Let F and F' be covariant functors on $\mathcal{C}_\Lambda$ such that $F(k)$ and $F'(k)$ are both singletons. Then a morphism $\Theta\colon F' \longrightarrow F$ is said to be *smooth* if it satisfies the following lifting property: given any surjection $f\colon B \twoheadrightarrow A$ in $\mathcal{C}_\Lambda$, any element $\alpha' \in F'(A)$ and any lifting of $\alpha = \Theta(\alpha') \in F(A)$ via $F(f)$ to an element $\beta \in F(B)$, there exists an element $\beta' \in F'(B)$ which is a lifting of α' via $F'(f)$ such that $\Theta(\beta') = \beta$. Equivalently, we may rephrase this lifting property as the condition that the natural mapping

$$F'(B) \longrightarrow F'(A) \times_{F(A)} F(B)$$

is surjective for all the surjective maps $B \twoheadrightarrow A$ in $\mathcal{C}_\Lambda$.

Remark 2.4.9. Since, as proved in Remark 2.4.3, every surjective map factors through a sequence of small extensions it is sufficient to check the last conditions just for small maps. Indeed, it is easy to check that the lifting property mentioned in the definition above is compatible with the composition of surjective maps: taking α', $\alpha = \Theta(\alpha')$, β' and $\beta = \Theta(\beta')$ as in definition and a surjection $g : C \twoheadrightarrow B$ in $\mathcal{C}_\Lambda$, for any lifting $\gamma \in F(C)$ of β there exists $\gamma' \in F'(C)$ which is a lifting of β' and such that $\Theta(\gamma') = \gamma$. Then it is obvious that γ is a lift of α with respect to the surjective map $g \circ f$ and that γ' is a lifting of α such that $\Theta(\gamma') = \gamma$. Therefore, if F satisfies the lifting property for every small map then thanks to the compatibility with composition the lifting property holds for every surjective map.

Definition 2.4.10. Let $F\colon \mathcal{C}_\Lambda \longrightarrow$ Sets be a covariant functor. A *pro-representable hull* for F is a pair (R, ξ), where R is a coefficient $\Lambda-$algebra, and $\xi\colon h_R \longrightarrow F$ is a morphism of functors, satisfying two properties

1. the morphism ξ is smooth;

2. the induced mapping on Zariski tangent spaces $t_R \longrightarrow t_F$ is an isomorphism of k-vector spaces, where t_R is the Zariski vector space relative to the functor h_R.

We are now ready to give the proof of Schlessinger's theorem: first we will show that any covariant set-valued functor on $\mathcal{C}_\Lambda$, that satisfies conditions $(\mathbf{H_1}), (\mathbf{H_2}), (\mathbf{H_3})$ and such that $F(k)$ is a singleton, has a pro-representable hull (R, ξ). Then we will see that, if F satisfies also $(\mathbf{H_4})$, then ξ is a bijection and hence F is representable by R.

Proof. Suppose F satisfies conditions $\mathbf{H_1}, \mathbf{H_2}, \mathbf{H_3}$. We will construct a hull R by successive approximation. For the first step of induction, we look for a couple (R_2, ξ_2) such that $\xi_2 : h_{R_2} \longrightarrow F$ is a morphism of functors (that by the way may not be smooth) and $t_{R_2} \simeq t_F$.

Let $t_1, ..., t_r$ be a basis of t_F and set $S = \Lambda[[T_1, ..., T_r]]$, which is a coefficient ring whose unique maximal ideal is $m_S = (T_1, ..., T_r)$. Let

$$R_2 = S/(m_S^2 + m_\Lambda S) \simeq \frac{(\Lambda/m_\Lambda)[[T_1, ..., T_r]]}{(T_i^2, T_iT_j)_{1\leq i,j\leq r}} \simeq \underbrace{k[\epsilon] \times_k k[\epsilon] \times_k \cdots \times_k k[\epsilon]}_{r \text{ times}}.$$

Now, since $F(k) = \{*\}$ and therefore, as explained in Remark 2.3.12, $\times_{F(k)} = \times$, then by $\mathbf{H_2}$

$$F(R_2) \simeq \underbrace{F(k[\epsilon]) \times F(k[\epsilon]) \times \cdots \times F(k[\epsilon])}_{r \text{ times}} \simeq \underbrace{t_F \times t_F \times \cdots \times t_F}_{r \text{ times}}.$$

The right hand side is isomorphic to $\mathrm{Hom}_k(t_F, t_F)$ by the choice of a basis for t_F. Hence, the identity element $\mathrm{id} \in \mathrm{Hom}_k(t_F, t_F)$ defines an element $\xi_2 \in F(R_2)$, that corresponds by Yoneda's lemma to a natural transformation $\xi_2 \colon h_{R_2} \longrightarrow F$. Then let $x_i \in \mathrm{Hom}(k[[T_1]] \times \cdots \times k[[T_r]], k[\epsilon])$ denotes, for any $1 \leq i \leq r$ the map that sends the r-tuple $(0, \ldots, T_i, \ldots, 0)$ with element T_i in position $1 \leq j \leq r$ and 0 otherwise to $\delta_{ij}\epsilon$, where δ_{ij} denotes the Kronecker delta function and the r-tuple $(0, \ldots, 1, \ldots, 0)$ with element 1 in position $1 \leq j \leq r$ and 0 otherwise to δ_{ij} (note that x_i defines a coeffiecient ring map). The map

$$\begin{aligned} t_{R_2} = \mathrm{Hom}(R_2, k[\epsilon]) = \mathrm{Hom}(k[[T_1]] \times \cdots \times k[[T_r]], k[\epsilon]) &\longrightarrow F(k[\epsilon]) = t_F \\ x_i &\longmapsto t_i \end{aligned}$$

is an isomorphism of k-vector spaces because the set $\{x_i \colon \leq i \leq r\}$ is a basis. We have then completed the first step of our induction.

Now suppose by induction that we have found (R_q, ξ_q) with $R_q = S/J_q$ for some

ideal J_q and $\xi_q \colon h_{R_q} \longrightarrow F$ is a morphism of functors. We seek an ideal J_{q+1} minimal among ideals $J \subset S$ satisfying $m_s J_q \subseteq J \subseteq J_q$ such that ξ_q lifts to S/J, which means that there exists $\xi_J \colon h_{S/J} \longrightarrow F$ such that the diagram must commutes

$$\begin{array}{ccc} \mathrm{Hom}(R_q, -) & \xrightarrow{-\circ\pi_J} & \mathrm{Hom}(S/J, -) \\ & \searrow^{\xi_q} & \downarrow{\scriptstyle \xi_J} \\ & & F, \end{array} \tag{2.1}$$

where $\pi_J \colon S/J \longrightarrow R_q$ is the projection map. Each such J corresponds to a vector subspace of $J_q/m_S J_q$, hence it is sufficient to show that the set $\mathcal{S}$ of such ideals is stable under pairwise intersection. So let $J, K \in \mathcal{S}$ and enlarge J such that $J + K = J_q$ without changing the intersection $J \cap K$. We can do it because if $J \subseteq J'$ is such that $J' + K = J_q$ then we have $J' \subseteq J_q$ and $m_s J_q \subseteq J \subseteq J'$ and the composition $S/J \longrightarrow S/J' \longrightarrow R_q$ is a factorization of the projection π_J. Now since the map $S/J \longrightarrow S/J'$ is surjetive and for every coefficient ring A the functor $\mathrm{Hom}(-, A)$ is a contravariant right exact functor, then we can see $\mathrm{Hom}(S/J', A)$ as contained in $\mathrm{Hom}(S/J, A)$. Therefore we can see $\mathrm{Hom}(S/J', -)$ as a subfunctor of $\mathrm{Hom}(S/J, -)$ and if we consider $\xi_{J'}$ as the restriction of ξ_J to $\mathrm{Hom}(S/J', A)$ then it is clear that ξ_q lifts to S/J'.

Moreover

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

since, by the universal property of fiber product and because we choose J such that $J + K = J_q$,

$$S/J \times_{(S/J_q)} S/K = \{(\bar{a}, \bar{b}) \in S/J \times S/K \colon \bar{a} = \bar{b} \text{ in } S/J_q = S/(J + K)\}.$$

But this means that $a - b \in J + K$, i.e. $a - b = j + k$ for some $j \in J$ and $k \in K$. Therefore, $S/J \times_{(S/J_q)} S/K = \{(\bar{a}, \bar{a} - \bar{j}) \in S/J \times S/K \colon j \in J\}$ and simultaneously we must have that $S/J \times_{(S/J_q)} S/K = \{(\bar{b} + \bar{k}, \bar{b}) \in S/J \times S/K \colon k \in K\}$. This implies that

$$S/J \times_{(S/J_q)} S/K = \{(\bar{a}, \bar{b}) \in S/J \times S/K : a - b \text{ in } J \cap K\},$$

which is isomorphic to $S/(J \cap K)$ through the map

$$\begin{array}{ccc} S/J \times_{(S/J_q)} S/K & \longrightarrow & S/(J \cap K) \\ (a, b) & \longmapsto & a. \end{array}$$

Now, since the projection map $S/J \longrightarrow S(J\cap K)$ is surjective by $\mathbf{H_1}$ and Remark 2.4.7, we have

$$F(S/(J\cap K)) \simeq F(S/J \times_{(S/J_q)} S/K) \longrightarrow F(S/J) \times_{F(S/J_q)} F(S/K)$$

is surjective.
Using once again Yoneda's Leemma, we have

$$F(S/J) \times_{F(S/J_q)} F(S/K) = \{(\xi,\xi') \in \mathrm{Nat}(h_{S/K}, F) \times \mathrm{Nat}(h_{S/K}, F) \colon \xi \circ \pi_J = \xi' \circ \pi_K\},$$

where the composition with the projection maps is in the sense of the Diagram (2.1). However, since $J, K \in \mathcal{S}$, there exist ξ_J, ξ_K such that $\xi_J \circ \pi_J = \xi_q = \xi_K \circ \pi_K$, which means that $(\xi_J, \xi_K) \in F(S/J) \times_{F(S/J_q)} F(S/K)$. Then, thanks to the surjectivity of the map above there exists $\xi_{J\cap K} \in \mathrm{Nat}(h_{S/J\cap K}, F)$ such that $\xi_{J\cap K} \circ \pi_{J\cap K} = {\xi_q}^2$. Hence $J \cap S$ is also in $\mathcal{S}$. Let now J_{q+1} be the intersection of all ideals in $\mathcal{S}$ and let $R_{q+1} = S/J_{q+1}$ and ξ_{q+1} any lifting of ξ_q. Set $J = \cap_q J_q$, $R = S/J$, which is a complete local noetherian quotient of S (note that the properties of being local, noetherian and complete all pass to quotients). For every $q \in \mathbf{N}$, $m_S^q J_q \subseteq m_S J_q \subseteq J_q$. Then, since $\{(m_S^q J_q + J)/J \colon q \in \mathbf{N}\}$ is a fundamental system of neighborhood of the identity element of S/J, the set $\{J_q/J \colon q \in \mathbf{N}\}$ is a basis of the topology of $S/J = R$. Therefore, since R is a profinite ring (as quotient of a profinite ring), $R = \varprojlim_q (S/J)/(J_q/J) = \varprojlim_q S/J_q$. Hence, it makes sense to define $\xi = \varprojlim_q \xi_q$.
Notice then $t_F \simeq t_{R_2} \simeq t_R$, where the second isomorphism in given by the map

$$\mathrm{Hom}(R, k[\epsilon]) = \varprojlim_q \mathrm{Hom}(R_q, k[\epsilon]) \longrightarrow \mathrm{Hom}(R_2, k[\epsilon])$$

$$\varprojlim_q f_q \longmapsto f_2.$$

Hence, in order to show that R is a hull for F it is sufficient to prove that the map $\xi \colon h_R \longrightarrow F$ is smooth. Recalling Definition 2.4.8, it is enough to check that $h_R(A') \longrightarrow h_R(A) \times_{F(A)} F(A')$ is surjective for any small extension $p \colon A' \longrightarrow A$. Let us say $A = A'/I$, where I is the kernel of p. In other words, let $\eta \in F(A) \simeq \mathrm{Nat}(h_A, F)$ be the image of $\eta' \in F(A') \simeq \mathrm{Nat}(h_{A'}, F)$, $f \colon R \longrightarrow A$ taking ξ to η, we have to show that f lifts to $f' \colon R \longrightarrow A'$ taking ξ to η', in the sense that if

[2]Fixing a coefficient ring A then it is easy to check that $\mathrm{Hom}(S/(J\cap K), A) \simeq \mathrm{Hom}(S/J \times_{S/J_q} S/K, A) \simeq \mathrm{Hom}(S/J, A) \times_{\mathrm{Hom}(S/J_q, A)} \mathrm{Hom}(S/K, A)$ and then it is clear that $S/J \cap K$ lifts S/J_q.

$F(f)\colon F(R) \longrightarrow F(A)$ is such that $F(f)(\xi) = \eta$ then $F(f')\colon F(R) \longrightarrow F(A')$ satisfies $F(f')(\xi) = \eta'$.

It is time now to interpret condition $\mathbf{H_1}$. We have

$$\psi\colon A' \times_A A' \longrightarrow A' \times_k k[I], (x, y) \longmapsto (x, x_0 + y - x)$$

is an isomporphism, where $k[I]$ is the k-algebra $k \oplus I$ with $I^2 = 0$ and $x_0 = x \mod m_{A'} \in k$. In fact, this is obviously a bijection since $A' \times_A A' \simeq A' = \{(x, y) \in A' \times A'\colon \bar{x} = \bar{y} \in A/I\}$, which means that $y - x \in I$ and so

$$(x, x_0 + y - x) \in A' \times_k k[I] = \{(z, w) \in A'k[I]\colon \bar{z} = \bar{w} \in k\}.$$

We want now to check that it is a bijection of algebras. We have to show that if (a, b) and (c, d) are in $A' \times_A A'$ and $a = a_0, b = b_0 \mod m_{A'}$ then

$$(a, a_0 + b - a) \cdot (c, c_0 + d - c) = (ac, a_0c_0 + bd - ac),$$

which means we have to show that

$$bd - ac = a_0(d - c) + c_0(b - a) + (b - a)(d - c) \text{ in } k[I].$$

The trick is to prove that

$$a_0(d - c) + c_0(b - a) = a(d - c) + c(b - a),$$

which is true because $(a-a_0)(d-c)+(c-c_0)(b-a)$ is zero since $a-a_0$ and $b-b_0$ are in $m_{A'}$ and $d-c$ and $b-a$ are in $I = \ker(p)$ (recall that since p is a small extension whose kernel is I then $m_{A'}I = 0$ and so I can be seen as a k-vector space).
Now if $p\colon A' \longrightarrow A$ is a small extension and $\ker(p) = I = (x)$, then

$$k[I] \longrightarrow k[\epsilon] \otimes_k I,\ (a + bx) \longmapsto (a + b\epsilon) \otimes_k x$$

is an isomorphism. Therefore, since by hypothesis $F(k)$ is a singleton, we have by $\mathbf{H_2}$ that

$$F(A') \times (t_F \otimes_k I) \simeq F(A') \times_{F(k)} F(k[\epsilon]) \otimes_k I \simeq^3$$
$$F(A') \times_{F(k)} F(k[I]) \simeq F(A' \times_k k[I]) \simeq F(A' \times_A A') \longrightarrow F(A') \times_{F(A)} F(A'),$$

[3] Again we can see that $F(k[\epsilon]) \otimes_k I \simeq F(k[I])$.

where the last map is surjective if we assume $\mathbf{H_1}$ (respectively bijective if we assume $\mathbf{H_4}$). Therefore, composing with the projection on the second factor, we get the map

$$F(A') \times (t_F \otimes_k I) \longrightarrow F(A') \times_{F(A)} F(A') \longrightarrow F(A'),$$

which defines an action of $t_F \otimes_k I$ on $F(A')$. More precisely, for very $\eta \in F(A)$ there is an action of $t_F \otimes_k I$ on $F(p)^{-1}(\eta) \in F(A')$ (provided that subset is not empty). Hypothesis $\mathbf{H_1}$ implies that this action is transitive, while, if we assume $\mathbf{H_4}$, $F(p)^{-1}(\eta)$ is a principal homogeneous space[4].

Let us return now to the lifting problem. Recall that we need to lift the map $f\colon (R,\xi) \longrightarrow (A,\eta)$ to a map $f'\colon (R,\xi) \longrightarrow (A',\eta')$. We claim that it is sufficient to lift f to a map f' such that $p \circ f' = f$. Indeed, given such an f' we have

$$(F(p) \circ F(f'))(\xi) = F(f)(\xi) = \eta.$$

Therefore, $F(f')(\xi)$ is in the fiber of $F(p)^{-1}(\eta)$, which from the previous considerations equals the orbit of η' under $t_F \otimes I$. At the same time $t_F \otimes I$ also acts transitively on $h_R(p)^{-1}(f)$ which is thus the orbit of f'. In other words there exists $\sigma \in t_F \otimes I$ such that $\sigma[F(f')(\xi)] = \eta'$ and we can replace f' with $g' = \sigma \cdot f'$ to obtain

$$F(g')(\xi) = \eta' \text{ and } p \circ g' = f.$$

We have left to lift f to f'. Since $f\colon R \longrightarrow A$ and $R = \varprojlim_q R_q$, f must factor through R_q for some $q \in \mathbf{N}$. Therefore, if we consider the fiber product

$$\begin{array}{ccc} R_q \times_A A' & \longrightarrow & A' \\ \downarrow & & \downarrow p \\ R_q & \xrightarrow{f} & A, \end{array}$$

it is sufficient to complete the following diagram

$$\begin{array}{ccccc} \Lambda[[T_1,..,T_r]] & \xrightarrow{w} & R_q \times_A A' & \xrightarrow{pr_2} & A' \\ \downarrow & & \downarrow pr_1 & & \downarrow p \\ R_{q+1} & \xrightarrow{\pi_{q+1}} & R_q & \xrightarrow{f} & A \end{array}$$

[4]A non-empty set X is an homogeneous space for a group G if X is equipped with a transitive action of G and where the stabilizer subgroup of every point is trivial (meaning that for every $x, y \in X$ there exists a unique $g \in G$ such that $xg = y$).

by lifting to a map $h\colon R_{q+1} \longrightarrow R_q \times_A A'$. This way, thanks to the commutativity, we get a map $f' \coloneqq pr_2 \circ h$ such that $p \circ f' = f$.

Now either pr_1 has a section, in which case the lift is obvious, or pr_1 is essential[5], in which case w is surjective by definition. Now $\mathbf{H_1}$ implies the map $F(R_q \times_A A') \longrightarrow F(R_q) \times_{F(A)} F(A')$ is surjective, hence $\xi_q \in F(R_q)$ lifts back to $F(R_q \times_A A')$. This implies $J_{q+1} \subseteq \ker(w)$ by minimality of J_{q+1}, hence w factors through R_{q+1}, which completes the proof of smoothness. Hence (R, ξ) is a hull.

Finally, under $\mathbf{H_4}$, we prove that $h_R(A) \longrightarrow F(A)$ is an isomorphism by induction on the length of A. Suppose it's true for A and let $p\colon A' \longrightarrow A = A'/I$ be a small map. Let $\eta \in F(A)$. Now $h_R(p)^{-1}(f)$ and $F(p)^{-1}(\eta)$ are principal homogeneous spaces under $t_F \otimes_k I$. This implies $h_R(A) \longrightarrow F(A)$ is injective since for every $\eta \in F(A)$ there is a unique $\sigma \in t_F \otimes_k I$ such that $\sigma[F(f)](\xi) = \eta$, i.e there is a unique $g = \sigma \cdot f$ such that $F(g)(\xi) = \eta$. Moreover, $h_R(A') \longrightarrow F(A')$ is surjective since $h_R \longrightarrow F$ is smooth, and it follows that $h_R(A') \longrightarrow F(A')$ is bijective, which completes the proof. □

2.4.1 Relatively representable functors

Given a functor $F\colon \mathcal{C}_\Lambda \longrightarrow$ Sets, let us now consider a subfunctor $\mathcal{F} \subseteq F$ such that $\mathcal{F}(A) \subseteq F(A)$ for every object A and $\mathcal{F}(k) = F(k)$ is a singleton. We would like to apply Schlessinger's criterion to $\mathcal{F}$. We need firstly the following definitions.

Definition 2.4.11. In any category where fiber products exist a commutative diagram of the form

$$\begin{array}{ccc} D & \longrightarrow & B \\ \downarrow & & \downarrow \\ A & \longrightarrow & C \end{array}$$

is *cartesian* if the induced map $D \longrightarrow A \times_C B$ is an isomorphism.

Definition 2.4.12. The subfunctor $\mathcal{F}$ is *relatively representable* if for all the diagrams in $\mathcal{C}_\Lambda$ of the form

$$\begin{array}{ccc} A \times_C B & \xrightarrow{q} & B \\ \downarrow{\scriptstyle p} & & \downarrow{\scriptstyle g} \\ A & \xrightarrow{f} & C \end{array}$$

[5]The map $p : B \longrightarrow A$ is essential if for very $q\colon C \longrightarrow B$ surjectivity of $p \circ q$ implies surjectivity of q.

the square

$$\begin{array}{ccc} \mathcal{F}(A \times_C B) & \xrightarrow{\tilde{\Phi}_{A\times_C B}} & \mathcal{F}(A) \times_{\mathcal{F}(C)} \mathcal{F}(B) \\ \downarrow\subseteq & & \downarrow\subseteq \\ F(A \times_C B) & \xrightarrow{\Phi_{A\times_C B}} & F(A) \times_{F(C)} F(B) \end{array}$$

is Cartesian.

$\mathcal{F}$ is said *relatively representable* because in a certain sense its representability depends on the representability of the "main" functor F. Indeed, if F satisfies condition $\mathbf{H_1}, \mathbf{H_2}, \mathbf{H_3}, \mathbf{H_4}$ so does $\mathcal{F}$. In the same way, if F satisfies the tangent space hypothesis so does $\mathcal{F}$ and so $\mathcal{F}$ is nearly representable if so is F. This comes directly from the definition we gave above of relatively representable because

- the injectivity of the upper horizontal map just depends on the injectivity of the lower horizontal map thanks to the commutativity of the diagram. Indeed, $\tilde{\Phi}_{A\times_C B}$ is just the restriction of $\Phi_{A\times_C B}$ to $\mathcal{F}(A \times_C B)$ and so it is injective in and only if so is $\tilde{\Phi}_{A\times_C B}$;
- the surjectivity of the upper horizontal map depends on the fact the diagram is cartesian. Indeed, considered any cartesian diagram in the category of set of the form

$$\begin{array}{ccc} D & \xrightarrow{h} & B \\ \downarrow & & \downarrow \\ A & \xrightarrow{h} & C, \end{array}$$

  we have that

$$D \simeq A \times_C B = \{(a, b) \in A \times_C B : h(a) = b\} = \{(a, h(a)) \in A \times B\}$$

  Then if the map h is surjective, then $D \simeq h^{-1}(B) \times B$ and then the upper horizontal map is just the canonical projection and so it is surjective.

Therefore, if $\mathcal{F}$ is relatively representable, $\tilde{\Phi}_{A\times_C B}$ is bijective if $\Phi_{A\times_C B}$ is so. Moreover, since $t_{\mathcal{F}} = \mathcal{F}(k[\epsilon]) \subseteq F(k[\epsilon]) = t_F$, if t_F is a finite dimensional vector space over k then so is $t_{\mathcal{F}}$.

Remark 2.4.13. Assumed that F is pro-representable and that $\mathcal{R}_F$ is its representation ring, one could wonder if there is a relation between this ring and the ring that represents $\mathcal{F}$. It turns out that $\mathcal{F}$ is represented by a quotient Λ-algebra $\mathcal{R}_{\mathcal{F}}$ of $\mathcal{R}_F$. This is a consequence of the following lemma.

Lemma 2.4.14. *Let $\mathcal{R}$ be a coefficient Λ-algebra and let $h_{\mathcal{R}}\colon \mathcal{C}_\Lambda \longrightarrow$ Sets the covariant functor represented by $\mathcal{R}$. Let $\varphi\colon R_1 \longrightarrow R_2$ be a homomorphism of coefficients Λ-algebras and denote by φ again the natural transformation of functors on $\mathcal{C}_\Lambda$ which is induced by φ, $\varphi\colon h_{R_2} \longrightarrow h_{R_1}$. Then the following properties are equivalent*

1. *the ring homomorphism $\varphi\colon R_1 \longrightarrow R_2$ is surjective;*
2. *the natural transformation $\varphi\colon h_{R_2} \longrightarrow h_{R_1}$ is injective[6], i.e. we may identify h_{R_2} as a subfunctor of h_{R_1}.*

Proof. Since for every object A of $\mathcal{C}_\Lambda$, the functor $\mathrm{Hom}(-, A)$ is controvariant and left-exact, if $\varphi\colon R_1 \longrightarrow R_2$ is surjective then $\mathrm{Hom}(R_1, A) \longrightarrow \mathrm{Hom}(R_2, A)$ is injective. Hence, 1. implies 2.. To prove that 2. implies 1. note that since φ is a homomorphsim of coefficient Λ-algebras it induces the identity on residue fields. Since R_i are complete, noetherian, local rings then it is sufficient that $\varphi\colon R_2 \longrightarrow R_1$ is surjective on the Zariski cotangent spaces $t^*_{R_1}$ and $t^*_{R_2}$[7]. But, thanks again to the controvariant left-exact functor $\mathrm{Hom}(-, k)$, we must show dually that the map induced by φ

$$\mathrm{Hom}(t^*_{R_1}, k) \longrightarrow \mathrm{Hom}(t^*_{R_2}, k)$$

is injective. By Proposition, 2.3.10, this is equivalent to check that the map $\varphi\colon h_{R_2}(k[\epsilon]) \longrightarrow h_{R_1}(k[\epsilon])$ is injective, which is by 2.. □

Therefore, assuming that F and $\mathcal{F}$ are both pro-representable, since $\mathcal{F}$ is a subfunctor of F, there in an injective natural transformation between them. Then, for the lemma above, there is a surjective map $\varphi\colon \mathcal{R}_F \longrightarrow \mathcal{R}_{\mathcal{F}}$, which means, by the First Isomorphism Theorem, that $\mathcal{R}_{\mathcal{F}} \simeq \mathcal{R}_F/\ker(\varphi)$.

Remark 2.4.15. It's worth explaining why, if R_1 and R_2 are objects of $\mathcal{C}_\Lambda$, an homomorphism $\varphi\colon R_1 \longrightarrow R_2$ is surjective if and only if it is surjective on the corrispondent Zariski tangent space. We can state the following lemma.

Lemma 2.4.16. *Let $f\colon A \longrightarrow B$ a morphism in $\mathcal{C}_\Lambda$. The following are equivalent.*

(1) *f is surjective;*

(2) *$m_A/m_A^2 \longrightarrow m_B/m_B^2$ is surjective;*

(3) *$m_A/(m_A^2, m_\Lambda A) \longrightarrow m_B/(m_B^2, m_\Lambda B)$ is surjective.*

[6] A natural transformation in injective if and only if each component in injective.

[7] For the definition of Zariski cotangent space see Definition 2.3.8.

Proof. Let us show that (**1**) $\Longrightarrow$ (**2**). Assume that f is surjective. Since f is a ring coefficient homomorphism, we have $f(m_A) \subseteq m_B$. Let $y \in m_B$ and $x \in A$ such that $f(x) = y$. Moreover, we know that f induces an isomorphism $A/m_A \longrightarrow B/m_B$, which means that $x \in m_A$. Hence the induced map $m_A/m_A^2 \longrightarrow m_B/m_B^2$ is surjective. It is clear that (**2**) $\Longrightarrow$ (**3**). Let us now show that (**3**) $\Longrightarrow$ (**2**). The map f gives rise to a canonical commutative diagram

$$\begin{array}{ccccccc} (m_\Lambda A + m_A^2)/m_A^2 & \longrightarrow & m_A/m_A^2 & \longrightarrow & m_A/(m_\Lambda A, m_A^2) & \longrightarrow & 0 \\ \downarrow & & \downarrow & & \downarrow & & \\ (m_\Lambda B + m_B^2)/m_B^2 & \longrightarrow & m_B/m_B^2 & \longrightarrow & m_B/(m_\Lambda B, m_B^2) & \longrightarrow & 0 \end{array}$$

with exact rows. Hence, if (**3**) holds so does (**2**). We have left to prove (**2**) $\Longrightarrow$ (**1**). Let us then assume (**2**). By one of the equivalent formulations of Nakayama's Lemma, it is sufficient to show that $A/m_A \longrightarrow B/m_AB$ is surjective. But since $k = A/m_A = B/m_B$, then it suffices to show that $m_AB \longrightarrow m_B$ is surjective. Indeed, this way we'd get $B/m_AB \simeq B/m_B$ and hence $A/m_A \longrightarrow B/m_AB \simeq B/m_B$ would be bijective. Applying Nakayama's Lemma once more it is sufficient to show that $m_AB/(m_ABm_B) \longrightarrow m_B/m_B^2$ is surjective. But since (**2**) holds and we have the following factorization

$$m_A/m_A^2 \longrightarrow m_AB/(m_ABm_B) \longrightarrow m_B/m_B^2,$$

$m_AB/(m_ABm_B) \longrightarrow m_B/m_B^2$ must be surjective. □

2.5 Existence of the universal deformation

2.5.1 Mazur–Ramakrishna's Theorem

In this section we will apply Schlessinger's criterion to the deformation functor introduced above

$$D_\Lambda \colon \mathcal{C}_\Lambda \longrightarrow \text{Sets}$$

given by

$$D_\Lambda(A) = \{\text{deformations of } \bar{\rho} \text{ to } A\}$$

where

$$\bar{\rho} \colon \Pi \longrightarrow \mathrm{GL}_n(k)$$

is a fixed residual representation with Π a profinite group satisfying the p-finitness condition (see Definition 1.4.5) and k a finite field of characteristic p. Before stating the main theorem of this section which will prove that D^0_Λ is pro-representable we need some definitions.

Definition 2.5.1. Let $\bar{\rho}$ be a fixed residual representation. Then we define

$$C(\bar{\rho}) = \mathrm{Hom}_\Pi(k^n, k^n) \simeq \{P \in \mathrm{M}_n(k) \colon P\bar{\rho}(g) = \bar{\rho}(g)P \quad \forall g \in \Pi\}.$$

Definition 2.5.2. Let $\bar{\rho}$ be a fixed residual representation and let ρ be a deformation of $\bar{\rho}$ to a coefficient Λ-algebra. We define

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

Remark 2.5.3. In particular $C(\bar{\rho}) = C_k(\rho)$.

We can now state the theorem.

Theorem 2.5.4 (Mazur, Ramakrishna)**.** *Suppose Π is a profinite group that satisfies the p-finiteness condition Φ_p, $\bar{\rho}\colon \Pi \longrightarrow \mathrm{GL}_n(k)$ is a continuous residual representation and Λ is a complete Noetherian local ring with residue field k. Then the deformation functor D_Λ always satisfies properties $\mathbf{H_1}, \mathbf{H_2}$ and $\mathbf{H_3}$. Moreover, if $C(\bar{\rho}) = \{\lambda\,\mathrm{id}_n \colon \lambda \in k\}$, then D_Λ also satisfies property $\mathbf{H_4}$.*

We will prove the theorem above in different steps, but before exposing the proof it is worth talking a little bit about the last hypothesis of the theorem, i.e. $C(\rho) = \{\lambda\,\mathrm{id}_n \colon \lambda \in k\}$. In order to do this, let us give the following definition.

Definition 2.5.5. A representation $\bar{\rho}\colon \Pi \longrightarrow \mathrm{GL}_n(k)$ is called *reducible* if the representation space k^n has a proper subspace that is invariant under the action of $\bar{\rho}$. It is called *irreducible* if no such subspace exists. Finally $\bar{\rho}$ is said to be *absolutely irreducible* if there is no extension k'/k such that $\bar{\rho} \otimes k'$ is reducible.

Remark 2.5.6. $\bar{\rho} \otimes_k k'\colon \Pi \longrightarrow \mathrm{GL}_n(k')$ is the representation obtained by $\bar{\rho}$ extending the scalars and considering $(k')^n$ with the action of $\bar{\rho}$ on the first factor of $(k^n \otimes_k k') \simeq (k \otimes_k k')^n \simeq (k')^n$. Therefore, $\bar{\rho}$ and $\bar{\rho} \otimes_k k'$ are essentially the same representation viewing $\mathrm{GL}_n(k) \subseteq \mathrm{GL}_n(k')$. If we then choose $k' = \bar{k}$ the algebraic closure of k and $\bar{\rho}$ is absolutely irreducible then $\bar{\rho}$ is irreducible when we extends the scalar to $\bar{k}$.

Then the following lemma holds.

Lemma 2.5.7 (Schur's lemma)**.** *If $\bar{\rho}\colon \Pi \longrightarrow \mathrm{GL}_n(k)$ is absolutely irreducible then $C(\bar{\rho}) = \{\lambda\,\mathrm{id}_n \colon \lambda \in k\}$.*

Proof. First of all let us consider $\bar{k}$ a fixed algebraic closure of k. Then since $\bar{\rho}$ is absolutely irreducible, $\bar{\rho} \otimes_k \bar{k}$ is irreducible. Despite the little abuse of notation, let us call $\bar{\rho} \otimes_k \bar{k}$ again $\bar{\rho}$. Let us now take $P \in \mathrm{M}_n(\bar{k})$ such that $P\bar{\rho}(g) = \bar{\rho}(g)P$ for all $g \in G$. Then, since $\bar{k}$ is algebraically closed, P has an eigenvalue $\lambda \in \bar{k}$. If we consider the matrix $P - \lambda \,\mathrm{id}_n$ and the endomorphism Φ associated with this matrix, then $\Phi \in C(\bar{\rho})$ is not injective. But since $\bar{\rho}$ is irreducible and $\ker(\Phi)$ is stable under the action of $\bar{\rho}$, we must have $\ker(\Phi) = \bar{k}^n$, i.e. $P = \lambda \,\mathrm{id}_n$ for some $\lambda \in \bar{k}$. □

2.5.2 Proof of Mazur–Ramakrishna's Theorem

We will now prove Mazur–Ramakrishna's theorem in different steps. Note first of all that if R_0, R_1, R_2 are artinian coefficient Λ-algebras and $\Phi_1 \colon R_1 \longrightarrow R_0$, $\Phi_2 \colon R_2 \longrightarrow R_0$ are coefficient homomorphisms, then for every $i = 1, 2, 3$, $\Gamma_n(R_i)$ (defined in Remark 2.2.2) acts by conjugation on $E_i = \mathrm{Hom}_{\bar{\rho}}(\Pi, \mathrm{GL}_n(R_i))$, the set of homomorphism that reduce to $\bar{\rho}$ when going modulo m_{R_i}. From Definition 2.2.8 of the deformation functor

$$D_\Lambda(R_i) = E_i/\Gamma_n(R_i),$$

where we denote by $E_i/\Gamma_n(R_i)$ the set of equivalence classes of the representations in E_i determined by the conjugacy action of $\Gamma_n(R_i)$ (see Definition 2.2.3).

Remark 2.5.8. If A, B are coefficient rings and $f : A \longrightarrow B$ is surjective, then the induced map $\tilde{f} : \Gamma_n(A) \longrightarrow \Gamma_n(B)$ is well defined and surjective. In fact, the following diagram

$$\begin{array}{ccc} \mathrm{GL}_n(A) & \xrightarrow{\pi_A} & \mathrm{GL}_n(A/m_A) \\ \big\downarrow f & & \big\downarrow g \\ \mathrm{GL}_n(B) & \xrightarrow{\pi_B} & \mathrm{GL}_n(B/m_B) \end{array}$$

commutes and so if $P \in \Gamma_n(A) = \ker(\pi_A)$ then $(\pi_B \circ f)(P) = \pi_A(P) = \mathrm{id}_{A/m_A}$ because g is an isomorphism and so $f(P) \in \Gamma_n(B)$. Moreover $\tilde{f}$ is surjective. Indeed, if $Q \in \Gamma_n(B)$, then since f is surjective there exists $P \in \mathrm{GL}_n(A)$ such that $f(P) = Q$. Then $P \in \Gamma_n(A)$ because $\pi_A(P) = g^{-1}(\pi_B(f(P))) = g^{-1}(\pi_B(Q)) = \mathrm{id}_{A/m_A}$.

Recalling the map

$$\Phi_{R_1 \times_{R_0} R_2} \colon E_3/\Gamma_n(R_3) \longrightarrow E_1/\Gamma_n(R_1) \times_{E_0/\Gamma_n(R_0)} E_2/\Gamma_n(R_2),$$

where $R_3 = R_1 \times_{R_0} R_2$. we are now ready to start the prove of the theorem.

Lemma 2.5.9. *D_Λ satisfies property* $\mathbf{H_1}$.

Proof. Let us consider the following diagram:

$$\begin{array}{ccc} R_1 \times_{R_0} R_2 & \xrightarrow{q} & R_2 \\ \downarrow{\scriptstyle p} & & \downarrow{\scriptstyle g} \\ R_1 & \xrightarrow{f} & R_0 \end{array}$$

and suppose that the map $g\colon R_2 \longrightarrow R_0$ is small. We want to prove that if we have a pair (ρ_1, ρ_2) of deformations to R_1 and R_2 respectively which induce the same representation to R_0, we can paste them together to get a deformation of $R_1 \times_{R_0} R_2 = R_3$. This is clear for homomorphism, i.e. for elements of E_i but we need to check we can pick representatives for the strict equivalence classes so that they match when projected down to R_0. Let us then pick any two representatives ϕ_1 and ϕ_2 of ρ_1 and ρ_2 respectively. Since they are equivalent when projected down to R_0, there exists a matrix $\bar{M} \in \Gamma_n(R_0)$ such that $\bar{\phi_1} = \bar{M}^{-1}\bar{\phi_2}\bar{M}$. But since the map g is surjective, so is the induced map $\Gamma_n(R_2) \longrightarrow \Gamma_n(R_0)$. Therefore, we can lift $\bar{M}$ to $M \in \Gamma_n(R_2)$. Then ϕ_1 and $M^{-1}\phi_2 M$ have the same image in $\mathrm{GL}_n(R_0)$ and so they define an homomrphism $\phi_3 \in E_3$. The strict equivalence class of ϕ_3 maps to (ρ_1, ρ_2) and so $\Phi_{R_1 \times_{R_0} R_2}$ is surjective. □

We want now to understand when the map $\Phi_{R_1 \times_{R_0} R_2}$ is injective. In order to do this we need the following two lemmas.
Let $\phi_2 \in E_2$ and let $\phi_0 \in E_0$ be its image through the composition with the homomorphism $R_2 \longrightarrow R_0$. Then we can define

$$G_i(\phi_i) = \{P \in \Gamma_n(R_i)\colon P \text{ commutes with the image of } \phi_i \text{ in } \mathrm{GL}_n(R_i)\}.$$

Lemma 2.5.10. *If for all $\phi_2 \in E_2$ the map*

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

is surjective then the map $\Phi_{R_1 \times_{R_0} R_2}$ is injective.

Proof. Suppose ϕ and ψ are elements of E_3 that induce elements ϕ_i and ψ_i in E_i for every $i = 0, 1, 2$. If ϕ and ψ have the same imagine under $\Phi_{R_1 \times_{R_0} R_2}$, for every $i = 1, 2$ there is a matrix $M_i \in \Gamma_n(R_i)$ such that $\phi_i = M_i \psi_i M_i^{-1}$. Mapping down to E_0 we have

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

and so $\bar{M}_2 \bar{M}_1{}^{-1}$ commutes with the image of ϕ_0, i.e. $\bar{M}_2 \bar{M}_1{}^{-1} \in G_0(\phi_0)$. Thanks to the surjectivity we know that there exists $N \in G_2(\phi_2)$ which maps to $\bar{M}_2 \bar{M}_1{}^{-1}$. Let now, $N_2 = N^{-1} M_2$. We have

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

Moreover the image of N_2 in $\Gamma_n(R_0)$ is:

$$\bar{N_2} = (\bar{M_2}\bar{M_1}^{-1})^{-1}\bar{M_2} = \bar{M_1}.$$

Since M_1 and N_2 have the same image in $\Gamma_n(R_0)$, the pair (M_1, N_2) defines an element $M \in \Gamma_n(R_3)$ and we have $M\psi M^{-1} = \phi$. Thus ψ and ϕ are strictly equivalent and the lemma is proved. □

We can then state the following lemma.

Lemma 2.5.11. *D_Λ satisfies hypothesis* $\mathbf{H_2}$.

Proof. Set $R_0 = k$ and $R_2 = k[\epsilon]$. Since the reduction $k[\epsilon] \longrightarrow k$ is small, by Lemma 2.5.9 the map $\Phi_{R_1 \times_{R_0} R_2}$ is surjective. Injectivity will the follow if we know that the map $G_2(\phi_2) \longrightarrow G_0(\phi_0)$ is always surjective. But when $R_0 = k$, $\Gamma_n(R_0)$ consists only of the identity matrix and consists only of identity matrix. So surjectivity holds and the thesis is proved. □

Before proving hypothesis $\mathbf{H_3}$ we need the following definition.

Definition 2.5.12. An *abelian elementary group* is an abelian group in which all elements have the same order,which is a prime number.

Remark 2.5.13. An abelian elementar group of order p is a $(\mathbf{Z}/p\mathbf{Z})$-vector space.

Remark 2.5.14. If k is a finite field of characteristic p, then $\Gamma_n(k[\epsilon])$ is a finite p-elementar abelian group. Indeed, $\Gamma_n(k[\epsilon]) = \mathrm{id}_k + \epsilon\, \mathrm{M}_n(k)$, where id_k is the identity matrix in $\mathrm{M}_n(k)$. Then, since for every $M \in \mathrm{M}_n(k)$, using the binomial expansion and considering that k has characteristic p, $(\mathrm{id}_k + \epsilon M)^p = \mathrm{id}_k + \epsilon M$, every element in $\Gamma_n(k[\epsilon])$ has order p.

We are now ready for the following lemma.

Lemma 2.5.15. *D_Λ satisfies hypothesis* $\mathbf{H_3}$.

Proof. Let $\Pi_0 = \ker(\bar{\rho})$ and let ρ be a lift or $\bar{\rho}$ to $k[\epsilon]$. If $x \in \Pi_0$ then we have $\bar{\rho}(x) = \mathrm{id}_k$ and so $\rho(x) \in \Gamma_n(k[\epsilon])$. Hence ρ determines a map from Π_0 to $\Gamma_n(k[\epsilon])$. Moreover, two lifts that determine the same map must be identical. Indeed, if ρ and ρ' are two lifts that coincide on Π_0, since we have the following factorizations

$$\Pi/\Pi_0 \longrightarrow \rho(\Pi)/\rho(\Pi_0) \simeq \bar{\rho}(\Pi)$$

$$\Pi/\Pi_0 \longrightarrow \rho'(\Pi)/\rho'(\Pi_0) = \rho'(\Pi)/\rho(\Pi_0) \simeq \bar{\rho}(\Pi),$$

then $\rho(\Pi) \simeq \rho'(\Pi)$, i.e. they are equivalent representation.

Since Π is profinite and Π_0 is closed and of finite order, Π_0 is open. Moreover, as we said above $\Gamma_n(k[\epsilon])$ is a finite p-elementary abelian group and hence it is a $(\mathbf{Z}/p\mathbf{Z})$-vector space. By the p-finiteness condition Φ_p, there are many finitely maps from Π_0 to $\Gamma_n(k[\epsilon])$. Hence $D_\Lambda(k[\epsilon])$ is a finite set because, as we just proved, two lifts that determine the same map from from Π_0 to $\Gamma_n(k[\epsilon])$ must be equivalent. □

Remark 2.5.16. This proof relies on the fact that the residue field k is finite. Indeed, if we consider a field k of characteristic p which is a finitely dimensional $(\mathbf{Z}/p\mathbf{Z})$-vector space, then so is $\Gamma_n(k[\epsilon])$. Then if $d = \dim_k(\Gamma_n(k[\epsilon]))$, $\Gamma_n(k[\epsilon]) \simeq (\mathbf{Z}/p\mathbf{Z})^{\oplus d}$ and $\mathrm{Hom}_{\mathrm{cont}}(\Pi_0, \Gamma_n(k[\epsilon])) \simeq \mathrm{Hom}_{\mathrm{cont}}(\Pi_0, (\mathbf{Z}/(p\mathbf{Z}))^{\oplus d}) \simeq (\mathrm{Hom}_{\mathrm{cont}}(\Pi_0, \mathbf{Z}/p\mathbf{Z}))^{\oplus d}$. Then, thanks to the p-finiteness condition $\mathrm{Hom}_{\mathrm{cont}}(\Pi_0, \Gamma_n(k[\epsilon]))$ is finite.

We have left to prove the last part of Mazur–Ramakrishna theorem. However, we need first the following lemma.

Remark 2.5.17. By a little abuse of notation we will say that $C(\bar{\rho}) = k$ when $C(\bar{\rho}) = \{\lambda \,\mathrm{id}_k \colon \lambda \in k\}$ to ease the notation.

Lemma 2.5.18. *If $C(\bar{\rho}) = k$, then for every $i = 0, 1, 2$ we have $G_i(\phi_i) \subseteq R_i$, i.e. $G_i(\phi_i)$ consists only of scalar matrices in $\Gamma_n(R_i)$.*

Proof. We will prove the stronger assertion that for any deformation ρ of $\bar{\rho}$ to an artinian coefficient ring A we have $C_A(\rho) = A$.
Since $A \longrightarrow k$ is surjective, by Remark 2.4.3 it factors through a sequence of small extensions. We know that $C(\bar{\rho}) = k$ by assumption. It is then sufficient to prove the alternative claim: if $A \longrightarrow B$ is a coefficient ring small homomorphism and $C_B(\rho_B) = B$ then $C_A(\rho_A) = A$, where ρ_B is the representation induced by the map $A \longrightarrow B$. Let $c \in C_A(\rho_A)$. Then by assumption the image of $c \in C_B(\rho_B)$ is a scalar matrix (note that if $C \in \mathrm{M}_n(A)$ commutes with ρ_A and $f \colon A \longrightarrow B$ then $f(c)$ commutes with ρ_B). Suppose $c \longmapsto \bar{r}$, where the scalar $\bar{r} \in B$ is the image of $r \in A$. Then we can write $c = r\,\mathrm{id} + tM$, where t is a generator of the kernel of $A \longrightarrow B$ (recall that the kernel is a principal ideal for the small assumption) and $M \in \mathrm{M}_n(A)$. Since c commutes with ρ_A we have that for every $g \in \Pi$

$$(r\,\mathrm{id} + tM)\rho_A(g) = \rho_A(g)(r\,\mathrm{id} + tM).$$

Since scalars commute with everything we have

$$M\rho_A(g) = \rho_A(g)M.$$

Reducing modulo m_A and using the hypothesis $C(\bar{\rho}) = k$ then we see that M must be of the form $M = s\,\mathrm{id} + M_1$, where $s \in A$ and $M_1 \in \mathrm{M}_n(m_A)$. But since the map $A \longrightarrow B$ is small, we know that $tm_A = 0$ and so $tM_1 = 0$. Therefore

$$c = r\,\mathrm{id} + tM = r\,\mathrm{id} + t(s\,\mathrm{id} + M_1) = (r + ts)\,\mathrm{id}$$

and the thesis is proved. □

We are now ready to state the following lemma which prove the last part of Mazur–Ramakrishna's theorem.

Lemma 2.5.19. *Suppose $C(\bar{\rho}) = k$. Then property* $\mathbf{H_4}$ *is true.*

Proof. From the previous lemma we know that for every $i = 0, 1, 2$, $G_i(\phi_i)$ consists only of scalar matrices in $\Gamma_n(R_i)$. Indeed, $G_i(\phi_i) \simeq 1 + m_{R_i}$. Then for $i = 1, 2$, since by the hypothesis of $\mathbf{H_4}$ $R_i \longrightarrow R_0$ is small we have that the map $1 + m_{R_i} \simeq G_i(\phi_i) \longrightarrow G_0(\phi_0) \simeq 1 + m_{R_0}$ is surjective. Then combining Lemma 2.5.9 and Lemma 2.5.10 the thesis follows. □

We have finally proved that if Π is a profinite group satisfying the p-finiteness condition Φ_p and

$$\bar{\rho}\colon \Pi \longrightarrow \mathrm{GL}_n(k)$$

is a continuous residual representation such that $C(\bar{\rho}) = k$, then there exists a ring $\mathcal{R} = \mathcal{R}(\Pi, k, \bar{\rho}) \in \mathcal{C}_\Lambda$ and a deformation ρ of $\bar{\rho}$ to $\mathcal{R}$

$$\rho_{\mathcal{R}}\colon \Pi \longrightarrow \mathrm{GL}_n(\mathcal{R})$$

such that any deformation of $\bar{\rho}$ to a coefficient Λ-algebra A is obtained by $\rho_{\mathcal{R}}$ by a unique morphism $\mathcal{R} \longrightarrow A$. More precisely, for every coefficient Λ-algebra A and every lift $\rho\colon \Pi \longrightarrow \mathrm{GL}_n(A)$ of $\bar{\rho}$, there exists a unique coefficient Λ-algebra homomorphism $h\colon \mathcal{R} \longrightarrow A$ such that $\rho = h \circ \rho_{\mathcal{R}}$.

Definition 2.5.20. We call $\mathcal{R}$ the *universal deformation ring* and $\rho_{\mathcal{R}}$ the *universal deformation* of $\bar{\rho}$.

The ring $\mathcal{R} = \mathcal{R}(\Pi, k, \bar{\rho})$ is unique in the followimg sense.

Theorem 2.5.21 (Mazur)**.** *Suppose*

$$\bar{\rho}\colon \Pi \longrightarrow \mathrm{GL}_n(k)$$

is a continuous residual representation such that $C(\bar{\rho}) = k$. If $\bar{\rho}'$ is a representation equivalent to $\bar{\rho} \otimes \chi$, for some character χ, then there is an isomorphism

$$r(\bar{\rho}', \bar{\rho}) \colon \mathcal{R}(\Pi, k, \bar{\rho}) \longrightarrow \mathcal{R}(\Pi, k, \bar{\rho}')$$

mapping the universal deformation of $\bar{\rho}$ to the universal deformation of $\bar{\rho}'$.

Proof. See [5, Theorem 3.11]. □

Chapter 3

Properties of the universal deformation and Galois representations

In the previous chapter, we proved that under certain precise conditions universal deformations exist. The aim of this chapter will be to study the properties of the universal deformation ring. In order to be consistent with the previous sections we'll continue to use the same notation. In particular, Π will be a profinite group satisfying the p-finiteness condition Φ_p. We will more and more think of Π as being either $G_{K,S}$ (defined in Subsection 1.4.2) for some number field K and some set of primes S including the archimedean primes or the absolute Galois group of a number field.

Introducing the powerful tool of Galois cohomology, we will prove a very interesting result: the universal deformation ring $\mathcal{R}$ is simply a quotient of a power series ring. Moreover, if the deformation problem is 'unobstructed', the universal deformation ring is precisely a power series ring over a fixed coefficient ring Λ. Finally, when $\Pi = G_{\mathbf{Q},S}$ and $k = \mathbf{F}_p$ and certain conditions are satisfied, R can be proved to be isomorphic to $\mathbf{Z}_p[[T_1, T_2, T_3]]$, i.e. a power series ring of just three variables.

3.1 Tangent spaces and cohomology groups

In this section we will express the tangent space of the deformation functor in terms of cohomology groups. In order to do that, we need first to review the following definitions.

Definition 3.1.1. Let G be a group and A an abelian group endowed with an action φ of G by automorphisms, i.e. a group homomorphism $\varphi\colon G \longrightarrow \mathrm{Aut}(A)$ where $\mathrm{Aut}(A)$ is the automorphism group of A. Then, if we suppress φ and indicate its action by $\cdot$ we have the following definitions.

- A *1-cocycle of G in A* is a function $f\colon G \longrightarrow A$ satisfying
$$f(gh) = f(g) + g \cdot f(h).$$
- A *1-coboundary* is a function $f\colon G \longrightarrow A$ such that there exists $a \in A$ such that for all $g \in G$
$$f(g) = g \cdot a - a.$$

Remark 3.1.2. Both 1-cocycles and 1-coboundaries form an abelian group under pointwise addition of functions. Moreover, it is easy to check that 1-coboundaries are 1-cocycles. It is then natural to give the following definition.

Definition 3.1.3. The *first cohomology group of G on A*, which we denote by $H^1(G, A)$, is the quotient of the group of 1-cocycles by the subgroups of 1-coboundaries.

Let us now go back to the study of our deformation functor fixing a residual representation $\bar{\rho}\colon \Pi \longrightarrow \mathrm{GL}_n(k)$ such that $C(\bar{\rho}) = k$ and a coeffiecient ring Λ. From Theorem 2.5.4 we know that the functor $D = D_{\bar{\rho},\Lambda}$ is representable by a coefficient ring $\mathcal{R}$. Recalling the definition of the tangent space t_D of D, namely $t_D = D(k[\epsilon])$, thanks to the representability of D and Proposition 2.3.10, we have

$$t_D = D(k[\epsilon]) = \mathrm{Hom}_\Lambda(\mathcal{R}, k[\epsilon]) = \mathrm{Hom}_k(m_\mathcal{R}/(m_\mathcal{R}^2, m_\Lambda), k) = t_F.$$

Let $g \in \Pi$. Suppose that $\bar{\rho}(g) = a$ for some $a \in \mathrm{GL}_n(k)$ and that ρ_1 is a deformation of $\bar{\rho}$ to $k[\epsilon]$. Then we must have $\rho_1(g) = a + b_g\epsilon$ for some matrix $b_g \in \mathrm{M}_n(k)$. In other words ρ_1 determines and it is determined by a map $b\colon \Pi \longrightarrow \mathrm{GL}_n(k)$ sending g to the matrix b_g. Imposing the condition that ρ_1 must be an homomorphism, up to left multiplication for ρ_1^{-1}, we have that the map

$$\Pi \longrightarrow \mathrm{M}_n(k)$$

$$g \longmapsto b_g$$

is a 1-cocycle, where the action of Π on $\mathrm{M}_n(k)$ is via conjugation, i.e.

$$g \cdot b_g = \bar{\rho}(g) b_g \bar{\rho}(g)^{-1}.$$

We are now ready for the following definition.

Definition 3.1.4. The k-vector space $\mathrm{M}_n(k)$ with the conjugation of Π is called *the adjoint representation* of $\bar{\rho}$ and we denote it by $Ad(\bar{\rho})$.

One can check that the association defined above, i.e.

$$t_D \longrightarrow H^1(\Pi, Ad(\bar{\rho}))$$

$$\rho_1 \longmapsto b$$

is an isomorphism and in particular cocycles corresponding to stricly equivalent lifts differ by a coboundary. Moreover, it is not difficult to prove that the map above is not just a group isomorphism but is an isomorphisms of k-vector spaces. This gives a powerful result. Indeed, if we denote by $d_1 = \dim_k H^1(\Pi, Ad(\bar{\rho}))$, thanks to the isomorphism above we have that $d_1 = \dim_k(t_D)$. Consequently, we have that $d_1 = \dim_k(\mathrm{Hom}_k(m_{\mathcal{R}}/(m_{\mathcal{R}}^2, m_\Lambda), k)) = \dim_k(m_{\mathcal{R}}/(m_{\mathcal{R}}^2, m_\Lambda))$. Since $\mathcal{R}$ is a local and noetherian ring we can then apply Nakayama's lemma to conclude that $\mathcal{R}$ is a Λ-algebra generated by d_1 elements $\{r_1, ..., r_{d_1}\}$. That means that $\mathcal{R}$ is a quotient of a power series ring in d_1, variables over Λ, equivalently, there exists an exact sequence

$$0 \longrightarrow I \longrightarrow \Lambda[[X_1, ..., X_{d_1}]] \longrightarrow \mathcal{R} \longrightarrow 0,$$

where I is the kernel of the surjective Λ-algebra homomorphism

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

$$X_i \longmapsto r_i.$$

Then one possible approach to understand $\mathcal{R}$ is so try to determine the dimension d_1 and the ideal I.

3.2 Obstructed and unobstructed deformation problems

In this section we'll try to deepen the connection between deformation theory and cohomology introducing the concept of obstruction to the lifting of a homomorphism.

Suppose we have two rings R_1 and R_0 in $\mathcal{C}_\Lambda$ and a surjective Λ-algebras homomorphism $R_1 \longrightarrow R_0$ with kernel I satisfying $I \cdot m_{R_1} = 0$. Suppose we are given a

homomorphism $\rho\colon \Pi \longrightarrow \mathrm{GL}_n(R_0)$. We want to study when we can find a deformation of ρ to the ring R_1. Of course we can find a set-theoretical lift, i.e. we can find a function $\gamma\colon \Pi \longrightarrow \mathrm{GL}_n(R_1)$ that set-theoretically lifts ρ. But we look for γ to be a group homomorphism. In order to test when it is a group homomorphism we have to compute the following quantity

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

for every $g_1, g_2 \in \Pi$. Obviously, if γ was a group homomorphism then $c(g_1, g_2)$ would be equal to 1. However, we know that when we reduce modulo the ideal I we get a group homomorphism. Therefore, we have that

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

where $d(g_1, g_2) \in \mathrm{M}_n(I) \simeq Ad(\bar{\rho}) \otimes_k I$, where we can think of I as k-vector space thanks to the assumption $I \cdot m_{R_1} = 0$. It is not difficult to check that the map

$$\Pi \times \Pi \longrightarrow Ad(\bar{\rho}) \otimes_k I$$

$$(g_1, g_2) \longmapsto d(g_1, g_2)$$

is a 2-cocycle[1] and replacing γ by a different lift changes this cocycle by a $2-$coboundary[2].

Therefore, the element $d(g_1, g_2)$ gives an element $\mathcal{O}(\rho_0)$ in the cohomology group $H^2(\Pi, Ad(\bar{\rho}) \otimes_k I) = H^2(\Pi, Ad(\bar{\rho})) \otimes_k I$ and this element is trivial if and only if it exists a homomorphism $\Pi \longrightarrow \mathrm{GL}_n(R_1)$ lifting ρ_0. This justifies the following definition.

Definition 3.2.1. $\mathcal{O}(\rho_0)$ is called *the obstruction class* of ρ_0 relative to the map $R_1 \longrightarrow R_0$.

Remark 3.2.2. It is not easy to compute obstruction classes in general. However, the fact that lifts exist exactly when $\mathcal{O}(\rho_0) = 0$ tells us that when $H^2(\Pi, Ad(\bar{\rho})) = 0$ the deformation problem should be simpler, as it is shown in the following theorem.

Theorem 3.2.3. *Suppose that $C(\bar{\rho}) = k^3$ and let $\mathcal{R}$ be the universal deformation ring representing the functor D_Λ. Set then*

$$d_1 = \dim_k H^1(\Pi, Ad(\bar{\rho})),\ d_2 = \dim_k H^2(\Pi, Ad(\bar{\rho})).$$

[1] A 2-cocycle of the group G on a abelian group A is a map $f\colon G \times G \longrightarrow A$ such that for every $g_1, g_2, g_3 \in G$ $g_1 \cdot f(g_2, g_3) + f(g_1, g_2 g_3) = f(g_1 g_2, g_3) + f(g_1, g_2)$.

[2] A $2-$coboundary of the group G on the abelian group A is a map $f\colon G \times G \longrightarrow A$ such that $f(g_1, g_2) = g_1 \cdot \Phi(g_2) - \Phi(g_1 g_2) + \Phi(g)$.

[3] See Definition 2.5.2.

We have

$$\dim_{Krull}(\mathcal{R}/m_\Lambda\mathcal{R}) \geq d_1 - d_2.$$

Moreover, if $d_2 = 0$ we have equality in the formula above and precisely

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

Proof. See [5, Theorem 4.2]. □

Definition 3.2.4. If $d_2 = 0$ we say that the lifting problem is *unobstructed*.

There is, moreover, an open conjecture, called the *Dimension Conjecture*, which says that if $\bar{\rho}\colon \Pi \longrightarrow \mathrm{GL}_n(k)$ is an absolutely irreducible representation and $\mathcal{R}$ is the universal deformation ring, we have

$$\dim_{\mathrm{Krull}}(\mathcal{R}/m_\Lambda\mathcal{R}) = d_1 - d_2.$$

3.3 Galois representations

Let now K be a number field and S a set of primes of K. We will assume that S contains all the primes p above and the primes at infinity. Finally let $\Pi = G_{K,S}$ and let

$$\bar{\rho}\colon G_{K,S} \longrightarrow \mathrm{GL}_n(k)$$

be a residual representation such that $C(\bar{\rho}) = k$ and let $\mathcal{R}$ be its universal deformation ring. From the previous section we know a lower bound for $\dim_{\mathrm{Krull}}(\mathcal{R}/m_\Lambda\mathcal{R})$. We want know to find a more explicit bound using results of Galois cohomology, in particular the *Tate's Global Euler Characteristic Formula*.

Theorem 3.3.1. *Let us consider an extension $K/\mathbf{Q}$ of degree $d \in \mathbf{N}$, a finite set S of primes in K including all the infinite primes, M a finite $G_{K,S}$-module such that S contains all the primes dividing the order of M. For each prime v of K, let K_v be the completion of K at v. In particular if v is a prime at infinity then K_v is either $\mathbf{R}$ or $\mathbf{C}$. Then the globar Euler's characteristic formula is*

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

where S_∞ is the set of primes at infinity.

Remark 3.3.2. In our situation we have $M = Ad(\bar{\rho})$ which is a k-vector spaces and so it has order a power of p. Therefore, S will include all the primes p above. In this case all the cohomology groups will be also k-vector spaces and therefore all the groups in the formula above have order a power of p. This means we can translate the formula into the following statement about dimensions

$$\dim_k H^0(G_{K,S}, M) - \dim_k H^1(G_{K,S}, M) + \dim_k H^2(G_{K,S}, M) = \sum_{v \in S_\infty} \dim_k H^0(G_{K_v}, M) - d \cdot \dim_k M.$$

Now let $M = Ad(\bar{\rho})$ and $d_i = \dim_k H^i(G_{K,S}, Ad(\bar{\rho}))$, then the formula becomes

$$d_0 - d_1 + d_2 = \sum_{v \in S_\infty} \dim_k H^0(G_{K_v}, M) - d \cdot n^2$$

and so

$$d_1 - d_2 = d_0 + d \cdot n^2 - \sum_{v \in S_\infty} \dim_k H^0(G_{K_v}, Ad(\bar{\rho})).$$

We can improve the formula, by computing d_0. Indeed, we know that:

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

which is the set of matrices in $\mathrm{M}_n(K)$ fixed by the conjugation of $G_{K,S}$, i.e. $C(\bar{\rho}) = k$. Therefore $d_0 = 1$. This proves the following proposition.

Proposition 3.3.3. *Let K be a number field of degree d over $\mathbf{Q}$. Consider $\bar{\rho}\colon G_{K,S} \longrightarrow \mathrm{GL}_n(k)$ a residual representation such that $C(\bar{\rho}) = k$ and let $\mathcal{R}$ be its universal deformation ring. Then*

$$\dim_{Krull} \mathcal{R}/m_\Lambda \mathcal{R} \geq 1 + d \cdot n^2 - \sum_{v \in S_\infty} \dim_k H^0(G_{K_v}, Ad(\bar{\rho})).$$

This last formulas has many advantages, among which

- it only refers to the 0-th cohomology groups, which are only the fixed points under the Galois action and so are easy to compute;
- the groups acting are the G_{K_v}, for v an archimedean prime, so that K_v is either $\mathbf{R}$ or $\mathbf{C}$ and so G_{K_v} has either order one or two.

Example 3.3.4. *Let $n = 2$, p an odd prime number, $K = \mathbf{Q}$, S containing p and ∞. In this situation there is only one infinite prime, and G_∞ is a group of order two generated by the complex conjugation σ. Since $\sigma^2 = 1$ and p is odd, $\bar{\rho}(\sigma)$ is a matrix of order two in $\mathrm{GL}_2(k)$ and hence we must have*

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

In the first case $\det(\bar{\rho}) = 1$ and we call $\bar{\rho}$ an even representation; in the second case $\det(\bar{\rho}) = -1$ and we say that $\bar{\rho}$ is odd. It's then easy to compute the dimension d_0. In fact if $\bar{\rho}$ is even then $\bar{\rho}(\sigma)$ is a scalar matrix and so the action of G_∞ on $Ad(\bar{\rho})$ is fixed. Therefore $\dim_k H^0(G_\infty, Ad(\bar{\rho})) = \dim_k Ad(\bar{\rho}) = 4$. If $\bar{\rho}$ is odd, instead, one can easily check that $\dim_k H^0(G_\infty, Ad(\bar{\rho})) = 2$.

Recalling the formula of Proposition 3.3.3, we have then proved the following proposition.

Proposition 3.3.5. *Let p be an odd prime, let S be a set of rational primes including p and ∞, let $\bar{\rho}\colon G_{\mathbf{Q},S} \longrightarrow \mathrm{GL}_2(k)$ be a residual representation satisfying $C(\bar{\rho}) = k$ and let $\mathcal{R}$ be the universal deformation ring of $\bar{\rho}$. Then*

- *if $\bar{\rho}$ is even then $\dim_{Krull} R/m_\Lambda \geq 1$;*
- *$\bar{\rho}$ is odd then $\dim_{Krull} R/m_\Lambda \geq 3$.*

3.4 Universal ring of a Galois representation

In this section we will try to give an explicit description of the universal deformation ring of a Galois representation. Let us introduce the general setup.

- k a finite field of positive characteristic p;
- S a finite set of primes in $\mathbf{Q}$ including p and ∞;
- $\mathbf{Q}_S$ the maximal extension of $\mathbf{Q}$ unramified outside S;
- $\Pi = G_{\mathbf{Q},S} = \mathrm{Gal}(\mathbf{Q}_S/\mathbf{Q})$;
- $\bar{\rho}$ an absolutely irreducible representation or more generally $C(\bar{\rho}) = k$.

Let now $\Pi_0 = \ker(\bar{\rho})$. Then Π_0 is open, closed and of finite index and so it corresponds to a subfield K of $\mathbf{Q}_S$, whose elements are fixed by Π_0. Therefore, there is a tower of field $\mathbf{Q} \subseteq K \subseteq \mathbf{Q}_S$ where the extension $K/\mathbf{Q}$ is Galois since Π_0 is a normal subgroup and finite since $H = \mathrm{Gal}(K/\mathbf{Q}) \simeq \mathrm{Im}(\bar{\rho}) \subseteq \mathrm{GL}_n(k)$. Let S_1 be the set of primes of K above S.

Let $\rho\colon \Pi \longrightarrow \mathrm{GL}_n(\mathcal{R})$ be the universal deformation of $\bar{\rho}$. As above, let $\Gamma_n(\mathcal{R})$ be the kernel of the natural projection $\mathrm{GL}_n(\mathcal{R}) \longrightarrow \mathrm{GL}_n(k)$. If $\gamma \in \Pi_0$ then $\bar{\rho}(\gamma) = 1$ and therefore $\rho(\gamma) \in \Gamma_n(\mathcal{R})$. This shows that the restriction of ρ to Π_0 gives an homomorphism $\Pi_0 \longrightarrow \Gamma_n(\mathcal{R})$. In order to continue this analysis we need the following definition and lemma.

Definition 3.4.1. A *pro-p-group* is the inverse limit of an inverse system of discrete finite p-groups.

Lemma 3.4.2. *For any ring coefficient $R \in \mathcal{C}$, $\Gamma_n(R)$ is a pro-p-group.*

Proof. See [5, Lemma 5.1]. □

Summing up, he have that the universal deformation ρ induces a homomorphism $\Pi_0 \longrightarrow \Gamma_n(\mathcal{R})$ and $\Gamma_n(\mathcal{R})$ is a pro-p-group. Therefore the homomorphism $\Pi_0 \longrightarrow \Gamma_n(\mathcal{R})$ must factor trough some pro-p-quotient of Π_0. Any such quotient will be the Galois group of a pro-p-extension of K. So let L be the maximal pro-p-extension of K unramified outside S_1. Then $P = \mathrm{Gal}(L/K)$ is a pro-p-group and we see that ρ must factor trough $\tilde{\Pi} = \mathrm{Gal}(L/\mathbf{Q})$. It follows that all the deformations must factor through $\tilde{\Pi}$. Hence, the upshot of this discussion is that we can replace Π with $\tilde{\Pi}$ when studying the deformation theory of $\bar{\rho}$. The crucial feature of $\tilde{\Pi}$ is that it has a big normal subgroup P which is a pro-p-group, and the quotient $\tilde{\Pi}/P$ is isomorphic to the image of $\bar{\rho}$, so that the sequence

$$1 \longrightarrow P \longrightarrow \tilde{\Pi} \longrightarrow \mathrm{Im}(\bar{\rho}) \longrightarrow 1$$

is exact. The basic idea is now the following: in order to understand deformations of $\bar{\rho}$ to a coefficient Λ-algebra R, we need to understand all maps from P to $\Gamma_n(R)$ and then to consider how they may be extended to $\tilde{\Pi}$ in such a way as to be a deformation of $\bar{\rho}$. In order to simplify a little bit the situation, we will focus on *tame representations*, whose definition is the following one.

Definition 3.4.3. We say that a residual representation $\bar{\rho}$ is *tame* of the order if $\mathrm{Im}(\bar{\rho})$ is not divisible by p.

In this case the short exact sequence above tells us that $\tilde{\Pi}$ is a profinite group with a normal pro-p-Sylow subgroup, which allows us to get the structure of $\tilde{\Pi}$ in a quite explicit way.

In order to better understand the universal deformation of a tame representation we need some group-theoretical results. Let us start with the following lemma.

Lemma 3.4.4 (Schur-Zassenhaus)**.** *Let G be a profinite group with a normal pro-p Sylow group P of finite index in G. Let $\pi\colon G \longrightarrow G/P$ be the projection on the quotient. Then G contains a subgroup A such that π induces an isomorphism $\varphi\colon A \xrightarrow{\sim} G/P$. Furthermore, any two subgroups with this property are conjugate by an element of P.*

Remark 3.4.5. The main consequence of the lemma above is that G is the semi-direct product of P and A. Indeed, the exact sequence

$$1 \longrightarrow P \longrightarrow G \xrightarrow{\pi} G/P \longrightarrow 1$$

splits since $\pi \circ \varphi^{-1} = id_{G/P}$. Then, equivalently, $G = P \oplus G/P \simeq P \oplus A$. Thanks to this result, any homomorphism on G can be defined on P and A in a compatible way.

Let us now go back to our background and assume that $\bar{\rho}$ is a tame residual representation. Since, P is a normal pro-p-Sylow subgroup of $\tilde{\Pi}$, by lemma 3.4.4, $\tilde{\Pi}$ is the semi-direct product of P and a subgroup $A \simeq \tilde{\Pi}/P \simeq \mathrm{Im}(\bar{\rho})$. Moreover, since by lemma 3.4.2 $\Gamma_n(W(k))$[4] is a pro-p-group and the quotient $\mathrm{GL}_n(W(k))/\Gamma_n(W(k)) \simeq \mathrm{Im}(\bar{\rho})$, which has order not divisible by p, $\Gamma_n(W(k))$ is a pro-p Sylow subgroup. Then, applying once again Lemma 3.4.4, we can find a subgroup H_1 of $\mathrm{GL}_n(W(k))$ which is ismorphic to $\mathrm{Im}(\bar{\rho})$ and such that $\mathrm{GL}_n(W(k)) \simeq H_1 \oplus \Gamma_n(W(k))$. Therefore, supposing we have fixed a map $P \longrightarrow \Gamma_n(W(k))$, we can find a lift

$$\rho_1\colon \tilde{\Pi} \longrightarrow \mathrm{GL}_n(W(k))$$

inducing an isomorphism from A to H_1. We get, then, an induced inclusion $\sigma\colon A \hookrightarrow \mathrm{GL}_n(W(k))$, which we will fix from now on.

But for any coefficient ring R there is a canonical homomorphism $W(k) \longrightarrow R$ and hence a homomorphism $\sigma_R\colon A \longrightarrow \mathrm{GL}_n(R)$. We let A acting on $\Gamma_n(R)$ by conjugation via this homomorphism (a direct computation shows that if $M \in \Gamma_n(R)$ and $a \in A$, then $\sigma(a)M\sigma(a)^{-1} \in \Gamma_n(R)$).

[4] $W(k)$ denotes the ring of Witt vectors over the field k.

Given all this setup, recall that any deformation of $\bar{\rho}$ induces an homomorphism from P to $\Gamma_n(R)$. We can now make this into a precise correspondence by taking into account the A-action. Define a set-valued functor $\mathbf{E}_{\bar{\rho}}$ on $\mathcal{C}$, by defining for each coefficient ring R

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

where Hom_A denotes the set of continuous homomorphism form P to $\Gamma_n(R)$ which commute with the action of A (A acts on P by conjugation, being P a normal subgroup of G). We can now compare this functor to the deformation one. Notice that since $\tilde{\Pi}$ is the semi-direct product of P and A and we considered the A-action, any element $\phi \in \mathbf{E}_{\bar{\rho}}(R)$, together with the map σ_R, defines a deformation of $\bar{\rho}$ to R. Hence there is a natural morphism $\mathbf{E}_{\bar{\rho}} \longrightarrow D_{\bar{\rho}}$. Moreover, we have the following result.

Theorem 3.4.6 (Boston)**.** *The functor $\mathbf{E}_{\bar{\rho}}(R)$ is always representable. Furthermore,*

1. *if $C(\bar{\rho}) = k$, the natural morphism of functors $\mathbf{E}_{\bar{\rho}}(R) \longrightarrow D_{\bar{\rho}}$ is an isomorphism;*

2. *otherwise, the morphism is smooth and it induces an isomorphism on tangent spaces.*

Proof. See [5, Theorem 5.6]. □

To conclude this part on tame residual representations we can give the following result, that gives a characterization of their universal deformation rings under certain additional hypothesis. Before stating the theorem, we have to introduce some other notations and recall the definition of the class number of a number field.

Let $\bar{\rho}\colon \Pi \longrightarrow \mathrm{GL}_n(k)$ be a residual representation and let K be the field fixed by the kernel of $\bar{\rho}$ and set $H = \mathrm{Gal}(K/\mathbf{Q}) \simeq \mathrm{Im}(k)$. Let then S be a set of rational prime and let S_1 be the set of primes of K that lie above the primes in S. Let, then, Z_S be the set of non-zero elements $x \in K$ such that the fractional ideal (x) generated by x is the p-th power of some ideal and such that x is a p-th power in each completion K_v for $v \in S_1$. Of course, if x is already a p-th power in K, then $x \in Z_S$. Both $(K^*)^p$ and Z_S are stable under the Galois action of H. Let B_S denote the $\mathbf{F}_p[H]$-module $Z_S/(K^*)^p$.

We can recall now the definition of ideal class group and class number of a number field.

Definition 3.4.7. The *ideal class group* of an algebraic number field K is the quotient group J_K/P_K, where J_K is the group of fractional ideals of the ring of integers of K and P_K is its sbugroup of principal ideals.

Definition 3.4.8. Let K be a number field. The *class number* of K is the order of the ideal class group of its ring of integers.

We are now ready to state the following the theorem.

Theorem 3.4.9 (Boston)**.** *Let p be an odd prime. Suppose that $\bar{\rho}\colon G_{\mathbf{Q},S} \longrightarrow \mathrm{GL}_2(\mathbf{F}_p)$ is odd and absolutely irreducible. Let $H = \mathrm{Im}(\bar{\rho})$, and suppose that p does not divide the order of H, so that $\bar{\rho}$ is tame. Let K be the field fixed by the kernel of $\bar{\rho}$, and let S_1 be the set of primes of K which lie above the prime in S. Let*

$$V = \mathrm{coker}\Big(\mu_p(K)) \longrightarrow \bigoplus_{v\in S_1} \mu_p(K_v)\Big),$$

i.e. the cokernel of the map that coincides with the inclusion map in each factor, and let $B = B_S$ defined as above. Both V and B are $\mathbf{F}_p[H]$-modules. Suppose that the class number of K is not divisible by p and that V and B are relatively prime to $Ad(\bar{\rho})$ as $\mathbf{F}_p[H]$-modules. Then, the universal deformation $\mathcal{R}(\bar{\rho})$ satisfies

$$\mathcal{R}(\bar{\rho}) \simeq \mathbf{Z}_p[[T_1, T_2, T_3]].$$

Proof. See [5, Theorem 5.7]. □

Chapter 4

Applications of deformation theory: from the modularity theorem to Fermat's Last Theorem

In this final chapter we will explore the profound implications of deformation theory in algebraic number theory, focusing particularly on its role in proving some of the most famous problems in modern Mathematics, such as the modularity theorem and Fermat's Last Theorem. For references for preliminaries notions about elliptic curve and modular forms see respectively [13] and [4].

After recalling some fundamental concepts and constructions related to modular forms, we will state the modularity theorem, which asserts that every elliptic curve over $\mathbf{Q}$ is modular, meaning it can be associated with a modular form in the sense we will explain in detail later on. This theorem was first proved for semistable elliptic curves by the Andrew Wiles in 1993 with an important help from Richard Taylor and involves sophisticated techniques from deformation theory of profinite groups.
In the last part of this chapter we will expose one of the most famous problems in the history of Mathematics: Fermat's Last Theorem. We will pay great attention on the intuition had by the German mathematician Gerhard Frey in 1986. He realized that there was a fundamental connection between the modularity theorem and the proof of Fermat's Last Theorem: once solved the former the latter follows in a very natural way. An important role is played by Ribet's theorem, a particular case of Serre's Epsilon Conjecture, which states that, under certain conditions, every residual Galois representation is modular.

4.1 Recall of some definitions and constructions about modular forms

In the first section of this chapter we will recall a few definitions about modular forms, which we will need to state the modularity theorem.

4.1.1 Congruence subgroups and modular curves

Definition 4.1.1. Let N be a positive integer. The *principal congruence subgroup of level* N is

$$\Gamma(N) = \left\{ \gamma \in \mathrm{SL}_2(\mathbf{Z}) \colon \gamma = \begin{pmatrix} a & b \\ d & c \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} (\mathrm{mod}\ N) \right\}.$$

Definition 4.1.2. A subgroup Γ of $\mathrm{SL}_2(\mathbf{Z})$ is a *congruence subgroup of level* N if $\Gamma(N) \subseteq \Gamma$ for some $N \in \mathbf{Z}^+$.

The main congruence subgroups are

$$\Gamma_0(N) = \left\{ \gamma \in \mathrm{SL}_2(\mathbf{Z}) \colon \gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} * & * \\ 0 & * \end{pmatrix} (\mathrm{mod}\ N) \right\},$$

$$\Gamma_1(N) = \left\{ \gamma \in \mathrm{SL}_2(\mathbf{Z}) \colon \gamma = \begin{pmatrix} a & b \\ d & c \end{pmatrix} = \begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix} (\mathrm{mod}\ N) \right\}.$$

We know that $\mathrm{SL}_2(\mathbf{Z})$ acts on the upper complex half-plane $\mathcal{H}$ via Möbius transformations

$$\begin{pmatrix} a & b \\ d & c \end{pmatrix} (z) \coloneqq \frac{az+b}{cz+d},$$

where $z \in \mathcal{H}$. We can then give the following definition.

Definition 4.1.3. The *modular curve* $Y(\Gamma)$ is defined as the quotient space of orbits

$$Y(\Gamma) = \Gamma \setminus \mathcal{H} = \{\Gamma\tau : \tau \in \mathcal{H}\}.$$

The modular curves with respect to $\Gamma_0(N), \Gamma_1(N), \Gamma(N)$ are respectively $Y_0(N)$, $Y_1(N)$, $Y(N)$. They all inherit the quotient topology from the Euclidean topology of $\mathcal{H}$ seen as a subspace of $\mathbf{R}^2$. One can endow $Y(\Gamma)$ with a canonical structure of Riemann surface which by the way is not compact. In order to compactify it,

we add finitely many cusps in the following way: we extend the action of $\mathrm{SL}_2(\mathbf{Z})$ to $\mathcal{H}_\infty \coloneqq \mathcal{H} \cup \mathbf{P}^1(\mathbf{Q})$. Since $\mathrm{SL}_2(\mathbf{Z})$ acts transitively on $\mathbf{P}^1(\mathbf{Q})$, we can define a topology on $\mathcal{H}_\infty$ by saying that for all $\gamma \in \mathrm{SL}_2(\mathbf{Z})$, $\gamma(\infty)$ has a basis of neighborhoods of the form $\gamma(\{\tau \in \mathcal{H} \colon \mathcal{I}(\tau) > M > 0\} \cap \{\infty\})$.

Proposition 4.1.4. *The modular curve $X_0(N) \coloneqq \Gamma_0(N) \setminus \mathcal{H}_\infty$ is a compact and connected Riemann surface.*

Proof. See [4, Proposition 2.4.2]. □

We also have the following important result.

Theorem 4.1.5 (Shimura, Katz, Mazur, Eichler, Mumford)**.** *$X_0(N)$ is the set of complex points of a smooth and projective curve defined over $\mathbf{Q}$.*

4.1.2 Oldforms and newforms

The complex vector space $S_k(\Gamma_1(N))$ of cusp forms of weight k with respect to $\Gamma_1(N)$ can be enowed with an inner product, which is defined as an integral over a compactified modular curve and it is called the *Petersson product*.

Suppose $M|N$, then we have the trivial inclusion $S_k(\Gamma_1(M)) \subseteq S_k(\Gamma_1(N))$. We want now to isolate the part that comes from the lower levels in $S_k(\Gamma_1(N))$.

Definition 4.1.6. Let $N \in \mathbf{Z}^+$. For each d divisor of N, define

$$(S_k(\Gamma_1(Nd^{-1})))^2 \longrightarrow S_k(\Gamma_1(N))$$

given by $(f, g) \longmapsto f(z) + d^{k-1}g(dz)$ (it is easy to check that this map is well defined). Then the *subspace of old forms at level N* is :

$$S_k(\Gamma_1(N))^{old} = \sum_{p|N} i_p((S_k(\Gamma_1(Np^{-1})))^2),$$

where p is a prime and the *subspace of new forms at level N* is the orthogonal with respect to the Peterson inner product :

$$S_k(\Gamma_1(N))^{new} = (S_k(\Gamma_1(N))^{old})^\perp.$$

Proposition 4.1.7. *$S_k(\Gamma_1(N))^{new}$ and $S_k(\Gamma_1(N))^{old}$ are stable under the Hecke operators $\langle n \rangle$ and T_n for all $n \in \mathbf{Z}^+$ and they have orthogonal bases of eigenforms away from the level N, i.e for all $n \in \mathbf{Z}^+$ such that $(n, N) = 1$.*

Proof. See [4, Proposition 5.6.2]. □

We are now ready for the following definition.

Definition 4.1.8. We say that $f = \sum_{n\geq 0} \in S_k(\Gamma_1(N))$ is a *newform* if it is a normalized (i.e. $a_1(f) = 1$) eigenform (for all the Hecke operators T_n and $\langle n\rangle$) in $S_k(\Gamma_1(N))$.

4.1.3 Galois representation attached to a modular form

We would like to construct a Galois representation attached to a modular curve. We could try to imitate the action of $G_{\mathbf{Q}}$ on the ℓ-adic Tate module of an elliptic curve $E/\mathbf{Q}$, $T_\ell(E) = \varprojlim_n E[\ell^n]$, which gives a Galois representation associated with E (up to a change of basis of $\mathbf{Z}_\ell^2$) :

$$\rho_{E,\ell}\colon G_{\mathbf{Q}} \longrightarrow \mathrm{GL}_2(\mathbf{Z}_\ell) \subseteq \mathrm{GL}_2(\mathbf{Q}_\ell).$$

However, this is not possible because modular curves do not have a group structure like elliptic curves. We need then to use the notions of Jacobian variety associated with a Riemann surface and abelian variety associated with a normalized eigenform $f \in S_2(N, \chi)$.

Firstly, recall that the Jacobian variety of a Riemann surface X, that we denote by $J(X)$, is an abelian variety defined over $\mathbf{Q}$ isomorphic to a torus of dimension equal to the genus of X, i.e. we have $J(X) \simeq \mathbf{C}^g/\Lambda$, where Λ is a suitable lattice and g is the genus of X. If then $f \in S_2(N, \chi)$ is a normalized eigenform, the abelian variety associated with f is the quotient $A_f \coloneqq J(X_1(N))/I_{\mathbf{Z},f}J(X_1(N))$, where $I_{\mathbf{Z},f}$ is a prime ideal of the algebra generated by the Hecke operators $\mathbb{T}_{\mathbf{Z}} = \mathbf{Z}[\{T_n, \langle n\rangle : n \in \mathbf{Z}^+\}]$, which acts on the Jacobian . Thanks to this notion we are now ready to state and give a sketch of proof of the following theorem.

Theorem 4.1.9 (Theorem 9.5.4 in [4])**.** *Let $N \in \mathbf{Z}_{\geq 1}$ and $f = \sum_n a_n q^n \in S_2(\Gamma_1(N), \chi)$ be a normalized eigenform of weight 2, level N, nebentypus χ and Hecke field*[1] *K_f. Then for any rational prime ℓ and any prime $\lambda|\ell$ of K_f there exists a Galois representation $\rho_{f,\lambda}\colon G_{\mathbf{Q}} \longrightarrow \mathrm{GL}_2(K_{f,\lambda})$ unramified at every prime $p \nmid \ell N$ and such that $\rho_{f,\lambda}(Frob_{\mathfrak{P}})$ satisfies the equation*

$$x^2 - a_p(f)x + \chi(p)p = 0$$

[1] Let $f = \sum_n a_n q^n \in S_2(\Gamma_1(N), \chi)$ be a normalized eigenform. The Hecke field of f is $K_f = \mathbf{Q}(\{a_n\}_n)$. One can prove K_f is a number field.

for any $\mathfrak{P}|p$ and $p \nmid \ell N$. In particular, if $f \in S_2(\Gamma_0(N)) = S_2(\Gamma_1(N), \mathbf{1})$, then the characteristic polynomial of $\rho_{f,\lambda}(Frob_{\mathfrak{P}})$ is $x^2 - a_p(f)x + p$.

Sketch of proof. For the first step we want to build a Galois representation of the form $\rho_{X_1(N),\ell} \colon G_{\mathbf{Q}} \longrightarrow \mathrm{GL}_{2g}(\mathbf{Q}_\ell)$ attached to $X_1(N)$, where g is the genus of the modular curve $X_1(N)$. Thanks to algebraic geometry we know that there is an isomoprhism $\mathrm{Pic}^0(X_1(N)) \simeq J_1(N) \simeq \mathbf{C}^g/\Lambda$, where $J_1(N) = J(X_1(N))$. Then it makes sense to naturally define the ℓ-adic Tate module of $\mathrm{Pic}^0(X_1(N))$ as $\mathrm{Ta}_\ell(\mathrm{Pic}^0(X_1(N)) = \varprojlim_n \mathrm{Pic}^0(X_1(N))[\ell^n]$. Then fixing a basis of $\mathrm{Pic}^0(X_1(N))[\ell^n]$ in a compatible way, we have that $\mathrm{Pic}^0(X_1(N))[\ell^n] \simeq (\mathbf{Z}/\ell^n\mathbf{Z})^{2g}$ and consequently $\mathrm{Ta}_\ell(\mathrm{Pic}^0(X_1(N)) \simeq (\mathbf{Z}_\ell)^{2g}$. Since the action[2] of $G_{\mathbf{Q}}$ on $\mathrm{Pic}^0(X_1(N))$ restricts to compatible actions on $\mathrm{Pic}^0(X_1(N))[\ell^n]$ for any $n > 1$, it induces an action on $\mathrm{Ta}_\ell(\mathrm{Pic}^0(X_1(N))$. Then we have a continuous representation $\rho_{X_1(N),\ell} \colon G_{\mathbf{Q}} \longrightarrow \mathrm{GL}_{2g}(\mathbf{Z}_\ell) \subseteq \mathrm{GL}_{2g}(\mathbf{Q}_\ell)$, which is unramified at any prime $p \nmid \ell N$ and such that $\rho_{X_1(N),\ell}(\mathrm{Frob}_{\mathfrak{P}})$ satisfies the equation $x^2 - T_p x + \langle p \rangle p = 0$ (note that the Hecke operators T_p and $\langle p \rangle$ and $\mathrm{Frob}_{\mathfrak{P}}$ all act on $\mathrm{Pic}^0(X_1(N)))[\ell^n]$).

For the second step we want to build a Galois representation $\rho_{A_f,\ell} \colon G_{\mathbf{Q}} \longrightarrow \mathrm{GL}_{2d}(\mathbf{Q}_\ell)$ attached to A_f, where $d = [K_f : \mathbf{Q}]$. Again from algebraic geometry, we know that A_f is a complex torus of dimension d, i.e. $A_f \simeq \mathbf{C}^d/\Lambda$, for a suitable lattice Λ. Then it makes sense to define its ℓ-adic Tate module as $\mathrm{Ta}_\ell(A_f) = \varprojlim_n A_f[\ell^n]$. Now, If for every $n \geq 1$, we fix a basis of $A_f[\ell^n]$ in a compatible way we have that $\mathrm{Ta}_\ell(A_f) \simeq (\mathbf{Z}_\ell)^{2d}$. The natural map

$$G \colon \mathrm{Pic}^0(X_1(N))[\ell^n] \longrightarrow J_1(N)[\ell^n] \longrightarrow (J_1(N)/I_{\mathbf{Z},f}J_1(N))[\ell^n] = A_f[\ell^n]$$

is surjective and $\ker(G)$ is $G_{\mathbf{Q}}$-stable. Hence, the action of $G_{\mathbf{Q}}$ on $\mathrm{Ta}_\ell(\mathrm{Pic}^0(X_1(N)))$ induces an action of $G_{\mathbf{Q}}$ on $\mathrm{Ta}_\ell(A_f)$, which gives a continuous Galois representation $\rho_{A_f,\ell} \colon G_{\mathbf{Q}} \longrightarrow \mathrm{GL}_2(\mathbf{Z}_\ell) \subseteq \mathrm{GL}_2(\mathbf{Q}_\ell)$. One can prove that $\rho_{A_f,\ell}$ is unramified at every prime $p \nmid \ell N$ and that $\mathrm{Frob}_{\mathfrak{P}}$ satisfies the equation $x^2 - a_p(f)x + \chi(p)p = 0$ for every prime $\mathfrak{P}|p$ and $p \nmid \ell N$.

For the last step we build the representation $\rho_{f,\lambda}$. First of all we define the $\mathbf{Q}_\ell$-vector space $V_\ell(A_f) \coloneqq \mathrm{Ta}_\ell(A_f) \otimes_{\mathbf{Z}_\ell} \mathbf{Q}_\ell$ endowed with an action of $\mathcal{O}_f = \mathbb{T}_{\mathbf{Z}}/I_{\mathbf{Z},f}$ and $G_{\mathbf{Q}}$. All these action commute with each other and so we can see $V_\ell(A_f)$ as a $\mathcal{O}_f \otimes_{\mathbf{Z}} \mathbf{Q}_\ell$-module. Recalling the last part of Subsection 1.5.3, we know that

[2]The action of $G_{\mathbf{Q}}$ on $Div^0(X_1(N))$ is defined as $\sigma(\sum n_P P) = \sum n_P \sigma(P)$. In particular, it respects the degree of a divisor and hence it induces an action on $\mathrm{Pic}^0(X_1(N))$.

$\mathcal{O}_f \otimes_{\mathbf{Z}} \mathbf{Q}_\ell \simeq (\mathcal{O}_f \otimes_{\mathbf{Z}} \mathbf{Q}) \otimes_{\mathbf{Q}} \mathbf{Q}_\ell \simeq K_f \otimes_{\mathbf{Q}} \mathbf{Q}_\ell \simeq \prod_{\lambda|\ell} K_{f,\lambda}$. Then $V_\ell(A_f) = \prod_{\lambda|\ell} V_\lambda(A_f)$, where $V_\lambda(A_f) = V_\ell(A_f) \otimes_{\mathbf{Q}_\ell} K_{f,\lambda}$. Obviously $V_\lambda(A_f)$ is a $K_{f,\lambda}$-vector space and thanks to the commutativity of the actions it is stable under $G_{\mathbf{Q}}$. Moreover, it $V_\lambda(A_f)$ has dimension 2 over $K_{f,\lambda}$ for every $\lambda|\ell$. Finally the representation $\rho_{f,\lambda}$ is given by the action of $G_{\mathbf{Q}}$ on $V_\lambda(A_f)$. Thanks to the considerations in the previous steps, it is clear that it satisfies the properties stated in the theorem. □

4.2 Equivalent definitions of modularity

We will now introduce the concept of modular elliptic curve defined over $\mathbf{Q}$. In order to give an idea of what this means, we can think of a modular elliptic curve $E/\mathbf{Q}$ as a quotient of a modular curve. However, there are many equivalent ways to define when an elliptic curves is modular and in this section we will analyze some of them. Our main goal will be to give a sketch of the proof of the modularity theorem using the tools of deformation theory. Its statement is very easy and it is the following one.

Theorem 4.2.1 (Modularity theorem)**.** *Every elliptic curve over* $\mathbf{Q}$ *is modular.*

4.2.1 Modularity via modular curves

Definition 4.2.2 (Modularity-Version X)**.** We say that an elliptic curve $E/\mathbf{Q}$ is *modular* if for some $N \geq 1$ there exists a surjective morphism of algebraic curves defined over $\mathbf{Q}$

$$X_0(N) \longrightarrow E.$$

Definition 4.2.3 (Modularity-Version J)**.** We say that an elliptic curve $E/\mathbf{Q}$ is *modular* if for some $N \geq 1$ there exists a surjective morphism of algebraic curves defined over $\mathbf{Q}$

$$J_0(N) \longrightarrow E.$$

Proposition 4.2.4. *Version X is equivalent to version J.*

Proof. See [4, Section 6.1 and 6.2]. □

Definition 4.2.5. Let $E/\mathbf{Q}$ be an elliptic modular curve. The smallest N that can occur in the definitions above is called the *analytic conductor* of E.

4.2.2 Modularity via modular forms

Definition 4.2.6 (Modularity-Version A)**.** We say that an elliptic curve $E/\mathbf{Q}$ is *modular* if for some $N \geq 1$, there exists a newform $f \in S_2(\Gamma_0(N))$ and a surjective morphism of abelian varieties defined over $\mathbf{Q}$

$$A_f \longrightarrow E.$$

Proposition 4.2.7. *Version A is equivalent to version J.*

Proof. See [4, Section 6.6]. □

In order to give other definitions of modularity via modular forms we need to introduce the notion of algebraic conductor of an elliptic curve.

Definition 4.2.8. Given an elliptic curve $E/\mathbf{Q}$ in minimal form[3], we define the *algebraic* (or *Arithmetic*) *conductor* of E as the integer

$$N_E = \prod_{p \text{ prime}} p^{f_p},$$

where

$$\begin{cases} 0 & \text{if } E \text{ has good reduction at } p \\ 1 & \text{if } E \text{ has multiplicative reduction at } p \\ 2 & \text{if } E \text{ has additive reduction at } p \neq 2,3 \\ 2+\delta_p & \text{if } E \text{ has additive reduction at } p = 2,3. \end{cases}$$

(Here δ_p depends on wild ramification of the action of inertia groups at p of $G_{\mathbf{Q}}$ on the Tate module $T_p(E)$ and can be computed using Tate's algorithm [14, Chapter 4]).

Remark 4.2.9. Note that N_E is well-defined, since the primes of bad reduction are those primes dividing the discriminant, so that the product is finite.

Definition 4.2.10. Let $E/\mathbf{Q}$ be an elliptic curve in minimal form. Then for every prime p, we define

$$a_p(E) \coloneqq p + 1 - \#\tilde{E}(\mathbf{F}_p)$$

, where $\tilde{E}$ is the reduction modulo p of E.

[3] A Weierstrass equation $E/\mathbf{Q}$ is minimal if it is minimal at p for all primes p (see [2]).

Remark 4.2.11. This definition extends to prime powers as

$$a_{p^e}(E) \coloneqq p^e + 1 - \#\tilde{E}(\mathbf{F}_{p^e})$$

and, if we define $a_1(E) = 1$, we can give a recurrence similar to the one satisfied by the coefficients $a_{p^e}(E)$ of a normalized eigenform[4] in $S_2(\Gamma_0(N))$:

$$a_{p^e}(E) = a_p(E)a_{p^{e-1}}(E) - \mathbf{1}_{N_E}(p)a_{p^{e-2}}(E)$$

for all $e \geq 2$, where $\mathbf{1}_{N_E}$ is the trivial character modulo the algebraic conductor of E, so that $\mathbf{1}_{N_E}(p)$ is 1 for primes of good reduction and 0 for primes of bad reduction. Finally, we define $a_n(E)$ for n not a prime power, by requiring $a_{nm}(E) = a_n(E)a_m(E)$. Therefore, the $a_n(E)$ behave in the same way as the coefficients $a_n(f)$ of a newform $f \in S_2(\Gamma_0(N))$.

We can then give the following definition.

Definition 4.2.12 (Modularity-Version a_p)**.** We say that an elliptic curve $E/\mathbf{Q}$ with conductor N_E is modular if there exists a newform $f \in S_2(\Gamma_0(N_E))$ such that $a_p(E) = a_p(f)$ for every prime p.

Proposition 4.2.13. *Version X implies version a_p.*

Proof. See [4, Section 8.8] □

4.2.3 Modularity via Galois representations

Let E be an elliptic curve with algebraic conductor N_E and attached Galois representation $\rho_{E,\ell}$, where l is a prime number. We then have the followimg result.

Theorem 4.2.14 (Theorem 9.4.1 in [4])**.** *The Galois representation $\rho_{E,\ell}$ is irreducible and it is unramified at every prime $p \nmid \ell N_E$. For any such p, let $\mathfrak{P} \subseteq \bar{\mathbf{Z}}$ be a maximal ideal over p. Then characteristic polynomial of $\rho_{E,\ell}(Frob_{\mathfrak{P}})$ is $x^2 - a_p(E)x + p$.*

We can now define when a Galois representation is modular.

Definition 4.2.15. An irreducible Galois representation $\rho\colon G_{\mathbf{Q}} \longrightarrow \mathrm{GL}_2(\mathbf{Q}_l)$ such that $\det(\rho) = \chi_\ell$ is the ℓ-adic cyclotomic character, is called *modular* if there exists a newform $f \in S_2(\Gamma_0(M_f))$ such that $K_{f,\lambda} \simeq \mathbf{Q}_\ell$ for some $\lambda|\ell$ and such that $\rho_{f,\lambda} \sim \rho$.

[4]For every p prime, the Hecke operator T_p satisfies $T_{p^e} = T_p T_{p^{e-1}} - p^{k-1}\langle p\rangle T_{p^{e-2}}$ for $e > 1$. Then if $f \in S_2(\Gamma_0(N)) = S_2(\Gamma_1(N), \mathbf{1})$ is a newform, $T_p(f) = a_p(f)f$ and so $a_{p^e}(f) = a_p(f)a_{p^{e-1}}(f) - \mathbf{1}(p)a_{p^{e-2}}(f)$, where $\mathbf{1}$ is the trivial character modulo N.

We are now ready for the last two definitions of modularity.

Definition 4.2.16 (Modularity-Version R)**.** We say that an elliptic curve $E/\mathbf{Q}$ is *modular* if $\rho_{E,\ell}$ is modular for some prime ℓ.

This is the definition used to prove the modularity theorem, first for semistable[5] elliptic curves (in 1995, by Wiles and Taylor) and later, for every elliptic curve (in 2001, by Breuil, Conrad, Diamond and Taylor).

Definition 4.2.17 (Modularity-Strong version R)**.** We say that an elliptic curve $E/\mathbf{Q}$ with algebraic conductor N_E is *modular* if there exists a newform $f \in S_2(\Gamma_0(N_E))$ with number field $K_f = \mathbf{Q}$ such that $\rho_{f,\ell} \sim \rho_{E,\ell}$ for all primes ℓ.

Remark 4.2.18. Note that if $K_f = \mathbf{Q}$, then $K_{f,\lambda} = \mathbf{Q}_\ell$ for some ℓ prime. Then the Galois representation $\rho_{f,\lambda}$ coincides with $\rho_{f,\ell}$.

With the next proposition we will prove that these two definitions are in fact equivalent to Version a_P.

Proposition 4.2.19. *Version $R \Rightarrow$ Version $a_p \Rightarrow$ Strong Version R ($\Rightarrow$ Version R)*

Sketch of proof. (**Version** $R \Rightarrow$ **Version** a_p) Let $E/\mathbf{Q}$ be an elliptic curve with algebraic conductor N_E. Then assuming that E is modular in the sense of version R, there exists a newform $f \in S_2(\Gamma_0(M_f))$, as in the definition above, such that $\rho_{f,\lambda} \sim \rho_{E,\ell}$ for a suitable maximal ideal λ of $\mathcal{O}_{K_f}$, the ring of integers of K_f. Thus, by Theorem 4.1.9, $x = \rho_{E,\ell}(\mathrm{Frob}_\mathfrak{P})$ satisfies $x^2 - a_p(f) + p = 0$, for any Frobenius element $\mathrm{Frob}_\mathfrak{P}$, where $\mathfrak{P}$ lies over any prime $p \nmid \ell M_f$, since this is true for $\rho_{f,\lambda}(\mathrm{Frob}_\mathfrak{P})$. However the characteristic polynomial of $x = \rho_{E,\ell}(\mathrm{Frob}_\mathfrak{P})$, for any $\mathrm{Frob}_\mathfrak{P}$ such that $p \nmid \ell N_E$, is $x^2 - a_p(E)x + p$. Therefore, $a_p(f) = a_p(E)$ for all but finitely many primes (namely $p \nmid \ell M_f N_E$). Then one can prove that $a_p(f) = a_p(E)$ for all primes p and that $M_f = N_E$, which is exactly Version a_p.
(**Version** $a_p \Rightarrow$ **StrongVersion** R) Again let $E/\mathbf{Q}$ be an elliptic curve with algebraic conductor N_E. Then assuming that E is modular in the sense of Version a_p, there exists a newform $f \in S_2(\Gamma_0(N_E))$ such that $a_p(f) = a_p(E)$ ($\in \mathbf{Z}$) for every prime p. So $a_p(f) \in \mathbf{Z}$ for every p, which implies, thanks the recursive formula of Remark 4.2.11, that $K_f = \mathbf{Q}$. Hence, since $\mathcal{A}_f$ is an abelian variety of dimension $[K_f\colon \mathbf{Q}]$, it is an elliptic curve. Recalling the proof of Theorem 4.1.9, it is clear that this also implies that $\rho_{f,\ell} = \rho_{\mathcal{A}_f,\ell}$, which shows that $\rho_{f,\ell}$ is irreducible by Theorem 4.2.14.
For an arbitrary prime ℓ, the characteristic polynomial of the elements $\rho_{f,\ell}(\mathrm{Frob}_\mathfrak{P})$ and $\rho_{E,\ell}(\mathrm{Frob}_\mathfrak{P})$ are $x^2 - a_p(f)x + p$ and $x^2 - a_p(E)x + p$, respectively, for all but

[5] An elliptic curve $E/\mathbf{Q}$ is semistable is it has multiplicative reduction at every bad prime.

finitely many primes p (namely $p \nmid \ell N_E$). Thus, the characteristic polynomials of $\rho_{f,\ell}(\mathrm{Frob}_{\mathfrak{P}})$ and $\rho_{E,\ell}(\mathrm{Frob}_{\mathfrak{P}})$ are equal on a dense set[6] of $G_{\mathbf{Q}}$ and since the trace and the determinant are continuous, the characteristic polynomial of $\rho_{f,\ell}(\sigma)$ and $\rho_{E,\ell}(\sigma)$ are equal for every $\sigma \in G_{\mathbf{Q}}$. One can prove that this implies that $\rho_{f,\ell} \sim \rho_{E,\ell}$. Since ℓ was arbitrary, this is strong Version R. □

Corollary 4.2.20. *Let $E/\mathbf{Q}$ be an elliptic curve. If $\rho_{E,\ell}$ is modular for some prime ℓ, then it is modular for every l.*

4.3 The modularity theorem: Wiles's proof

In this section we will focus on some aspects of the proof of Wiles's theorem, which is a version of the modularity theorem for semistable elliptic curves.

Theorem 4.3.1 (Wiles)**.** *Every semistable elliptic curve E over $\mathbf{Q}$ is modular.*

4.3.1 Outline of the proof

In this section we will start explaining the way Wiles's proof of the modularity theorem works. It will be clear that the proof deeply relies on deformation theory. Indeed, let us start considering a residual Galois representation $\rho_0 \colon G_{\mathbf{Q}} \longrightarrow \mathrm{GL}_2(k)$, where k is a finite field of characteristic $p \geq 3$. We want ρ_0 to satisfy the following properties:

(A) ρ_0 has determinant χ_p;

(B) ρ_0 is semistable;

(C) ρ_0 is absolutely irreducible;

(D) ρ_0 is modular and if $p = 3$, $\rho_0|_{G_{(\mathbf{Q}(\sqrt{-3}))}}$ is absolutely irreducible.

Let us now explain the meaning of these conditions.

The condition (A). Let $\chi_p \colon G_{\mathbf{Q}} \longrightarrow \mathbf{Z}_p^*$ denote the cyclotomic character (Example 1.5.6). Since we are working with representation defined over k and later on more generally on coefficient rings A, the determinant of the representation doesn't take values in $\mathbf{Z}_p^*$. However in both cases we have a canonical (continuous in the

[6]This is another statement of Chebotarev's density theorem.

case of coefficient rings) ring morphism $\mathbf{Z}_p \twoheadrightarrow F_p \hookrightarrow k$ and $\mathbf{Z}_p \to A$, and composing χ_p with this canonical ring homomorphism we get a cyclotomic character (which we still denote by χ_p) with values respectively in k^* and A^*.

The condition (B).We need now to define the notion of semistability for a general Galois representation. The reason for the name is not immediately clear reading the definition but it is what one imagines: if E is a semistable elliptic curve, then the representation $\rho_{E,p}\colon G_{\mathbf{Q}} \longrightarrow \mathrm{GL}_2(\mathbf{Z}_p)$ attached to its Tate module is semistable in the sense we are going to define.

Definition 4.3.2. Let R be a ring. We say that a representation $\rho\colon G_{\mathbf{Q}} \longrightarrow \mathrm{GL}_2(R)$ is *ordinary* at p if its restriction to the inertia subgroup I_p is (equivalent to one) of the form

$$\begin{pmatrix} \chi_p & * \\ 0 & 1 \end{pmatrix}.$$

Definition 4.3.3. Let k be a finite field of characteristic p, consider a representation $\bar{\rho}\colon G_{\mathbf{Q}_p} \longrightarrow \mathrm{Aut}(M)$ on a finite abelian p-group M and denote by $M_{\bar{\rho}}$ is associated $G_{\mathbf{Q}_p}$-module. We say that $\bar{\rho}$ is *flat* if there exist a finite flat group scheme $H/\mathbf{Z}_p$ such that $M_{\bar{\rho}} \simeq H(\bar{\mathbf{Q}}_p)$, as $G_{\mathbf{Q}_p}$-modules. We say then that a representation $\bar{\rho}\colon G_{\mathbf{Q}} \longrightarrow \mathrm{Aut}(M)$ is flat at p if its restriction to $G_{\mathbf{Q}_p}$ is so.

Definition 4.3.4. Let R be a coefficient ring with finite residue field of characteristic p, as defined in Section 2.1. We say that a Galois representation $\rho\colon G_{\mathbf{Q}} \longrightarrow \mathrm{GL}_2(R)$ is *flat* at p if for any ideal I of R with finite quotient ring R/I, the representation $\rho\colon G_{\mathbf{Q}_p} \longrightarrow \mathrm{GL}_2(R/I)$ is flat in the previous sense.

We can now define what a semistable representation is.

Definition 4.3.5. A Galois representation

$$\rho\colon G_{\mathbf{Q}} \longrightarrow \mathrm{GL}_2(R)$$

is called *semistable* at ℓ if

- (if $\ell = p$) is either flat or ordinary (or both) at p;
- (if $\ell \neq p$) $\rho|_{I_\ell} \simeq \begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix}$.

Moreover we just say that ρ is semistable if so it is for every prime ℓ.

The conditions (C) and (D). We have already introduced the notion of absolute irreducibility of a representation (Definition 2.5.5). We have then left to define modularity for finite fields.

Definition 4.3.6. Let k be a field of finite characteristic p. We say that a representation $\rho_0 \colon G_{\mathbf{Q}} \longrightarrow \mathrm{GL}_2(k) \subseteq \mathrm{GL}_2(\bar{\mathbf{F}}_p)$ is modular if there exists a newform $f \in S_2(\Gamma_0(M_f))$ and a prime λ of $\mathcal{O}_f \subseteq K_f$ such that the residual representaion[7] of $\rho_{f,\lambda}$, namely $\bar{\rho}_{f,\lambda} \colon G_{\mathbf{Q}} \longrightarrow \mathrm{GL}_2(\mathcal{O}_f/\lambda) \subseteq \mathrm{GL}_2(\bar{\mathbf{F}}_p)$ is equivalent to ρ_0.

Remark 4.3.7. Note that the definition above is consistent with theorem 4.1.9. Indeed, $\mathrm{Ta}_\ell(A_f)$ is an $\mathcal{O}_f = \prod_{\lambda|\ell} \mathcal{O}_{f,\lambda}$-module, where $\mathcal{O}_{f,\lambda}$ is the ring of integers of $K_{f,\lambda}$. Then $\mathrm{Ta}_\lambda(A_f) \coloneqq \mathrm{Ta}_\ell(A_f) \otimes_{\mathbf{Z}_\ell} \mathcal{O}_{f,\lambda}$ is an $\mathcal{O}_{f,\lambda}$-module of dimension 2 endowed with a $G_{\mathbf{Q}}$-action. Hence, we get a map $\rho_{f,\lambda} \colon G_{\mathbf{Q}} \longrightarrow \mathrm{GL}_2(\mathcal{O}_{f,\lambda}) \subseteq \mathrm{GL}_2(K_{f,\lambda})$. It makes then sense to consider the reduction of $\rho_{f,\lambda}$ modulo λ.

Remark 4.3.8. If ℓ is a prime number and $\bar{\rho}_{E,\ell} \colon G_{\mathbf{Q}} \longrightarrow \mathrm{GL}_2(\mathbf{Z}/\ell\mathbf{Z})$ is the Galois representation attached to the point of ℓ-torsion of E, then Corollary 4.2.20 still holds, i.e. if $\bar{\rho}_{E,\ell}$ is modular according to the definition above, for one prime ℓ, then it is modular for every prime ℓ.

We want now to introduce a more general notion of modularity for coefficient rings. We denote by $\mathbb{T}'(N)$ the subalgebra of $\mathrm{End}(S_2(\Gamma_0(N)))$ generated over $\mathbf{Z}$ by the Hecke operators T_ℓ for $\ell \nmid pN$ and the diamond operators $\langle d \rangle$, for $d \in (\mathbf{Z}/N\mathbf{Z})^*$.

Definition 4.3.9. Let A be a coefficient ring with residue characteristic p. A representation $\rho \colon G_{\mathbf{Q}} \longrightarrow \mathrm{GL}_2(A)$ is said to be *modular* if there exists an integer $N > 0$ and homomorphism $\pi \colon \mathbb{T}'(N) \longrightarrow A$ such that ρ is unramified outside Np and for every $\ell \nmid pN$ the characteristic polynomial of any Frobenius at ℓ is $x^2 + \pi(T_\ell)x + \pi(\langle \ell \rangle)\ell$.

We can now come to deformation theory and give the following definition.

Definition 4.3.10. Let A be a coefficient ring. A deformation type $\mathcal{D}$ is a subfunctor of the deformation functor D_{ρ_0}, defined in Definition 2.2.8. A representation $\rho \colon G_{\mathbf{Q}} \longrightarrow \mathrm{GL}_2(A)$ is said to be *deformation of type* $\mathcal{D}$ if $[\rho] \in \mathcal{D}(A)$, where $[\rho]$ is the equivalence class of ρ as in Definition 2.2.3.

As the functor D_{ρ_0}, also the functor $\mathcal{D}$ is representable in many cases (in particular in those of interest for us) and we have an analogous notion of universal deformation ring $R_{\mathcal{D}}$ and universal deformation $\rho_{\mathcal{D}} \colon G_{\mathbf{Q}} \longrightarrow \mathrm{GL}_2(R_{\mathcal{D}})$ satisfying the following

[7] Obtained by composing the $\rho_{f,\lambda}$ with the projection map $\mathcal{O}_{f,\lambda} \longrightarrow \mathcal{O}_{f,\lambda}/\lambda\mathcal{O}_{f,\lambda} \simeq \mathcal{O}_f/\lambda$.

universal property: for any deformation $\rho\colon G_{\mathbf{Q}} \longrightarrow \mathrm{GL}_2(A)$ of ρ_0 of type $\mathcal{D}$ there is a unique homomorphism $\pi_A\colon R_{\mathcal{D}} \longrightarrow A$ such that the triangle

$$\begin{array}{ccc} G_{\mathbf{Q}} & \xrightarrow{\rho_{\mathcal{D}}} & \mathrm{GL}_2(R_{\mathcal{D}}) \\ & \searrow^{\rho} & \downarrow{\scriptstyle \pi_A} \\ & & \mathrm{GL}_2(A) \end{array}$$

commutes, or in other terms each deformation ρ of type $\mathcal{D}$ factors through $\mathrm{GL}_2(R_{\mathcal{D}})$ via $\rho_{\mathcal{D}}$.
We will be interested in deformation of ρ_0 of type $\mathcal{D}$, for $\mathcal{D}$ of a particular kind: let S be the set of primes $l \neq p$ at which ρ_0 is ramified, for any Σ finite set of primes disjoint from S let $\mathcal{D}_\Sigma(R)$ be the set of deformations ρ of ρ_0 that roughly speaking have the same local properties of ρ_0, more precisely such that

- ρ has determinant χ_p;
- ρ is unramified outside $S \cup \{p\} \cup \Sigma$;
- ρ is semistable outside Σ;
- if $p \notin \Sigma$ and ρ_0 is flat at p, then also ρ is flat at p.

The key abstract lemma in the proof of Wiles's theorem is the following.

Lemma 4.3.11. *Suppose ρ_0 satisfies properties* (**A**)-(**D**)*. Then any deformation ρ of ρ_0 of type $\mathcal{D}_\Sigma$, for Σ a finite set of primes as above, is modular in the sense of Definition 4.3.10.*

Remark 4.3.12. Let us denote $T_\Sigma = \Sigma \cup S \cup \{p\}$. The condition that every ρ of type D_Σ is unramified outside T_Σ implies that every such ρ factorizes through $G_{\mathbf{Q},T_\Sigma}$. Let $\rho_0'\colon G_{\mathbf{Q},T_\Sigma} \longrightarrow \mathrm{GL}_N(k)$ be a residual representation

$$\begin{aligned} \mathcal{D}_{T_\Sigma}\colon \mathcal{C} &\longrightarrow \mathrm{Sets} \\ A &\longmapsto \{\rho\colon G_{\mathbf{Q},T_\Sigma} \longrightarrow \mathrm{GL}_N(A)\colon \rho \text{ deformation of } \rho_0'\} \end{aligned}$$

be the deformation functor relative to ρ_0'. Since $G_{\mathbf{Q},T_\Sigma}$ satisfies the p-finiteness condition (see 1.4.5) for every prime p, the functor $\mathcal{D}_\Sigma$ satisfies the hypothesis of Mazur–Ramakrishna's theorem 2.5.4. Moreover, there is an isomorphism of functors

$$\begin{aligned} \mathcal{D}_{T_\Sigma} &\xrightarrow{\sim} \mathcal{D}_\Sigma \\ (\rho\colon G_{\mathbf{Q},T_\Sigma} \longrightarrow \mathrm{GL}_N(A)) &\longmapsto (\rho \circ \pi\colon G_{\mathbf{Q}} \longrightarrow \mathrm{GL}_N(A)), \end{aligned}$$

where $\pi\colon G_{\mathbf{Q}} \longrightarrow G_{\mathbf{Q},T_\Sigma}$ is the canonical projection. Then up to substitute D_Σ with $\mathcal{D}_{T_\Sigma}$, we can assume the conditions of Mazur–Ramakrishna's theorem are satisfied.

Let us now come back to the concrete situation and let $E/\mathbf{Q}$ be a semistable elliptic curve. Denote by $\rho_{E,p}\colon G_{\mathbf{Q}} \longrightarrow \mathrm{GL}_2(\mathbf{Z}_p)$ the representation attached to the p-adic Tate module of E and by $\bar{\rho}_{E,p}\colon G_{\mathbf{Q}} \longrightarrow \mathrm{GL}_2(\mathbf{F}_p)$ its reductionmod p, i.e. the representation attached to the p-torsion group $E[p]$.

For any prime p, $\bar{\rho}_{E,p}$ satisfies hypothesis (**A**). Indeed, $E[p] \simeq \mathbf{Z}/p\mathbf{Z} \times \mathbf{Z}/p\mathbf{Z}$ and there exists a pairing, called the Weil pairing

$$\begin{aligned} e_p\colon E[p] \times E[p] &\longrightarrow \mu_p \\ (S,T) &\longmapsto \zeta, \end{aligned}$$

which is bilinear, alternating, non-degenerate, Galois-invariant and moreover $e_p(S,T) = e_p(nS,T)$ for every $n \in \mathbf{Z}$, where $\mu_p \subseteq \mathbf{C}$ is the multiplicative group of p-th roots of unity. Then, if we fix a basis (P,Q) of $E[p]$, then necessarily $e_p(P,Q) = \zeta$, where ζ is a primitive p-th root. If we consider now $\sigma \in G_{\mathbf{Q}}$ that acts on $E[p]$ as the matrix $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$, i.e. $\sigma P = aP + cQ$ and $\sigma Q = bP + dQ$, then if ζ is a primitive p-th root we have

$$\begin{aligned} \sigma(\zeta) = \sigma(e_p(P,Q)) = e_p(\sigma P, \sigma Q) = e_p(aP + cQ, bP + dQ) = {}^{8} \\ = e_p(P,Q)^{ad} e_p(Q,P)^{bc} = e_p(P,Q)^{ad-bc} = \zeta^{ad-bc}. \end{aligned}$$

Then by the definition of cyclotomic character, we have that $\sigma(\zeta) = \zeta^{\chi_p(\sigma)}$ and so $\det(\bar{\rho}_{E,p}(\sigma)) = ad - bc = \chi_p(\sigma)$. That completes the prove that condition (**A**) holds.

Since E is semistable then $\bar{\rho}_{E,p}$ is semistable as well. Proving this implication is not easy at all since more advanced tools are needed. However, as we said above the definition of semistable representation is designed such that if E is a semistable elliptic curve then the rappresentation associated with its Tate module is semistable too.

In order to have (**C**) it is enough to ask for the irreducibility of $\bar{\rho}_{E,p}$. In fact, by a theorem of Serre, for $p \geq 3$, $\bar{\rho}_{E,p}$ is either surjective or reducible, and hence, as we will see in the following remark, the absolute irreducibility of $\bar{\rho}_{E,p}$ its equivalent to its irreducibility (see [10]).

[8] Bilinearity and $e_p(P,P) = 1$

Remark 4.3.13. Note that for a representation $\rho\colon G \longrightarrow \mathrm{GL}_2(F)$ over any field F, surjective implies irreducible as being reducible for ρ means that its image is contained in a subgroup conjugate to

$$B(F) = \left\{ \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} : a, b, d \in F \right\},$$

but the converse is in general false. The statement of the theorem of Serre cited above can be therefore red as: for $p \geq 3$, $\bar{\rho}_{E,p}$ is surjective if and only if it is irreducible.

Let us explain moreover why this implies that irreducibility and absolute irreducibility are therefore the same thing for $\bar{\rho}_{E,p}$. If $\bar{\rho}_{E,p}$ is surjective then its image contains matrices that cannot belong to the same $\bar{\mathbf{F}}_p$-conjugate of $B(\bar{\mathbf{F}}_p)$, e.g.

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

In fact suppose that they both belong to $\alpha B(\bar{\mathbf{F}}_p)\alpha^{-1}$, where $\alpha = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}_2(\bar{\mathbf{F}}_p)$. Then the lower-left entry of

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

has to be 0, then both $cd = 0$ and $c^2 = d^2$, but this means that $c = d = 0$, but this contradicts the fact that $\alpha \in \mathrm{GL}_2(\bar{\mathbf{F}}_p)$. This shows that the image of

$$\bar{\rho}_{E,p} \otimes \bar{\mathbf{F}}_p\colon G_{\mathbf{Q}} \xrightarrow{\bar{\rho}_{E,p}} \mathrm{GL}_2(\mathbf{F}_p) \subseteq \mathrm{GL}_2(\bar{\mathbf{F}}_p)$$

is not contained in any conjugate of $B(\bar{\mathbf{F}}_p)$, as we observed this means that $\bar{\rho}_{E,p} \otimes \bar{\mathbf{F}}_p$ is irreducible and so $\bar{\rho}_{E,p}$ is absolutely irreducible.

Similarly as above, for $p = 3$ the irreducibility of $\bar{\rho}_{E,3}$ is equivalent to the absolute irreducibility of $\bar{\rho}_{E,p}|_{G_{\mathbf{Q}(\sqrt{-3})}}$, hence in (**D**) is enough to ask for the modularity condition. Summing all these together Lemma 4.3.11 applied to this concrete case becomes the following one.

Lemma 4.3.14. *Let $E/\mathbf{Q}$ be semistable and suppose that $\bar{\rho}_{E,p}$ is both modular and irreducible for some $p \geq 3$. Then E is modular.*

It's worth explaining a little more why the lemma above is an application of Lemma 4.3.11. Let p be a prime number such that $\bar{\rho}_{E,p}\colon G_{\mathbf{Q}} \longrightarrow \mathrm{GL}_2(\mathbf{Z}/p\mathbf{Z})$ is both modular and irreducible as in the lemma above. Then let us show that the lifting $\rho_{E,p}\colon G_{\mathbf{Q}} \longrightarrow \mathrm{GL}_2(\mathbf{Z}_p)$ is of type $\mathcal{D}_\Sigma$ for a particular set of primes Σ, that we will define. Firstly, $\rho_{E,p}$ has determinant $\chi_p\colon G_{\mathbf{Q}} \longrightarrow \mathbf{Z}_p^*$, as above for $\bar{\rho}_{E,p}$.
Talking about irreducibilty and flatness we have the following result.

Theorem 4.3.15. *Let $E/\mathbf{Q}$ be an elliptic curve. If E is semistable with miminal discriminant Δ_E, then for every prime p the residual representation $\bar{\rho}_{E,p}$ has the following local properties*

- *if $\ell \neq p$ then $\bar{\rho}_{E,p}$ is unramified at ℓ if and only if $p|ord_\ell(\Delta_E)$;*
- *$\bar{\rho}_{E,p}$ is flat at p if and only if $p|ord_p(\Delta_E)$.*

It follows that in our case $S = \{\ell \text{ prime}\colon \ell \neq p, p \nmid ord_\ell(\Delta_E)\}$ and then choosing the set Σ such that it is disjoint from S and contains the remaining prime numbers that divide Δ_E (the ones which are not already contained in S), we have, thanks to Theorem 4.2.14, that $\rho_{E,p}$ is unramified outside $S \cup \{p\} \cup \Sigma$.

Moreover, since our elliptic curve is semistable then the representation $\rho_{E,p}$ is semistable at every prime. In particular it is semistable outside Σ.

Let us now show that if $p \notin \Sigma$ and $\bar{\rho}_{E,p}$ is flat at p then also $\rho_{E,p}$ is flat at p. We have that $p \notin S$ and if $p \notin \Sigma$ then $p \nmid \Delta_E$. Then E has good reduction at p. From algebraic geometry we know that the kernel of an isogeny of degree n of abelian varieties of dimension g is, at a place of good reduction, a finite flat group scheme of order n^{2g} over the local ring of the place. Then, the points of n torsion $E[n]$, which are the kernel of the multiplication by n isogeny of E, are a finite flat group scheme over $\mathbf{Z}_p$. It directly follows that $\rho_{E,p}$ is flat at p, since any ideal of $\mathbf{Z}_p$ is of the form $p^m\mathbf{Z}_p$ for some $m \in \mathbf{N}$ and the representation space of $G_{\mathbf{Q}_p} \longrightarrow \mathrm{GL}_2(\mathbf{Z}_p/(p^m\mathbf{Z}_p))$ is $E[p^m]$, which, as we said, is a finite flat group scheme over $\mathbf{Z}_p$.

Thanks to this discussion we have shown that the lifting $\rho_{E,p}$ satisfies all the conditions to be of type $\mathcal{D}_\Sigma$. Then thanks to Lemma 4.3.11 we can conclude that $\rho_{E,p}$ is modular and then E is modular.

The case $p = 3$ is particularly easy to treat as we have the following lemma.

Lemma 4.3.16 (Laglands-Tunnel)**.** *Let E be an arbitrary elliptic curve and suppose $\bar{\rho}_{E,3}$ irreducible, then it is modular.*

Hence, if $\bar{\rho}_{E,3}$ were irreducible, we would be done. This always almost the case. In fact, by an explicit computation of the rational points of $Y_0(15)$, one has the following.

Theorem 4.3.17. *Let E be a semistable elliptic curve. Then at least one of $\bar{\rho}_{E,3}$ and $\bar{\rho}_{E,5}$ is irreducible.*

In particular, the only thing left to prove is that if $\bar{\rho}_{E,5}$ is irreducible, then it is also modular, as in the case we could apply Lemma 4.3.14 for $p = 5$. This follows by the following theorem.

Theorem 4.3.18. *Let $E/\mathbf{Q}$ be semistable and suppose $\bar{\rho}_{E,5}$ is irreducible, then there is another semistable elliptic curve $E'/\mathbf{Q}$ such that*

(a) *$\bar{\rho}_{E',3}$ is irreducible;*

(b) *$\bar{\rho}_{E',5} \sim \bar{\rho}_{E,5}$.*

Therefore if $\bar{\rho}_{E,5}$ is irreducible, let E' be the elliptic curve given by the previuous theorem: E' is modular by **(a)** and Lemma 4.3.16 and therefore by Remark 4.3.8 $\bar{\rho}_{E',5}$, but then also $\bar{\rho}_{E,5}$ is modular by **(b)** and hence E is modular by Lemma 4.3.14.

This finally concludes our sketch of the proof of the modularity for semistable elliptic curves defined over $\mathbf{Q}$.

4.4 Hecke rings and numerical criterion

In the outline of the proof we used an abstract lemma of deformation theory, Lemma 4.3.11. We will describe now why we introduced this lemma in order to appreciate the cleverness of Wiles ideas.

The starting question is the following: what happens if we restrict our attention only on the modular deformations of type $\mathcal{D} = \mathcal{D}_\Sigma$? In fact, as ρ_0 is modular, there are for sure deformations of ρ_0 that are modular deformations. The answer is that we will get a subfunctor $\mathcal{D}_{\Sigma,\mathrm{mod}}$ of $\mathcal{D}_\Sigma$, which will be still representable and hence we will get a *universal modular deformation ring* $\mathbb{T}_\mathcal{D}$ and a *universal modular deformation* $\rho_{\mathcal{D},\mathrm{mod}} \colon G_\mathbf{Q} \longrightarrow \mathrm{GL}_2(\mathbb{T}_\mathcal{D})$ characterized by the analogous universal property: each modular deformation ρ of ρ_0 factors trough $\mathrm{GL}_2(\mathbb{T}_\mathcal{D})$ via $\rho_{\mathcal{D},\mathrm{mod}}$.

Now one has only to make a little observation to go further: if all representations of type $\mathcal{D}$ were modular, as we would like to show, there would be no difference between $R_\mathcal{D}$ and $\mathbb{T}_\mathcal{D}$. Indeed, thanks to their universal properties, there would be two unique homomorphisms, let us say $f \colon R_\mathcal{D} \longrightarrow \mathbb{T}_\mathcal{D}$ and $g \colon \mathbb{T}_\mathcal{D} \longrightarrow R_\mathcal{D}$ such that $\rho_{\mathcal{D},\mathrm{mod}} = f \circ \rho_\mathcal{D}$ and $\rho_\mathcal{D} = g \circ \rho_{\mathcal{D},\mathrm{mod}}$, but then substituting in the first equality we get $\rho_{\mathcal{D},\mathrm{mod}} = f \circ g \circ \rho_{\mathcal{D},\mathrm{mod}}$ from which, by uniqueness, $f \circ g$ must be the identity map of $R_\mathcal{D}$. Similarly, $g \circ f$ must be the identity map of $\mathbb{T}_\mathcal{D}$. Therefore $R_\mathcal{D}$ and $\mathbb{T}_\mathcal{D}$ would be isomorphic.

The vice versa holds, too, as then any deformation of type $\mathcal{D}$ would factorize through $\rho_{\mathcal{D},\mathrm{mod}}$ that is modular and hence would be itself modular. In other terms, lemma 4.3.11 is equivalent to the following theorem.

Theorem 4.4.1. *Let $\phi_{\mathcal{D}}\colon R_{\mathcal{D}} \longrightarrow \mathbb{T}_{\mathcal{D}}$ be the canonical morphism whose existence is ensured by the universal property of $\rho_{\mathcal{D}}$, namely the unique morphism such that $\rho_{\mathcal{D},mod} = \phi_{\mathcal{D}} \circ \rho_{\mathcal{D}}$. Suppose ρ_0 satisfies hypothesis **(A)-(D)**, then $\phi_{\mathcal{D}}$ is an isomorphism.*

Wiles proved a slightly stronger version of the previous theorem giving also the structure of the rings $R_{\mathcal{D}}$ and $\mathbb{T}_{\mathcal{D}}$; they are complete intersection rings[9]. Its proof makes use of the following criterion, the so called numerical criterion.

Theorem 4.4.2. *Let R, T be coefficient rings, $\mathcal{O}$ a complete discrete valuation ring and suppose to have a commutative diagram:*

$$\begin{array}{ccc} R & \xrightarrow{\quad\phi\quad} & T \\ & {\scriptstyle\pi_R}\searrow \quad \swarrow{\scriptstyle\pi_T} & \\ & \mathcal{O} & \end{array}$$

with all surjective arrows. Let $I_R = \ker(\pi_R)$, $I_T = \ker(\pi_T)$ and $\eta_T = \pi_T(\mathrm{Ann}_T(I_T))$. Then the following three assertions are equivalent:

(1) *ϕ is an isomorphism of complete intersection rings;*

(2) *I_R/I_R^2 is finite and $|(I_R/I_R^2)| \leq |\mathcal{O}/\eta_T|$;*

(3) *I_R/I_R^2 is finite and $|(I_R/I_R^2)| = |\mathcal{O}/\eta_T|$.*

Wiles used it in the following setting: suppose that f is a weight two newform and that its representation $\rho_{f,\lambda}\colon G_{\mathbf{Q}} \longrightarrow \mathrm{GL}_2(\mathcal{O}_{f,\lambda})$ is a deformation of ρ_0 of type $\mathcal{D}$ (it exists since ρ_0) is modular. By the universal property of $\mathbb{T}_{\mathcal{D}}$ there is a unique morphism $\pi_{\mathbb{T}_{\mathcal{D}}}\colon \mathbb{T}_{\mathcal{D}} \longrightarrow \mathcal{O}_{f,\lambda}$ such that $\rho_{f,\lambda} = \pi_{\mathbb{T}_{\mathcal{D}}} \circ \rho_{\mathcal{D},\mathrm{mod}}$. Define $\pi_{R_{\mathcal{D}}} = \pi_{\mathbb{T}_{\mathcal{D}}} \circ \phi_{\mathcal{D}}$, so that we have the commutative diagram

$$\begin{array}{ccc} R_{\mathcal{D}} & \xrightarrow{\quad\phi_{\mathcal{D}}\quad} & \mathbb{T}_{\mathcal{D}} \\ & {\scriptstyle\pi_{R_{\mathcal{D}}}}\searrow \quad \swarrow{\scriptstyle\pi_{\mathbb{T}_{\mathcal{D}}}} & \\ & \mathcal{O}_{f,\lambda} & \end{array} .$$

[9] A complete intersection local ring is a Noetherian local ring whose completion is the quotient of a regular local ring by an ideal generated by a regular sequence

By the numerical criterion to establish Theorem 4.4.1 it is enough to prove the inequality (2) above. The proof of this crucial numerical inequality divides into two parts. The case where $\Sigma = \emptyset$, which is called the *minimal case*, was proved by Wiles and Taylor (see [2]). The *non-minimal case* is proved by induction on the number of primes in Σ. The proof shows as certain groups and modules grow as Σ is enlarged to conclude that if the numerical inequality is satisfied for one $\mathcal{D}_\Sigma$ then it is also satisfied when more primes are included in Σ.

4.5 Representability of $\mathcal{D}_\Sigma$

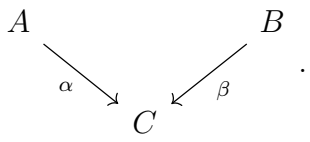
In this section we will discuss the representability of the subfuctor $\mathcal{D}_\Sigma$, introduced in Definition 4.3.10, providing a sketch of proof. We'll introduce the concept of *deformation conditions* for a subfunctor of the deformation functor and show that the conditions $\mathcal{D}_\Sigma$ are indeed deformation conditions and that this makes the subfuctor $\mathcal{D}_\Sigma$ to be representable.

Let us fix our background. First of all, recall that Remark 1.5.12 tells us that we can give a Galois representation defining a linear action of the Galois group on a module of finite rank over a topological ring. From now on, we will use this definition of representation that can be clearly extended to all profinite groups.

Let N be a natural number, $N \geq 1$, Π a profinite group and Λ a coefficient ring. Moreover, let us define the category $F_N = F_N(\Lambda; \Pi)$, whose objects are pairs (A, V) consisting of an artinian coefficient Λ-algebra A and a free A-module V of rank N endowed with an A-linear continuous Π-action. A morphism in F_N from an object (A, V) to an object (A_1, V_1) consists of a pair of morphisms $A \longrightarrow A_1$ (of artinian coeffiecient Λ-algebras) and $V \longrightarrow V_1$ (of A-modules) inducing an isomorphism of A-modules $V \otimes_A A_1 \simeq V_1$, which is compatible with the Π-action. Consider now the following three conditions on a full subcategory $\mathcal{D}F_N \subseteq F_N$:

(1) for any morphism $(A, V) \longrightarrow (A_1, V_1)$ in F_N, if (A, V) is an object of $\mathcal{D}F_N$ then so is (A_1, V_1);

(2) let A, B, C be artinian coefficients Λ-algebras fitting into the following diagram



Consider an object $(A \times_C B, V)$ in F_N and let V_A and V_B denote the tensor products of V with respect to the natural projections from $A \times_C B$ to A and B respectively. Then $(A \times_C B, V)$ is an object in $\mathcal{D}F_N$ if and only if both (A, V_A) and (B, V_B) are objects of $\mathcal{D}F_N$;

(3) for any morphism $(A, V) \longrightarrow (A_1, V_1)$ in F_N, if (A_1, V_1) is an object of $\mathcal{D}F_N$ and $A \longrightarrow A_1$ is injective, then (A, V) is an object of $\mathcal{D}F_N$.

Definition 4.5.1. Fix Λ and Π as before and a continuous residual representation

$$\bar{\rho}\colon \Pi \longrightarrow \mathrm{GL}_N(k).$$

We denote by $\bar{V}$ the N-dimensional k-vector space k^N with k-linear action given by $\bar{\rho}$. By a *deformation condition* $\mathcal{D}$ for $\bar{\rho}$, we mean a full subcategory $\mathcal{D}F_N \subseteq F_N$ satisfying (**1**)-(**3**) containing $(k, \bar{V})$ as object.

Suppose that we are given a deformation condition $\mathcal{D}F_N \subseteq F_N$. For a coefficient Λ-algebra A and a homomorphism

$$\rho\colon \Pi \longrightarrow \mathrm{GL}_N(A)$$

lifting $\bar{\rho}$, let $V(\rho)$ be the free A-module A^N with a Π-action given by ρ. If $(A, V(\rho))$ is in $\mathcal{D}F_N$ then we will say that ρ is of type $\mathcal{D}$, and its strict equivalence class is a deformation of $\bar{\rho}$ type $\mathcal{D}$. Define then a subfunctor

$$\mathcal{D}_\rho \subseteq D_\rho\colon \mathcal{C}_\Lambda(A) \longrightarrow \mathrm{Sets}$$

by the following rule: for any artinian A-augmented[10] coefficient Λ-algebra B and element $\xi \in D_\rho(B)$ representing a strict equivalence class of lifting ρ_1 relative to ρ to B then ξ is in the subset $\mathcal{D}_\rho(B) \subseteq D_\rho(B)$ if and only if ρ_1 is of type $\mathcal{D}$. We now discuss the representability of $\mathcal{D}_\rho$.

Proposition 4.5.2. *If $\mathcal{D}$ is a deformation condition for $\bar{\rho}$, and the representation $\rho\colon \Pi \longrightarrow \mathrm{GL}_N(A)$ is a deformation of $\bar{\rho}$, then the subfunctor $\mathcal{D}_\rho$ is relatively representable*[11]*.*

Corollary 4.5.3. *If $\mathcal{D}$ is a deformation condition for $\bar{\rho}$ and the functor $\mathcal{D}_{\bar{\rho}}$ (on $\mathcal{C}_\Lambda$) satisfies hypothesis $(\mathbf{H_1}), (\mathbf{H_2}), (\mathbf{H_3})$ defined in Theorem 2.4.4, then the functor $\mathcal{D}_\rho$ has a pro-representable hull. For ρ any lifting of $\bar{\rho}$ the functor $\mathcal{D}_\rho$ is nearly representable. If $\bar{\rho}$ is absolutely irreducibile then $\mathcal{D}_{\bar{\rho}}$ is pro-representable by a quotient ring of the ring pro-representing $D_{\bar{\rho}}$.*

[10] For the definition of A-augemntation see Remark 2.2.7.

[11] For the definition of relatively representable functor see Definition 2.4.12.

Now we would like to use the strong theoretical results above for our concrete case. More precisely, we would like to sketch a proof that the conditions $\mathcal{D}_\Sigma$ introduced in section 4.3.1 are indeed deformation conditions for every set of primes Σ. This way, since our residual representation $\rho_0 \colon G_{\mathbf{Q}} \longrightarrow \mathrm{GL}_2(k)$ is fixed to be absolute irreducibile, then by Corollary 4.5.3 the subfunctor $\mathcal{D}_\Sigma$ is pro-representable, i.e. there exists a universal coefficient ring $R_{\mathcal{D}_\Sigma}$ and a universal deformation $\rho_{\mathcal{D}_\Sigma} \colon G_{\mathbf{Q}} \longrightarrow \mathrm{GL}_2(R_{\mathcal{D}_\Sigma})$ such that all the deformations of ρ_0 of type $\mathcal{D}_\Sigma$ factor through $\rho_{\mathcal{D}_\Sigma}$.

The first condition of $\mathcal{D}_\Sigma$ asks deformations ρ of ρ_0 to have fixed determinant χ_p. The following result holds.

Proposition 4.5.4. *The condition $\mathcal{D}$ of being of fixed determinant is a deformation condition. Moreover, if $\rho \colon \Pi \longrightarrow \mathrm{GL}_N(A)$ is a continuous homomorphism that satisfies the fixed determinant condition and $V = V(\rho)$ we have*

$$H^1_{\mathcal{D}}(\Pi, \mathrm{End}_A(V)) = H^1(\Pi, \mathrm{End}^0_A(V)) \subset H^1(\Pi, \mathrm{End}_A(V)),$$

where $\mathrm{End}^0_A(V) \subset \mathrm{End}_A(V)$ is the sub-A-module of endomorphisms whose trace is zero and we will define $H^1_{\mathcal{D}}(\Pi, \mathrm{End}_A(V))$ in the following remark. The sub-A-module $\mathrm{End}^0_A(V)$ is stable under the action of Π, the cohomology group $H^1(\Pi, \mathrm{End}^0_A(V))$ being computed with respect to this action.

Proof. See [2, Chapter 8, Section 24]. □

Remark 4.5.5. Corollary 4.5.3 assures that the functor $\mathcal{D}_\rho$ is nearly representable, i.e. it satfisfies the tangent space hypothesis. Then it makes sense to consider the tangent A-module to $\mathcal{D}_\rho$ which is a sub-module of t_ρ (the tangent A-module to D_ρ) and denote it $t_{\mathcal{D},\rho} \subseteq t_\rho$. Moreover, since we showed in chapter 3 that we can identify t_ρ with the cohomology group $H^1(\Pi, \mathrm{End}_A(V))$, then the sub-$A$-module $t_{\mathcal{D},\rho}$ is identified with some sub-A-module of $H^1(\Pi, \mathrm{End}_A(V))$. Let us call this sub-$A$-module $H^1_{\mathcal{D}}(\Pi, \mathrm{End}_A(V))$, which finally explains the notation of the proposition above.

The second condition of $\mathcal{D}_\Sigma$ asks the deformation ρ to be unramified outside the set $S \cup \Sigma \cup \{p\}$, where p is the characteristic of the residue field k, S is the set of primes $\ell \neq p$ at which the residual representation ρ_0 is ramified and Σ is a finite set of primes disjoint by S. As above we have the following result.

Proposition 4.5.6. *Let $\bar{\rho} \colon \Pi \longrightarrow \mathrm{GL}_N(k)$ be a residual representation unramified at $\ell \neq p$, where p is the characteristic of k. The condition of being unramified at $\ell \neq p$ is a deformation condition.*

Sketch of proof. The proof directly follows from checking one by one the conditions (**1**)-(**3**) which define the subcategory $\mathcal{D}F_N$ introduced above. We will just check condition (**1**) since the proof of the other two is very similar.

Let $\ell \neq p$ be a prime such that $\bar{\rho}$ is unramified at p. Let $(A, A^N) \longrightarrow (A_1, A_1^N)$ be a morphism in the category $F_N(\Lambda; G_{\mathbf{Q}})$. Moreover, let $\rho\colon G_{\mathbf{Q}} \longrightarrow \mathrm{GL}_N(A)$, $\rho_1\colon G_{\mathbf{Q}} \longrightarrow \mathrm{GL}_N(A_1)$ be the correspondent representations. Suppose that ρ is unramified at ℓ, namely $\rho(I_\ell) = 1$, the identity matrix. Then, since morphisms between ρ and ρ_1 corresponds to unitary Λ-algebra coefficient ring homomorphism between A and A_1, $\rho_1(I_\ell) = 1$ and so ρ_1 is unramified at ℓ, too. This shows that condition (**1**) is verified. □

The third condition of $\mathcal{D}_\Sigma$ that ρ must satisfy is to be semsistable outside the set of primes Σ. This can be proved to be a deformation condition as well. Indeed, from Definition 4.3.1, ρ is semistable at a prime ℓ if for $\ell = p$, ρ is either flat or ordinary at p and for $\ell \neq p$, $\rho|_{I_\ell} \simeq \begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix}$. In order to understand this last condition let us give the following definition.

Definition 4.5.7. Let $\bar{\rho}\colon G_{\mathbf{Q}} \longrightarrow \mathrm{GL}_2(k)$ be a residual representation, with k a finite field of characteristic $p \neq \ell$. Then

(A) suppose that the image of the inertia group $I_\ell \subseteq G_{\mathbf{Q}}$ under $\bar{\rho}$ is non trivial and it is contained in a subgroup of $\mathrm{GL}_2(k)$ which is conjugate to $\begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix}$. We say that a deformation ρ of $\bar{\rho}$ to a coefficient ring A with residue field k is *minimally ramified* if the image of I_ℓ under ρ is contained in a subgroup of $\mathrm{GL}_2(A)$ which is conjugate to $\begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix}$;

(B) suppose that the image of the inertia group I_ℓ under $\bar{\rho}$ is non zero, and it is contained in a subgroup of $\mathrm{GL}_2(k)$ which is conjugate to $\begin{pmatrix} * & 0 \\ 0 & 1 \end{pmatrix}$. We say that a deformation ρ of $\bar{\rho}$ to a coefficient ring A with residue field k is *minimally ramified* if the image of I_ℓ under ρ is finite and of order prime to p (or equivalently if $\rho(I)$ is finite and has the same order as $\bar{\rho}(I)$).

Then we have the following result.

Proposition 4.5.8. *Fix Λ a coefficient ring with finite residue field k of characteristic $p \neq \ell$. For any coefficient Λ-algebra A, let $\mathcal{D}$ be the condition on a representation $\rho\colon G_{\mathbf{Q}} \longrightarrow \mathrm{GL}_2(A)$ that its associated residual representation $\bar{\rho}\colon G_{\mathbf{Q}} \longrightarrow \mathrm{GL}_2(k)$ be*

*minimally ramified at ℓ, either in the sense of **(A)** or of **(B)** above, and that ρ itself be correspondingly minimally ramified. Then $\mathcal{D}$ is a deformation condition.*

Proof. Once again the proof directly follows from checking one by one the conditions (**1**)-(**3**) which define the subcategory $\mathcal{D}F_N$ introduced above. Indeed, as Proposition 4.5.6, the proof bases on the fact that morphism between representations correspond to unitary Λ-algebra coeffiecient ring homomorphisms. □

Then, since semistability for $\ell \neq p$ coincides with case (**A**) of the definition, the proposition above shows that it is indeed a deformation condition.

We have then left to analyze the case $\ell = p$ and the condition or being either flat or ordinary at it.

The flatness at p is a *categorical condition* in the following sense. Fix, as usual, a coefficient ring Λ and a profinite group Π. Let $\mathrm{Rep}_\Lambda(\Pi)$ denote the category of Λ-modules of finite length which are endowed with a continuous and Λ-linear action of Π. A full subcategory $\mathcal{P}$ of $\mathrm{Rep}_\Lambda(\Pi)$, which is closed under passage to subojects, quotients and direct sums determined a deformation condition, as is shown in the following proposition.

Proposition 4.5.9. *Let $\mathcal{P}$ be a full subcategory of $\mathrm{Rep}_\Lambda(\Pi)$ closed under subojects, quotients and direct sums. For any N positive integer let $\mathcal{P}F_N$ denote the full subcategory of F_N (defined at the beginning of this section) consisting of those objects (A, V) such that V, viewed as Λ-linear representation of Π, lies in $\mathcal{P}$. Then $\mathcal{P}F_N$ is a deformation condition.*

Proof. See [2, Chapter 8, Section 25, Proposition 1]. □

The condition of being flat at p satisfies the passage to subojects, quotients and direct sums and hence it is a deformation condition.
The ordinarity at p is a deformation condition, too. It can be treated in a very similar way to part **(B)** of Definition 4.5.7. Indeed, we can give the following general definition.

Definition 4.5.10. Let Π be a profinite group and let $I \subseteq \Pi$ be a closed subgroup. Consider a representation $\rho\colon \Pi \longrightarrow \mathrm{GL}_2(A)$, where A is a coefficient ring with residual field k. Suppose then that ρ is equivalent to a representation of the form

$$g \longmapsto \begin{pmatrix} \chi_1(g) & * \\ 0 & \chi_2(g) \end{pmatrix}$$

for characters $\chi_1,\ \chi_2\colon \Pi \longrightarrow A^*$ such that the residual character $\bar{\chi}_1\colon \Pi \longrightarrow k^*$ is non trivial on I and χ_2 is trivial on I. We will say that ρ is *I-ordinary* and if the subgroup I is understood we will just say that ρ is *ordinary*.

The following result holds.

Proposition 4.5.11. *Fix a profinite group Π and fix a closed normal subgroup $I \subseteq \Pi$. If $\mathcal{D}$ is the class of I-ordinary representations of Π, then $\mathcal{D}$ is a deformation condition.*

Proof. See [2, Chapter 8, Section 30, Propostion 3]. □

In our concrete case the profinite group Π coincides with the absolute Galois group $G_{\mathbf{Q}}$ and the subgroup I with the inertia group I_p. By Definition 4.3.2 we know that the condition of being ordinary at p means that the restriction of the representation ρ to I_p is equivalent to one of the form $\begin{pmatrix} \chi_p & * \\ 0 & 1 \end{pmatrix}$. But then, we know that the cyclotomic character $\chi_p\colon G_{\mathbf{Q}} \longrightarrow (\mathbf{Z}/p\mathbf{Z})^* \hookrightarrow k^*$ is ramified at p, which means that $\chi_p(I_p)$ is not trivial. Moreover, we can see 1 as the trivial character $\mathbf{1}\colon G_{\mathbf{Q}} \longrightarrow A^*$, sending all the elements of $G_{\mathbf{Q}}$ to $1 \in A^*$. Then, provided that the representation ρ is equivalent to one of the form of Definition 4.5.10, the condition of being ordinary at p can be translated into the condition of being I_p-ordinary, which thanks to the proposition above is a deformation condition.

We have then shown that all the conditions $\mathcal{D}_\Sigma$ of Section 4.3.1 are indeed deformation conditions. Moreover, since the intersection of deformation conditions is a deformation condition, the existence of the universal ring $R_{\mathcal{D}_\Sigma}$ directly follows from Corollary 4.5.3.

4.6 The universal deformation modular ring $\mathbb{T}_{\mathcal{D}}$

In this section we will give a sketch of the explicit construction of the universal modular ring $\mathbb{T}_{\mathcal{D}}$ introduced in Section 4.4.
Let us once again fix a residual representation

$$\bar{\rho}\colon G_{\mathbf{Q}} \longrightarrow \mathrm{GL}_2(k)$$

where k is a finite field of characteristic p. Let us moreover assume that:

(a) p is odd;

(b) $\bar{\rho}$ is irreducible;

(c) the restriction of $\bar{\rho}$ to a decomposition group at p is finite flat or ordinary;

(d) $\bar{\rho}$ has cyclotomic determinant.

(e) $\bar{\rho}$ has square-free conductor;

(f) $\bar{\rho}$ is modular.

In order to understand condition (**e**), we have to introduce an idea of the notion of conductor of a Galois representation. Let p be a prime number and let us consider the inertia subgroup $I_p \subseteq G_{\mathbf{Q},p}$. Then, one can consider the *higher ramification groups*[12] and build the filtration $\{I_p^u \colon u \in [-1,\infty]\}$ of I_p made up by them. We have that:

- $I_p^u \trianglelefteq G_{\mathbf{Q},p}$ and I_p^u is closed for every $u \in [-1,\infty]$;
- if $u \leq v$ then $I_p^u \supseteq I_p^v$;
- if $u \leq 0$ then $I_p^u = I_p$ and $I_p^\infty = \{1\}$.

We can now give the definition of conductor of a representation.

Definition 4.6.1. Let N be a positive integer, A a topological ring and $\rho \colon G_{\mathbf{Q}} \longrightarrow \mathrm{GL}_N(A) \subseteq \mathrm{GL}_N(F)$ a continuous representation where F is the fraction field of A. The conductor of ρ is

$$N(\rho) = \prod_{\substack{\ell \text{ prime} \\ \ell \neq p}} \ell^{n_\ell(\rho)}$$

where

$$n_\ell(\rho) = \mathrm{codim}(V(\rho)^{I_\ell}) + \int_{-1}^{\infty} \mathrm{codim}(V(\rho)^{I_\ell^u})\, du$$

and $V(\rho)^{I_\ell}$ and $V(\rho)^{I_\ell^u}$ indicate the representation space of ρ fixed by I_ℓ and I_ℓ^u respectively and where we define $\mathrm{codim}(V(\rho)^{I_\ell}) = \dim_F V(\rho) - \dim_F V(\rho)^{I_\ell}$ and $\mathrm{codim}(V(\rho)^{I_\ell^u}) = \dim_F V(\rho) - \dim_F V(\rho)^{I_\ell^u}$. Moreover, the integral in the sum is defined as

$$\int_{-1}^{\infty} \mathrm{codim}(V(\rho)^{I_\ell^u})\, du = \lim_n \sum_{i=1}^{n} \mathrm{codim}\, V(\rho)^{I_\ell^{u_i^*}} \Delta u_i,$$

where we have that $-1 = u_1 < u_2 < u_3 < \dots$ is a partition of $[-1,\infty]$, $\Delta_i = u_i - u_{i-1}$ and $u_i^* \in [u_i, u_{i-i}]$.

[12] For the defintion of higher ramification groups see [12].

Remark 4.6.2. The number $n_\ell(\rho)$ introduced in the definition above is an integer. Moreover, recall that a Galois representation can be ramified only at a finite number of primes. It follows that the action of the inertia group on the representation space can be no non-trivial only at a finite number of primes. Hence, $\mathrm{codim}(V(\rho)^{I_\ell})$ and $\mathrm{codim}(V(\rho)^{I_\ell^u})$ are zero for almost every prime ℓ. Therefore, $N(\rho)$ is a product of a finite numbers of factors.

Let now Σ be a finite set of primes. For the application of modularity to semistable elliptic curves, it is sufficient to give a preliminary definition of type Σ in terms of the conductors $N(\bar{\rho})$ and $N(\rho)$ where ρ is a deformation of $\bar{\rho}$. We say that ρ is of *type* Σ if Σ contains the set of prime divisors of $N(\rho)/N(\bar{\rho})$, which can be proved to be an integer. In order to have an idea of why this definition of Σ is sufficient, it is useful to recall why Lemma 4.3.14 was an application to semistable elliptic curves of the more general Lemma 4.3.11. It's not difficult to understand that if $\bar{\rho} = \bar{\rho}_{E,p}$, then the only primes dividing $N(\bar{\rho})$ can be the ones contained in S thanks to Theorem 4.3.15 (because for all the primes $\ell \notin S$, I_ℓ has trivial image under $\bar{\rho}$ and then $\mathrm{codim}(V(\bar{\rho})^{I_\ell}) = 0$). Similarly, the only primes dividing $N(\rho)$ can be the ones dividing the discriminant Δ_E since ρ is ramified only at them. Then because $N(\rho)/N(\bar{\rho})$ is an integer, $(\prod_{\ell|\Delta_E} \ell)/(\prod_{\ell' \in S} \ell')$ must be an integer, too. Hence, by choosing Σ as the set of prime divisors of $N(\rho)/N(\bar{\rho})$, we obtained the same exact definition of Σ previously given for the case of semistable elliptic curves.

Given this finite set of primes Σ, we wonder then which newforms of weight two can give rise to a representation of type Σ.

Remark 4.6.3. Suppose that f is a newform of weight two, trivial character and level N_f and let K_f denote the number field generated by its coefficient $a_n(f)$, then the choice of the embeddings $\bar{\mathbf{Q}} \hookrightarrow \bar{\mathbf{Q}}_p$ and $\bar{\mathbf{Q}} \hookrightarrow \mathbf{C}$ determines a prime λ of $\mathcal{O}_f$, the ring of integers of K_f. Indeed, for the primitive element theorem, $K_f = \mathbf{Q}[\alpha]$ for some $\alpha \in \bar{\mathbf{Q}}$, then, depending on the previous embeddings, $\mathbf{Q}[\alpha] \hookrightarrow \mathbf{Q}_p[\alpha']$ for some $\alpha' \in \bar{\mathbf{Q}}_p$ and that there exists a maximal ideal λ of $\mathbf{Q}[\alpha]$ such that the completion $\mathbf{Q}[\alpha]_\lambda \simeq \mathbf{Q}_p[\alpha']$. From now on, we will fix this ideal $\lambda \subseteq \mathcal{O}_f$.

The following lemma gives sufficient conditions for a new form of weight two to give rise to a representation of type Σ.

Lemma 4.6.4. *Let f be a newform of weight two and level N_f and consider the attached Galois representation $\rho_{f,\lambda} \colon G_{\mathbf{Q}} \longrightarrow \mathrm{GL}_2(K_{f,\lambda})$. Then $\rho_{f,\lambda}$ is of type Σ if the following conditions hold*

- $\bar{\rho}_{f,\lambda} \sim \bar{\rho}$;

- *the character* $\chi_{\rho_{f,\lambda}}$ *of* ρ_f *is trivial;*
- N_f *divides* $N_\Sigma = N(\bar{\rho}) \prod_{\ell \in \Sigma} \ell^{m_\ell}$ *where* m_ℓ *are defined as follows:*
  - $m_\ell = 2$ *if* ℓ *does not divide* $pN(\bar{\rho})$*;*
  - $m_\ell = 1$ *if* $\ell \neq p$ *and* ℓ *divides* $N(\bar{\rho})$*;*
  - $m_p = 1$ *if* $\bar{\rho}$ *is finite flat and ordinary at* p*;*
  - $m_p = 0$ *otherwise.*

Remark 4.6.5. The motivation for this definition of N_Σ is that this condition is known to be necessary as well as sufficient, as long as we restrict our attention to forms f with trivial character and and level not divisible by p^2.

Let now Φ_Σ denote the set of newforms f of weight two, trivial character and level dividing N_Σ. One can prove that for every Σ, the set Φ_Σ is not empty. Therefore, we can consider the ring

$$\tilde{\mathbb{T}}_\Sigma \coloneqq \prod_{f \in \Phi_\Sigma} \mathcal{O}_{f,\lambda},$$

where $\mathcal{O}_{f,\lambda}$ is the ring of integers of $K_{f,\lambda}$, the completion of K_f with respect to the prime λ of $\mathcal{O}_f$.

Remark 4.6.6. The ring $\tilde{\mathbb{T}}_\Sigma$ is semi-local[13] and finitely generated as a $\mathbf{Z}_p$-module.

For each prime $\ell \notin \Sigma$, let T_ℓ denote the element $(a_\ell(f))_{f \in \Phi_\Sigma}$. We define the *Hecke algebra* $\mathbb{T}_\Sigma$ as the $\mathbf{Z}_p$-subalgebra generated by the elements T_ℓ for $\ell \notin \Sigma \cup \{p\}$.

Remark 4.6.7. The ring $\mathbb{T}_\Sigma$ is well defined since if $\ell \notin \Sigma \cup \{p\}$, then $a_\ell(f) \in \mathcal{O}_{f,\lambda}$ for every $f \in \Phi_\Sigma$. Indeed, Theorem 4.1.9 tells us that the Galois representation $\rho_{f,\lambda}$ attached to f is unramified outside the primes dividing pN_f. Then, since $N(\rho)$ is the prime-to-p part of N_f (see [3, Thorem 3.1]), Theorem 4.7.5 states that $\bar{\rho}_{f,\lambda}$ is ramified only at p and $N(\bar{\rho})/N(\rho)$ is an integer, it's not difficult to understand that if $\ell \notin \Sigma \cup \{p\}$ then $\ell \nmid pN_f$. Moreover, one can choose a basis such that the image of the Galois representation $\rho_{f,\lambda}$ attached to f is contained in $\mathrm{GL}_2(\mathcal{O}_{f,\lambda})$. Then, thanks again to Theorem 4.1.9, we know that if $\ell \nmid pN_f$ then $\mathrm{tr}_{\rho_{f,\lambda}}(\mathrm{Frob}_\ell) = a_\ell(f)$. Hence we can conclude that if $\ell \notin \Sigma$ then $a_\ell(f) \in \mathcal{O}_{f,\lambda}$.

One could give another description of $\mathbb{T}_\Sigma$ in terms of the subring $\mathbb{T}$ of the ring of endomorphisms of $S = S_2(\Gamma_0(N_\Sigma))$ generated by the operators T_q for all primes q. We suppose that $f \in \Phi_\Sigma$ and we defined f_Σ as a certain $\mathbb{T}$-eigenform in S for which f is the associated newform. The eigenform f_Σ is characterized by these properties:

[13] A ring is said semilocal if has if it has finitely many maximal ideals.

- if $\ell \in \Sigma \setminus \{p\}$, then $a_\ell(f_\Sigma) = 0$;
- if $p | N_\Sigma$ then $a_p(f_\Sigma)$ is a p-adic unit.

The map sending T_ℓ to the reduction of $a_\ell(f_\Sigma)$ defines an homorphism $\mathbb{T} \longrightarrow \bar{\mathbf{F}}_\ell$, and we write $\mathbb{T}_m$ for the completion of $\mathbb{T}$ at the kernel m of this homomorphism. We then have the following lemma.

Lemma 4.6.8. *If $q \notin \Sigma$, then the element T_q of $\tilde{\mathbb{T}}_\Sigma$ is in $\mathbb{T}_\Sigma$. For arbitrary Σ there is an isomorphism $\mathbb{T}_m \simeq \mathbb{T}_\Sigma$, such that $T_q \longmapsto T_q$ for all $q \notin \Sigma$.*

Proof. See [3, Chapter 4]. □

4.7 Modularity implies Fermat's Last Theorem

The modularity theorem has a very important application in algebraic number theory: it is the main tool used for the proof of Fermat's Last Theorem, one of the longest open problem in Mathematics. Indeed, Wiles and Taylor's proof of the modularity theorem for semistable elliptic curves (1993-1995, see the original articles of Wiles [16] and Taylor [15]) directly implies Fermat's Last Theorem. It was the German mathematician Gerhard Frey that in 1986 suggested this important implication. He showed that any counterexample of Fermat's Last Theorem would imply the existence of at least one non-modular elliptic curve, contradicting the modularity conjecture.

In this section we will then show how the implication 'modularity theorem $\Longrightarrow$ Fermat's Last Theorem concretely works, arriving to the contradiction found by Frey.

Let us first of all state Fermat's Last Theorem (FLT).

Theorem 4.7.1 (FLT)**.** *The equation (F_n): $x^n + y^n = z^n$, where n is a natural number, $n \geq 3$, has no non trivial solutions $a, b, c \in \mathbf{Z}$ such that $abc \neq 0$.*

First of all note that it is enough to prove FLT for $n = p$ an odd prime, as if $n = mp$ and (F_n) has a solution $(a, b, c) \in \mathbf{Z}^3$, then (a^m, b^m, c^m) is a solution of (F_p). Suppose then by contradiction that (F_p) has a nontrivial solution, then since p is odd also the equation $(F'_p) : a^p + b^p + c^p = 0$ has a no non trivial solution. Moreover, the following lemma holds.

Lemma 4.7.2. *Let $(a, b, c) \in \mathbf{Z}^3$ be a solution of (F'_p) for an odd prime p. Then we can assume without loss of generality that $a \equiv -1$ modulo 4 and b is even.*

Proof. We know that exactly one of a, b and c must be even, as if two of them were even the third would be even, too, but then 2 would be a common factor. Thus at least two of them must be odd, but then the other one must be even. Permuting a, b and c, fix the even one to be b. But then we have two possibilities: $a \equiv 1 \bmod 4$ or $a \equiv -1 \bmod 4$, but in the former case we may change the sign of the triple (a, b, c), as in this way it is still a solution of (F'_p). □

4.7.1 Frey curves

Now we make the crucial construction. Let A, B and C be a triple of integers with no common factors such that $A + B + C = 0$ and consider the curve

$$E_{A,B,C} \colon y^2 = x(x - A)(x - B).$$

It is an elliptic curve respectively of discriminant and j-invariant:

$$\Delta = 16(ABC)^2 \text{ and } j = 2^8 \frac{(A^2 + B^2 + AB)^3}{(ABC)^2}.$$

If we suppose $A \equiv 1 \bmod 4$ and $B \equiv 0 \bmod 16$, the the change of coordinates

$$\begin{cases} u = 4x \\ v = 8y + 4x \end{cases}$$

shows that $E_{A,B,C}$, has a model defined by the equation

$$v^2 + uv = u^3 + \frac{(B - A - 1)}{4}u^2 - \frac{AB}{16}u$$

that can be proved to be a minimal Weierstrass equation (for all primes!). Furthermore, from this equation and the original one one can see that this elliptic curve is semistable. In particular if $A = a^p$, $B = b^p$ and $C = c^p$ we get the following theorem.

Theorem 4.7.3. *Let $p \geq 5$, $\gcd(a, b, c) = 1$ and assume $a \equiv -1 \bmod 4$ and b even. If $a^p + b^p + c^p = 0$, the E_{a^p,b^p,c^p} is a semistable elliptic curve defined over $\mathbf{Q}$ with minimal discriminant*

$$\Delta_{a^p,b^p,c^p} = 2^{-8}(abc)^{2p}$$

and conductor

$$N_{a^p,b^p,c^p} = \prod_{\substack{\ell \text{ prime} \\ \ell | abc}} \ell.$$

Moreover, $\bar{\rho}_{E_{a^p,b^p,c^p},p}$ is odd and absolutely irreducible.

Remark 4.7.4. Recalling the Definition 4.2.8 of algebraic conductor of an elliptic curve, it is immediate to see that E_{a^p,b^p,c^p} is semistable.

Using Wiles's theorem 4.3.1, we can deduce that E_{a^p,b^p,c^p} is modular. Then thanks to Definition 4.2.16 of modularity, there exists a newform $f \in S_2(\Gamma_0(N))$ such that $\rho_{E,p} \sim \rho_{f,p}$. Reducing mod p this shows that $\bar{\rho}_{f,p}$ is absolutely irreducible and theorem 4.3.15 states that it has good local properties. Indeed, it shows that $\bar{\rho}_{E,p}$ is unramified outside 2 and p and flat at p since $2 \in \mathbf{Z}_\ell^*$ for every prime $\ell \neq 2$ and hence $v_\ell(\Delta_{a^p,b^p,c^p}) = 2pv_\ell(abc)$ and therefore it is divisible by p. It follows that the hypothesis of the following theorem, that is a particular case of Serre's conjecture known as epsilon conjecture (nowadays Ribet's theorem) hold.

Theorem 4.7.5. *Let f be a weight 2 newform, with rational coefficients of level $\Gamma_0(N\ell)$, with $\gcd(N,\ell) = 1$ and suppose that*

- *$\bar{\rho}_{f,p}$ is absolutely irreducible;*
- *either $\bar{\rho}_{f,p}$ is unramified at ℓ or $\ell = p$ and $\bar{\rho}_{f,p}$ is flat at p.*

Then there is another weight 2 newform g with rational coefficients of level $\Gamma_0(N)$ such that $\bar{\rho}_{g,p} \sim \bar{\rho}_{f,p}$.

Inductively applying Ribet's theorem we find then another modular form $g \in S_2(\Gamma_0(2))$ such that $\bar{\rho}_{g,p} \sim \bar{\rho}_{f,p} \sim \bar{\rho}_{E,p}$. But the dimension of $S_2(\Gamma_0(2))$ is known to be equal to the genus of $X_0(2)$, that is 0, therefore there isn't such a g and we are led to a contradiction, finally proving FLT.

It is interesting to spend some words about Serre's conjecture. Formulated between 1975 and 1987, it states that, given a prime p and a mod p Galois representation satisfying certain conditions, it arises from a modular form. The conjecture comes into two parts, a weaker existence statement and another refined form that makes exact predictions about a modular form from which the Galois representation arises. The refined form, known as Epsilon Conjecture, can be stated in the following way.

Conjecture 4.7.6 (Serre's Epsilon Conjecture)**.** *Let*

$$\bar{\rho}\colon G_{\mathbf{Q}} \longrightarrow \mathrm{GL}_2(\mathbf{F}_p)$$

be a continuous, odd and irreducible residual representation. Let $N(\bar{\rho})$ be its condutor and $\epsilon(\bar{\rho})\colon (\mathbf{Z}/N(\bar{\rho})\mathbf{Z})^* \longrightarrow \mathbf{F}_p^*$ a character. Then there exists a normalised eigenform

$f \in S_{k(\bar{\rho})}(N(\bar{\rho}), \epsilon(\bar{\rho}))$[14] whose associated mod p *Galois representation is equivalent to $\bar{\rho}$. Moreover $N(\bar{\rho})$ and $k(\bar{\rho})$ are the minimal level and weight for which there exists such a newform.*

Nowadays Serre's conjectures have been proved by the mathematicians Khare, Wintenberger, and Kisin (see [10]) in 2009.

[14]The weight $k(\bar{\rho})$ is a natural number that only depends on the restriction of $\bar{\rho}$ to the inertia subgroup I_p.

Bibliography

[1] Michael F. Atiyah and I. G. Macdonald. Introduction to commutative algebra. Reading, Mass.-Menlo Park, Calif.-London-Don Mills, Ont.: Addison-Wesley Publishing Company (1969)., 1969.

[2] Gary Cornell, Joseph H. Silverman, and Glenn Stevens, editors. *Modular forms and Fermat's last theorem. Papers from a conference, Boston, MA, USA, August 9–18, 1995*. New York, NY: Springer, paperback ed. edition, 2000.

[3] Henri Darmon, Fred Diamond, and Richard Taylor. Fermat's Last Theorem. In *Current developments in mathematics, 1995. Lectures of a seminar, held in Boston, MA, USA, May 7-8, 1995*, pages 1–107 (1–154, preliminary version 1994). Cambridge, MA: International Press, 1995.

[4] Fred Diamond and Jerry Shurman. *A first course in modular forms*, volume 228 of *Grad. Texts Math.* Berlin: Springer, 2005.

[5] Fernando Q. Gouvêa. Deformations of Galois representations. In *Arithmetic algebraic geometry. Expanded lectures delivered at the graduate summer school of the Institute for Advanced Study/Park City Mathematics Institute, Park City, UT, USA, June 20–July 10, 1999*, pages 233–406. Providence, RI: American Mathematical Society (AMS), 2001.

[6] Haruzo Hida. *Modular forms and Galois cohomology*, volume 69 of *Camb. Stud. Adv. Math.* Cambridge: Cambridge University Press, paperback reprint of the 2000 original edition, 2008.

[7] B. Mazur. Deforming Galois representations. Galois groups over $\mathbb{Q}$, Proc. Workshop, Berkeley/CA (USA) 1987, Publ., Math. Sci. Res. Inst. 16, 385-437 (1989)., 1989.

[8] Barry Mazur. An introduction to the deformation theory of Galois representations. In *Modular forms and Fermat's last theorem. Papers from a conference,*

Boston, MA, USA, August 9–18, 1995, pages 243–311. New York, NY: Springer, 1997.

[9] James S. Milne. Algebraic number theory (v3.08), 2020. Available at www.jmilne.org/math/.

[10] Michael M. Schein. Serre's modularity conjecture. In *Special issue: Proceedings of the Winter School on Galois theory, Universtity of Luxembourg, Luxembourg, February 15–24, 2012. Vol. II*, pages 139–172. Luxembourg: University of Luxembourg, Faculty of Science, Technology and Communication, 2013.

[11] M. Schlessinger. Functors of Artin rings. *Trans. Am. Math. Soc.*, 130:208–222, 1968.

[12] Jean-Pierre Serre. *Corps locaux*. Paris: Hermann, Éditeurs des Sciences et des Arts, 4th corrected ed. edition, 2004.

[13] Joseph H. Silverman. *The arithmetic of elliptic curves*, volume 106 of *Grad. Texts Math.* Springer, Cham, 1986.

[14] Joseph H. Silverman. *Advanced topics in the arithmetic of elliptic curves*, volume 151 of *Grad. Texts Math.* New York, NY: Springer-Verlag, 1994.

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

[16] Andrew Wiles. Modular elliptic curves and Fermat's Last Theorem. *Ann. Math. (2)*, 141(3):443–551, 1995.

Ringraziamenti

Ed eccomi arrivata qui, alla fine di un percorso travagliato, ma che mi ha dato infinite soddisfazioni e mi ha riempito il cuore. Quasi un anno fa tornavo dall'Australia, piena di dubbi ed emozioni. Pensavo che la matematica non facesse più per me, pensavo di essermi dimenticata tutto quello che avevo imparato, pensavo che l'università non mi avrebbe più accolto come prima. Piano piano, ho scoperto che erano tutte paure senza senso perchè la passione per la matematica era tornata più forte di prima: vendere gelati (buonissimi) per sei mesi mi aveva fatto capire che studiare e laurearmi era quello che più desideravo veramente. Per questo, prima di tutto mi sento di ringraziare l'Australia, una terra che mi ha dato tanto, ma che soprattutto mi ha fatto ritrovare me stessa. A lei mi sento di dire: ci vediamo presto, ma questa volta a studiare matematica (e certamente anche a fare party negli ostelli). Direi che l'Australia si è già presa abbastanza spazio nei miei ringraziamenti. Ora procediamo.

Vorrei ringraziare i miei relatori, il professore Stefano Vigni e il dottor Luca Mastella.

Ringrazio Stefano per aver visto in me tanta potenzialità, in un momento in cui io non la vedevo, e per avermi aiutato a riappassionarmi alla matematica. Anche se non farò il dottorato con lui, spero che questa tesi sia solo l'inizio di tanta altra matematica insieme.

Ringrazio Luca per avermi insegnato tantissime cose nuove e per essere stato sempre disponibile, senza di lui il lavoro sarebbe stato sicuramente più difficile. Grazie per avermi seguito così scrupolosamente.

Vorrei ringraziare la mia famiglia, mia mamma, mio papà e le mie tre sorelle.

Grazie mamma, senza di te non sarei mai arrivata a questo traguardo. Grazie per avermi salvato la vita, quando io non mi stavo accorgendo di tutto quello che stavo perdendo. Anche se litighiamo e saremo lontane, il nostro rapporto non cambierà mai.

Grazie papà per essere stato uno dei miei più grandi fan fin dalle scuole elementari. Grazie per aver supportato tutte le mie manie di perfezionismo senza mai arrabbiarti

(o quasi). Anche se non ci vediamo spesso, so quando sei fiero di me.

Grazie Rebecca per essere la mia migliore amica. Senza di te niente sarebbe stato lo stesso. Sono fiera di te, spacca il mondo.

Grazie Laura per il tuo affetto a volte un po' nascosto. Sappi che sei fortissima, ti sosterrò sempre ovunque andrai e ovunque sarai io sarò con te. Siamo tanto simili quanto diverse. Ti voglio tanto bene.

Grazie Camilla per la tua infinita dolcezza. Grazie per i tuoi abbracci e per i tuoi baci che hanno alleggerito questi anni e soprattutto i momenti difficili. Ti voglio bene, sappi che ovunque sarò sarai la prima persona che penserò al mattino.

Ringrazio mia nonna Nina, perchè anche se negli ultimi due anni siamo state distanti, ha sempre creduto in me.

Grazie Lucci per essere stata sempre presente in tutti i miei traguardi e quelli delle mie sorelle. Sei come una seconda mamma per noi.

E ora i miei fantastici amici.

Ringrazio la mia migliore amica Greta per essere stata sempre al mio fianco, nella felicità e nelle difficoltà. La ringrazio per essere il mio porto sicuro in cui rifugiarmi sempre e per volermi incodizionatamente bene come una sorella.

Grazie agli amici che l'università mi ha fatto incontrare, grazie a voi ho scoperto che oltre lo studio la vita è fatta di tanto altro. Grazie Lollo per l'amore che hai sempre investito nella nostra amicizia. Anche se con il tempo ci siamo un pochino distaccati, sappi che sarai sempre uno dei regali più grandi che l'università mi ha fatto, insieme a Greta. Grazie Greta per i tuoi gossip, per i tuoi infiniti incoraggiamenti, per i tui sorrisi e per il tuo pizzico ti pazzia. Grazie Virgi, perchè anche se non ci vediamo quasi mai, parlare con te mi arrichisce sempre e mi fa sentire speciale. Grazie Gloria per essere diventata una vera amica, per essere il mio portafortuna speciale e per esserci stata sempre in questo ultimo periodo (grazie perchè non ti dà fastisdio quando mi autoinvito hihihi). Grazie Izzi per tutto il supporto che mi hai dato, per capirmi sempre e aiutarmi con la mia ansia. Grazie FraBrazz per i tuoi stritolamenti di polso mattutini, con cui mi hai dimostrato tanto affetto. Grazie Cricco per avermi fatto ridere tanto, ti voglio bene. Grazie Atti per tutte gli esercizi che con pazienza mi hai spiegato e per l'autostima che mi hai trasmesso. Grazie Fede per tutte le giornate passate in uni a ripetere e condividere una lavagna.

Grazie a tutti quei pazzerelli che hanno deciso di studiare matematica come me, facendo parte di questi anni bellissimi.

Grazie alle Gazzelle, che mi hanno accolto tornata dall'Australia, facendomi capire che l'Università era il mio posto nel mondo.

Grazie Nati per la tua tenerezza e genuinità, grazie per i tuoi consigli e il tuo amore. Grazie Andre per avermi accolto tra i tuoi amici col sorriso, sei importante per me.

Thanks again to Australia because it made me meet a beautiful girl: Eilish. Thanks to have been with me even if so far away, I love you. Thank you Cork to make me meet precoius friends and live one the best experience of my life. Thanks to my O12 family, Afra, Davide, Hugo and Matteo and to my amazing Kerry girls, Afra, Julie and Julia. Even if we don't see each other often you are always in my hearth and I'll keep forever all our splendid memories together.

Infine voglio ringraziare Marcello per avermi insegnato ad amare. Ti amo e non desidero altro che crescere e scoprire nuove cose insieme. Il mondo ci aspetta.

Vi voglio bene, conquistate il mondo, la vostra Greta.